

**KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN MẠNG & TT**

Lê Khánh Dương (Chủ biên)

Nhóm biên soạn:

- Đỗ Đình Cường
- Lê Tuấn Anh

**GIÁO TRÌNH
HỆ ĐIỀU HÀNH MẠNG
(Hệ Cao đẳng)**

THÁI NGUYÊN 2007

CHƯƠNG 1: GIỚI THIỆU HỆ ĐIỀU HÀNH WINDOWS 2000 SERVER

1. Tổng quan về Windows 2000 server

Windows 2000 Server là một hệ điều hành mạnh với nhiều tính năng. Dưới đây là một vài tính năng chính:

Active Directory, dựa trên cơ sở là DS (chuẩn x.500) cung cấp những kiến trúc mạng có thể thay đổi, sử dụng dịch vụ đơn cung cấp cho một vài đối tượng hay hàng ngàn dịch vụ với hàng triệu đối tượng.

- ✓ Giao tiếp quản lý gọi là MMC cho phép tùy chỉnh bởi người quản lý, cung cấp những công cụ quản lý được yêu cầu trong cơ cấu logic.
- ✓ Cài tiến phần cứng, bao gồm khả năng Plug-and-play và Hardware Wizard làm cho việc cài đặt phần cứng trở nên thuận tiện hơn.
- ✓ Dịch vụ quản lý File bao gồm những tính năng phân phối file hệ thống. Nâng cao tính bảo mật với EFS và khả năng thiết lập những vùng đĩa được chỉ định cho số lượng lớn người dùng.
- ✓ Tính an toàn cao với tiện ích Security Configuration and Analysis, giao thức Kerberos (truy nhập nguồn tài nguyên trong Windows 2000 domain) và IP Security Protocol cùng các cam người dùng thông minh.
- ✓ Khả năng cung cấp điều khiển hệ điều hành, cài đặt thông qua dịch vụ disk imaging.
- ✓ Tính năng offline tệp tin và thư mục, tự động cài đặt và sửa chữa những ứng dụng mạng và khả năng điều khiển Desktop của người dùng bằng cấu hình của Desktop.
- ✓ Dịch vụ thiết bị đầu cuối cho phép từ Desktop truy nhập mạng máy tính sử dụng tính năng xử lý mạnh mẽ của máy chủ.
- ✓ Kết nối Internet với Internet Information Service (IIS).
- ✓ Sẵn có tùy chọn khôi phục hệ thống bằng Startup and Recovery.

Windows 2000 Server có 3 phiên bản khác nhau, và ta có thể lựa chọn phiên bản nào phù hợp nhất cho công việc của mình:

Windows 2000 Server: được thiết kế để sử dụng cho các công ty nhỏ và vừa.

Windows 2000 Advance Server và Datacenter được thiết kế dành cho các công ty cỡ vừa và cỡ lớn, hoặc các nhà cung cấp dịch vụ Internet ISPS.

Windows 2000 Server: Có tất cả các tính năng chính của Windows 2000. Windows 2000 Server có các dịch vụ như file and print các dịch vụ ứng dụng, dịch vụ

web và truyền thông bao gồm:

- Tính bảo mật cao bởi khoá Keberos và khoá cơ sở công khai.
- Thiết bị đầu cuối.
- 4GB bộ nhớ.
- 2 bộ xử lý trên phiên bản cài đặt mới và 4 cách đa xử lý đối xứng (SMP) hỗ trợ các dịch vụ có thể Upgrade từ Windows NT.

Windows 2000 Advance Server: Có nhiều tính năng mạnh hơn nữa, được thiết kế cho các điều hành cỡ vừa và cỡ lớn. Nó có tất cả các ưu điểm của Windows 2000 Server và hơn thế nữa:

- Tải mạng đối xứng.
- Dịch vụ Cluster cho các ứng dụng chấp nhận lỗi.
- Cung cấp 8GB bộ nhớ.
- Có 8 cách hỗ trợ SMP.

Windows 2000 Datacenter Server: Windows 2000 Datacenter Server là dịch vụ mạnh nhất trong bộ Server. Hệ điều hành này được thiết kế đáp ứng cho 1 số lượng lớn các công việc trên mạng. Windows 2000 Datacenter Server bao gồm tất cả các tính năng của Windows 2000 Advance Server và còn:

- Nhiều hơn các dịch vụ cung cấp Cluster cao cấp.
- 64GB bộ nhớ.
- 16 cách hỗ trợ SMP (Phiên bản OEM có thể có đến 32 cách).

Chú ý: Tất cả các tính năng của Windows 2000 Server đều có trong Windows 2000 Advance Server và Windows 2000 Datacenter Server.

2. Hướng dẫn cài đặt window 2000 Server

a) Yêu cầu cấu hình phần cứng

Bảng 1.1

Thành Phần	Yêu cầu tối thiểu	Khuyến cáo
Bộ xử lý	Pentium 133MHZ hoặc cao hơn.	Pentium 166MHZ hoặc cao hơn.
Bộ nhớ trong	128MB	256MB

Đĩa trống	2GB đĩa cứng với 1 GB trống (cần nhiều hơn nếu muốn cài đặt Windows 2000 Server từ trên mạng xuống).	Tùy thuộc vào các ứng dụng và dữ liệu mà ta muốn lưu trữ trên máy.
Mạng	Không cần	Card mạng và bất cứ thiết bị nào khác được yêu cầu tùy theo tình trạng mạng (nếu ta muốn kết nối mạng toàn cầu)
Hiển thị	Bộ điều khiển video và màn hình phân giải VGA.	Bộ điều khiển video và màn hình phân giải VGA hoặc cao hơn.

b) Các bước cài đặt

Phần này sẽ trình bày một số chú ý trong quá trình cài đặt Windows 2000 server.

Kích cỡ, dung lượng đĩa:

Một điều cần quan tâm là cần phải định rõ dung lượng các ổ đĩa của ta. Ta cần lưu ý đến dung lượng phần trống dành cho hệ điều hành, dành cho các ứng dụng khác mà ta sẽ cài đặt, và cuối cùng là dành cho việc lưu trữ dữ liệu.

Đối với Windows 2000 Server, Microsoft khuyến cáo ta nên dành ra ít nhất 1GB phần trống. Dung lượng phần trống này cho phép chứa đựng các file của hệ điều hành và giới hạn các file sẽ phát sinh trong tương lai khi nâng cấp và cài đặt.

Vùng hệ thống và vùng khởi động:

Khi cài đặt Windows 2000, các file sẽ được lưu trữ ở 2 nơi, đó là vùng hệ thống và vùng khởi động.

Vùng hệ thống chứa đựng những file cần thiết để khởi động hệ điều hành Windows 2000 Server. Những file lưu trữ trong vùng hệ thống chiếm 1 phần không đáng kể phần trống, chúng được mặc định sử dụng vùng tích cực của máy tính, thường là ổ đĩa C:

Vùng khởi động chứa những file của hệ điều hành Windows, và chúng được mặc định đặt tại thư mục có tên là WindowsNT. Tuy nhiên ta cũng có thể thay đổi mặc định này trong quá trình cài đặt. Microsoft khuyến cáo vùng khởi động nên có dung lượng tối thiểu là 1GB.

Lựa chọn file hệ thống:

Một nhân tố khác cũng quyết định kế hoạch tổ chức phân vùng đĩa của ta là loại file hệ thống mà ta sẽ sử dụng. Windows 2000 Server hỗ trợ 3 loại file:

- ✓ FAT 16 (File Allocation Table).

- ✓ FAT 32.
- ✓ NTFS (New Technology File System)

FAT 16: FAT 16 là kiểu file hệ thống 16 bit được sử dụng rộng rãi trong DOS và Windows 3x. Những rãnh ghi trong FAT 16 lưu trữ file trên đĩa sử dụng bảng phân phối file và bảng chỉ dẫn. Với FAT, bảng chỉ dẫn đặt ở rãnh ghi của khối đầu tiên của file, tên file và phần mở rộng, ngày và thời gian và bất cứ giao tiếp nào khác với file.

Sự bất lợi của FAT 16 là nó chỉ hỗ trợ phân vùng với dung lượng khoảng 2GB và nó có tính năng bảo mật an toàn như NTFS.

Sự thuận lợi của FAT là có sự tương thích với những hệ cũ. Điều này rất quan trọng nếu máy tính của ta chạy dual-boot với DOS hay bất kỳ hệ điều hành nào khác. Ví dụ như DOS, Unix, Linux, OS/2, Windows 3.1 và Windows 9x đều thích hợp với FAT 16.

FAT 32: FAT 32 là phiên bản 32 bit của FAT, nó được đưa ra giới thiệu vào năm 1996 với Windows 95, OEM Server Release 2 (OSR2). FAT 32 có nhiều tính năng vượt trội hơn FAT 16:

- ✓ Disk Partition có thể có dung lượng lớn hơn 2TB (terabytes).
- ✓ Nhiều hơn những tính năng bảo vệ được thêm vào để dự phòng những sai sót nếu xảy ra lỗi ổ đĩa.
- ✓ Nó cải tiến cách sử dụng phần trống đã bởi việc thay đổi lại cỡ của cluster

Nhược điểm của FAT 32 là nó thiếu 1 vài tính năng cho Windows 2000 so với NTFS, ví dụ như: bảo mật cục bộ, mã hoá file, trích dẫn đĩa (disk quotas) và nén.

Nếu ta quyết định sử dụng FAT, Windows 2000 sẽ tự động định dạng các partition với FAT 16 nếu dung lượng partition dưới 2GB và FAT 32 nếu dung lượng trên 2 GB .

Chú ý: Windows NT 4 và các phiên bản sớm hơn của NT không hỗ trợ FAT 32.

NTFS: NTFS là những file hệ thống được thiết kế để cung cấp những tính năng thêm vào cho Window NT và Windows 2000. NTFS phiên bản 5 gắn với Window 2000. Dưới đây là các tính năng của NTFS :

- ✓ Khả năng thiết lập bảo mật cục bộ cho file và các thư mục.
- ✓ Các tùy chọn nén dữ liệu. Tính năng này có thể biến đổi, làm giảm bớt phần đĩa lưu trữ ít hơn yêu cầu.
- ✓ Uyển chuyển trong việc quy định đưa trích dẫn disk quotas. Đĩa trích dẫn được dùng để giới hạn số lượng phần trống mà 1 user có thể sử dụng.
- ✓ Tuỳ chọn mã hoá file. Việc mã hoá tăng thêm tính an toàn cho dữ liệu.

Trừ trường hợp ta muốn dual-boot máy của ta với hệ điều hành khác

Windows NT, nếu không, Microsoft khuyên ta nên dùng NTFS.

Kiểu giấy phép:

Có 2 cách chính để được cấp phép. Ta trả tiền cho hệ điều hành địa phương, và ta trả cho khách truy nhập. Cách này nên dùng nếu ta chạy Windows 2000 Server như một dịch vụ của ta và Windows 2000 Professional và Windows 98 cho khách hàng của ta. Ta phải lấy giấy phép cho hệ điều hành và với mỗi máy tính cá nhân. Ta cũng phải có giấy phép truy nhập dịch vụ mạng.

Khi cài đặt Windows 2000 Server, ta phải chọn giữa giấy phép Per Server và Per Seat. Per Server sẽ chỉ ra số lượng kết nối mạng hiện tại có thể được làm bởi một máy chủ. Per Seat chỉ ra mỗi máy khách được cấp phép và mỗi máy khách có thể truy nhập nhiều máy chủ mà nó cần.

Ta nên chọn loại Per Server nếu những người dùng của ta chỉ truy nhập một máy chủ tại một thời điểm. Ví dụ: ta có 10 người dùng và một máy chủ, sẽ rẻ hơn nếu ta lựa chọn Per Server thay vì Per Seat. Nếu những người dùng của ta truy nhập nhiều hơn một máy chủ tại cùng một thời điểm, ta nên chọn Per Seat. Ví dụ ta có 10 người dùng và 2 máy chủ, với kiểu Per Seat, ta chỉ cần mua 10 giấy phép gọi là Client Access Licenses (CALS). Nếu ta dùng Per Server, ta cần 10 giấy phép cho mỗi Server.

Thành viên của Domain hoặc của Workgroup:

Một lựa chọn cài đặt Windows 2000 Server để máy tính của ta sẽ trở thành một thành phần của một miền hay một thành phần của một nhóm làm việc.

Ta nên cài đặt như một phần của Workgroup nếu ta là một thành phần của một nhóm nhỏ, phân quyền hóa mạng máy tính hay ta chạy Windows 2000 Server mà không kết nối mạng. Để ra nhập một Workgroup, đơn giản ta chỉ việc chọn Workgroup đó.

Domains là một phần rộng hơn với quyền quản lý mạng trung tâm. Ta nên cài máy tính của mình như một thành phần của một Domain nếu bắt cứ một máy chủ Windows 2000 Server nào trên mạng của ta cũng đều được cấu hình theo Domain Controller với Active Directory đã được cài đặt. Để ra nhập một Domain, ta phải chỉ ra tên chính xác của Domain và cung cấp 1 tên người dùng (username) và mật khẩu người dùng để kết nối thêm máy tính của ta vào Domain. Một bộ điều khiển miền của Domain và máy chủ Domain Name System (DNS) phải có sẵn để xác nhận khi gia nhập Domain.

Nâng cấp một Member Server lên Domain Controller:

Một Server đã được cài đặt thành công với hệ điều hành Windows 2000, ta có thể nâng cấp từ Server lên Domains Controller bằng cách sử dụng tiện ích DCPROMO. Ta có thể chỉ ra Server nào là Domain Controller đầu tiên trong domains mới hoặc thêm nó từ một domain sẵn có. Nếu ta sẵn có Active Directory cài đặt trên mạng của ta, ta

có thể tạo mới một domains.con với một cây domains có sẵn hay cài đặt một cây domains như một phần của 1 rừng đã có sẵn.

Các bước trong phần này xem như ta đã tạo một domains controller đầu tiên trong domains mới, và ta đang cài Active Directory lần đầu tiên. Những bước này cũng xem như DNS vẫn chưa được định cấu hình cho mạng của ta.

Để nâng cấp từ Server lên Domán Controller, ta hãy làm theo các bước sau:

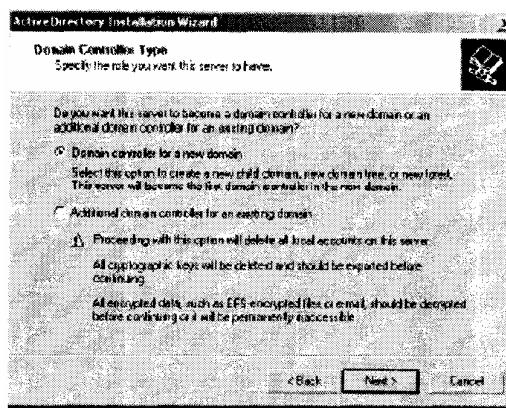
1. Chọn Start > Run, gõ DCPROMO trong hộp thoại Run, và nhấn OK.
2. Chương trình Active Directory Installation Wizard bắt đầu. Ta nhấn vào nút Next như trong hình 1.1 .

Hình 1.1



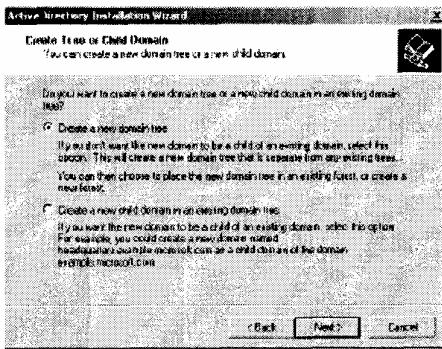
3. Hộp thoại Domain Controller Type xuất hiện, xem hình 1.2. Chọn Domain Controller ở tuỳ chọn New Domain và nhấn Next. Nếu ta muốn thêm domain controller tới một domain có sẵn, ta chọn tuỳ chọn Additional Domain Controller for an Existing Domain.

Hình 1.2



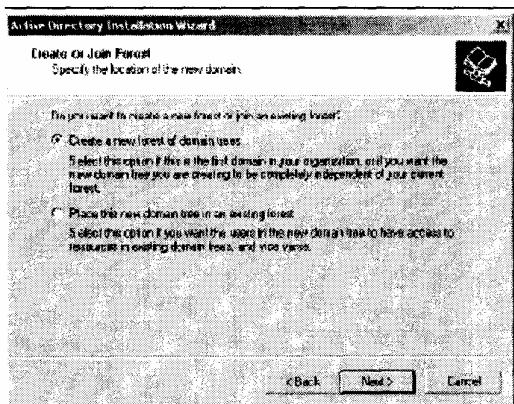
4. Hộp thoại Create Tree or Child Domain xuất hiện. Để tạo một domain tier mới, chọn tuỳ chọn Create a New Domain Tree và nhấn nút Next như trong hình 1.3 (Nếu ta đã cài đặt sẵn Active Directory trên mạng của mình và ta muốn tạo mới một cây domain con trong một cây domain đã có sẵn, ta chọn tuỳ chọn "Create a New Child Domain in an Existing Domain Tree").

Hình 1.3



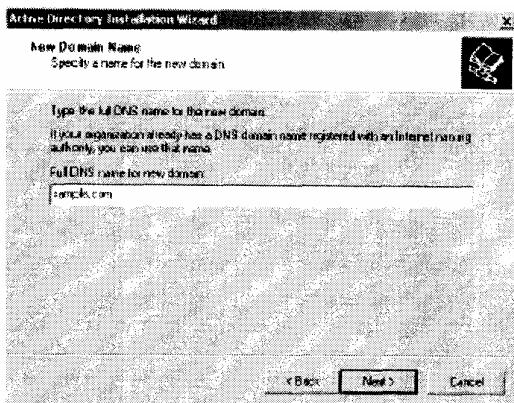
5. Hình 1.4 là hộp thoại Create or Join Forest. Chọn tùy chọn "Create a New Forest of Domain Trees" và nhấn vào nút Next. (Nếu ta đã có sẵn Active Directory trên mạng của mình và muốn cây domain sẽ được cài đặt như là một phần của một *rừng* đã có sẵn, ta chọn "Place This New Domain Tree" trong tùy chọn Existing Forest).

Hình 1.4



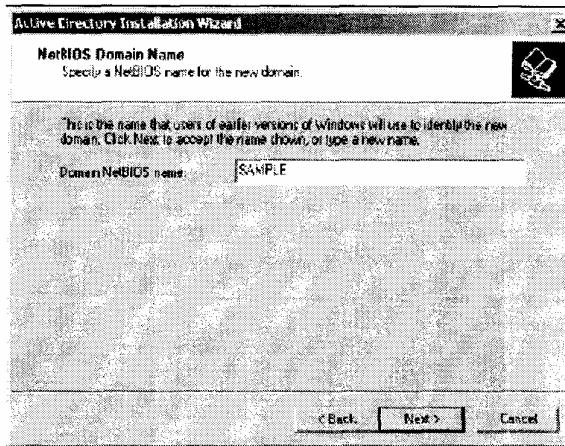
6 . Hộp thoại New Domain Name xuất hiện như trong hình 1.5 , chỉ ra tên DNS đầy đủ cho domain mới. Ví dụ như sampledomain.com và nhấn nút Next để tiếp tục. Thông thường DNS được định cấu hình cho mạng trước khi ta tạo một domain controller.

Hình 1.5



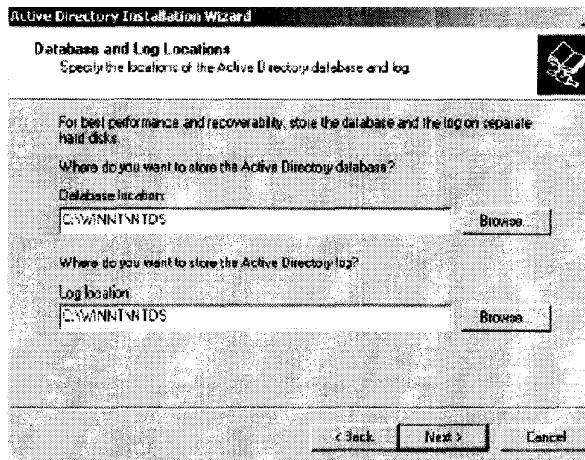
7. Tiếp đến là hộp thoại NetBIOS Domain Name như trong hình 1.6 Tên NetBIOS Domain được sử dụng để thuận tiện với máy trạm dùng WinNT. Mặc định là tên domain NetBIOS được đặt giống như tên DNS. Ta có thể thay đổi bằng một tên khác hoặc là chấp nhận cái tên mặc định này. Nhấn Next để tiếp tục.

Hình 1.6



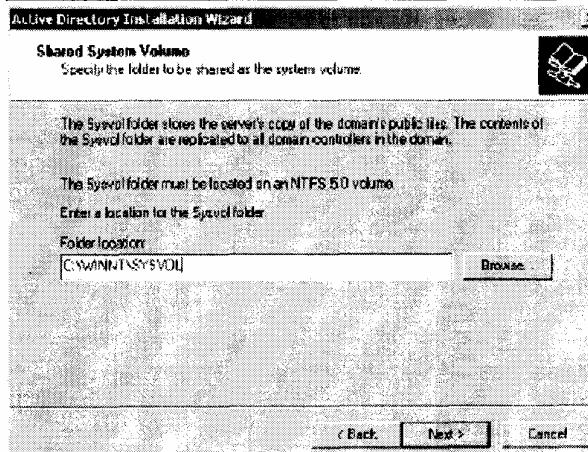
8. Sau đó là đến hộp thoại Database and Log Locations như trong hình 1.7 Hộp thoại này cho phép ta xác định vị trí của cơ sở dữ liệu Active Directory và các file sổ ghi cơ sở dữ liệu. Ta có thể chấp nhận vị trí mặc định cho những file này hoặc lựa chọn một vị trí khác. Sau đó ta nhấn nút Next.

Hình 1.7



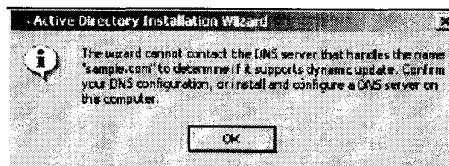
9. Hộp thoại Shared System Volume sẽ xuất hiện như trong hình 1.8. Volume này phải là NTFS 5 volume. Ta có thể chấp nhận vị trí thư mục mặc định hoặc là lựa chọn một thư mục khác. Sau đó nhấn Next (Nếu partition không phải là NTFS 5, ta sẽ thấy thông báo lỗi chỉ ra rằng file hệ thống phải được chuyển đổi).

Hình 1.8



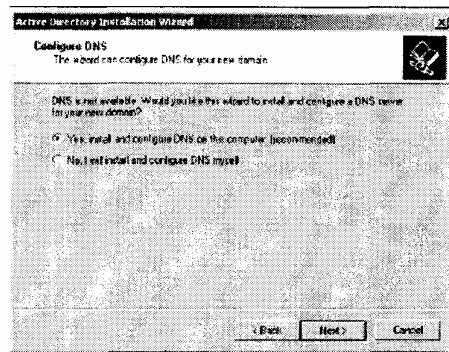
10. Nếu DNS vẫn chưa được định cấu hình, ta sẽ thấy thông báo bắt đầu rằng dịch vụ DNS không thể định vị được như trong hình 1.9 Nhấn nút OK để tiếp tục.

Hình 1.9



11. Hộp thoại Configure DNS xuất hiện như trong hình 1.10. Để định cấu hình DNS, chọn tùy chọn Yes, Install and Configure DNS on This Computer (Recommend). Nếu ta muốn tự cài đặt DNS (bằng tay) chọn tùy chọn No, I Will Install and Configure DNS Myself. Sau khi ta đã tạo ra lựa chọn của mình, nhấn Next để tiếp tục.

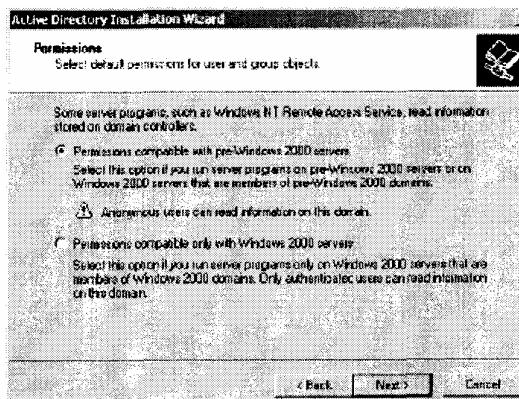
Hình 1.10



12. Hộp thoại Permissions xuất hiện như trong hình 1.11 Nếu ta muốn có thể sử dụng các chương trình máy chủ trên máy chủ để chạy các phiên bản trước đó của Windows hoặc trong một domain điều hành các phiên bản trước đây của Windows chọn tùy chọn Permissions Compatible with pre-windows 2000 Server. Các trường hợp khác, lựa chọn tùy chọn Permissions Compatible giầy with Windows 2000 Server.

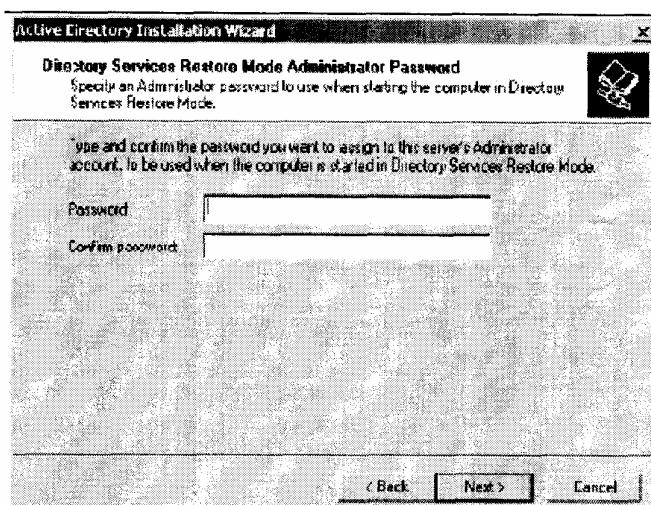
sau đó, nhấn Next để tiếp tục.

Hình 1.11



13. Tiếp đến là hộp thoại Directory Services Restore Mode Administrator Password như trong hình 1.12 Hộp thoại này cho phép ta xác định password có thể sử dụng khi máy chủ cần khởi động lại ở chế độ Directory Services Restore Mode. Nhập lại password một lần nữa để xác nhận và nhấn nút Next.

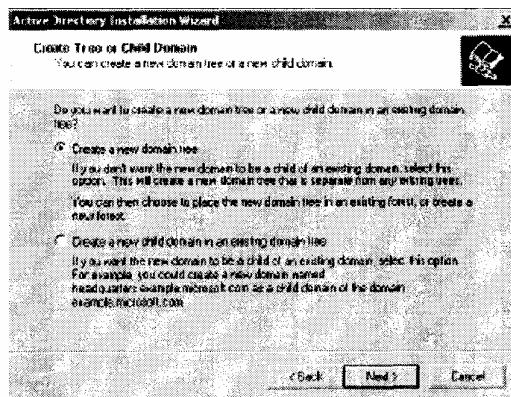
Hình 1.12



Chú ý: Directory Services Restore Mode là một tùy chọn trên trình đơn Advanced Options, có sẵn khi Windows 2000 khởi động. Xem chương 15 để biết thêm chi tiết về những tùy chọn khác của Advanced Options này.

14. Sau đó là đến hộp thoại Summary như trong hình 1.13 Hộp thoại này cho phép ta xác nhận lại tất cả các lựa chọn ta đã làm. Nếu tất cả các thông tin đều chính xác, nhấn Next.

Hình 1.13



15. Ta sẽ nhìn thấy hộp thoại Configuring Active Directory để ta biết rằng Wizard đang định cấu hình Active Directory và quá trình này có thể mất vài phút. Sau đó ta sẽ được nhắc đưa đĩa CD Windows 2000 Server của ta vào để copy thêm các file cần thiết. Cho đĩa CD vào Ổ CD-ROM và nhấn OK.

16. Hộp thoại Configuring Active Directory xuất hiện. Khi quá trình này hoàn thành, hộp thoại Completing the Active Directory Installation Wizard xuất hiện như trong hình 1.14 Nhấn Finish.

Hình 1.14



17.Ta sẽ được nhắc khởi động tại Windows 2000 để thay đổi các ảnh hưởng. Nhấn Restart Now.

CHƯƠNG 2 : QUẢN TRỊ NGƯỜI DÙNG

(8 tiết lý thuyết)

1. Giới thiệu về tài khoản người dùng

Một trong những nhiệm vụ cơ bản nhất trong việc quản trị mạng là tạo ra những tài khoản người dùng và nhóm người dùng. Khi không có tài khoản thì người dùng không thể đăng nhập vào hệ thống máy tính, khi không có tài khoản nhóm sẽ khiến quản trị viên khó có thể phân quyền người dùng trong việc truy cập và khai thác tài nguyên của hệ thống một cách chặt chẽ và linh hoạt.

1.1. Tổng quan về tài khoản người dùng

Trong Windows 2000 server hỗ trợ hai kiểu người dùng: người dùng cục bộ và người dùng Active Directory. Một máy tính đang sử dụng hệ điều hành Windows 2000 server (được cấu hình là một máy chủ) có khả năng tự lưu trữ cơ sở dữ liệu tài khoản người dùng. Những người dùng được lưu trữ trong những máy cục bộ được gọi là người dùng địa phương.

Active Directory là một dịch vụ thư mục được tích hợp sẵn trong Windows 2000 Server. Nó chứa thông tin trong một cơ sở dữ liệu trung tâm cho phép người dùng có thể có một tài khoản đơn lẻ trên mạng. Những người dùng hay nhóm người dùng được lưu trong Active Directory được gọi là người dùng Active Directory hay người dùng miền.

1.2. Các tài khoản người dùng có sẵn

Khi cài đặt Windows 2000 Server, có một số tài khoản mặc định được tạo sẵn.

Bảng 2.1 Các tài khoản mặc định

Người dùng định sẵn	Mô tả	Phạm vi
Administrator	Tài khoản Administrator là một tài khoản đặc biệt có quyền đầy đủ đối với máy tính	Cục bộ hay miền (local Domain)
Guests	Cho phép người dùng truy cập vào máy tính ngay cả khi không có username và password. Tài khoản này mặc định bị vô hiệu hóa, khi tài khoản này được phép sử dụng thì cũng chỉ được cung cấp một số quyền hạn chẽ.	Local và Domain
ILS_Anonymous User	Là một tài khoản đặc biệt của dịch vụ ILS, ILS hỗ trợ môi trường telephony với các tính năng như hội nghị qua vi deo, fax... để sử dụng dịch vụ này cần cài đặt IIS.	Domain

IUSR-computername	Là tài khoản đặc biệt để truy cập nặc danh vào IIS ở những máy có cài IIS	Local và Domain
IWAM-computername	Tài khoản này là tài khoản đặc biệt được dùng cho IIS để bắt đầu một ứng dụng trên một máy có cài đặt IIS	Local và Domain
Krbtgt	Tài khoản này dùng cho dịch vụ Key Distribution Center.	Domain
TSInternetUser	Là tài khoản dành Terminal Service.	Domain

Theo mặc định thì tên tài khoản Administrator được trao cho tài khoản có quyền đầy đủ với hệ thống. Có thể tăng cường an ninh của hệ thống bằng cách đổi tên tài khoản Administrator sau đó tạo ra một tài khoản có tên là Administrator nhưng không có quyền gì. Bằng cách này thì ngay cả khi một hacker có thể truy cập vào hệ thống với tên Administrator thì cũng không thể truy cập tới bất cứ tài nguyên nào của hệ thống.

1.3. Tổng quan về tài khoản nhóm

Trên một máy chủ Windows 2000, chỉ có thể sử dụng những nhóm cục bộ. Một nhóm cục bộ sẽ lưu trong csdl của máy chủ Windows 2000.

Trên Windows 2000 Domain controller trong Active Directory, có thể có những nhóm "an toàn" (security) và những nhóm "chia" sẽ (distribution). Một nhóm an toàn là một nhóm những người dùng mà chỉ truy cập đến một số tài nguyên xác định. Sử dụng nhóm người dùng an toàn gán quyền truy cập cho những tài nguyên. Một nhóm chia sẻ là một nhóm những người dùng có những đặc điểm chung. Nhóm chia sẻ có thể được dùng bởi những chương trình ứng dụng và thư điện tử. Windows 2000 domain controller cho phép lựa chọn phạm vi của nhóm có thể là domain, global hoặc universal. Mỗi kiểu phạm vi được sử dụng như sau:

- ✓ Những nhóm vùng cục bộ được dùng để xác lập quyền truy xuất đối với các tài nguyên. Những nhóm cục bộ có thể chứa những tài khoản người dùng, những nhóm dùng chung và những nhóm toàn cục từ bất cứ vùng nào. Một nhóm vùng cục bộ cũng có thể chứa những nhóm vùng cục bộ khác trong vùng của mình.
- ✓ Nhóm toàn cục được dùng để tổ chức những người dùng có những yêu cầu truy cập tương tự nhau. Nhóm toàn cục có thể chứa những người dùng và nhóm toàn cục từ vùng địa phương.
- ✓ Nhóm đa năng được sử dụng để tổ chức người dùng và xuất hiện trong danh mục toàn cầu (một danh sách đặc biệt chứa những thông tin về tất cả các đối tượng trong Active Directory).

Trên các máy tính cài Windows 2000 Professional và Windows 2000 server, tạo

ra và quản lý những nhóm cục bộ thông qua tiện ích Local User and Groups - Trên Windows 2000 Server domain controller việc quản lý những nhóm người dùng thông qua tiện ích Microsoft Active Directory Users and Computers.

1.4 Tài khoản nhóm có sẵn

Khi cài đặt Windows 2000 Server, có một số tài khoản nhóm được tạo sẵn theo mặc định.

Bảng 2.2

Nhóm định sẵn	Mô tả	Phạm vi
Account Operators	Những thành viên của nhóm Account Operator có thể tạo ra những người dùng và những tài khoản của người dùng và nhóm nhưng họ chỉ có thể quản lý những tài khoản người dùng và nhóm mà họ tạo ra	Domain
Administrators	Nhóm Administrators có đầy đủ những đặc quyền đặc lợi. Những thành viên của nhóm có thể cấp cho mình tất cả những quyền mà theo mặc định họ chưa có để có thể quản lý toàn bộ các đối tượng trên hệ thống (Các đối tượng trên hệ thống bao gồm hệ thống file, máy in, quản lý tài khoản)	Local và Domain
Backup Operators	Các thành viên của nhóm Backup Operator có quyền sao lưu và phục hồi hệ thống file ngay cả khi hệ thống file là NTFS và họ không được cấp quyền về hệ thống file. Tuy nhiên thành viên của nhóm này chỉ có quyền truy cập vào hệ thống file thông qua tiện ích Backup. Để có thể truy cập trực tiếp vào hệ thống file họ phải được cấp quyền truy nhập. Theo mặc định thì không có thành viên nào trong nhóm Backup Operator.	Local và Domain
Guests	Nhóm Guests có quyền rất hạn chế đối với hệ thống. Ta có thể cung cấp tài khoản này cho những người dùng không thường xuyên có thể truy cập tới một số tài nguyên xác định trên mạng. Nói chung thì hầu hết các quản trị viên đều không cho phép quyền truy cập Guest bởi vì tính nguy hiểm của nó. Mặc định thì tài khoản người dùng Guest là thành viên của	Local và Domain

	nhóm Guest.
Power Users	Nhóm Power User có ít quyền hơn nhóm Local Administrators nhưng nhiều quyền hơn nhóm User. Power User có thể tạo ra người dùng và nhóm nhưng cũng chỉ có quản lý những người dùng và nhóm người dùng do nó tạo ra. Nó cũng có thể tạo ra sự chia sẻ mạng và máy in.
Print Operator	Thành viên của nhóm này có quyền quản trị Domain máy in.
Replicator	Nhóm này được tạo ra nhằm hỗ trợ việc tái tạo Local và thư mục là một tính năng của máy chủ. Chỉ có Domain những người dùng vùng mới có thể được cấp quyền vào nhóm này. Mặc định là không có thành viên nào trong nhóm này cả
Server Operators	Thành viên nhóm này có thể quản trị các máy Domain chủ vùng.
Users	Nhóm Users được dùng cho những người dùng cuối là những người có quyền truy cập rất hạn chế đối với hệ thống. Nếu ta cài đặt mới Server thì những thiết lập mặc định cho nhóm này sẽ ngăn cản không cho những người dùng trong nhóm có thể phá hỏng hệ điều hành cũng như những file trên máy. Theo mặc định thì toàn bộ người dùng trên hệ thống , trừ Guest, là thành viên của nhóm User.
Cert Publishers	Thành viên của nhóm Cert Publisher có thể Global quản lý những chứng chỉ, chứng nhận của công ty hay các đại lý.
DHCP Administrators	Nhóm DHCP Administrator có quyền quản trị Domain để quản lý máy chủ.
DHCP Users	Nhóm này có những quyền cần thiết để có thể Domain sử dụng các dịch vụ DHCP
DnsAdmins	Nhóm này có quyền quản lý những máy chủ Domain Name System (DNS).
Dnsupdateproxy	Nhóm này có quyền cho phép những máy Global

	khách DNS có thể thực hiện những cập nhật động thay mặt những máy khách khác cũng như là những máy chủ DHCP.
Domain Admins	Nhóm Domain Admins có quyền điều hành Global toàn bộ trên domain.
Domain Computers	Nhóm này chứa toàn bộ những máy trạm và Global máy chủ thuộc về Domain.
Domain Controllers	Nhóm này chứa toàn bộ những điều khiển miền Global trên miền.
Domain Guests	Nhóm này có những quyền truy cập rất hạn chế Global đến miền. Nhóm này được tạo ra nhằm giúp ta có thể cho phép những người dùng không thường xuyên truy cập đến những tài nguyên xác định trên hệ thống...
Domain Users	Nhóm này chứa toàn bộ những người dùng Global miền. Ta nên cấp những quyền rất hạn chế cho nhóm này.
Enterprise Admins	Nhóm này có quyền điều hành toàn bộ trên hệ thống. Nó là nhóm có quyền cao nhất trong tất cả các nhóm
Group Policy Creator Owners	Nhóm này có quyền thay đổi chính sách của Global nhóm đối với miền
RAS and IAS	Chứa những dịch vụ truy cập từ xa (RAS- Domain Server Remote Access Service) và các máy chủ Internet Authentication Service (IAS) trong miền. Những máy chủ trong nhóm này có thể truy cập từ xa đến những thuộc tính của người dùng
Schema Admins	Nhóm có quyền đặc biệt có thể thay đổi lược đồ Global của Active Directory
WINS Users	Nhóm WIN User có quyền đặc biệt có thể xem Domain những thông tin trên các máy chủ Windows Internet Name Service (wins)

Chú ý: Trên một điều khiển miền Windows 2000 Server, các nhóm được đặt trong các thư mục Users và Builtn.

2. Làm việc với các tài khoản người dùng cục bộ

Để cài đặt và quản lý những người dùng cục bộ sử dụng tiện ích Local Users and Groups. Với tiện ích này có xóa bỏ, đặt lại thêm mới người dùng. Và thay đổi mật khẩu của người dùng.

2.1. Sử dụng tiện ích Local Users and Groups

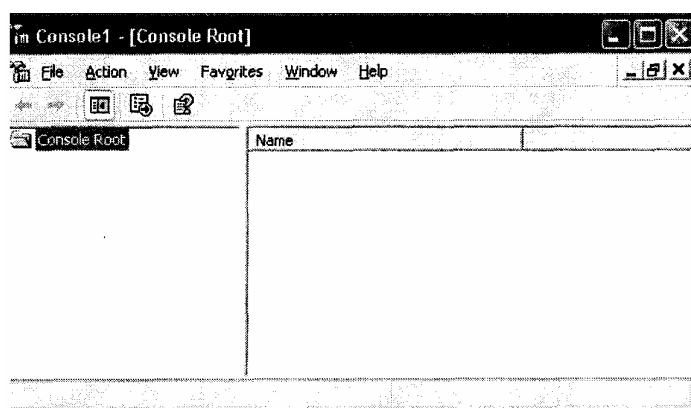
Có hai cách để truy cập đến tài khoản này:

- ✓ Sử dụng Microsoft Management Console (MMC).
- ✓ Sử dụng thông qua Computer Management.

a) Sử dụng MMC

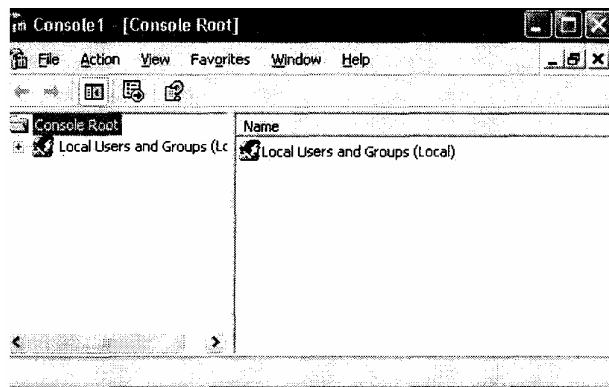
Chọn Start → Run, nhập vào MMC, sau đó nhấn Enter để mở cửa sổ MMC.

Hình 2.1



Chọn file → Add/Remove Snap-in để mở hộp thoại. Chọn Add để mở hộp thoại Add Standard Snap-in. Chọn Local Users and Group và cách vào nút Add. Hộp thoại Choose Target Machine xuất hiện với Local Computer được chọn. Click vào nút Finish. Sau đó quay lại hộp thoại Add Standard Snap-in cách vào nút Close. Sau đó click vào nút OK. Khi đó Local Users and Group được thêm vào MMC .

Hình 2.2

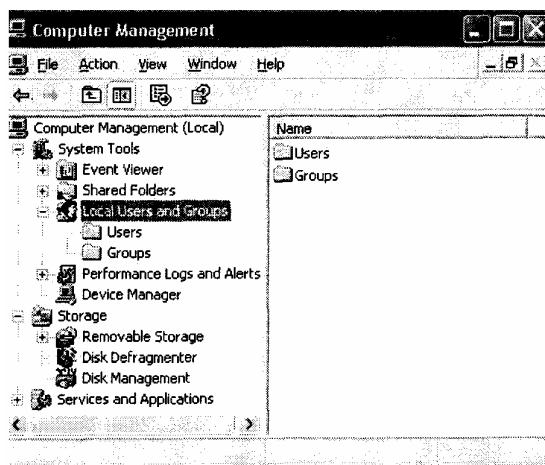


Lưu lại bằng cách chọn Save và đặt đường dẫn (nên để ở Desktop để dễ truy cập).

b) Sử dụng Computer Management

Click chuột phải vào My Computer chọn Manager. Sau đó chọn Local Users and Groups.

Hình 2.3



2.2 Tạo tài khoản người dùng

Để tạo ra người dùng mới trên Windows 2000 Server ta phải đăng nhập vào hệ thống với tư cách là một người dùng có quyền tạo ra người dùng mới và phải là thành viên của nhóm Administrators hoặc là nhóm Power Users.

a) Những quy tắc đặt tên người dùng:

Yêu cầu duy nhất khi tạo ra người dùng mới đó là ta phải cung cấp tên người dùng hợp lệ. Hợp lệ tức là phải tuân theo những quy tắc của Windows 2000 về tên người dùng.

Độ dài tên phải từ 1 đến 20 ký tự.

- ✓ Tên của người dùng phải duy nhất, tức là phải khác với tất cả các tên và nhóm có

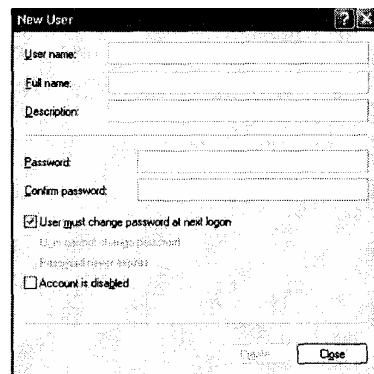
trong hệ thống.

- ✓ Tên người dùng phải không được chứa các ký tự sau: /\[1 : ; 1 = ' + * ? < >"
- ✓ Tên của người dùng không chứa dấu cách.

b) Các tùy chọn đối với tài khoản người dùng mới:

Mở Local User and Group tạo một tài khoản mới.

Hình 2.4



Bảng 2.3 mô tả các tùy chọn trên:

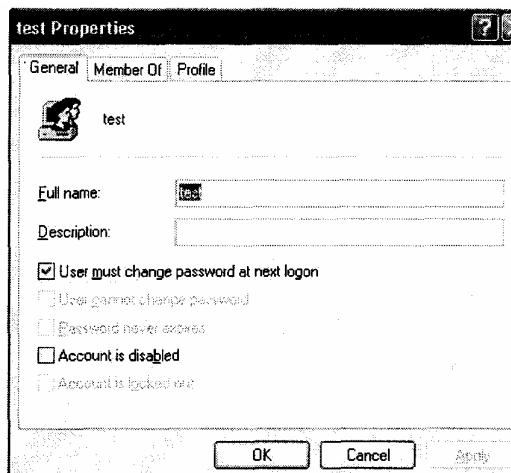
Tùy chọn	Mô tả
User Name	Xác định tên của người dùng.
Full Name	Cung cấp thêm thông tin chi tiết về người dùng
Description	Bổ xung thêm những thông tin phụ.
Password	Mật khẩu của người dùng có thể dài tới 14 ký tự, phân biệt chữ hoa chữ thường
Confirm Password	Xác nhận lại mật khẩu.
User Must Change Password	Nếu mục này được chọn thì hệ thống sẽ bắt người dùng phải thay đổi mật khẩu trong lần đầu tiên đăng nhập.
Password at Next Login	Nhằm tăng tính bảo mật. theo mặc định thì mục này được chọn.
User Cannot Change Password	Nếu mục này được chọn thì người dùng không thể thay đổi mật khẩu, nó hữu ích với các tài khoản Guest. Mặc định mục này không được chọn
Password Never Expires	Nếu chọn mục này thì mật khẩu sẽ không bao giờ hết hiệu lực ngay cả khi chính sách về mật khẩu được thiết lập
Account is Disabled	Nếu chọn thì tài khoản này không thể được dùng để đăng nhập vào hệ thống, chọn mục này cho những tài khoản

mẫu hoặc các tài khoản hiện tại không được sử dụng, nó làm tăng tính bảo mật của hệ thống.

c) Quản lý các đặc tính của người dùng cục bộ:

Để có nhiều điều khiển hơn đối với tài khoản người dùng, có thể thiết lập cấu hình các đặc tính người sử dụng. Thông qua hộp thoại Properties ta có thể thay đổi các tùy chọn mật khẩu ban đầu, thêm một người sử dụng vào nhóm, và chỉ định những thông tin và hiện trạng người sử dụng. Để mở hộp thoại Properties vào tiện ích Local Users and Groups, mở thư mục Users và thao tác chọn tài khoản.

Hình 2.5

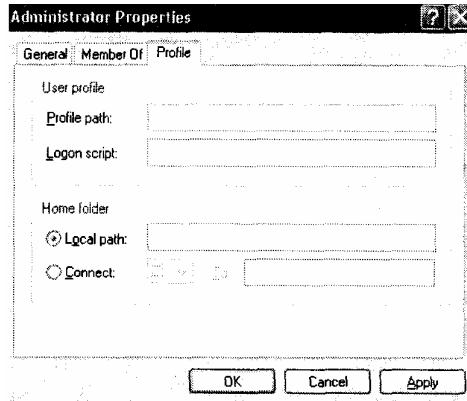


Thẻ General: chứa những thông tin mà ta cung cấp khi tạo tài khoản mới, bao gồm: Full Name (tên đầy đủ), Description, tùy chọn mật khẩu và tài khoản có bị vô hiệu hóa hay không.

Thẻ Member Of: dùng để quản lý tư cách thành viên của các nhóm của người sử dụng (người sử dụng là thành viên của nhóm nào).

Thẻ Profile: cho phép thiết lập các đặc tính để tùy chỉnh môi trường người dùng. Ta có thể chỉ định các mục sau đây cho người sử dụng.

Hình 2.6



- ✓ *Thiết lập đường dẫn hiện trạng (Profile Path):* Hiện trạng người sử dụng chứa các thông tin về môi trường Windows 2000 dành cho từng người dùng cụ thể. Ví dụ: thiết đặt hiện trạng bao gồm sắp xếp màn hình, các nhóm chương trình, màu màn hình người sử dụng nhìn thấy khi đăng nhập. Nếu tùy chọn cấu hình là một sở thích cá nhân, nó gần như sẽ là một phần của hiện trạng người sử dụng. Tuy chọn cấu hình liên quan đến máy tính không phải là một phần của hiện trạng người sử dụng. Ví dụ trình điều khiển chuột không phải là một phần của hiện trạng người sử dụng. Tuy nhiên, các đặc tính của cấu hình chuột như tốc độ, con trỏ, thiết đặt nút chuột phản ánh các sở thích cá nhân, là một phần của hiện trạng người sử dụng. Mặc định, khi người sử dụng đăng nhập, một hiện trạng sẽ được mở ra cho người đó. Lần đầu tiên người sử dụng đăng nhập, họ sẽ nhận được hiện trạng người sử dụng mặc định. Một thư mục trùng với tên đăng nhập của người sử dụng sẽ được tạo ra trong thư mục Documents and Settings. Thư mục hiện trạng người sử dụng chứa một file có tên là NTUSER.DAT và các thư mục con chứa các liên kết tới các biểu tượng trên màn hình của người sử dụng. Bất cứ thay đổi nào trên màn hình của người sử dụng sẽ được lưu trên máy cục bộ khi người sử dụng rời hệ thống. Ví dụ, giả sử người dùng Nam đăng nhập, chọn wallpaper cho anh ta, tạo các lối tắt, tùy chỉnh màn hình theo ý thích của anh ta. Khi anh ta thoát khỏi hệ thống, hiện trạng của anh ta sẽ được lưu lại. Khi một người dùng khác đăng nhập vào cùng máy tính, hiện trạng của người đó (chứ không phải là hiện trạng của Nam) sẽ được nạp. Tùy chọn Profile Path (đường dẫn hiện trạng) trong thẻ Profile được sử dụng để chỉ định một vị trí khác cho các file hiện trạng mà không dùng vị trí mặc định. Điều này cho phép người dùng truy cập vào các hiện trạng được lưu trữ trong các file được chia sẻ trên mạng. Với cách này, các hiện trạng có thể được sử dụng cho các cá nhân người dùng hoặc được chia sẻ cho một nhóm người dùng. Để chỉ định một đường dẫn chỉ cần gõ nó vào hộp kí tự Profile Path.
- ✓ *Sử dụng các Script đăng nhập (Logon Scripts):* Các script đăng nhập là các file chạy lúc người sử dụng đăng nhập vào mạng. Chúng thường là tệp BAT nhưng chúng có thể là bất cứ loại tệp thi hành nào ta có thể sử dụng các script đăng nhập để thiết lập các ánh xạ ổ đĩa hoặc chạy file thi hành nào đó mỗi lần một người sử dụng đăng nhập vào máy. Ví dụ ta có thể chạy một file thu thập thông tin về cấu hình máy và gửi dữ liệu tới cơ sở dữ liệu quản lý trung tâm. Các script đăng nhập cũng hữu ích cho việc tương thích với các máy khách không sử dụng Windows 2000, muốn đăng nhập nhưng vẫn duy trì các thiết đặt với hệ điều hành của họ. Để chạy một script đăng nhập cho một người dùng, nhập tên script vào hộp kí tự Logon Script trong thẻ Profile của hộp hội thoại Properties. Script đăng nhập không được sử dụng nhiều lắm trong Windows 2000 mạng. Windows 2000 tự động thiết đặt hầu hết các cấu hình người dùng.
- ✓ *Thiết đặt thư mục chủ:* Người sử dụng thường lưu trữ các file cá nhân hoặc các

thông tin trong các thư mục riêng gọi là thư mục chủ. Trong thẻ Profile của hộp thoại Properties, ta có thể xác định vị trí của thư mục chủ là thư mục cục bộ hoặc thư mục trên mạng. Để chỉ định một thư mục có đường dẫn cục bộ, chọn tùy chọn Local Path và gõ đường dẫn vào hộp kí tự. Để chỉ định một đường dẫn trên mạng cho một thư mục, chọn tùy chọn Connect và chỉ định đường dẫn trên mạng bằng đường dẫn UNC (Universal Naming Convention). Trong trường hợp này thư mục trên mạng đó phải tồn tại và phải được chia sẻ.

Thẻ Dial-in: dùng để định nghĩa các đặc tính Dial-in như quyền truy cập từ xa hay tùy chọn Callback. Các tùy chọn này được dùng trong kết nối tới các máy chủ ở xa và các máy chủ của các mạng riêng ảo.

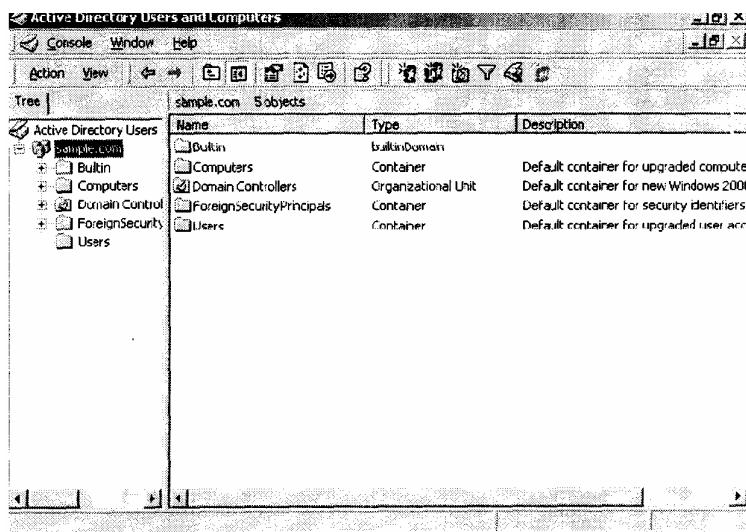
3. Làm việc với tài khoản người dùng Active Directory

Để tạo tài khoản miền cho người sử dụng, ta sử dụng tiện ích Active Directory Users and Computers. Với tiện ích này, ta có thể thêm một người dùng vào một miền trong Active Directory. Phần dưới đây sẽ mô tả làm thế nào để tạo người dùng miền mới và quản lý các đặc tính của người dùng miền.

3.1 Tạo người dùng Active Directory

Tiện ích Active Directory Users and Groups, là công cụ chính để quản lý người dùng, nhóm và máy tính Active Directory. Ta truy cập đến tiện ích này thông qua Administrator Tools.

Hình 2.7

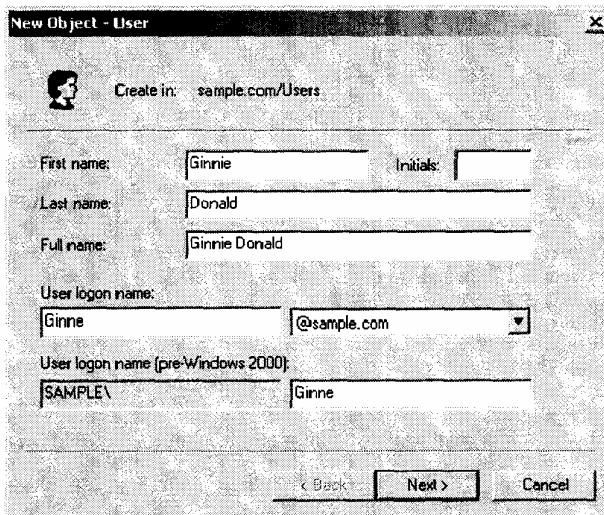


Để tạo người dùng Active Directory làm theo các bước sau:

- Chọn Start -> Programs -> Administrative Tools -> Active Directory Users and Computers .
- Cửa sổ Active Directory Users and Computers xuất hiện. Nhấn chuột phải vào Users, chọn New từ menu thả xuống, chọn User.

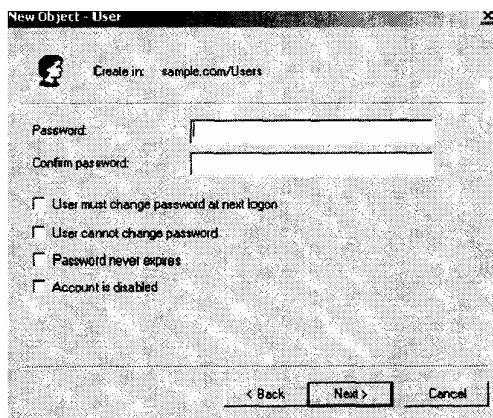
3. Hộp hội thoại New Object-user xuất hiện, xem hình 2.8 . Gõ vào tên người dùng, họ, tên đăng nhập. Tên đầy đủ và tên đăng nhập pre-Windows 2000 (dành cho các máy khách không dùng Windows 2000 muốn đăng nhập) sẽ được tự động thêm vào khi ta điền đủ các thông tin khác nhưng ta vẫn có thể thay đổi chúng nếu muốn. Nhấn nút Next.

Hình 2.8



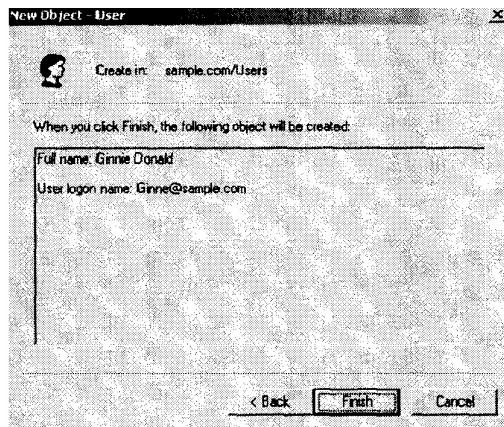
4. Hộp hội thoại New Object - User thứ 2 xuất hiện, xem hình 2.9. Gõ và xác nhận mật khẩu người dùng. Các hộp chéch trong hộp hội thoại này cho phép ta chỉ định việc người dùng phải thay đổi mật khẩu lúc đăng nhập, người dùng không thể thay đổi mật khẩu, mật khẩu không bao giờ hết hạn, hoặc tài khoản bị vô hiệu hóa. Nhấn nút Next.

Hình 2.9



5. Hộp hội thoại New Object - User cuối cùng xuất hiện, xem hình 2.10. Hộp hội thoại này hiển thị tài khoản ta vừa cấu hình. Nếu tất cả các thông tin là chính xác, nhấn nút Finish.

Hình 2.10



3.2 Quản lý các đặc tính người dùng Active Directory

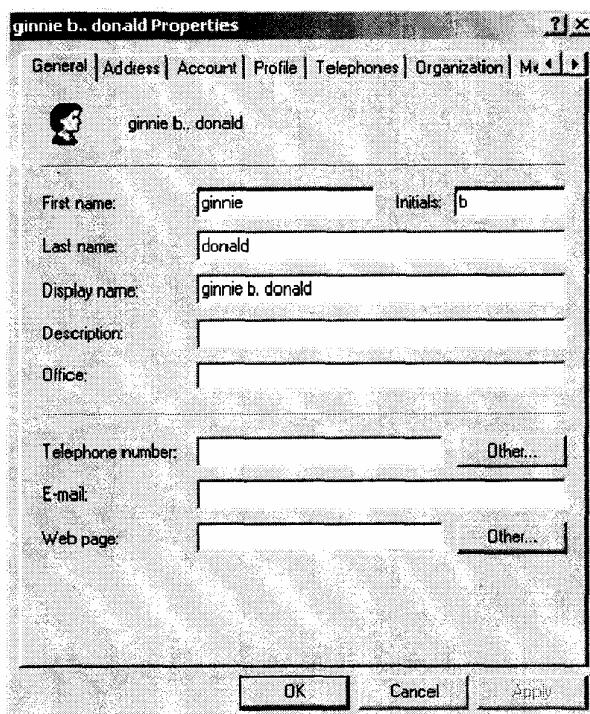
Với người dùng Active Directory, ta có thể cấu hình rất nhiều đặc tính khác nhau. Để duy cập tới hộp hội thoại Properties của một người dùng Active Directory, mở tiện ích Active Directory Users and Computers (bằng cách chọn Start -> Programs -> Administrative Tools -> Active Directory Users and Computers), mở thư mục Users, nhấn đúp vào tài khoản người dùng. Hộp hội thoại Active Directory user Properties xuất hiện với các thẻ cho 12 loại đặc tính chính:

General	Member Of
Address	Dial-in
Account	Environment
Profile	Sessions
Telephones	Remote Control
Organization Terminal	Services Profile

a) Định cấu hình các đặc tính chung của người dùng Active Directory:

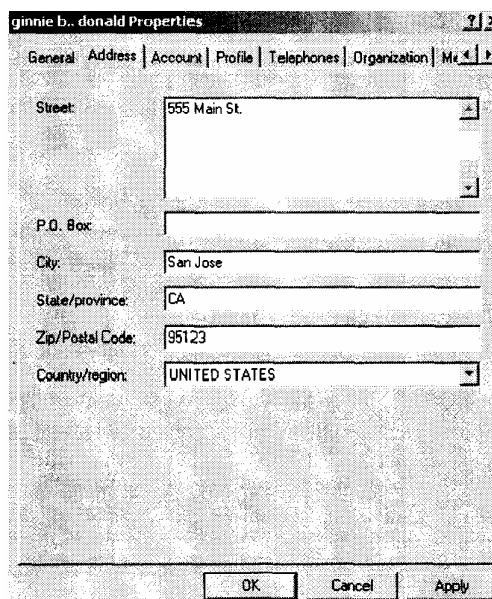
Thẻ đặc tính General, xem hình 2.11 , chứa các thông tin mà ta cung cấp khi thiết lập một tài khoản người dùng mới. Ta có thể thêm thông tin vào các hộp Description và Office. Ta cũng có thể thêm các thông tin liên hệ với người sử dụng như số điện thoại, email, địa chỉ, địa chỉ trang Web.

Hình 2.11



b) Thêm thông tin về địa chỉ của người dùng Active Directory:

Ta có thẻ cung cấp thông tin về địa chỉ của người dùng thông qua thẻ Address, xem hình 2.12. Thẻ này có các hộp kí tự dành cho tên phố, số hòm thư, thành phố, tỉnh, mã zip code. Ta cũng có thể chọn tên nước hoặc tên vùng từ danh sách thả xuống Country/Region. **Hình 2.12**



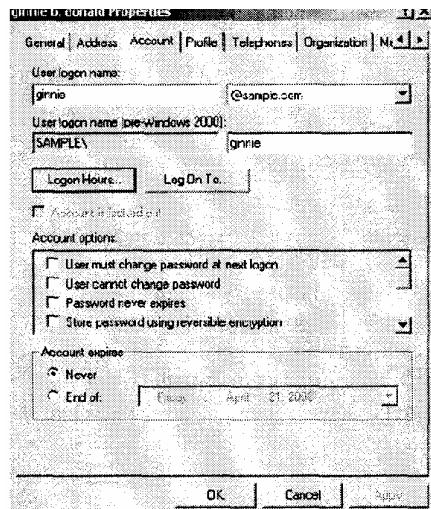
c) Điều khiển tài khoản người dùng Active Directory:

Thông qua thẻ Accounts, xem hình 2.13, ta có thể điều khiển tài khoản của người sử dụng. Thẻ này hiển thị thông tin về tên đăng nhập mà ta cung cấp khi ta thiết lập tài

khoản người dùng mới và cho phép ta định cấu hình những thiết đặt sau:

- ✓ Những giờ đăng nhập được cho người dùng.
- ✓ Những máy tính mà người dùng có thể đăng nhập.
- ✓ Các chính sách tài khoản áp dụng cho người dùng.
- ✓ Khi nào tài khoản hết hạn.
- ✓ Những thiết đặt này được mô tả trong các phần sau.

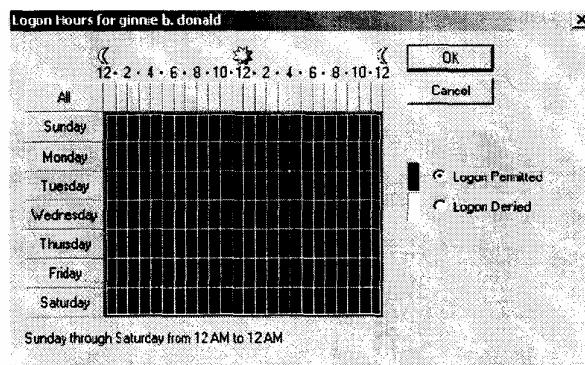
Hình 2.13



d) Điều khiển giờ đăng nhập

Khi ta nhấn vào nút Logon Hours, ta sẽ thấy hộp thoại Logon Hours, xem hình dưới. Mặc định, người dùng được phép đăng nhập 24 giờ một ngày, 7 ngày 1 tuần. Giờ đăng nhập được hạn chế trong quá trình backup máy tính. Ta cũng có thể muốn giới hạn giờ đăng nhập vì một số lý do bảo mật. Hộp màu xanh chỉ ra là ta được phép đăng nhập, hộp màu trắng là không được phép đăng nhập. Ta có thể thay đổi giờ đăng nhập bằng cách chọn giờ ta muốn vay đổi và nhấn vào nút radio Logon Permitted (cho phép đăng nhập) hoặc nút radio Logon Denied (không cho phép đăng nhập).

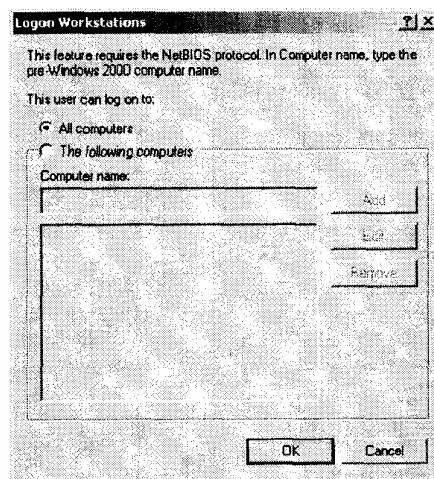
Hình 2.14



e) Điều khiển truy cập vào máy tính:

Khi nhấn vào nút Log On To, sẽ thấy hộp hội thoại Logon Workstations (đăng nhập vào trạm làm việc), xem hình 2.15. Hộp hội thoại này cho phép chỉ định việc người dùng có thể truy cập vào tất cả các máy tính trong mạng hoặc chỉ cho người dùng truy cập vào một số máy xác định trong mạng. Ví dụ, nếu Quản trị viên làm việc trong một môi trường bảo mật, ta có thể giới hạn chỉ cho tài khoản Quản trị viên được đăng nhập từ một máy nào đó. Ta có thể định cấu hình các máy tính để người dùng có thể truy cập dựa vào tên máy tính. Ta có thể thêm các máy các máy tính được cho phép bằng cách gõ vào tên máy tính và nhấn nút Add.

Hình 2.15



f) Thiết đặt các tuỳ chọn cho tài khoản

Các tuỳ chọn cho tài khoản được liệt kê trong thẻ Account cho phép ta điều khiển việc bảo mật mật khẩu cho tài khoản người dùng. Ta có thể xác định các tuỳ chọn tài khoản sau:

- ✓ Người dùng phải đổi mật khẩu vào lần đăng nhập tiếp theo.
- ✓ Người dùng không thể thay đổi mật khẩu.
- ✓ Mật khẩu không bao giờ hết hạn.
- ✓ Lưu trữ mật khẩu bằng cách mã hóa có thể đảo ngược lại được.

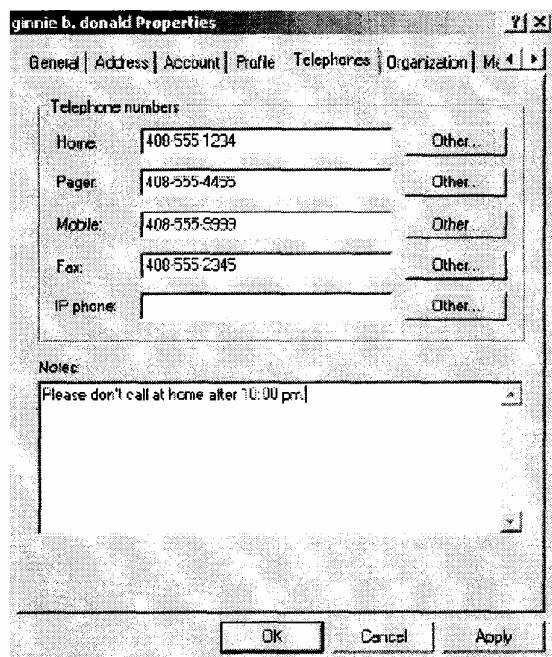
g) Thiết đặt việc hết hạn của tài khoản:

Nút radio End Of ở cuối thẻ Account cho phép thiết đặt việc hết hạn của tài khoản vào một ngày tháng cụ thể. Mặc định, các tài khoản là không hết hạn. Ta có thể muốn thiết đặt ngày hết hạn nếu ta có một nhân viên tạm thời và ta muốn vô hiệu hóa tài khoản của họ vào một ngày tháng nào đó. Tuỳ chọn này cũng hữu ích trong môi trường các trường học nơi các học viên cần tài khoản người dùng, những tài khoản của họ cần bị vô hiệu hóa vào cuối khoá học.

h) Thiết đặt môi trường người dùng Active Directory:

Thẻ Profile cho phép ta thiết đặt các hiện trạng người dùng, các script đăng nhập và thư mục chủ. Các tùy chọn này được định cấu hình theo cách tương tự như ta thiết đặt cho tài khoản người dùng cục bộ. Xem thêm phần "Setting Up the Local User Environment" trong chương này để biết thêm chi tiết về việc sử dụng các tùy chọn trong thẻ Profile. Thêm thông tin về số điện thoại của người dùng Active Directory Thẻ Telephone, xem hình 2.16, cho phép ta định cấu hình số điện thoại của người dùng như địa chỉ nhà, trang Web, số ĐT di động và địa chỉ IP. Ta cũng có thể ghi chú như : "Không gọi về nhà sau 10 giờ tối".

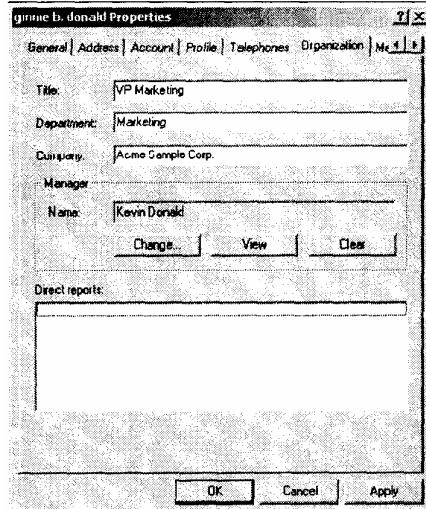
Hình 2.16



i) Thêm thông tin về tổ chức Active Directory:

Thẻ Organization, xem hình 2.17, cho phép ta cung cấp thông tin về vai trò của người dùng trong tổ chức của ta. Ta có thể đưa vào tiêu đề của người dùng, phòng, công ty và giám đốc. Ta cũng có thể chỉ ra người dùng sẽ báo cáo trực tiếp cho ai.

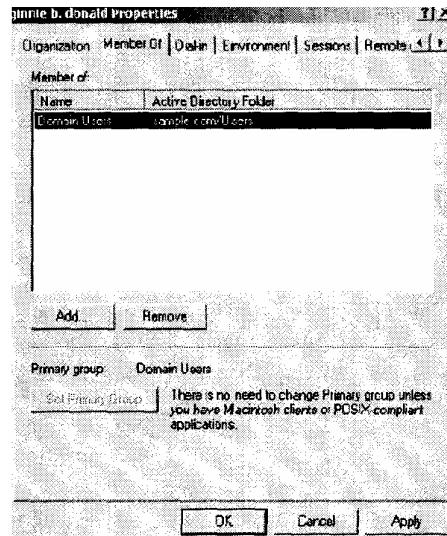
Hình 2.17



j) Quản lí Active Directory User Group Membership:

Thẻ Member Of hiển thị các nhóm mà người dùng là thành viên, xem hình 2.18 . Ta có thể thêm một người dùng vào một nhóm bằng cách nhấn vào nút Add. Để loại bỏ người dùng khỏi một nhóm đã được liệt kê, tô sáng nhóm đó và nhấn nút Remove.

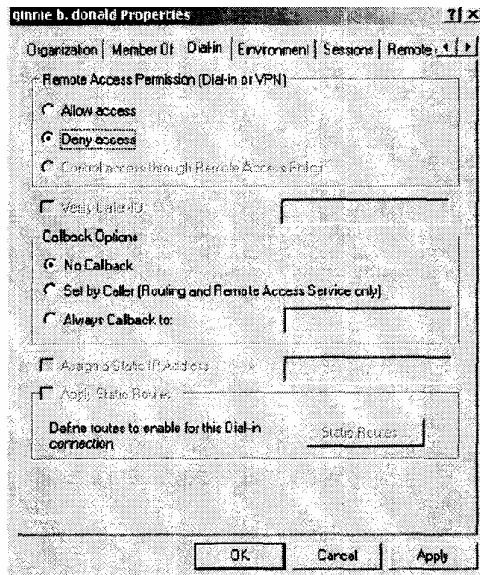
Hình 2.18



k) Quản lí các đặc tính Dial-in:

Qua thẻ Dial-in, xem hình 2.19, ta có thể định cấu hình quyền truy cập từ xa của người dùng cho các kết nối VPN hoặc dial-in.

Hình 2.19



I) Định cấu hình các đặc tính Terminal Services (các dịch vụ đầu cuối):

Bốn thẻ trong hộp hội thoại Active Directory user Properties chứa các đặc tính liên quan tới các dịch vụ đầu cuối là: environment (Môi trường), Sessions (phiên), Remote Control (điều khiển từ xa) và Terminal Services Profile (hiện trạng các dịch vụ đầu cuối).

CHƯƠNG 3: QUẢN LÝ BẢO MẬT (8 lý thuyết)

Với windows2000 Server, ta có thể quản lý bảo mật tại mức cục bộ hoặc mức miền. Tại mức miền, ta quản lý các chính sách bảo mật miền. Và tại mức cục bộ, ta quản lý các chính sách bảo mật cục bộ.

Việc thiết lập bảo mật được cấu hình thông qua chính sách về nhóm người dùng. Các chính sách tài khoản người dùng được sử dụng điều khiển tiến trình đăng nhập, như việc cấu hình mật khẩu và tài khoản "lockout". Các chính sách cục bộ được sử dụng để định nghĩa các chính sách bảo mật cho chính máy tính này, như kiểm định quyền người dùng và các tùy chọn về bảo mật.

Trong WinNT 4, ta có thể điều khiển Desktops của người dùng thông qua các chính sách hệ thống. Chức năng này cũng có trong Windows 2000 để tương thích với các phiên bản trước, nhưng nó được khuyến cáo là ta sử dụng các chính sách nhóm người dùng thay thế chính sách hệ thống để quản lý các tùy chọn.

Công cụ "Security and Analysis Configuration" là các tiện ích mới của Windows 2000 Server, qua đó ta có thể phân tích cấu hình bảo mật của ta. Các tiện ích sử dụng khuôn mẫu bảo mật để so sánh cấu hình bảo mật hiện tại của ta với cấu hình ta yêu cầu.

Trong chương này, ta sẽ học cách quản lý bảo mật trong môi trường Windows 2000 Server. Đầu tiên ta sẽ cài đặt trình điều khiển MMC để quản lý việc thiết lập tính bảo mật, sau đó học cách cấu hình các chính sách về tài khoản người dùng, các chính sách cục bộ và các chitlhd sách bảo mật. Phần cuối chương này sẽ mô tả cách để sử dụng tiện ích "Security and Analysis Configuration" để phân tích cấu hình bảo mật của ta.

1. Thiết lập quản lý bảo mật

Windows 200 Server cho phép ta quản lý các thiết lập về bảo mật tại mức cục bộ cho máy tính cụ thể hoặc trên mức miền lớn. Mọi chính sách bảo mật miền ta định nghĩa đè lên các chính sách cục bộ của một máy tính. Ta quản lý các chính sách với chính sách nhóm người dùng cà đối tượng thích hợp:

- ✓ Để quản lý chính sách cục bộ, ta sử dụng chính sách nhóm người dùng thông qua đối tượng Local Computer Group Policy.
- ✓ Để quản lý chính sách miền, ta sử dụng chính sách nhóm người dùng thông qua đối tượng Domain Controllers Group Policy.

Để thuận tiện cho công việc quản lý chính sách của ta, ta có thể thêm đối tượng Local Computer Policy and Domain Controller Security vào Microsoft Management Console (MMC). Ta cũng có thể truy cập các chính sách tài khoản người dùng và các chính sách cục bộ bằng cách chọn :

Start -> Programs->Administrative Tools -> Domain Security Policy or Local Security Policy.

1.1. Tạo trình điều khiển quản lý cho các thiết lập bảo mật.

1. Chọn Start -> Run, gõ "MMC" vào hộp hội thoại Run và bấm nút OK để mở MMC.
2. Từ thực đơn chính, chọn Console ->Add/Remove Snap-in.
3. Trong hộp hội thoại Add/Remove Snap-in bấm nút Add.
4. Chọn Group Policy và bấm nút Add.
5. Đối tượng Group Policy chỉ định Local Computer là mặc định. Bấm nút Finish.
6. Trong hộp hội thoại Add/Remove Snap-in bấm nút OK.
7. Từ thực đơn chính, chọn Console ->Add/Remove Snap-in.
8. Trong hộp hội thoại Add/Remove Snap-in bấm nút Add.
9. Chọn Event Viewer và bấm nút Add.
10. Hộp hội thoại để chọn máy tính hiện ra với Local Computer được chọn mặc định. Bấm nút Finish sau đó bấm nút Close.
11. Trong hộp hội thoại Add/Remove Snap-in bấm nút OK.
12. Chọn Console ->save As. Ghi trình điều khiển với tên Security trong thư mục Administrative Tools (đây là vùng mặc định) và bấm nút Save.

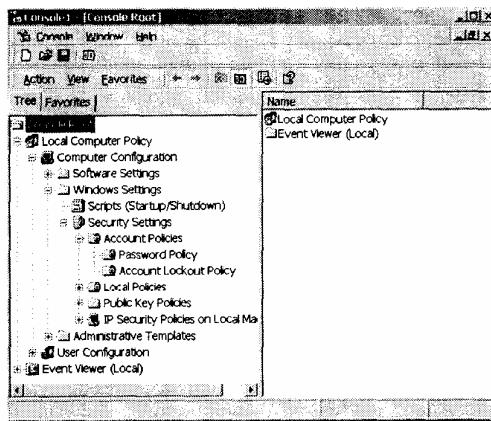
Ta có thể truy cập trình điều khiển bằng cách chọn:

Start -> Programs -> Administrative Tools -> Security.

2. Sử dụng các chính sách tài khoản người dùng.

Các chính sách tài khoản người dùng được sử dụng để chỉ rõ các thuộc tính tài khoản người dùng liệt kê trong tiến trình đăng nhập. Nó cho phép ta cấu hình việc thiết lập sự bảo mật máy tính cho mật khẩu và chỉ định tài khoản "lockout" và xác nhận Kerberos với một miền. Sau khi ta đã nạp MMC cho Group Policy, ta sẽ nhìn thấy một lựa chọn cho Local Computer Policy. Để truy cập các mục Account Policies, mở ra Local Computer Policy, Computer Configuration, Windows Settings, Security Settings và Account Policies.

Hình 3.1



Nếu ta đang dùng Windows 2000 member server, ta sẽ thấy hai mục: Password Policy và Account Lockout Policy. Nếu ta đang dùng Windows 2000server, máy được cấu hình là domain controller, ta sẽ thấy ba mục: Password Policy, Account Lockout Policy và Kerberos Policy. Các chính sách tài khoản người dùng có hiệu lực cho các member server và domain controller được giải thích trong phần kế tiếp.

2.1 Thiết lập các chính sách mật khẩu

Các chính sách về mật khẩu bảo đảm các yêu cầu bảo mật phải bắt buộc trên máy tính. Chú ý rằng chính sách mật khẩu được đặt trên nền tảng mỗi máy tính là rất quan trọng; nó không thể được cấu hình cho người dùng cụ thể. Hình 3.2 thể hiện các chính sách về mật khẩu được định nghĩa trên Windows 2000 member server, nó được giải thích trong bảng dưới. Trên Windows 2000 domain controller, tất cả các chính sách được cấu hình là “not define” (không được định nghĩa).

Hình 3.2

The screenshot shows the Windows 2000 Local Computer Policy snap-in. The left pane displays a tree view of policy settings under 'Local Computer Policy' (Computer Configuration\Windows Settings\Scripts (Startup/Shutdown) and Computer Configuration\Security Settings\Account Policies). The right pane shows a table with columns 'Policy', 'Local Setting', and 'Effective Setting' for the 'Password Policy' settings. The table lists:

Policy	Local Setting	Effective Setting
Enforce password history	0 passwords...	0 passwords rememb...
Maximum password age	42 days	42 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	0 characters
Passwords must meet complex...	Disabled	Disabled
Store password using revers...	Disabled	Disabled

Bảng 3.1 Các lựa chọn về chính sách mật khẩu:

Chính sách	Giải thích	Giá trị mặc định	Giá trị tối thiểu	Giá trị tối đa
Enforce Password History	Lưu giữ lịch sử mật khẩu của người dùng	Nhớ 0 mật khẩu	Giống giá trị mặc định	Nhớ 24 mật khẩu
Maximum Password Age	Xác định số ngày tối đa người dùng có thể giữ mật khẩu hợp lệ.	Giữ mật khẩu cho người dùng có 42 ngày	Giữ mật khẩu cho 1 ngày	Giữ mật khẩu cho 999 ngày.
Minimum Password Age	Chỉ định khoảng thời gian mật khẩu phải giữ sau khi nó bị thay đổi	0 ngày (mật khẩu có thể bị thay đổi ngay lập tức)	Giống như giá trị mặc định	999 ngày
Minimum Password Length	Chỉ định số tối thiểu các ký tự của mật khẩu phải có	0 ký tự (không yêu cầu mật khẩu).	Giống giá trị mặc định.	14 ký tự.
Password Must Meet Complexity Requirements	Cho phép ta cài đặt bộ lọc mật khẩu	Vô hiệu (disabled)	Giống giá trị mặc định	Có hiệu lực (Enable).
Store Password Using Reversible	Chỉ định mức cao hơn của việc mã hóa cho việc lưu trữ các mật	Vô hiệu (Disabled)	Giống giá trị mặc định	Có hiệu lực (Enable).

Encryption khẩu của người
for All Users dùng.
in the Domain.

Các chính sách mật khẩu được sử dụng như sau:

- ✓ Lựa chọn Enfore Password History được sử dụng để người dùng không thể sử dụng như những mật khẩu đã được sử dụng. Người dùng buộc phải tạo rẽ mật khẩu mới khi mà mật khẩu của họ chấm dứt hoặc bị thay đổi.
- ✓ Lựa chọn Maximun Password Age được sử dụng để sau khi vượt quá số ngày tồn tại của mật khẩu, người dùng bị ép buộc phải thay đổi mật khẩu của họ.
- ✓ Lựa chọn Minimum Password Age được sử dụng để ngăn cản người dùng không thay đổi mật khẩu vài lần liên tiếp nhanh chóng để mà làm thất bại mục đích của chính sách Enfore Password History.
- ✓ Lựa chọn Minimum Password Length được sử dụng để bảo đảm rằng người dùng tạo ra mật khẩu tốt để chỉ ra rằng nó đáp ứng độ dài yêu cầu. Nếu lựa chọn này không được thiết lập, người dùng không được yêu cầu tạo mật khẩu.
- ✓ Lựa chọn Password Must Meet Complexity Requirements được sử dụng để ngăn cản người dùng tránh sử dụng những mục mật khẩu được tìm thấy trong từ điển của tên phổ biến.
- ✓ Lựa chọn Store Password Using Revesible Encryption for All Users in the Domain được sử dụng để cung cấp một mức cao hơn cho việc giữ an toàn mật khẩu của người dùng.

Thiết lập các chính sách mật khẩu:

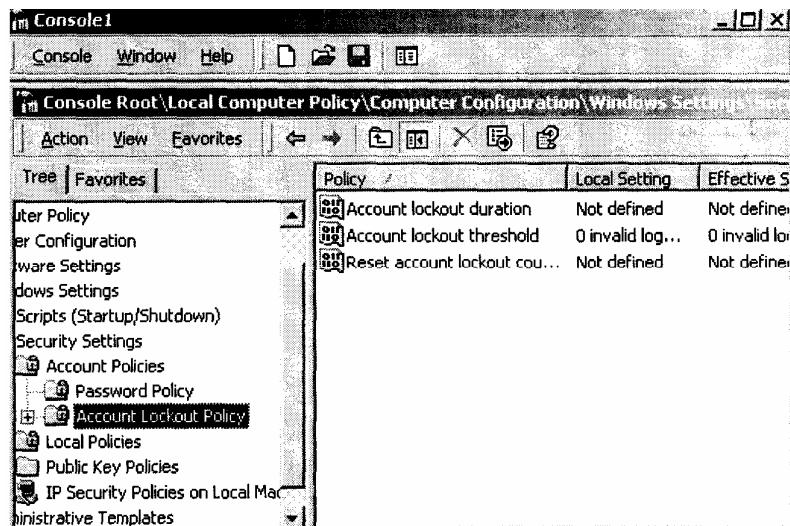
1. Chọn Start -> Programs -> Administrative Tools ->security và mở rộng nút Local Computer Policy.
2. Mở rộng nút làm xuất hiện: Computer Configuration, Windows Setting, Security Seulings, Account Policies, Password Policy.
3. Mở chính sách Enforce Password History. Trong trường Effective Policy Setting, chỉ định 5 mật khẩu được ghi nhớ. Bấm nút OK.
4. Mở chính sách Maximum Password Age. Trong trường Local Policy Setting chỉ định mật khẩu kết thúc trong 60 ngày. Bấm nút OK.

2.2 Thiết lập các chính sách về đăng nhập không hợp lệ

Các chính sách Account Lockout được sử dụng để chỉ định số lần thử đăng nhập khung hợp lệ có thể cho phép. Ta thiết lập các chính sách này sau x số lần thử đăng nhập không thành công trong khoảng y phút, tài khoản sẽ bị khóa trong khoảng thời gian xác định hoặc cho đến khi người quản trị mở trở lại tài khoản đó Các chính sách

về số lần cho phép đăng nhập không hợp lệ cũng giống như cách các nhà băng điều khiển ATM truy cập mã bí mật. Ta có lượng chắc chắn các khả năng để đăng nhập thành công mã truy cập. Bằng cách đó, nếu ai đó ăn trộm thẻ họ không thể làm được việc là thử các phỏng đoán về mã truy cập cho đến khi họ có kết quả đúng. Nhưng sau khi thử không thành công với mã truy cập, máy ATM sẽ giữ thẻ. Sau đó cần yêu cầu thẻ mới từ ngân hàng. Hình 3.3 thể hiện các chính sách về đăng nhập không hợp lệ, nó được giải thích trong bảng 3.2.

Hình 3.3



Bảng 3.2 các lựa chọn về đăng nhập không hợp lệ:

Giá trị đề nghị	Giá trị đề nghị	Giá trị đề nghị	Giá trị đề nghị	Giá trị đề nghị	Giá trị đề nghị
Account Lockout Threshold	Chỉ rõ số lần thử truy cập không hợp lệ trước khi khóa.	0 (vô hiệu hóa).	Giống giá trị mặc định.	999 lần thử.	5 lần thử.
Account Duration	Chỉ rõ khoảng thời gian bị khóa nếu Account Lockout threshold vượt quá.	0, nếu Account Lockout threshold có hiệu lực thì Lockout sẽ là 30 phút.	Giống giá trị mặc định	99,999 phút.	5 phút.
Reset account lockout counter after					

Reset	Chỉ định	0 nếu	Giống giá	99,999 phút	5 phút
Account	khoảng thời	Acccount	trị mặc		
Lockout	gian bộ	Lockout	định		
Counter	đếm sẽ nhớ	Threshold			
After	các lần thử đăng nhập không hợp lệ	có hiệu lực thì sẽ là 5 phút			

Các chính sách thiết lập Account lockout:

- Chọn Start -> Programs -> Admininitrative Tools ->security và mở nút Local Computer Policy.
- Mở rộng nút làm xuất hiện: Computer Configuration, Windows Seuings, Security Seuings, Account Policies, Account Lockout Policy.
- Mở chính sách Account Lockout Threshold. Trong trường Local Pelicy Setting, chỉ định tài khoản sẽ bị khoá sau 3 lần cố thủ đăng nhập. Bấm nút Ok.
- Hộp hội thoại Suggestd Value Changes sẽ xuất hiện. Nhận giá trị mặc định cho Account lockout duration và Reset account lockout counter bằng cách bấm nút OK.
- Rời khỏi hệ thống. Thủ đăng nhập với tên Nam cùng với 3 lần nhập sai password.
- Sau đó ta sẽ thấy thông điệp lỗi tuyên bố tài khoản bị khoá, đăng nhập với tài khoản Administrator.
- Để khôi phục tài khoản của Nam, hãy mở mục Local Users and Groups trong MMC, mở nút Users, và nhấp kép chuột vào tài khoản Nam. Trong phần General của hộp hội thoại thuộc tính của Nam, bấm loại bỏ đánh dấu trong hộp chọn Account Locked Oặt. Sau đó bấm nút OK.

2.3 Thiết lập chính sách Kerberos

Phiên bản Kerberos 5 là giao thức bảo mật được sử dụng trong Windows 2000 Server để xác thực người dùng và các dịch vụ mạng. Nó được gọi là xác minh kép hay xác thực lẩn nhau. Khi Windows 2000 Server được cài đặt như domain controller, nó tự động trở thành trung tâm phân phối khoá (key distribution center-KDC). KDC sẽ chịu trách nhiệm vụ tất cả các mật khẩu và các thông tin tài khoản người dùng trong các máy khách. Các phục vụ của Kerberos cũng được cài đặt trên mỗi máy khách và máy chủ Windows 2000.

- Các yêu cầu kiểm định máy khách từ KDC sử dụng mật khẩu hoặc thẻ thông

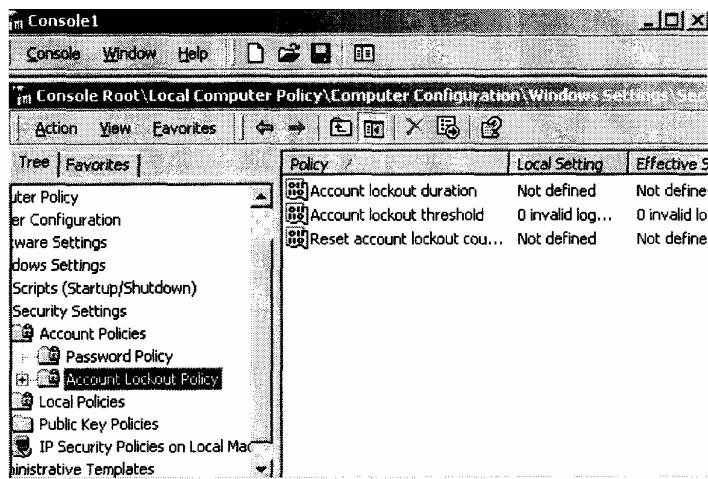
minh.

2. KDC phát cho máy khách thẻ gọi là thẻ công nhận (ticket-granting ticket - TGT). Máy khách có thể sử dụng TGT để truy cập các dịch vụ về thẻ này (ticket-granting service - TGS). TGS cung cấp các thẻ phục vụ cho các máy khách.

3. Máy khách trình thẻ phục vụ để yêu cầu các dịch vụ mạng. Các thẻ phục vụ sẽ kiểm định lẫn nhau phục vụ từ người dùng và phục vụ đến người dùng.

Hình 3.4 hiển thị các chính sách Kerberos và các giải thích trong bảng 3.3 dưới.

Hình 3.4



Bảng 3.3 các lựa chọn Kerberos.

Chính sách	Giải thích	Thiết lập môi trường mặc định	Thiết lập hiệu quả
Enforce User Logon Restrictions	Chỉ định hạn chế đăng nhập là bắt buộc.	Không xác định.	Cho phép.
Maximum LifeTime for Service Ticket	Chỉ định tuổi tối đa cho thẻ phục vụ trước khi thay mới.	Không xác định.	600 phút.
Maximum Lifetime for User Ticket	Chỉ định tuổi tối đa cho thẻ người dùng trước khi thay mới.	Không xác định.	10 giờ.
Maximum Lifetime for User Renewal	Chỉ định khoảng thời gian thẻ có thể bị thay mới trước khi nó được tái sinh	Không xác định.	7 ngày.

Maximum Tolerance Computer Synchronization	Chỉ định thời gian tối đa cho sự đồng bộ hoá giữa máy khách và KDC	Không xác định.	5 phút.
--	--	-----------------	---------

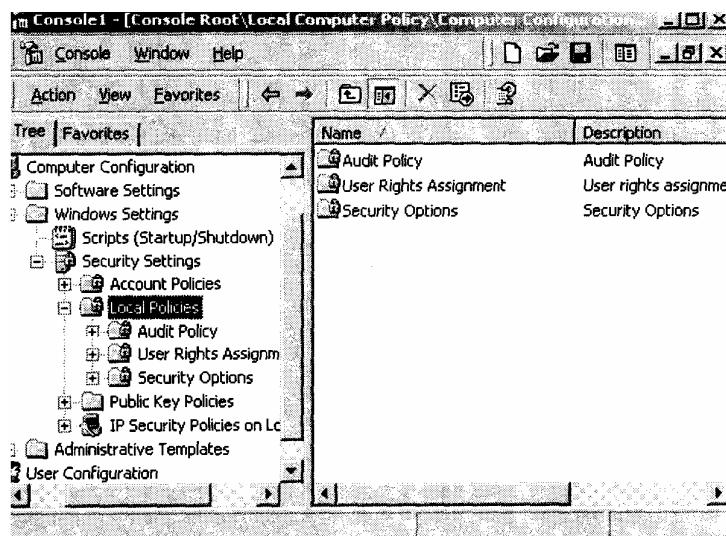
3. Sử dụng các chính sách cục bộ

Sau khi đã học hết các phần trước, các chính sách tài khoản được sử dụng điều khiển thủ tục đăng nhập. Khi muốn điều khiển những thứ có thể làm sau khi đăng nhập, sử dụng các chính sách cục bộ. Với các chính sách cục bộ có thể thi hành việc kiểm định, chỉ định quyền người dùng và đặt các tùy chọn bảo mật.

Thi hành, cấu hình, quản lý và gỡ rối các chính sách trong môi trường Windows 2000.

- ✓ Thi hành, cấu hình, quản lý và gỡ rối các chính sách cục bộ trong môi trường Windows 2000.
- ✓ Thi hành, cấu hình, quản lý và gỡ rối các chính sách hệ thống trong môi trường Windows 2000.

Để sử dụng các chính sách cục bộ, đầu tiên ta thêm mục Local Computer Policy vào MMC. Sau đó từ MMC lần theo đường dẫn thư mục để truy cập thư mục Local Policies: Local Computer Policy, Computer Configuration, Window Setting, Security Settings, Local Policies. Hình 3.5 hiển thị các thư mục của Local Policies. **Hình 3.5**



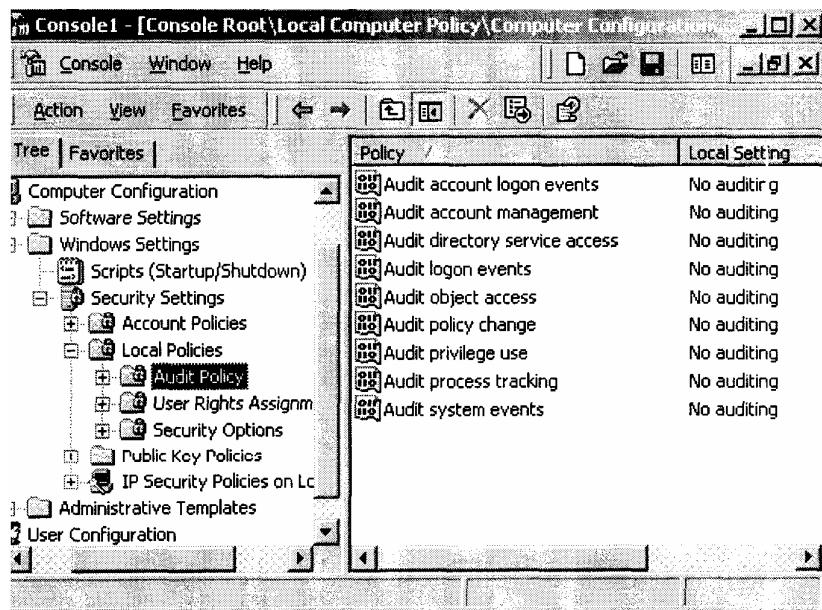
Có ba thư mục trong Local Policies : Audit Policy, User Rights Assignment và Security Options. Các chính sách bao chùm các phần tiếp theo.

3.1 Thiết lập chính sách kiểm định

Thi hành, cấu hình, quản lý và gỡ rối việc kiểm định.

Ta kiểm định các sự kiện liên quan đến quản lý người dùng thông qua chính sách kiểm định. Bằng cách lưu lại vết của các sự kiện chính, ta có thể đưa ra được tiến trình của một nhiệm vụ được chỉ định, như tạo người dùng, hoàn thành hoặc không hoàn thành trong thủ tục đăng nhập. Ta có thể nhận ra sự xâm phạm bảo mật được phát sinh khi người dùng cố thử truy cập các nhiệm vụ quản lý hệ thống mà không có sự cho phép. Khi ta định nghĩa một chính sách kiểm định cần lựa chọn kiểm định việc hoàn thành hay thất bại của sự kiện được chỉ định. Sự kiện hoàn thành có nghĩa là nhiệm vụ được hoàn thành một cách hoàn hảo. Sự kiện thất bại có nghĩa là nhiệm vụ đó không hoàn thành một cách trọn vẹn. Bình thường thì việc kiểm định không hoạt động và nó phải được người dùng cấu hình. Khi việc kiểm định được cấu hình ta sẽ thấy kết quả kiểm định thông qua tiện ích Event Viewer. Kiểm định nhiều sự kiện quá sẽ làm giảm khả năng thực hiện của hệ thống nguyên nhân là do yêu cầu xử lý cao của nó. Việc kiểm định cũng có thể sử dụng quá mức không gian đã để lưu trữ nhật ký kiểm định. Ta hãy sử dụng các tiện ích một cách hiệu quả. Hình 3.6 biểu diễn các chính sách kiểm định và diễn được giải trong bảng 3.4 dưới.

Hình 3.6



Bảng 3.4 Các lựa chọn chính sách kiểm định:

Chính sách	Giải thích
Audit Account Logon Events	Lưu lại vết khi người dùng đăng nhập, thoát khỏi hệ thống hoặc tạo ra liên kết mạng.
Audit Account Management	Lưu lại vết việc tạo, xóa và quản lý tài khoản người dùng và nhóm người dùng.
Audit Directory Service Access	Lưu lại vết truy cập phục vụ thư mục.
Audit Logon Events	Kiểm định các sự kiện liên quan đến đăng nhập, như chạy kịch bản đăng nhập hoặc là việc truy cập hiện trạng máy tính.
Audit Privilege Use	Lưu lại vết bất kỳ sự thay đổi người có thể hoặc không thể hoặc được xem kết quả của việc kiểm định.
Audit Process Tracking	Lưu lại vết các sự kiện như kích hoạt một chương trình truy cập một đối tượng và thoát khỏi một tiến trình.
Audit System Events	Lưu lại vết các sự kiện hệ thống như tắt máy, khởi động lại máy giống như các sự kiện liên quan đến Security log trong Event Viewer.

Thiết lập các chính sách kiểm định.

1. Chọn Start -> Programs -> Administrative Tools - Security và mở mục Local Computer Policy.
2. Mở các lần lượt các thư mục: Computer Configuration, Windows Settings, Security Settings, Local Policies, Audit Policy.
3. Mở chính sách Audit Account Logon Events. Trong trường Local Policy Setting, chỉ định Audit These Attempts. Chọn Success và Failure. Bấm nút OK.
4. Mở chính sách Audit Account Management. Trong trường Local Policy Setting, chỉ định Audit These Attempts, Chọn Success và Failure. Bấm nút OK.
5. Thoát khỏi hệ thống và thử truy cập với tên người dùng NamD. Việc đăng nhập sẽ thất bại (vì không có tài khoản nào có tên là NamD).
6. Đăng nhập lại hệ thống với tên người dùng là Administrator. Mở MMC và mở Event Viewer.
7. Từ Event Viewer mở Security log. Ta sẽ thấy các sự kiện được kiểm định

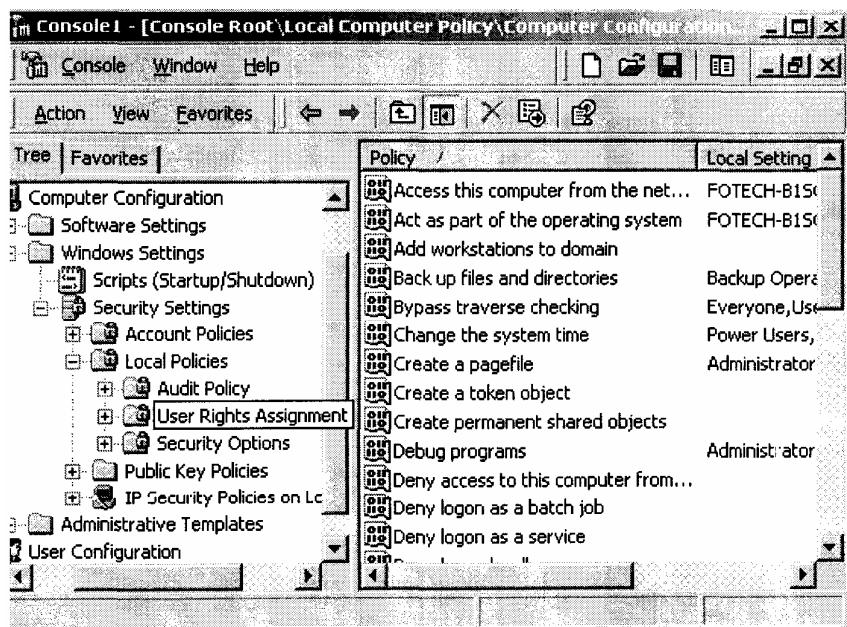
được liệt kê trong bản ghi này.

3.2 Án định quyền người dùng

Các chính sách về quyền người dùng xác định tính hợp pháp một người dùng hoặc nột nhóm người dùng trong máy tính. Quyền người dùng tham gia vào hệ thống. Nó không giống như sự cho phép, nó chỉ áp dụng cho các đối tượng được chỉ định.

Ví dụ như một quyền người dùng chỉ được quyền Bách Up Files and Directories. Nó cho phép người dùng sao lưu tệp và các thư mục dù là người dùng đó không có quyền đi qua các tệp hệ thống. Các quyền người dùng khác cũng tương tự bởi vì chúng được phân phối truy cập hệ thống chỉ định để truy cập tài nguyên. Hình 3.7 thể hiện các chính sách án định quyền người dùng và các diễn giải trong bảng 3.5 dưới.

Hình 3.7



Bảng 3.5 Các chính sách án định quyền người dùng

Quyền	Giải thích
Access This Computer from the Network	Cho phép người dùng truy cập máy tính từ mạng.
Act as Part of the Operating System	Cho phép sự xác nhận mức thấp phục vụ việc xác minh với bất kỳ người dùng nào.
Add Workstations to the Domain	Cho phép người dùng tạo tài khoản truy cập vào domain.
Back Up File and Directories	Cho phép người dùng sao lưu tất cả các tệp và các thư mục bất kể có sự cho phép về tệp hay thư mục đó có được đặt hay

	không.
Bypass Traverse Checking	Cho phép người dùng duyệt cây thư mục cho dù người dùng đó không được phép liệt kê các thành phần thư mục.
Change the System Time	Cho phép người dùng thay đổi thời gian trong máy tính.
Create a Pagefile	Cho phép người dùng thay đổi kích thước trang tệp.
Create Permanent Shared Object	Cho phép một tiến trình tạo một mã thông báo nếu tiến trình sử dụng NtCreate Token API.
Debug Programs	Cho phép người dùng đính kèm chương trình gỡ lỗi vào bất kỳ một tiến trình.
Deny Access to This Computer from the Network	Cho phép ta từ chối những người dùng chỉ định hoặc nhóm người dùng truy cập vào máy tính từ mạng.
Deny Logon as a Batch File	Cho phép ta ngăn những người dùng chỉ định hoặc nhóm người dùng đăng nhập với tệp batch (batch file).
Deny Logon as Service	Cho phép ta ngăn những người dùng chỉ định hoặc nhóm người dùng đăng nhập với các phục vụ.
Deny Logon Locally	Cho phép ta từ chối những người dùng chỉ định hoặc nhóm người dùng truy cập vào nội bộ máy tính.
Enable Computer and User Accounts to Be Trusted by Delegation	Cho phép người dùng hoặc nhóm người dùng thiết lập Trusted hy Delegation cho người dùng hoặc đối tượng máy tính.
Force Shutdown from a Remote System	Cho phép hệ thống có thể tắt bởi người dùng tại vị trí từ xa trên mạng.
Generate Security Audits	Cho phép người dùng, nhóm người dùng hoặc tiến trình để tạo các mục vào trong Security log
Increase Scheduling Priority	Cho phép người dùng thao tác các tiến trình được phục vụ bởi việc thực hiện các

	hạn ngạch xử lý.
Load and Unload Device Drivers	Cho phép người dùng tự động gỡ và nạp các trình điều khiển thiết bị Plug-and-Play.
Lock Page in Memory	Quyền người dùng không được sử dụng trong Windows 2000 (nó dự kiến bắt buộc dữ liệu được giữ trong bộ nhớ vật lý và không cho phép dữ liệu được phân trang vào các tệp trang).
Log On as Batch Job	Cho phép một tiến trình đăng nhập hệ thống và chạy một tệp bao gồm một hoặc nhiều lệnh thao tác hệ thống
Log On as Service	Cho phép phục vụ đăng nhập hệ thống hợp lệ chạy các phục vụ được chỉ định.
Log On as Locally	Cho phép người dùng đăng nhập vào máy tính nơi mà tài khoản người dùng đã được định nghĩa.
Manage Audting and Security Log	Cho phép người dùng quản lý Security log.
Modify Firmware Environment Variables	Cho phép n hoặc một tiến trình thay đổi môi trường hệ thống
Profile Single Process	Cho phép người dùng giám sát tiến trình phi hệ thống thông qua các công cụ như Performance Logs và tiện ích Alerts.
Profile System Performance	Cho phép người dùng giám sát các tiến trình hệ thống thông qua các công cụ như Performance Logs và tiện ích Alerts.
Remove Computer from Docking Station	Cho phép người dùng tách rời một máy tính xách tay thông qua giao diện người dùng Windows 2000.
Replate a Process Level Token	Cho phép một tiến trình thay thế mã thông báo mặc định bởi mã được tạo tiến trình con với mã thông báo được chỉ định.
Restore File and Directories	Cho phép người dùng khôi phục các tệp và các thư mục bất chấp sự cho phép về tệp và thư mục.

Shut Down the System	Cho phép người dùng tắt máy từ tại máy hiện tại.
Synchronize Directory Service Data	Cho phép người dùng đồng bộ hóa dữ liệu được kết hợp với phục vụ thư mục.
Take Ownership of Files or Other Objects	Cho phép người dùng giữ quyền sở hữu các đối tượng hệ thống.

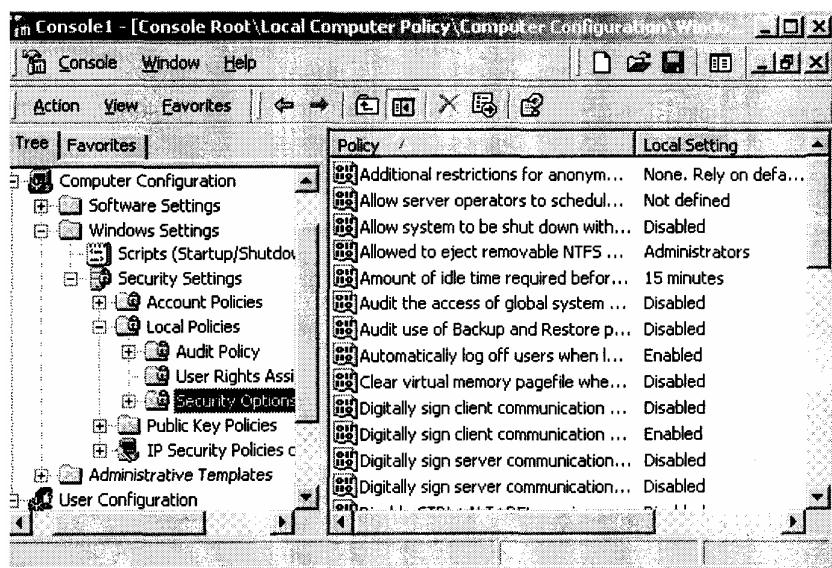
Thiết lập các quyền người dùng nội bộ:

1. Chọn Start -> Program -> Administrative Tools -> Security và mở mục Local Computer Policy.
2. Mở lần lượt các thư mục: Computer Configuration, Windows Settings, Security Settings, Local Policies, User Rights Assignment.
3. Mở quyền người dùng Log On as a Service. Hộp thoại Local Security Policy Setting xuất hiện.
4. Bấm nút Add. Hộp thoại Select Users or Group xuất hiện.
5. Chọn người dùng Nam. Bấm nút Add, sau đó bấm nút OK

3.3 Định nghĩa các tùy chọn bảo mật

Các tùy chọn bảo mật được sử dụng để thiết lập sự bảo mật cho máy tính. Không giống như các chính sách về quyền người dùng được sử dụng cho 1 người hoặc 1 nhóm người dùng, các chính sách về cơ chế bảo mật chỉ áp dụng cho máy tính. Hình 3.8 chỉ ra các chính sách lựa chọn bảo mật, các chính sách này được miêu tả ở bảng 3.6 dưới.

Hình 3.8



Bảng 3.6 các lựa chọn bảo mật:

Lựa chọn	Miêu tả	Giá trị mặc định
Additional Restrictions for Anonymous Users	Cho phép thêm các hạn chế cho các kết nối ẩn.	Không có.
Allow Server Operators to Schedule Tasks (domain controller only)	Cho phép người quản lý Server lên lịch làm việc xác định để chỉ ra thời gian chỉ định hoặc khoảng thời gian nghỉ.	Không xác định.
Allow System to Be Shut Down Without Having Logon	Cho phép người dùng thoát khỏi hệ thống mà không nhất thiết người đó phải đăng nhập vào hệ thống	Cho phép (nhưng sự thiết lập chính sách cục bộ bị ghi đè lên nếu như các thiết lập chính sách của mức domain được cài đặt.)
Allow to Eject Removable NTFS Media	Cho phép đóng các phương tiện NTFS có thể di chuyển được.	Administrator.
Amount of Time Idle Before Disconnecting Session	Cho phép các phiên làm việc ngừng kết nối khi chúng rỗi	15 phút.
Audit the Access of Global System Object	Cho phép truy nhập vào đối tượng hệ thống bao trùm để kiểm định.	Vô hiệu.
Audit Use of All User Rights including Backup and Restore Privilege	Cho phép quyền người dùng, bao gồm các đối tượng sao lưu dữ liệu phải được kiểm định.	Vô hiệu.
Automatically Log Off User when Logon Time Expires.	Tự động kết thúc phiên làm việc của người dùng nếu họ đã hết thời gian đăng nhập vào hệ thống.	Cho phép.
Clear Virtual Memory Pagefile when System Shutdown.	chỉ định rằng trang (của bộ nhớ ảo) sẽ được xoá hết khi hệ thống tắt.	Vô hiệu.
Digitally Sign Client Communication (always)	Chỉ định rằng Server luôn giao tiếp với cháu bằng tín hiệu số.	Vô hiệu.
Digitally Sign Client Communication (when possible)	Chỉ định rằng Server giao tiếp với client bằng tín hiệu số khi có thể.	Cho phép.

Digitally Sign Server Communication (always)	Đảm bảo rằng các giao tiếp của Server luôn là tín hiệu số.	Vô hiệu.
Digitally Sign Server Communication (When possible)	Đảm bảo rằng các giao tiếp của Server là tín hiệu số khi có thể.	Vô hiệu.
Disable CTRL+ALT+DEL Requirement for Logon	Cho phép vô hiệu hóa yêu cầu nhấn CTRL+ALT+DEL để đăng nhập vào hệ thống.	Không xác định.
Do Not Display Last User Name in Logon Screen	Không hiện tên của người dùng cuối trên màn hình đăng nhập vào hệ thống.	Vô hiệu.
LAN Manager Authentication Level	Chỉ định cấp độ xác nhận người quản lý mạng cục bộ.	Gửi phản hồi của nhà quản lý mạng LAN Và NTLM (NT LAN Manager).
Message Text for User Attempting to Logon	Hiển thị dòng thông báo khi người dùng đang cố đăng nhập vào hệ thống.	Dòng trống.
Message Title for User Attempting to Logon.	Hiển thị tiêu đề thông báo khi người dùng đang cố đăng nhập vào hệ thống.	Dòng trống.
Number of Previous Logon Attempts to Cache (in case domain controller is available).	Chỉ định số lần có gắng đăng nhập được lưu trong bộ nhớ đệm.	10
Prevent System Maintenance of Computer Account Password	Ngăn chặn sự thi hành hệ thống của các tài khoản máy tính.	Vô hiệu.
Prevent Users from installing print drivers	Ngăn không cho người sử dụng cài đặt các trình điều khiển máy in.	Vô hiệu.
Prompt User to change Password Before Expiration.	Nhắc người dùng thay đổi mật khẩu trước khi mật khẩu hết hạn.	14 ngày trước khi hạn mật khẩu.
Recovery console:Allow	Chỉ định rằng khi Recovery Console được nạp, đăng nhập của	Vô hiệu.

Automatic Administrative Logon	nhà quản trị phải là tự động, không phải tự đăng nhập nữa.
Recovery console:	Cho phép sao chép các tệp từ tất cả các ổ đĩa và các thư mục khi Recovery Console được nạp.
Allow Floppy Copy and Access to All Divers and Folders.	Vô hiệu
Rename Administrator Account	Cho phép tài khoản Không xác định. Administrator có thể đổi tên.
Rename Guest Account.	Cho phép tài khoản Guest có thể Không xác định. đổi tên.
Restric CD-ROM Access Locally Logged on users only	Hạn chế những người dùng - đăng nhập cục bộ truy nhập vào CD-ROM.
Restric Floppy Access Locally Logged-on users only	Hạn chế những người dùng đăng nhập cục bộ truy nhập vào ổ đĩa mềm.
Secure Channel: Digitally Encrypt or Sign Secure Channel Data (always).	Chỉ định rằng dữ liệu kênh an Vô hiệu. toàn luôn được mã số hoá hoặc tín hiệu số hoá.
Secure Channel: Digitally Encrypt Secure Channel Data (when possible).	Chỉ định rằng dữ liệu kênh an Vô hiệu. toàn được mã số hoá khi có thể.
Secure Channel: Digitally Sign Secure Channel Data (when possible).	Chỉ định rằng dữ liệu kênh an Cho phép toàn được tín hiệu số hoá khi có thể.
Secure Channel:Require Strong (Window 2000 or later) Session Key	Cung cấp một kênh đảm bảo và Vô hiệu. yêu cầu một khoá phiên làm việc tốt (trong Window 2000 hoặc phiên bản cũ)
Send Unencrypted Passwords to Connect to Third-party SMB Servers	Cho phép mật khẩu không được mã hoá kết nối đến Thirdparty SMB Server.
Shut Down System	Chỉ định rằng hệ thống tắt ngay Vô hiệu

immediately if Unable to Log Security Audits.	lập tức nếu nó không thể ghi lại sự kiểm định bảo mật
Smart Card Removal Behavior	Thay đổi sự giao tiếp với thẻ Không hành động thông minh.
Strengthen Default Permission of Global System Object (e.g. Symbolic Links)	Làm tăng sự cho phép mặc định Cho phép của đối tượng hệ thống toàn cục.
Unsigned Driver Installation Behavior	Điều khiển sự cài đặt các thiết bị Cảnh báo nhưng cho phép không được đánh dấu. cài đặt.
Unsigned Non-Driver Installation Behavior	Điều khiển sự cài đặt của các Non-Driver được đánh dấu.

Nếu ta thay đổi các chính sách bảo mật và chú ý rằng các thay đổi của ta không có tác dụng, nó có thể do đã có chính sách của nhóm được áp dụng định kỳ. ta có thể ép các chính sách của ta được cập nhật bằng cách gõ: secedit/ refreshpolicy machine-policy tại dấu nhắc dòng lệnh.

Định nghĩa các lựa chọn bảo mật:

1. Chọn Start -> Programs -> Administrative Tools -> security và mở mục Local Computer Policy.
2. Mở các thư mục sau: Computer Configuration, Window Settings, Local Policies, Security Options.
- 3 . Mở chính sách Message Text for Users Attempting to Log On. Trong trường Local Policy Setting gõ Wellcom to all authorized user. Bấm nút OK.
4. Mở chính sách Prompts Uer to Changes Password Before Expiration. Trong trường Local Policy Setting. Chỉ định 3 ngày. Bấm nút OK.
5. Chọn Start -> Program -> Accessories -> Command Prompt. Tai dấu nhắc lệnh gõ: **secedit lrefesholicy machine_policy** và nhấn phím Enter.
6. Tại dấu nhắc lệnh gõ **exit** và nhấn phím Enter.
7. Thoát khỏi hệ thống và đăng nhập với tên người dùng **BẮC** (với mật khẩu **congnghehongtin**).
8. Thoát khỏi hệ thống và đăng nhập với tên người dùng Administrator.

4. Sử dụng các chính sách hệ thống

Thông qua các chính sách hệ thống, ta có thể điều khiển cấu hình hệ thống máy

tính và môi trường làm việc của người dùng. Họ làm việc bằng cách soạn thảo Registry tương ứng với việc thiết lập chính sách. Ta có thể đặt các chính sách hệ thống cho những người dùng, nhóm và máy tính riêng biệt như tất cả người dùng và tất cả máy tính.

Thi hành, cấu hình, quản lý và gỡ rối các chính sách trong môi trường Windows 2000:

- ✓ Thi hành, cấu hình, quản lý và gỡ rối các chính sách cục bộ trong môi trường Windows 2000.
- ✓ Thi hành, cấu hình, quản lý và gỡ rối các chính sách hệ thống trong môi trường Windows 2000.

Các chính sách hệ thống thường được liên quan tới Window NT 4. Windows 2000 đề nghị ta sử dụng Group Policy để quản lý việc thiết đặt nền màn hình của người dùng như đã giải thích phần trước. Mặc dù vậy, ta vẫn có thể sử dụng System Policy Editor (POLEDIT) để quản lý các chính sách hệ thống trong Windows 2000. Các tệp chính sách hệ thống làm việc như sau trong dòng hệ điều hành Windows:

- ✓ Các tệp chính sách hệ thống đã tạo trong windows 2000 hoặc WindowsNT 4 sẽ làm việc với các máy khách Windows 2000 và WindowsNT 4.
- ✓ Các tệp chính sách hệ thống đã tạo trong Windows98 hoặc Windows95 sẽ làm việc với các máy khách Windows98 hoặc Windows 95.

Thông qua System Policy Editor, ta có thể cấu hình các chính sách hệ thống theo các bước sau:

Người dùng mặc định: Chọn mặc định cho bất cứ người dùng nào đăng nhập vào từ máy tính NT (ghi vào khóa HKEY_CURRENT_USER của Registry).

Người dùng: Cho phép ta tạo các chính sách hệ thống theo yêu cầu cho người dùng cụ thể (ghi vào khóa HKEY_CURRENT_USER của Registry).

Nhóm: Những người sử dụng giống nhau các chính sách hệ thống. nhưng cho phép ta áp dụng các chính sách hệ thống đến các nhóm người dùng (ghi vào khóa HKEY_CURRENT_USER của Registry).

Default Computer: Chỉ định thiết lập mặc định cho bất kỳ máy tính Windows 2000 hoặc Windows NT 4 trong miền (ghi vào khoá HKEY_LOCAL_MACHINE của Registry)

Computer: Cho phép ta tạo các chính sách tùy ý cho một máy tính cụ thể (ghi vào khoá HKEY_LOCAL_MACHINE của Registry).

Mặc định rằng không chính sách hệ thống nào được sử dụng trừ khi người quản trị tạo ra chúng.

Trong phần tiếp theo, ta sẽ học cách chọn để có thể cấu hình các chính sách

người dùng hoặc nhóm người dùng và các lựa chọn được quản lý thông qua các chính sách máy tính.

Để mà quản lý các chính sách hệ thống cho các người dùng và nhóm người dùng chỉ định, máy tính cài Windows 2000 Server của ta phải được cấu hình là **domain controller**.

4.1 Cấu hình các chính sách hệ thống người dùng và nhóm người dùng

Các chính sách đó ta có thể áp dụng cho tất cả mọi người dùng (through qua biểu tượng Default User), đến người dùng chỉ định hoặc đến một nhóm người dùng, nó cho phép ta điều khiển màn hình nền và các thiết lập hệ thống. Các lựa chọn chính sách hệ thống của người dùng và nhóm người dùng được diễn giải trong bảng sau. Các chính sách hệ thống nhắc đến WindowsNT vì chúng được thiết kế chủ yếu để điều khiển máy khách NT để tương thích với các thế hệ trước.

Bảng 3.7

Chính sách	Lựa chọn
Control Panel	Cho phép ta chỉ định thiết lập việc hiển thị như ẩn Screen Saver và Appearance của hộp thoại Display Properties.
Desktop	Cho phép ta cấu hình hình ảnh nền và cách phối màu.
Shell	Cho phép ta cấu hình sự hạn chế như việc ẩn Network Neighboothood và không ghi các thiết lập khi người dùng thoát.
System	Cho phép ta đặt các hạn chế như làm vô hiệu các công cụ soạn thảo Registry và chỉ cho phép chạy các ứng dụng Windows.
WindowsNT System	Cho phép ta chỉ định dù có phân tích được hay không tệp AUTOEXEC.BAT và dù có chạy đồng bộ hoá các kịch bản đăng nhập.
WindowsNT Shell	Cho phép ta cấu hình các thư mục Window NT và chỉ định hạn chế liên quan đến NT shell.

Mặc định, hệ thống khoá các chính sách hệ thống domain controller xác định trong NETLOGON dùng chung tệp NTCONFIG.POL. Nếu ta muốn các chính sách hệ thống của ta phải có hiệu lực trong hệ thống rộng, ta phải lưu ý và chia sẻ tệp này vì nó được chỉ định do người dùng khi chính sách hệ thống được tạo ra.

4.2 Quy định các chính sách hệ thống phù hợp

Dựa theo các điều kiện, quy định chính sách hệ thống sẽ được sử dụng nếu người dùng có nhiều chính sách hệ thống được định nghĩa do người dùng hoặc do các thành viên của nhóm.

Nếu người dùng có cấu hình tùy chọn chính sách hệ thống sẽ được sử dụng và các chính sách hệ thống này trong HKEYCURREN USER của Registry. Điều này cho phép chỉ định các chính sách người dùng để lấy thứ tự lên trên bất kỳ các chính sách hệ thống người dùng mặc định hoặc nhóm đang tồn tại. Điều này có nghĩa là các chính sách hệ thống của 1 nhóm sẽ không được sử dụng nếu tồn tại một chính sách hệ thống của một người dùng.

- ✓ Nếu người dùng là thành viên của bất kỳ nhóm nào có cấu hình các tùy chọn chính sách hệ thống và không có bất kỳ lựa chọn chính sách hệ thống cho người dùng được định nghĩa. Các chính sách hệ thống nhóm sẽ được hợp nhất vào phần HKEY_CURREN_USER trong Registry bởi thứ tự ưu tiên. Nếu có nhiều chính sách nhóm được định nghĩa, nó có thể xác định quyền ưu tiên của nhóm trong các tùy chọn của System Policy Editor.
- ✓ Nếu người dùng không lựa chọn bất kỳ chính sách hệ thống người dùng hoặc chính sách hệ thống nhóm nào được áp dụng, khoá HKEY_CURRENT_USER sẽ được cập nhật với bất kỳ sự thay đổi nào được tạo ra bởi các chính sách hệ thống Default User.
- ✓ Nếu hiện trạng người dùng và chính sách hệ thống cùng được thể hiện có các thiết lập xung đột cho các lựa chọn giống nhau, các lựa chọn chính sách hệ thống sẽ ghi đè lên cấu hình hiện trạng người dùng trong Registry.

Ví dụ: thưa nhận rằng Nam là một thành viên của các nhóm HR và Managers. Anh ta có các chính sách hệ thống người dùng thiết lập cho Nam và chính sách hệ thống nhóm được thiết lập cho HR mà Managers. Chính sách hệ thống nhóm cho Managers cao so với của HR. Các tùy chọn chính sách hệ thống người dùng và nhóm người dùng được cấu hình được liệt kê như sau:

Tùy chọn	HR	Manager	Nam
Color Schema	Xanh lá cây 256	Hồng 256	Xanh và đen
Hide Screen Server	Không thiết lập	Không thiết lập.	Ấn
Tab in Control Panel			
Hide Apperance	Không thiết lập	Ấn	Không thiết lập
Tab in Control Panel			

Shell Restriction, Hide Network Neighbohood	Không thiết lập	Ấn	Không thiết lập
Save Setting on Exit	Không thiết lập	Không thiết lập	Không thiết lập

Bảng 3.8 cơ sở của chính sách hệ thống:

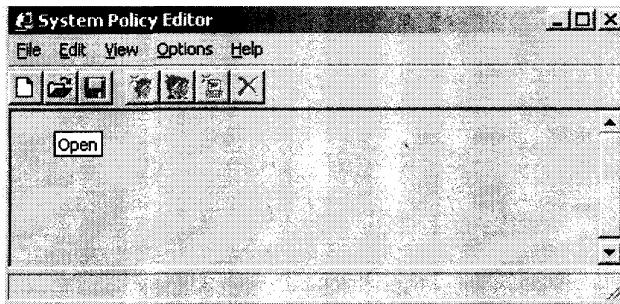
Tùy chọn	Các chính sách được so sánh với Nam
Color Schema	Xanh và đen (thông qua Nam thiết lập).
Hide Screen Saver Tab in Control Panel	Ấn (thông qua Nam thiết lập)
Hide Apperance Tab in Control Palnel	Ấn (thông qua Nam thiết lập)
Sell Restriction, Hide Neighborhood.	Không thiết lập (các chính sách hệ thống người Network dùng không sử dụng nếu các chính sách hệ thống tông tại).
Shell Restriction, Save Setting on Exit	Không thiết lập (các chính sách hệ thống người dùng không sử dụng nếu các chính sách hệ thống tông tại).

4.3 Tạo các chính sách hệ thống cho người dùng và nhóm người dùng

Nó rất rẽ sử dụng cho soạn thảo cấu hình người dùng thông qua System Policy Editor, nó là giao diện đồ họa (GUI), hơn thế nó có thể soạn thảo trên cơ sở văn bản Registry. Mặc dù vậy, khi ta sử dụng System Policy Editor, ta đang soạn Registry của ta, nhưng ta cần cẩn thận. Ta nên sao lưu Registry của ta trước khi thay đổi. Để cấu hình các chính sách hệ thống cho người dùng hoặc nhóm người dùng, hãy thực hiện theo các bước:

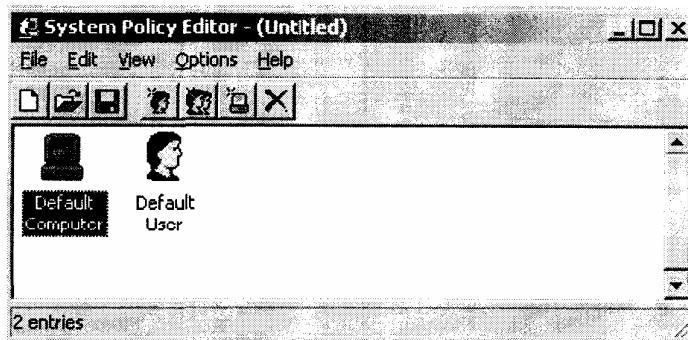
1. Chọn Start ->Run, gõ POLEDIT trong hộp hội thoại Run và bấm nút OK.
2. Cửa sổ System Policy Editor mở ra như trong hình 3.9. Chọn File -> New Policy.

Hình 3.9



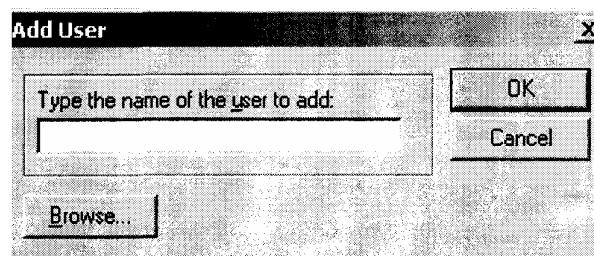
3. System Policy Editor hiển thị các biểu tượng cho Default Computer và Default User như hiển thị hình 3.10 . Chọn Edit -> Add User (hoặc Add Group) .

Hình 3.10



4. Hộp hội thoại Add User(hoặc Add Group) xuất hiện như trong hình 3.11. Ta cần gõ tên của người dùng (hoặc của nhóm) hoặc bấm vào nút Browse để chọn từ danh sách các người dùng (hoặc nhóm người dùng) được liệt kê sẵn. Sau khi ta thêm người dùng (mặc nhóm người dùng) bấm phím OK.

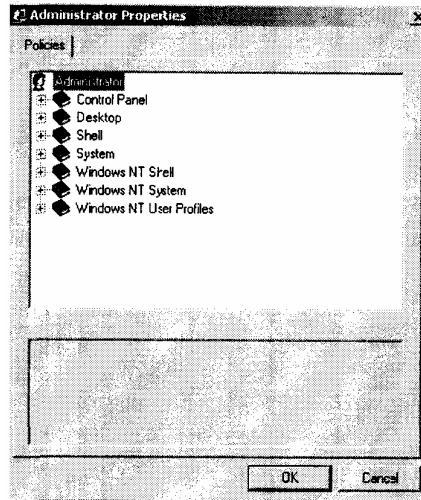
Hình 3.11



5. Người dùng hoặc nhóm người dùng được ta chọn xuất hiện trong cửa sổ System Policy Editor. Để soạn thảo hoặc hiển thị các thiết lập chính sách của người dùng (hoặc của nhóm người dùng) hãy nhấp kép vào người dùng hoặc nhóm người dùng).

6. Các chính sách sẽ được liệt kê trong phần Polices của hộp hội thoại Properties như trọng hình 3.12. Bấm vào các lựa chọn mà ta muốn cấu hình.

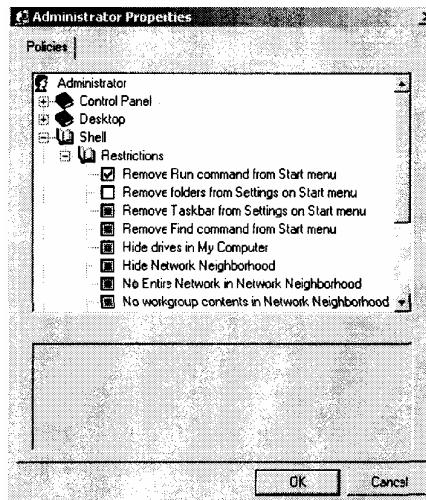
Hình 3.12



7. Ta xem trong danh sách tất cả các chính sách ta có thể định nghĩa. Hình 3.13 hiển thị một ví dụ về các chính sách Shell, Restriction. Bấm vào hộp chọn (check box) có thể cấu hình mỗi lựa chọn như sau:

- ✓ Hộp chọn màu xám có nghĩa là không chính sách nào được áp dụng.
- ✓ Đánh dấu trong hộp chọn có nghĩa là chính sách đó được áp dụng. Coi như đó là giá trị đúng.
- ✓ Hộp chọn trống (hay trắng) có nghĩa là chính sách đó không được áp dụng. Coi như đó là giá trị sai.

Hình 3.13



8. Lặp lại các bước 6 và 7 để cấu hình cho mỗi lựa chọn mà ta muốn. Sau khi tắt cả các lựa chọn được cấu hình. Bấm nút Ok

9. Sau khi kết thúc việc soạn thảo các chính sách về người dùng và nhóm người dùng, ghi lại các chính sách bằng cách chọn File -> Save.

Tạo các chính sách hệ thống cho một người dùng trên domain controller:

1. Sử dụng tiện ích Active Directory Users and Computer để tạo một người dùng Nam.
2. Chọn Start -> Run, gõ POLEDIT trong hộp hội thoại Run và bấm nút OK.
3. Trong cửa sổ System Policy Editor chọn File ->New Policy.
4. Chọn Edit ->Add User. Trong hộp hội thoại Add User bấm vào nút Browse. Chọn người dùng Nam và bấm nút Add, Sau đó bấm nút OK.
5. Nhấp kép vào người dùng Nam. Trong thành phần giao tiếp Policy chọn Shell tiếp đó là Restrictions. Đánh dấu hộp chọn Remove Run Command from Start Menu và hộp chọn Hide Drives in My Computer. Sau đó bấm nút OK.
6. Chọn File -> Save trong hộp hội thoại Save As chọn C:\WINNT\sysvol\sysvol\yourdomain\Scripts\NTCONFIG.POL.

4.4 Cấu hình các chính sách hệ thống máy tính

Cần quản lý thiết lập máy tính thông qua các chính sách hệ thống. Sau đây là một số các lựa chọn mà ta có thể cấu hình:

- ✓ Thiết lập mạng được sử dụng để điều khiển cập nhật chính sách hệ thống.
- ✓ Thiết lập hệ thống được sử dụng chạy các mục lúc khởi động.
- ✓ Thiết lập Windows NT Network để điều khiển cách các sự chia sẻ thiết bị ẩn được tạo.
- ✓ Thiết lập Windows NT Printers để điều khiển lựa chọn cấu hình máy in.
- ✓ Thiết lập Windows NT Remove Access để điều khiển lựa chọn truy cập từ xa.
- ✓ Thiết lập Windows NT Shell để điều khiển các mục đối tượng được khách hàng chia sẻ như các mục trong Desktop và trong thực đơn Start.
- ✓ Thiết lập Windows NT System được sử dụng cấu hình đăng nhập và thiết lập tệp hệ thống.

Thiết lập Windows NT User Profiles được sử dụng cấu hình các thiết lập hiện trạng người dùng. .

5. Sử dụng công cụ Security Configuration and Analysis

Windows 2000 Server bao gồm một tiện ích được gọi là Security Configuration and Analysis, ta có thể sử dụng để phân tích nhằm hỗ trợ việc cấu hình các thiết lập bảo mật nội bộ trong máy tính. Tiện ích này làm việc bằng cách so sánh cấu hình bảo mật hiện thời của ta với cấu hình mẫu trong các thiết lập đề nghị của ta.

Thực thi, cấu hình, quản lý và gỡ rối vấn đề bảo mật bằng cách sử dụng tập công cụ cấu hình bảo mật (Security Configuration Tool Set). Tiến trình phân tích bảo mật

gồm các bước sau:

1. Sử dụng tiện ích Security Configuration and Analysis, chỉ định cơ sở dữ liệu làm việc sẽ được sử dụng suốt thời gian phân tích bảo mật.
2. Mở mẫu về bảo mật mà ta sử dụng làm nền tảng để ta cấu hình sự bảo mật tương tự như mẫu này.
3. Thực hiện phân tích vấn đề bảo mật. Nó sẽ so sánh lại cấu hình của ta với mẫu mà ta đã chỉ định trong bước 2.
4. Xem lại kết quả của việc phân tích.
5. Quyết định bất cứ sự khác nhau nào được chỉ ra thông kết quả phân tích.

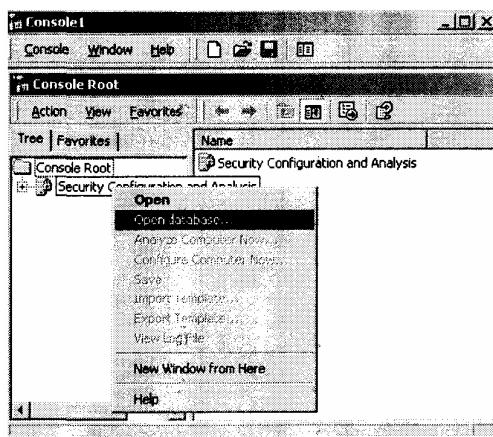
Tiện ích Security Configuration and Analysis có trong MMC. Sau khi ta thêm tiện ích này vào trong MMC, ta có thể chạy tiến trình phân tích bảo mật, nó được diễn giải trong phần tiếp theo.

5.1 Chỉ định cơ sở dữ liệu bảo mật

Cơ sở dữ liệu bảo mật được sử dụng để lưu trữ kết quả phân tích bảo mật của ta. Để chỉ định cơ sở dữ liệu bảo mật hãy thực hiện theo các bước sau:

1. Trong MMC bấm chuột phải vào Security Configuration and Analysis và chọn Open Database từ menu như trong hình 3.14:

Hình 3.14



Hộp hội thoại Open Database sẽ xuất hiện như trong hình 3.15. Trong ô Filename gõ tên tệp cơ sở dữ liệu ta sẽ tạo. Mặc định phần mở rộng của tệp là .sbd (cho cơ sở dữ liệu bảo mật). Bấm nút OK.

Hình 3.15

System Services	Đặt cơ chế bảo mật cho các phục vụ hệ thống mô hình khởi động mà các phục vụ của hệ thống nội bộ sẽ được sử dụng.
-----------------	---

Sau khi ta thêm Security vào MMC, ta có thể mở 1 mẫu bảo mật đơn giản và

thay đổi chúng như sau:

1. trong MMC bung nút Security Templates và mở thư mục cho \Windir\Security\Templates.
2. Nhập kép chuột vào bản mẫu mà ta muốn soạn thảo bao gồm **basicv** (basic server) và **basicdc** (basic domain controller).
3. Tạo mọi sự thay đổi mà ta muốn từ bản mẫu đơn giản này. Cũng thường chỉ là các chỉ định mà ta muốn hệ thống được cấu hình.

Sau đó ta ghi bản mẫu được lựa chọn, bấm chuột phải làm xuất hiện thực đơn và chọn tùy chọn Save As từ thực đơn này. Chỉ định vị trí và tên tệp cho bản mẫu mới này. Mặc định nó sẽ được ghi với phần mở rộng là .inf trong thư mục \Windir\Security\Templates

b) Mở mẫu bảo mật:

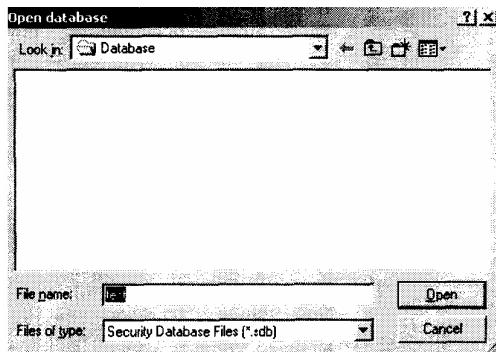
Sau khi ta cấu hình bản mẫu, ta có thể nhập nó để sử dụng cùng tiện ích Security Configuration and Analysis. Để nhập mẫu bảo mật trong MMC, bấm chuột phải vào tiện ích Security Configuration and Analysis và chọn Import Template. Sau đó chọn tệp mà ta muốn mở và bấm nút Open.

5.3 Phân tích bảo mật

Bước tiếp theo là thực hiện phân tích bảo mật. Để thực hiện việc phân tích này, bấm chuột phải vào tiện ích Security Configuration and Analysis và chọn Analyze Computer Now. Ta sẽ thấy hộp hội thoại Perform Analysis xuất hiện cho phép ta chỉ định vị trí và tên tệp cho đường dẫn tệp lưu trữ các lỗi sẽ được phát sinh trong suốt quá trình phân tích. Sau khi các thông tin đã được cấu hình, bấm nút OK. Khi việc phân tích hoàn thành, ta sẽ quay trở lại cửa sổ MMC chính. Từ đây ta có thể xem kết quả của quá trình phân tích bảo mật.

Hiển thị kết quả phân tích bảo mật và xác định những sự sai khác.

Kết quả của việc phân tích bảo mật được lưu trữ trong Security Configuration and Analysis, dưới mục bảo mật được cấu hình (xem bảng 3.9). Ví dụ để xem kết quả của các chính sách mật khẩu, nhấp kép chuột vào Security Configuration and Analysis, nhấp kép chuột vào Account Policies và nhấp kép chuột vào Password Policy. Hình 3.16 hiển thị ví dụ của kết quả của sự phân tích bảo mật cho các chính sách mật khẩu.



2. Hộp hội thoại Import Template mở ra, chọn mẫu mà ta muốn sử dụng. Ta có thể chọn các mẫu định nghĩa sẵn thông qua hộp hội thoại này. Trong phần tiếp theo, ta sẽ học cách tạo ra và sử dụng các tệp mẫu tùy biến. Ta chọn và bấm nút OK.

5.2 Mẫu bảo mật

Bước tiếp theo trong tiến trình phân tích bảo mật là nhập một mẫu về bảo mật. Mẫu này được sử dụng như công cụ so sánh. Tiện ích Security Configuration and Analysis so sánh thiết lập bảo mật của các thiết lập trong bản mẫu với các thiết lập hiện thời của ta. Ta không đặt bảo mật thông qua các mẫu. Đúng hơn là mẫu bảo mật chỉ là nơi mà ta tổ chức tất cả các thuộc tính bảo mật của ta trên vị trí đơn lẻ.

Với nhà quản trị, ta có thể định nghĩa một bản mẫu về bảo mật trên máy tính đơ lẻ và chuyển chúng cho tất cả các máy chỉ thông qua mạng.

a) Tạo mẫu bảo mật:

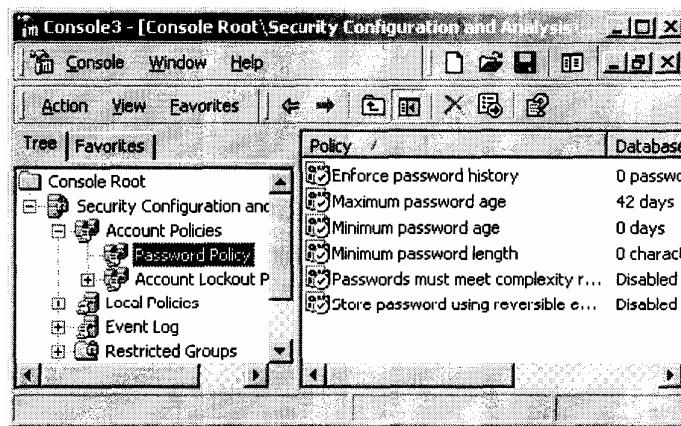
Ta tạo bản mẫu bảo mật thông qua Security Templates trong MMC. Ta có thể cấu hình nó với các mục như trong bảng 3.9 các cấu hình mẫu bảo mật sau:

Bảng 3.9

Mục của mẫu bảo mật	Giải thích
Account Policies	Chỉ định cấu hình phải được sử dụng cho các chính sách mật khẩu, các chính sách kiểm soát tài khoản thử đăng nhập và các chính sách Kerberos.
Local Policies	Chỉ định cấu hình phải được sử dụng cho các chính sách kiểm định, các chính sách quyền người dùng và các lựa chọn bảo mật.
Event Log	Cho phép ta đặt thiết lập cấu hình áp dụng cho các tệp nhật ký của Event Viewer.
Restricted Groups	Cho phép ta quản trị các thành viên của nhóm nội bộ

Registry	Chỉ định bảo mật cho các khoá Registry nội bộ.
File System	Chỉ định bảo mật cho các tệp hệ thống nội bộ.

Hình 3.16



Các chính sách đã được phân tích sẽ có các dấu X hoặc ✓ tại mỗi chính sách như hiển thị trong hình trên. Dấu X có biểu thị chính sách mẫu và chính sách hiện thời là không tương ứng. Dấu ✓ có biểu thị chính sách mẫu và chính sách hiện thời là tương ứng. Nếu có bất kỳ sự trái ngược nào đã được biểu diễn, ta phải sử dụng Group Policy để giải quyết sự tranh chấp ấy.

Ví dụ: Sử dụng Security Configuration and Analysis ở phần này ta sẽ thêm Security Configuration and Analysis vào MMC, chỉ định ra một cơ sở dữ liệu bảo mật, tạo một mẫu bảo mật, nhập mẫu bảo mật, thực hiện phân tích và xem xét kết quả. Thêm tiện ích Security Configuration and Analysis

1. Chọn Start -> Programs ->Administrative Tools ->security.
2. Chọn Console -> Add/Remove Snap-in.
3. Trong hộp hội thoại Add/Remove Snap-in bấm chuột vào nút Add. Chọn Security Configuration and Analysis rồi bấm vào nút Add. Rồi bấm vào nút Close.
4. Trong hộp hội thoại Add/Remove Snap-in bấm nút OK

Chỉ định cơ sở dữ liệu bảo mật:

1. Trong MMC bấm chuột phải vào Security Configuration and Analysis, chọn Open Database.
2. Trong hộp hội thoại Open Database gõ sampledb trong hộp nhập tên tệp. Sau đó bấm Open.
3. Trong hộp hội thoại Import Template chọn mẫu baicsv và bấm nút Open.

Tạo mẫu bảo mật:

1. Trong MMC chọn Chọn Console -> Add/Remove Snapin.
2. Trong hộp hội thoại Add/Remove Snap-in bấm chuột vào nút Add. Chọn Security Template rồi bấm vào nút Add. Rồi bấm vào nút Close.
3. Trong hộp hội thoại Add/Remove Snap-in bấm nút OK.
4. Mở mục Security Template sau đó mở thư mục Window NT\Security\Templates.
5. Nhấp đúp vào tệp basicsv.
6. Chọn Account Policies, sau đó là Password Policy.
7. Soạn thảo các chính sách mật khẩu theo các bước sau:
 - ✓ Đặt tùy chọn Enforce Password History là nhớ 10 mật khẩu.
 - ✓ Thiết lập tùy chọn Passwords Must Meet Complexity Requirements là cho phép.
 - ✓ Đặt tuổi thọ tối đa là 30 ngày.
8. Chọn tệp basicsv và bấm vào tựu chọn Save As.
9. Trong hộp hội thoại Save As gõ tên tệp servertest vào thư mục mặc định. Bấm nút Save.

Nhập mẫu bảo mật:

1. Chọn Security Configuration and Analysis, bấm chuột phải và chọn Import Template.
2. Trong hộp hội thoại Import Template chọn tệp servertest và bấm nút Open.

Thực hiện và xem xét kết quả phân tích bảo mật:

1. Chọn Security Configuration and Analysis bấm chuột phải và chọn Analyze Computer Now.
2. Trong hộp hội thoại Perform Analysis chấp nhận đường dẫn mặc định cho tệp ghi lại lỗi và bấm nút OK.
3. Khi quay trở lại cửa sổ chính MMC nhấp đúp vào Security Configuration and Analysis.
4. Nhấp đúp vào Account Policies và nhấp đúp vào Password Policy. Ta sẽ thấy kết quả của sự phân tích cho mỗi chính sách được chỉ định bởi dấu X và √ cạnh mỗi chính sách.

Tổng kết chương

Trong chương này ta đã học được về các đặc tính của Windows 2000 Server. Nó bao phủ các chủ đề :

- ✓ Thiết lập bảo mật, nó có thể được áp dụng cho mức nội bộ hoặc mức miền. Việc quản lý các chính sách bảo mật nội bộ, sử dụng Group Policy với đối tượng Local Computer Group Policy. Để quản lý các chính sách bảo mật miền sử dụng Group Policy với đối tượng Domain Controller Group Policy.
- ✓ Các chính sách tài khoản điều khiển tiến trình đăng nhập. Có 3 loại chính sách tài khoản là mật khẩu, chính sách kiểm soát sự vi phạm đăng nhập và chính sách Kerberos.
- ✓ Các chính sách nội bộ điều khiển những cái mà ta có thể làm với máy tính nội bộ. Có 3 loại chính sách gồm: kiểm định, ấn định quyền người dùng, và các chính sách lựa chọn bảo mật.
- ✓ Các chính sách hệ thống được sử dụng định nghĩa môi trường Desktop của người dùng. Trong Window 2000 các chính sách hệ thống này được giữ lại nhằm tương thích với máy khách Window 9x và WindowsNT.
- ✓ Tiện ích Security and Analysis Configuration được sử dụng phân tích cấu hình bảo mật của ta. ta thực hiện tiện ích này để so sánh thiết lập bảo mật tồn tại với cấu hình mẫu đi ta thiết lập sự sai khác.

CHƯƠNG 4: QUẢN TRỊ TÀI NGUYÊN (4 lý thuyết)

1. Quản lý ổ đĩa

Các ví dụ nhằm mục đích trực quan của Microsoft sẽ được trình bày trong chương này.

- ✓ Điều khiển, cấu hình, khắc phục sự cố ổ đĩa và bộ đĩa (volumes).
- ✓ Cấu hình nén dữ liệu.
- ✓ Điều khiển và cấu hình Disk Quotas.
- ✓ Khôi phục dữ liệu từ đĩa lỗi.
- ✓ Mã hoá dữ liệu trên một ổ đĩa cứng bằng Hệ thống mã hoá file (EFS - Encrypting File System).

Khi tiến hành cài đặt Windows 2000 Server, ta sẽ phải chọn lựa cách định dạng ban đầu cho các ổ đĩa của mình. Với các tiện ích và các đặc tính sẵn có của Windows 2000 Server, chúng ta có thể thay đổi cấu hình và thực hiện các tác vụ quản lý đĩa.

Đối với việc cấu hình hệ thống file, ta có thể chọn FAT, FAT32 hoặc NTFS. Chúng ta cũng có thể chuyển đổi các phân vùng FAT16 hay FAT32 sang NTFS. Một nhân tố khác trong quản lý đĩa là phải quyết định xem các ổ đĩa vật lý được cấu hình như thế nào. Windows 2000 Server hỗ trợ hai kiểu lưu trữ đó là lưu trữ cơ sở và lưu trữ động. Trong trường hợp cài đặt Windows 2000 Server hay cập nhật từ WinNT, các ổ đĩa đều được cấu hình dưới dạng lưu trữ cơ sở. Lưu trữ động là một kỹ thuật mới của Windows 2000 Server, nó cho phép tạo ra các bộ đĩa (volumes) simple, spanned, striped, minored và RAID-5.

Một khi đã quyết định được việc các ổ đĩa của mình cần được cấu hình như thế nào, ta sẽ sử dụng tiện ích Disk Management để làm điều đó. Tiện ích này cho phép xem và quản lý các địa vật lý và các volumes. Trong phạm vi của chương này, ta sẽ học cả hai kiểu lưu trữ và việc cập nhật từ kiểu lưu trữ cơ sở thành kiểu lưu trữ động. Các tính năng khác của quản lý ổ đĩa như nén dữ liệu, disk quotas, mã hóa dữ liệu, tối ưu đĩa dọn đĩa cũng sẽ được đề cập trong chương này.

Trên cả hai hệ điều hành Windows 2000 Server và Professional, các thủ tục của các tác vụ quản lý đĩa là giống nhau. Sự khác biệt lớn nhất là Windows 2000 Professional không hỗ trợ các volumes Minored và RAID-5.

Cấu hình các hệ thống tập tin Các hệ thống tập tin được sử dụng để lưu trữ và định vị các tập tin được lưu trên ổ đĩa cứng. Như đã nói trong chương I, "Bắt đầu với Windows 2000 Server", Windows 2000 Server hỗ trợ các hệ thống file FAT16, FAT32 và NTFS. Ta nên chọn FAT16 hoặc FAT32 nếu muốn khởi động theo chế độ dual-boot. Hoặc chọn NTFS để có các tính năng nâng cao khác chẳng hạn như bảo mật cục bộ, nén file và mã hóa file. Bảng 4.1 tóm tắt những tính năng của mỗi hệ thống file.

Bảng 4.1 các tính năng của hệ thống file:

Tính năng	FAT16	FAT32	NTFS
Hỗ trợ các hệ điều hành	Hầu hết	Win95, OSR2, Windows98, Windows2000	WindowsNT, Windows2000
Hỗ trợ tên file dài	Có	Có	Có
Sử dụng hiệu quả không gian đĩa trống	Không	Có	Có
Hỗ trợ nén	Không	Không	Có
Hỗ trợ Quota	Không	Không	Có
Hỗ trợ mã hóa	Không	Không	Có
Hỗ trợ bảo mật cục bộ	Không	Không	Có
Hỗ trợ bảo mật mạng	Có	Có	Có
Kích thước Volumes lớn nhất	2GB	32GB	2TB

Windows 2000 Server cũng hỗ trợ CDFS (Compact Disk File System). Tuy nhiên CDFS không được quản lý. Chúng chỉ được sử dụng để cài đặt và đọc đĩa CDs.

Windows 2000 cung cấp tiện ích dòng lệnh CONVERT để chuyển đổi các phân vùng FAT16 hoặc FAT32 sang NTFS. Cú pháp của lệnh CONVERT : CONVERT [ô đĩa:] / fs : ntfs

Chuyển đổi một phân vùng FAT 16 sang NTFS .

1. Copy một số thư mục sang ô đĩa D.
2. Chọn Start ->Programs -> Accessories ->command Prompt.
3. Trong hộp thoại Command Prompt, đánh lệnh CONVERT D: /fs:ntfs và nhấn Enter.
4. Sau khi quá trình chuyển đổi hoàn tất, đóng cửa sổ Command Prompt. Quá trình chuyển đổi không xảy ra ngay nhưng nó sẽ có hiệu lực sau khi máy được khởi động lại.
5. Kiểm tra tại xem thư mục của ta đã copy trong bước 1 vẫn tồn tại trên phân vùng này.

1.1. Sử dụng các tiện ích quản lý đĩa

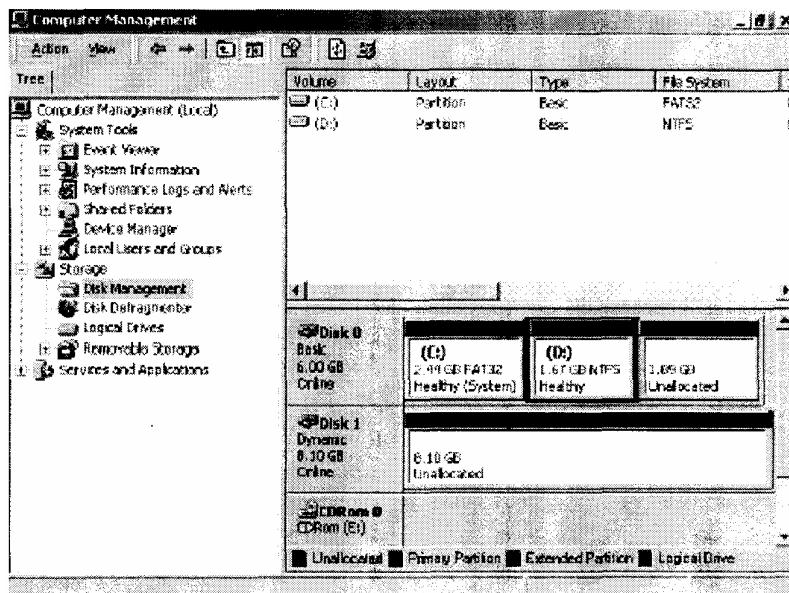
Trên môi trường Windows 2000 Server, công cụ quản lý đĩa là một công cụ đồ họa cho công việc quản lý đĩa và volumes. Trong phần này, ta sẽ học cách làm thế nào để truy cập một tiện ích quản lý đĩa và cách sử dụng nó để thực hiện các tác vụ cơ bản, quản lý các vùng lưu trữ cơ sở và lưu trữ trong.

Điều khiển, cấu hình, và sửa lỗi đĩa và volumes.

Để có được các quyền đầy đủ trong việc sử dụng tiện ích quản lý đĩa, ta nên đăng nhập vào hệ thống với quyền quản trị hệ thống. Để sử dụng công cụ này, mở Control Panel -> Administrator Tools -> Computer Management. Mở rộng thư mục Storage để thấy công cụ quản lý đĩa (Disk Management Utility). Công cụ này đang được mở như trong hình 4.1.

Một cách khác để kích hoạt công cụ Disk Management là kích chuột phải vào My Computer -> chọn Manage -> mở rộng mục Computer Management, mở rộng mục Storage và cuối cùng là Disk Management. Tất nhiên, chúng ta cũng có thể thêm Disk Management vào cửa sổ MMC.

Hình 4.1.



Cửa sổ chính thể hiện các thông tin:

- ✓ Các Volumes được nhìn thấy bởi máy tính.
- ✓ Kiểu của một phân vùng: cơ sở hoặc là động.
- ✓ Kiểu của file hệ thống được sử dụng cho mỗi phân vùng.
- ✓ Trạng thái của mỗi phân vùng để biết được phân vùng đó chứa phân vùng hệ thống hay phân vùng khởi động.
- ✓ Dung lượng, tổng số không gian đĩa trống định phần trên một phân vùng.

- ✓ Tổng số không gian đĩa trống còn lại trên mỗi phân vùng.
- ✓ Sự vượt quá giới hạn liên quan đến phân vùng.

Các tác vụ quản lý đĩa cơ bản:

Với tiện ích Disk Management, ta có thể thực hiện hàng loạt các tác vụ cơ bản như:

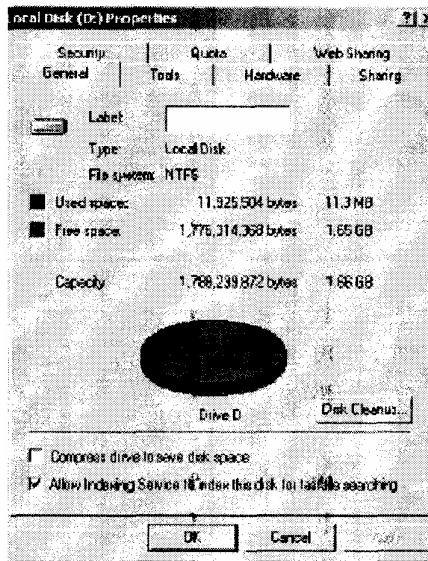
- ✓ Xem thuộc tính đĩa và volume.
- ✓ Thêm vào một đĩa mới.
- ✓ Tạo các phân vùng và volumes.
- ✓ Chuyển từ đĩa cơ sở lên thành đĩa động.
- ✓ Thay đổi tên và đường dẫn của đĩa.
- ✓ Xóa các phân vùng và các volumes.

Xem các thuộc tính của Volume và đĩa cục bộ:

Trên địa động, ta quản lý các thuộc tính của volume. Trên đĩa cơ sở, ta quản lý các thuộc tính của đĩa cục bộ. Các volumes và các đĩa cục bộ thực hiện những chức năng như nhau, và các tùy chọn được thảo luận trong phần sau đây được áp dụng cho cả hai loại trên. Một ví dụ dựa trên một đĩa động sử dụng simple volume. Nếu ta sử dụng lưu trữ cơ sở, ta sẽ xem các thuộc tính của đĩa cục bộ hơn là thuộc tính của các volume.

Để xem các thuộc tính của một volume, kích chuột phải lên phần trên của cửa sổ chính Disk Management và chọn Properties. Một hộp thoại Properties sẽ hiện ra như hình 4.2.

Hình 4.2.



Trong hộp thoại này, các thuộc tính của volume được tổ chức trên bảy Tab (5 tạo thông tin FAT của volumes): General, Tools, Hardware, Sharing, Security, Quota và Web Sharing. Tab ,Security và Quota chỉ xuất hiện đối với các volumes NTFS. Các Tab này sẽ được trình bày chi tiết trong các phần dưới đây.

Thiết lập các thuộc tính chung

Các thông tin trên Tab General (hình 4.2) chỉ ra cho ta các thông tin về cấu hình volumes. Hộp thoại này cho ta biết tên, kiểu, hệ thống file, không gian đĩa đã sử dụng, không gian đĩa trống và dung lượng của volume. Tên của volumes được chứa trong hộp văn bản có thể thay đổi. Không gian của volumes được thể hiện đồng thời dưới dạng đồ họa và văn bản.

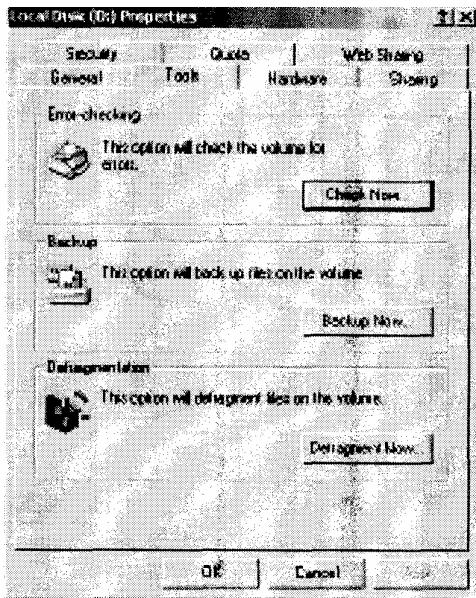
Tên của volume hay ổ đĩa cục bộ chỉ có mục đích thể hiện thông tin. Ví dụ tùy thuộc vào mục đích sử dụng ta có thể đặt tên là APPS hoặc ACCTDB. Nút Disk Cleanup sẽ kích hoạt tiện ích Disk Cleanup, cho phép ta xoá các file không cần thiết và giải phóng không gian đĩa. Tiện ích này sẽ được đề cập chi tiết hơn trong mục sau của chương này " Sử dụng tiện ích Disk Cleanup".

Làm việc với các công cụ.

Tab Tools trong hộp thoại Properties của ổ (Hình 4.3) cung cấp 3 công cụ:

- ✓ Kích chuột vào nút Check Now để chạy tiện ích kiểm tra đĩa (Check Disk). Ta muốn kiểm tra lỗi của ổ nếu ta thấy các lỗi về truy suất ổ đĩa hoặc ổ này đang được mở trong khi hệ thống phải khởi động với việc tắt máy không đúng cách. Tiện ích Check Disk sẽ được đề cập đến trong phần " Khắc phục lỗi các đĩa và ổ chín của chương này".
- ✓ Kích chuột vào nút Backup Now để chạy tiện ích sao lưu (Backup Wizard).Quá trình sao lưu file có các bước hướng dẫn để ta làm theo.
- ✓ Kích chuột vào nút Defragment để chạy tiện ích chống phân mảnh đĩa (Defragmentation). Tiện ích này chống phân mảnh các tệp trên volume bằng cách sắp các tệp một cách liên tục trên ổ đĩa cứng. Công cụ chống phân mảnh sẽ được bàn chi tiết hơn trong chương này trong phần "Chống phân mảnh đĩa".

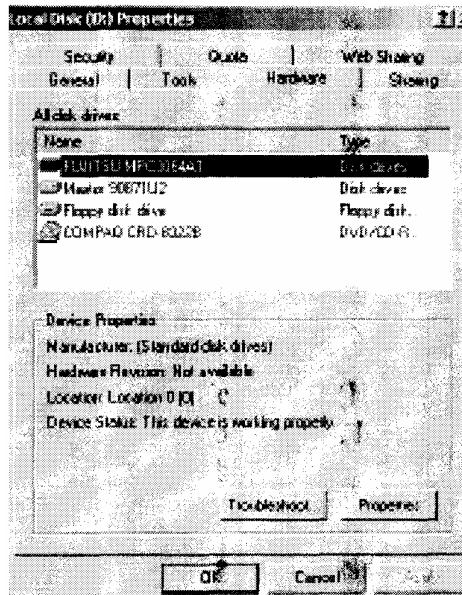
Hình 4.3.



Xem các thông tin phần cứng.

Tab Hardware trong hộp thoại Properties của ổ (Hình 4.4) liệt kê phần cứng kết hợp với các ổ đĩa được nhận ra bởi hệ điều hành Windows 2000. Nửa dưới của hộp thoại chỉ ra các thuộc tính của thiết bị được chọn ở nửa trên của hộp thoại.

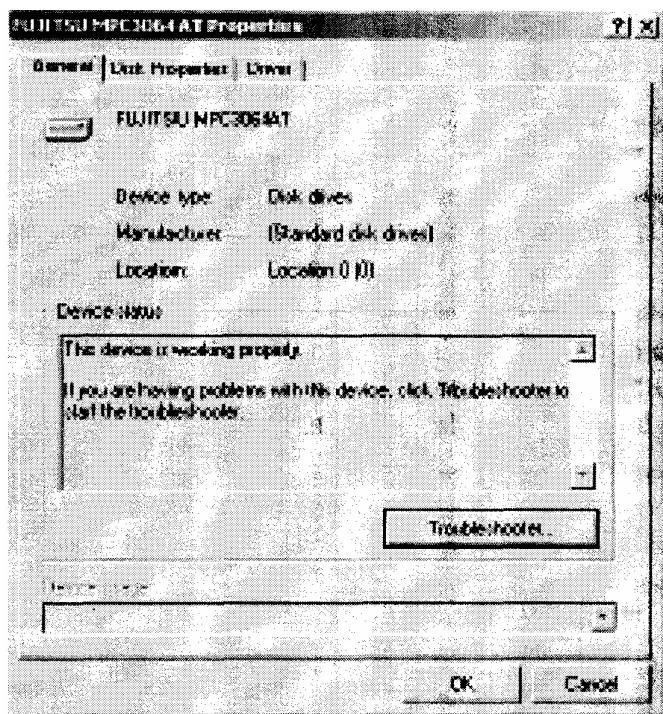
Hình 4.4



Để có thêm chi tiết hơn về mỗi thiết bị phần cứng, hiện thanh sáng lên phần cứng đó và nhấp vào nút Properties ở góc bên trái của hộp thoại. Một hộp thoại Properties của thiết bị này sẽ xuất hiện. Hình 4.5 chỉ ra một ví dụ của hộp thoại các thuộc tính của ổ đĩa. Nếu may mắn trạng thái thiết bị của ta sẽ đưa ra là: thiết bị đang hoạt động bình thường". Nếu thiết bị làm việc không bình thường, ta có thể nhấp vào

nút Troubleshooting Wizard tìm ra lỗi mà thiết bị đó đang gặp phải.

Hình 4.5.

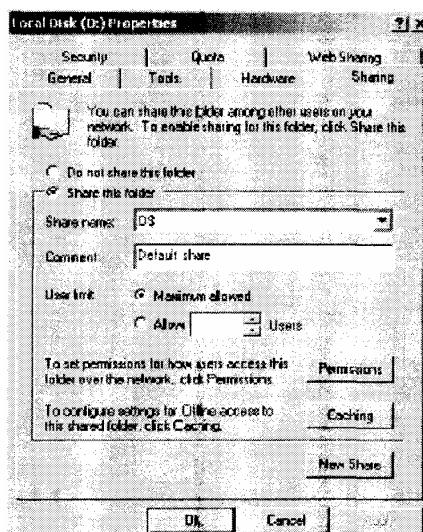


Chia sẻ các Volumes

Tab Sharing trong hộp thoại Properties của ổ (trong hình 4.6) cho phép ta xác định ổ nào có được chia sẻ hay không. Mặc định tất cả các ổ đĩa đều được chia sẻ.

Tên chia sẻ là ký tự ổ đĩa được sau bởi ký hiệu \$ (ký hiệu dollar). Ký hiệu \$ biểu thị rằng sự chia sẻ này đã được ẩn đi. Từ hộp thoại này ta có thiết đặt quyền hạn người dùng, cấp phép, bộ nhớ tạm thời cho sự chia sẻ này. Vấn đề về chia sẻ sẽ được đề cập trong phần sau "Quản lý tệp tin và thư mục".

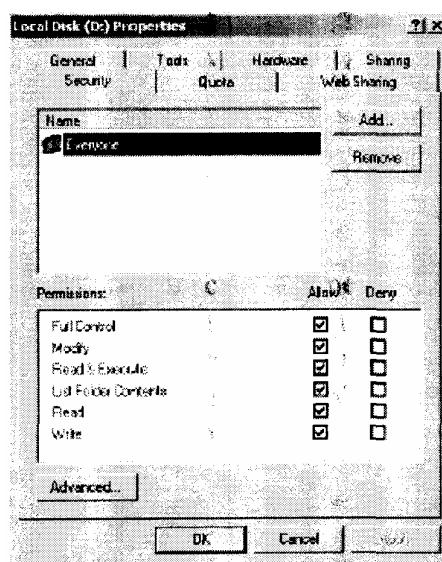
Hình 4.6



Thiết lập các tùy chọn bảo mật.

Tab Security trên hộp thoại Properties của volumes (Hình 4.7) chỉ xuất hiện nếu ổ đĩa là NTFS. Tab Security thường được dùng để thiết đặt các quyền NTFS cho ổ đĩa. Chú ý rằng quyền mặc định cho phép nhóm Everyone có tất cả các quyền trên thư mục gốc của ổ đĩa. Điều này là nguyên nhân chính gây ra các vấn đề về bảo mật khi có một người dùng nào đó thực hiện các thao tác hay xóa dữ liệu trên volumes này. Vấn đề về quản lý bảo mật hệ thống file sẽ được trình bày trong phần 2 quản lý tệp tin và thư mục.

Hình 4.7



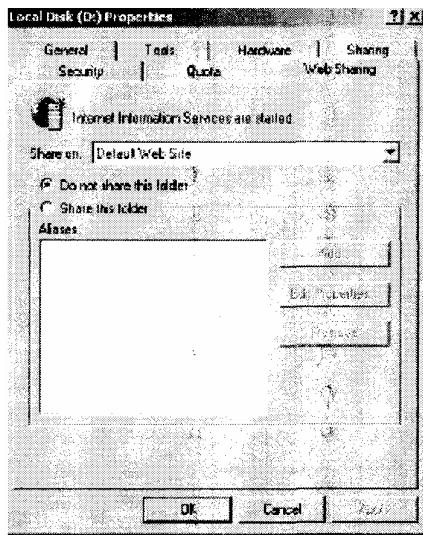
Đặt hạn ngạch đĩa

Giống như Tab Security, tab Quota trên hộp thoại Properties chỉ xuất hiện nếu volume là NTFS. Thông qua tập này ta có thể giới hạn không gian đĩa của người dùng. Các giới hạn sẽ được đề cập chi tiết trong phần "Đặt các giới hạn của ổ đĩa" trong chương này.

Thiết lập chia sẻ Web.

Theo mặc định, Internet Information Services (IIS) được cài đặt và khởi động trên máy tính có hệ điều hành Windows 2000 Server. Nếu phục vụ này đang chạy ta sẽ thấy một Tab cho sự chia sẻ Web, tab Web Sharing (giống như hình 4.8) nó thường dùng để thiết lập các thư mục chia sẻ cho IIS.

Hình 4.8



Thêm một ổ đĩa mới.

Để tăng dung lượng lưu trữ của ổ đĩa, ta có thể thêm một ổ đĩa mới. Đây là công việc phổ biến mà ta cần phải thực hiện khi các chương trình ứng dụng và các tệp của ta có kích thước lớn lên nhanh chóng. Việc thêm một ổ đĩa phụ thuộc vào máy tính của ta có cung cấp sự chuyển đổi nóng (Hot Swapping) giữa các ổ đĩa hay không. Hot Swapping là khả năng thêm ổ cứng mới trong khi máy tính đang bật. Hầu hết máy tính không cung cấp khả năng này.

Các máy tính không cung cấp Hot Swap.

Nếu máy tính của ta không cung cấp Hot Swapping, ta cần phải tắt máy trước khi thêm một ổ cứng mới. Việc cài điều kiện cho ổ đĩa tiến hành theo hướng dẫn của nhà sản xuất. Khi công việc kết thúc, hãy khởi động lại máy tính. Ổ đĩa mới này được liệt kê trong tiện ích Disk Management. Ta sẽ được nhắc nhớ để đặt tên cho đĩa mới này vì nó sẽ được nhận ra bởi Windows 2000 Server. Theo mặc định, ổ mới này sẽ được cấu hình giống như ổ Dynamic.

Các máy tính cung cấp Hot Swap.

Nếu máy tính cung cấp Hot Swapping, ta không nhất thiết phải tắt máy tính mà chỉ cần cài đặt bộ điều khiển theo hướng dẫn của nhà sản xuất. Tiếp đến, ta mở công cụ quản lý đĩa Disk Management và chọn Action -> Rescan Disk. Ổ đĩa mới sẽ xuất hiện trong Disk Management.

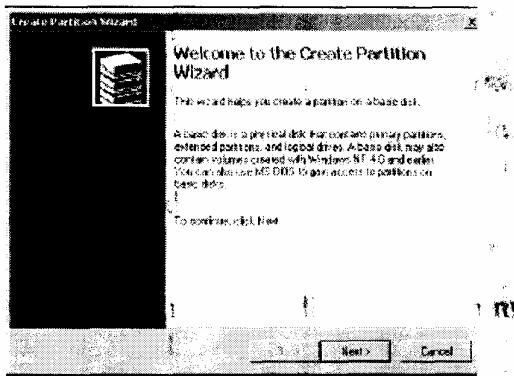
Tạo các phân vùng và ổ đĩa (Volumes).

Nếu ta có khoảng trống chưa được định dạng trên ổ đĩa cơ sở (basic disk) và ta muốn tạo một ổ đĩa logical, ta phải tạo một phân vùng. Nếu có một không gian chưa được định dạng trên ổ đĩa động (Dynamic) và muốn tạo ổ đĩa logic, ta phải tạo một đĩa mới (volumes). Quá trình tạo các phân vùng và volumes được mô tả ở phần dưới đây.

Tạo một phân vùng (Partition).

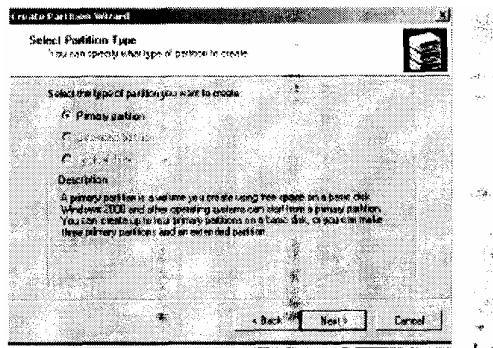
Để tạo một phân vùng từ không gian chưa được định dạng trên một đĩa Basic, ta sử dụng tiện ích Create Partition theo các bước hướng dẫn sau:

1. Kích chuột phải vào diện tích của không gian trống và chọn Create Logical Drive từ menu thả xuống.
2. Hộp thoại Create Partition Wizard hiện lời chào như hình 4.9. Nhấp vào nút Next để tiếp tục.



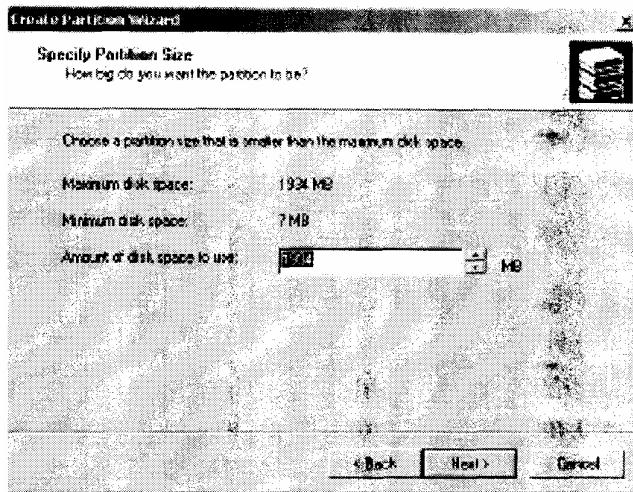
3. Hộp thoại Select Partition Type xuất hiện như hình 4.10. Trong hộp thoại này ta chọn kiểu của phân vùng muốn tạo: primary, extended, logic drive. Chỉ có các tùy chọn được hỗ trợ bởi máy tính của ta là có sẵn. Kích chuột vào nút radio để lựa chọn kiểu, sau đó nhấn vào nút Next.

Hình 4.10



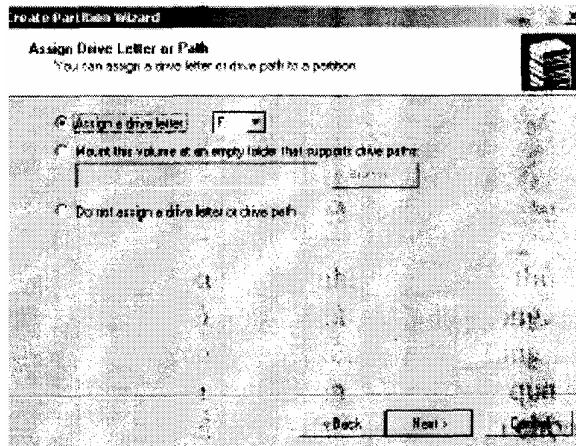
4. Hộp thoại Specify Partition Size xuất hiện, như hình 4.11. Ở đây ta xác định kích thước lớn nhất của phân vùng, Kích thước tối đa là lượng không gian còn trống được hệ điều hành nhận ra. Sau đó nhấp vào nút Next để tiếp tục.

Hình 4.11



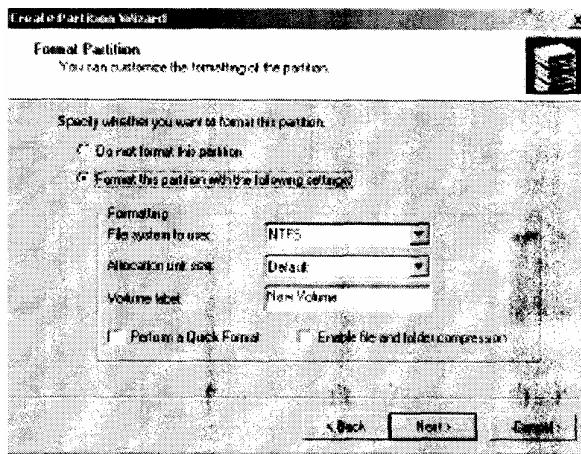
5. Hộp thoại Assign Drive Letter or Path xuất hiện như hình 4.12, thông qua hộp thoại này ta có thể xác định tên ổ đĩa, dung lượng ổ đĩa thư là một mục rỗng, hoặc chọn không chọn không gán tên cho ổ đĩa hay đường dẫn ổ đĩa. Nếu ta chọn dung lượng ổ giống như một thư mục rỗng, ta có thể có số lượng không giới hạn các ổ và bỏ qua giới hạn tên ổ đĩa. Hãy quyết định sự lựa chọn của ta sau đó nhấp vào nút next. Nếu ta chọn không xác định tên ổ đĩa hoặc đường dẫn, người dùng sẽ không thể truy cập tới phân vùng này.

Hình 4.12



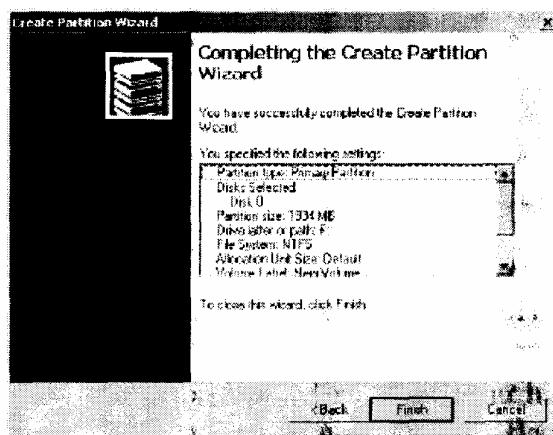
6. Hộp thoại Format Partition xuất hiện, như hình 4.13. Hộp thoại này cho phép ta có Forlnat phân vùng này hay không. Nếu ta chọn để format ổ này (volume) ta có thể format nó là FAT, FAT32, hoặc NTFS. Ta cũng có thể lựa chọn kích thước cho một đơn vị. Nhập vào một nhãn cho đĩa (thể hiện thông tin), xác định một format nhanh, hoặc chọn cho phép nén thư mục và ổ đĩa. Xác định một format nhanh thì rất mạo hiểm bởi vì nó không quét đĩa để tìm ra các sector bị hỏng (format bình thường sẽ làm điều này). Sau khi ta đưa ra lựa chọn của mình, nhấp vào nút Next.

Hình 4.13



7. Khi hoàn thành hộp thoại Create Partition Wizard xuất hiện như hình 4.14. Xác nhận lựa chọn của ta. Nếu cần thay đổi lại các thiết đặt, nhấp vào nút Back để quay lại các hộp thoại mong muốn. Ngược lại nhấp vào nút Finish.

Hình 4.14



Tạo một Volume:

Khi ta nhấp chuột phải vào diện tích của khoảng trống trên đĩa dynamic và chọn Create Volum, tiệm Create volume sẽ bắt đầu. Tiệm ích này sẽ hiện một chuỗi các hộp thoại để hướng dẫn ta trong suốt quá trình tạo partition.

Hộp thoại Select Volume Type cho phép ta chọn kiểu của volum ta muốn tạo. Các lựa chọn bao gồm simple volume, spanned volume, striped volume, mirrored volume, hoặc RAID-5 volume.

Hộp thoại Select Disks cho phép ta chọn đĩa và kích thước của volume để bắt đầu tạo.

Hộp thoại Assign Drive Letter or Path cho phép gán tên ổ đĩa hoặc giống như một đường dẫn. Đây cũng là tùy chọn không gán tên ổ đĩa hay đường dẫn, nhưng nếu ta chọn lựa chọn này người dùng sẽ không truy cập được volume này.

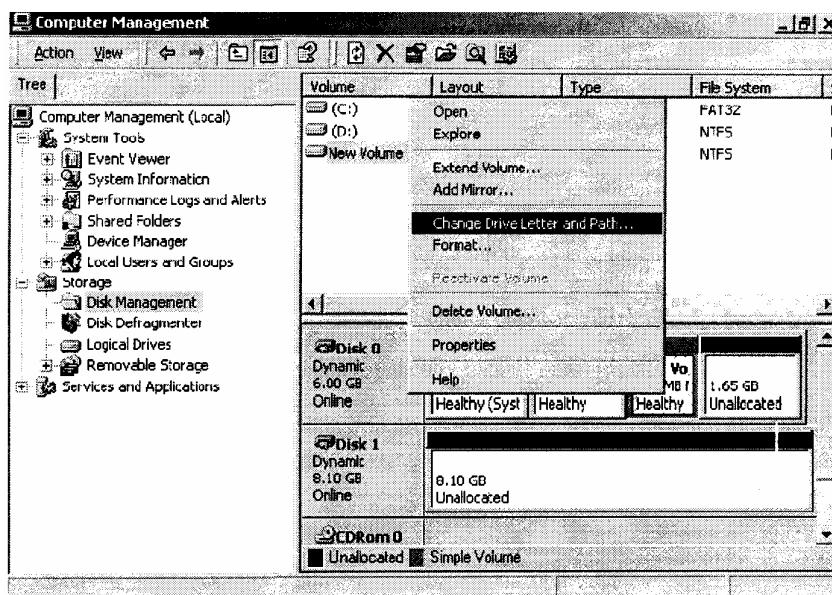
Hộp thoại Format Volume chỉ cho ta có muốn format volume này hay không, ta có thể chọn tệp hệ thống, xác định kích thước và tên của volume. Ta cũng có thể chọn để thực hiện thao tác format nhanh và cho phép nén tệp và thư mục.

Thay đổi tên ổ đĩa và đường dẫn.

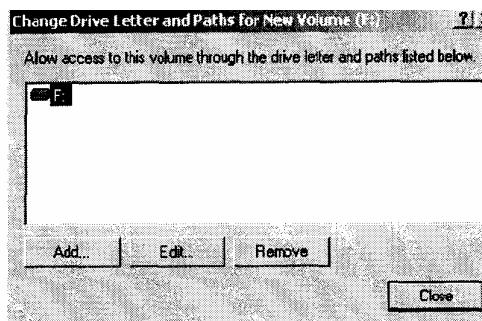
Giả sử rằng ta có ổ đĩa C : được xác định là partition đầu tiên và ổ đĩa D: được xác định là ổ đĩa CD. Ta thêm 1 ổ đĩa và partition mới với một volume mới. Theo mặc định, partition mới thêm vào được đặt tên là ổ đĩa E. Nếu ta muốn các ổ đĩa logic của ta xuất hiện trước ổ đĩa CD, ta có thể sử dụng tùy chọn Change Drive Letter and Path của tiện ích Disk Management để tổ chức lại các ký tự hiển thị ổ đĩa của ta.

Khi ta muốn tổ chức lại các ký tự hiển thị ổ đĩa, kích chuột phải vào volume mà ta muốn đổi tên và chọn tùy chọn Change Driver Letter and Path, như chỉ ra trên hình 4.15. Cửa sổ Change Drive Letter and Path cho ổ đĩa hiện ra như ở trong hình 4.16. Nhấn nút Edit để mở cửa sổ Edit Drive Letter or Path. Sử dụng danh sách thả xuống cạnh tùy chọn Assign a Drive Letter để chọn ký tự ổ đĩa mà ta muốn đặt cho ổ đĩa đó. Cuối cùng, hãy xác nhận các thay đổi khi được hỏi.

Hình 4.15



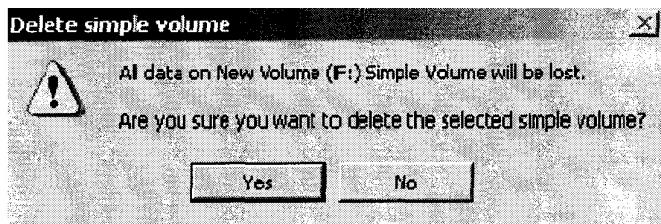
Hình 4.16



Xóa các phân vùng đĩa và các ổ đĩa

Ta có thể muốn xóa một phân vùng đĩa hoặc ổ đĩa nếu ta muốn tổ chức lại đĩa cứng của ta hoặc để đảm bảo rằng dữ liệu sẽ không còn được truy cập. Một khi ta xóa một phân vùng đĩa hoặc ổ đĩa nó sẽ bị loại bỏ mãi mãi. Để xóa một phân vùng đĩa hoặc ổ đĩa ta muốn xóa và chọn tùy chọn Delete Volume (hay Delete Partition). Ta sẽ bắt gặp một hộp thoại cảnh báo rằng ta sẽ mất tất cả các dữ liệu trên phân vùng đĩa hoặc ổ đĩa đó, như được chỉ ra trong hình 4.17. Nhấn Yes để xác nhận rằng ta muốn xóa ổ đĩa hoặc phân vùng đĩa đã chọn.

Hình 4.17



2. Quản lý tệp tin và thư mục

Trong phần này, ta đã học cách quản lý các files và các thư mục. Gồm những nội dung sau:

- ✓ Quản lý truy nhập địa phương liên quan đến việc thiết lập quyền NTFS.
- ✓ Quản lý truy nhập mạng bao gồm việc tạo chia sẻ thư mục, thiết lập quyền chia sẻ và truy nhập tài nguyên mạng.
- ✓ Cách thức các tài nguyên được truy nhập khi các quyền NTFS cục bộ và chia sẻ mạnh đã được thiết lập.
- ✓ Luồng truy cập tài nguyên, bao gồm việc tạo thẻ bài truy nhập đối với tượng bằng việc kiểm tra ACL và ACES.

Quyền truy xuất cục bộ xác định quyền truy xuất của người dùng đối với các tài nguyên cục bộ. Ta có thể hạn chế quyền truy xuất cục bộ bằng việc thực hiện các phân quyền trên phân vùng NTFS cho các file hoặc các thư mục. Một trong những tính năng nổi bật của hệ thống kết nối mạng chính là khả năng cho phép các truy nhập từ xa đến các tài nguyên cục bộ. Đối với Win 2000 Server, việc chia sẻ các thư mục là rất dễ dàng. Việc thực hiện cơ chế bảo mật lên các thư mục chia sẻ trong Win 2000 Server được thực hiện tương tự như việc phân quyền NTFS. Ngay khi ta chia sẻ một thư mục, những người dùng có quyền truy nhập thích hợp có thể truy xuất vào thư mục đó theo nhiều cách khác nhau. Để có thể quản lý một cách hiệu quả các truy xuất cục bộ, truy xuất mạng hoặc các sự cố, ta phải hiểu một cách thấu đáo tiến trình truy nhập tài nguyên. Trong Win 2000 Server quản lý việc truy nhập tài nguyên thông qua một số cơ chế như: thẻ bài truy nhập, danh sách điều khiển truy nhập hoặc các điểm quản lý

truy nhập.

Trong chương này, ta sẽ học cách quản lý một cách hiệu quả nhất các truy xuất cục bộ cũng như các truy xuất mạng đến các tài nguyên bao gồm việc thiết lập quyền NTFS và các quyền truy xuất trên mạng.

2.1. Quản lý truy nhập cục bộ (địa phương)

Có hai kiểu hệ thống file được sử dụng phổ biến trên các phân vùng cục bộ là FAT (bao gồm FAT32 và FAT16) và NTFS. Phân vùng theo hệ thống FAT không hỗ trợ cơ chế bảo mật cục bộ, nhưng NTFS lại có. Điều này có nghĩa là nếu phân vùng mà người sử dụng đang truy nhập đến là FAT thì ta không thể áp đặt các quy tắc bảo mật cần thiết lên hệ thống file đó khi người dùng đăng nhập vào hệ thống. Tuy nhiên nếu phân vùng được thiết lập theo hệ thống NTFS thì ta có thể xác định quyền truy xuất mà mỗi người dùng có đối với các thư mục xác định dựa trên tên của người dùng và nhóm mà người dùng đó thuộc về.

Chương này cung cấp các thông tin cần thiết về việc quản lý các truy xuất cục bộ và truy xuất mạng cho các file và các thư mục, bao gồm việc điều khiển, quản trị, thiết đặt và khắc phục sự cố cho các truy xuất lên các thư mục, các file.

Sự phân quyền NTFS sẽ điều khiển các truy xuất tới các file và thư mục trên phân vùng NTFS. Ta thiết lập quyền truy xuất bằng việc cấp hay thu hồi các quyền NTFS cho các người dùng hay các nhóm người dùng. Thông thường các quyền loại NTFS có tính chất tích luỹ, và dựa trên quyền của các nhóm mà người dùng thuộc về. Tuy nhiên nếu người dùng bị thu hồi quyền truy xuất thông qua cơ chế người dùng hoặc thành viên của nhóm thì các quyền này sẽ làm ảnh hưởng đến các truy xuất được phép khác.

a) Với quyền điều khiển toàn bộ các truy xuất, ta có các quyền cụ thể như sau:

1. Truy xuất các thư mục và tất cả các file chương trình trong thư mục đó.
2. Liệt kê nội dung của thư mục và đọc dữ liệu trong các file của thư mục đó.
3. Xem và thay đổi thuộc tính của thư mục và của các file trong thư mục.
4. Tạo file mới và nội dung của file đó.
5. Tạo thư mục mới và thêm dữ liệu vào cuối file.
6. Xoá file và thư mục.
7. Thay đổi các quyền truy xuất cho các thư mục và file

b) Quyền Modify được phép thực hiện các thao tác sau:

1. Truy xuất thư mục và thực hiện các file chương trình trong thư mục.
2. Liệt kê nội dung của thư mục và đọc nội dung của các file trong thư mục đó.

- 3 . Xem các thuộc tính của thư mục và của file.
4. Thay đổi thuộc tính của file và thư mục.
5. Tạo một file mới và ghi dữ liệu lên file đó.
6. Tạo một thư mục mới và thêm dữ liệu vào cuối nội dung file.
7. Xoá các file.

c) Quyền "Read and Execute" được phép thực hiện các thao tác sau:

1. Truy xuất các thư mục và thực hiện các file chương trình trong thư mục đó.
2. Liệt kê tất cả nội dung của thư mục và đọc nội dung của các file trong thư mục đó.
- 3 . Xem thuộc tính của thư mục và của các file trong thư mục đó

d) Quyền "List Folder Contents" được phép thực hiện các thao tác sau:

1. Truy xuất các thư mục và thi hành các file chương trình trong thư mục đó.
2. Liệt kê nội dung của một thư mục và đọc nội dung của các file trong thư mục đó.
- 3 . Xem thuộc tính của thư mục và của các file trong thư mục đó.

e) quyền "Read" được phép thực hiện các thao tác như sau:

1. Liệt kê nội dung của thư mục và đọc nội dung của tất cả các file trong thư mục đó.
2. Xem thuộc tính của thư mục cũng như thuộc tính của các file trong thư mục đó.

f) Quyền "Write" được phép thực hiện các thao tác như sau:

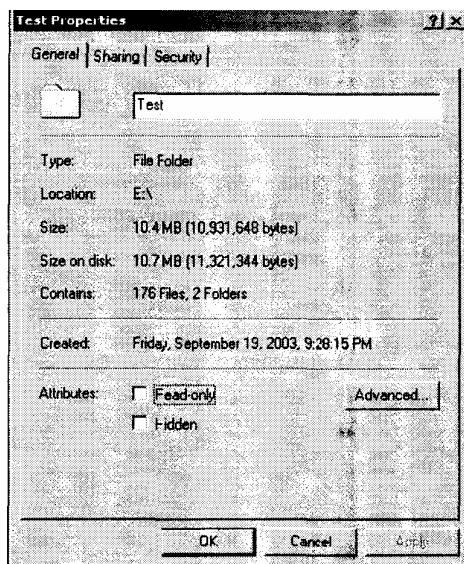
1. Thay đổi thuộc tính của thư mục cũng như thuộc tính của các file trong thư mục đó.
2. Tạo một file mới và ghi dữ liệu lên file.
3. Tạo một thư mục mới và thêm dữ liệu vào cuối file.

Bất cứ một người nào có quyền "Full Control" đều có thể thiết lập cơ chế bảo mật cho một thư mục nào đó. Mặc định nhóm "Everyone" có quyền "Full Control" trên toàn bộ phân vùng NTFS. Tuy nhiên để có thể truy xuất được vào thư mục người sử dụng phải có quyền truy xuất vật lý đối với máy đó cũng như một tài khoản hợp lệ. Mặc nhiên, người dùng mặc định không thể truy xuất tới các thư mục ở trên mạng trừ khi thư mục đó đã được chia sẻ. Các vấn đề liên quan đến thư mục chia sẻ được bàn đến trong phần "Quản lý truy xuất mạng" ở chương này.

Triển khai các quyền NTFS

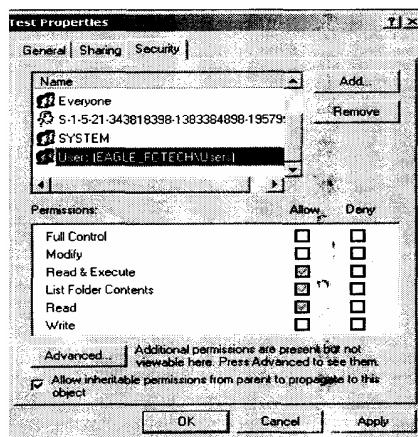
Chúng ta tiến hành áp dụng các quyền NTFS thông qua Windows Explorer. Nhấn chuột phải vào thư mục hoặc file mà ta muốn điều khiển các truy xuất tới chúng, sau đó chọn "Properties" từ menu thả xuống. Khi đó xuất hiện hộp hội thoại "file Properties". Hình 4.18 thể hiện một hộp thoại "folder Properties".

Hình 4.18



Các tab trong hộp thoại "File and fulder Properties" tùy thuộc vào các tuỳ chọn mà ta đã thiết lập cho máy tính của ta. Đối với các file và folder trên phân vùng NTFS, hộp hội thoại sẽ xuất hiện với tab "Security". Qua đó ta có thể thiết lập các quyền NTFS. (Tab "Security" không tồn tại trong hộp thoại "Properties" của phân vùng FAT vì phân vùng FAT không hỗ trợ cơ chế bảo mật cục bộ) Tab Security liệt kê các người dùng và nhóm có quyền trên thư mục (file) này. Khi ta nhấp chuột vào một người dùng hay nhóm người dùng trong nửa trên của hộp hội thoại, ta sẽ thấy các quyền đã được cấp phát hay thu hồi của người dùng hay nhóm người dùng đó trong nửa dưới của hộp hội thoại giống như hình 4.19.

Hình 4.19



Permissions:	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Modify	<input type="checkbox"/>	<input type="checkbox"/>
Read & Execute	<input type="checkbox"/>	<input checked="" type="checkbox"/>
List Folder Contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>

Advanced... Additional permissions are present but not viewable here. Press Advanced to see them.

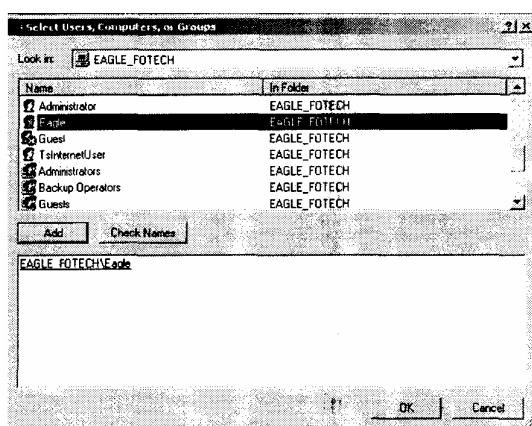
Allow inheritable permissions from parent to propagate to this object

Để tạo ra một quyền mới cho một người dùng hay nhóm người dùng ta cần theo các bước các bước sau đây :

1. Trong Windows Explorer, nhấp chuột phải vào thư mục hay file mà ta muốn kiểm soát truy xuất tới nó. Chọn "Properties" từ menu đầy xuống và chọn tạo "Security" từ hộp thoại này.

2. Nhấp chuột vào nút "Add" để mở hộp thoại "Select Users, Computer or Group" như được trình bày trong hình 4.20. Ta có thể chọn người dùng trong cơ sở dữ liệu cục bộ của máy hay tên miền của ta từ danh sách thả xuống ở định của hộp thoại. Danh sách ở cuối của hộp thoại liệt kê tất cả các nhóm người dùng và người dùng của vùng đã được xác định ở danh sách định.

Hình 4.20



3 . Nhấp chuột vào người dùng, máy tính hay nhóm mà ta muốn phân thêm quyền, nhấn nút "Add"; Thông tin về người dùng, máy tính, nhóm sẽ xuất hiện danh sách bên dưới. Sử dụng tổ hợp phím Chí và nhấp chuột vào các người dùng, các máy tính, các nhóm liên tục hay giữ phím Start để chọn các người dùng, máy tính, nhóm liên tục.

4. Ta chọn tạo “Security” của hộp thoại "Properties", chọn lần lượt các người dùng, máy tính, nhóm trong danh sách bên trên để thiết lập quyền NTFS. Sau khi ta kết thúc ấn nút OK.

Chú ý:

Thông qua nút “Advances” của tao Security”, ta có thể thiết lập thêm các quyền NTFS khác như: Truy xuất thư mục, thi hành file chương trình và đọc các thông tin về quyền truy xuất. Để thu hồi quyền NTFS của một người dùng, máy tính, nhóm hãy chọn người dùng, máy tính, nhóm mà ta muốn thu hồi trong tập "Security" và nhấp nút “Remove”. Chú ý rằng nếu quyền đê đang được kế thừa thì trước hết ta phải xoá bỏ tuỳ chọn "Allow Inheritable Permissions from Parent to Propagate to This Object".

Phải hết sức thận trọng khi quyết định thu hồi các quyền NTFS. Không giống như việc ta xoá các loại đối tượng trong Win 2000 Server, ta sẽ không được hệ thống

cảnh báo về việc xoá bỏ quyền NTFS.

Điều khiển sự kế thừa các quyền:

Thông thường cấu trúc của thư mục được tổ chức theo mức. Điều này có nghĩa là các quyền của một thư mục nào đó cũng được áp dụng cho tất cả các thư mục trong của nó. Trong Win 2000 Server mặc nhiên tất cả các quyền của thư mục cha được áp dụng cho tất cả các thư mục và các file con của thư mục đó. Ta gọi nó là các quyền được kế thừa.

Chú ý: Trên Windows 4NT, mặc định các file trong một thư mục kế thừa tất cả các quyền của thư mục cha nhưng các thư mục con lại không kế thừa các quyền của thư mục cha. Đối với Win 2000 Server thì các thư mục con được phép kế thừa các quyền từ thư mục cha. Ta có thể thiết lập sao cho thư mục con hoặc các file không kế thừa các quyền từ thư mục cha thông qua tập "Security" của hộp thoại Properties bằng cách loại bỏ lựa chọn "Allow inheritable Permissions from parent to Propagate to this Object" ở cuối của hộp thoại. Sau đó ta phải đưa ra lựa chọn hoặc là sao chép các hoặc xoá bỏ quyền từ thư mục cha.

Nếu như hộp "Allow and "Deny" trong danh sách các quyền của ta Security có một mặt nạ kiểm tra có bóng đen, điều này có nghĩa là quyền này được kế thừa từ thư mục cha. Nếu hộp kiểm tra không bị tô đen, nó có nghĩa rằng quyền đã được áp dụng tại một lớp cụ thể nào đó. Điều đó được biết như là một quyền được phân bố một cách chính xác. Việc xem xét các quyền kế thừa là rất cần thiết để xây dựng một hệ tốt hơn. Ngoài ra, nó còn có khả năng khắc phục sự cố liên quan đến quyền.

Xác định các quyền chính thức:

Để xác định quyền chính thức của một người dùng, là các quyền mà người dùng đó thực sự có trên một file hay thư mục, ta thêm tất cả các quyền đã được xác định thông qua tài khoản của người dùng. Sau khi quyết định người dùng nào được phép, ta loại bỏ bất cứ quyền nào đã được huỷ bỏ thông qua tài khoản người dùng.

Với ví dụ sau, giả sử rằng người dùng Nam là một thành viên của nhóm "Accounting and Execs". Các bước thao tác sau đây đã được thực hiện:

Accounting Group Permissions		
Permission	Allow	Deny
Full Control		
Modify	✓	
Read & Execute	✓	
List Folder Contents		
Read		
Write		

Execs Group Permissions		
Permission	Allow	Deny
Full Control		
Modify		
Read & Execute		
List Folder Contents		
Read	✓	
Write		

Để xác định quyền chính thức của Nam, ta kết hợp các quyền đã được thiết đặt cho Nam. Kết quả là Nam có các quyền tích cực như: Modify, Read & Execute và Read

Với một ví dụ khác, giả sử rằng người dùng Bắc là một thành viên của nhóm Sales and Temps. Các thiết lập sau đây đã được thực hiện :

Sales Group Permissions		
Permission	Allow	Deny
Full Control		
Modify		✓
Read & Execute		
List Folder Contents		
Read		
Write	✓	

Temps Group Permissions		
Permission	Allow	Deny
Full Control		
Modify	✓	
Read & Execute	✓	
List Folder Contents	✓	
Read	✓	
Write	✓	

Để xác định quyền chính thức của Bắc, ta bắt đầu bằng việc xác định xem Bắc đã được thiết lập những quyền nào: Modify, Read & Execute, List Folder Contents, Read, and Write. Sau đó ta loại bỏ tất cả những quyền nào của Bắc đã bị thu hồi: Modify và Write. Trong trường hợp này quyền chính thức của Bắc là : Read & Execute, List Folder Content và Read .

Xác định quyền NTFS cho các file được copy hoặc di chuyển:

Khi ta copy hoặc di chuyển các file NTFS thì các quyền đã được thiết lập cho các file đó rất có thể bị thay đổi. Sau đây là các hướng dẫn mà ta có thể sử dụng để đoán nhận được điều gì sẽ xảy ra:

1. Nếu ta di chuyển một file từ thư mục này sang một thư mục khác trên cùng một ổ đĩa thì file đó vẫn có các quyền NTFS như ban đầu.

2. Nếu ta di chuyển một file từ thư mục này sang thư mục khác giữa hai ổ đĩa NTFS, khi đó nó sẽ được xem như là một bản sao và sẽ được thiết lập các quyền của thư mục đích.

3. Nếu ta copy một file từ thư mục này sang thư mục khác (có thể trên cùng một ổ đĩa hoặc có thể không) thì file đó sẽ được thiết lập các quyền như là các quyền của thư mục đích.

4. Nếu ta copy hoặc di chuyển một thư mục hay một file tới một phân vùng FAT thì file của ta sẽ không còn được thiết lập các quyền NTFS nữa .

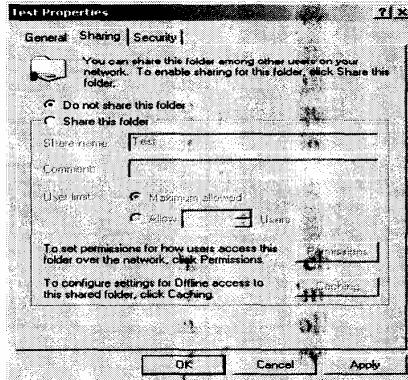
2.2 Quản lý các truy xuất mạng

Việc chia sẻ các tài nguyên là quá trình cho phép các người dùng trên mạng truy xuất các thư mục ở trên máy tính chạy Windows 2000 Server, thư mục này được gọi là thư mục chia sẻ. Một chia sẻ mạng cung cấp một phương pháp rất đơn giản để quản lý dữ liệu được dùng chung bởi nhiều người dùng. Việc chia sẻ còn cho phép nhà quản trị mạng cài đặt các trình ứng dụng chỉ một lần, nếu không sẽ phải cài đặt trên từng máy tính địa phương. Hơn thế nữa nó còn cho phép quản lý trình ứng dụng từ một vị trí trong mạng .

Tạo thư mục chia sẻ

Để chia sẻ một thư mục trên máy tính thành viên chạy Win 2000 Server, ta phải đăng nhập vào máy với tài khoản là một thành viên của nhóm Administrator hay là nhóm Power User. Để chia sẻ một thư mục trên Windows 2000 Domain Controller, ta phải đăng nhập vào hệ thống như là một thành viên của nhóm Administrators hay nhóm Server Operators. Ta tạo ra và thiết lập việc chia sẻ thông qua tập Sharing của hộp thoại folder Properties, được trình bày trong hình 4.21.

Hình 4.21



Nếu ta chia sẻ một thư mục và sau đó quyết định rằng ta không muốn chia sẻ nó nữa thì ta chỉ việc chọn nút "Do Not Share This Folder" trong tập Sharing của hộp thoại "Folder Properties".

Thiết lập cấu hình quyền chia sẻ (Share permission)

Ta có thể điều khiển việc truy nhập của người dùng tới thư mục chia sẻ bằng cách thiết lập quyền chia sẻ. Các quyền chia sẻ ít phức tạp hơn quyền chia sẻ NTFS và chỉ có thể được áp dụng cho các thư mục (Không giống như quyền NTFS, có thể được áp dụng cho các thư mục và các file). Để thiết lập các quyền chia sẻ, chọn nút Pemllission trong tập "Sharing" của hộp thoại Folder Properties.

Ta có thể thiết lập ba kiểu của quyền chia sẻ:

- ✓ Quyền chia sẻ Full Controll cho phép truy nhập đầy đủ tới thư mục chia sẻ.
- ✓ Quyền chia sẻ Change cho phép người dùng thay đổi dữ liệu trong file hoặc xóa các file.
- ✓ Quyền chia sẻ Read cho phép người dùng xem và chạy các file trong thư mục chia sẻ.

Full Controll là sự cho phép mặc định trên các thư mục chia sẻ cho nhóm người dùng Everyone. Khi quyền "*Full Controll*" được thiết lập, các quyền Change và Read cũng sẽ được thiết lập

Chú ý: Các thư mục chia sẻ không sử dụng quan điểm kế thừa như các thư mục NTFS. Nếu ta chia sẻ một thư mục, chẳng có cách nào để cấm truy nhập tới các tài nguyên mức thấp hơn thông qua các quyền chia sẻ.

Quản lý các chia sẻ với tiện ích Shared Folders

Shared Folders là một trình tiện ích quản lý máy tính dùng để tạo và quản lý các thư mục chia sẻ trên máy tính. Cửa sổ của Shared Folders hiển thị tất cả các chia sẻ đã được tạo ra trên máy tính, các phiên người dùng được mở trên mỗi chia sẻ và các file đang được mở được liệt kê theo người dùng.

Để truy nhập Shared Folders, cách chuột phải lên My Computer trên Desktop và chọn Manage từ menu ngữ cảnh. Trong Computer Management, mở rộng System Tools rồi mở rộng Shared Folders.

Ngoài các chia sẻ mà ta đã thiết lập, ta cũng có thể nhìn thấy các chia sẻ đặc biệt của Windows 2000, các chia sẻ này được tạo ra một cách tự động bởi hệ thống làm thuận tiện cho việc quản trị hệ thống. Một chia sẻ theo sau bởi dấu đê (\$) cho biết rằng chia sẻ đó bị che dấu khi người dùng truy nhập vào các tiện ích khác như là My Network Places và duyệt qua các tài nguyên mạng. Các chia sẻ đặc biệt sau có thể xuất hiện trong Windows 2000 Server, phụ thuộc vào cách định cấu hình cho máy tính:

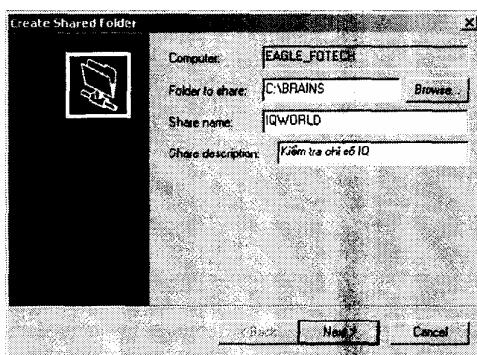
Chia sẻ drive_letter\$ là chia sẻ cho gốc (root) của ổ đĩa. Theo mặc định, thư mục gốc của tất cả các ổ đĩa đều được chia sẻ. Ví dụ, Ổ đĩa C: được chia sẻ như là C\$.

Tạo các chia sẻ mới

Trong tiện ích Shared Folders, ta có thể tạo các chia sẻ mới thông qua các bước sau:

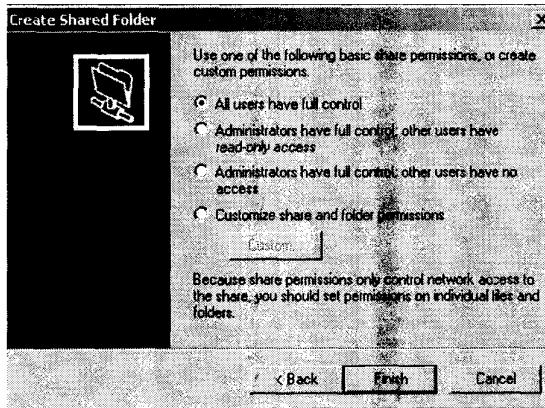
1. Click chuột phải vào thư mục Shares và chọn New File Share từ menu pop-up.
2. Tiện ích Create Shared Folder Wizard được khởi động như hình 4.22. Xác định thư mục sẽ được chia sẻ (ta có thể sử dụng nút Browse để chọn thư mục) và cung cấp một tên chia sẻ và mô tả. Click nút Next.

Hình 4.22



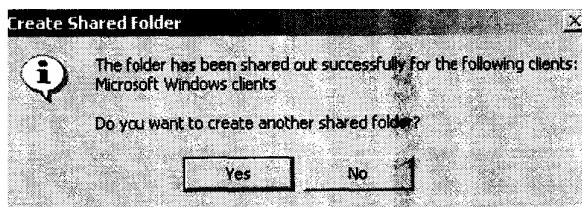
3. Hộp thoại Create Shared Folder sẽ xuất hiện để thiết lập quyền chia sẻ như trong hình 4.23. Ta có thể chọn một trong các quyền đã được chỉ định trên hộp thoại hoặc có thể tùy biến quyền chia sẻ. Sau khi ta xác định xong các quyền chia sẻ, click nút Finish.

Hình 4.23



4. Hộp thoại Create Shared Folder xuất hiện như trong hình 4.24. Hộp thoại này xác nhận rằng thư mục đã được chia sẻ thành công. Cách nút Yes để chia sẻ một thư mục khác hoặc nút No để kết thúc.

Hình 4.24



Ta có thể dừng việc chia sẻ một thư mục bằng cách click chuột phải lên chia sẻ và chọn Stop Sharing từ menu thả xuống. Ta sẽ được cảnh báo để xác nhận rằng ta có muốn dừng chia sẻ thư mục này nữa hay không.

Xem các Phiên chia sẻ (Share Session)

Khi ta chọn mục Sessions trong tiện ích Shared Folders, ta sẽ nhìn thấy tất cả những người dùng hiện thời đang truy nhập vào thư mục chia sẻ trên máy tính. Hình 4.25 chỉ ra một ví dụ về danh sách các phiên trong Shared Folder. **Hình 4.25**

The screenshot shows the Windows Taskbar at the top with icons for Start, Task View, Back, Forward, File Explorer, Task Switcher, and Task View. Below is the 'Computer Management' window. The left pane shows a tree view with 'Computer Management (Local)' expanded, revealing 'System Tools' (Event Viewer, System Information, Performance Logs and Alerts), 'Shared Folders' (Shares, Open Files), 'Device Manager', 'Local Users and Groups', 'Storage' (Disk Management, Disk Defragmenter, Logical Drives, Removable Storage), and 'Services and Applications'. The right pane is titled 'Sessions' and lists two entries:

User	Computer	Type	Open Files	Connect
Administrator	Eagle_Fotech	Windows	3	
Eagle	Eagle_Fotech	Windows	2	

Danh sách các phiên bao gồm các thông tin sau:

- ✓ Tên người dùng đã kết nối đến chia sẻ.

- ✓ Tên máy tính mà người dùng dùng để kết nối từ đó.
- ✓ Hệ điều hành client được sử dụng bởi máy tính kết nối.
- ✓ Số file mà người dùng đã mở.
- ✓ Lượng thời gian người dùng đã kết nối.
- ✓ Lượng thời gian nhàn rỗi cho kết nối.
- ✓ Có hay không người dùng đã kết nối thông qua truy nhập khách (Guest).

Xem các file được mở trong tiện ích Shared Folders

Khi ta chọn mục Open Files trong tiện ích Share Folders, ta sẽ thấy danh sách của tất cả các file hiện thời đang được mở từ các thư mục được chia sẻ. Hình 4.26 đưa ra một ví dụ về danh sách các file đang được chia sẻ trong Shared Folders.

Hình 4.26

Open File	Accessed By	Type	# Locks	Open Mode
C:\OMAT\Wkepln D...	Administrator	Windows	0	Read
D:\Poemo\DTISuytu...	Eagle	Windows	1	Write

Danh sách các file được mở bao gồm các thông tin sau:

- ✓ Các file và đường dẫn đang được mở hiện thời.
- ✓ Tên người dùng đang truy nhập đến file.
- ✓ Hệ điều hành được sử dụng bởi người dùng đang truy nhập đến file.
- ✓ Có hay không khóa file đã được áp dụng (khóa file-file locks được sử dụng để ngăn chặn hai người dùng mở cùng một file và sửa đổi cùng lúc).
- ✓ Cách thức mở file (open mode) đang được sử dụng (như là đọc hay ghi).

Cung cấp truy nhập tới các tài nguyên chia sẻ

Có rất nhiều cách mà người dùng có thể truy nhập tới một tài nguyên chia sẻ. Trong chương này chúng ta chỉ quan tâm đến ba phương thức phổ biến nhất:

- ✓ Thông qua My Network Places.
- ✓ Ánh xạ ổ đĩa mạng trong Windows Explorer.
- ✓ Thông qua tiện ích dòng lệnh NET USE.

Truy nhập một tài nguyên chia sẻ thông qua My Network Places

Điểm thuận lợi của việc ánh xạ một vùng trong ứng thông qua My Network Places là ta không sử dụng các tên ổ đĩa. Điều này sẽ thực sự hữu ích khi tên ổ đĩa của ta vượt qua giới hạn của 26 ký tự. Để truy nhập một tài nguyên chia sẻ thông qua My Network Places, làm theo các bước sau:

1. Nháy kép lên biểu tượng My Network Places trên desktop.
2. Nháy kép lên Add Network Place.
3. Tiện ích Add Network Place khởi động. Gõ đưa dẫn của Network Place. Đây có thể là một đường dẫn UNC tới một thư mục chia sẻ trên mạng, hay một đường dẫn HTTP tới một thư mục Web, hay một đường dẫn FTP tới một sít FTP. Nếu ta không chắc về đường dẫn, ta có thể dùng nút Browse để tìm kiếm đường dẫn. Sau khi xác định đường dẫn, cách nút Next button.
4. Gõ vào tên mà ta muốn dùng trong mạng. Tên này sẽ xuất hiện trong danh sách My Network Places của máy tính.

Ánh xạ một ổ đĩa mạng qua Windows Explorer

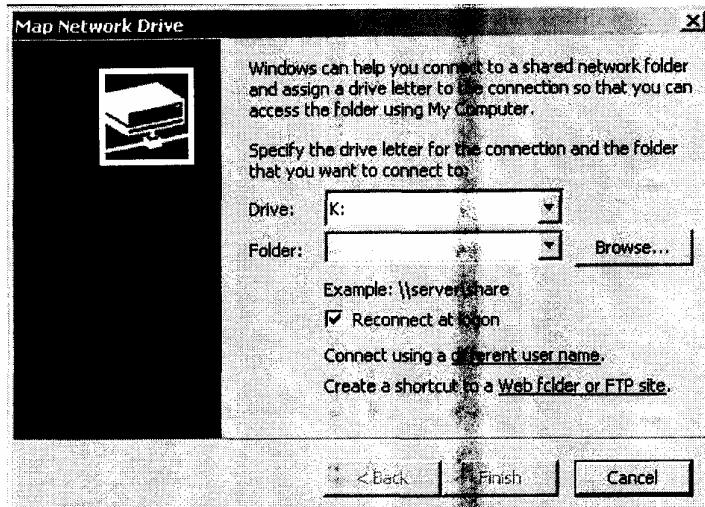
Thông qua Windows Explorer, ta có thể ánh xạ một ổ đĩa mạng thành một kí hiệu (letter) ổ đĩa xuất hiện tới người dùng như là một kết nối địa phương tới máy tính của họ. Mỗi lần ta tạo ra một ổ đĩa được ánh xạ, nó có thể được truy nhập thông qua drive letter bằng cách sử dụng My Computer.

Các bước sau được sử dụng để ánh xạ một ổ đĩa mạng:

1. Chọn Start -> Programs -> Accessories -> Windows Explorer để mở Windows Explorer.
2. Chọn Tools -> Map Network Drive.
3. Hộp thoại Map Network Drive xuất hiện như trong hình 4.27.

Chọn một kí hiệu chữ cái sẽ được ánh xạ vào ổ đĩa mạng

Hình 4.27

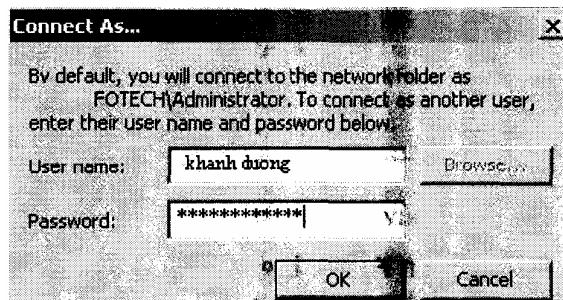


4. Chọn thư mục chia sẻ trên mạng mà ta sẽ ánh xạ vào ô đĩa từ danh sách thả xuống Folder.

5. Nếu ta muốn kết nối này bền (ta muốn ghi lại kết nối này và sử dụng mỗi khi đăng nhập), hãy chắc chắn rằng hộp kiểm Reconnect at Logon được đánh chọn.

6. Nếu ta sẽ kết nối tới chia sẻ sử dụng tên người dùng khác, cách phần gạch chân của dòng "Connect using a different user name". Hộp thoại Connect As xuất hiện như trong hình 4.28. Nhập tên người dùng vào hộp User name và mật khẩu vào hộp Password, rồi click OK.

Hình 4.28



7. Nếu ta muốn tạo một shortcut tới một thư mục Web, cách phần gạch chân của dòng 'Create a shortcut to a Web folder or FTP site' Điều này sẽ khởi động tiện ích Add Network Place.

Sử dụng tiện ích dòng lệnh NET USE

Tiện ích dòng lệnh NET USE cung cấp một cách nhanh chóng và dễ dàng để ánh xạ một ô đĩa mạng. Lệnh có cú pháp như sau:

NET USE x:\\computename\\sharename

Ví dụ, lệnh sau sẽ ánh xạ ô đĩa G thành một chia sẻ có tên là AppData trên máy

tính có tên Appserver:

NET USE G:\AppServer\ UserData

Xem lại Luồng Truy cập Tài nguyên

Việc hiểu rõ về tiến trình xử lý luồng tài nguyên (resource-flow) sẽ giúp ta khắc phục các sự cố về vấn đề truy nhập. Như ta vừa học, một tài khoản người dùng phải có quyền phù hợp để truy nhập tài nguyên. Truy nhập tài nguyên được xác định qua các bước sau:

1. Khi đăng nhập, một thẻ bài truy nhập được tạo ra cho tài khoản đăng nhập.
2. Khi tài nguyên được truy nhập, Window 2000 Server kiểm tra danh sách điều khiển truy nhập (ACL-access control list) xem người dùng có được chấp nhận truy nhập hay không.
3. Nếu người dùng có trong danh sách, ACL kiểm là mục nhập điều khiển truy cập (ACES- access control entries) xem loại truy nhập nào mà người dùng sẽ được cấp. Thẻ bài, ACL, ACE được diễn giải trong các phần sau.

Tạo thẻ bài truy cập (access to ken)

Mỗi lần tài khoản người dùng đăng nhập, một thẻ bài truy cập được tạo ra. Thẻ bài truy cập chứa định danh bảo mật (SID-security identifier) của người dùng hiện thời đăng nhập vào máy tính. Nó cũng chứa các SID cho bất kỳ nhóm nào mà người dùng được thuộc về. Ngay khi thẻ bài truy cập được tạo ra, nó sẽ không được cập nhật do đến lần đăng nhập kế tiếp.

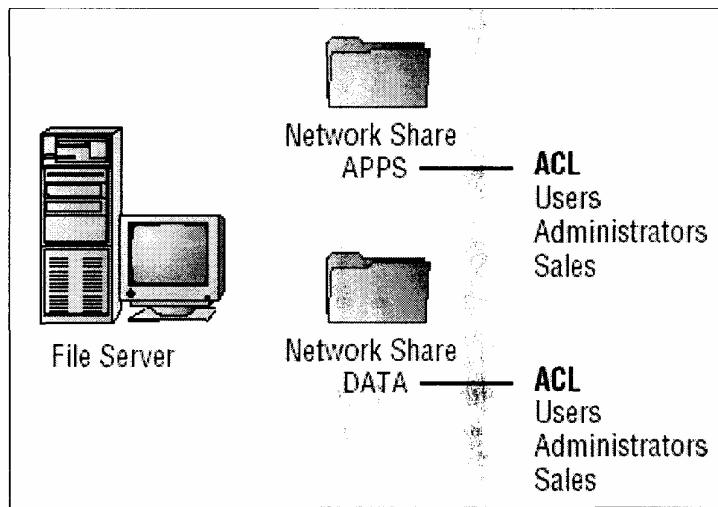
Giả sử rằng người dùng Nam cần truy nhập CSDL, Sales và SALESDB là tên của thư mục chia sẻ chứa đựng CSDL. Kevin đăng nhập vào hệ nhưng không thể truy nhập vào CSDL này. Ta thực hiện công việc tìm kiếm và nhận ra Nam chưa định thêm vào nhóm Sales, điều này là cần thiết cho bất cứ người dùng muốn truy xuất tới SALESDB. Ta thêm người dùng Nam vào nhóm Sales và thông báo cho anh ấy về điều đó. Nam cố truy xuất vào SALESDB, nhưng anh ấy vẫn không thể. Nam thoát khỏi hệ thống và đăng nhập lại và hệ thống, và anh ấy đã có thể truy nhập tới CSDL này. Sở dĩ như thế là vì thẻ bài truy nhập của Nam đã không được cập nhật để tuệ nó ứng với việc anh ấy là thành viên mới của nhóm cho đến khi anh ấy thoát khỏi hệ thống và đăng nhập trở lại hệ thống. Khi anh ấy đăng nhập lại vào hệ thống, một thẻ bài truy nhập mới đã được tạo ra, xác định Nam là thành viên của nhóm Sales. ..

Thẻ bài truy nhập chỉ được cập nhật trong suốt quá trình đăng nhập vào hệ thống. Chúng không được cập nhật tự động. Điều này có nghĩa là nếu ta thêm một người dùng vào nhóm, người dùng này cần thoát khỏi hệ và nhập lại vào hệ để cho thẻ bài truy nhập của họ được cập nhật.

ACL và ACEs

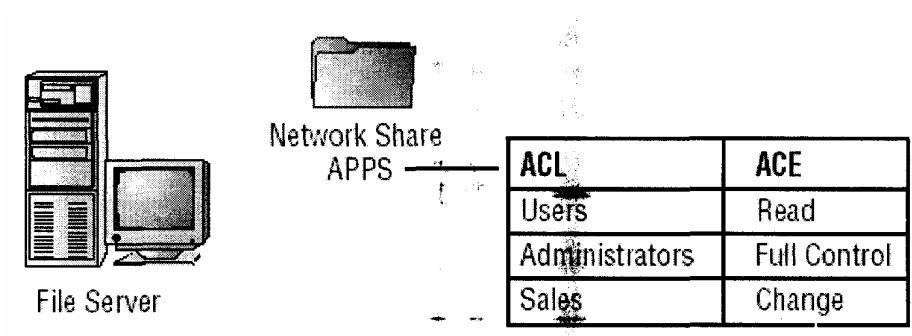
Mỗi đối tượng trong Windows 2000 Server có một ACL. Mỗi đối tượng được xác định như một tập hợp dữ liệu có thể được sử dụng bởi hệ ứng hoặc một tập hợp các hành động có thể được sử dụng để thao tác dữ liệu hệ thống. Đối tượng có thể là thư mục, files, chia sẻ mạng và máy in. ACL là một danh sách tài khoản người dùng và nhóm người dùng được quyền truy nhập tài nguyên. Hình 4.29 đưa ra ACLS được gắn với mọi đối tượng như thế nào.

Hình 4.29



Mỗi ACL có một ACE xác định một người dùng hoặc một nhóm người dùng thực sự có thể làm việc với tài nguyên. Quyền Deny là luôn được liệt kê đầu tiên. Điều này có nghĩa là, nếu người dùng có quyền Deny, họ sẽ không được phép truy nhập tài nguyên, thậm chí ngay cả khi họ Allow. Hình 4.30 minh họa sự tương tác giữa ACL và ACE.

Hình 4.30



Truy nhập tài nguyên cục bộ và tài nguyên mạng

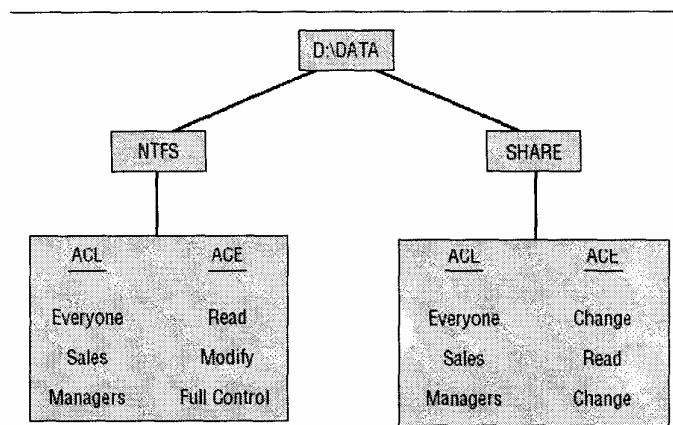
Cơ chế bảo mật mạng và bảo mật địa phương làm việc cùng nhau. Hầu như các quyền truy xuất đều xác định cái gì người dùng có thể làm. Ví dụ nếu thư mục cục bộ là NTFS và quyền mặc định không bị thay đổi, nhóm người dùng Everyone có quyền

Full Control. Nói cách khác, ngư thư mục cục bộ được chia sẻ và quyền là 1 tập hợp sao chỉ duy nhất nhóm người dùng Sales đã cung cấp quyền đọc, khi đó chỉ duy nhất nhóm Sales có thể truy nhập thư mục chia sẻ này.

Ngược lại, nếu quyền truy xuất NTFS địa phương cho phép duy nhất manager được đọc các thư mục cục bộ và những thư mục này được chia sẻ với các quyền mặc sao cho nhóm Everyone có quyền Full Control, chỉ duy nhất nhóm Manager có thể truy xuất tới thư mục với quyền Read.

Ví dụ: Giả sử rằng ta đã cài đặt NTFS và chia sẻ các quyền cho thư mục DATA như hình 4.31 và Jose là một thành viên của nhóm Sales và muốn truy nhập tới thư mục DATA. Nếu anh ấy truy nhập tại thư mục địa phương, anh ấy sẽ bị quản lý chỉ bởi cơ chế bảo mật NTFS, vì vậy anh ấy sẽ có quyền được Modify. Tuy nhiên, nếu Jose truy nhập từ远处 làm việc khác qua chia sẻ mạng, anh ấy cũng sẽ bị quản lý bởi các quyền chia sẻ với nhiều hạn chế.

Hình 4.31



Ví dụ khác: giả sử rằng Chandler là một thành viên của nhóm Everyone. Anh ấy muốn truy nhập thư mục DATA. Nếu anh ấy truy nhập thư mục đó từ máy của mình anh ấy sẽ có quyền Read. Nếu anh ấy truy nhập từ xa qua chia sẻ mạng anh ấy vẫn có quyền Read. Mặc dù quyền chia sẻ cho phép nhóm Everyone có quyền thay đổi thư mục, các quyền với nhiều giới hạn (trong trường hợp này, là quyền đọc NTFS) sẽ được áp dụng.

CHƯƠNG 5: CÀI ĐẶT VÀ THIẾT LẬP CẤU HÌNH CARD MẠNG, GIAO THỨC MẠNG VÀ CÁC DỊCH VỤ MẠNG (4 lý thuyết)

Trước khi ta có thể kết nối các máy tính thành một mạng, ta cần phải cài đặt và thiết lập cấu hình cho các card mạng trên các máy tính. Ta cũng cần phải cài Driver cho các card mạng đó

Kết nối mạng yêu cầu một giao thức mạng cơ sở. Windows 2000 Server hỗ trợ 3 giao thức mạng chính là : TCP/IP, NWlink IPX/SPX/NetBIOS và NetBEUI.

Các dịch vụ mạng sẽ cung cấp các hàm quản lý địa chỉ IP và giải pháp địa chỉ. Các dịch vụ chủ yếu sử dụng để tương tác trên mạng Windows 2000 là giao thức thiết lập địa chỉ IP động (DHCP), hệ thống tên miền (DNS) và dịch vụ quản lý việc ánh xạ giữa tên máy với các địa chỉ IP (WINS).

Trong chương này ta sẽ tìm hiểu các cài đặt và thiết lập cấu hình card mạng, quản lý giao thức mạng và cài đặt cấu hình cho các dịch vụ mạng.

1. Cài đặt cấu hình cho card mạng

Card mạng là phần cứng sử dụng để kết nối máy tính (hoặc các thiết bị) vào mạng. Card mạng chịu trách nhiệm quản lý việc kết nối vật lý vào mạng và quản lý địa chỉ vật lý của các máy tính (thiết bị) được kết nối mạng. Cũng giống như các thiết bị phần cứng khác, card mạng đòi hỏi Driver điều khiển riêng tương thích với Windows 2000. Phần tiếp theo sẽ nói về việc cài đặt cấu hình card mạng cũng như việc gỡ rời trong trường hợp card mạng không làm việc.

1.1.Cài đặt một card mạng

Trước khi cài đặt card mạng, bạn cần phải đọc kỹ hướng dẫn đi kèm theo phần cứng. Nếu card mạng mới, có thể sẽ tự thiết lập cấu hình và có khả năng tự đồng nhất hóa (Plug and Play). Sau khi cài đặt card mạng có thể hoạt động ngay sau khi ta khởi động lại Windows.

Nếu card mạng của ta không có khả năng tự đồng nhất hóa, sau khi ta cài đặt, hệ điều hành sẽ tự động phát hiện phần cứng mới và hướng dẫn ta từng bước cài đặt Driver cho card mạng. Nếu công cụ Add New Hardware Wizard không tự động nhận diện phần cứng, ta có thể vào Add/Remove Hardware trong Control Panel để thiết lập.

1.2 Cấu hình một card mạng

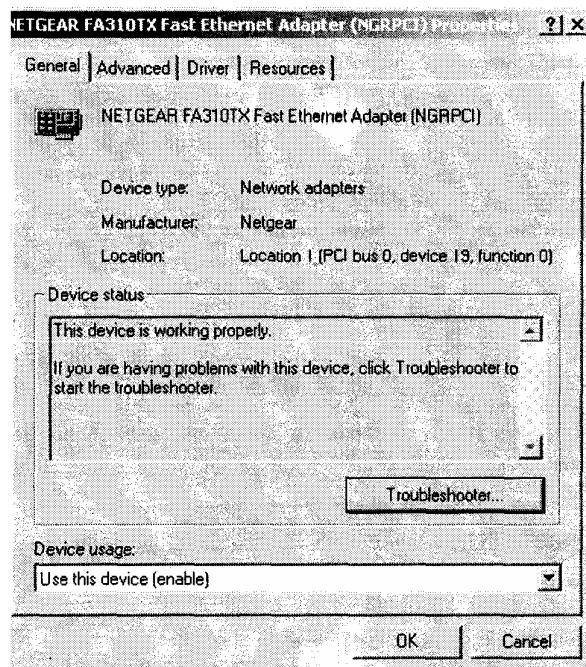
Sau khi ta cài đặt card mạng xong, ta cần phải thiết lập cấu hình thông qua hộp thoại properties của card mạng. Để mở hộp thoại này ta chọn Start-> Seatings -> Control Panel và nhấp đúp vào biểu tượng Dial-up Connections. Sau đó ta nhấp đúp vào Local Area Connection và nhấn nút Configure. Một cách khác ta kích chuột phải vào biểu tượng My Network Places và chọn Properties, sau đó kích chuột phải vào Local Area Connections và chọn Properties, sau đó nhấn Configure.

Trong hộp thoại Properties hiện ra, các thuộc tính được chia thành bốn nhóm (4Tab) General, Advanced, Driver, và Resources. Các nhóm này sẽ được nói rõ hơn ở phần sau.

Nhóm thuộc tính General của Card mạng

Nhóm thuộc tính này bao gồm, tên của Card mạng, kiểu thiết bị, nhà sản xuất và địa chỉ của nhà sản xuất. Khung Device Status mô tả trạng thái làm việc của thiết bị tốt hay lỗi. Nếu thiết bị làm việc không tốt ta có thể nhấn vào nút Troubleshooter để xem một số giúp đỡ trong việc gỡ lỗi các lỗi của thiết bị. Ta cũng có thể bật hoặc tắt thiết bị thông qua hộp danh sách Device Usage.

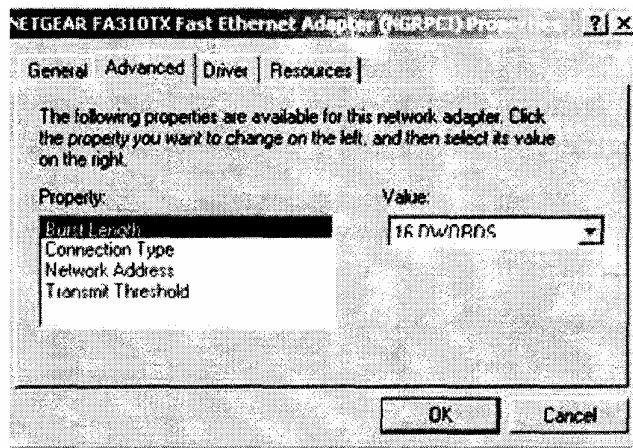
Hình 5.1



Nhóm thuộc tính Advanced

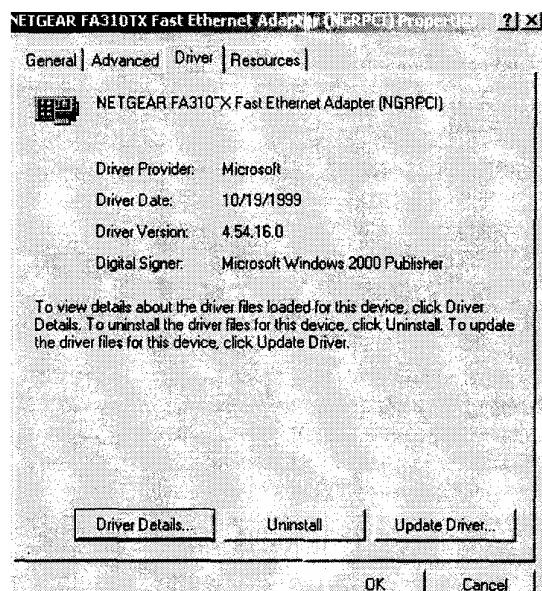
Nội dung của nhóm Advanced chủ yếu phụ thuộc vào card mạng và driver của ta đang sử dụng. Hình 5.2 là một ví dụ của card mạng Fast Ethernet. Để thiết lập cấu hình cho các thuộc tính trong nhóm, ta chọn thuộc tính ở danh sách bên trái, và xác định giá trị cho thuộc tính đó ở hộp danh sách thả xuống nằm bên phải. Ta không nên thay đổi giá trị của các thuộc tính trong nhóm này trừ phi có sự hướng dẫn của nhà sản xuất.

Hình 5.2



Nhóm thuộc tính Driver

Hình 5.3



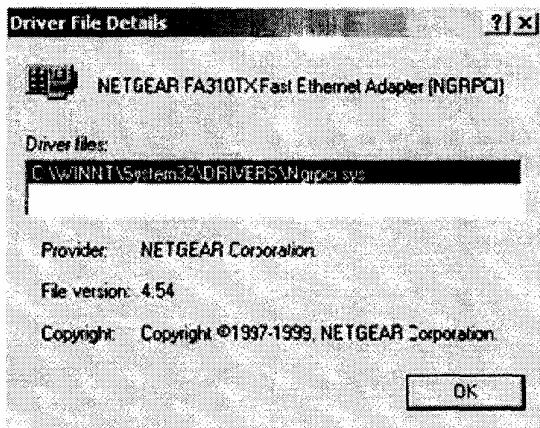
- ✓ Nhà cung cấp Driver cho card mạng (thường là Microsoft hoặc chính nhà sản xuất).
- ✓ Ngày được phát hành chính thức.
- ✓ Phiên bản của Driver.
- ✓ Thông tin về người cung cấp chữ ký điện tử dành cho Driver.

Nhấn vào nút Driver Details để mở hộp thoại Driver File Details (hình 5.4) để xem các thông tin chi tiết về Driver :

- ✓ Đường dẫn tuyệt đối đến tệp Driver.
- ✓ Nhà cung cấp chính thức của Driver.
- ✓ Phiên bản của tệp Driver.

- ✓ Thông tin bản quyền của Driver.

Hình 5.4



Nút Uninstall (hình 5.3) sẽ gỡ bỏ Driver của card mạng khỏi máy tính của ta. Ta nên gỡ bỏ Driver khi muốn thay thế Driver cũ bằng một Driver mới tốt hơn, thích hợp hơn. Thông thường ta thường cập nhật Driver hơn.

Để cập nhật Driver cho thiết bị, ta nhấn vào nút Update Driver, Update Device Driver Wizard sẽ được khởi động hướng dẫn ta từng bước cập nhật Driver mới.

Nếu ta không thể tìm thấy Driver phù hợp, hãy kiểm tra trang web của nhà cung cấp thường ở đó luôn có Driver mới nhất và thường xuyên được cập nhật. Ta cũng có thể tìm kiếm thông tin liên quan đến Driver ta đang sử dụng ở mục những câu hỏi thường gặp (FAQS).

Nhóm thuộc tính Resources

Mỗi phần cứng được cài đặt trên máy tính của ta sẽ sử dụng một phần tài nguyên của máy tính bao gồm: các ngắt (IRQ), bộ nhớ, và các thiết lập vào ra (IO Settings). Nhóm thuộc tính Resources sẽ liệt kê cho ta các thông tin về tài nguyên được sử dụng bởi card mạng. Những thông tin này rất quan trọng cho việc gỡ rời, vì nếu thiết bị khác cũng đang dùng chung tài nguyên với card mạng thì card mạng sẽ không làm việc đúng. Hộp danh sách Conflicting Device List phía dưới sẽ liệt kê các thiết bị đang xung đột tài nguyên với card mạng.

Gỡ rối lỗi của Card mạng

Nếu card mạng của ta không làm việc tốt, vấn đề có thể là do card mạng hoặc Driver điều khiển, hoặc do giao thức mạng sử dụng.

Một số lỗi phổ biến: Card mạng không nằm trong danh sách các phần cứng được hỗ trợ bởi hệ điều hành (HCL). Ta nên liên hệ với nhà cung cấp Card mạng.

Driver card mạng quá cũ	Ta phải chắc chắn rằng Driver card mạng ta sử dụng là mới và đã được cập nhật thông tin về card mạng của ta. Ta có thể tìm kiếm Driver trên trang Web của nhà sản xuất
Card mạng không nhận diện được bởi Windows 2000	Kiểm tra trong Device Manager xem Windows có nhận được card mạng của ta không. Nếu không thấy ta có thể tự cài đặt bằng. Ta cũng cần phải kiểm tra xem có xung đột tài nguyên khi cài đặt hay không.
Phần cứng không làm việc tốt	Kiểm tra lại phần cứng của ta. Nếu vẫn làm việc tốt, hãy kiểm tra cáp nối phần cứng với máy tính. Kiểm tra xem có cáp rỗng để nối với thiết bị không, hoặc có xung đột đường truyền trên cáp giữa card mạng và thiết bị khác không.
Giao thức mạng thiết lập sai	Kiểm tra lại giao thức mạng đã được thiết lập. Thông tin về giao thức mạng sẽ được mô tả chi tiết trong phần sau.

2. Cài đặt và thiết lập cấu hình cho giao thức mạng

Giao thức mạng là chức năng ở tầng mạng và tần chuyển vận của mô hình mạng 7 tầng OSI. Chúng có trách nhiệm truyền tải thông tin trên mạng. Ta có thể kết hợp các giao thức mạng trên Windows 2000 Server.

Windows 2000 Server hỗ trợ các giao thức sau :

- ✓ TCP/IP, là giao thức phổ biến mặc định được cài đặt trên Windows 2000 Server.
- ✓ NWlink IPX/SPX/NetBIOS sử dụng để kết nối máy tính trong mạng Novell Netware.
- ✓ NetBEUI được sử dụng hỗ trợ các máy Macintosh với đầy đủ chức năng và hỗ trợ định tuyến.
- ✓ Data Link Control (DCL) là giao thức chính dùng kết nối với máy in và môi các kết nối môi trường của IBM.

Phần tiếp theo sẽ đặc tả các cài đặt và thiết lập cấu hình cho giao thức TCP/IP, NWlink IPX/SPX/NetBIOS, và NetBEUI là những giao thức chính được sử dụng bởi Windows 2000 Server. Ta cũng sẽ được học cách quản lý các kết nối mạng.

2.1. Sử dụng TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) là một trong những giao thức mạng phổ biến hiện nay. TCP/IP được phát triển lần đầu tiên vào những năm 70 dành cho Bộ Quốc Phòng Mỹ như một phương pháp để kết nối các mạng không đồng nhất. Kể từ đó, TCP/IP trở thành một chuẩn công nghiệp.

Khi cài mới Windows 2000 Server, TCP/IP mặc định được cài đặt. TCP/IP có những lợi điểm:

- ✓ Là một giao thức mạng phổ biến, và được hỗ trợ bởi hầu hết các hệ điều hành mạng. Do cũng là giao thức bắt buộc cho việc kết nối Internet.
- ✓ TCP/IP cũng có thể dùng cho các mạng nhỏ, lớn tùy ý. Trong các mạng lớn TCP/IP hỗ trợ dịch vụ định tuyến.
- ✓ TCP/IP được thiết kế để kiểm soát các lỗ và có khả năng định tuyến lại nếu như kết nối mạng bị ngắt (giả sử rằng có một đường dẫn khác tồn tại).
- ✓ Các giao thức đi kèm DHCP và DNS cung cấp các chức năng tiên tiến.

Thiết lập cấu hình TCP/IP

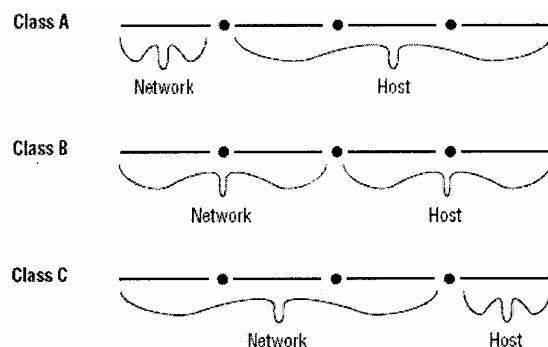
TCP/IP yêu cầu một địa chỉ IP và mặt nạ cho địa chỉ mạng (Subnet mask). Ta cũng có thể thiết lập rất nhiều các tham số khác liên quan đến DNS và WINS. Tuỳ thuộc vào việc cài đặt mạng của ta mà có thể thiết lập tự động hay bằng tay cho TCP/IP.

Địa chỉ IP

Địa chỉ IP là số định danh duy nhất của máy tính của ta trên mạng. Địa chỉ IP bao gồm 4 phần (địa chỉ 32-bit) được phân tách bởi dấu chấm. Một số phần được sử dụng để xác định địa chỉ mạng, phần còn lại để xác định địa chỉ máy của ta.

Nếu ta sử dụng Internet, ta phải đăng ký địa chỉ IP của ta tới một trang Web đăng ký nhất định. Có 3 lớp địa chỉ IP chính. Phụ thuộc vào lớp mạng ta sử dụng mà kích thước địa chỉ mạng và địa chỉ máy tính sẽ khác nhau. (Hình 5.6).

Hình 5.6



Ta có thể biết thêm thông tin về việc đăng ký địa chỉ IP trên trang

Bảng 5.1 Mô tả mô tả địa chỉ mạng, số mạng thuộc lớp và số máy trên mỗi mạng thuộc lớp:

Lớp mạng	Miền địa chỉ mạng	Số mạng thuộc lớp	Số máy trên mỗi mạng thuộc lớp
A	1-126	126	16.777.214
B	128-191	16.384	65.534
C	192-223	2,097,152	254

Mặt nạ (Subnet Mask)

Mặt nạ được dùng để đặc tả phần nào của địa chỉ IP là địa chỉ mạng, phần nào là địa chỉ máy tính. Mặc định, các mặt nạ tương ứng cho các lớp mạng như sau:

A 255.0.0.0

B 255.255.0.0

C 255.255.255.0

Sử dụng 255, nghĩa là ta đang dùng 8 bit (hoặc các bộ 8 bit) để xác định địa chỉ mạng. Ví dụ với một máy tính lớp B có địa chỉ IP: 191.200.2.1 thì mặt nạ là 255.255.0.0 và địa chỉ mạng là 192.200, còn 2.1 là địa chỉ máy.

Default Gateway

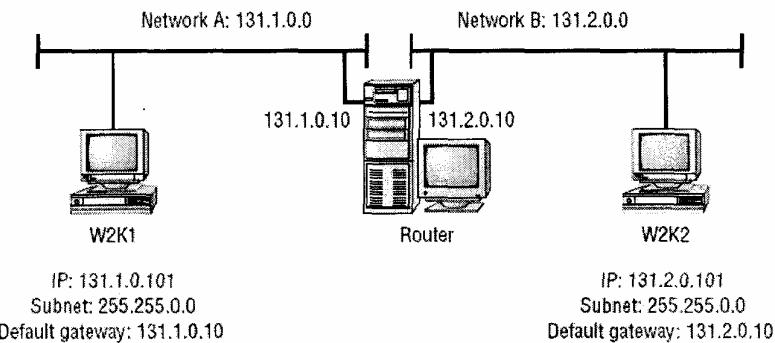
Ta thiết lập cấu hình cổng kết nối nếu mạng sử dụng các bộ định tuyến. Bộ định tuyến là thiết bị kết nối 2 hay nhiều mạng, hoạt động ở tầng mạng.

Ta cũng có thể thiết lập cấu hình để Windows 2000 Server hoạt động như một bộ định tuyến bằng cách cài đặt 2 hay nhiều card mạng trên máy tính và kết nối mỗi card tới một mạng khác nhau và thiết lập cấu hình card mạng cho mỗi đoạn mạng mà nó kết nối tới. Ta cũng có thể sử dụng các bộ định tuyến của các nhà sản xuất thứ 3 (third-party), thường được cung cấp nhiều chức năng hơn là Windows 2000 Server khi được thiết lập như một bộ định tuyến.

Ví dụ, giả sử mạng của ta được thiết lập như hình 5.7. Mạng A sử dụng địa chỉ 131.1.0.0. Mạng B sử dụng địa chỉ 131.2.0.0. Trong trường hợp này, mỗi card mạng của bộ định tuyến sẽ được thiết lập với một địa chỉ mạng của đoạn mạng nó được định địa chỉ tới. Ta thiết lập cấu hình các máy tính trong từng đoạn mạng với địa chỉ IP của card mạng trên bộ định tuyến tương ứng. Ví dụ, trong hình 5.7, máy tính W2KI thuộc mạng A, cổng kết nối mặc định cho máy tính này là 131.1.0.10.

Máy tính W2K2 thuộc mạng B, cổng kết nối mặc định là 131.2.0.10.

Hình 5.7 Cấu hình Default Gateway



Máy chủ DNS

Các máy chủ DNS được sử dụng để quản lý việc ánh xạ các tên máy tính với các địa chỉ IP. Giúp việc truy cập tới các máy tính dễ dàng hơn. Địa chỉ IP của Nhà Trắng là gì? Đó là 198.137.240.91. Vậy tên máy của Nhà Trắng là gì? Đó là www.whitehouse.gov. Ta có thể dễ dàng hiểu là có rất nhiều người không cần quan tâm đến địa chỉ IP chính xác mà chỉ cần biết tên Web sắc hay tên máy. Khi ta truy cập Internet và gõ www.whitehouse.gov, các máy chủ DNS sẽ tự động ánh xạ tên máy tới địa chỉ IP chính xác. Nếu ta không có một máy chủ DNS nào để hỗ trợ truy cập Internet, ta có thể tự thiết lập một tệp ánh xạ các tên máy trên máy của ta. Tệp này chứa các thông tin ánh xạ tên máy với các địa chỉ IP. Máy chủ DNS sẽ được nói kỹ hơn trong phần "Sử dụng DNS".

Máy chủ WINS

Máy chủ WINS sử dụng để quản lý hệ thống tên máy NetBIOS với các địa chỉ IP. Windows 2000 Server sử dụng các tên NetBIOS để xác định các máy tính trong mạng của ta. Dịch vụ này chủ yếu để nhằm tương thích với các phiên bản Windows NT 4 chủ yếu sử dụng các lược đồ định địa chỉ. Khi ta cố gắng truy cập tới một máy tính sử dụng tên NetBIOS, hệ thống cần phải biết là sẽ ánh xạ tên máy tới địa chỉ IP nào. Giải pháp địa chỉ này có thể được tiến hành bởi nhiều phương thức :

- ✓ Thông qua truyền tải rộng (broadcast) trên cùng một đoạn mạng
- ✓ Thông qua máy chủ WINS.
- ✓ Thông qua tệp LMHOSTS, lưu giữ các ánh xạ tĩnh giữa các địa chỉ IP tới các tên máy NetBIOS.

Phần "Sử dụng WINS" sẽ nói kỹ hơn về Máy chủ WINS.

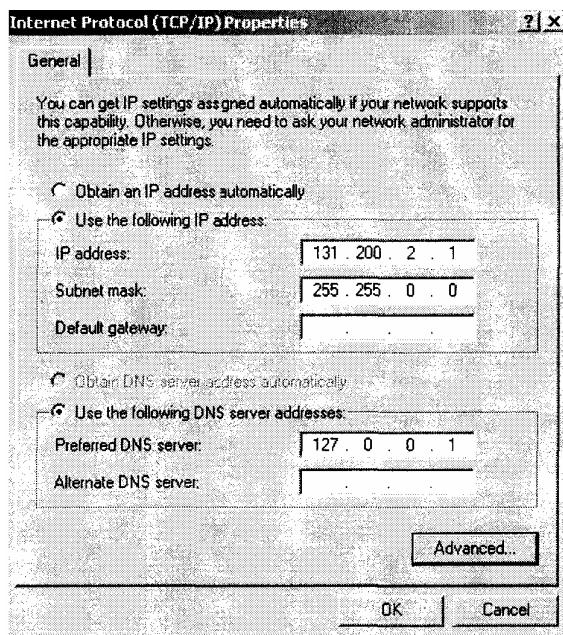
Thiết lập địa chỉ IP theo hướng dẫn

Ta có thể tự thiết lập IP nếu ta biết địa chỉ IP của ta và mặt nạ mạng. Nếu ta sử dụng các thành phần tùy biến như cổng nối kết và máy chủ DNS, ta cần phải biết chính xác địa chỉ IP của máy cung cấp các dịch vụ đó.

Để thiết lập IP, thực hiện theo các bước sau :

1. Từ Desktop, kích chuột phải vào My Network Places và chọn Properties.
2. Kích chuột phải vào Local Area Connection và chọn Properties.
3. Trong hộp thoại Local Area Connection Properties, chọn Internet Protocol (TCP/IP) và nhấn Properties.
4. Hộp thoại Internet Protocol (TCP/IP) Properties hiện ra (hình 5.8), chọn Using following IP Address.
5. Trong các hộp soạn thảo tương ứng, ta nhập vào địa chỉ IP, mặt nạ, và cổng kết nối mặc định.
6. Tuỳ chọn, ta có thể điền thêm một địa chỉ cổng kết nối khác vào ô soạn thảo tương ứng (Alternate DNS Server).
7. Nhấn OK để ghi lại các thay đổi và đóng hộp thoại

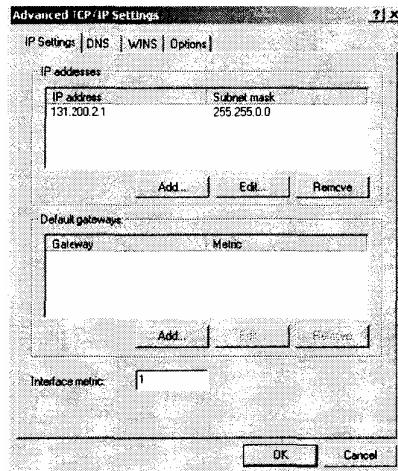
Hình 5.8



Thiết lập mở rộng (Advanced Configuration)

Chọn nút Advanced trong hộp thoại Internet Protocol (TCP/IP) Properties để mở hộp thoại Advanced TCP/IP Settings (Hình 5.9). Trong hộp thoại này ta có thể thiết lập mở rộng cho DNS và WINS.

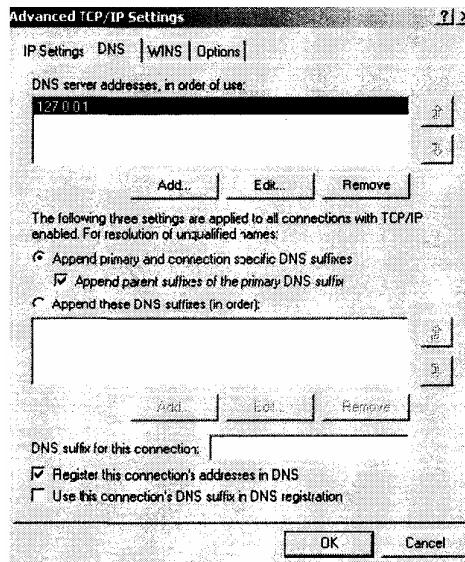
Hình 5.9 Hộp thoại Advanced TCP/IP Setting



Các thiết lập DNS mở rộng

Ta có thể thiết lập cấu hình thêm cho máy chủ DNS về giải pháp tên và nhiều mở rộng khác. (Hình 5.10). Các mở rộng cho phần này được đặc tả trong bảng 5.2.

Hình 5.10 Tạo DNS của Hộp thoại Advanced TCP/IP Setting



Bảng 5.2

Tùy chọn

DNS Servers Addresses, in Order of Use

Append Primary and Connection Specific
DNS Sufflxes

Đặc tả

Đặc tả các địa chỉ máy chủ DNS sử dụng để ánh xạ tên với địa chỉ IP. Sử dụng nút nhấn mũi tên bên cạnh để thay đổi thứ tự của các máy chủ DNS.

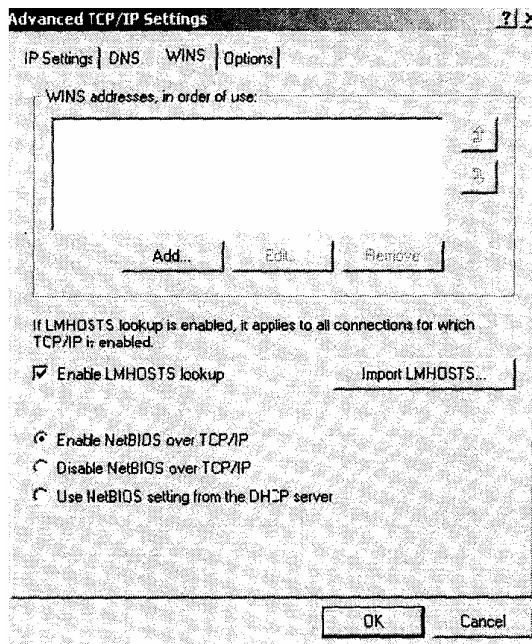
Đặc tả các phần không công bố được hỗ trợ bởi các máy chủ DNS. Chẳng hạn ta có hậu tố Testcorp.com, khi ta gõ nữa thì

	máy chủ DNS sẽ coi như là làm.Testcorp.com.
Append Parent Suffixes in the Primary DNS Suffix	Xác định giải pháp tên miền cho hậu tố cha của các hậu tố DNS (cấp 2 của tên miền). Chẳng hạn ta có Sanjose.Testcorp.com, ta gõ lala, thì DNS sẽ tìm kiếm lala.Sanjose.Testcorp.com, nếu không thấy sẽ tìm lại.Testcorp.com
Append These DNS Suffixes (in order)	Sử dụng các hậu tố để tìm kiếm theo thứ tự tên miền. Giả sử ta có Testcorp.com và Mycorp.com. Ta gõ lala, thì DNS sẽ tìm tên miền lala.Testcorp.com, nếu không thấy sẽ tìm tiếp lala.Mycorp.com
DNS Suffix for This Connection	Xác định hậu tố DNS cho các kết nối. Nếu ta sử dụng dịch vụ DHCP và ta có hậu tố DNS, thì khi kết nối DNS sẽ tự động ghi đè (nếu có trùng lặp) lên các giá trị được thiết lập bởi DHCP.
Register This Connection's address in DNS	Tự động đăng ký tên máy tính với máy chủ DNS khi có thay đổi tên máy (Network Identification trong hộp thoại System Properties).
Use This Connection's DNS Suffix in DNS Registration	Sử dụng tên miền kết hợp giữa tên máy và hậu tố DNS khi đăng ký tự động tên máy với máy chủ DNS

Thiết lập WINS mở rộng

Ta có thể thiết lập các tùy chọn mở rộng dành cho WINS thông qua nhóm WINS trong hộp thoại Advanced TCP/IP Settings (Hình 5.11).

Hình 5.11 Tab WINS của hộp thoại Advanced TCP/IP Setting



Cấu hình IP động

Cấu hình IP động mặc định rằng trong mạng của ta, đã có một máy chủ DHCP. Các máy chủ DHCP đã được cấu hình để cung cấp một cách tự động đầy đủ thông tin về cấu hình IP của các máy khách. Các máy chủ DHCP sẽ được trình bày rõ hơn trong phần "Sử dụng DHCP".

Khi TCP/IP được cài đặt trên một máy tính chạy Windows 2000 server, mặc định rằng máy tính đó sẽ được cấu hình cho IP động. Nếu máy của ta được cấu hình để cấu hình IP bằng tay và ta muốn sử dụng cấu hình IP động, hãy làm theo các bước sau:

1. Trên màn hình Desktop, nhấp chuột phải vào My Network Places và chọn Properties.
2. Nhấp chuột phải vào Local Area Network và chọn Properties.
3. Trong hộp thoại Properties, đánh dấu Internet Protocol (TCP/IP) và chọn Properties.
4. Hộp thoại Properties của Internet Protocol (TCP/IP) sẽ xuất hiện như trong hình 9.8. Chọn nút radio *Obtain an IP Address Automatically*, sau đó nhấn OK.

Kiểm tra cấu hình IP

Sau khi ta đã cấu hình IP, ta có thể kiểm tra cấu hình IP bàn cách sử dụng các lệnh IPCONFIG và PING.

- ✓ **Lệnh IPCONFIG:** Lệnh này sẽ hiển thị cấu hình IP.
- ✓ **Lệnh PING:** Lệnh PING được sử dụng để gửi một yêu cầu ICMP và hồi đáp để xác định xem một máy tính có tồn tại không. Lệnh này có cú pháp như sau:

PING địa chỉ IP Ví dụ, nếu địa chỉ IP là 131.200.2.30, gõ lệnh sau:

PING 131.200.2.30

PING thường được dùng để kiểm tra sự nối kết giữa 2 máy. Ví dụ, nếu ta gặp vấn đề khi kết nối với 1 máy ở trong một mạng khác, ta nên sử dụng PING để xác định xem có tồn tại nội đường kết nối hợp lệ không bằng cách gõ lệnh PING với các địa chỉ sau:

- Địa chỉ quay vòng 127.0.0.1
- Địa chỉ máy cục bộ.
- Địa chỉ của router cục bộ.
- Địa chỉ của máy tính ở xa.

Nếu lệnh PING gặp trục trặc ở 1 trong các câu lệnh trên, hãy tìm hiểu trong Troubleshooting để sửa.

2.2. Sử dụng NWlink IPX/SPX/NetBIOS

NWLink IPX/SPX/NetBIOS Compatible Transport là sự thể hiện của tập các giao thức Novell Internetwork Packet Exchange/sequence Package Exchange (IPX/SPX) của Microsoft. Thể hiện của tập các giao thức IPX/SPX trong Windows 2000 còn thêm cả sự hỗ trợ cho NetBIOS.

Chức năng chính của NWlink là hoạt động như một giao thức vận tải để định tuyến các nối trong liên mạng. Bản thân giao thức Nwlink không cho phép ta truy nhập vào Netware File và các dịch vụ máy in. Tuy nhiên nó cung cấp các phương thức để truyền dữ liệu trong mạng. Nếu ta muốn truy nhập Netware File và các dịch vụ máy in thì ta cần phải cài đặt NWlink and Client Services cho Netware (CSNW) trên máy Windows 2000 khách hoặc Gateway Services or Netware (GSNW) trên máy cài Windows 2000 server. CSNW và GSNW là các gói phần mềm làm việc trên các tầng ở trên cao của mô hình OSI, chúng cho phép truy nhập vào NetWare File và Print Services.

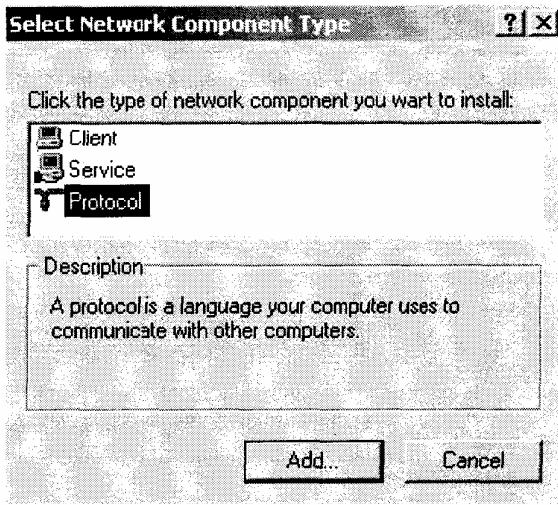
Một ưu điểm của việc sử dụng NWLink là nó dễ dàng cài đặt và cấu hình. Các phần sau sẽ mô tả việc cài đặt và cấu hình giao thức này.

Cài đặt NWlink IPX/SPX/NetBIOS

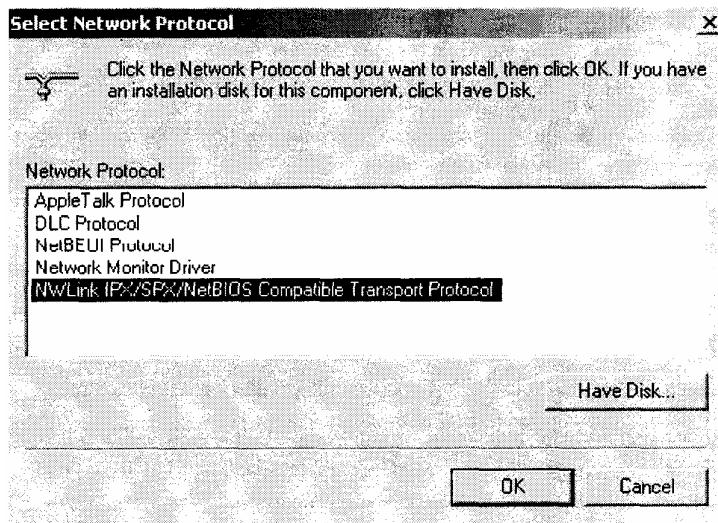
Để cài đặt NWlink, làm như sau:

1. Ở Desktop, nhấp chuột phải vào My Network Places và chọn Properties.
2. Nhấp chuột phải vào Local Area Connection và chọn Properties.
3. Trong hộp thoại Properties của Local Area Connection, nhấn nút Install.
4. Khi hộp thoại Select Network Component Type xuất hiện như hình 5.12, chọn Protocol và nhấn nút Add.

Hình 5.12 Hộp thoại Select Network Component Type



5. Hộp thoại Select Network Protocol xuất hiện như hình 5.13. Chọn NWlink IPX/SPX/NetBIOS Compatible Transport Protocol trong danh sách, sau đó nhấn nút OK. Hình 5.13 Hộp thoại Select Network Protocol



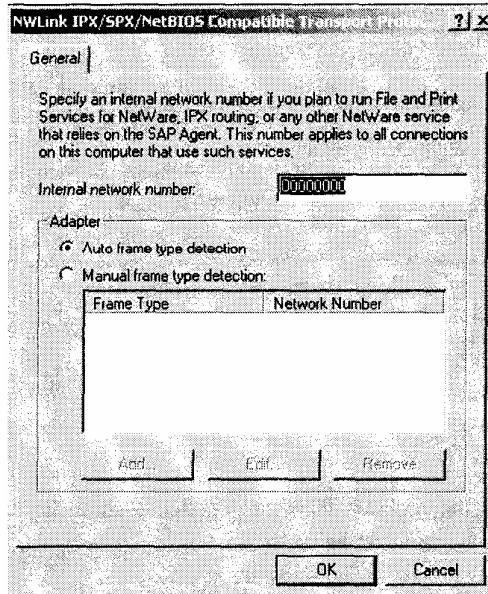
Cấu hình NWlink IPX/SPX

Các lựa chọn ta cần để cấu hình cho NWlink là *Internal network number* và *frame type*. Nếu không có gì đặc biệt, để nguyên giá trị mặc định. Internal network number thường dùng để xác định các máy chủ tệp Netware. Nó cũng được sử dụng nếu ta chạy các dịch vụ tệp và máy in trong Netware hoặc đang sử dụng định tuyến IPX. Frame type xác định dữ liệu được gói như thế nào để truyền trong mạng. Nếu các máy sử dụng NWlink dùng các frame type khác nhau, chúng không thể kết nối tới các máy kia được. Frame type được mặc định là Auto Detect, tức là chế độ luôn cố gắng chọn một cách tự động 1 frame type thích hợp cho mạng của ta. Để cấu hình NWlink IPX/SPX, làm như sau:

1. Ở Desktop, nhấp chuột phải vào My Network Places và chọn Properties.

2. Nhấp chuột phải vào Local Area Connection và chọn Properties.
3. Trong hộp thoại Properties của LocalArea Connection, chọn Nwlink IPX/SPX/NetBIOS Compatible Transport Protocol và nhấn vào nút Properties.
4. Hộp thoại Properties của NWlink IPX/SPX/NetBIOS Compatible Transport Protocol xuất hiện như trong 5.14. Trong hộp thoại này, ta có thẻ cấu hình internal network number và frame type.

Hình 5.14 Hộp thoại Properties của NWlink IPX/SPX/NetBIOS Compatible Transport Protocol



2.3 Sử dụng NetBEUI

NetBEUI (NetBIOS Extended User Interface) được phát triển vào giữa những năm 1980 để kết nối các nhóm làm việc chạy trên các hệ điều hành OS/2 và LAN Manager.

Các ưu điểm của giao thức NetBEUI:

- ✓ Dễ dàng cài đặt.
- ✓ Không cần phải cấu hình.
- ✓ NetBEUI có các khả năng tự thích ứng.
- ✓ NetBEUI "nhẹ" hơn TCP/IP và IPX/SPX và do đó nó hoạt động tốt hơn.

Khuyết điểm chủ yếu của giao thức NetBEUI là nó không có khả năng định tuyến, vì vậy ta không thể sử dụng nó trong các mạng có nhiều hơn 1 đoạn mạng. Và NetBEUI cũng không được công nhận rộng rãi so với giao thức TCP/IP.

Để cài đặt NetBEUI, làm như sau:

1. Ở Desktop, nhấp chuột phải vào My Network Places và chọn Properties.

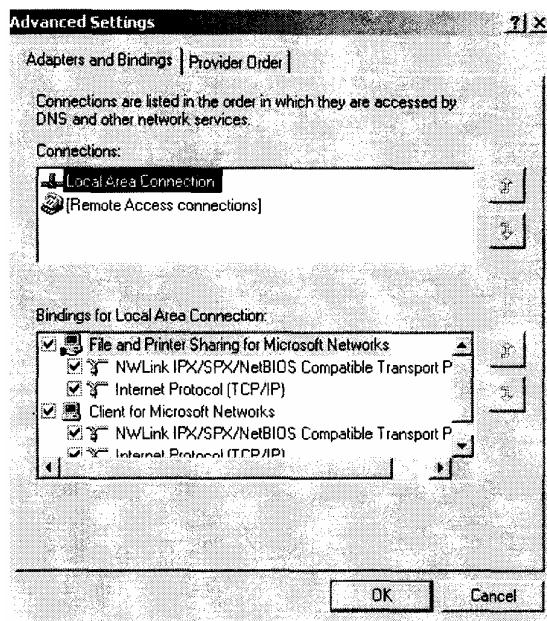
2. Nhấp chuột phải vào Local Area Connection và chọn Properties.
3. Trong hộp thoại Properties của Local Area Connection, nhấn nút Install.
4. Khi hộp thoại Select Network Component Type xuất hiện như hình 9.12, chọn Protocor và nhấn nút Add.
5. Trong hộp thoại Select Network Protocol (hình 5.13), chọn NetBEUI Protocol trong danh sách và nhấn OK.

2.4 Quản lý Network Bindings

Bindings (nối kết) được sử dụng để thiết lập sự truyền thông giữa cam mạng của ta và các giao thức mạng được cài đặt. Nếu ta có nhiều giao thức mạng được cài đặt trên máy, ta có thể cải thiện sự hoạt động bằng cách đặt các giao thức được sử dụng thường xuyên nhất lên trên thứ tự nối kết.

Để cấu hình các nối kết mạng, truy nhập vào cửa sổ Network and Dial-up Connections và chọn Advanced -> Advanced Settings trong thanh thực đơn. Tab Adapter and Binding của hộp thoại Advanced Seuings xuất hiện (hình 5.15). Với mỗi kết nối nội bộ, nếu có nhiều giao thức được liệt kê, ta có thể dùng các nút mũi tên phía bên phải của hộp thoại để chuyển các giao thức tới đầu hoặc cuối của thứ tự nối kết.

Hình 5.15 Tab Adapter and Binding của hộp thoại Advanced Settings



3. Cài đặt và cấu hình các dịch vụ mạng

Các dịch vụ chính được sử dụng cho sự hoạt động giữa các thành phần của mạng là DHCP, DNS, và WINS. Trong các mạng Windows 2000, chỉ có các máy Windows 2000 Server có thể làm việc như các máy chủ DHCP, WINS và DNS. Một máy tính có thể có cả 3 dịch vụ trên cùng lúc .

Các hệ điều hành sau được hỗ trợ về phía các máy khách (clients):

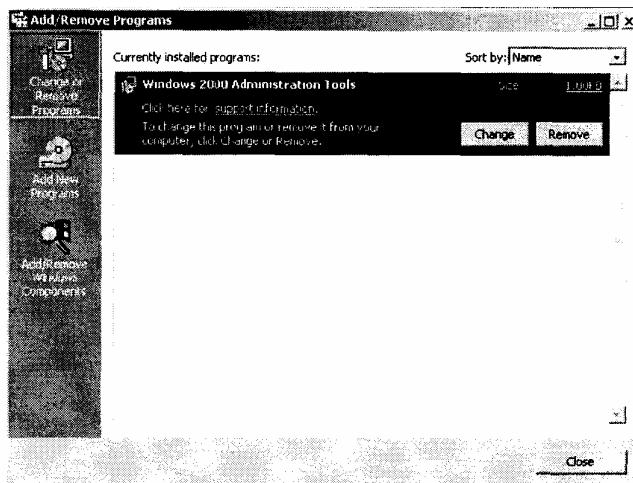
- ✓ Windows 2000 Professional hoặc Server.
- ✓ Windows NT 3.51 Workstation , Server hoặc mới hơn.
- ✓ Windows 95 hoặc 98.
- ✓ Windows cho WorkGroup 3.11 (với TCP/IP-32).
- ✓ Microsoft Network Client phiên bản 3.0 cho Microsoft MS-DOS với driver TCP/IP chế độ thực .
- ✓ Microsoft LAN Manager phiên bản 2.2c (phiên bản OS/2 không được hỗ trợ).

3.1 Cài đặt các dịch vụ mạng

Ta cài đặt các dịch vụ DHCP, WINS và DNS thông qua Add/Remove Programs trong Control Panel. Các bước như sau:

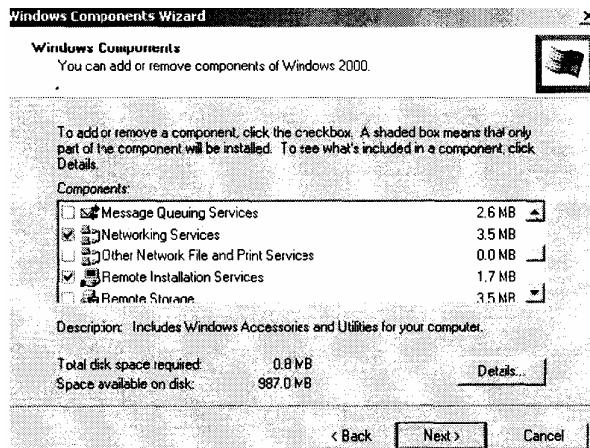
1. Hãy chắc chắn rằng máy chủ đã được cấu hình với địa chỉ IP anh bằng cách kiểm tra TCP/IP properties.
2. Chọn Start > Settings > Control Panel. Nhấp đúp lên biểu tượng Add/Remove Programs.
3. Cửa sổ Add/Remove Programs sẽ xuất hiện như trong hình 5.16. Cách vào tùy chọn Add/Remove Windows Components

Hình 5.16 Cửa sổ Add/Remove Programs



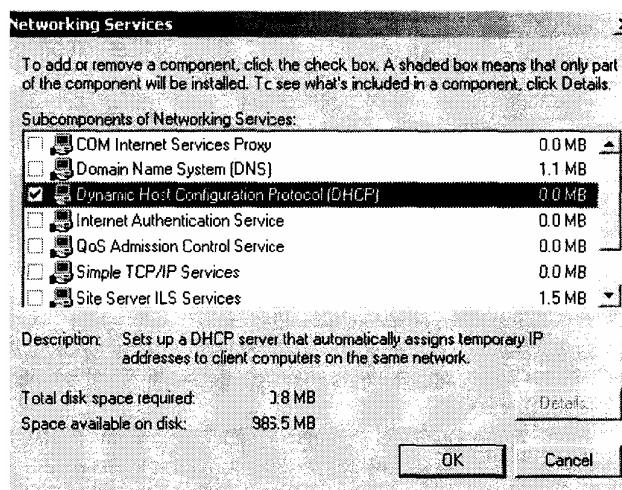
4. Khi Windows Components Wizard chạy như trong hình 5.17, chọn Networking Services và nhấp vào nút Details.

Hình 5.17 Hộp thoại Windows Components Wizard



5 . Hộp thoại Networking Services xuất hiện như hình 5.18 . Chéch vào chéch box cho các dịch vụ mà ta muốn cài đặt: Dynamic Host Configuration Protocol (DHCP), Windows Intemet Name Services(WINS) hoặc Domain Name Services (DNS). Sau đó nhấn OK.

Hình 5.18 Hộp thoại Networking Services



6. Ta trở lại hộp thoại Windows Components, nhập vào nút Next.

7. Hộp thoại Completing the Windows Components Wizard xuất hiện, nhập vào nút Finish.

8. Ta trở lại cửa sổ Add/Remove Programs. Nhập vào nút Close. Đóng Control Panel.

Sau khi đã cài đặt xong các dịch vụ mạng phù hợp, ta có thể cấu hình máy chủ DHCP, WINS, hoặc DNS. Với mỗi dịch vụ đã cài đặt, ta có thể thấy một mục tương ứng trong nhóm Administrative Tools.

3.2 Sử dụng DHCP

Mỗi thiết bị sử dụng TCP/IP trong mạng của ta phải có địa chỉ IP hợp lệ duy

nhất. Để làm bớt khó khăn trong việc lưu và gán các địa chỉ IP hợp lệ, Internet Engineering Task Force (IETF) đã phát triển DHCP.

Để chạy được DHCP, máy tính cài Windows 2000 Server phải thỏa mãn các yêu cầu sau:

- ✓ Đã cài đặt dịch vụ mạng DHCP.
- ✓ Đã cấu hình địa chỉ IP tĩnh.
- ✓ Có một dãy các địa chỉ IP để có thể gán cho các máy khách của DHCP.

Tất cả các hệ điều hành của Microsoft được liệt kê ở trên đều được hỗ trợ để làm máy khách DHCP, cả UNIX và Macintosh cũng được hỗ trợ.

Sự cần thiết của DHCP

Để biết được máy nào có địa chỉ IP nào là cả một vấn đề khó khăn. Các công ty đã sử dụng các cơ sở dữ liệu, bảng tính, và thậm chí cả các nhãn dính để quản lý máy nào có địa chỉ IP nào.

Không may là các phương thức sử dụng để quản lý bằng tay các địa chỉ IP chỉ hoạt động tốt vào lần cập nhật cuối cùng. Nếu người quản trị quên ghi chú rằng một địa chỉ đã được gán, địa chỉ đó có thể được gán 2 lần. Người quản trị cũng có thể gõ sai địa chỉ IP dẫn đến việc trùng địa chỉ hoặc địa chỉ vừa gõ là hoàn toàn sai. Đôi khi người dùng cũng gây ra các lỗi như khi chép thông tin cấu hình của máy người làm việc bên cạnh hoặc cố đoán một địa chỉ IP khi người quản trị hệ thống không có ở đó.

TCP/IP Microsoft có gắng giảm thiểu các vấn đề về sự trùng lặp địa chỉ IP bằng cách gửi ra một thông báo Address Resolution Protocol (ARP) khi một máy tính khởi tạo tập giao thức TCP/IP. Nếu một máy tính trả lời cho thông báo quảng bá ARP, có nghĩa là địa chỉ IP đó đã được sử dụng và TCP/IP sẽ không được khởi trên máy tính mới đó. Cả 2 máy tính đều sẽ nhận được một cảnh báo rằng một địa chỉ IP đã bị lặp.

Việc một máy tính chuyển từ một mạng con này sang một mạng con khác mà không cấu hình lại địa chỉ IP cũng thường gây ra lỗi. Nếu một máy tính chuyển sang một mạng con khác, địa chỉ IP phải được thay đổi để phản ánh địa chỉ mạng con và mạng mới. Nếu địa chỉ IP không được cập nhật sau khi chuyển, TCP/IP sẽ được khởi tạo, nhưng máy tính này không thể kết nối được với các máy tính khác trong mạng vì nó sẽ cho rằng đoạn mạng của nó là ở ngoài và đoạn mạng ở ngoài là đoạn mạng mà nó đang ở trong đó.

Tìm hiểu sự thực thi của DHCP

DHCP được thực thi như một dịch vụ khách/chủ (hình 5.19). DHCP làm việc như sau:

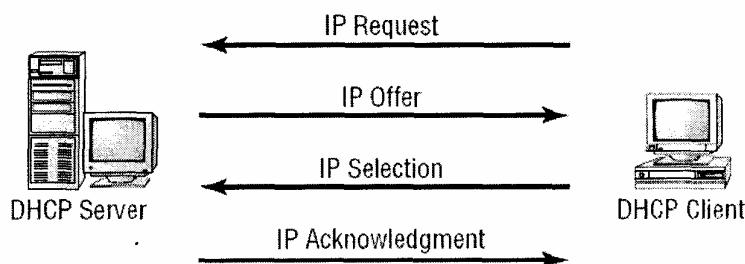
1. Khi một máy khách khởi động, nó sẽ gửi một thông báo quảng bá DHCP-DISCOVER, yêu cầu một máy chủ DHCP. Yêu cầu này bao gồm cả địa chỉ vật lý của

máy khách.

2. Bất kỳ máy chủ DHCP nào nhận được thông báo mà có các địa chỉ IP rồi sẽ gửi lại một thông báo DHCPOFFER cho máy khách, đề nghị một địa chỉ IP cho một khoảng thời gian (gọi là một *lease - khoảng cho thuê*), một mặt nạ mạng con và một cách nhận dạng máy chủ (địa chỉ IP của máy chủ DHCP). Địa chỉ được đề nghị bởi máy chủ sẽ được đánh dấu là bận và sẽ không được đề nghị cho các máy client khác trong giai đoạn dàn xếp DHCI).

3. Máy khách sẽ chọn một trong các địa chỉ được đề nghị và phát quảng bá thông báo DHCPREQUEST để chỉ ra địa chỉ mà nó chọn. Điều này cho phép các địa chỉ DHCP được đề nghị khác sẽ trở về trạng thái rỗng.

4. Máy chủ DHCP được chọn sẽ gửi trả một thông báo DHCPPACK như một sự thửa nhận bao gồm địa chỉ IP, mặt nạ mạng và khoảng thời gian cho thuê mà máy khách sẽ sử dụng. Nó cũng có thể gửi thông tin cấu hình thêm như địa chỉ của Gateway mặc định hoặc địa chỉ máy chủ DNS. **Hình 5.19 Tiến trình tạo-cho thuê DHCP**



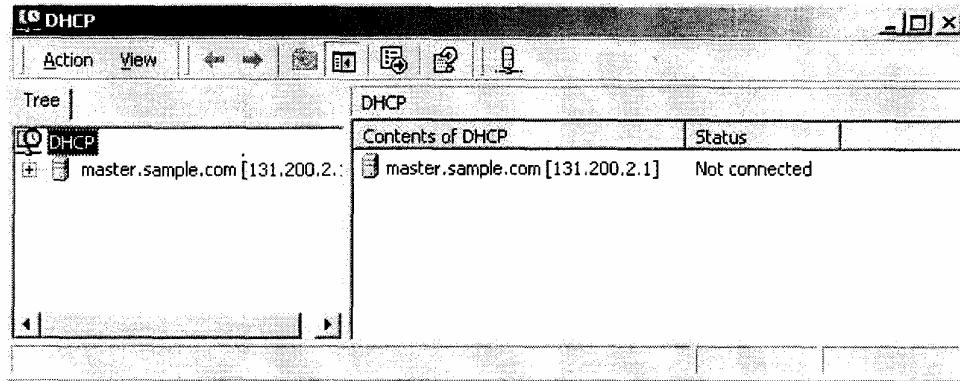
Cấu hình một máy chủ DHCP

Sau khi dịch vụ DHCP đã được cài đặt, ta sẽ thấy mục chương trình DHCP trong Administrative Tools.

Để cấu hình DHCP làm như sau:

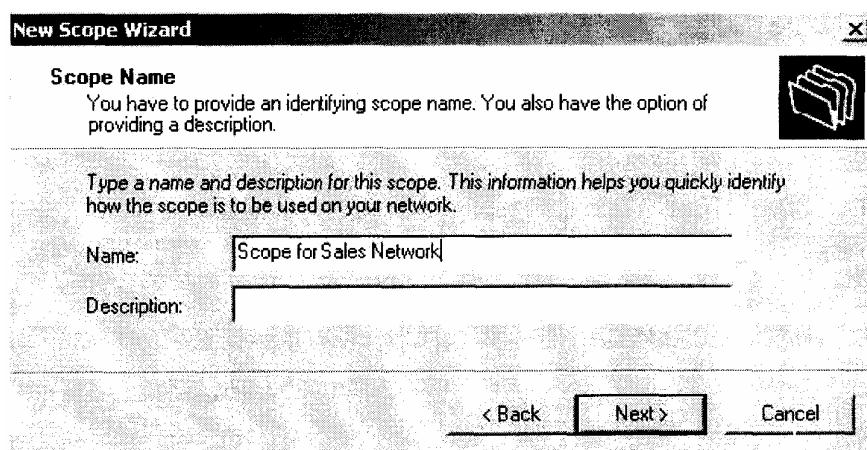
- Chọn Start > Programs > Administrative Tools > DHCP.
- Cửa sổ DHCP sẽ xuất hiện như hình 5.20. Nhấp chuột phải máy chủ của ta và chọn New Scope trong thực đơn đồ họa.

Hình 5.20



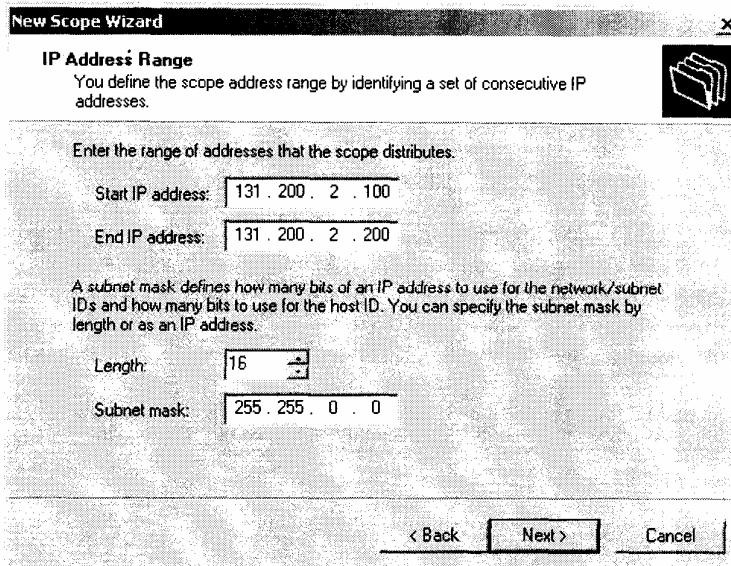
3. Khi New Scope Wizard khởi động, nhấn nút Next.
4. Hộp thoại Scope Name xuất hiện như hình 5.21. Nhập vào tên và chú giải dùng để xác định phạm vi đó. Nhấn nút Next.

Hình 5.21 Hộp thoại Scope Name



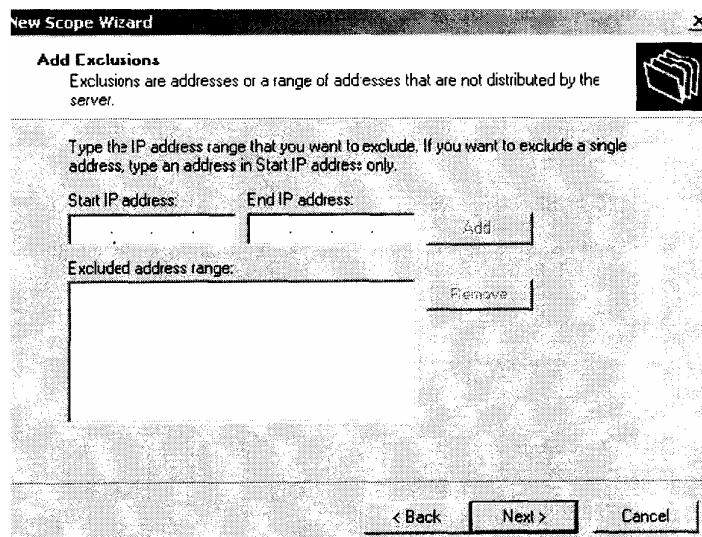
5. Hộp thoại IP Address Range xuất hiện như hình 5.22. Nhập các địa chỉ đầu IP và cuối của vào các hộp tương ứng để định nghĩa dãy các địa chỉ cho phạm vi của DHCP. Xác định mặt nạ mạng con sẽ được sử dụng trong bởi phạm vi DHCP, hoặc độ dài hoặc gõ vào địa chỉ IP, và nhấn nút Next.

Hình 5.22



6. Hộp thoại Add Exclusions xuất hiện như hình 5.23. Trong hộp thoại, ta có thể xác định bất kỳ địa chỉ nào để loại trừ trong phạm vi xác định của DHCP. Những sự loại trừ này dùng để lấy lại địa chỉ IP đã sử dụng hoặc được lấy lại. Để loại trừ một địa chỉ đơn, gõ địa chỉ trong hộp văn bản Suất IP Address và nhấn nút Add. Để loại trừ một dãy liên tục các địa chỉ IP, nhập vào địa chỉ IP bắt đầu và kết thúc vào trong các hộp văn bản và nhấn nút Add. Nút Remove dùng để gỡ các địa chỉ được loại bỏ. Sau khi đã cấu hình xong các địa chỉ này, nhấn nút Next.

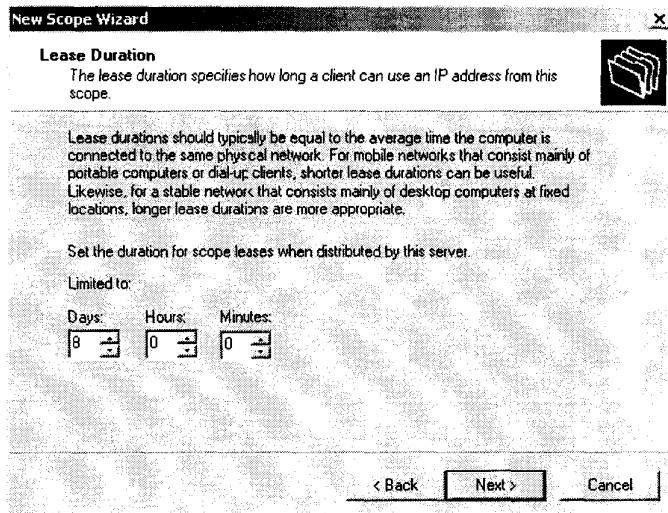
Hình 5.23 Hộp thoại Add Exclusions



7. Hộp thoại Lease Duration xuất hiện như trong hình 5.24. Trong hộp thoại này, ta xác định thời gian mà máy khách sẽ sử dụng địa chỉ IP trước khi địa chỉ IP trở về phạm vi của DHCP. Mặc định, một máy khách DHCP sẽ cố gắng lấy lại địa chỉ IP của nó khi một nửa thời gian cho thuê đã hết. Thời gian cho thuê mặc định là 8 ngày. Ta có

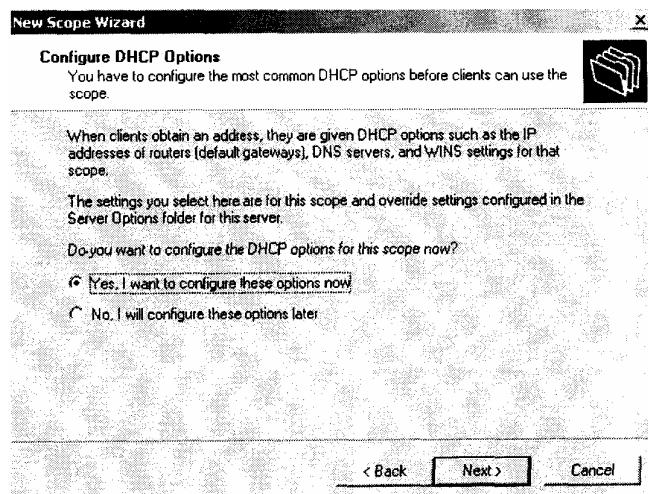
thể rút ngắn thời gian cho thuê nếu ta chỉ có một số lượng hạn chế các địa chỉ IP trong phạm vi so với số lượng các máy khách yêu cầu địa chỉ IP. Sau khi cấu hình xong phạm vi, nhấn nút Next.

Hình 5.24 Hộp thoại Lease Duration



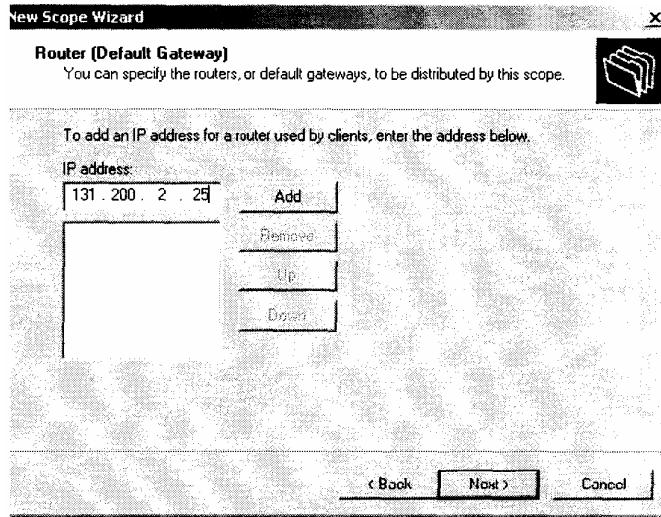
8. Hộp thoại Configure DHCP Options xuất hiện như hình 5.25. Ta có thể chọn để cấu hình các tùy chọn IP thông dụng nhất trong hộp thoại này. Ngược lại, chọn No, I will Configure These Options Later, và sẽ gán Gateway mặc định, các máy chủ DNS, và các máy chủ WINS vào lúc khác (nhưng trước khi các máy khách sử dụng bất kỳ một địa chỉ IP nào trong phạm vi của DHCP). Trong ví dụ dưới đây, tùy chọn "Yes, I Want to Configure These Options Now" được chọn để cấu hình các thiết đặt thêm của DHCP. Nhấn nút Next để tiếp tục

Hình 5.25 Hộp thoại Configure DHCP Options



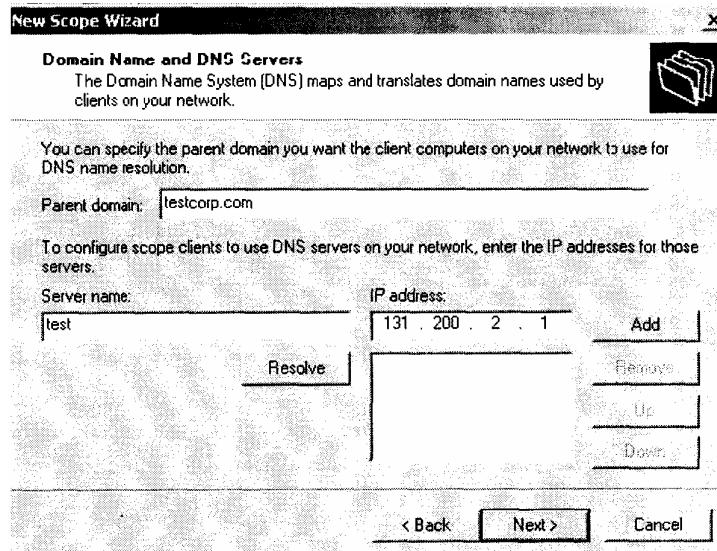
9. Hộp thoại Router (Default Gateway) xuất hiện như trong hình 5.26. Xác định địa chỉ IP cho Gateway mặc định sẽ được sử dụng bởi các máy khách DHCP và nhấn nút Add. Nhấn nút Next.

Hình 5.26 Hộp thoại Router (Default Gateway)



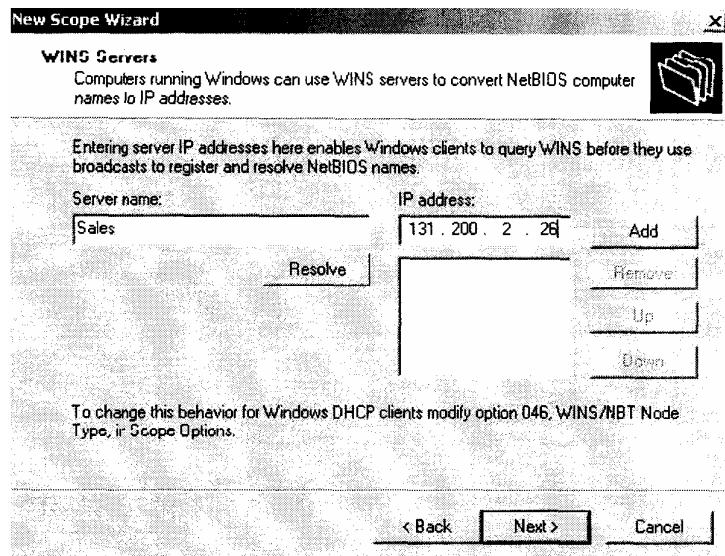
10 Hộp thoại Domain Name and DNS servers xuất hiện như hình 5.27. Hộp thoại này cho phép ta cấu hình miền cha mà các máy khách DHCP sẽ sử dụng cho việc phân giải tên DNS. Ta cũng có thể cấu hình tên máy chủ và địa chỉ của các máy chủ DNS sẽ được sử dụng cho việc phân giải tên DNS. Sau khi ta xác định các thông tin này, nhấn nút Next Hình

5.27 Hộp thoại Domain Name and DNS servers



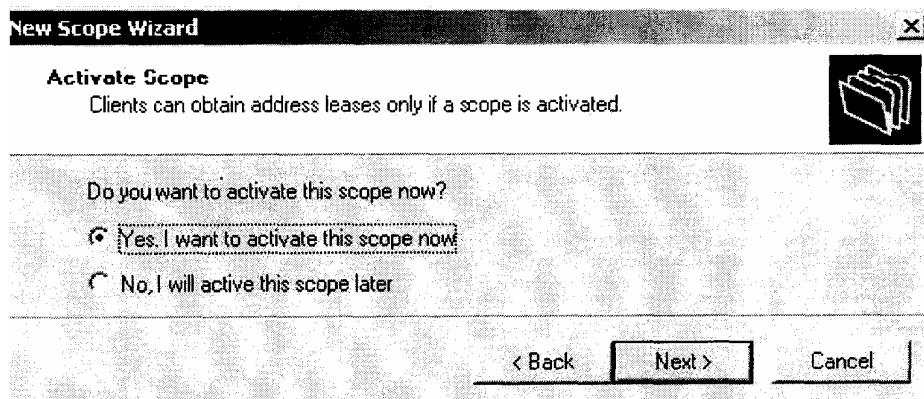
11. Hộp thoại WINS Servers xuất hiện như trong hình 5.28. Hộp thoại này cho phép ta cấu hình các máy chủ WINS chính và phụ được sử dụng để phân giải các tên máy tính NetBIOS sang địa chỉ IP. Xác định lại thông tin về máy chủ WINS và nhấn nút Next.

Hình 5.28 Hộp thoại WINS Servers



12. Hộp thoại Activeate Scope xuất hiện như hình 5.29. Hộp thoại này cho phép ta xác định xem có kích hoạt phạm vi DHCP hay không. Các máy khách DHCP chỉ có thể sử dụng các dịch vụ của phạm vi DHCP hoạt động. Ta có thể chọn để kích hoạt ngay bây giờ hoặc để sau. Sau đó, nhấn nút Finish.

Hình 5.29 Hộp thoại Activeate Scope



13. Hộp thoại Completing the New Scope Wizard xuất hiện, nhấn Finish.

14. Nếu máy chủ DHCP là một phần của Active Directory, ta cũng phải ủy quyền cho máy chủ DHCP. Để làm như vậy, nhấp chuột phải vào máy chủ DHCF trong cửa sổ DHCP chính và chọn Authorize từ thực đơn.

3.3 Sử dụng WIN

Trước Windows2000, các bản phia khách như Windows 98, NT sử dụng tên NetBIOS để liên lạc với các máy khác trên mạng. Máy chủ WINS được sử dụng để ánh xạ tên NetBIOS với địa chỉ IP.

Khi một máy khách có gắng liên lạc với máy tính khác sử dụng tên NetBIOS

trong môi trường WINS, các bước sau được tiến hành để chuyển địa chỉ NetBIOS sang địa chỉ IP.

1. Máy khách sẽ kiểm tra bộ nhớ tạm (cache) lưu tên NetBIOS nội bộ để xem có ánh xạ nào từ tên NetBIOS đó sang địa chỉ IP không.
2. Nếu không, máy khách sẽ gửi một yêu cầu tên tới máy phục vụ WINS chính.
3. Nếu máy phục vụ WINS chính không đáp ứng sau ba lần yêu cầu, máy khách sẽ gửi yêu cầu tên tới máy phục vụ WINS thứ cấp.
4. Nếu không có máy phục vụ WINS nào có thể chuyển đổi tên đó sang địa chỉ IP, một gói tin broadcast sẽ được gửi lên mạng để có gắng xác định được địa chỉ IP của máy đích.

Một khi máy phục vụ WINS được cài đặt và máy khách sử dụng WINS được cấu hình, việc đăng ký tên WINS sẽ được thực hiện một cách tự động. Khi máy khách WINS bắt đầu, nó sẽ tự động gửi địa chỉ IP của nó và tên NetBIOS tới máy phục vụ WINS đã được định sẵn. Nó yêu cầu máy phục vụ WINS xác định xem tên NetBIOS mà nó đang dùng là chưa được thiết đặt cho máy nào cả. Quá trình này cũng xảy ra nếu địa chỉ IP thay đổi (ví dụ, máy tính được chuyển tới một mạng con hay DHCP gán một thông tin cấu hình mới). Việc đăng ký tên là tạm thời, do đó máy khách WINS cần phải làm mới việc đăng ký tên sau một khoảng thời gian xác định.

Ta có thể cài đặt máy chủ WINS như mô tả trong phần "Cài đặt các dịch vụ mạng" trong chương này. Để có thể hoạt động như một máy chủ WINS, máy tính Windows 2000 server cần thỏa mãn các yêu cầu sau:

- ✓ Có dịch vụ WINS đã được cài.
- ✓ Có một địa chỉ IP tĩnh, mặt nạ mạng con, và cổng giao tiếp mặc định (nếu định tuyến làm việc) được cấu hình rồi.

Sau khi WINS được cài, bạn sẽ thấy chương trình WINS trong nhóm các công cụ quản trị Administrative Tools. Ta có thể xem nội dung cơ sở dữ liệu WINS và cấu hình WINS thông qua tiện ích này.

3.4 Sử dụng DNS

DNS được sử dụng cùng với Internet và cùng với mạng riêng để chuyển tên máy thành địa chỉ IP. Tên máy không cần phải giống như tên của máy tính Windows 2000 nhưng đó là thiết lập mặc định.

DNS là một cấu trúc phân cấp được sử dụng để quản lý tên miền của tổ chức. Định của cấu trúc phân cấp này được biểu diễn bởi một dấu (.). Ví dụ của các miền mức cao nhất là .com, .edu, .net, .org, .gov và mở rộng cho các vùng địa lý. Các công ty, tổ chức và các cá nhân đăng ký tên miền mức 2.

Để có thể truy cập một máy tính, ta sử dụng một máy phục vụ tên miền đầy đủ

(FQDN), và sử dụng FQDN để chuyển tên miền sang địa chỉ IP xác định.

Để thiết lập trở thành máy phục vụ DNS, máy tính Windows2000 server cần phải được cấu hình cùng với giao thức TCP/IP sử dụng địa chỉ IP tĩnh. DNS có thể được cài trên nhiều máy Windows2000.

Năm bước giải pháp tên miền.

Quá trình sau được sử dụng khi một máy khách gửi yêu cầu tới DNS server để tham chiếu tên:

1. Máy khách yêu cầu máy phục vụ DNS rằng nó được cấu hình để sử dụng cho việc giải quyết tên.

2. Nếu máy phục vụ DNS có thể đáp ứng được yêu cầu này, nó sẽ phản hồi lại máy khách. Cái này gọi là yêu cầu tương tác.

3. Nếu máy phục vụ DNS không thể trả lời được yêu cầu, máy phục vụ DNS sẽ liên hệ với các máy phục vụ DNS khác trên tư cách một máy khách để cố gắng giải quyết được yêu cầu mà nó cần phải giải quyết. Đó là yêu cầu chi tiết hay đệ quy.

Khi ta truy vấn một DNS server, ta có thể sử dụng 2 kiểu truy vấn:

- ✓ Truy vấn tìm kiếm tiến là yêu cầu để ánh xạ FQDN tới một địa chỉ IP xác định.
- ✓ Truy vấn tìm kiếm lùi là yêu cầu để ánh xạ IP thành FQDN.

Chú ý: Windows 2000 hỗ trợ DNS động, có nghĩa là nếu ta sử dụng DHCP để gán địa chỉ IP, ánh xạ tên-địa chỉ IP sẽ được tự động đăng ký với máy phục vụ DNS khi DHCP thông tin cấu hình được thiết lập.

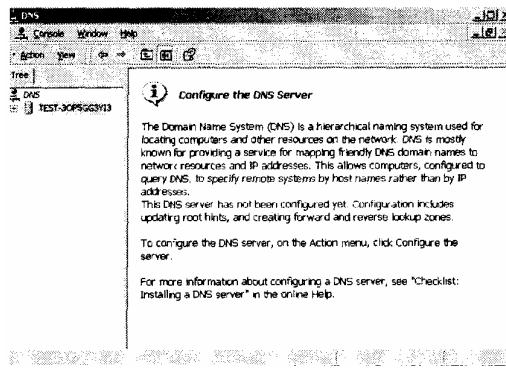
Cấu hình một máy phục vụ DNS:

Sau khi DNS được cài đặt, ta sẽ thấy chương trình DNS trong nhóm Administrative Tools.

Thực hiện các bước sau để cấu hình một máy phục vụ DNS:

1. Chọn Start > Program > Administrative Tools > DNS.
2. Cửa sổ DNS xuất hiện, như trong hình 5.30. Nhấn chuột phải vào máy phục vụ DNS của ta và chọn Configure the Server từ menu thả xuống.

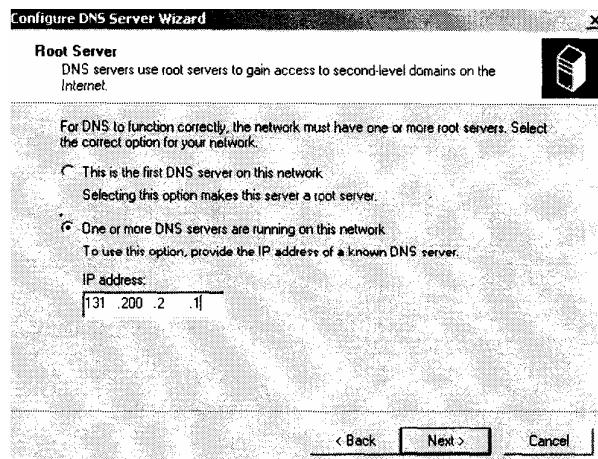
Hình 5.30. Cửa sổ DNS



3. Phần Configure DNS Server Wizard khởi động. Nhấn nút Next.

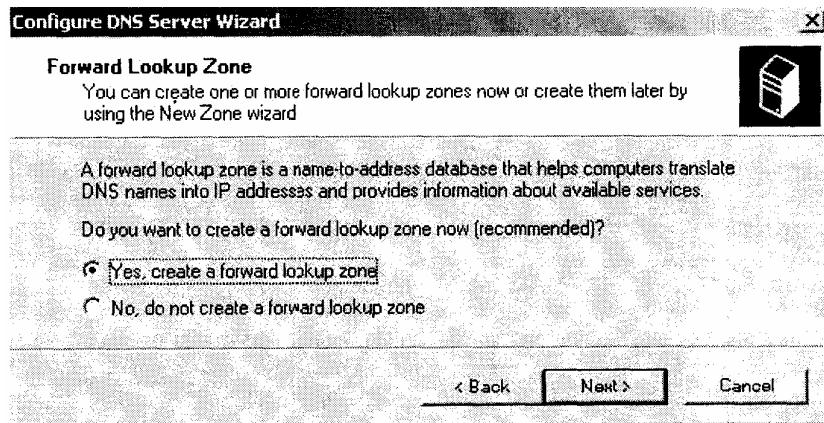
4. Hộp thoại Root Server xuất hiện như trong hình 5.31. Trong cửa sổ này, ta xác định đó là máy phục vụ DNS thứ nhất trên mạng hay là mạng của ta đã có máy phục vụ DNS rồi. Nếu ta chọn "*This is the first DNS Server on This Network*" thì máy tính này sẽ trở thành máy phục vụ DNS gốc. Nếu ta cấu hình DNS trên một máy phục vụ trong mạng cổ sử dụng dịch vụ Active Directory, một máy phục vụ DNS sẽ tự động được chạy. Trong ví dụ này, tùy chọn "*One or More DNS Servers Are Running on This Network*" được chọn. Nhấn nút Next.

Hình 5.31 Hộp thoại Root Server



5. Hộp thoại Forward Lookup Zone xuất hiện như Hình 5.32. Vùng tìm kiếm tiến là các file cơ sở dữ liệu lưu giữ ánh xạ tên DNS-địa chỉ IP. Lựa chọn xem có tạo file này không. Trong ví dụ này, chọn "*Yes, Create a Forward Lookup Zone*". Nhấn nút Next.

Hình 5.32. Hộp thoại Forward Lookup Zone



6. Hộp thoại Zone Type xuất hiện, hình 5.33. Trong hộp thoại này, ta chỉ định kiểu vùng sẽ được chọn. Có ba kiểu vùng có thể chọn lựa:

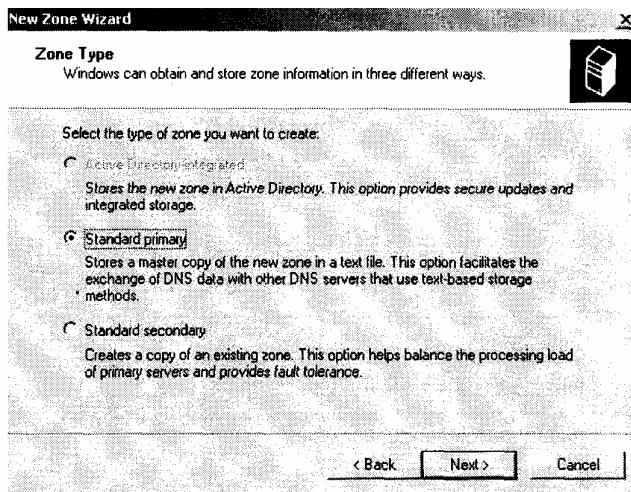
Tích hợp Active Directory, được sử dụng cùng với Active Directory để lưu và sao chép file zone. Cơ sở dữ liệu Zone được sao chép khi việc sao chép Active Directory xảy ra. Tùy chọn này không được kích hoạt trên máy phục vụ chưa cài Active Directory.

Sơ cấp chuẩn (Standard Primary) là bản copy chính của một vùng mới và lưu cơ sở dữ liệu zone như là file text.

Thứ cấp chuẩn (Standard Secondary) là bản copy của một file zone đã có. Tùy chọn này được sử dụng để cân đối giữa việc đỗ thửa và tải.

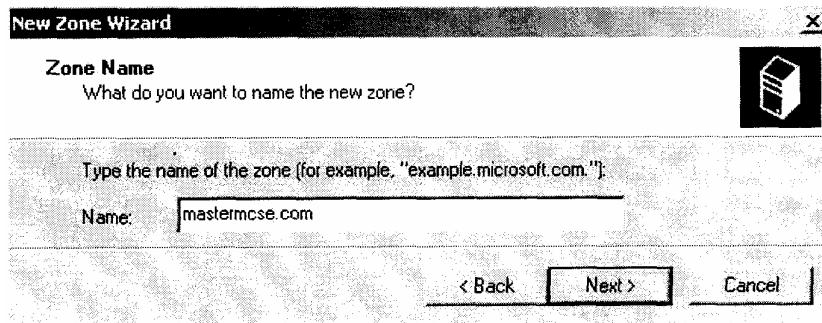
Sau khi ta chọn được tùy chọn của mình, nhấn Next.

Hình 5.33 Hộp thoại Zone Type



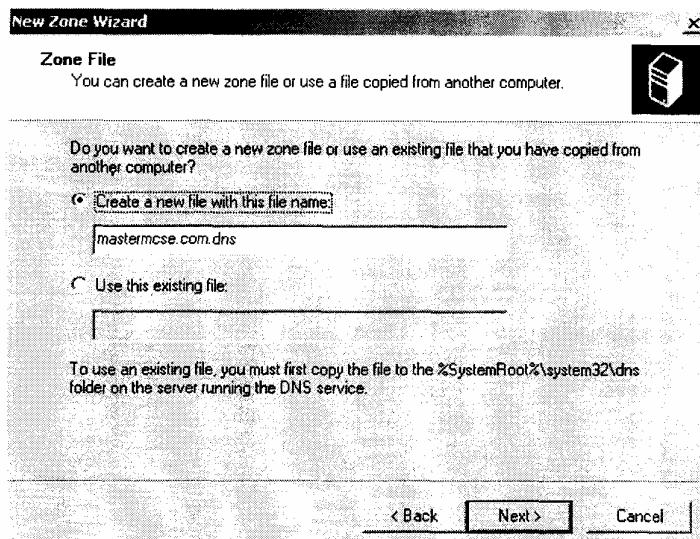
7. Nếu ta chọn để tạo một vùng sơ cấp chuẩn trong bước 6, hộp thoại Zone Name xuất hiện như hình 5.34. Nó cho phép ta chỉ định tên của zone. Nhập vào một tên và nhấn nút Next.

Hình 5.34. Hộp thoại Zone Name



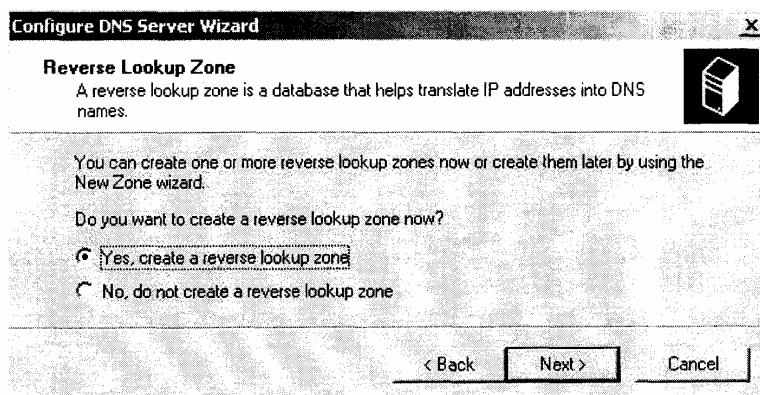
8. Hộp thoại Zone File xuất hiện như hình 5.35. Hộp thoại này cho phép ta tạo một file mới cho vùng đó hay sử dụng một file sẵn có copy từ máy khác. Sau khi lựa chọn, nhấn nút Next.

Hình 5.35 Hộp thoại Zone File



9. Hộp thoại Vùng tìm kiếm lùi xuất hiện như Hình 5.36. Một vùng tìm kiếm lùi được sử dụng để chuyển IP -> tên DNS. Hãy lựa chọn xem có tạo file không. Trong ví dụ này, chọn "No, Do Not Create a Reverse Lookup Zone". Nhấn nút Next.

Hình 5.36 Hộp thoại vùng tìm kiếm lùi



10. Hộp thoại Completing the Configure the DNS Server Wizard xuất hiện. Nếu tất cả thông tin là đúng, hãy nhấn Finish.

4. Tổng kết

Chương này đã mô tả cách quản lý các kết nối mạng như thế nào, bao gồm các chủ đề sau:

- ✓ Làm thế nào để cài đặt, cấu hình và giải quyết sự cố card mạng, ta cài card mà không thuộc loại Plug and Play thông qua chức năng Add/Remove Hardware Wizard. Trong hộp thoại Properties của nó ta có thể cấu hình card mạng này.
- ✓ Làm thế nào để cài, cấu hình và kiểm tra các giao thức mạng. Giao thức mặc định được cài với Windows 2000 Server là Tcp/IP. Ta có thể cũng cài các giao thức NWlink IPX/SPX/ NetBIOS, NetBEUI, Apple Talk và DLC.
- ✓ Làm thế nào để cài và cấu hình các dịch vụ mạng. Các dịch vụ mạng bao gồm DHCP, WINS, và DNS.

CHƯƠNG 6: QUẢN LÝ MÁY IN (4 lý thuyết)

Chương này đã chỉ dẫn cách kiểm soát in ấn với Windows 2000 Server thông qua các chủ đề sau:

- ✓ Khởi tạo máy in mạng và máy in cục bộ.
- ✓ Các đặc tính bao gồm đặc tính chung, khả năng chia sẻ, điều khiển tổng và các tính năng nâng cao, tính bảo mật và cài đặt thiết bị.
- ✓ Quản lý in ấn như cài đặt các ngầm định và hủy bỏ in ấn.
- ✓ Quản lý tài liệu như tạm ngừng, tiếp tục và hủy quá trình in tài liệu.
- ✓ Quản lý các chức năng của dịch vụ in gồm định dạng, quản lý cổng, trình cài đặt và các tính năng nâng cao.

1. Cài đặt máy in

Kiểm soát, cấu hình, khắc phục lỗi và điều khiển truy nhập máy in. Quá trình xử lý của việc cài đặt mới, quản lý và xoá máy in khá đơn giản. Khi cài đặt mới một máy in, ta sử dụng kịch bản có sẵn (Wizard), kịch bản này hướng dẫn ta từ đầu đến cuối từng bước để thiết lập máy in. Những thông số không thiết lập được bởi kịch bản Add Printer Wizard có thể thay đổi thông qua việc cấu hình các đặc tính của máy in (Printer's Properties). Ta cũng có thể quản lý các tùy chọn của máy in như dừng và xoá công việc in cho toàn bộ máy in hoặc các tài liệu in riêng biệt. Trong chương này ta sẽ học những điều cơ bản về in ấn trong Windows 2000 Server, làm thế nào để cài đặt và cấu hình máy in, hay quản lý máy in và công việc in ấn, cũng như quản lý máy dịch vụ in (Quá trình xử lý in trong Windows 2000 Server và Windows 2000 professional là như nhau).

Thiết lập máy in

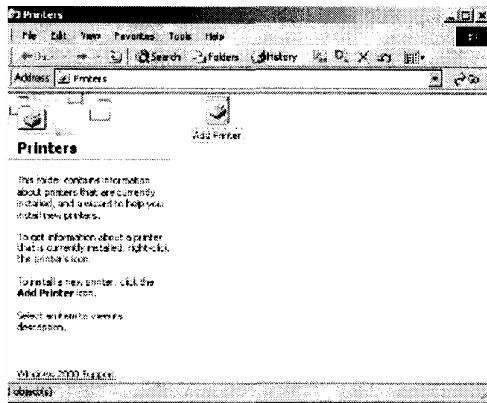
Trước khi truy cập vào thiết bị in vật lý với Windows 2000 Server, đầu tiên ta phải thiết lập máy in logic. Sau đó, ta có thể phải xoá hoặc đổi tên những máy in đó. Các quá trình này sẽ được trình bày trong phần tiếp theo.

Để tạo mới một máy in, ta sử dụng Add Printer Wizard, kịch bản này sẽ hướng dẫn ta qua tất cả các bước. Để tạo một máy in mới trong Windows 2000 Server ta phải đăng nhập người dùng thuộc nhóm Administrators hoặc Power Users. Máy tính dùng kịch bản Add Printer Wizard để tạo máy in tự động trở thành máy dịch vụ in (phát server) cho máy in đó. Máy tính là máy dịch vụ in phải đủ khả năng xử lý để hỗ trợ việc in và có đủ khoảng (ra trống để kiểm soát tất cả chuỗi công việc in).

Để tạo một máy in cục bộ (local printer) hay một máy in mạng mới (network printer), thực hiện những bước sau:

1. Chọn Start > Settings > Printers để mở thư mục Printers (xem hình 6.1). Sau đó nhấp đúp vào biểu tượng Add Printer.

Hình 6.1 Thư mục Printers với biểu tượng Add Printer



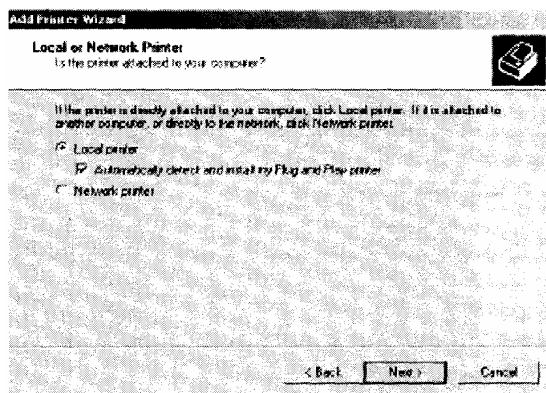
2. Add Printer Wizard bắt đầu (xem hình 6.2). Nhấn nút Next để tiếp tục.

Hình 6.2 Hộp thoại Welcome to the Add Printer Wizard



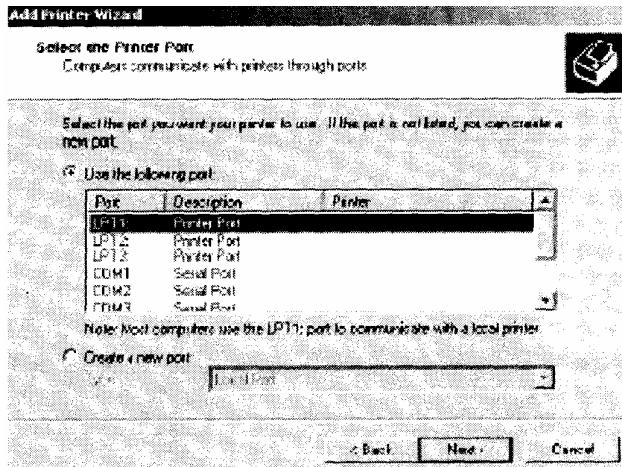
3. Khi hộp thoại Local or Network Printer sẽ xuất hiện (xem hình 6.3), chọn Local Printel nếu ta có một máy in được gắn trực tiếp với máy tính của ta, hoặc chọn Network Printel nếu ta có một máy in được nối qua mạng. Sau đó nhấn nút Next. Nếu ta có một thiết bị in Plug-and-play gắn với máy tính, máy tính sẽ được tự động dò tìm, và ta có thể chuyển tới bước 6. Nếu thiết bị in của ta chưa được gắn vào máy hoặc máy chưa nhận ra, bỏ tùy chọn Automatically Detect and Install My Plug and Play Printer và chuyển sang bước tiếp diệc để chỉ định bằng tay hình của thiết bị in.

Hình 6.3 Hộp thoại Local or Network Printer



4. Nếu ta chọn cấu hình thiết bị in bằng tay thì khi hộp thoại Select the Printer Port xuất hiện (xem hình 6.4), chỉ định cổng của thiết bị in sẽ sử dụng và nhấn nút Next.

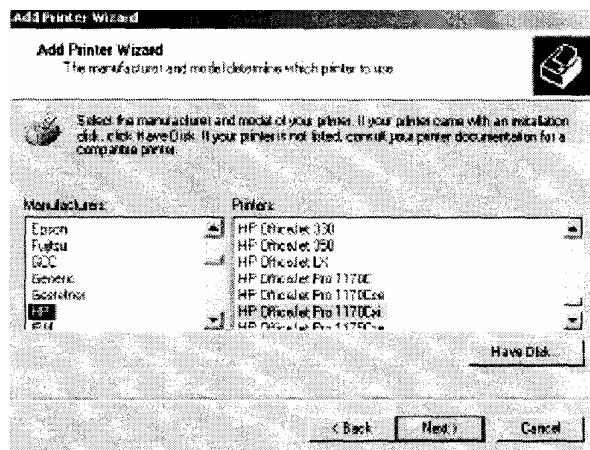
Hình 6.4 Hộp thoại Select the Printer Port



5. Khi hộp thoại liệt kê hãng sản xuất và kiểu máy in xuất hiện (xem hình 6.5), chỉ rõ hãng sản xuất và kiểu của thiết bị sau đó nhấn nút Next. Nếu thiết bị in không có trong liệt kê, nhấn nút Have Disk và đưa vào đĩa chứa driver của máy in đó.

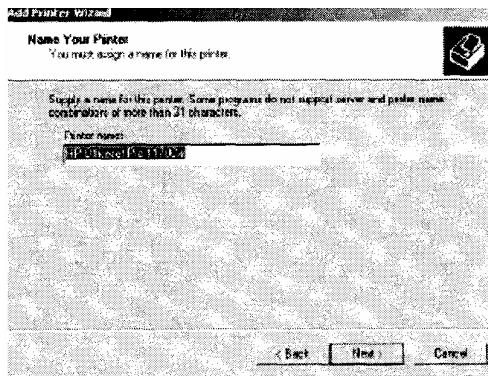
Chú ý: Nếu ta đã cài đặt driver này trên máy tính, trên hộp thoại liệt kê hãng sản xuất và kiểu máy in sẽ có thêm nút Windows Update cạnh nút Have Disk.

Hình 6.5 Chọn lựa hãng sản xuất và kiểu vữa máy in



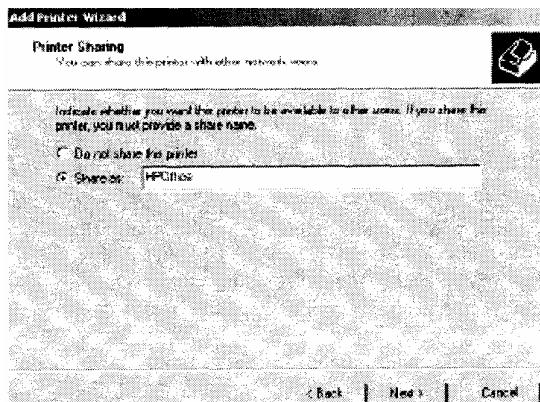
6. Hộp thoại Name Your Printer xuất hiện (xem hình 6.6). Dùng tên mặc định hoặc nhập vào tên khác cho máy in của ta và nhấn nút Next.

Hình 6.6 Hộp thoại Name Your Printer



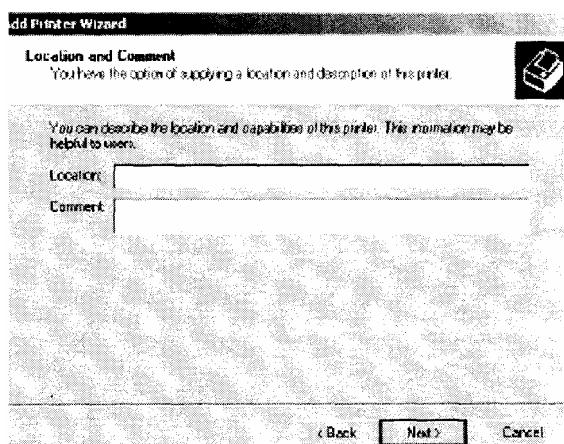
7. Hộp thoại Printer Sharing xuất hiện (xem hình 6.7). Ta có thể chọn không chia sẻ hoặc chia sẻ máy in. Nếu ta chọn chia sẻ máy in thì phải chỉ rõ tên các máy in logic được sử dụng thiết bị in vật lý. Sau đó nhấn Next để tiếp tục.

Hình 6.7 Hộp thoại Printer Sharing



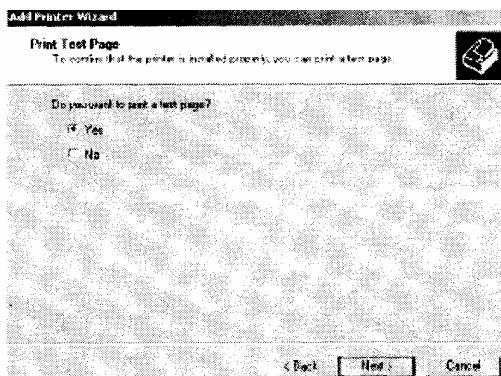
8. Nếu ta chọn chia sẻ máy in, hộp thoại Location and Comment xuất hiện (xem hình 6.8). Trong hộp thoại này ta chỉ định thông tin về vị trí và ghi chú. Người dùng trên mạng có thể sử dụng thông tin này để tìm kiếm mô tả vị trí máy in, cấu hình và khả năng của máy in. Nhấn Next để tiếp tục.

Hình 6.8 Hộp thoại Location and Comment



9. Hộp thoại Print Test Page xuất hiện (xem hình 6.9). Nếu thiết bị in được gắn với máy tính, ta nên in một trang thử nghiệm để kiểm chứng rằng mọi thứ được cấu hình đúng. Nếu không ta có thể bỏ qua bước này. Nhấn Next để tiếp tục.

Hình 6.9 Hộp thoại Print Test Page



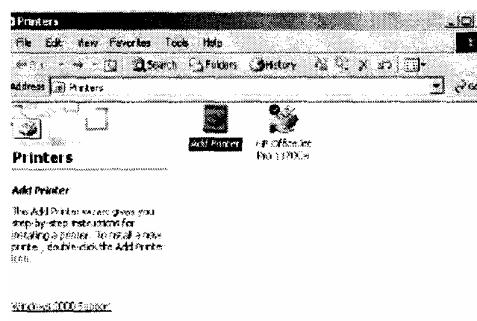
10. Hộp thoại Completing the Add Printer Wizard xuất hiện (xem hình 6.10). Đây là cơ hội để ta xác nhận mọi thiết lập của ta là hoàn toàn đúng. Nếu có vấn đề, nhấn nút Bách để sửa chữa. Nếu mọi thứ đều được cấu hình đúng thì nhấn nút Finish.

Hình 6.10 Hộp thoại Completing the Add Printer Wizard



Để hoàn tất quá trình cài đặt, Add Printer Wizard sao chép các file (nếu cần thiết) và tạo máy in cho ta. Một biểu tượng cho máy in mới sẽ xuất hiện trong thư mục Printers (xem hình 6.11).

Hình 6.11 Một biểu tượng cho máy in trong thư mục Printers



2. Quản lý thuộc tính của máy in

Các thuộc tính của máy in cho phép ta thiết lập những tùy chọn như tên máy in, máy in có lược chia sẻ hay không, và bảo mật máy in. Để truy cập vào hộp thoại Properties của máy in, mở hổ mục Printers, kích chuột phải vào máy in ta muốn quản lý, chọn Properties.

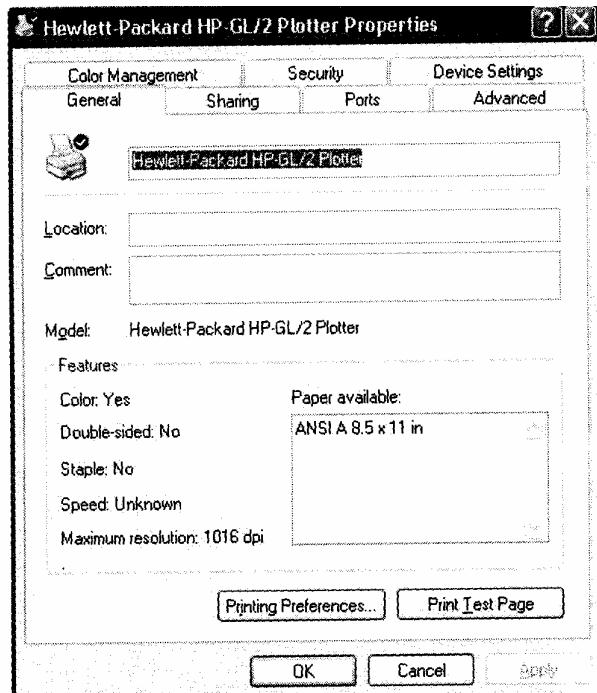
Hộp thoại Properties của máy in có 6 mục: General, Sharing, Ports, Advance, Security, và Device Settings. Phản tiếp theo mô tả những thuộc tính của các mục này.

Chú ý: Hộp thoại Properties của một số máy in có chứa thêm các mục cho phép thiết lập tính năng nâng cao của máy in đó. Ví dụ, nếu ta cài máy in HP Deskjet 970Cse, hộp thoại Properties sẽ có thêm một số mục cho việc quản lý màu và các dịch vụ (Color Management and Services).

Cấu hình thuộc tính General

Mục General của hộp thoại Properties (xem hình 6.12), chứa thông tin về máy in đồng thời cho phép cài đặt các ưu tiên in và trang in thử nghiệm.

Hình 6.12 Mục General trên hộp thoại Properties



Tên, vị trí, chú thích của máy in phản ánh sự nhập vào của ta khi ta thiết lập máy in (như mô tả trong phần trước). Ta có thể thêm vào hoặc thay đổi thông tin này trong các hộp kí tự. Bên dưới hộp Comment, ta sẽ thấy kiểu máy in. Danh mục trong phần Features của hộp thoại phụ thuộc vào kiểu vụ driver của máy in mà ta dùng. Tiếp theo là một số ví dụ về những tính năng của máy in:

- ✓ Hỗ trợ in màu.

- ✓ Hỗ trợ in hai mặt (Double-sided).
- ✓ Hỗ trợ ghim giấy (stapling support).
- ✓ Số trang lớn nhất có thể in trong một phút.
- ✓ Độ phân giải lớn nhất của máy in (in dots per inch).
- ✓ Phía dưới của hộp thoại, ta thấy nút Printing Preferences và nút Print Test Page.

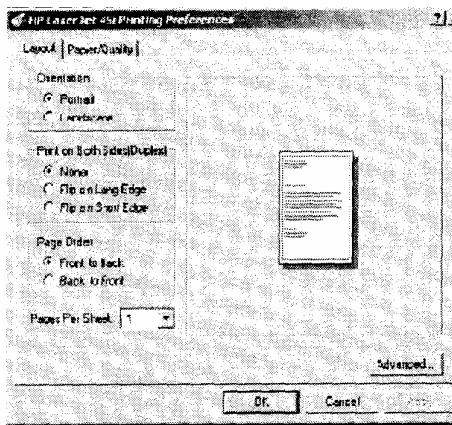
Thiết lập Printing Preferences

Nhấn nút Printing Preferences để hiển thị hộp thoại Printing Preferences, hộp thoại này cho phép ta bố trí giấy, thứ tự trang và nguồn giấy. Mục Layout and Paper Quality cùng với nút Advanced trên hộp thoại này cho phép ta cấu hình thêm các tùy chọn của máy in.

Bố trí trang in

Mục Layout của hộp thoại Printing Preferences (xem hình 6.13), cho phép ta chỉ rõ hướng trang in và thứ tự trang. Ta có thể chọn trang in là Portrait (thẳng đứng theo chiều dọc) hoặc Landscape (nằm ngang).

Hình 6.13 Mục Layout của hộp thoại Printing Preferences



Việc thiết lập thứ tự trang (Page Order settings) mới có ở Windows 2000. Nó chỉ định nếu ta muốn trang 1 của tài liệu ở trên cùng của ngăn xếp (Front to Back) hoặc trang 1 của tài liệu ở dưới cùng của ngăn xếp (Back to Front).

Chú ý: Trong Windows NT 4, tài liệu luôn được in từ đầu tới cuối, nghĩa là trang 1 được in trước tiên. Khi kết thúc công việc in, phải sắp xếp lại những trang của ta.

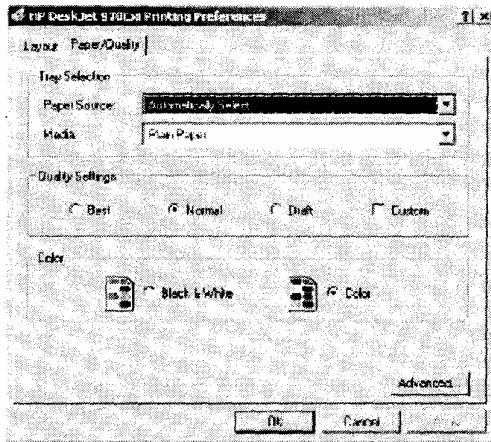
Việc thiết lập Pages Per Sheet quyết định bao nhiêu trang sẽ được in trong một trang đơn. Ta có thể sử dụng tính năng này nếu ta in một quyển sách và muốn rằng 2 trang được in liền nhau trong một trang đơn.

Thiết lập Paper/Quality

Mục Paper/Quality trên hộp thoại Printing Preferences cho phép ta cấu hình các thuộc tính liên quan đến giấy và chất lượng của công việc in. Các tùy chọn này phụ

thuộc vào tính năng của máy in. Ví dụ, máy in có thể chỉ có một tùy chọn, như Paper Source. Nhưng với máy in HP Deskjet 970Cxi, ta có thể cấu hình những tùy chọn như Paper Source, Media, Quality Settings, và Color (xem hình 6.14).

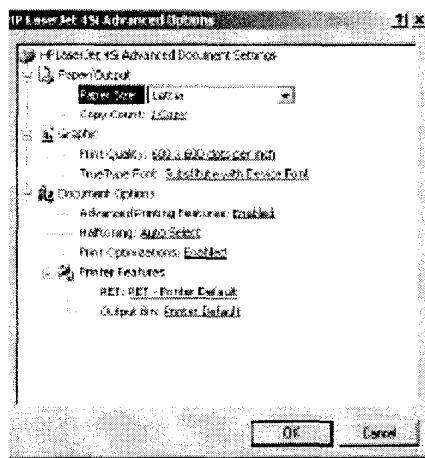
Hình 6.14 Mục Paper/Quality trên hộp thoại Printing Preferences



Các thiết lập nâng cao

Nhấn nút Advanced phía dưới góc bên phải của hộp thoại Printing Preferences sẽ đưa ta tới hộp thoại Advanced Options (xem hình 6.15). Tại đây ta có thể cấu hình một số tùy chọn của máy in như Paper/output, Graphic, Document Options, Printer Features. Các tùy chọn có hay không này phụ thuộc vào driver thiết bị in mà ta đang dùng.

Hình 6.15 Hộp thoại Advanced Options



In trang thử nghiệm

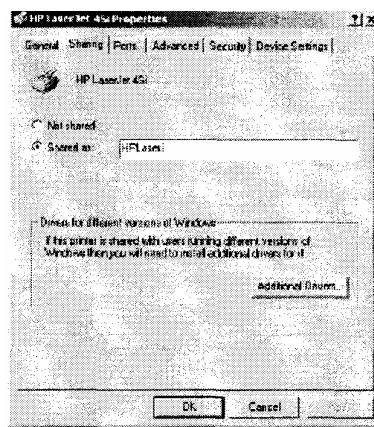
Nút Print Test Page ở phía dưới trong mục General trên hộp thoại Properties của máy in cho phép ta in một trang thử nghiệm. Tùy chọn này đặc biệt có tác dụng để xử lý sự cố khi máy in có vấn đề. Ví dụ, ta có thể dùng tùy chọn Print Test Page trong trường hợp không có driver nào tương thích với thiết bị in và ta muốn cố thử sử dụng một driver tương thích. Nếu máy in không in hoặc in không đúng (chẳng hạn mỗi

trang chỉ in một ký tự), ta sẽ biết rằng driver này không tương thích.

Cấu hình Sharing Properties

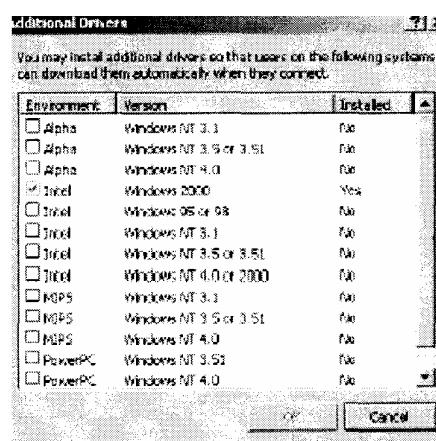
Mục Sharing trong hộp thoại Properties của máy in (xem hình 6.16) cho phép ta chỉ định máy tính được cấu hình như một máy in cục bộ hay được chia sẻ như một máy in mạng. Nếu ta định chia sẻ máy in, ta cũng cần phải định rõ tên máy dùng để chia sẻ như đó người dùng trên mạng sẽ nhìn thấy máy in của ta.

Hình 6.16 Mục Sharing trên hộp thoại Properties



Một tùy chọn nữa có thể được thiết lập thông qua mục Sharing là driver hỗ trợ cho máy in (hách không dùng Windows 2000). Đây là tính năng hỗ trợ in đặc biệt của Windows 2000 Server, rồi vì Windows 2000 Server cho phép ta chỉ định các drivers để những máy khách khác có thể Download tự động. Mặc định, driver tải vào là Intel driver cho Windows 2000. Để thêm vào Driver khác, nhấn nút Additional Driver ở phía dưới của mục Sharing. Hộp thoại Additional Driver sẽ hiển thị (xem hình 6.17).

Hình 6.17 Hộp thoại Additional Drivers



Windows 2000 Server hỗ trợ việc thêm drivers của máy in cho các nạn sau đây :

- ✓ Windows 95 hoặc Windows 98 Intel.
- ✓ Windows NT 3 . 1 Alpha, Intel, và MIPS.

- ✓ Windows NT 3.5 or 3.51 Alpha, Intel, MIPS, và Powerpc.
- ✓ Windows NT 4 Alpha, Intel, MIPS, và Powerpc.

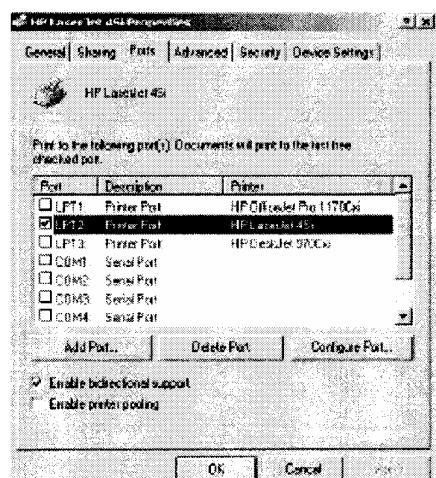
Thiết lập các đặc tính của cổng (Port Properties)

Cổng (port) được xác định như thiết bị ghép nối, cho phép máy tính giao tiếp với thiết bị in. Windows 2000 Server hỗ trợ cổng địa phương (hay cổng vật lý) và cổng TCP/IP tiêu chuẩn (hay cổng logic). Cổng địa phương được sử dụng khi máy in nối trực tiếp với máy tính. Trường hợp ta dùng Windows 2000 Server trong một nhóm làm việc nhỏ, ta thường đề máy in nối thông qua cổng LPT1.

Cổng TCP/IP tiêu chuẩn được sử dụng khi máy in nối qua mạng bằng cách cài đặt lý một cam mạng trong máy in. ưu thế của máy in mạng là nhanh hơn máy in địa phương và có thể định vị ở bất cứ nơi đâu trên mạng. Khi ta chỉ định cổng TCP/IP, ta phải biết địa chỉ IP của máy in mạng. Mục Ports (xem hình 6.18) cho phép ta có thể cấu hình toàn bộ cổng được xác định sử dụng cho máy in. Cùng với việc xoá và cấu hình các cổng đã có, ta có thể cài đặt printer pooling và dẫn hướng công việc in tới một máy in khác, điều này được mô tả ở phần tiếp theo.

Chú ý: Tuỳ chọn Enable Bidirectional Support trong mục Ports dùng được nếu máy in của ta hỗ trợ chức năng này. Nó cho phép máy in có thể giao tiếp với máy tính. Ví dụ, máy in của ta có thể gửi nhiều hơn những thông tin về lỗi máy in.

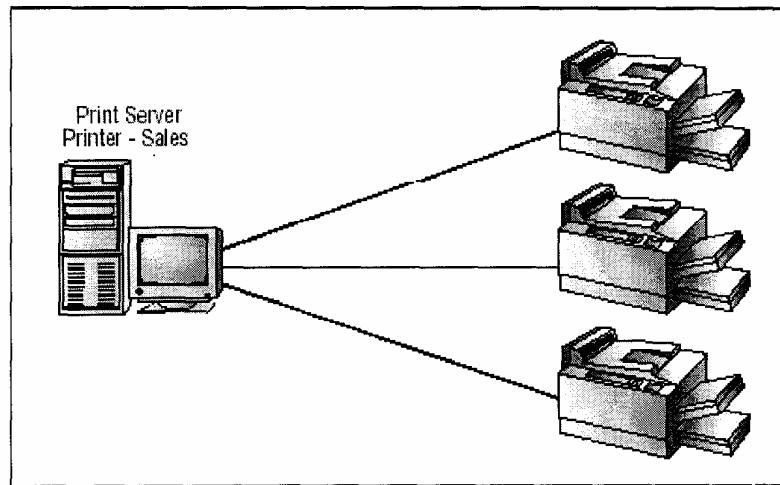
Hình 6.18 Mục Ports trong hộp thoại Properties của máy in



Printer Pooling

Printer Pools được sử dụng để kết hợp nhiều thiết bị in vật lý với một máy in logic (xem hình 6.19). Ta có thể sử dụng Printer pool nếu ta có nhiều máy in vật lý cùng kiểu ở cùng chỗ và có thể sử dụng chung driver của máy in. Sử dụng printer pool tiện lợi ở chỗ thiết bị in đầu tiên sẵn sàng sẽ in công việc của ta. Nó có tác dụng trong trường hợp có một nhóm thiết bị in được chia sẻ cho một nhóm người dùng, ví dụ như secretarial pool.

Hình 6.19 Printer pooling



Để cấu hình printer pool, tích vào tùy chọn Enable Printer Pooling ở phía dưới mục Ports và chọn mọi cổng mà các thiết bị in nối tới. Nếu ta không chọn Enable Printer Pooling, ta có thể chọn mỗi máy in một cổng khác nhau.

Chú ý: Mọi thiết bị in trong printer pool phải có khả năng dùng chung driver cho máy in.

Chuyển công việc in tới máy in khác

Nếu thiết bị bị lỗi, ta có thể chuyển các công việc in được xếp lịch chờ in tới thiết bị in khác. Để thực hiện việc này, thiết bị in mới phải có khả năng dùng chung driver như của máy in cũ

Để chuyển việc in, nhấp nút Add Port trong mục Ports, chọn New Port rồi New Port Type. Trong hộp thoại Port Name, nhập tên UNC của máy in ta muốn chuyển công việc tới dưới dạng `\computername\printer`.

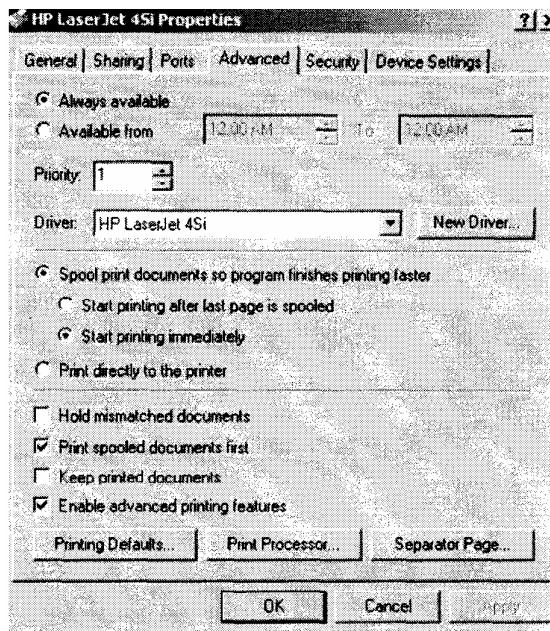
Thiết lập các đặc tính nâng cao

Mục Advanced trong hộp thoại các đặc tính của máy in (Printer Properties) như trong hình 6.20 cho phép ta kiểm soát nhiều tính năng của máy in. Ta có thể thiết lập các tùy chọn sau:

- ✓ Tính sẵn sàng của máy in.
- ✓ Quyền ưu tiên của máy in.
- ✓ Trình điều khiển (driver) mà máy in sử dụng.
- ✓ Đặc tính "Spooling".
- ✓ Cách thức văn bản được in.
- ✓ Chế độ in mặc định.
- ✓ Bộ xử lý in được sử dụng.

- ✓ Trang phân tách

Hình 6.20 Mục Advanced trong hộp thoại Printer Properties



Chú ý: Những tùy chọn có trong mục Advanced của hộp thoại Printer Properties ở Windows2000 Server Advanced được đặt trong mục General và Scheduling của hộp thoại Printer Properties ở Windows NT 4.

Tính sẵn sàng của máy in (Printer Availability)

Tính sẵn sàng của máy in (availability) hay lập lịch chương trình (scheduling) cho máy in chỉ rõ máy in phục vụ cho nhiều công việc. Thông thường ta kiểm soát tính sẵn sàng khi ta có nhiều máy in logic đều sử dụng chung một thiết bị máy in vật lý. Lấy ví dụ, ta có thể thiết lập tùy chọn này nếu ta có những công việc lớn cần đến máy in trong những khoảng thời gian khác nhau. Ta có thể lập lịch cho những công việc lớn này để in trong một khoảng thời gian xác định, ví dụ như từ 10:00PM đến 4:00AM. Để làm được việc này ta cần phải tạo ra hai máy in (logic) sử dụng cùng một cổng, ví dụ như máy in có tên là LASER và REPORTS sử dụng chung cổng LPT1. (Cả hai máy in logic trên cùng một cổng có nghĩa là một máy in vật lý phục vụ cho cả hai máy in logic này). Thiết lập máy in LASER là luôn sẵn sàng (chọn mục "Always Available") và thiết lập máy in REPORTS chỉ sẵn sàng trong khoảng thời gian từ 10:00PM đến 4:00AM. Nhờ đó những người sử dụng vừa có thể gửi những công việc cần ít thời gian đến cho máy in LASER và những công việc cần nhiều thời gian đến cho máy in REPORTS với điều kiện là công việc in chỉ gửi đến máy in REPORTS trong những khoảng thời gian đã thiết lập.

Ở chế độ ngầm định, nút bấm tùy chọn "Always Available" luôn được chọn, do đó người dùng có thể sử dụng máy in suốt 24/24 giờ trong ngày. Để hạn chế tính sẵn sàng của máy in, chọn nút bấm tùy chọn "Available From" và đặt khoảng thời gian mà

máy in cần sẵn sàng.

Tính ưu tiên của máy in

Tính ưu tiên cũng là một tùy chọn khác mà ta có thể thiết lập nếu ta có nhiều máy in logic sử dụng chung một thiết bị máy in. Ta thiết lập tính ưu tiên là chỉ ra cách thức - thứ tự gửi các công việc đến cho máy in. Lấy ví dụ, ta có thể sử dụng tùy chọn này khi hai nhóm cùng chia sẻ một máy in và ta cần điều khiển thứ tự ưu tiên của các công việc mà máy in phục vụ.

Trong mục Advanced của hộp thoại Printer Properties , ta có thể chọn giá trị của "Priority" từ 1 đến 99, với 1 là mức ưu tiên thấp nhất và 99 là mức ưu tiên cao nhất. Ví dụ, giả sử có một thiết bị máy in được sử dụng bởi phòng kế toán. Người quản lí của phòng kế toán luôn muốn việc in của họ được thực hiện trước việc in ấn của các nhân viên khác trong phòng. Để thiết lập việc xắp đặt này ta tạo một máy in có tên là MANAGERS sử dụng cổng LPTI với mức ưu tiên là 99. Sau đó tạo máy in có tên là WORKERS cũng sử dụng cổng LPTI với mức ưu tiên là 1 Trong mục Security của hộp thoại Printer Properties, ta chỉ cho phép người quản lí sử dụng máy in MANAGERS và cho phép những người sử dụng khác sử dụng máy in WORKERS (các tùy chọn về an toàn bảo mật - Security được đề cập chi tiết ở phần sau của chương này). Khi trình quản lí máy in (chương trình có nhiệm vụ kiểm soát hàng đợi của máy in để in và gửi công việc in đến đúng cổng) nhận được các công việc, nó luôn yêu cầu máy in có mức ưu tiên cao hơn thực hiện công việc in trước máy in có mức ưu tiên thấp hơn.

Trình điều khiển thiết bị in (Print Driver)

Việc thiết lập trình điều khiển thiết bị trong mục Advanced của hộp thoại Printer Properties chỉ ra trình điều khiển thiết bị được thiết lập cho máy in của ta. Nếu ta thiết lập nhiều máy in ở máy tính của ta, ta có thể chọn sử dụng bất kì trình điều khiển đã được cài đặt. Bằng cách nhấp chọn nút New Driver để bắt đầu trình Add Printer Driver Wizard cho phép ta cập nhật và thêm mới trình điều khiển thiết bị máy in.

Spooling

Khi ta thiết lập đặc tính đồng tác vụ có nghĩa là ta thiết lập phương án xếp công việc vào hàng đợi máy in hay gửi trực tiếp các công việc đến cho máy in. Spooling có nghĩa là các công việc in ấn được ghi trên ổ đĩa ở hàng đợi trước khi chúng được gửi đến cho máy in. Như là điều khiển giao thông của việc in ấn, Spooling thực hiện việc giữ tất cả các công việc in ấn đòi hỏi in ở cùng một thời điểm và thực hiện lần lượt theo thứ tự xắp hàng đợi. Ở chế độ mặc định thì spooling được thiết lập. Một tùy chọn khác là đợi cho đến khi trang cuối cùng được xắp hàng thì mới in. Tương tự với những lựa chọn này là các hành động mà ta làm khi xếp hàng tính nền trong cửa hàng bán tạp phẩm. Giả sử ta có một xe hàng đầy các tạp phẩm và chàng trai ngay sau ta chỉ có một vài món hàng. Ngay cả khi ta đã bắt đầu bỏ các thứ trong xe hàng lên bàn tính tiền,

chứng nào mà người tính tiền chưa bắt đầu với những món hàng của ta thì ta có thể cho phép người phía sau có ít món hàng hơn được tính trước hoặc ta bắt anh ta phải đợi. Khi người tính tiền đã bắt đầu tính tiền các món hàng của ta thì lúc đó ta không còn có quyền chọn lựa nữa. Chế độ spooling của Windows 2000 Server cho phép ta thiết lập điều kiện in trong các trường hợp tương tự như vậy.

Trong mục Advanced, ta có thể để tùy chọn Start Printing Immediately hoặc chọn tùy chọn Start Printing After Last Page Is Spooled. Nếu ta chọn tùy chọn sau, công việc nhỏ mà đã kết được xếp hàng sẽ được in trước công việc của ta ngay cả khi công việc của ta được "đặt vào đường ống máy in" trước. Nếu ta chỉ định tùy chọn Start Printing Immediately, công việc nhỏ hơn đó phải đợi cho đến khi công việc của ta được in xong thì mới được bắt đầu. Một tùy chọn chính nữa là Print Directly to the Printer, bỏ qua chế độ spooling. Tùy chọn này không hoạt động tốt trong môi trường đa người sử dụng khi nhiều công việc cùng được gửi đến cùng một thiết bị máy in. Tuy nhiên nó hữu ích trong việc gỡ rối các lỗi máy in. Nếu ta có thể in bằng máy in một cách trực tiếp trong khi không thể in qua trình spooler, khi đó ta biết được rằng trình spooler của ta bị ngắt hoặc bị một lỗi khác nào đó, do đó không thể in trong chế độ spooling. Ta cũng sử dụng tùy chọn Print Directly trong các tùy chọn của máy in để in từ DOS.

Các tùy chọn về in ấn

Trong mục Advanced có một hộp chọn gồm bốn tùy chọn cho việc in ấn:

Tùy chọn "*Hold Mismatched Documents*" hữu ích khi ta đang sử dụng nhiều mẫu in cho một máy in. Tính năng này mặc định là tắt và các công việc được in dựa trên cơ sở FIFO. Ví dụ, ta có thể bật tùy chọn này nếu ta cần in trên giấy thuần túy và cả trên những mẫu đã được công nhận. Khi đó tất cả các công việc cùng mẫu in được in trước. Mẫu in sẽ được bàn đến sau một cách chi tiết hơn ở mục quản lý máy dịch vụ in - Managing Print Servers - trong chương này.

Tùy chọn "*Print Spoiled Documents First*" chỉ định trình spooler in các công việc đã qua xếp hàng trước các công việc lớn vẫn đang thực hiện xếp hàng (spooling) ngay cả khi công việc đó có mức ưu tiên cao hơn. Tùy chọn này được thiết lập mặc định để tăng hiệu quả máy in.

Tùy chọn "*Keep Printed Documents*" chỉ định là các công việc không bị xóa đi khỏi trình spooler phục vụ in (không xóa khỏi hàng đợi) khi chúng đã được in xong. Ta thường muốn xóa các công việc khi chúng được in xong vì việc lưu trữ trong hàng đợi sẽ làm tốn bộ nhớ. Do đó mặc định, tùy chọn này không được thiết lập.

Tùy chọn "*Enable Advanced Printing Features*" chỉ định rằng bắt kì một tính năng nào máy in hỗ trợ như Page Order hay Pages Per Sheet, sẽ được thiết lập. Mặc định, tùy chọn này được thiết lập. Ta nên tắt tùy chọn này nếu gặp các lỗi về tương thích. Ví dụ, nếu ta đang sử dụng một thiết bị máy in cùng loại nhưng không hỗ trợ tắt

cả các tính năng như máy in có trình điều khiển đang cài đặt, khi đó ta nên tắt các tính năng in cao cấp.

Chú ý: Bật tùy chọn Keep Printed Documents có thể sẽ hữu ích nếu ta cần nhận dạng tài liệu nguồn hay các thuộc tính khác của công việc đã được in. Ví dụ, tùy chọn này sẽ giúp cho việc theo dõi kiểm tra người nào đã gửi bản in nội dung xấu đến cho đồng nghiệp. Những nhân viên biết rằng bản in đó đang được in trên một máy in laser của công ty. Do hàng đợi của máy in nằm trên một đĩa NTFS, người quản trị thiết lập chế độ Keep Printed Documents và do đó có thể xác định người phạm lỗi thông qua các thuộc tính về người có file đó.

Mặc định in ấn

Nút "Printing Default" ở góc trái bên dưới của mục Advanced trong hộp thoại Printer Properties là để mở hộp thoại Printing Preferences (xem trong hình 6.13 ở phần trước của chương). Hộp thoại này cũng chính là hộp thoại hiện ra khi ta ấn nút Printing Preferences trong mục General của hộp thoại đặc tính máy in, và các tùy chọn của nó được mô tả trong phần "Configuring General Properties" được nói phía trên.

Bộ xử lý in (Print Processor)

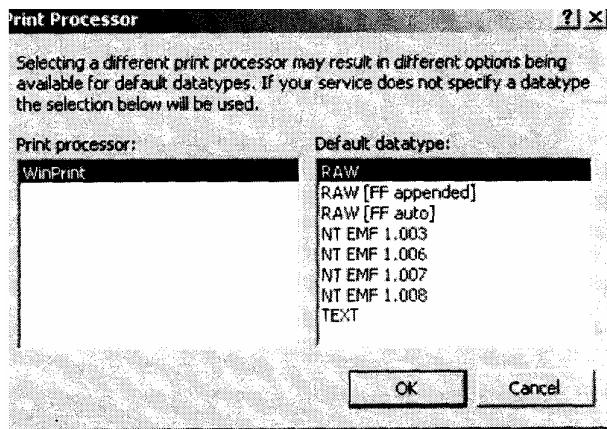
Các bộ xử lý in được sử dụng để xác định Windows 2000 Server có cần các xử lý thêm để in hay không. Năm bộ xử lý in được Windows 2000 Server hỗ trợ được liệt kê trong bảng 6.1:

Bảng 6.1 Các bộ xử lý in được Windows 2000 Server hỗ trợ

Bộ xử lý	Mô tả
RAW	Không thay tài liệu in.
RAW (FF Appended)	Không thay tài liệu in trừ việc luôn thêm kí tự lệnh cưỡng bức máy in đẩy trang hiện hành ra và bắt đầu một trang mới.
RAW (FF Auto)	Không thay đổi tài liệu in trừ việc luôn cố gắng dò tìm liệu có cần thêm kí tự lệnh cưỡng bức máy in đẩy trang hiện hành ra và bắt đầu một trang mới hay không.
NT EMF	Xử lý spool thông thường đối với các tài liệu in được gửi từ các máy khách sử dụng Windows 2000.
TEXT	Thông dịch tất cả dữ liệu thành dạng "plain text" - văn bản thuần túy, và máy in sẽ in dữ liệu bằng cách sử dụng các câu lệnh text chuẩn.

Để thay đổi các thiết lập về bộ xử lí in, nhấp chuột vào nút Print Processor ở cuối mục Advanced để mở hộp thoại Print Processor như trong hình 6.21. Ta có thể chọn thiết lập mặc định trong hộp thoại này, hoặc theo hướng dẫn của nhà sản xuất thiết bị máy in.

Hình 6.21 Hộp thoại Print Processor

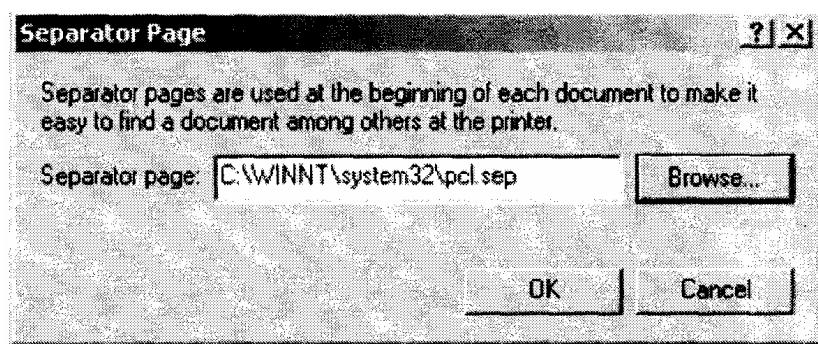


Trang phân tách (Separator Pages)

Trang phân tách được sử dụng ở đầu mỗi tài liệu để xác định người sử dụng đã đưa ra in. Nếu máy in của ta không được chia sẻ, trang phân tách thường là tờ giấy bỏ đi. Nếu máy in của ta được chia sẻ cho nhiều người sử dụng, trang phân tách sẽ rất hữu ích cho việc phát lại các bản đã in về cho người chủ cần chúng.

Để thêm một trang phân tách, nhấp chuột vào nút Separator Page ở góc phải dưới của mục Advanced trong hộp thoại Printer Properties. Hộp thoại Separator Page sẽ hiện lên như trong hình 6.22. Nhấp chuột vào phím Browse để xác định và chọn tệp trang phân tách mà ta muốn sử dụng. Windows 2000 Server cung cấp các tệp trang phân tách được liệt kê trong bảng 6.2, những tệp này được lưu trữ ở thư mục \Windir\system32.

Hình 6.22: Hộp thoại Separator Page



Bảng 6.2 Các tập tin trang phân tách

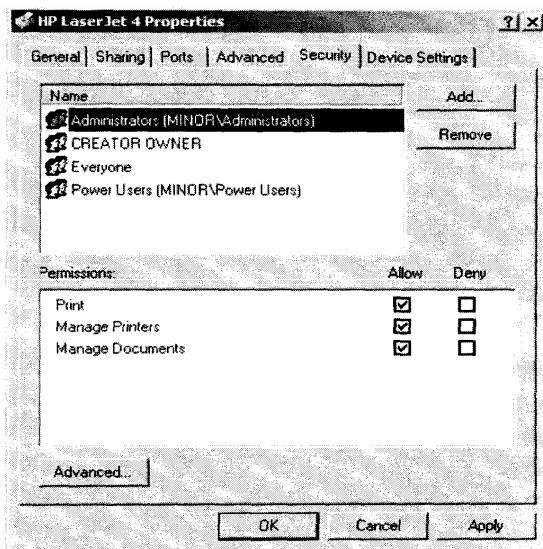
Tập tin	Mô tả
pc1.sep	Được sử dụng để gửi một trang phân tách đến máy in ngôn ngữ kép HP sau khi chuyển máy in về PCL.(Printer Control Language - ngôn ngữ điều khiển máy in) một chuẩn thông dụng của máy in.
pscript.sep	Không gửi trang phân tách nhưng chuyển sang chế độ in Postscript.
sysprint.sep	Được sử dụng bởi máy in ở chế độ Postscript để gửi trang phân tách.
sysprintj .sep	Giống như sysprint.sep nhưng hỗ trợ kí tự tiếng Nhật.

Đặc tính bảo mật

Ta có thể kiểm soát những người dùng nào hay nhóm người dùng nào có thể truy cập máy in điều khiển bởi Windows 2000 bằng cách thiết lập phân quyền sử dụng máy in. Trong Windows 2000 Server, ta có thể cho phép hoặc từ chối các truy cập vào máy in. Nếu ta từ chối cho truy cập, người sử dụng hoặc nhóm người sử dụng sẽ không có khả năng sử dụng máy in, trừ khi phân quyền của họ hay nhóm sử dụng của họ là cho phép.

Ta đặt phân quyền máy in cho người sử dụng hay nhóm người sử dụng thông qua mục Security trong hộp thoại Printer Properties như trong hình 6.23. Các phân quyền máy in có thể thiết lập được định nghĩa trong bảng 6.3.

Hình 6.23 Mục Security trong hộp thoại Printer Properties



Bảng 6.3 Phân quyền sử dụng máy in

Phân quyền sử dụng máy in	Mô tả
Print	Cho phép một người sử dụng hoặc một nhóm kết nối đến máy in và có thể gửi công việc đến máy in
Manage Printers	Cho phép các điều khiển quản trị đối với máy in. Với quyền hạn này, một người sử dụng hoặc một nhóm người sử dụng có thể tạm dừng, khởi động lại máy in, thay đổi các thiết lập spooling, chia sẻ hay không chia sẻ máy in, thay đổi phân quyền, và quản lý các đặc tính của máy in.
Manage Documents	Cho phép người sử dụng hay nhóm người sử dụng quản lý tài liệu bằng cách tạm dừng, khởi tạo lại, và xóa các tài liệu có trong hàng đợi máy in. Người sử dụng không có khả năng điều khiển trạng thái của máy in.

Mặc định, khi một máy in được tạo, các phân quyền mặc định được thiết lập. Các phân quyền mặc định này thường thích hợp với hầu hết các môi trường mạng. Bảng 6.4 cho ta thấy các phân quyền mặc định.

Bảng 6.4 Phân quyền in mặc định

Nhóm	Print	Manager Prints	Manage Documents
Administrators	✓	✓	✓
Power Users	✓	✓	✓
Creator Owner			✓
Everyone	✓		

Chỉ định phân quyền máy in

Thông thường ta có thể chấp nhận các phân quyền mặc định, tuy nhiên ta cũng có thể cài thay đổi chúng trong những trường hợp đặc biệt. Ví dụ, nếu công ty của ta mua một máy in mất đắt tiền cho phòng marketing, ta có thể không muốn cho phép các truy cập thông thường vào máy in đó. Trong trường hợp này ta bỏ chọn Allow ứng với nhóm Everyone, thêm nhóm Marketing vào danh sách trong mục Security và thiết lập phân quyền cho phép đối với nhóm này. Để theo phân quyền, thực hiện theo các bước

sau:

1. Trong mục Security ở hộp thoại Printer Properties, nhấp chuột chọn nút Add.
2. Hộp thoại Select Users, Computers or Groups xuất hiện. Nhấp chọn user, computer hoặc group mà ta muốn đặt phân quyền và nhấp chọn nút Add. Sau khi đã xác định tất cả người: sử dụng mà ta muốn thiết lập phân quyền, nhấp chuột chọn OK.
3. Tô sáng user, computer hoặc nhóm và chọn Allow hoặc Deny access cho phân quyền mục Print, Manage Printers, Manage Documents. Nhấp chọn OK khi được hoàn thành việc chỉ định phân quyền.

Để xóa một nhóm đã có khỏi danh sách phân quyền, tô sáng nhóm đó và nhấp chọn nút Remove. Nhóm đó sẽ không còn được liệt kê trong hộp thoại Security và không thể chỉ định phân quyền.

Các thiết lập nâng cao

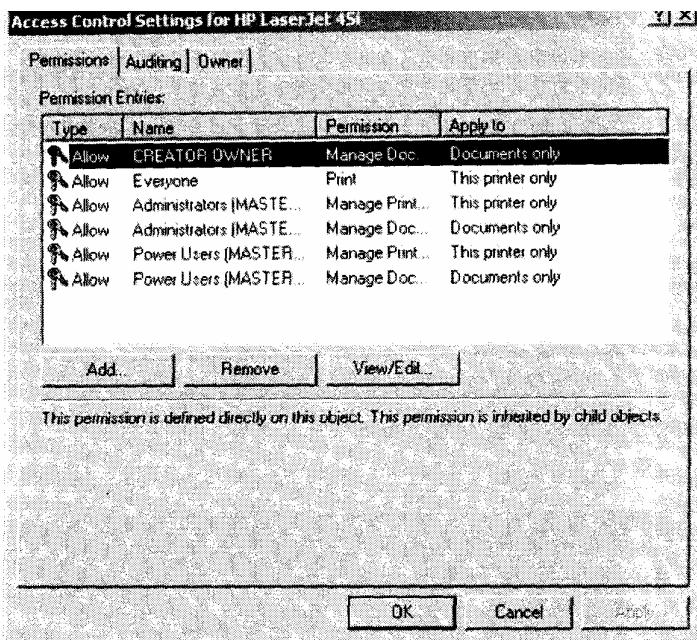
Truy cập vào các thiết lập nâng cao (Advanced Settings) trong mục Security cho phép chỉ định các tính năng phân quyền, kiểm định và chủ sở hữu. Nhấp chọn nút Advanced ở góc dưới bên trái của mục Security, hộp thoại Access Control Settings hiện ra như trong hình 6.24. Hộp thoại này có ba mục để ta có thể sử dụng để thêm, xóa và sửa phân quyền in:

Mục Permission liệt kê tất cả người sử dụng, máy tính và nhóm người sử dụng được phân quyền đối với máy in dù quyền đó là đối với máy in hay đối với tài liệu.

Mục Auditing cho phép ta lưu trữ những theo dõi về đối tượng đang sử dụng máy in và kiểu truy cập đang sử dụng. Ta có thể theo dõi sự kiện thành công hay lỗi của việc in, quản lý in, quản lý tài liệu, quyền đọc, thay đổi quyền hay chiếm quyền sở hữu.

Mục Owner chỉ ra chủ sở hữu của máy in (người sử dụng hay nhóm người sử dụng đã tặc ra máy in), là thuộc tính mà ta có thể thay đổi nếu có quyền. Ví dụ, nếu phân quyền máy in không cho phép Administrator sử dụng hay quản lý máy in, và phân quyền in cần được thiết lập lại. Một người quản trị (Administrator) có thể chiếm quyền sở hữu (ownership) máy in và thiết lập lại phân quyền.

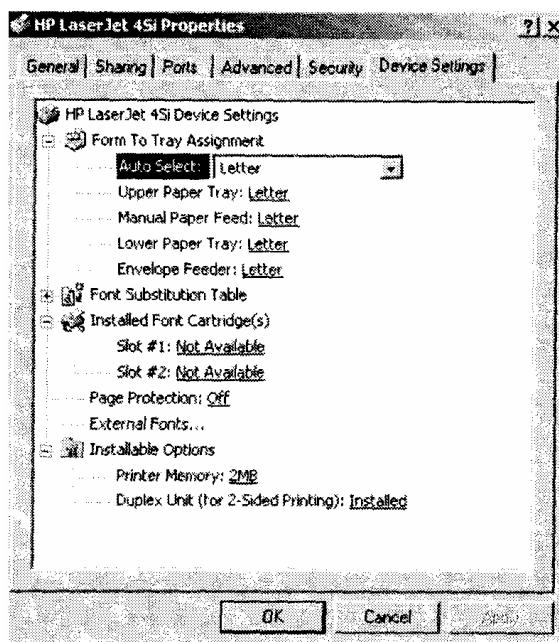
Hình 6.24 Hộp thoại Access Control Settings



Các đặc tính về thiết lập thiết bị (Device Settings Properties)

Các đặc tính có thể nhìn thấy trong mục Device Settings của hộp thoại Printer Properties phụ thuộc vào máy in và trình điều khiển máy in mà ta cài đặt. Ta có thể định cấu hình các tính năng này nếu ta muốn quản lý các mẫu liên quan đến các khay giấy. Ví dụ, ta có thể cấu hình khay trên dùng để in phần đầu trang và khay dưới để in các trang bình thường. Một ví dụ của mục Device Settings cho máy in HP Laserjet 4Si được cho trong hình 6.25 ở dưới.

Hình 6.25 Mục Device Settings trong hộp thoại Printer Properties



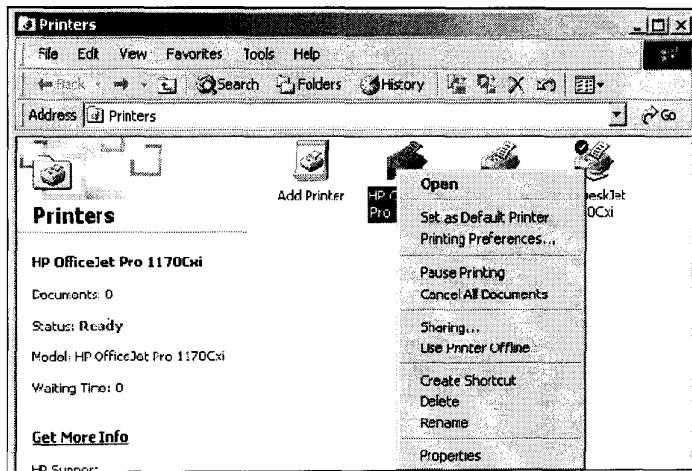
3. Quản lí máy in và tài liệu in

Các nhà quản trị hoặc người sử dụng có quyền quản lí máy in (Manage Printers permission) có thể quản lí dịch vụ máy in và tài liệu in trong hàng đợi máy in. Khi ta quản lí tài liệu in có nghĩa là ta quản lí các tài liệu cụ thể.

a) quản lí máy in (Managing Printers)

Để quản lí máy in, nhấp chuột phải chọn máy in mà ta cần quản lí. Từ thanh thực đơn hiện ra như trong hình 6.26, chọn các tùy chọn liên quan đến vấn đề mà ta cần quản lí. Bảng 6.5 miêu tả các tùy chọn này.

Hình 6.26 Các tùy chọn về quản lí máy in



Bảng 6.5 Các tùy chọn quản lí máy in

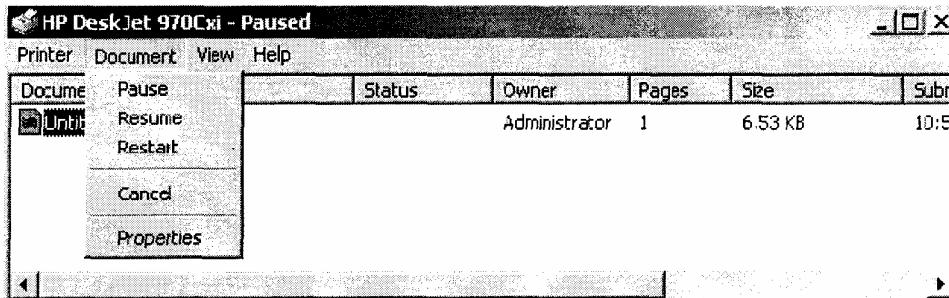
Tùy chọn	Mô tả
Set as Default	Printer Cho phép ta chỉ định máy in mặc định được sử dụng mỗi khi người dùng không gửi tài liệu in đến đích danh một máy in nào (máy tính được cài đặt nhiều máy in).
Printing Preferences	Gọi hộp thoại Printing (xem hình 6.13), cho phép ta cấu hình các thiết lập của máy in về xếp đặt trang hay chất lượng trang in.
Pause Printing	Tạm ngừng việc in. Các công việc in có thể đăng ký với máy in nhưng không được gửi đến thiết bị máy in cho đến khi ta tiếp tục lại việc in (bằng cách bỏ chọn tùy chọn này). Ta có thể sử dụng tùy chọn này khi ta gỡ rời máy in hoặc bảo dưỡng

	máy in.
Cancel All Documents	Chỉ định rằng mọi công việc đang có trong hàng đợi sẽ bị xóa. Ta có thể sử dụng tùy chọn này khi các công việc trong hàng đợi là không cần nữa.
Sharing	Cho phép chia sẻ hay không chia sẻ máy in.
Use Printer Offline	Tạm ngưng máy in. Tài liệu in vẫn còn trong hàng đợi ngay cả khi ta khởi động lại máy.
Delete	Gỡ bỏ máy in. Ta có thể sử dụng tùy chọn này nếu ta không còn cần đến máy in, hoặc nếu ta muốn chuyển máy in đến một máy dịch vụ in khác hoặc khi ta ngờ rằng máy in bị ngắt và cần gỡ bỏ để cài lại.
Rename	Cho phép đặt lại tên máy in. Ta có thể sử dụng tùy chọn này để đặt tên có ý nghĩa hơn cái tên thường.

b) Quản lý tài liệu in

Là một người quản trị hoặc người sử dụng có quyền quản lý máy in hay quản lý tài liệu in, ta có thể quản lý tài liệu in trong hàng đợi phục vụ in. Ví dụ, một người dùng gửi đến một công việc nhiều lần một lúc, khi đó ta cần xóa đi những công việc bị lặp thừa. Để quản lý tài liệu in, trong thư mục Printers nhấp đúp chuột vào máy in chứa các tài liệu đó để mở hộp thoại với các thông tin về tài liệu in trong hàng đợi phục vụ in. Chọn Documents trên thanh thực đơn để mở thực đơn cuộn xuống bao gồm các tùy chọn để quản lý tài liệu in như trong hình 6.27. Những tùy chọn trong thực đơn này được mô tả trong bảng 6.6.

Hình 6.27 Các tùy chọn trong thực đơn Documents



Bảng 6.6 Các tùy chọn quản lý tài liệu in

Tùy chọn	Mô tả
Pause	Đặt tình trạng in của các tài liệu là tạm dừng.
Resume	Cho phép mọi tài liệu tiếp tục in bình thường (sau khi đã tạm dừng)
Restart	Gửi lại công việc in từ đầu ngay cả khi đã in được một phần.
Cancel	Xóa tài liệu in trong trình spooler của máy in.
Properties	Mở hộp thoại Printer Properties, cho phép ta đặt các tùy chọn như khai báo người dùng, ưu tiên tài liệu, thời gian in, xấp đặt trang in và chất lượng trang in.

Quản lý máy dịch vụ in (Managing Print Server)

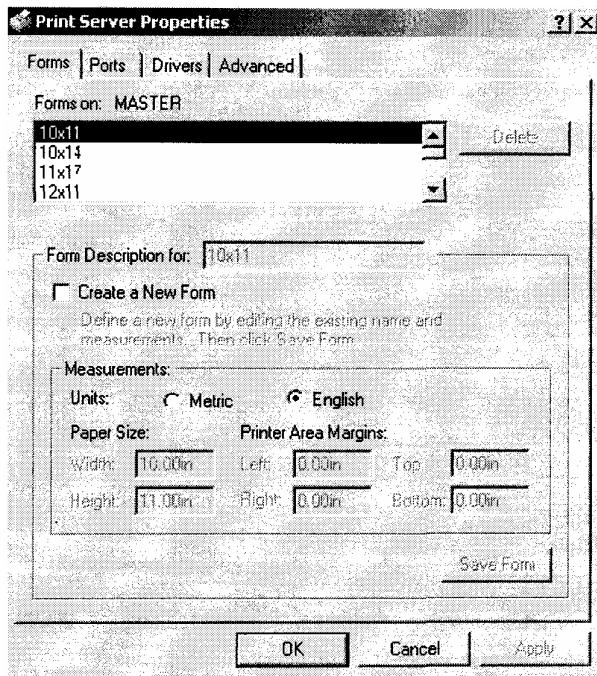
Máy dịch vụ in là máy tính có cài đặt máy in. Khi gửi yêu cầu với máy in mạng, thực tế là ta đã gửi yêu cầu đó tới máy dịch vụ in trước.

Ta có thể kiểm soát máy dịch vụ in bằng cách thiết lập các cấu hình. Để truy nhập tới hộp thoại Print Server Properties, mở thư mục Printers và chọn File/server Properties. Hộp thoại Print Server Properties gồm các mục Forms, Ports, Drivers và Advanced. Các đặc tính trong mỗi mục sẽ được thảo luận sau đây.

Thiết lập cấu hình Form

Nếu máy in của ta hỗ trợ nhiều khay giấy và ta sử dụng các loại giấy khác nhau trong mỗi khay, ta sẽ phải định dạng và chỉ định mỗi dạng ứng với một khay giấy cụ thể. Mục Forms trong hộp thoại Print Server Properties trên hình 6.28 cho phép ta tạo và điều khiển định dạng cho máy in. Có thể định dạng bằng mô tả kích cỡ giấy.

Hình 6.28 Mục Forms trong hộp thoại Print Server Properties



Để thêm định dạng mới hãy thực hiện những bước sau:

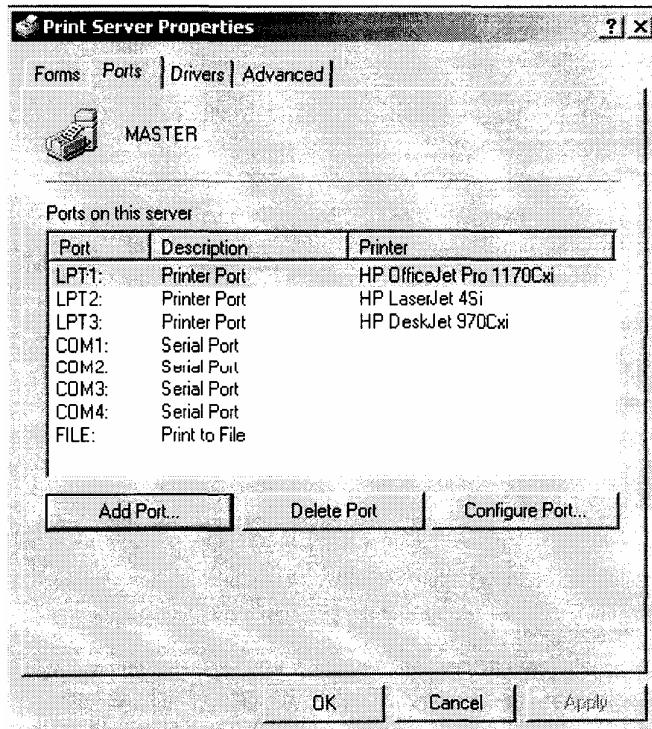
1. Trong mục Forms, chọn Create a New Form.
2. Nhập tên định dạng vào hộp text Form Description For.
3. Chọn các số đo kích thước trong phần Measurements của hộp thoại.
4. Nhấp chuột vào nút Save Form.

Ta phải kết hợp một định dạng với từng khay máy in cụ thể thông qua hộp thoại Properties của máy in chứ không phải qua hộp thoại Printer Server Properties. Trong mục Device Settings của hộp thoại Properties của máy in (xem hình 6.25 ở trên), phía dưới Form To Tray Assignment, chọn khay giấy. Sau đó chọn định dạng sẽ sử dụng với khay giấy trong danh sách kéo xuống.

Thiết lập cấu hình các đặc tính của cổng máy in (Print Server Port)

Mục Ports trong hộp thoại Printer Server Properties, như hình 6.29, tương tự mục Ports trong hộp thoại Properties của máy in. Các đặc tính có thể sửa được mô tả trong phần "Configuring Port Properties" đã thảo luận ở trên trong chương này. Điểm khác nhau giữa hai mục Ports là mục Ports trong hộp thoại Print Server Properties được dùng để kiểm soát mọi cổng trên máy dịch vụ in chứ không phải chỉ những cổng dành cho thiết bị in.

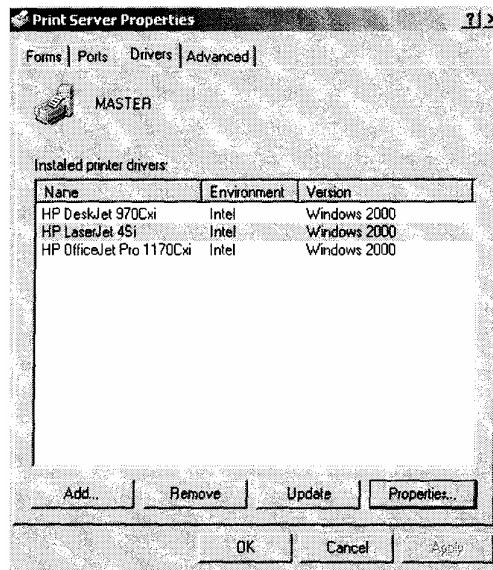
Hình 6.29 Mục Ports trong hộp thoại Print Server Properties



Thiết lập các đặc tính của trình điều khiển (Driver Properties)

Mục Drivers trong hộp thoại Print Server Properties, như hình 6.30, cho phép điều khiển các bộ điều khiển máy in được cài trên máy dịch vụ in. Với mỗi bộ điều khiển máy in, trên mục Drivers sẽ hiển thị tên, môi trường viết bộ điều khiển (như Intel hay Alpha) và hệ điều hành mà bộ điều khiển đó hỗ trợ.

Hình 6.30 Mục Drivers trong hộp thoại Print Server Properties



Thông qua mục Drivers, ta có thể thêm, xóa và cập nhật các trình điều khiển máy in. Để xem đặc tính của một trình điều khiển, chọn vào trình điều khiển tương ứng và

nhấn chuột vào nút Properties. Các đặc tính của trình điều khiển máy in bao gồm:

- ✓ Tên (Name).
- ✓ Phiên bản (Version).
- ✓ Môi trường (Environment).
- ✓ Ngôn ngữ điều khiển (Language monitor).
- ✓ Kiểu dữ liệu ngầm định (Default dâm type).
- ✓ Đường dẫn tới trình điều khiển (Driver trình).

Thiết lập các tính năng nâng cao

Mục Advanced trong hộp thoại Print Server Properties, như hình 6.31, cho phép ta thiết lập cấu hình tập tin spool, spooler event logging và các thông báo về tài liệu từ xa. Ta có thể đặt lựa chọn như sau:

- ✓ Tập tin Spool, trên ổ đĩa cứng, là nơi lưu giữ thông tin các file in ẩn chờ được phục vụ (ngầm định thư mục này được lưu giữ trên thư mục \Windir\system32\spool\printers).
- ✓ Các sự kiện báo lỗi, cảnh báo hay thông tin đều được lưu lại trong Event Viewer.
- ✓ Máy dịch vụ in sẽ luôn phát ra tiếng kêu nếu các tài liệu in từ xa bị lỗi.
- ✓ Thông báo được gửi về máy dịch vụ khi tài liệu đã được in.
- ✓ Máy tính người dùng được thông báo khi có tài liệu được in.

CHƯƠNG 7. QUẢN LÝ DỊCH VỤ MẠNG

Windows 2000 Server xuất hiện kèm theo IIS (Internet Information Services - Các thông tin dịch vụ về Internet) cho phép ta thiết lập và quản lý trang Web. Phần mềm này cung cấp một diện rộng các tùy chọn để định hình nội dung, quá trình thực hiện và điều khiển sự truy nhập cho trang Web của ta.

Trong chương này, ta sẽ học cách làm thế nào để cài đặt IIS (nếu như nó không được cài đặt trong bộ cài Windows 2000 Server nguyên bản) và làm thế nào để định hình và quản lý các thuộc tính trong trang Web. Ta cũng sẽ học làm thế nào để tạo ra một trang Web. Và phần cuối của chương này bao gồm những lời khuyên để gỡ rối các vấn đề khi truy nhập trang Web.

1. Cài đặt Internet Information Services

Windows 2000 Server sử dụng Internet Information Services (IIS) để khai thác các tài nguyên trên Internet hoặc trên một mạng intranet riêng nào đó. IIS cũng cung cấp đầy đủ các tính năng cho các máy chủ Web, nó được thiết kế để hỗ trợ sử dụng Internet một cách thuận tiện. Phần mềm IIS được cài đặt trong Windows 2000 Server một cách mặc định. Nếu ta chọn không cài IIS trong quá trình cài Windows 2000 Server, hoặc ta nâng cấp lên Windows 2000 Server từ máy tính không chạy IIS, ta có thể dễ dàng cài IIS qua các bước sau :

1. Chọn Start -> Setting -> Control Panel và kích đúp chuột vào biểu tượng Add/Remove Programs.

2. Cửa sổ Add/Remove Programs xuất hiện. Kích chuột vào lựa chọn Add-/Remove Windows Components.

3. Cửa sổ Windows Components Wizard xuất hiện. Đánh dấu chọn vào Internet Information Service (IIS) và kích chuột vào nút Next.

4. Khi có lời nhắc, hãy đưa đĩa CD Windows 2000 Server vào ổ CD và kích chuột vào nút OK. Nếu ta nhìn thấy yêu cầu các file cần thiết trong hộp thoại, ta sẽ cần phải định vị rõ đường dẫn tới CD của ta (có thể sử dụng nút Browse) và thư mục I386. Tiếp theo ta cần OK.

5. Sau khi tất cả các file đã được copy, ta sẽ nhìn thấy cửa sổ hoàn thành của Windows Components Wizard. Kích chuột vào nút Finish.

6. Đóng cửa sổ Add/Remove Programs.

2. Cấu hình và quản lý IIS (Internet Information Services)

Khi IIS đã được cài, ta sẽ nhìn thấy mục chương trình Internet Services Manager trong Administrator Tools. Đây là tiện ích chính được sử dụng để quản lý IIS.

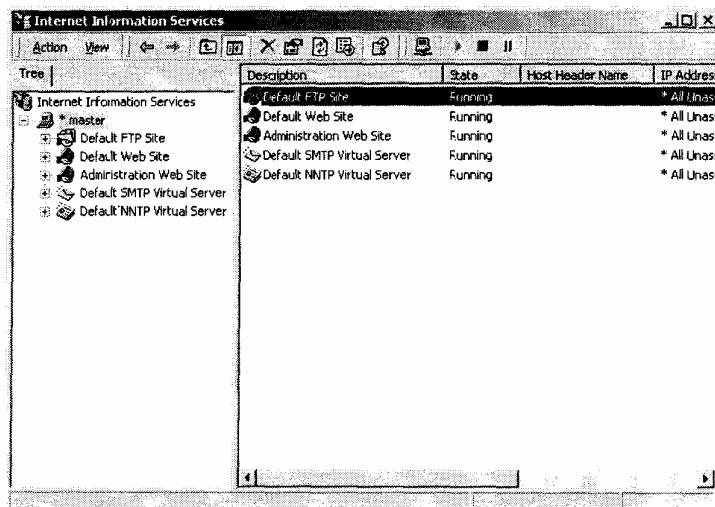
Các dịch vụ đã được cài đặt như là một phần của IIS :

- ✓ *Giao thức truyền File (File Transfer Protocol - FTP)*, nó được sử dụng để truyền các file giữa 2 máy tính dùng giao thức TCP/IP.
- ✓ *Giao thức truyền siêu văn bản (Hypertext Transfer Protocol - HTTP)*, nó được sử dụng để tạo ra nội dung các trang Web cũng như định hướng cho trang Web đó.
- ✓ *Giao thức truyền thư đơn giản (Simple Mail Transfer Protocol- SMTP)*, nó được sử dụng để truyền thư giữa 2 hệ thống thư SMTP.
- ✓ *Giao thức truyền tin trên mạng(Network News Transfer Protocol - NNTP)*, nó được sử dụng để cung cấp các nhóm dịch vụ giữa máy chủ NNTP và máy khách NNTP.

2.1 Quản lý một trang Web

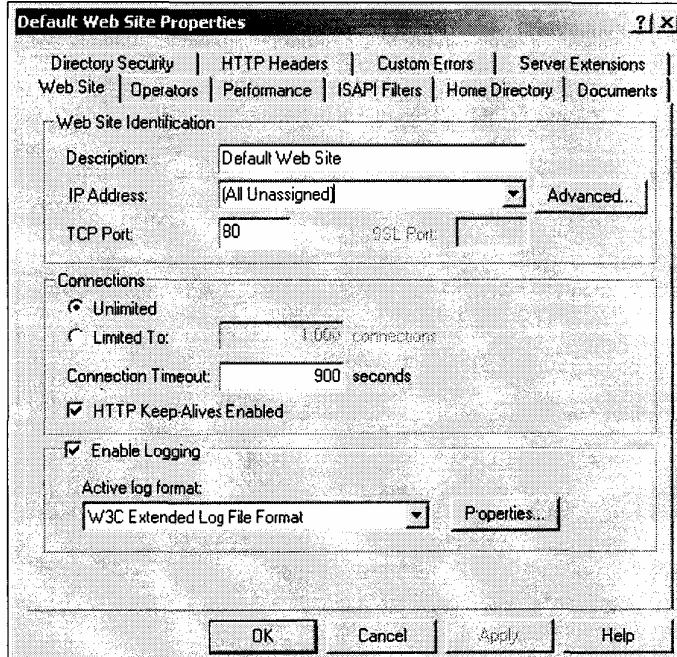
Để truy nhập Internet Services Manager (Quản lý các dịch vụ trên Internet), chọn Start -> Programs -> Administrative Tools -> Internet Services Manager. Một cửa sổ xuất hiện như trong hình 7.1 Khi ta bắt đầu vào Internet Services Manager, ta sẽ nhìn thấy 5 mục được định nghĩa là mặc định: Default FTP Site, Default Web Site, Administrator Web Site, Default SMTP Virtual Server và Default NNTP Virtual Server. Các trang mặc định và các máy chủ ảo mặc định được cung cấp để giúp ta xây dựng IIS và chạy càng nhanh càng tốt.

Hình 7.1 Cửa sổ Internet Information Services :



Qua Internet Services Manager ta có thể định hình nhiều tùy chọn cho trang Web của ta, ví dụ như số người được phép truy kết vào, các thiết đặt để thực hiện và các điều khiển truy nhập. Để truy nhập các thuộc tính của một trang Web, hãy nhấp chuột phải vào trang Web mà ta muốn quản lý trên cửa sổ Internet Information Services và chọn Properties từ menu đồ xuống. Hộp thoại thuộc tính của trang Web được đưa lên như sự trình bày trong hình 7.2.

Hình 7.2 Hộp thoại Default Web Site Properties



Hộp thoại Web Site Properties gồm 10 thẻ với các tuỳ chọn để định hình và quản lý trang Web của ta. Các tuỳ chọn trên các bảng này được miêu tả tóm tắt trong bảng 7.1 và chi tiết hơn trong các mục tiếp theo.

Bảng 7.1. Các thẻ trong hộp thoại Web Site Properties

Bảng	Miêu tả
Website	Cho phép ta định hình nhận diện, các kết nối và đăng nhập cho trang Web
Operators	Cho phép ta định nghĩa những người dùng nào hay những nhóm nào có thể quản lý Trang Web.
Performance	Cho phép ta định hình sự điều chỉnh chỉ tiêu, điều khiển bằng thông, điều khiển quá trình xử lý.
ISAPI Filters	Cho phép ta thiết lập ISAPI(Giao diện lập trình ứng dụng máy chủ trên Internet)
Home Directory	Cho phép ta định vị nội dung, quyền truy nhập, các nội dung điều khiển và cài đặt các tiện ích.
Documents	Cho phép ta chỉ rõ cho người dùng những tài liệu mặc định sẽ hiển thị nếu truy nhập vào trang Web mà không chỉ rõ một tài

	liệu.
Directory Security	Cho phép ta thiết lập điều khiển truy nhập, chứng thực giấu tên, hạn chế tên địa chỉ, miền IP và truyền thông an toàn.
HTTP Headers	Cho phép ta thiết lập các giá trị mà sẽ được trả về cho trình duyệt Web trong những đầu mục ngôn ngữ siêu văn bản (html) của trang Web.
Custom Errors	Cho phép ta trình diễn một thông báo lỗi tùy biến mà sẽ xuất hiện khi có một lỗi trong chương trình duyệt Web.
Server Extensions	Cho phép ta định hình các điều khiển xuất bản cho các tùy chọn Frontpage

Thiết lập các thuộc tính cho trang Web.

Bảng Web site (nhìn hình 7.2) bao gồm các tùy chọn cho việc nhận diện trang Web, điều khiển kết nối, và cho phép đăng nhập.

Nhận diện trang Web.

Sự xuất hiện của trang Web được mô tả trong cửa sổ Internet Information Services. Theo mặc định thì sự mô tả trang Web giống như là tên của trang Web. Ta có thể nhập một mô tả khác trong hộp thoại mô tả.

Ta cũng có thể định hình địa chỉ IP mà có liên hệ với các trang. Địa chỉ IP phải được định hình sẵn cho máy tính. Nếu ta bỏ đi địa chỉ IP ở địa chỉ mặc định là All Unassigned, thì tất cả các địa chỉ IP mà được gán vào máy và chưa được gán cho các trang Web khác sẽ được sử dụng.

Các cổng TCP được chỉ định sẽ được sử dụng để trả lời tới các đòi hỏi HTTP theo mặc định. Cổng mặc định của TCP được sử dụng là cổng 80. Nếu ta thay đổi giá trị này, các máy khách muốn kết nối vào Internet phải xác định lại giá trị chính xác của cổng này. Lựa chọn này có thể sử dụng để tăng thêm tính bảo mật.

Các kết nối

Ta có thể cho phép một số lượng không giới hạn các kết nối tới trang Web, hoặc là điều khiển số lượng các kết nối. Để chỉ định giới hạn các kết nối hãy chọn Limited To, và nhập vào số lượng tối đa các kết nối cho phép.

Mục Connection Timeout cho phép ta chỉ định thời lượng người dùng không hoạt động có thể trả lại trang Web được nữa sau khi kết nối tự động kết thúc.

Nếu ta chọn HTTP Keep-Alives Enabled, thì máy khách sẽ được duy trì một kết nối cùng với máy chủ, ngược với mở một kết nối mà khách hàng đòi hỏi. Điều này làm

tăng sự thực hiện của máy khách và có thể làm giảm sự thực hiện của máy chủ.

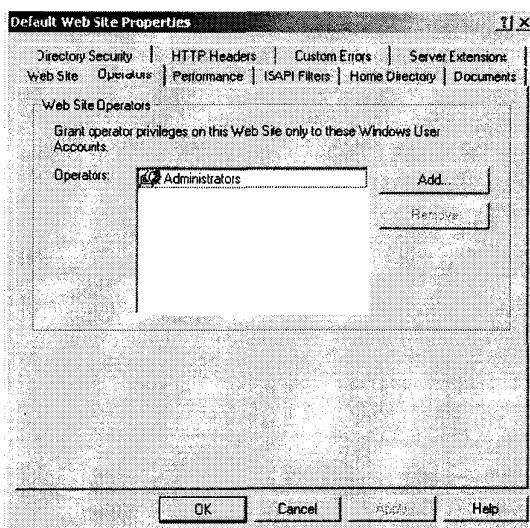
Đăng nhập

Đăng nhập được sử dụng để thiết lập các đặc trưng, các bản ghi chi tiết của trang Web truy nhập. Nếu đăng kí được chọn, ta có thể chọn từ một vài các định sẵn đăng nhập đã được tập hợp trong một khuôn mẫu định sẵn. Nếu ta muốn để cho một người dùng truy cập vào trang Web, hộp chọn Loa Visits trên bảng Home Directory phải được đánh dấu (giá trị cài đặt mặc định).

Định rõ các thao tác

Ta có thể định nghĩa những người dùng nào hay các nhóm nào có thể quản lý trang web qua tao Operators, như hình 7.3. Theo mặc định thì nhóm Administrators có quyền thao tác. Ta có thể thêm hoặc bỏ các nhóm thao tác từ bảng chọn.

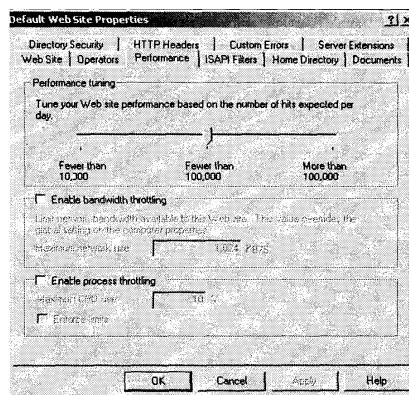
Hình 7.3 tab Operator trong hộp thoại Web Site Properties



Cài đặt các tùy chọn thực thi.

Tab Performance, hình 7.4, cho phép ta thiết lập các thực thi, cho phép điều chỉnh dải thông, và điều chỉnh sự xử lý.

Hình 7.4 Tab Performance của hộp thoại Web Site Properties



Bộ điều chỉnh sự thực thi :

Bộ chỉnh sự thực thi cho phép ta để trang web của ta dựa trên số lượng các tác động trên mạng tới trang web của ta mỗi ngày. Dựa trên con số được ta chỉ định, bộ nhớ máy chủ sẽ cố định số lượng tối đa các truy cập. Tuỳ chọn này cho phép ta định nghĩa các truy nhập vào mỗi ngày có thể ít hơn 10000, ít hơn 100000 (giá trị cài đặt mặc định), hoặc nhiều hơn 100000.

Bộ điều chỉnh dải thông

Dải thông được định nghĩa như tổng khả năng truyền thông. Đơn vị của nó có thể là số lượng các bít trong 1 giây (bps) hoặc tần suất (Hertz). IIS cho phép ta có thể định nghĩa dải thông được dùng trong giới hạn bao nhiêu kilobyte trên giây. (KB/s).

Nếu máy chủ được sử dụng để quản lý các trang web hoặc được sử dụng vì mục đích khác, như gửi thư điện tử, hoặc muốn giới hạn toàn bộ băng thông được sử dụng bởi trang Web chủ. Điều này được gọi là bộ điều chỉnh dải thông (bandwidth throttling). Nếu bộ điều chỉnh dải thông không được bật, trang Web chủ có thể sử dụng tối đa lượng băng thông đang còn rỗi.

Bộ điều chỉnh sự xử lý

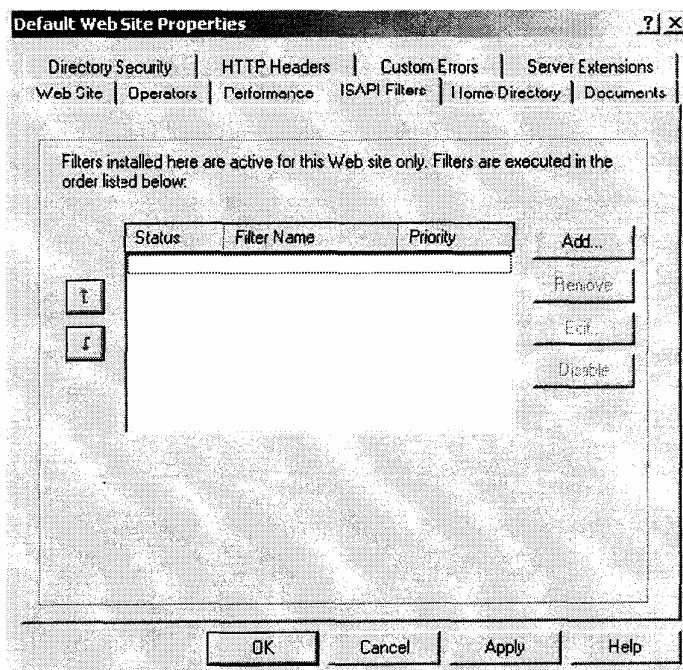
Khi ta bật *process throttling*, ta có thể chỉ rõ số phần trăm CPU xử lý được phục vụ cho trang Web. Nếu ta chọn Enforce Limits, thì bất kì giá trị nào ta đặt cho process throttling sẽ được bắt buộc. Nếu lựa chọn này không được đánh dấu, thì trang Web có thể sử dụng vượt quá cài đặt giới hạn xử lý và một sự kiện sẽ được ghi vào bản ghi sự kiện.

Cài đặt: ISAPI Filters

Bộ lọc Giao diện lập trình ứng dụng trình chủ Internet (ISAPI) điều chỉnh các yêu cầu bộ duyệt mạng cho URLs chuyển qua ứng dụng ISAPI, khi đã chạy, bộ lọc ISAPI được sử dụng để quản lý sự chứng thực đăng nhập tùy biến. Những lọc này làm việc dựa trên các yêu cầu HTTP và các đáp ứng tới các sự kiện chỉ định mà được định nghĩa qua bộ lọc. Bộ lọc được tải đưa vào trong bộ nhớ của trang Web.

Qua bảng ISAPI, trong hình 7.5, ta có thể thêm bộ lọc ISAPI cho trang Web của ta. Các bộ lọc được liệt kê trong một danh sách. Ta có thể sử dụng mũi tên lên hoặc xuống để thay đổi thứ tự của các bộ lọc.

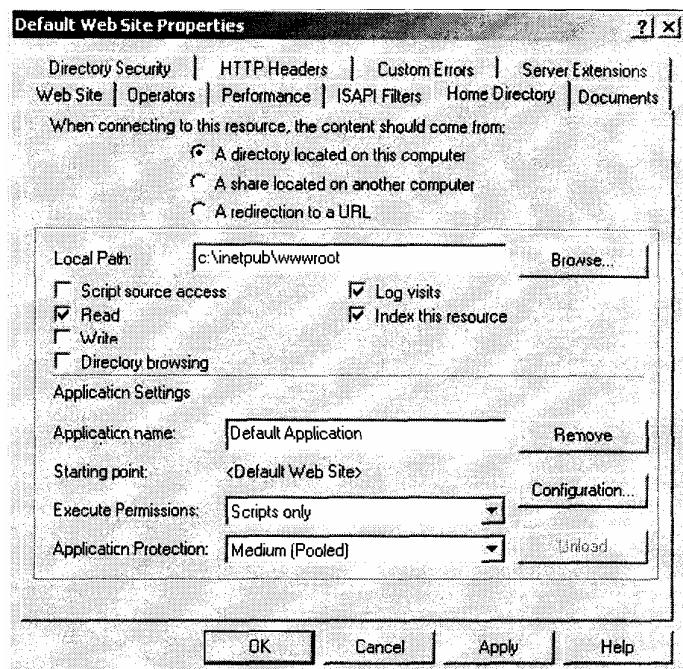
Hình 7.5 Tab ISAPI Filters của hộp thoại Web Site Properties



Định hình lựa chọn thư mục chủ

Thẻ Home Directory, hình 7.6, bao gồm các chọn lựa cho vị trí nội dung, quyền truy nhập, điều khiển nội dung, và các cài đặt ứng dụng.

Hình 7.6 Bảng Home Directory của hộp thoại Web Site Properties



Vị trí của nội dung

Thư mục chủ được dùng để cung cấp nội dung trang Web. Thư mục mặc định có tên là `inetpub\wwwroot`. Ta có ba lựa chọn đặt vị trí thư mục chủ:

- ✓ Một thư mục trên máy tính địa phương của ta.
- ✓ Một thư mục được chia sẻ trên máy tính khác (được lưu trữ trên mạng cục bộ và đặc nhận biết bằng một tên UNC).
- ✓ Một địa chỉ mới tới một tài nguyên sử dụng một URL.

Quyền truy xuất và quản lý nội dung

Quyền truy xuất cho phép xác định những quyền truy nhập Web của người dùng. Quản lý nội dung quy định trang Web có khả năng *ghi lại* và *đánh chỉ số* về mỗi lần truy cập của người dùng. Về mặc định, người sử dụng có quyền đọc, được ghi lại mỗi lần truy cập và đánh chỉ số. Các quyền truy xuất và quản lý nội dung được mô tả dưới bảng 7.2 như sau:

Bảng 7.2 Quyền truy xuất và Lựa chọn quản lý nội dung

Lựa chọn	Mô tả
Scrip Source Access	Cho phép người sử dụng truy cập vào từng đoạn mã kịch bản giống như ứng dụng ASP, nếu như người sử dụng có quyền đọc và ghi thông tin
Read	Quyền này cho phép người sử dụng có khả năng đọc hoặc tải những file được đặt trong thư mục Home. Quyền này thường được cấp phát khi trong thư mục Home của ta có chứa những file HTML, còn nếu như ta có chứa những ứng dụng CGI hoặc là ISAPI ta không nên lựa chọn chức năng này để ngăn cản người dùng có thể tải về những file ứng dụng của ta.
Write	Quyền này cho phép người sử dụng có thể thay đổi hoặc thêm nội dung vào trang web. Quyền truy xuất này cần phải được cân nhắc cẩn thận.
Directory Browsing	Cho phép người sử dụng biết được thư mục trang Web. Lựa chọn này thường không được dùng phổ biến vì nó để lộ ra cấu trúc thư mục tới người dùng.
Log Visits	Cho phép ta ghi lại mỗi lần truy cập vào trang web, để thực hiện được chức năng này ta phải đánh dấu vào chức năng chọn

Index This Resource	Enable Logging trong tập Web Súc của trang thuộc tính. Cho phép ta đánh chỉ số vào thư mục Home bằng sử dụng dịch vụ Microsoft Indexing Service.
---------------------	---

Quyền truy xuất dịch vụ Web và quyền truy xuất trên hệ thống NTFS hoạt động cùng nhau. Thiết lập quyền càng nghiêm ngặt trên 2 hệ thống thì hoạt động của hệ thống càng hiệu quả.

Thiết lập cho ứng dụng

Ứng dụng được nói đến ở đây được xác định liên quan một thư mục quy định cụ thể có chứa ứng dụng (và các thư mục con của nó và các file) mà được coi như là một ứng dụng. Thí dụ như nếu ta chỉ định một thư mục chủ của ta là một ứng dụng thì mọi thư mục con nằm trong nó đều có liên quan đến ứng dụng của ta.

Thiết lập Execute Permission chỉ định cách mà ứng dụng có thể được truy xuất trong thư mục. Nếu ta chọn None, không có ứng dụng hoặc kịch bản có thể được thực thi từ thư mục này. Thiết lập Script Only cho phép chạy đoạn mã kịch bản mặc dù không có quyền thực thi nào được thiết lập. Quyền này thường được dùng cho những thư mục chứa đoạn mã kịch bản ASP. Các lựa chọn còn lại là Scripts và Executable, cho phép các kiểu file khác được thực thi (những file nhị phân .EXE và .DLL mở rộng).

Thiết lập Application Protection chỉ định cách mà ứng dụng sẽ được chạy. Có 3 các sự lựa chọn:

Tháp (IIS Process) : có nghĩa rằng ứng dụng chạy đồng thời với tiến trình xử lý của dịch vụ web.

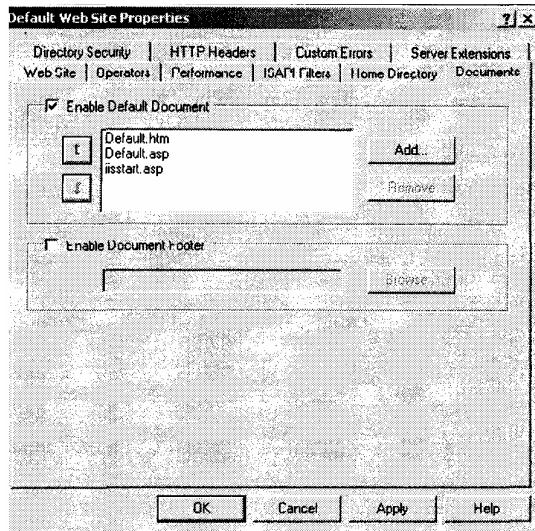
Trung bình (Pooled): ứng dụng chạy với một tiến trình riêng so với các ứng dụng khác.

Cao (Isolated): mỗi ứng dụng chạy giống như một ứng dụng tách biệt.

Thiết lập một tài liệu mặc định

Thẻ Document trong hình 7.7 cho phép ta quy định những tệp mặc định chạy khi truy cập vào trang web mà không gõ tên một tệp nào khác. Thông thường ta phải thiết lập các tệp mặc định này cho thư mục chủ.

Hình 7.7 Thẻ Documents trong hộp thoại Web site Properties

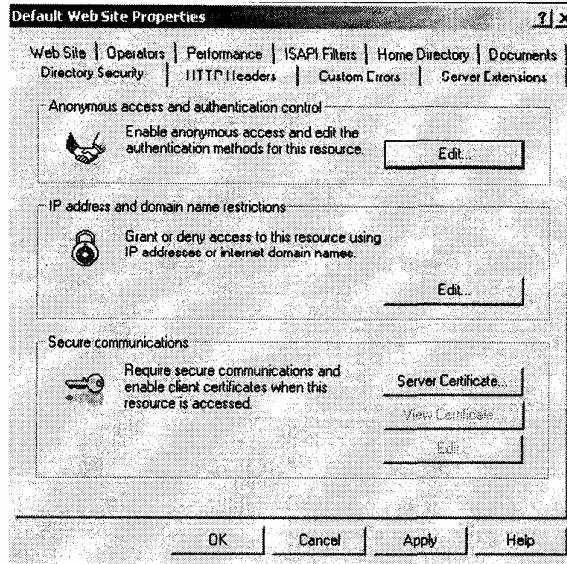


Ta có thẻ quy định có nhiều tệp mặc định trong hộp thoại. Bằng cách này, nếu một tệp nào đó không tồn tại nó sẽ tìm tệp kế tiếp nó. Ta cũng có thể quy định các phần cuối của tài liệu. Một phần cuối tệp là một tệp HTML xuất hiện ở phía cuối trang Web mà được gửi đến các khách.

Thiết Lập Bảo Mật cho Thư Mục

Thẻ Directory Security chỉ ra trong hình 10.8 bao gồm các lựa chọn: Truy cập nặc danh, thẩm định quyền điều khiển, địa chỉ IP và hạn chế tên miền, và siết chặt liên lạc truyền thông.

Hình 7.8 Thẻ Directory Security trong hộp thoại Web site Properties

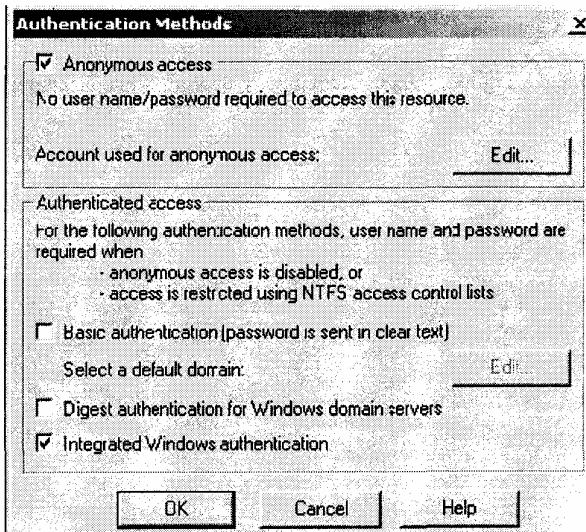


Truy Cập Nặc Danh và Thẩm Định Quyền Điều Khiển

Nhân chuột vào nút Edit trong khung hộp thoại Anonymous Access and Authentication Control để quy định cho phép truy cập nặc danh và thẩm định quyền

điều khiển. Hộp thoại Authentication Methods như hình 7.9 xuất hiện cho ta xác định phương thức

Hình 7.9 Hộp thoại Authentication Methods



Nếu trang Web của ta thuần dành cho tất cả mọi người sử dụng ta nên để chế độ truy cập nặc danh. Nếu để chế độ truy cập nặc danh, mặc định máy tính của ta sẽ dùng tài khoản với tên người sử dụng là *IUSR_computername*. Ta cũng có thể giới hạn số tài khoản truy cập nặc danh bằng việc xác định quyền truy xuất ở hệ thống NTFS trong nội dung trang Web của ta. Có 3 lựa chọn xác định thẩm quyền truy xuất trong hộp thoại Authentication Methods:

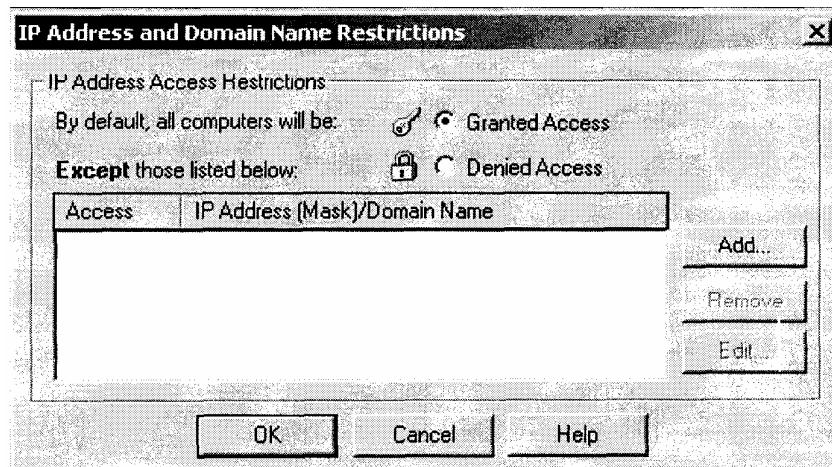
- ✓ Quyền cơ bản (*Basic Authentication*): lựa chọn này đòi hỏi phải có tài khoản sử dụng ở Windows 2000rserver. Nếu bỏ đi quyền truy xuất nặc danh hoặc một tài khoản nặc danh nào đó đang cố truy xuất vào một vùng dữ liệu mà không được cấp phát quyền thì hệ thống Window 2000 server đưa ra thông báo là tài khoản không có giá trị (*tài khoản không tồn tại trong hệ thống*). Với phương pháp này mật khẩu không được gửi đi. Ta nên cân nhắc để lựa chọn phương pháp này khi tính đến sự thiếu an toàn trong vấn đề bảo mật.
- ✓ Phân loại thẩm quyền cho Windows Domain Server: chỉ dùng cho tài khoản domain của Windows 2000. Phương pháp này yêu cầu một tài khoản để lưu trữ *Password*, mã hoá dưới dạng *Clear text*.
- ✓ Tích hợp các quyền của người dùng Window (The *Intergrated Windows Authentication*): lựa chọn này để siết chặt thẩm quyền quy định việc truyền đi tên tài khoản và mật khẩu của người sử dụng.

Giới hạn địa chỉ IP và tên miền

Trong khung hộp thoại địa chỉ IP và tên miền, nhấp chuột lên nút Edit để thiết lập điều khiển việc truy cập lên trang web thông qua địa chỉ IP hoặc tên miền. Hộp thoại

trên hình 7.10 cho phép ta thiết lập cấu hình:

Hình 7.10 Hộp thoại giới hạn địa chỉ IP và tên miền



Trong hộp thoại giới hạn địa chỉ IP và tên miền, ta có thể quy định rằng tất cả các máy tính được công nhận hay bị từ chối truy cập và sau đó quy định ngoại lệ. Những ngoại lệ này có thể phụ thuộc vào những địa chỉ *IP của nó*, địa chỉ *IP của mạng* và địa chỉ *Subnet mask*, hoặc là tên miền (điều này yêu cầu tên miền máy chủ đã có được đặt trước-điều này được mô tả ở chương IX "Quản lý các giao dịch trên mạng").

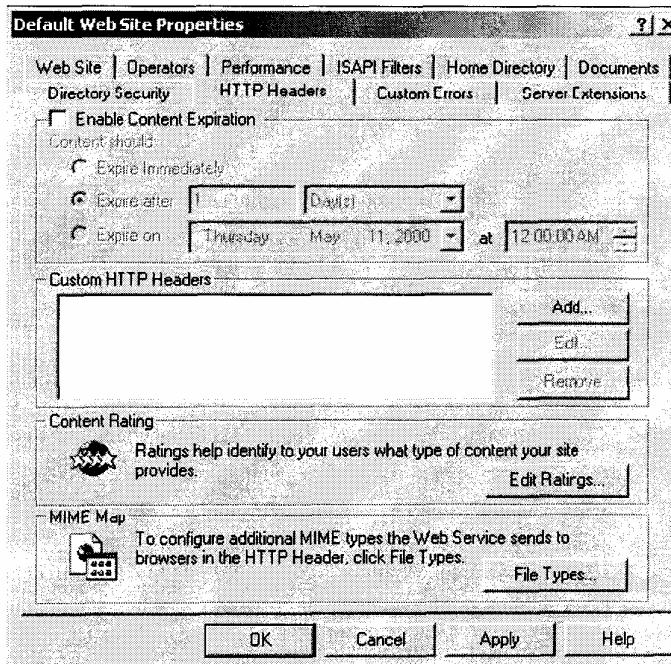
Thiết lập an toàn bảo mật trong truyền thông tin

Ta có thể tăng khả năng bảo mật của trang Web bằng cách thiết lập an toàn bảo mật trong truyền thông tin. Với cách thiết lập này ta có thể tạo ra và quản lý những khóa truy cập và có thể cấp phát chứng nhận những khoá được quyền truy cập. Những lựa chọn này thường được dùng trong sự kết hợp với hệ thống chứng nhận của máy chủ (Certificate Server). Điều này cho phép ta có thể quy định một số chế độ bảo mật thông tin trong việc truy cập trang Web của ta.

Thiết lập HTTP Headers

Thẻ HTTP Headers, trên hình 7.11 cho phép ta thiết lập cấu hình giá trị sẽ trả về trình duyệt Web trong đầu trang HTML của trang Web.

Hình 7.11 Thẻ HTTP Headers trong hộp thoại Web site Properties



Ta có thể cấu hình theo 4 lựa chọn:

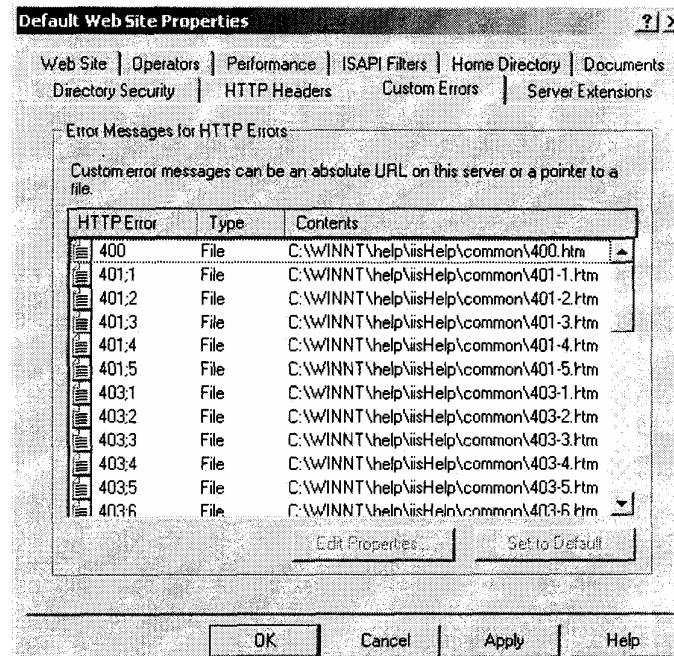
- ✓ Nếu trang Web của ta chứa đựng những thông tin mà cần phải cân nhắc đến vấn đề thời gian, ta có thể quy định khoảng thời gian cho phép trong việc hiển thị nội dung trang Web. Ta có thể quy định thời gian tới hạn theo phút hoặc theo ngày. Điều này giúp trình duyệt xác định liệu rằng nó sẽ dùng một bản sao chép của một trang được yêu cầu hay là nó cần thông tin cập nhật từ trang Web đó.
- ✓ Custom HTTP được dùng để gửi những tùy chỉnh đầu trang HTTP từ phía Web Server về phía trình duyệt máy khách. Thí dụ như ta có thể muốn quy định ở đầu trang HTTP gửi đi mệnh lệnh rằng nó có thể không hỗ trợ kiểu HTML đang sử dụng.
- ✓ Content Rating cho phép ta có thể quy định hạn chế đến những trang có nội dung xấu: *bạo lực tình dục, đồ truy...* Phần lớn các trình duyệt Web có hạn chế truy cập vào những trang có nội dung xấu, điều này phụ thuộc vào nội dung quy định những trang có quyền truy cập.
- ✓ MIME (*Multipurpose Internet Mail Extension*) được dùng để cấu hình cho trình duyệt Web có khả năng nhận biết được những kiểu file theo những định dạng khác nhau..

Chỉ định các thông báo lỗi cho khách hàng

Nếu như trình duyệt Web gặp phải lỗi nó sẽ hiển thị thông báo lỗi. Về mặc định những thông điệp lỗi được định nghĩa trước sẽ được hiển thị. Thông qua thẻ Errors, chỉ ra trong hình 7.12, ta có thể tuỳ chỉnh thông báo lỗi mà người sử dụng sẽ trông thấy.

Ta cũng có thể tạo ra một trang HTML và chỉ định một thông báo lỗi nào đó thay thế cho các lỗi HTML.

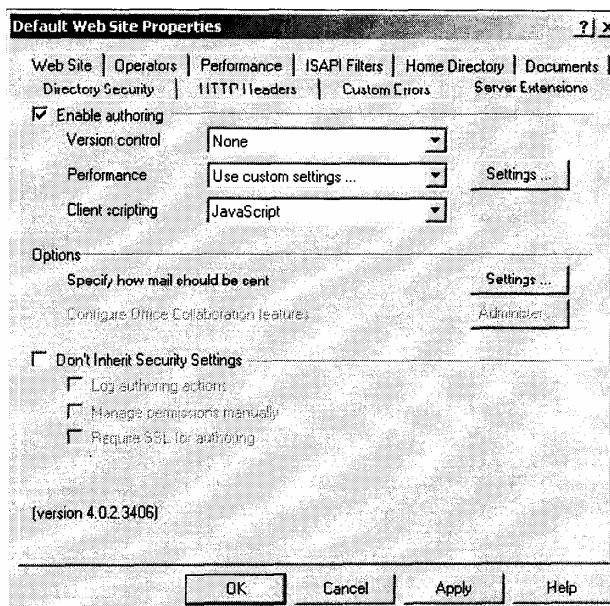
Hình 7.12 Thẻ Custom Errors trong hộp thoại Web site Properties



Thiết lập cấu hình mở rộng cho máy chủ

Thẻ cấu hình mở rộng cho Server, trong hình 7.13, cho phép ta cấu hình các quyền điều khiển xuất bản đối với các lựa chọn của Frontpage. Frontpage được dùng để tạo và chỉnh sửa các trang HTML cho trang Web của ta thông qua trình soạn thảo "Cái ta nhìn thấy là cái ta có được" (WYSIWYG).

Hình 7.13 Thẻ Server Extensions trong hộp thoại Web site Properties



Thẻ này bao gồm những tùy chọn sau:

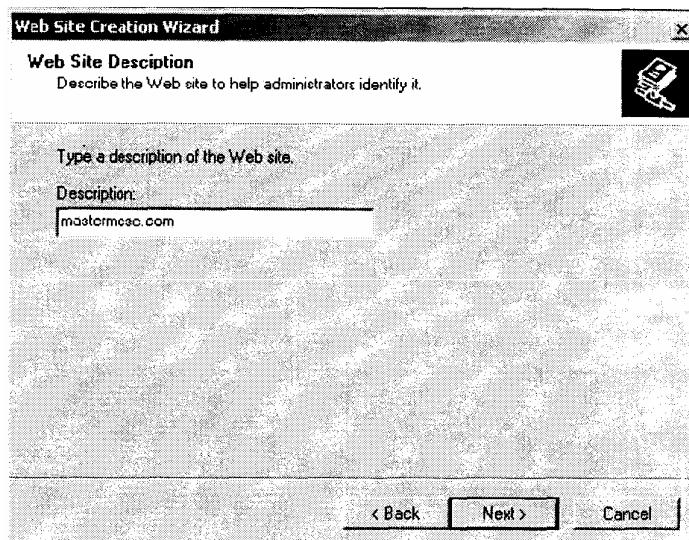
- ✓ Tùy chọn Enable Authoring chỉ định liệu rằng tác giả có thể thay đổi nội dung hiển thị của trang Web. Nếu hộp chọn này được đánh dấu, ta có thể thay đổi được phiên bản, trình diễn được bao nhiêu trang Web từ máy chủ và các phương thức kịch bản được dùng ở các máy trạm.
- ✓ Khung Option: bao gồm 2 phím Setting và Administer, quy định được phép gửi bao nhiêu lá thư (mail) và chức năng kết hợp với công cụ văn phòng (Office Collaboration).
- ✓ Hộp lựa chọn Don't Inherit Security Seuing nếu được lựa chọn sẽ ghi đè lên thiết lập chế độ bảo mật trước đó.

2.2 Tạo một trang Web mới

IIS cho phép ta có nhiều trang Web trên cùng một máy tính đơn. Để tạo ra một trang Web mới ta hãy thực hiện theo các bước sau:

1. Mở IIS.
2. Trong cửa sổ IIS, kích chuột phải lên máy tính chạy IIS và chọn New-web site trong menu pop-up.
3. Kích lên phím Next trong hộp thoại Welcome to the Web Site Creation Wizard.
4. Hộp thoại Web Site Description xuất hiện như trong hình 7.14. Đánh vào tên mô tả của trang Web và kích lên phím Next.

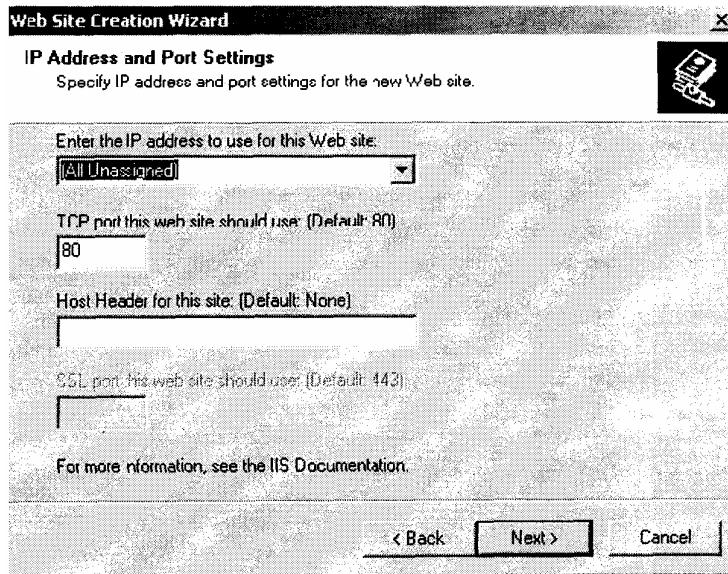
Hình 7.14



5 . Hộp thoại định cấu hình địa chỉ IP và hộp thoại thiết lập cổng xuất hiện, như hình 7.15. Ta có thể chỉ định địa chỉ IP, cổng TCP và Host Header (*đầu trang của máy chủ*) cho trang Web. Host Header dùng để xác định yêu cầu gửi đúng về trang Web

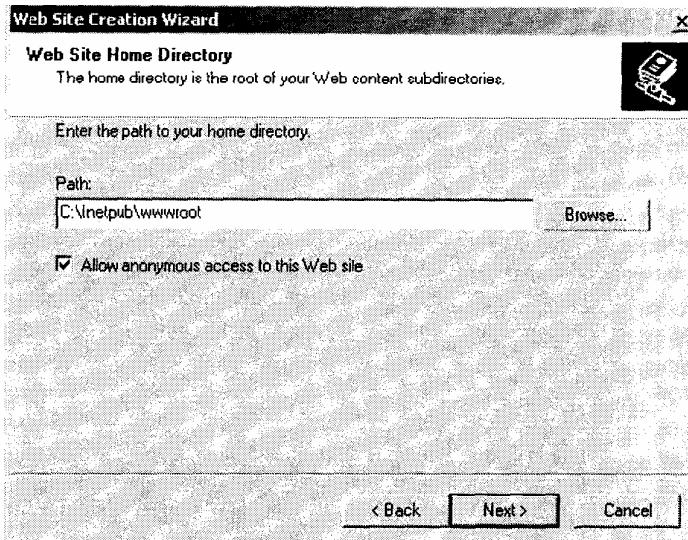
(khi mà máy tính phục vụ nhiều trang Web), mặc định là không có Host Header. Tiếp theo kích lên phím Next.

Hình 7.15



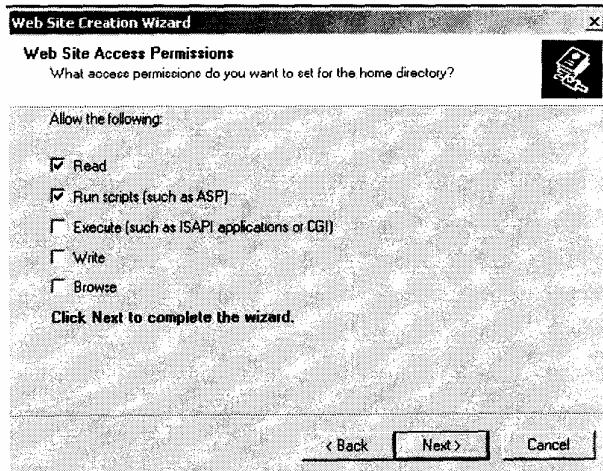
6. Hộp thoại Web Site Home Directory xuất hiện như hình 7.16. Yêu cầu ta đánh vào đường dẫn cho thư mục chủ. Ta cũng có thể quy định cho phép những người nặc danh được truy cập vào trang Web. Sau khi thông tin này được cấu hình, kích lên phím Next.

Hình 7.16



7. Hộp thoại Web Sức Access Permissions xuất hiện như hình minh họa 7.17. Lựa chọn các mục chọn đối với các truy nhập mà ta cho phép, tiếp theo chọn nút Next.

Hình 7.17



Sau khi đã tạo một trang Web mới, ta có thể thiết lập cấu hình và quản lý nó như đã được mô tả trong các phần trước.

Xử lý sự cố khi truy cập trang Web

Nếu người dùng không thể truy cập trang Web của mình, vấn đề này có thể do quyền truy nhập không hợp lệ, cấu hình thư mục gốc hoặc tệp mặc định không đúng, hoặc sử dụng sai cổng TCP. Đây là một vài lời khuyên để khắc phục các vấn đề truy nhập trang Web:

- ✓ Kết thúc nếu truy cập nặc danh được cho phép. Nếu vậy, xác minh rằng các tài khoản và mật khẩu mà đã được thiết lập trong Internet Services Manager phù hợp với tên của tài khoản và mật khẩu người dùng có trong cơ sở dữ liệu người dùng của Windows 2000.
- ✓ Xác nhận sự truy cập đã không bị từ chối căn cứ vào địa chỉ IP hoặc tên miền.
- ✓ Đảm bảo rằng các sự truy cập đúng cách đã được thiết lập.
- ✓ Xác nhận thư mục chủ được cấu hình đúng cách và tệp mặc định đã được cấu hình đúng.
- ✓ Đảm bảo rằng cổng TCP được đặt là cổng 80 hoặc ta đang truy cập trang Web mà sử dụng đúng cổng TCP.
- ✓ Đảm bảo rằng các sự cho phép NTFS đã không được thiết lập trên thư mục chủ để chúng hạn chế nhiều người dùng truy cập trang Web.

Tài liệu tham khảo

- [1] Lisa Donald, James Chellis: *MCSE Windows 2000 Server*, 2000.
- [2] Robin Walshaw: *Mission Critical Windows 2000 Server Administration*.
- [3] Microsoft Corporation: *MCSE Designing Windows 2000 Network Security*, 2001 .
- [4] Microsoft Corporation: *MCSE Training Kit Windows 2000 server*, 2000.

MỤC LỤC

CHƯƠNG 1: GIỚI THIỆU HỆ ĐIỀU HÀNH WINDOWS 2000 SERVER	1
1. Tổng quan về Windows 2000 server	1
2. Hướng dẫn cài đặt window 2000 Server	2
CHƯƠNG 2 : QUẢN TRỊ NGƯỜI DÙNG	12
1. Giới thiệu về tài khoản người dùng	12
1.1. Tổng quan về tài khoản người dùng	12
1.2. Các tài khoản người dùng có sẵn.....	12
1.3. Tổng quan về tài khoản nhóm	13
1.4 Tài khoản nhóm có sẵn.....	14
2. Làm việc với các tài khoản người dùng cục bộ	17
2.1. Sử dụng tiện ích Local Users and Groups	17
2.2 Tạo tài khoản người dùng	18
3. Làm việc với tài khoản người dùng Active Directory	22
3.1 Tạo người dùng Active Directory.....	22
3.2 Quản lý các đặc tính người dùng Active Directory	24
CHƯƠNG 3: QUẢN LÝ BẢO MẬT (8 lý thuyết).....	31
1. Thiết lập quản lý bảo mật	31
1.1. Tạo trình điều khiển quản lý cho các thiết lập bảo mật	32
2. Sử dụng các chính sách tài khoản người dùng	32
2.1 Thiết lập các chính sách mật khẩu.....	33
2.2 Thiết lập các chính sách về đăng nhập không hợp lệ	35
2.3 Thiết lập chính sách Kerberos	37
3. Sử dụng các chính sách cục bộ	39
3.1 Thiết lập chính sách kiểm định.....	40
3.2 Ân định quyền người dùng	42
3.3 Định nghĩa các tùy chọn bảo mật	45
4. Sử dụng các chính sách hệ thống.....	49
4.1 Cấu hình các chính sách hệ thống người dùng và nhóm người dùng.....	51
4.2 Quy định các chính sách hệ thống phù hợp	52
4.3 Tạo các chính sách hệ thống cho người dùng và nhóm người dùng	53
4.4 Cấu hình các chính sách hệ thống máy tính	56
5. Sử dụng công cụ Security Configuration and Analysis	56
5.1 Chỉ định cơ sở dữ liệu bảo mật	57
5.3 Phân tích bảo mật	58
5.2 Mẫu bảo mật	59
CHƯƠNG 4: QUẢN TRỊ TÀI NGUYÊN (4 lý thuyết)	63
1. Quản lý ổ đĩa	63
1.1. Sử dụng các tiện ích quản lý đĩa.....	65
2. Quản lý tệp tin và thư mục	76
2.1. Quản lý truy nhập cục bộ (địa phương).....	77
2.2 Quản lý các truy xuất mạng.....	83
CHƯƠNG 5: CÀI ĐẶT VÀ THIẾT LẬP CẤU HÌNH CARD MẠNG, GIAO THỨC MẠNG VÀ CÁC DỊCH VỤ MẠNG (4 lý thuyết).....	93
1. Cài đặt cấu hình cho card mạng	93
1.1.Cài đặt một card mạng.....	93
1.2 Cấu hình một card mạng.....	93
2. Cài đặt và thiết lập cấu hình cho giao thức mạng	97
2.1. Sử dụng TCP/IP	98
2.2. Sử dụng NWlink IPX/SPX/NetBIOS	105

2.3 Sử dụng NetBEUI.....	107
2.4 Quản lý Network Bindings	108
3. Cài đặt và cấu hình các dịch vụ mạng	108
3.1 Cài đặt các dịch vụ mạng.....	109
3.2 Sử dụng DHCP	110
3.3 Sử dụng WIN.....	117
3.4 Sử dụng DNS.....	118
4. Tổng kết.....	123
CHƯƠNG 6: QUẢN LÝ MÁY IN (4 lý thuyết).....	124
1. Cài đặt máy in.....	124
2. Quản lý thuộc tính của máy in.....	129
3. Quản lí máy in và tài liệu in	145
CHƯƠNG 7. QUẢN LÝ DỊCH VỤ MẠNG	151
1. Cài đặt Internet Information Services.....	151
2. Cấu hình và quản lý IIS (Internet Inforlination Services).....	151
2.1 Quản lý một trang Web	152
2.2 Tạo một trang Web mới.....	165
Tài liệu tham khảo	168