CHƯƠNG 1
TỔNG QUAN VỀ WINDOWS 2000

---

1. GIỚI THIỆU WINDOWS 2000

Windows 2000 là một hệ điều hành đa mục đích (*multipurpose operating system*) được tích hợp sẵn khả năng hỗ trợ cho các mạng khách/chủ (*client/server networks*) và mạng ngang hàng (*peer-to-peer networks*), hỗ trợ *Internet*.

Windows 2000 được thiết kế để nâng cao độ tin cậy (*reliability*), khả năng sống còn cao nhất của hệ thống (*system availability*) và khả năng thay đổi quy mô (*scalability*) cho phù hợp với đủ các loại mạng từ mạng cỡ nhỏ tới những mạng quy mô lớn cho cả một tổ chức/doanh nghiệp.

Họ sản phẩm *Windows 2000* bao gồm 4 phiên bản (*edition*):

- *Windows 2000 Professional.*
- *Windows 2000 Server.*
- *Windows 2000 Advanced server.*
- *Windows 2000 Data Center Server.*

1.1. Windows 2000 Professional

Windows 2000 Professional là hệ điều hành thế hệ mới cho máy tính để bàn thay thế *Win95/98* và *Windows NT for Workstation*. Nó là hệ điều hành được thiết kế cho người sử dụng bình thường trong các cơ sở kinh doanh. *Windows 2000 Professional* xây dựng trên nền tảng *Windows NT for Workstation* và *Win98*, nó chọn các ưu điểm của hai hệ điều hành này là tính ổn định và các chức năng bảo mật của NT và tính dễ sử dụng của *Win98*. Nó hỗ trợ việc nâng cấp từ *Win95, 98* và *Windows NT for Workstation*.

Các chức năng mới mở rộng trong *Windows 2000 Professional* bao gồm:

- Tính dễ sử dụng.
- Đơn giản hóa việc quản trị.
- Tăng sự hỗ trợ phần cứng: hỗ trợ khả năng cắm và chạy (*plug and play*), tăng cường khả năng quản lý nguồn điện (*enhanced power management*), và hỗ trợ cho một dải rất rộng các thiết bị phần cứng.
- Nâng cao việc quản lý File và bảo mật nhờ hệ thống mã hoá file: (f*ile encryption system*).

- Nâng cao việc kết nối *Internet*.
- Có thể được dùng như một network client.
- Có khả năng chia sẻ tài nguyên mạng.
- Cho phép 2 bộ xử lý chạy song hành & sử dụng 4GB bộ nhớ.

1.2. Windows 2000 Server

❖ Hệ điều hành *Windows 2000 Server* được thiết kế để dùng chủ yếu cho máy chủ của mạng (*network server*).

❖ *Windows 2000 Server* bao gồm tất cả các chức năng của *Windows 2000 Professional,* ngoài ra còn có thêm rất nhiều chức năng của một máy chủ, có thể đóng vai trò *File server, Print server, Application server & web server* và cho *Workgroup*.

❖ Nó hỗ trợ cho việc quản lý hệ thống mạng đơn giản hơn. *Terminal Service* được tích hợp trong phiên bản này để phục vụ cho việc chạy các ứng dụng mạnh trên Server.

❖ Nó có thể được cấu trúc như một máy chủ thành viên (*member server)* hoặc như một *Active Directory Domain Controller*.

❖ Thích hợp cho mạng của một cơ sở kinh doanh vừa và nhỏ.

❖ Hỗ trợ 2 bộ vi xử lý (CPU) khi cài đặt mới, 4 CPU khi nâng cấp từ NT4.0, 32 GB bộ nhớ vật lý trên hệ Alpha và 4 GB trên hệ Intel.

1.3. Windows 2000 Advanced Server

❖ Phiên bản này là hệ điều hành máy chủ mạnh hơn cho các ứng dụng hoặc các phòng ban.

❖ *Windows 2000 Advanced Server* bao gồm tất cả các tính năng của *Windows 2000 Server* và phát triển thêm các tính năng mở rộng quy mô (*scalability)* và khả năng sống còn cao (*high availability*).

❖ *Windows 2000 Advanced Server* được xây dựng cho những mạng doanh nghiệp lớn và trong môi trờng sử dụng cơ sở dữ liệu mạnh.

❖ Nó thích hợp cho mạng của cơ sở kinh doanh lớn.

❖ Ngoài ra nó còn có khả năng kết nối cụm máy chủ (*Clustering*) để đảm bảo tính luôn luôn sẵn sàng của hệ thống. Nó cho phép kết nối cụm 2 máy chủ (*2 ways clustering)*, tức là cho phép một server tự động gánh thêm nhiệm vụ của server kia khi server kia có sự cố.

❖ Nó cho phép hỗ trợ tối đa 8 bộ xử lý (CPU), 32 GB bộ nhớ vật lý trên hệ Alpha và 8 GB trên hệ Intel.

1.4. Windows 2000 Datacenter Server

❖ Phiên bản này được thiết kế để đáp ứng các yêu cầu của cơ quan/doanh nghiệp lớn và thích hợp cho các ứng dụng:

- Các ứng dụng xử lý giao dịch trực tuyến quy mô lớn (*Large Online Transaction Processing (OLTD) application*);
- Các ứng dụng khai thác kho dữ liệu (*Data warehousing application*);
- Các ứng dụng xử lý phân tích trực tuyến quy mô lớn (*Large-scale Online Analytical Processing (OLAP) application*);
- Các ứng dụng cung cấp dịch vụ *Internet* quy mô lớn (*Large-scale Internet service provide (ISPs)*).
- Các ứng dụng cung cấp dịch vụ Web quy mô lớn (*Large-scale Web site hosting*).

❖ Hỗ trợ kết nối cụm 4 máy chủ (*4 ways clustering*).

❖ Hỗ trợ đến 32 bộ xử lý & 64GB bộ nhớ.

2. CÁC NÉT ĐẶC TRƯNG CỦA WINDOWS 2000

Nét đặc trưng	Lợi ích
Chi phí sở hữu thấp nhất (*Lower total cost of ownership*)	Giảm chi phí chạy và quản trị mạng nhờ các khả năng: • Khả năng cài đặt và nâng cấp tự động các ứng dụng. • Dễ cài đặt và cấu hình các máy tính trạm. • Hỗ trợ việc quản trị, nâng cấp các máy trạm từ xa.
Bảo mật	❖ Xác thực người sử dụng (*Authenticates users*) trước khi họ được quyền truy nhập tới các tài nguyên hoặc dữ liệu. ❖ Cung cấp khả năng bảo mật và giám sát cục bộ hoặc trên mạng đối các files, folders, máy in và các tài nguyên khác. ❖ Hỗ trợ giao thức *Kerberos* và PKI (*public key infrastructure*).
Dịch vụ Thư mục (*Directory services*)	❖ Lưu giữ thông tin về các tài nguyên mạng như tài khoản người dùng, các ứng dụng, các tài nguyên in ấn, các thông tin bảo mật. ❖ Cung cấp dịch vụ cho phép người dùng có quyền truy nhập tới các tài nguyên trên toàn bộ mạng *Windows 2000* và xác định vị trí của các người dùng, máy tính và các tài nguyên khác. Cho phép các quản trị mạng quản trị và bảo

Nét đặc trưng	Lợi ích
	mật các tài nguyên đó. ❖ **Windows 2000 Server** lưu trữ và quản lý các thông tin về Dịch vụ thư mục chủ động (*Active Directory services*).
Tính năng cao và khả năng mở rộng lớn (*Performance and scalability*)	❖ Hỗ trợ đa xử lý song song (SMP) trên các máy tính có nhiều bộ xử lý. • *Windows 2000 Professional*: hỗ trợ tới **2 CPU**. • *Windows 2000 Server*: hỗ trợ tới **4 CPU**. Hỗ trợ xử lý đa nhiệm(*multitasking*) cho các tiến trình hệ thống và các chương trình.
Các dịch vụ kết nối mạng và truyền thông (*Networking and communication services*)	❖ Cung cấp các hỗ trợ có sẵn cho các giao thức mạng thông dụng nhất kể cả TCP/IP và IPX/SPX. ❖ Cung cấp khả năng kết nối với các mạng *Novell NetWare, UNIX, AppleTalk*. ❖ Cung cấp khả năng *dial-up networking:* ***Windows 2000 Server*** cho phép có tới 256 kết nối đồng thời qua điện thoại (*simultaneous inbound dial-up sessions*). **Windows 2000 Professional** cho phép có 1 kết nối.
Khả năng Tích hợp Internet (*Internet integration*)	❖ Cho phép kết nối các máy tính của người dùng với *Internet.* Người dùng có thể duyệt qua các tài nguyên trên mạng, mạng Intranet, Internet một cách an toàn, nhận và gửi các thư tín điện tử. ❖ **Windows 2000 Server** bao gồm *Microsoft Internet Information Server* (IIS). ❖ **Windows 2000 Professional** cung cấp một *personal Web server.*
Các công cụ quản trị tích hợp sẵn (*Integrated administration tools*)	❖ Cung cấp phương tiện để tạo ra các công cụ quản lý các máy tính cục bộ và ở xa theo ý của mình với một giao diện chuẩn duy nhất. ❖ Cung cấp phương tiện để gắn các công cụ quản trị của các hãng thứ 3 vào giao diện quản trị chuẩn chung.
Hỗ trợ phần cứng	❖ Hỗ trợ *universal serial bus* (USB). ❖ Hỗ trợ các phần cứng cắm và chạy (*Plug and Play*): *Windows 2000* tự động phát hiện, cài đặt và cấu hình các thiết bị phần cứng này.

3. GIỚI THIỆU VỀ ACTIVE DIRECTORY SERVICES

Một trong những phát triển lớn của *Windows 2000* là sự áp dụng dịch vụ thư mục (*directory service*) thông qua *Active Directory* (Thư mục chủ động). Toàn bộ tài nguyên mạng được quản trị tập trung qua những *Active Directory Ojects*. Người dùng sẽ không còn cần phải biết những tài nguyên này được thực sự ghi tại những máy cụ thể nào trên mạng.

*** Dịch vụ Active Directory là gì?**

Active Directory Services bao gồm:

- Thư mục (**directory**) trong đó chứa các thông tin về các tài nguyên trên mạng.
- Các dịch vụ (**services**) để làm cho các thông tin này trở nên sẵn sàng và hữu ích cho người sử dụng cũng như quản trị viên.

Các tài nguyên chứa trong thư mục bao gồm dữ liệu của người dùng, máy in, máy chủ, cơ sở dữ liệu, các nhóm người dùng, các máy tính, và các chính sách bảo mật (*security policies*). Những tập dữ liệu này được biết đến như những đối tượng (**objects)**.

Active Directory Services đơn giản hóa việc quản lý mạng nhờ việc tổ chức các tài nguyên mạng theo cấu trúc miền (*domains*). Mỗi *domain* là một nhóm logic bao gồm những máy chủ và các tài nguyên mạng khác và được nhận biết bởi tên của *domain*. Mỗi *domain* bao gồm 1 hoặc nhiều *domain controller*. Mỗi *domain controler* trong một *domain* là một máy tính chạy *Windows 2000 Server* chứa toàn bộ dữ liệu mạng của *domain* ấy. Tất cả các *domain controller* là những peers, và khi bạn thay đổi trên một domain controller thì sự thay đổi này sẽ được upgrade trên tất cả những *domail controller* khác trong *domain*.

Active Directory Services hỗ trợ tính năng scalability (mở rộng) nhờ việc lưu giữ thông tin trên những phần riêng biệt, mỗi phần cho phép lưu giữ một khối lượng rất lớn các đối tượng. Nhờ vậy *driectory* có thể mở rộng dễ dàng khi có yêu cầu mở rộng mạng.

Active Directory Services hỗ trợ việc mở rộng hệ thống tiêu chuẩn bằng cách tổ hợp các quy ước về *namespases* của *Internet* với dịch vụ thư mục của *Windows 2000*. Điều này cho phép việc thống nhất và quản lý nhiều *namespaces* hiện đang tồn tại trên phần mềm và phần cứng của các mạng máy tính. Active Directory Services sử dung domain name system (DNS) cho hệ thống tên của nó và có thể trao đổi thông tin với bất cứ trình ứng dụng hay thư mục nào dùng giao thức *Lightweight Directory Acess Protocol*

(LDAP) hoặc HTTP. LDAP là một chuẩn *Internet* để truy cập dịch vụ thư mục được phát triển để thay thế cho *Directory Access Protocol* (DAP). HTTP là một giao thức chuẩn để hiển thị các trang web trên *World Wide Web*. *Active Directory Services* có tính tương giao với LDAP và HTTP.

Active Directory Services hỗ trợ cho khuôn dạng đặt tên chuẩn (standard name formats) bao gồm:

- RFC 822: Đây là dạng dùng cho địa chỉ email: *usernames@domainname*
- HTTP URL (*Uniform Resource Locator*): Đây là dạng dung cho Web Browsers: *http//:domain/path-to-pages*
- *Universal Nameming Conversion* (UNC): Đây là dạng được dùng cho workgroup và domains để sử dụng chung các tài nguyên mạng. Ví dụ: *\\microsoft.com\xl\budget.xls*
- LDAP URL:

Dạng này bao gồm tên một *Active Directory Domain Controller* và tên của object. Ví dụ:

LDAP://someserver.microsoft.com/

CN=fmiller,OU=product,OU=division,DC=devel,O=class, C=us.

Trong đó:

CD là object's Common Name (tên của object)

OU là Organizasional Unit (một container có thể chứa các ojects)

DC là Domain Component Name

O là tên công ty (organization)

C là Country

4. GIỚI THIỆU VỀ WORKGROUP & DOMAIN TRONG WINDOWS 2000

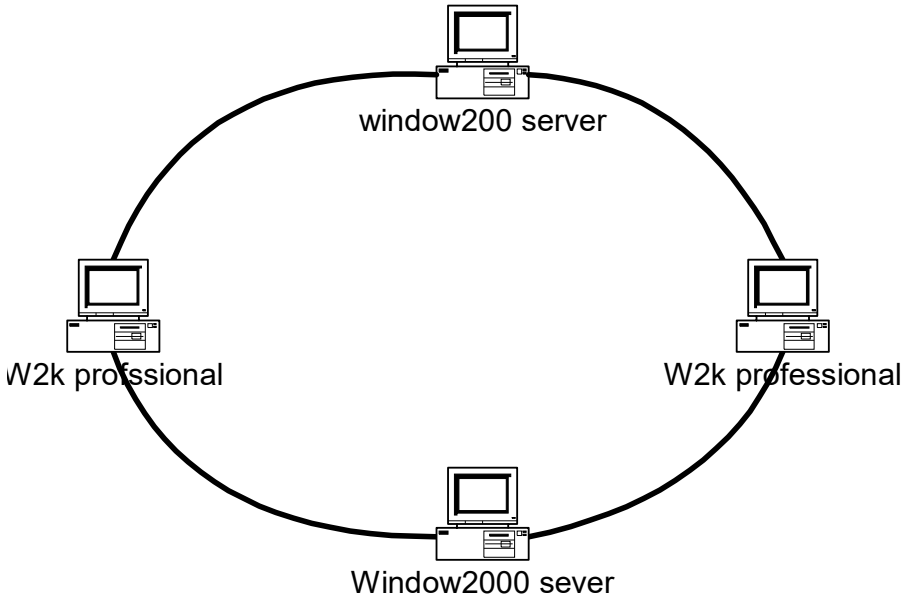
Windows 2000 hỗ trợ cho 2 loại mạng cơ bản là mạng theo nhóm làm việc (*Workgroup*) & mạng theo miền (*Domain*).

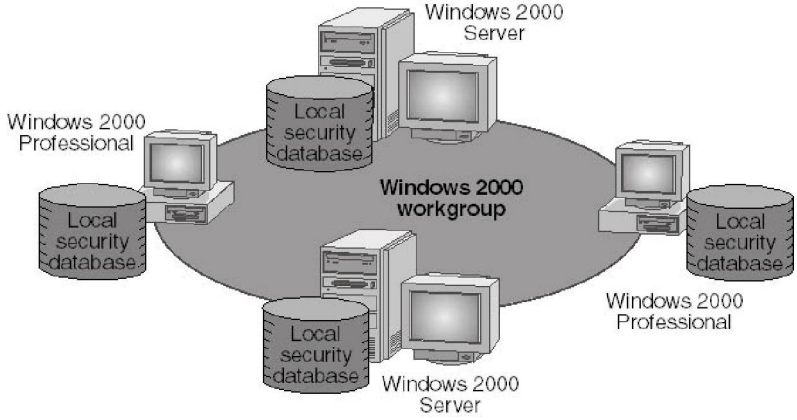
4.1. Window2000 Workgroups

Workgroups là một nhóm lôgic các máy tính được nối mạng với nhau chia sẻ sử dụng chung các tài nguyên. Mạng *Workgroups* còn được biết với tên mạng ngang hàng (*peer-to-peer networks*) bởi vì tất cả các máy trong mạng đều có thể chia sẻ dùng chung các tài nguyên mạng một cách bình đẳng.

Mỗi máy tính trong *Workgroups* có thể chạy *Windows 2000 Server* hoặc *Windows*

2000 Professional và lưu giữ một cơ sở dữ liệu tại chỗ về bảo mật (*local security database*) trong đó có chứa tất cả các tài khoản người dùng (*user account*) và các thông tin tài nguyên bảo mật của riêng máy đó.





Windows 2000 Workgroup

❖ Đặc điểm của mạng *Windows 2000 Workgroup* là:

- Mỗi người dùng phải có một tài khoản người dùng trên mỗi máy tính.
- Nếu có thay đổi gì về tài khoản người dùng thì phải thực hiện trên tất cả các máy tính.

❖ Ưu điểm của *Windows 2000 Workgroup* là:

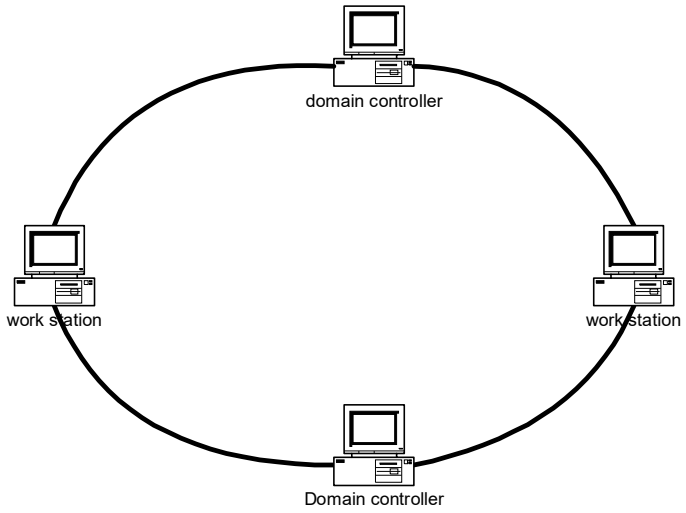
- Không cần phải có riêng một máy chạy *Windows 2000 Server* để chứa các thông tin của toàn mạng một cách tập trung.

- Dễ thiết kế và lắp đặt.
- Thuận tiện trong trường hợp một mạng gồm ít máy tính (thường chỉ áp dụng với mạng có dưới 10 máy tính).

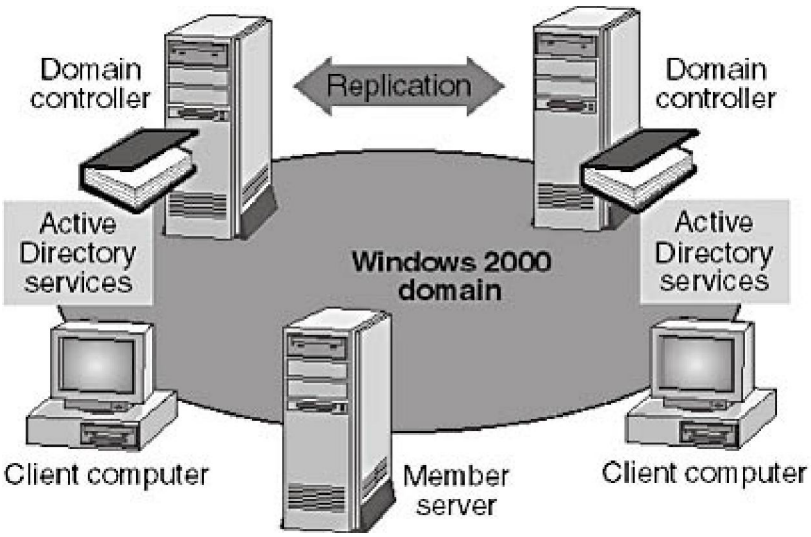
☞ Trong mạng *Workgroup,* máy tính chạy *Windows 2000 Server* được gọi là máy chủ đứng đơn lẻ (*Stand-alone Server*).

4.2. Windows 2000 Domains

Nếu như *workgroup* trong *Windows 2000* có cấu trúc gần như hoàn toàn giống với *WinNT*, thì *domain* trong *Windows 2000* lại là một sự phát triển đáng chú ý.



Windows 2000 Domain



Domain Directory

❖ *Domain* của *Windows 2000* là một nhóm logic các máy tính có cùng chung một

cơ sở dữ liệu tập trung về thư mục (*central directory database*). Cơ sở dữ liệu này chứa các thông tin về tất cả các *objects* của *domain*.

❖ Một *domain* có thể không hạn chế trong một khu vực địa lý nhỏ. Các máy tính trong 1 *domain* có thể nằm trong 1 mạng LAN hoặc nằm khắp nơi trên thế giới, liên lạc với nhau qua nhiều kiểu kết nối khác nhau như: *Integrated Services Digital Networks (ISDNs), Digital Subscriber Lines (DSLs)*.

Domain Controller

❖ *Domain controller* là một máy chủ quản lý tất cả các tương tác liên quan đến bảo mật user/domain và quản trị tập trung.

❖ Trong *Windows 2000* không còn khái niệm *Primary domain controller* & *Backup domain controller*, thay vào đó là các *domain controller* trong đó có chứa bản copy của *central directory*. Khi thay đổi thông tin trong một *directory* của một *domain controller*, *Windows 2000* sẽ tự động cập nhật cho toàn bộ các *domain controller* còn lại.

❖ Trong *domain* của *WinNT* sự quản lý mang tính tập trung ở *Primary Domain Controller* và *Backup Domain Controller*, tuy nhiên chỉ nằm ở mức độ rất thấp, khi một người dùng muốn truy cập một nguồn dữ liệu, anh ta không những cần được sự cho phép mà còn cần phải biết nguồn dữ liệu đó được lưu giữ ở ổ đĩa vật lý nào.

❖ Với *domain* của *Windows 2000* người dùng sẽ không còn cần phải biết nguồn tài nguyên mạng được thực sự chứa ở ổ đĩa vật lý nào mà chỉ cần biết địa chỉ logic của nó trong *directory* mà thôi.

Lợi ích của việc sử dụng Windows 2000 domains

- Cung cấp khả năng quản trị tập trung vì tất cả thông tin về người dùng được lưu trữ tập trung.
- Cho phép người dùng chỉ cần đăng nhập mạng 1 lần (*single logon process*) là có thể truy nhập tới tất cả các tài nguyên trong domain mà họ đã được phân truy nhập tới.
- Cung cấp khả năng mở rộng mạng vì có thể tạo ra các mạng rất lớn.

CHƯƠNG 2
CÀI ĐẶT WINDOWS 2000 SERVER
---

1. CHUẨN BỊ ĐỂ CÀI ĐẶT WINDOW2000 SERVER

1.1. Các công việc cần chuẩn bị

Bảng dưới đây liệt kê các bước bạn cần làm trước khi tiến hành cài đặt Window 2000 server.

Công Việc

Kiểm tra xem máy tính của bạn có đạt yêu cầu tối thiểu để cài đặt Window 2000 server không.

Kiểm tra tất các các bộ phận phần cứng (network adapters, video drivers, sound cards, CD-ROM drives, PC cards, and so on) xem có tương thích với hệ điều hành Window 2000 server không bằng cách so sánh với bảng *Windows 2000 Hardware Compatibility List (HCL)*.

Xác định rõ xem bạn muốn chia ổ đĩa cứng của banh như thế nào?

Chọn File hệ thống (FAT hay NTFS). Nên chon NTFS trừ khi bạn muốn cài đặt nhiều hợn một hệ điều hành trên máy tính của bạn.

Chọn loại mạng mà máy tính của bạn sẽ gia nhập vào (workgroup or domain). Nếu bạn định gia nhập vào một domain, bạn cần biết thêm một số thông tin như domain name và tài khoản của bạn. Nếu bạn có một administrator account và password trong domain, bạn có thể tạo một computer account trong domain đó.

Xác định xem bạn muốn cài mới Window 2000 server hay nâng cấp từ Windows NT Server.

Chọn phương pháp cài đặt: Setup boot disks, CD-ROM, or over-the-network.

Chọn các cấu hình mà bạn muốn cài đặt ví dụ Networking Services hay Microsoft Indexing Service.

Ngoài các công việc trên bạn còn cần thực hiện một số công việc sau để chuẩn bị cho việc cài đặt Window 2000.

Làm việc với Domain Name System (DNS)

Khi bạn tạo ra một window2000 domain, thì dịch vụ DNS phải được thiết lập và hoạt động. Nếu bạn gia nhập vào một domain bạn phải biết DNS name của domain đó.

Nếu DNS không hoạt động nó sẽ được thiết lập tự động khi bạn khởi tạo domain controler.

Ghi lại các thông tin cần thiết

Bạn cần ghi lại các thông tin cần thiết như hệ điều hành trước đó, tên của máy tính (nếu máy của bạn đang ở trên mạng), tên của workgroup hay domain, IP address v.v.

Backing Up Files

Bạn cần backup tất cả các file cần thiết trước khi thực hiện cài đặt Window 2000.

Xem lại các Applications

Bạn nên đọc file Readme.doc của chương trình window 2000 setup để xem thêm các thông tin về các file cần thiết phải được vô hiệu hoá hay loại bỏ trước khi cài đặt. Bạn có thể phải loại bỏ các phần mềm scan virus, các phần mềm máy khách v.v.

Kiểm tra Viruses cho Boot Sector

Boot sector virus sẽ làm cho việc cài đặt không thể thực hiên được. để đảm bảo nó không ảnh hưởng đến quá trình cài đặt bạn nên chạy chương trình *Makedisk.bat* trong thư mục *\Valueadd\3rdparty\CA_antiv* trên đĩa CD để chống vius này.

Các vật dụng cần thiết khác

- Đọc tất cả các file *.doc hay *.txt trông đĩa CD cài đặt.
- Đảm bảo là bạn có đủ các phần mềm driver cho tất cả các phần cứng của bạn.
- Tất nhiên là bạn phải có CD cài đặt window 2000 server hay một file window 2000 server được share chung trên mạng.
- Format khoảng 3 hay 4 ổ đĩa mềm 3.5-inch 1.44 MB (if creating optional Setup Startup disks).

1.2. Các yêu cầu tối thiểu về phần cứng

Các yêu cầu tối thiểu về phần cứng được liệt kê trong bảng sau.

Phần cứng của hệ thống	Yêu cầu tối thiểu cho Windows 2000 Server	Yêu cầu tối thiểu cho Windows 2000 Professional
Bộ xử lý	133-Mhz Pentium	133-Mhz Pentium
Bộ nhớ	128 MB of RAM (nên có 256 MB)	64 MB of RAM (Nên có 128 MB)
Dung lượng đĩa	671 MB còn trống (nên có 2 GB)	620 MB còn trống (nên có 2 GB)
Màn hình	VGA monitor 640x480	VGA monitor 680x480

CD-Rom	12x hoặc nhanh hơn	12x hoặc nhanh hơn

1.3.Chia phần cho ổ cứng (Disk Partitions)

Bạn nên thực hiện việc chia phần cho ổ cứng trước khi thực hiện cài đặt bao gồm việc chọn size co ổ cứng và chọn file hệ thông để định dạng cho mỗi phần.

Chọn size cho phần cài đặt

Window 2000 yêu cầu bạn có tối thiểu 671MB trống trên ổ cứng, tuy nhiên bạn nên dành khoảng 2 GB cho phần cài đặt để dự phòng cho các chương trình cài đặt thêm về sau.

Phần system patition là phần chứa các file hệ thống cần thiết để bắt đầu quá trình load window2000 như Ntldr, Ntdetect.com, boot.ini. Hệ điều hành sẽ không khởi động được nếu system patition không được đặt ở trạng thái Active.

Phần boot partition là nơi Windows 2000 Server được cài đặt vào. Nó chứa các thư mục của hệ điều hành như Winnt, \System32, Windows 2000 kernel, và tất cả các file cần thiết để chạy hệ điều hành window 2000. NếuWindows 2000 Server được cài trên phần active partition thì phần đó sẽ vừa là boot vừa là system partition.

Nếu bạn muốn cài đặt nhiều hệ điều hành trên cùng một máy thì bạn nên cài đặt window 2000 trên một partition riêng.

Các file hệ thống (File Systems)

Nếu bạn cài đặt Window 2000 lên một phần chưa định dạng của ổ đĩa, bạn sẽ được yêu cầu chọn loại file hệ thống dùng để định dạng cho phần đó. Windows 2000 hỗ trợ các loại file hệ thống bao gồm NTFS and the FAT .

NTFS

NTFS là loại file hệ thống được hỗ trợ bởi Window 2000 và WindowNT. Nó có tất cả các tính năng của FAT, cộng thêm các tính năng khác như security, compression, và khả năng mở rộng partition. Version mới nhất của NTFS là NTFS 5.0 được cung cấp kèm với các CD cai đặt window 2000. Ngoài 2 hệ điều hành trên, các hệ điều hành khác đều không nhìn thấy partition dưới dạng NTFS.

FAT16 and FAT32

FAT 16 và FAT32 là các file systems cho phép truy nhập bởi nhiều hơn một hệ điều hành. Nó không có nhiều tính năng mà NTFS hỗ trợ, tuy nhiên nếu bạn muốn partition của bạn được nhìn thấy bởi các hệ điều hành khác ngoài Window2000 và WindowNT thì bạn phải định dạng ổ đĩa với FAT.

Một vài điểm cần chú ý đối với File System cho một boot partition

- Bạn có thể dùng một partition đã tồn tại hay khởi tạo một partition mới.
- Bạn có thể chuyển một partition định dang FAT thành NTFS, nhưng không thể chuyển ngược lại.
- Bạn có thể định dạng lại cho một partition đang tồn tại theo dạng FAT hay NTFS, nhưng tất cả các thông tin trên đó sẽ mất.
- Bạn nên chọn FAT nếu bạn muốn có cài đặt hệ điều hành kép với Window95, 98 hay NT.
- Bạn nên chọn NTFS nếu bạn chọn Window 2000 để chạy và bạn muốn sử dụng các điểm ưu việt của NTFS.

Bảng sau so sánh các đặc điểm khác nhau của NTFS, FAT16 và FAT 32:

Operating system	**FAT16**	**FAT32**	**NTFS**
Các đặc điểm chung	Nhìn thấy bởi MS-DOS, Windows 3.*x,* Windows 95, Windows 98, Windows NT, Windows 2000, and OS/2.	Chỉ nhìn thấy bởi Windows 95 OSR2, Windows 98, Windows NT and Windows 2000.	Chỉ nhìn thấy bởi Windows NT and Windows 2000. Khi máy tính hoạt động với operating system khác (như MS-DOS, Windows 95, Windows 98, or OS/2), các operating system đó không thể truy cập vào các file trong NTFS volume trên cùng một máy tính.
Supported by MS-DOS and Windows 3.*x*	Yes	No	No
Supported by Windows 95 pre-OSR2 releases	Yes	No	No
Supported by Windows 95 OSR2 and Windows 98	Yes	Yes	No

Supported by Windows NT 3.51	Yes	No	Yes, but Windows NT 3.51 does not support NTFS version 5.0.
Supported by Windows NT 4.0	Yes	No	Yes. Windows NT 4.0 supports NTFS version 5.0 with Service Pack 4 or later installed.
Supported by Windows 2000	Yes	Yes	Yes

1.4. Workgroups and Domains

Trong quá trình cài đặt bạn cần phải chọn loại mạng mà bạn sẽ gia nhập vào, đó là workgroup or domain.

Gia nhập vào một Workgroup

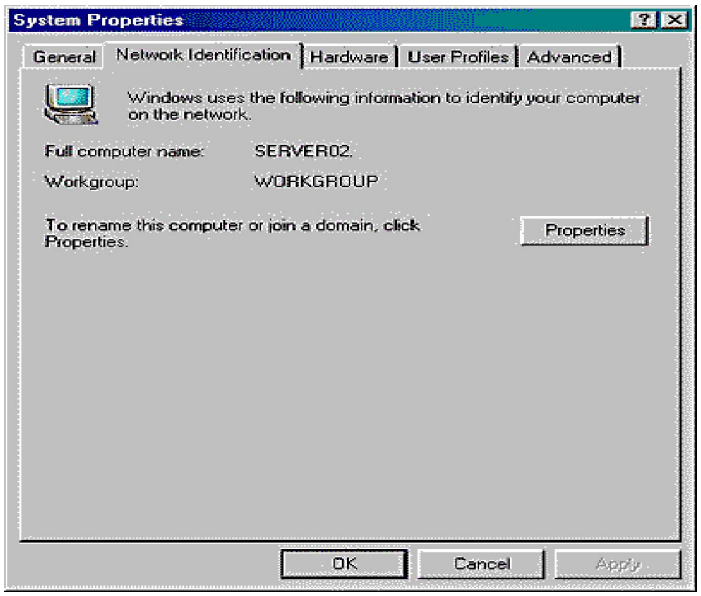
Bạn cần phải biết tên workgroup hay đặt tên cho workgroup mới của bạn khi cài đặt window 2000. Một domain và một workgroup có thể dùng chung một tên, nhưng phải chú ý một vài điểm sau:

- Những workgroup computers không phải là thành viên của domain và không nằm trong domain administration.
- Workgroup computers xuất hiện với các domain computers trong Windows 2000 Explorer.

Gia nhập vào một Domain

Bạn sẽ được yêu cầu điền vào tên DNS trong quá trình cài đặt tại trước khi bạn có thể gia nhập vào một domain bạn phải có một tài khoản trong domain database. Chỉ có người dùng có quyền *Join A Computer To The Domain permission* là có thể tạo tài khoản trên domaiâinccs thành viên của Administrators, Domain Administrators, hay Account Operators được mặc định có quyền này.

Ít nhất phải có một domain controller và một DNS server đang hoạt độngkhi cài đặt một máy tính vào domain đó. Nếu bạn cài đặt Windows 2000 Server như một máy tính độc lập bạn vẫn có thể gia nhập nó vào một domain sau bằng các sử dụng *Network Identification tab* trong cửa sổ *System Properties* như trong hình sau:



2. CÀI ĐẶT WINDOWS 2000 SERVER TỪ ĐẦU

Trong hầu hết các trường hợp cài đặt mới *Windows 2000* yêu cầu phải chuẩn bị ít nhất. Trong nhiều trường hợp màn hình hiển thị (*wizard*) cài đặt *Windows 2000 Server* và *Windows 2000 Professional* giống như nhau.

2.1. Tạo một bộ đĩa cài đặt Windows 2000 Server

- Chọn 4 đĩa mềm tốt, dán nhãn *Windows 2000 Server Setup* N^0 1 đến 4.
- Đưa đĩa CD cài đặt *Windows 2000 Server Setup* vào ổ CD.
- Nếu thấy xuất hiện *Wizard Setup* thì kích chuột vào **NO**.
- Open Command Prompt.
- Đổi đến ổ CD-ROM.
- Gõ vào lệnh **cd bootdisk** và ấn **Enter**.
- Gõ vào lệnh **makebt32 A:** và ấn **Enter**. *Windows* sẽ hiển thị một thông báo yêu cầu bạn phải có 4 đĩa mềm tốt.
- Ấn phím bất kì để tiếp tục, *Windows* sẽ yêu cầu bạn cho đĩa 1 vào ổ A. Sau khi *Windows* tạo xong đĩa 1, sẽ yêu cầu bạn cho tiếp đĩa 2, quá trình này tiếp tục cho đến đĩa 4.
- Gõ vào lệnh **Exit** và ấn **Enter**.

Bộ đĩa bạn vừa tạo có thể dùng để cài đặt *Windows 2000* trong trường hợp bạn có một máy mới lắp ráp, chưa có một hệ điều hành nào được cài đặt, ổ cứng của bạn cũng chưa được format và bạn cũng không thể khởi động máy từ CD-ROM được. Quá trình này được thực hiện như sau.

2.2. Kích hoạt Windows 2000 Server pre-copy và Text mode setup

- Đưa đĩa số 1 vào ổ A và đĩa CD *Windows 2000 Server Setup* vào ổ CD, khởi động máy.
- Khi được yêu cầu thì thay đĩa số 1 bằng đĩa số 2, quá trình này sẽ tiếp tục cho đến đĩa số 4.
- *Windows* sẽ hiển thị thông báo báo hiệu đang chạy chương trình *Setup*, ấn **Enter** để tiếp tục.
- Ấn **Enter** để qua màn hình chào mừng và chuyển đến màn hình nói về bản quyền (*Licence Agreement*), ấn **F8** để chấp nhận.
- Chọn ổ đĩa bạn muốn cài đặt *Windows 2000 Server* rồi ấn **Enter**.
- Chọn hệ thống file là NTFS rồi ấn *Enter*. Chương trình *Setup* sẽ format ổ đĩa để chuẩn bị cài đặt *Windows 2000 Server*, quá trình này có thể kéo dài vài phút.
- Lấy đĩa mềm ra khỏi ổ A.
- Chương trình *Setup* sẽ copy thêm các file cần thiết và khởi động lại máy để tải nạp chương trình *Windows 2000 Setup Wizard*.

2.3. Windows 2000 Server Setup Wizard

Phần này sẽ giải thích cặn kẽ các bước cần thực hiện trên các wizard của *Windows 2000 Setup*.

- Khi bạn bắt đầu quá trình setup, màn hình đầu tiên sẽ cho phép bạn chọn để nâng cấp lên *Windows 2000* từ một hệ điều hành cũ hoặc cài đặt mới hoàn toàn (*Clean Install*), trong trường hợp của bài này ta chọn cài đặt mới (*Install a new copy of Windows 2000*), nhấn **next** để tiếp tục.
- Trên màn hình **Regional Setting**, đảm bảo rằng các giá trị đặt cho *system locate, user locate và keyboard layout* là đúng, nhấn **next** để tiếp tục.
- Trên màn hình **Personalize Your Softwere**, điền vào tên của bạn, tên cơ quan v.v. vào các trường tương ứng. Những thông tin này được sử dụng để tạo các tên mặc định về sau. Nhấn chuột vào **Next** để tiếp tục.
- Trên màn hình **product key**, gõ vào mã số sản phẩm gồm 25 ký tự, nhấn chuột vào **next** để tiếp tục.
- Trên màn hình **Licensing Mode**, chọn **Per Server Number of Concurrent Connection**, gõ vào số **5** để khai báo số kết nối đồng thời cho phép (*concurent connection*), nhấn **next** để tiếp tục.

• Trên màn hình **Computer Name and Administrator Password**, điền vào tên máy tính của bạn. Nếu máy tính của bạn đã được kết nối vào mạng thì bạn cần hỏi quản trị mạng để biết tên máy tính bạn. Bạn cũng phải điền vào mật khẩu và nhắc lại để đảm bảo chắc chắn. Cần nhớ đây là mật khẩu của quản trị viên (*administrator password*).

• Trên màn hình **Windows 2000 Component**, bạn có thể chọn **Typical** hoặc **Customine**. Bạn có thể cài đặt thêm các thành phần khác sau này.

• Trên trang **Modem Dialing Information**, điền vào mã vùng và mã nước rồi nhấn **next**.

• Điền vào ngày và giờ phù hợp rồi nhấn Next.

• Trên màn hình **Networking Settings**, chọn **Typical setting**. Việc đặt các thông số này sẽ cấu hình các thành phần mạng dùng để truy cập cũng như chia sẻ các tài nguyên trên mạng bao gồm *Client for Microsoft Network, File and Printer Sharing for Microsoft Network* và tự động cấu hình *Internet Protocol* (TCP/IP) dùng DHCP.

• Bạn cũng sẽ được yêu cầu chọn *workgroup* hay *domain membership*, các thông tin này cũng có thể thay đổi sau khi cài đặt. Ban có thể chọn ngầm định là WORKGROUP.

• Trên màn hình cuối cùng của quá trình setup, lấy đĩa CD ra khỏi ổ đĩa và nhấn **Finish**.

3. NÂNG CẤP LÊN WINDOWS 2000 SERVER

❖ Chỉ có *WindowNT 3.51 Server, WindowNT 4.0 Server* là có thể nâng cấp (*upgrade*) lên được *Windows 2000 Server*. Với các hệ điều hành khác bạn phải xoá nó đi và cài đặt mới *Windows 2000 Server*.

❖ Quá trình nâng cấp cũng gần giống như quá trình cài đặt mới, bạn chỉ cần chọn **Upgrade to Windows 2000**.

❖ Tiếp theo bạn được yêu cầu đồng ý với thoả thuận về bản quyền sử dụng (*User License Agreement)*, bạn cũng phải điền vào mã số sản phẩm gồm 25 ký tự.

❖ Nếu đĩa cứng của bạn không được format theo hệ thống file NTFS, bạn sẽ được yêu cầu chuyển đổi thành NTFS format.

❖ Tiếp theo chương trình *Setup* sẽ copy những file ban đầu cần thiết, sau đó nó sẽ yêu cầu bạn khởi động lại máy, nếu bạn không thì nó cũng sẽ tự động khởi kộng lại máy sau 15 giây.

❖ Sau khi khởi động lại chương trình *Setup* sẽ kiểm tra ổ cứng của bạn xem có lỗi không, sau đó nó sẽ copy những file cần thiết để chạy quá trình cài đặt. Nó sẽ bắt đầu

giống như quá trình cài đặt bình thường. Chương trình *Setup* sẽ tự động:

- Dò tìm và cài đặt các ổ đĩa trong máy.
- Cài đặt các thành phần nối mạng (*networking components*) dựa trên cấu trúc hiện tại của mạng của bạn.
- Cài đặt các thành phần của *Windows 2000 Server*.
- Cài đặt các mục (items) trong *Start menu*.
- Đăng kí (register) các thành phần.
- Lưu giữ các cách đặt thống số đã thực hiện.

❖ Kết thúc qua trình nâng cấp, *Windows 2000* sẽ khởi động lại và sẵn sàng để chạy.

4. MỘT SỐ KHÓ KHĂN THƯỜNG GẶP KHI CÀI ĐẶT WINDOWS 2000 SERVER VÀ CÁCH KHẮC PHỤC

Bảng sau sẽ tổng kết các khó khăn thường gặp khi cài đặt window 2000 server.

Problem	Giải pháp
Media errors	Nếu bạn cài đặt từ CD-ROM, thay CD-ROM khác. Nếu vẫn thấy media errors, hãy tìm một đĩa CD-ROM gốc.
Unsupported CD-ROM drive	Thay một ổ CD khác được hỗ trợ bởi Window 2000. Nếu không thể được thì thử một cách cài đặt khác chẳng hạn cài qua mạng. Sau khi bạn cài đặt xong bạn có thể cài đặt thêm driver cho ổ CD đó nếu bạn có nó trên đĩa mềm.
Không đủ khoảng trống trên đĩa	- Sử dụng chương trình cài đặt để tạo partition từ những phần trống còn lại trên ổ đĩa. - Xoá và tạo những partition đủ rông để cài đặt. - Format lại partition đang tồn tại để tạo một partition rộng hơn.
Không sử dụng được các dịch vụ mạng	Dùng *Windows 2000 Setup wizard*, quay lại *Network Settings dialog box* và thẩm định chắc chắn rằng bạn cài đặt đúng protocol và network adapter. Chú ý rằng tên máy tính trên mạng phải là duy nhất.
Không nối được với domain controller	Thẩm định rằng domain name là đúng. Thẩm định rằng server đang chạy dịch vụ DNS và cả server và domain controllerd đều đang hoạt động.

	Thẩm định network adapter card và protocol settings đều đã đặt đúng. Nếu bạn cài đặt lại window 2000 và sử dụng cùng một computer name, hãy xoá tài khoản cũ đi và tạo một tài khoản mới.
Không thể cài đặt hoặc start Windows 2000	Hãy xác định rằng Windows 2000 đã nhận dạng được tất cả các thành phần phần cứng.

CHƯƠNG 3
CẤU HÌNH ACTIVE DIRECTORY VÀ DOMAIN CONTROLER

---

1. CẤU HÌNH ACTIVE DIRECTORY

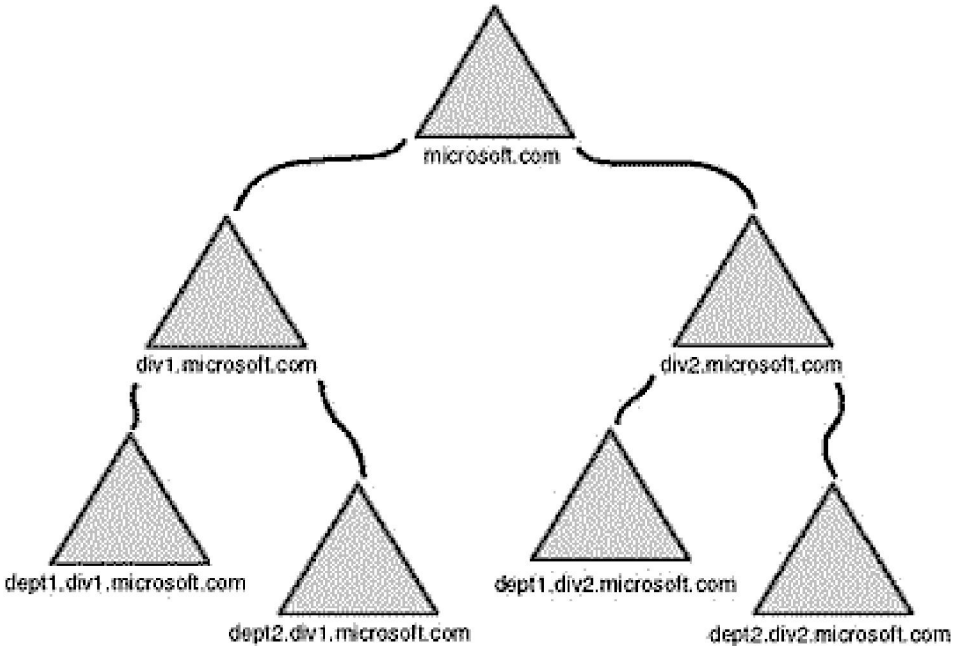
1.1. Active Directory & Domain Name System (DNS)

Việc cài đặt *Active Directory* (AD) yêu cầu phải có một *DNS Server* ở trên mạng. Sở dĩ như vậy vì AD sử dụng DNS như giải pháp đặt tên *domain* cũng như các dịch vụ địa phương của nó.

Mỗi *domain* và *object* trong *domain* đó phải có một tên duy nhất không trùng với bất cứ *domain* hay *object* nào khác. DNS được tổ chức theo một cấu trúc phân tầng được gọi là *domain namespace*. Ví dụ một *domain* có thể được đặt tên theo kiểu sau:

Microsoft.com.

Hình 3.1 sau biểu diễn cấu trúc namespace trong một miền của window 2000.



Hình 3.1: *Sơ đồ Namespace trong cùng một miền (domain)*

Từng máy tính riêng biệt được đặt tên bằng cách nối thêm tên của máy tính đó vào bên trái tên của miền, ví dụ:

sql1.Microsoft*.com*, **sql2**.Microsoft*.com*

1.2. Cấu trúc logic của Active Directory

Active Directory được cấu trúc theo kiểu phân tầng, từ trên xuống dưới bao gồm các thành phần sau:

- *Forests*
- *Trees*
- *Domains*
- *Organization Units (OU)*
- *Objects*

Sau đây chúng ta sẽ xem qua các thành phần này theo thứ tự từ dưới lên trên.

Objects

❖ *Object* (đối tượng) là một tài nguyên có thể nhận biết được của mạng, ví dụ như máy tính, máy in, người sử dụng, OU, *Group, Shared Folder* v.v..

❖ *Object* được nhận biết thông qua các thuộc tính (*attribute*) và đặc điểm của chúng.

❖ *Object Class* (lớp đối tượng): là nhóm lôgic các *object*. Ví dụ về các lớp đối tượng:

- Người sử dụng (*users*).
- Nhóm người sử dụng (*groups*).
- Máy tính.
- Miền (*domains*).
- *Organizational units*.

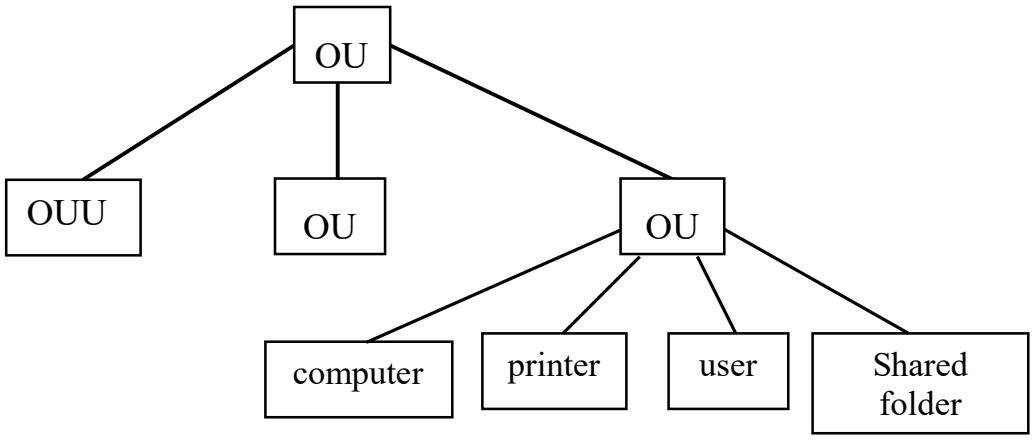
❖ *Container objects:* Một số *object* có thể bao gồm nhiều *object* khác và được gọi là *container objects* (đối tượng chứa). Ví dụ về *container objects* là OU hay *Domain*.

Organization Units (OU)

❖ OU (đơn vị tổ chức) là những *container objects* dùng để tổ chức các *object* trong một *domain* thành những nhóm quản trị lôgic nhỏ hơn.

❖ Một OU có thể chứa các *objects* khác nhau như: các tài khoản người dùng, các nhóm, các máy tính, các máy in, các trình ứng dụng, các tệp sử dụng chung (*file shares*), và các đơn vị tổ chức con khác.

❖ Cấu trúc phân tầng này là hoàn toàn độc lập trong mỗi *domain* trong mạng. Mỗi domain có thể có một sơ đồ tổ chức các OU riêng của mình.



Organization Units

❖ Điều quan trọng khi thiết lập các OU là phải xác định được phạm vi quản lý cho mỗi OU. Chẳng hạn như trong OU của toàn công ty mỗi phòng được chia làm một OU nhỏ, mỗi OU nhỏ này có một người quản trị và anh ta cũng có quyền thêm hay loại bỏ người dùng trong *domain*. Như vậy phải thiết lập sao cho anh ta chỉ có thể thêm hay bớt người dùng trong OU của phòng đó mà thôi.

Domains

❖ *Domain* (miền) là một đơn vị chủ chốt trong cấu trúc logic của *Active Directory services*.

❖ Tất cả các *objects* trên mạng trong *Active Directory* đều tồn tại trong một *domain* nhất định. Mỗi *domain* có thể bao gồm đến khoảng 1 triệu *objects*.

❖ *Domain* hoạt động như một đường biên an toàn cho mạng. Người quản trị *domain* chỉ được quyền quản lý các *objects* trong *domain* đó mà thôi. Mọi chính sách bảo mật (*security polices*) và thiết lập bảo mật (*settings*) như các quyền quản trị, các chính sách bảo mật, các danh sách kiểm soát truy nhập (*Access Control Lists -ACLs*) được lập riêng cho mỗi *domain* và không thể có tác dụng đối với các *domain* khác.

❖ Mỗi cơ quan hay cơ sở kinh doanh vừa và nhỏ được thiết lập thành một *domain*.

❖ Một *domain* thường bao gồm các loại máy tính sau:

- **Các máy Domain controllers** chạy *Windows 2000 Server:* Mỗi *domain controller* lưu giữ và duy trì một bản copy cơ sở dữ liệu thư mục (*directory*) của *domain*.
- **Các máy chủ thành viên (Member servers)** chạy *Windows 2000 Server:* Là các máy chủ Windows 2000 Server không được cấu hình như một *domain controller*. Máy chủ thành viên không chứa thông tin thư mục và không thể xác nhận người dùng, chúng có chức năng cung cấp các tài nguyên sử dụng chung như các *shared folders* hoặc các máy

in.

- **Các máy trạm (Client computers)** chạy *Windows 2000 Professional:* cho phép người dùng truy nhập tới các tài nguyên trong *domain*.

Trong giáo trình này chủ yếu tập trung vào việc thiết lập một *domain*, tuy nhiên chúng ta cũng xem lướt qua khái niệm về *trees* và *forests*.

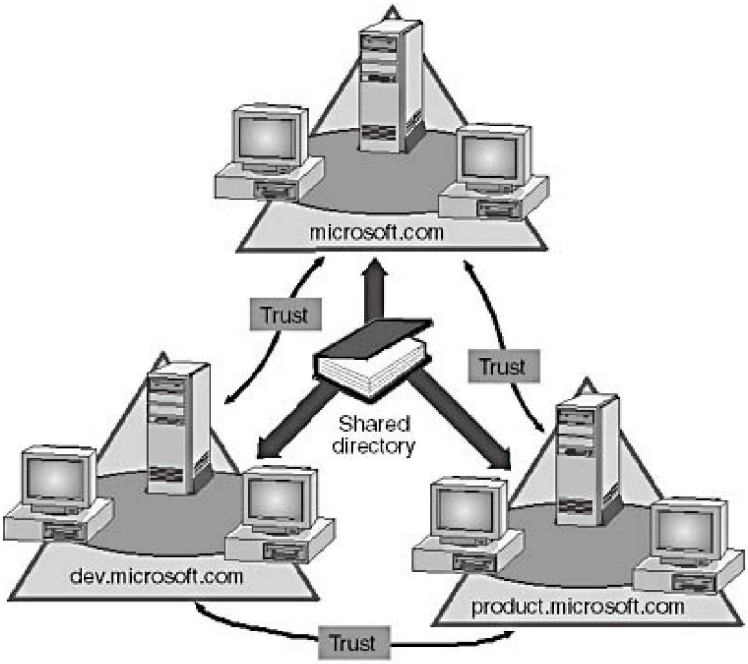
Trees

❖ *Tree* (cây)là một tổ chức phân tầng bao gồm một nhóm của một hay nhiều *domain*. Tất cả các *domain* trong một *tree* có thể chia sẻ sử dụng chung với nhau các thông tin và tài nguyên của *tree* đó.

❖ Mỗi *tree* có một thư mục duy nhất. Trong *directory* này có một catalog chung trong đó tập hợp thông tin của tất cả các *domain* trong *tree* đó và một *Catalog* chung trong đó chứa các định nghĩa của tất cả các *domain objects*.

❖ Mỗi *domain* duy trì một phần của *directory* bao gồm các thông tin tài khoản người dùng trong *domain* đó. Trong một *tree*, một người dùng khi đăng nhập vào 1 *domain* có thể sử dụng các tài nguyên trong các *domain* khác, nếu anh ta đã được uỷ quyền cho có các quyền truy nhập tương ứng.

❖ Tất cả các *domain* trong một *tree* đều sử dụng chung một không gian đặt tên (*namespace*) và một cấu trúc đặt tên phân cấp (*hierarchical naming structure*). *Namespace* là một tập hợp các quy tắc đặt tên tạo ra cấu trúc phân cấp hoặc đường dẫn của một *tree*. Theo chuẩn DNS, tên *domain* của *domain* con phải là tên tương đối của *domain* con đó gộp với tên của *domain* mẹ.



Windows 2000 domain tree

Forests

❖ *Forest* (rừng) là tập hợp của một hay nhiều *trees*.

❖ *Forest* cho phép một tổ chức/doanh nghiệp nhóm mạng của các chi nhánh (*divisions*) của mình hoặc cho phép kết hợp mạng của 2 cơ quan khi những mạng đó không sử dụng chung một sơ đồ đặt tên (*naming scheme*), hoạt động độc lập với nhau, nhưng vẫn cần liên lạc với toàn bộ tổ chức/doanh nghiệp.

1.3. Cấu trúc vật lý của Active Directory

Khi thiết kế một *Active Directory* một điều quan trọng là phải chú ý tới cấu trúc vật lý của nó. Mỗi *domain controller* sẽ có một bản copy của *active directory* của *domain* đó. Mỗi *domain* có thể có nhiều *domain controller*, và người quản trị *domain* có thể thực hiện những thay đổi trên bất cứ *domain controller* nào. Những thay đổi trên một *domain controller* sẽ tự động lặp lại trên tất cả các *domain controller* khác.

Một điểm mạnh của *Active Directory Service* là người dùng không cần phải biết về các đường biên địa lý của mạng. Tuy nhiên người quản trị mạng thì phải hiểu rõ về các đường biên này và sự kết nối giữa chúng. Điều này rất có ý nghĩa đối với mạng WAN. Bởi vì khi có một thay đổi ở một *domain controller*, sự thay đổi này phải lặp lại ở tất cả những *domain controller* khác, trong đó có nhiều cái ở những vùng xa. Điều này sẽ làm ảnh hưởng cho khả năng tải của đường nối của mạng WAN. Để tránh điều này người ta có thể thiết lập các *active directory site* nhỏ và quản trị viên có thể điều phối được sự truyền tải giữa các *site* bằng cách cho phép sự lặp lại các thay đổi ở trên *domain*

controller chỉ xảy ra ngoài giờ cao điểm.

2. THIẾT LẬP MỘT MÁY WINDOWS 2000 DOMAIN CONTROLLER

2.1. Giới thiệu về Windows 2000 Domain Controller

Windows 2000 Controller là một máy tính chạy *Windows 2000 Sever* trong đó có chứa một copy của *active directory database*. Nó được dùng để xác thực người dùng, thực thi các chính sách và định vị các *objects* trong *active directory*.

Windows 2000 Server không được gán chức năng làm *domain controller* khi cài đặt. Chức năng làm *domain controller* sẽ được gán cho ngay sau khi cài đặt xong, hoặc bất cứ thời điểm nào trong tương lai.

2.2. Các yêu cầu của Domain Controller

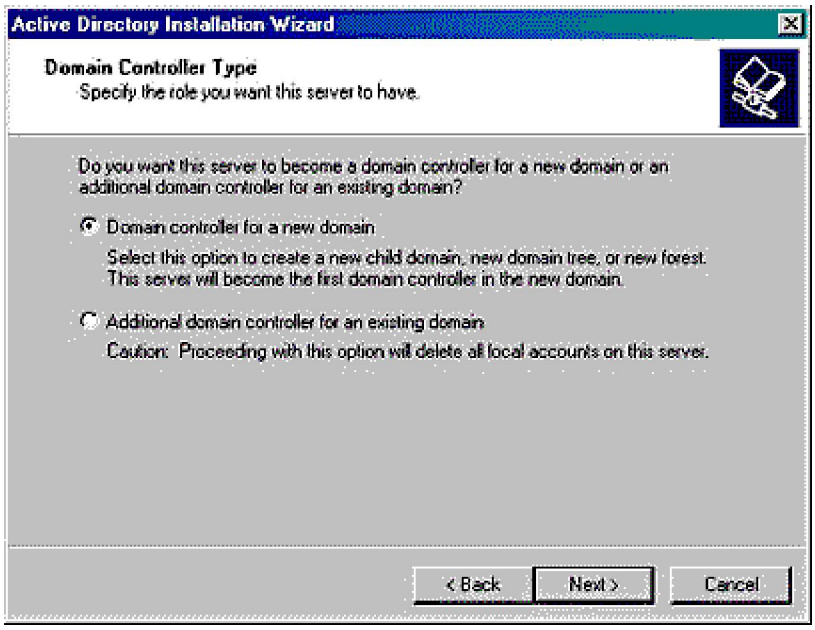
Để nâng cấp một máy chủ *Windows 2000 Server* thành *domain controller*, nó phải có đủ chỗ để chứa *active directory database* và file nhật ký (log file). Nó cũng phải có ít nhất một *partition* được format dưới dạng NTFS bởi *Windows 2000*. Chỗ trống trên ổ cứng để dành cho những dữ liệu này tối thiểu phải là 230 MB.

Ngoài ra *domain controller* còn đòi hỏi phải có một *domain name system (DNS) server*. Tuy nhiên nếu trong môi trường chưa thiết lập sẵn *DNS server*, bạn có thể chọn để cài đặt và thiết lập DNS trên *domain controller* này.

2.3.Thiết lập Domain Controller (cài đặt Active Directory)

Để bắt đầu thiết lập một máy chủ *Windows 2000 Server* thành một *domain controller* chúng ta cần phải chạy chương trình **Configure Your Server Wizard**. Chương trình này được chạy qua menu: **Start\Programs\Administrative Tools\ Configure Your Server.**

- Trên khung bên trái của *wizard* này nhấn chuột vào mục **Active Directory**. Một khung hiển thị với các thông tin về *active directory* và các chức năng mà máy tính có thể làm sẽ xuất hiện. Chúng ta cũng có thể cho chạy chương trình này bằng cách nhấn chuột vào **Strart**, chọn **Run** và đánh vào lệnh **DCPROMO.**
- Nhấn chuột vào mục **Start** để chạy **Active Directory Installation Wizard**.
- Nhấn chuột vào mục **Next** để tiếp tục. Màn hiển thị tiếp theo sẽ yêu cầu chọn để cài đặt máy *domain controller* này vào một *domain* mới, hay thêm *domain controller* này vào một *domain* có sẵn. (xem hình 3.2)



Hình 3.2: *Màn hình để chọn loại domain controler*

- Chọn **Domain controller for a new domain**, sau đó nhấn chuột vào mục **Next** để tiếp tục.

- Màn hiển thị tiếp theo hỏi bạn rằng *domain* mới này là một *domain* gốc hay nó là một *domain* con trong một *tree*, chọn **Create a new domain tree** và nhấn chuột vào **Next**.

- Màn hiển thị tiếp theo hỏi bạn rằng *tree* mới tạo ra thuộc về một *forest* có sẵn, hay nó là *domain* đầu tiên ở trong một *forest* mới. Chọn **Create a new forest of domain tree** và nhấn chuột vào **Next** để tiếp tục.

- Màn hiển thị tiếp theo yêu cầu phải cung cấp tên của *domain*. Tên cung cấp ở đây phải là một tên theo khuôn dạng DNS name, ví dụ *microsoft.com.* Nhấn chuột vào **Next** để tiếp tục.

- Trên màn hiển thị tiếp theo bạn sẽ cung cấp *NetBIOS name* để cho *Windows NT, Windows95, 98 và Windows3.x* sử dụng khi nối vào trong mạng. Trong trường hợp này chọn MICROSOFT (không có .com) để làm *NetBIOS name*. Nhấn chuột vào **Next** để tiếp tục.

- Màn hiển thị tiếp theo hỏi bạn về vùng để chứa *active directory database* và *log file*. *Log file* dùng để đảm bảo khả năng phục hồi của cơ sở dữ liệu. Cố gắng để chọn vùng chứa *log file* trong một ổ cứng khác với ổ cứng chứa cơ sở dữ liệu của *active directory*.

- Tiếp theo bạn sẽ được yêu cầu để chọn vùng chứa *SYSVOL directory*. *SYSVOL directory* chứa các file mà sẽ được lặp lại trong các *domain controller* khác. Thư mục này

bắt buộc phải chứa trong *partition* đã được format theo dạng NTFS 5.0.

- Nếu trong máy chưa được thiết lập một DNS thì màn hiển thị tiếp theo sẽ yêu cầu bạn cài đặt *DNS Server*. Nhấn chuột vào **Next** để tiếp tục.
- Màn hiển thị tiếp theo yêu cầu bạn quyết định các người dùng trong *domain* của bạn chỉ dùng toàn *Windows 2000* hay có cả các phiên bản khác như *Windows NT*.
- Màn hiển thị tiếp theo yêu cầu bạn gõ vào mật khẩu của người quản trị mạng.
- Màn hiển thị cuối cùng thông báo cho bạn một lần cuối cùng những thay đổi mà bạn sẽ thực hiện. Hãy đọc thật kỹ những thay đổi này để đảm bảo bạn biết chính xác những gì mà bạn muốn thay đổi. Sau khi bạn nhấn chuột vào **Next**, máy sẽ copy tất cả file cần thiết vào máy của bạn và thực hiện sự nâng cấp máy này thành *domain controller*.

CHƯƠNG 4

GIAO DIỆN NGƯỜI DÙNG VÀ CÔNG CỤ MMC TRONG WINDOW 2000

---

1. GIỚI THIỆU VỀ MICROSOFT MANAGEMENT CONSOLE (MMC)

MMC là gì?

Trong Window NT các quản trị viên phải nắm vững rất rất nhiều công cụ quản lý. Chỉ một số các công cụ này có thể làm việc từ xa, còn các công cụ khác thường độc lập và các quản trị viên thường phải cài đặt chúng trên các máy riêng rẽ, điều này gây cho các quản trị viên rất nhiều khó khăn. Để khắc phục tình trạng này Microsoft đưa ra công cụ MMC. MMC cung cấp một phương pháp chuẩn để tạo ra, ghi lại và mở các công cụ quản trị mạng, và được gọi là *consoles (cửa sổ điều khiển)*. MMC không cung cấp các chức năng quản lý, nó chỉ tích hợp chúng vào trong một giao diện duy nhất mà thôi. Nó sử dụng các thành phần gọi là snap-in (tạm dịch: Phần ghép thêm) để thực hiện tất cả mọi việc. MMC chỉ cung cấp một giao diện người dùng mà không thay đổi gì cách làm việc của từng snap-in cả.

Các ích lợi của MMC là:

- Bạn chỉ cần tìm hiểu một giao diện duy nhất mà thôi.
- Bạn có thể tích hợp các công cụ của các hãng khác vào trong MMC.
- Bạn có thể xây dựng một cửa sổ ĐK riêng của bạn

MMC cho phép bạn thực hiện các việc sau:

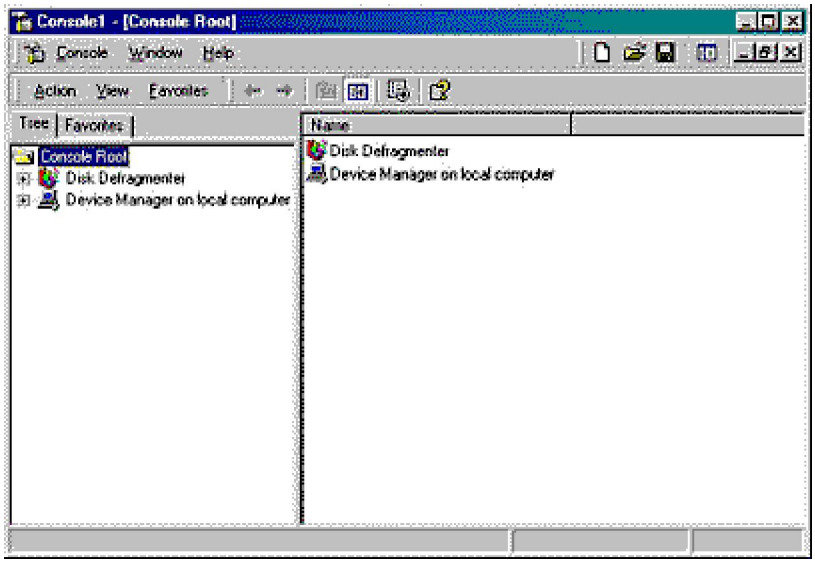
- Các công việc quản lý và khắc phục sự cố.
- Thực hiện sự quản trị tập trung từ một máy tính.
- Thực hiện các công việc quản lý và khắc phục sự cố từ xa.

Các consoles chứa một hay nhiều snap-in. Chúng được ghi như những file với duôi mở rông là .MSC

Các thành phần của MMC

Console Tree and Details Pane

Mỗi cửa sổ điều khiển đều có một console tree, nó hiển thị cấu trúc phân tầng của các snap-in chứa trong cửa sổ điều kiển đó (xem hình 3.1). Điều này cho phép bạn dễ dàng hơn trong việc tìm kiếm các snap-in.



Hình 3.1: *Cửa sổ MMC*

Administrative Tools

Các console thường được ghi trong thư mục Administrator Tools với đường dẫn có thể là:

C:\Documents and Settings\Administrator\Start Menu\Programs\Administrative Tools.

Trong window 2000 professional khi mới cài đặt sẽ không có thư mục Addministrator tools, bạn có thể gọi nó ra bằng cách click Start, point to Settings, click Taskbar & Start Menu, and select the Display Administrative Tools check box on the Advanced tab of the Taskbar And Start Menu Properties dialog box. Tuy nhiên khi bạn khởi chạy MMC và ghi lại các console của mình, Windows 2000 sẽ tự động hiển thị thư mục Administrative Tools cho mỗi người dùng.

Snap-Ins

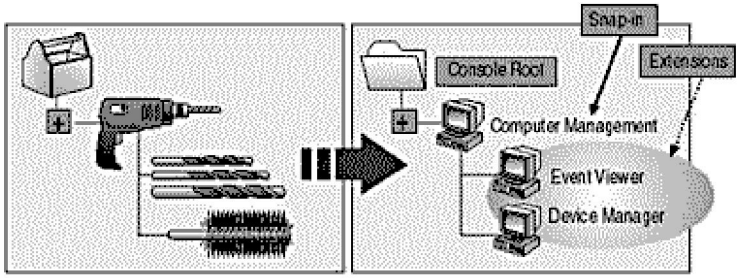
Snap-ins là các công cụ quản trị được đưa và trong một console. Bạn sẽ dùng các snap-in để thực hiện các công việc quản trị mạng. Ví dụ như công cụ DHCP là một snap-in, và Disk Management cũng vậy.

Extension

Extention cơ bản cũng là một snap-in nhưng không thể đứng độc lập một mình trong console, nó phải lệ thuộc vào một snap-in nào đó và bổ sung thêm các chức năng cho snap-in đó.

Hình 3.2 biểu diễn khái niệm về snap-in và extention. Một hộp dụng cụ đựng một máy khoan với một mũi khoan chuẩn. đó chính là snap-in. Nếu bạn thêm các mũi khoan

khác vào hộp, đó chính là các extention.



- **Snap-ins are administrative tools.**
- **Extensions provide additional functionality to snap-ins.**
  - Extensions are preassigned to snap-ins.
  - Multiple snap-ins may use the same extensions.

Hình 3.2: *Snap-ins and extensions*

Các tuỳ chọn của Console

Bạn có thể sử dụng console options để xác định console sẽ hoạt động như thế nào bằng cách chọn lựa console mode. Có 2 laọi console mode là *Author mode* and *User mode*.

Author Mode

Khi bạn ghi một console với Author mode, bạn sẽ có full access đối với tất cả cá chức năng của MMC. Bạn dùng phương pháp này trong trường hợp sau:

- Thêm vào hay xoá đi các snap-ins
- Tạo một cửa sổ điều khiển mới
- Xem tất cả các công cụ của console tree
- Ghi lại các consoles

User Mode

Bạn dùng phương pháp này khi bạn muốn share các MMC của bạn với một số quản trị viên khác. Khi bạn đặt một console với User mode, người dùng sẽ không thể thêm các snap-ins to, xóa snap-ins, hay ghi console. Có 3 dạng user mode, bảng 3.1 miêu tả khi nào thì dùng user mode nào.

Bảng 3.1 *Console User Modes*

Use	**When**
Full Access	Có toàn quyền
Delegated Access, Multiple Windows	Bạn không muốn cho phép người dùng nhìn được cấu trúc cây thư mục hoặc mở cửa sổ console mới Hoặc không cho phép mở nhiều cửa sổ

Delegated Access, Single Window	Không cho phép mở của sổ mới, chỉ cho phép sử dụng 1 của sổ làm việc

2. SỬ DỤNG CONSOLES

Creating Consoles

Bạn có thể tạo một console bằng cách tập hợp các snap-in để thực hiện những chức năng có liên quan. Sau đó bạn có thể thực hiện được các tác nghiệp sau:

- Ghi các console đó lại để sử dụng về sau.
- Phân phối các console đó cho những quản trị mạng khác.
- Sử dụng các console từ bất cứ máy tính nào để thực hiện việc quản trị tập trung và thống nhất.

Để bắt đầu mở một MMC rỗng bạn làm như sau:

1. Click the Start button.
2. Click Run.
3. Type **mmc** in the Open box, and then click OK.

Một cửa sổ console sẽ mở ra, nó chứa một cửa sổ mang tên Console Root. Nó là một cửa sổ rỗng cho phép bạn tạo mới, ghi lại và thao tác nó theo ý bạn. Bảng sau sẽ miêu tả khi nào thì dùng lệnh nào của console menu.

Command	Purpose
New	To create a new custom console
Open	To use a saved console
Save or Save As	To use the console later
Add/Remove Snap-In	To add or remove one or more snap-ins and their associated extensions to or from a console
Options	To configure the console mode and create a custom console

4. Close the MMC window.

Sử dụng Consoles để Quản trị Từ xa

Khi bạn tạo ra các console bạn có thể đặt cho nó chức năng để quản trị từ xa. Chức năng này cho phép bạn có thể thực hiện các tác nghiệp quản lý từ bất cứ máy tính nào. Để thực hiện quản trị từ xa:

- You có thể sử dụng các snap-ins từ computers chạy Windows 2000 Professional hay Windows 2000 Server.
- Bạn phải dùng các snap-ins được thiết kế đặc biệt để quản trị từ xa.

CHƯƠNG 5

THIẾT LẬP VÀ QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG & NHÓM

Quản lý tài khoản là một trong những nhiệm vụ chủ yếu của nhà quản trị Microsoft Windows 2000.Trong chương này chúng ta sẽ khảo sát tài khoản người dùng và tài khoản nhóm. Cách thiết lập và quản lý tài khoản người dùng, tài khoản nhóm và chính sách nhóm.

1. KHÁI NIỆM CHUNG

1.1. Tài khoản người dùng.

❖ Windows 2000 định nghĩa hai loại tài khoản người dùng:

- Tài khoản người dùng vùng: (domain user account) Là tài khoản người dùng được định nghĩa trong Active Directory. Thông qua Single Sign –On, tài khoản người dùng vùng có thể truy cập tài nguyên qua vùng. Tài khoản người dùng vùng được tạo thành trong Active Directory Users And Computer.

- Tài khoản người dùng cục bộ (local uers account) Là tài khoản được định nghĩa trên tài khoản người dùng cục bộ. Tài khoản người dùng cục bộ chỉ được phép truy cập máy tính cục bộ, và họ phải tự chứng thực mình trước khi có thể truy cập tài nguyên mạng. Người ta tạo tài khoản người dung với công cụ Local Users And Groups.

❖ **Tê**n đăng nhập, mật mã và chứng nhận công cộng**:**

- Chú ý tất cả tài khoản người dùng đều được nhận diện bằng *tên đăng nhập* (logon name). Trong Windows 2000 tên này gồm có hai phần:

User name: Tên tài khoản

User domain or workgroup: Vùng hay nhóm làm việc nơi người dùng là thành viên.

- Tài khoản người dùng cũng có mật mã và chứng nhận công cộng phối hợp với chúng. Mật mã (password) là chuỗi chứng thực dành cho tài khoản. Chứng nhận công cộng (public certificate) kết hợp khoá công với khoá riêng để nhận diện người dùng. Với mật mã bạn đăng nhập một cách tương tác .Với chứng nhận công cộng, ban truy cập bằng card thông minh và bộ đọc card thông minh.

❖ SID và tài khoản người dùng:

Mặc dù Windows 2000 hiển thị tên người dùng nhằm mô tả các đặc quyền và quyền truy cập nhưng các thành phần chủ chốt cho tài khoản chính là số nhận diện bảo

mật (Security Identifier -SID). SID là thành phần nhận diện không trùng lặp, được tạo thành đồng thời với tài khoản. SID bao gồm tiền tố của SID vùng, cộng thêm một ID quan hệ không trùng lặp, do chủ ID quan hệ cấp.

Windows 2000 sử dụng những thành phần nhận diện này theo dõi các tài khoản độc lập với tên người dùng. SID phục vụ rất nhiều mục đích. Hai mục đích quan trọng nhất là cho phép bạn dễ dàng thay đổi tên người dùng, và xoá bỏ tài khoản người dùng mà không lo có người khác tìm cách tái tạo tài khoản để truy cập tài nguyên. Khi đổi tên người dùng bạn yêu cầu Windows 2000 ánh xạ một một SID cụ thể thành tên mới. Lúc cần xoá bỏ tài khoản hãy cho Windows 2000 biết SID cụ thể nào đó không còn hợp lệ nữa. Sau đó cho dù bạn tạo tài khoản với cùng tên người dùng, tài khoản mới vẫn không có đặc quyền và quyền truy cập như tài khoản cũ. Lý do là tài khoản mới sẽ có SID mới hoàn toàn.

1.2. Tài khoản nhóm (Group Account)

Ngoài tài khoản người dùng. Windows 2000 còn cung cấp tài khoản nhóm. Bạn dùng nhóm để cấp quyền cho các dạng người dùng tương tự nhau, nhằm đơn giản hoá tác vụ quản trị.

❖ Trong windows 2000 có ba loại nhóm**:**

- Nhóm cục bộ (local group) Là nhóm được định rõ trên máy tính cục bộvà chỉ được dùng trên máy tính cục bộ. Bạn tạo nhóm cục bộ với tiện ích Local Users And Groups.
- Nhóm bảo mật (Sicurity Group) Là nhóm có bộ mô tả bảo mật phối hợp. Bạn định nghĩa nhóm bảo mật trong vùng, dựa vào Active Directory Users And Computers.
- Nhóm phân phối (Ditribution group) Là nhóm được dùng làm danh sách phân phối e-mail. Chúng không có bộ mô tả bảo mật phối hợp. Bạn thiết lập nhóm phân phối trong vùng thông qua Active Directory Users And Computers.

❖ Phạm vi nhóm.

❖ Nhóm có nhiều phạm vi khác nhau (tức những khu vực nơi chúng hợp lệ) bao gồm:

- Nhóm cục bộ vùng (domain local group) Dùng cấp quyền truy cập trong phạm vi vùng đơn. Thành viên nhóm cục bộcó thể chỉ chứa tài khoản (cả người dùng lẫn nhóm) và nhóm xuất xứ từ vùng nơi chúng được định nghĩa.
- Nhóm cục bộ cài sẵn: (built – in local group) Có phạm vi nhóm đặc biệt với với quyền truy cập đặc biệt trong vùng, và nhằm mục đích đơn giản hoá, thường được tham chiếu đến với tên nhóm cục bộ vùng. Đối với nhóm cục bộ cài sắn thì không thể tạo hay xoá bỏ chúng, mà chỉ được phép sửa đổi chúng.

• Nhóm toàn cục (global group) Dùng đẻ cấp quyền truy cập cho đối tượng thuộc vùng bất kỳ trong hệ vùng hay tập hợp hệ vùng cung cấp.Thành viên nhóm toàn cục chỉ có thể bao gồm tài khoản và nhóm xuất xứ từ vùng nơi chúng được định nghĩa.

• Nhóm tổng thể (universal group) Dùng để cấp quyền truy cập trên bình diện rộng khắp hệ vùng hay tập hợp hệ vùng. Thành viên nhóm tổng thể bao gồm tài khoản và nhóm xuất xứ từ vùng bất kỳ thuộc hệ vùng hay tập hợp hệ vùng.

❖ *SID và tài khoản nhóm*

• Cũng như với tài khoản người dùng, Windows 2000 dùng SID giám sát tài khoản nhóm. Điều này có nghĩa là bạn không thể huỷ bỏ tài khoản nhóm, tái tạo nó, rồi hy vọng tất cả đặc quyền và quyền truy cập vẫn còn được bảo toàn. Nhóm mới sẽ có ID mới, nhưng sẽ mất sạch quyền và quyền truy cập thuộc nhóm cũ.

1.3. Tài khoản người dùng và nhóm mặc định

Khi cài đặt Windows 2000, hệ điều hành cài các tài khoản người dùng và nhóm mặc định. Những tài khoản này được thiết kế nhằm cung cấp cơ cấu cơ bản cần thiết để phát triển mạng. Có ba loại tài khoản mặc định:

• Predefined (định trước) Tài khoản nhóm và người dùng được cài cùng với hệ điều hành (như tài khoản Administrator, Guest).

• Built In (cài sẵn) Tài khoản nhóm và tài khoản người dùng được cài cùng với hệ điều hành, chương trình ứng dụng, và dịch vụ mạng (Local System,....).

• Implicit (ngầm định) Những nhóm đặc biệt được tạo khi truy cập tài nguyên mạng.

❖ Nhóm cài sẵn.

Nhóm cài sẵn (built - in) được cài theo máy phục vụ và trạm làm việc của Windows 2000. Hãy dùng nhóm cài sẵn cấp cho người dùng các đặc quyền và quyền truy cập nhóm, bằng cách kết nạp người dùng vào nhóm. Nhóm cài sẵn cụ thể nào đó có khả dụng hay không phụ thuộc vào cấu hình hiện hành của hệ thống.

❖ Nhóm định trước**.**

Nhóm định trước (predefined) được cài đặt với vùng Active Directory, dùng để cấp quyền truy cập cho người dùng, máy tính và nhóm khác. Thủ tục quen thuộc là kết nạp người dùng vào nhóm. Nhóm định trước bao gồm nhóm cục bộ vùng, nhóm toàn cục và nhóm tổng thể. Nhóm định trước cụ thể có khả năng hay không còn phụ thuộc vào cấu hình của vùng.

❖ Nhóm ngầm định và Identity đặc biệt

Trong Windows NT, nhóm ngầm định (implicit group) được chỉ định ngầm trong

tiến trình đăng nhập, và dựa vào cách thức người dùng truy cập mạng. Lấy ví dụ, nếu người dùng truy cập tài nguyên thông qua quy trình đăng nhập tương tác, anh ta sẽ tự động trở thành thành viên của nhóm Interactive. Trong Windows 2000, phương pháp dựa trên thư mục đối tượng dẫn đến cấu trúc thư mục làm thay đổi các nguyên tắc ban đầu của nhóm ngầm định. Mặc dù vẫn không thể xem xét quan hệ thành viên của các Identity đặc biệt, nhưng bạn lại được ấn định quan hệ thành viên nhóm ngầm định cho người dùng, nhóm, và máy tính.

Để phản ánh vai trò mới, nhóm ngầm định còn được gọi là các Identity đặc biệt. Đây là một dạng nhóm có quan hệ thành viên được tự động hiểu ngầm, như trong tiến trình đăng nhập, hoặc được ấn định rõ ràng thông qua quyền truy cập bảo mật. Tương tự như các nhóm mặc định khác, tính khả dụng của một nhóm ngầm định phụ thuộc vào cấu hình hiện hành.

2. THIẾT LẬP VÀ QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG

Một trong những tác vụ quan trọng bậc nhất của nhà quản trị mạng là tạo tài khoản người dùng, trong phần này sẽ hướng dẫn cụ thể cách thực hiện tác vụ này. Khi mở tài khoản người dùng, bạn sẽ dùng đến những công cụ quản trị tài khoản chủ yếu sau đây:

❖ Active Directory Users And Computer, được thiết kế để quản trị tài khoản khắp vùng Active Directory.

❖ Local Users And Group, được thiết kế để quản trị tài khoản trên máy tính cục bộ.

2.1. Cấu hình và tổ chức của tài khoản người dùng

Khía cạnh quan trọng nhất của thủ tục tạo tài khoản là cấu hình và tổ chức của tài khoản. Không có chính sách thích hợp, bạn sẽ nhanh chóng nhận thấy bạn phải tạo lại tài khoản người dùng. Vì thế trước khi tạo tài khoản, bạn hãy xác định những chính sách sẽ dùng để lập cấu hình và tổ chức.

2.1.1. Chính sách tên tài khoản

Chính sách quan trọng nhất cần ban hành là phương pháp đặt tên tài khoản.Tài khoản người dùng có tên hiển thị (display name) và tên đăng nhập (logon name). Tên hiển thị (tức là tên đầy đủ) là tên hiển thị trước người dùng và tên tham chiếu trong phiên làm việc của người dùng. Tên đăng nhập là tên dùng để dăng nhập vùng.

❖ Quy tắc dành cho tên hiển thị

Trong Windows 2000 tên hiển thị thường là chuỗi ghép nối từ tên và họ, nhưng bạn có thể gán chuỗi bất kỳ, tên hiển thị phải tuân theo quy tắc sau:

- Tên hiển thị cục bộ không được phép trùng lặp trên trạm làm việc.

- Tên hiển thị toàn cục không được phép trùng lặp trong toàn vùng.
- Tên hiển thị phải ngắn hơn **64 kí tự.**
- Tên hiển thị có thể chứa ký tự chữ - số và ký tự đặc biệt.

❖ Quy tắc dành cho tên đăng nhập

- Tên đăng nhập không được phép trùng lặp trên trạm làm việc, tên đăng nhập toàn cục không được phép trùng lặp trong toàn vùng.
- Tên đăng nhập có thể dài tối đa 104 kí tự. Tuy nhiên đặt tên đăng nhập dài quá 64 ký tự là làm việc không thiết thực.
- Tên đăng nhập trong Windown NT từ 4.0 trở về trước được đặt cho mọi tài khoản, mặc định được ấn định ở 20 kí tự đầu của tên đăng nhập Windowns 2000. Tên đăng nhập Windows NT từ 4.0 trở về trước không được phép trùng lặp trong toàn vùng.
- Người dùng đăng nhập vùng từ máy tinh Windowns 2000, có thể dùng tên đăng nhập Windowns 2000 hay tên đăng nhập Windowns NT từ 4.0 trở về trước, bất chấp chế độ vận hành của vùng.
- Tên đăng nhập không thể chứa một số ký tự xác định:

" / \ []: ; | =, + * ? <>

Tên đăng nhập có thể chứa ký tự đặc biệt bao gồm ký tự trắng, dấu chấm, dấu gạch ngang, và dấu gạch dưới. Nhưng sẽ chẳng khôn ngoan chút nào khi sử dụng ký tự trắng trong tên tài khoản.

❖ Phương pháp đặt tên

Bạn thấy hầu hết tổ chức nhỏ có khuynh hướng đặt tên đăng nhập theo tên hoặc họ của người dùng. Nhưng trong công ty có thể có nhiều người trùng tên. Vì thế, thay vì phải chỉnh sửa phương pháp đặt tên đăng nhập khi gặp rắc rối, ngay từ bây giờ hãy chon phương pháp đặt tên thích hợp nhất và yêu cầu các nhà quản trị khác dùng phương pháp đó. Đối với việc đặt tên tài khoản bạn phải áp dụng một thủ tục nhất quán, hạn chế tình trạng trùng tên. Theo đúng những nguyên tắc này bạn sẽ có các phương pháp đặt tên sau đây:

- Tên và chữ tắt của họ: Kết hợp tên của người dùng với chữ đầu tiên của họ để hình thành tên đăng nhập. Tuy nhiên phương pháp này không thiết thực ở các tổ chức lớn.
- Chữ viết tắt của tên và họ: Kết hợp chữ cái đầu tiên của tên và họ để hình thành tên đăng nhập. Phương pháp này không thiết thực với các tổ chức lớn.
- Chữ tắt của tên, chữ tắt tên lót, và họ: Kết hợp chữ cái đầu tiên của tên, chữ cái đầu tiên của tên lót và họ để tạo tên đăng nhập.
- Chữ tắt tên chữ tắt tên lót và năm ký tự đầu tiên của họ.

• Tên và họ Tên đăng nhập là sự kết hợp giữa tên và họ của người dùng. Muốn phân cách tên, có thể dùng ký tự gạch dưới (_) hay gạch nối(-)

2.1.2. Mật mã và chính sách tài khoản

Tài khoản Windows 2000 dùng mật mã và chứng nhận công cộng để phê chuẩn yêu cầu truy cập tài nguyên mạng ở đây ta tập trung thảo luận về mật mã.

❖ Mật mã an toàn

Mật mã là chuỗi ký tự có phân biệt chữ hoa và chữ thường, dài tối đa 104 ký tự với dịch vụ Active Directiry, và tối đa 14 ký tự với Windows NT Security Manager. Các ký tự hợp lệ cho cho mật mã là chữ, số, ký hiệu. Khi ấn định mật mã cho tài khoản, Windows 2000 lưu mật mã theo dạng thức mã hoá trong cơ sở dữ liệu tài khoản.

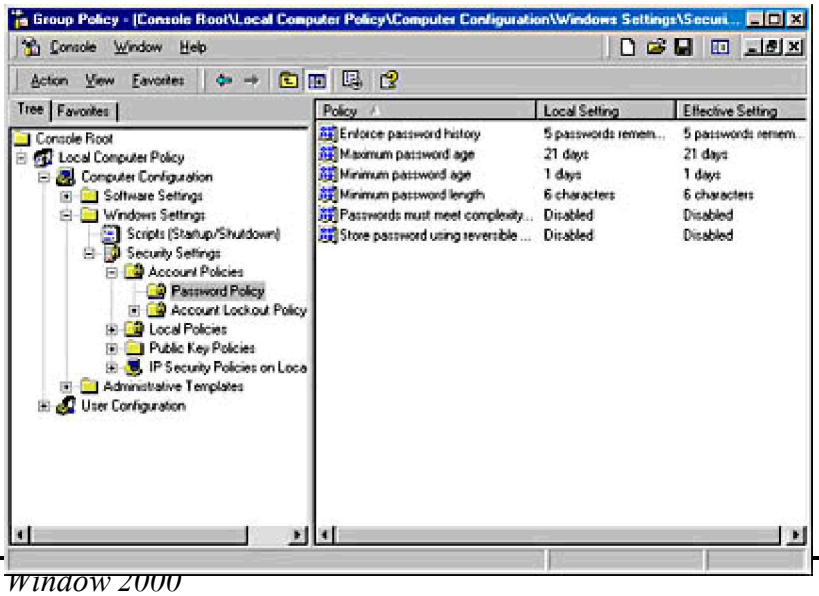
Nhưng, nếu chỉ có mật mã không thì chưa đủ. Bí quyết giúp ngăn ngừa tình trạng truy cập tài nguyên một cách bất hợp pháp là sử dụng *mật mã an toàn (secure password)*. Điểm khác biệt giữa mật mã trung bình và mật mã an toàn là rất khó giải đoán và bẻ khoá. Để mật mã trở lên khó giải đoán, hãy kết hợp mọi kiểu chữ khả dụng bao gồm chữ thường, chữ hoa, chữ số, kí hiệu.

❖ Thiết lập chính sách tài khoản

Chúng ta có thể áp dụng chính sách nhóm ở nhiều cấp độ khác nhau trong phạm vi cấu trúc mạng. Phần này sẽ trình bày ở phần sau. Một khi đã truy cập địa điểm chứa chính sách nhóm, cần sử lý theo các bước sau để ban hành chính sách tài khoản:

1. Truy cập mục Account Policies ở khung bên trái (xem hình sau). Mở rộng Computer Configuration tiếp đến là Windows Settings, sau cùng đến Security Settings.

2. Lúc này bạn có thể quản lý chính sách tài khoản thông qua Password Policy, Account Lockout Policy, và Kerberos Policy.

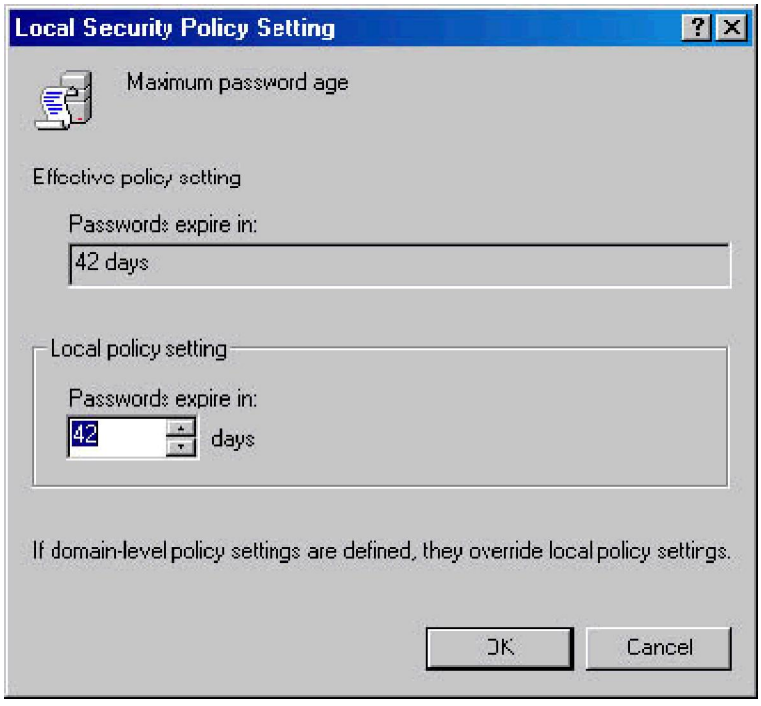


Hình 7.1: *Thiết lập chính sách cho mật mã và sủ dụng tài khoản thông qua Account Policies. Khung bên trái hiển thị tên của máy tính hay vùng đang được lập cấu hình. Hãy kiểm tra nhằm đảm bảo đây là tài nguyên mạng thích hợp để lập cấu hình.*

Thiết lập chính sách cho mật mã và sử dụng tài khoản thông qua Account Policies. Khung bên trái hiển thị tên của máy tính hay vùng đang được lập cấu hình. Hãy kiểm tra nhằm đảm bảo đây là tài nguyên mạng thích hợp để lập cấu hình.

3. Muốn lập cấu hình chính sách, bạn nhấp đúp mục nhập tương ứng, hoặc nhấp nút phải Mouse vào đó và chọn Security mở hộp thoại thuộc tính chính sách.

4. Đối với chính sách cục bộ, hộp thoại Propesrties tương tự như hộp thoại được minh hoạ trong Hình vẽ . Chính sách thực tế (effective policy) dành cho máy tính hiển thị, nhưng không thay đổi được. Tuy nhiên, bạn được phép thay đổi các xác lập chính sách cục bộ. Hãy lập cấu hình chính sách cục bộ dựa vào những trường cho sẵn. Đối với chính sách cục bộ bạn bỏ qua những bước còn lại, vì chúng chỉ áp dụng cho chính sách nhóm toàn cục.



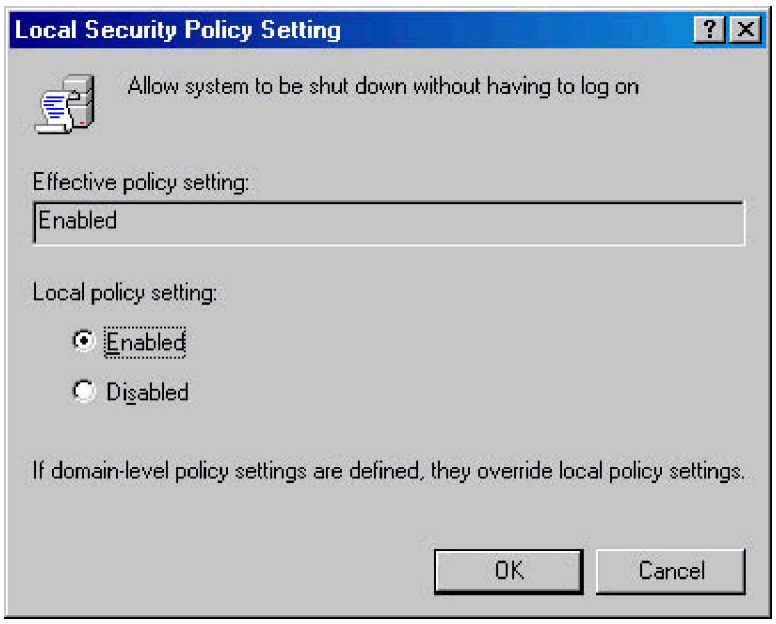
Hình 7.2*: Với chính sách cục bộ, bạn có dịp xem cả chính sách thực tế lẫn chính sách cục bộ*

5. Đối với site, vùng, đơn vị tổ chức, hộp thoại Properties tương tự hộp thoại minh

hoạ ở hình sau

6. Mọi chính sách hoặc được định rõ hoặc không. Có nghĩa, chúng được lập cấu hình để sử dụng hoặc không. Chính sách nào không được định rõ ở thư mục hiện hành có thể được kế thừa từ thư mục chứa khác.

7. Chọn hoặc xoá chọn Define This Policy Setting để xác định chính sách có được định rõ hay không.



Hình 7.3: *Định rõ và lập cấu hình chính sách nhóm toàn cục thông qua hộp thoại Properties*

2.1.3. Lập cấu hình chính sách tài khoản

Có ba loại chính sách tài khoản: chính sách mật mã, chính sách khoá tài khoản, và chính sách Kerberos.

Lập cấu hình chính sách mật mã

Chính sách mật mã được ban hành nhằm mục đích bảo vệ mật mã và bao gồm:

- Enforce Password History: Là chính sách ấn định chu kỳ tái sử dụng mật mã.
- Maximum Password Age: Là chính sách quyết định thời gian người dùng có thể lưu giữ mật mã trước khi buộc phải thay đổi. Mục đích buộc người dùng phải thay đổi mật mã theo định kỳ. Xác lập mặc định là 42 ngày và khoảng giá trị cho phép là từ 0-999.
- Minimum Password Age: Đây là chính sách quyết định thời gian người dùng người dùng *phải* lưu giữ mật mã trước khi thay đổi. Bạn dùng xác lập này ngăn không cho người dùng "đánh lừa " hệ thống mật mã bằng cách gõ vào mật mã mới rồi thay đổi

ngay thành mật mã cũ.

- Minimum Password Length: ấn định số lượng ký tự tối thiểu cho mật mã. Xác lập mặc định là cho phép để trắng mật mã (không gõ ký tự nào cho mật mã).

- Password Must Meet Complexity Requirement: Ngoài chính sách tài khoản và chính sách mật mã cơ bản, Windows 2000 còn cung cấp nhiều phương tiện giúp kiểm soát mật mã chặt chẽ hơn. Những phương tiện này khả dụng trong *bộ lọc mật mã* (password filter), vốn có thể cài đặt trên máy điều khiển vùng.

- Store Password using Reversible Encryption: Mật mã được mật mã trong cơ sở dữ liệu. Hiệu ứng mã hoá này không thể xoá bỏ một cách thông thường. Nếu muốn có thể giải mã, bạn kích hoạt *Store Password Using Reversible Encryption For All Users In The Domain.* Mật mã sau đó sẽ được lưu ở dạng mã hoá có thể giải mã, và được phục hồi trong tình tình huống khẩn cấp. Bất kỳ nhà quản trị nào cũng có thể thay đổi mật mã của người dùng.

Lập cấu hình chính sách tài khoản

Chính sách tài khoản chi phối cách thức và thời điểm khoá tài khoản bên ngoài vùng hay hệ thống vùng cục bộ. Có ba chính sách tài khoản:

- Account Lockout Threshold: ấn định số lần cố gắng đăng nhập cố gắng thực hiện trước khi tài khoản bị khoá. Nếu quyết định áp dụng chính sách khoá tài khoản, bạn nên chọn cho chính sách này một giá trị cân bằng giữa nhu cầu bảo vệ tài khoản trước kẻ xâm nhập bất hợp pháp với nhu cầu người dùng gặp khó khăn khi truy cập tài khoản của họ.

- Account Lockout Duration: Nếu có kẻ vi phạm chính sách tài khoản Account Lockout Duration sẽ ấn định khoảng thời gian khoá tài khoản, thay đổi trong khoảng 1-99999 phút, hoặc không ấn định thời gian này, bằng cách duy trì thời gian này bằng 0.

- Reset Account Lockout Threshold After: Mỗi một lần có một nỗ lực đăng nhập thất bại, Windows 2000 lại nâng giá trị ngưỡng theo dõi số lần đăng nhập bất thành lên. *Reset Account Lockout Threshold After* quyết định thời hạn duy trì ngưỡng khoá tài khoản.

Lập cấu hình chính sách Kerberos:

Kerberos phiên bản 5 là cơ chế chứng thực chính dùng trong vùng Active Directory nhằm kiểm tra nhận dạng của người dùng và các dịch vụ mạng, Kerberos sử dụng "vé dịch vụ" (service ticket) và "vé người dùng" (user ticket). Những vé này chứa dữ liệu được mã hoá, xác nhận nhận dạng của người dùng hay dịch vụ.

Bạn chi phối thời hạn, gia hạn và ban hành vé thông qua chính sách sau đây:

- Enforce User Logon Restrictions: Là chính sách đảm bảo thực thi mọi áp đặt lên tài khoản người dùng. Lấy ví dụ, nếu giới hạn ở số giờ đăng nhập, chính sách này sẽ

buộc phải thi hành giới hạn đó. Mặc định *Enforce User Logon Restrictions* được chọn và rất ít khi bị vô hiệu hoá.

- Maximum Life time: *Maximum Lifetime For Sevice Ticket* và *Maximum Lifetime For User Ticket* ấn định thời hạn hợp lệ tối đa cho vé dịch vụ hoặc vé người dùng cụ thể. Mặc định, vé dịch vụ có thời hạn hợp lệ tối đa là 41760 phút, còn với vé người dùng là 720 giờ.

- Maximum Tolerance: *Maximum Tolerance For Computer Clock Synchronization* là một trong số vài chính sách Kerberos có thể cần thay đổi. Mặc định máy tính vùng phải đồng bộ với nhau trong vòng 5 phút. Ngược lại, máy điều khiển vùng sẽ không chứng thực được nếu có người dùng ở xa truy cập vùng mà không chỉnh đồng hồ hệ thống theo đồng hồ mạng. Bạn nên điều chỉnh giá trị này với khoảng giá trị khả dụng là 0-99999.

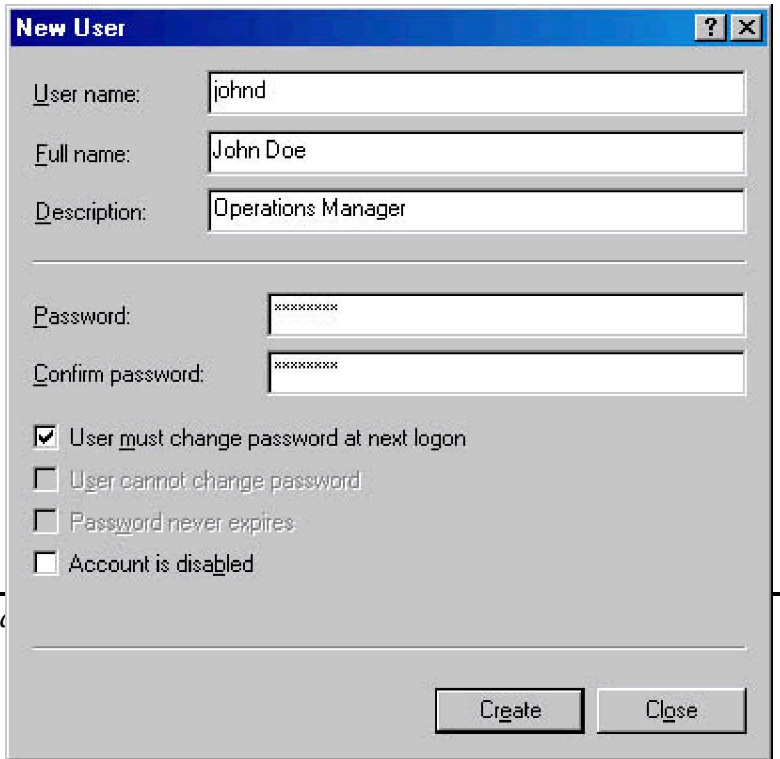
2.2. Thiết lập tài khoản người dùng

Bạn phải thiết lập tài khoản người dùng cho người dùng nào muốn sử dụng tài nguyên mạng. Tài khoản người dùng trong domain được thiết lập thông qua tiện ích Active Directory Users And Computers. Dùng tiện ích Local Users And Groups tạo tài khoản người dùng cục bộ.

2.2.1. Thiết lập tài khoản người dùng vùng

Thông thường có hai cách thiết lập tài khoản người dùng mới:

❖ Tạo tài khoản người dùng hoàn toàn mới: Mở cửa sổ Users and Computers trong thư mục Active Directory, nhấp phải vào Uer → New User. Hộp thoại New Object- User Wirard hiển thị. (Hình7.4) . Khi thiết lập tài khoản mới các xác lập hệ thống mặc định được sử dụng.



Hình 7.4: *Lập cấu hình tên đăng nhập và tên hiển thị của người dùng*

❖ Tạo tài khoản mới trên tài khoản hiện có: nhấp nút phải chuột vào tài khoản người dùng cần sao chép trong Active Directory User And Computer, rồi chọn Copy. Một Copy Object –User Wizard khởi động, về cơ bản cũng tương tự như hộp thoại New User. Tuy nhiên, khi tạo bản sao của tài khoản, tài khoản mới sẽ thu nhận hầu hết xác lập môi trường từ tài khoản hiện có.

Lúc cửa sổ New Object- User hoặc Copy Object-User khởi động bạn thiết lập tài khoản bằng cách:

1. Như hiển thị ở hình trên (Hình 7.4), hộp thoại đầu tiên của Wilzard cho phép lập cấu hình tên đăng nhập và tên hiển thị của người dùng .

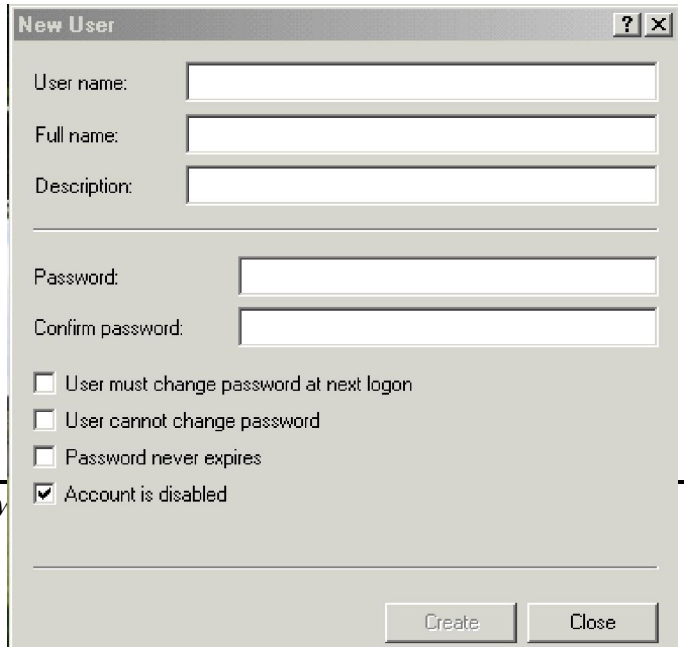
2. Gõ tên người dùng vào trường thích hợp. Họ tên người dùng hình thành Full name, tức tên hiển thị của người dùng.

3. Thực hiện thay đổi cho trường Full name, nếu cần. Tuỳ thuộc vào chính sách đặt tên.

4. Gõ tên đăng nhập của người dùng vào trường User Logon Name. Dùng danh sách xổ xuống chọn ra vùng sẽ phối hợp với tài khoản, Việc làm này giúp hình thành tên đăng nhập hoàn chỉnh.

5. 20 ký tự đầu tiên của tên đăng nhập được dùng để ấn định tên đăng nhập ở Windows NT 4.0 trở về trước. Tên này không được phép trùng lặp trong vùng. Nếu cần hãy thay đổi tên đăng nhập của Windows NT 4.0 trở về trước.

6. Nhấp Next. Tiếp đến ấn định mật mã của người dùng thông qua hộp thoại minh hoạ ở (Hình 7.5).



Hình 7.5: *Lập cấu hình mật mã của người dùng*

Những tuỳ chọn ở đây bao gồm:

- Password (Mật mã tài khoản): Mật mã này phải theo đúng các quy ước đã đặt ra trong chính sách mật mã.
- Confirm Password: Giúp đảm bảo bạn đã gõ đúng mật mã. Chỉ việc gõ lại mật mã để xách nhận nó.
- User Must Change Password At Next Logon: Nếu chọn thì người dùng phải thay đổi mật mã mỗi khi đăng nhập.
- User Cannot Change Password: Nếu được chọn người dùng không được phép thay đổi Password.
- Password Never Expires Đánh dấu chọn, mật mã dành cho tài khoản này sẽ không bao giờ hết hạn. Đây là xác lập dành quyềnvới chính sách tài khoản cục bộ.
- Account Is Disabled Đánh dấu vào tài khoản sẽ bị vô hiệu hoá và không sử dụng được.

7. Nhấp Next, nhấp tiếp Finish để tạo tạo tài khoản trường hợp có sai sót thông điệp báo lỗi hiển thị, bạn phải dùng nút Back gõ lại thông tin vào hộp thoại User Name và Password, nếu cần.

2.2.2. Tài khoản người dùng cục bộ

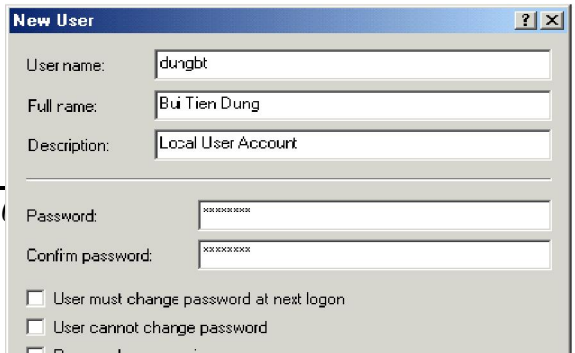
Với tác vụ này, bạn sử dụng tiện ích Local User And Group theo các bước sau:

1. Chon Start -> Program -> Administrative Tools -> Computer Management. Hoặc chọn Computer Management từ thư mục Administrative Tools.

2. Nhấp nút phải chuột vào mục nhập Computer Management bên khung trái và chọn Connect To Another Computer từ Menu tắt. Chọn tiếp hệ thống có tài khoản cục bộ cần quản lý. Máy điều khiển vùng không có người dùng và nhóm cục bộ.

3. Mở rộng System Tools (nhấp dấu +), chọn Local User And Groups.

4. Nhấp nút phải mouse vào User và chon New -> User. Hộp thoại New User hiển thị



Hình7.6: *Lập cấu hình tài khoản người dùng cục bộ có nhiều điểm khác với lập cấu hình tài khoản người dùng vùng.*

Những tuỳ chọn ở đây bao gồm:

- Username: tên đăng nhập của tài khoản người dùng, phải tuân theo đúng quy ước do chính sách tên cục bộ đặt ra.
- Full Name: Họ tên đầy đủ của người dùng
- Description: Thông tin mô tả người dùng, thông thường bạn gõ chúc vụ và bộ phận mà người dùng trực thuộc.
- Password Mật mã cho tài khoản. Phải theo đúng quy ước do chính sách mật mã đặt ra.
- Confirm Password: Giúp đảm bảo bạn đã gõ đúng mật mã. Chỉ việc gõ lại mật mã để xách nhận nó.
- User Must Change Password At Next Logon: Nếu chọn thì người dùng phải thay đổi mật mã mỗi khi đăng nhập.
- User Cannot Change Password: Nếu được chọn người dùng không được phép thay đổi Password.
- Password Never Expires: Nếu bạn chọn mục này thì mật mã dành cho tài khoản này sẽ không bao giờ hết hạn. Đây là xác lập dành quyềnvới chính sách tài khoản cục bộ.
- Account Is Disabled: Đánh dấu vào mục này thì tài khoản sẽ bị vô hiệu hoá và không sử dụng được.

5. Nhấp Create khi hoàn tất việc lập cấu hình cho tài khoản mới

1. Quản lý tài khoản người dùng.

Sau khi tạo tài khoản người dùng chúng ta phải dành nhiều thời gian để quản lý chúng bao gồm các tác vụ sau:

❖ Quản lý thông tin liên hệ:

Active Directory là dịch vụ thư mực (chính xác phải gọi là "dịch vụ danh bạ"). Khi thiết lập tài khoản người dùng, chúng ta có thể có thông tin liên hệ kèm theo. Thông tin này sau đó trở nên khả dụng cho mọi người thuộc hệ vùng hoặc tập hợp thuộc hệ vùng, dùng để tìm kiếm và bổ sung vào Address Book.

- Ấn định thông tin liên hệ:

Bạn ấn định thông tin liên hệ cho tài khoản người dùng như sau:

1. Nhấp đúp tên đăng nhập của người dùng trong Active Directory User And Computers. Như thường lệ hộp thoại thuộc tính tài khoản xuất hiện.

2. Nhấp tab General (Hình7.7). Sử dụng các tuỳ chọn sau đây:

First Name, Initials, Last Name Định họ tên đầy đủ của người dùng.

Display Name Định tên hiển thị của người dùng**,** hiện diện ở phiên đăng nhập hay trong Active Directory.

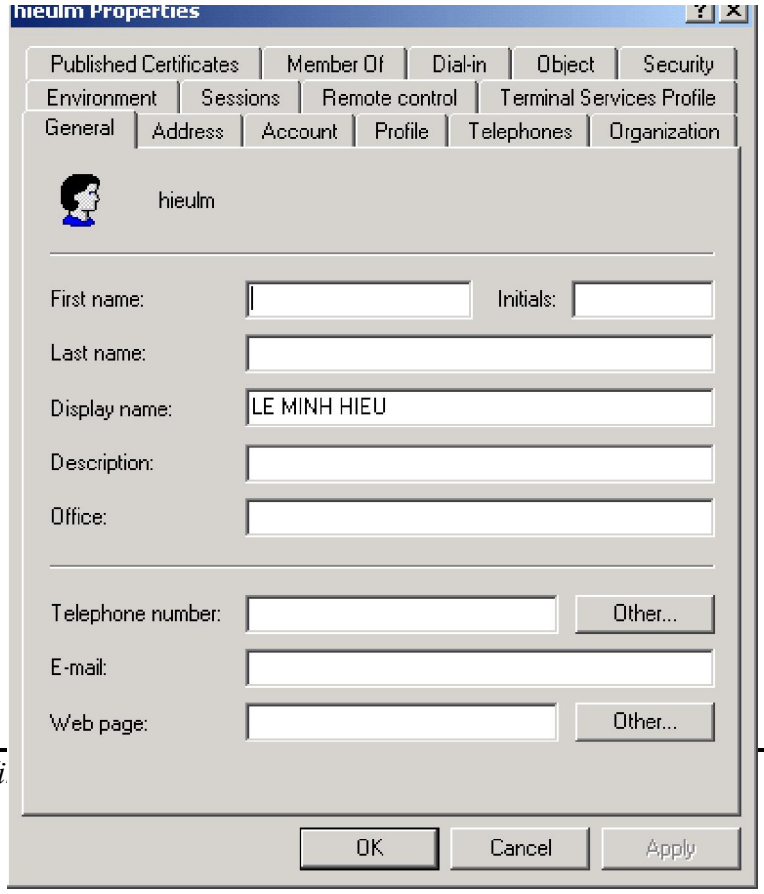
Description Gõ thông tin mô tả về người dùng.

Office Cho biết địa chỉ văn phòng làm việc của user.

Telephone Number Định rõ số điện thoại người dùng. Nếu người dùng có nhiều số điện thoại liên hệ, nhấp Other, gõ thêm số điện thoại phụ vào hộp thoại Phone Number (Others).

E-mail Định địa chỉ mail của user vào đây.

Web Page Định URL (Uniform Resouce Locator) của trang chủ trên Internet hay intranet của công ty.



Hình 7.7: *Lập cấu hình thông tin liên hệ cho người dùng thông qua trang Genaral. Thông tin này sau đó sẽ được dùng trong Address Book và trong các cuộc tìm kiếm.*

3. Chuyển sang trang Address. Định rõ địa chỉ nơi làm việc và nhà riêng của user.

4. Nhấp tab Telephone. Gõ (những) số điện thoại chính sẽ dùng để liên hệ với người dùng.

5. Nếu vẫn còn nhiều số điện thoại khác hãy nhấp nút Others phối hợp với từng loại và gõ thêm số điện thoại vào hộp thoại hiển thị ngay sau đó.

6. Nhấp tab Organization, gõ chức vụ phòng ban của người dùng.

7. Muốn định rõ người chịu trách nhiệm quản lý người dùng, nhấp Change, chọn tên người quản lý từ hộp thoại Select User Or Contact. Khi định rõ người quản lý, tài khoản người dùng sẽ xuất hiện ở dạng báo biểu trực tiếp trong tài khoản của người quản lý.

8. Nhấp OK hoặc Apply để áp dụng thay đổi.

- **Tìm người và đưa thông tin vào Address Book**

Active Directory giúp bạn dễ dàng tổ chức tìm kiếm người trong thư mục, sau đó bổ xung kết quả tìm được vào Address Book. Tác vụ này thường sử dụng cho người dùng thực hiện. Theo các bước sau:

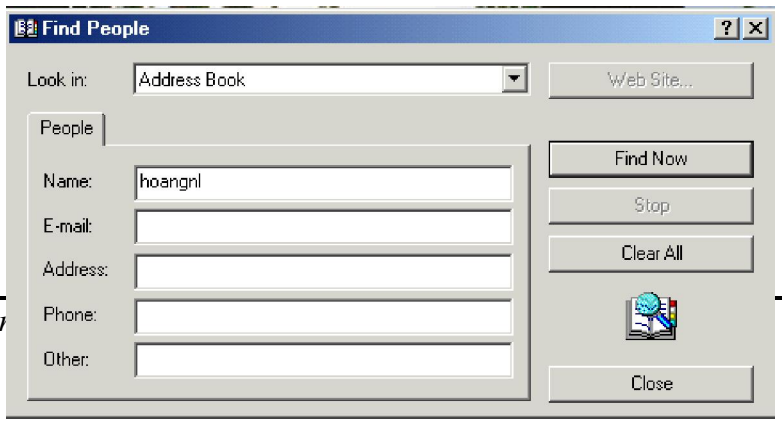
1. Chọn Star -> Seach -> For People mở hộp thoại minh hoạ (*Hình 7.8*)

2. Nhấp hộp thoại danh sách Look In, chọn Active Directory, gõ tên hoặc địa chỉ E-mail của người cần tìm.

3. Nhấp Find Now bắt đầu tìm kiếm. Kết quả so khớp sẽ được hiển thị. Bằng không kết quả không hiển thị.

4. Muốn xem thuộc tính tài khoản, chọn tên hiển thị và nhấp Properties.

5. Chọn tên hiển thị, nhấp Add To Addres Book.

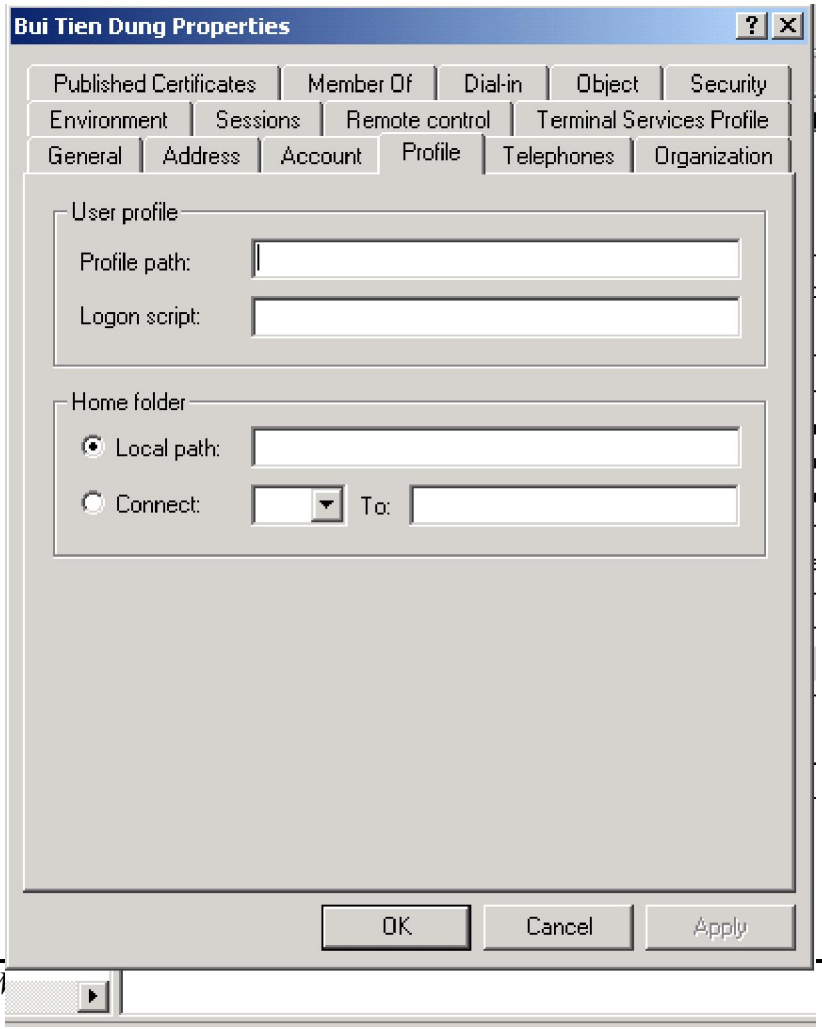


Hình 7.8: *Tìm người trong Active Directory, sau đó đưa kết quả tìm được vào Address Book.*

❖ Ấn định xác lập môi trường của người dùng

Tài khoản người dùng còn có bộ lưu trữ, kịch bản đăng nhập và thư mục cá nhân phối hợp với chúng, muốn lập cấu hình những xác lập tuỳ ý này, bạn nhấp đúng tên hiển thị bất kỳ trong Active Directory And Computers, rồi nhấp tab Profile (Hình 7.9). Trang Profile cho phép xử lý các trường sau đây:

Profile Path Đường dẫn đến bộ truy cập người dùng. Bộ lưu trữ cung cấp xác lập môi trường cho người dùng. Mỗi lần user đăng nhập máy tính, bộ lưu trữ của người dùng này lại được sử dụng nhằm quyết định các các lập Desktop và Control Panel, chính khả dụng của tuỳ chọn menu, của chương trình ứng dụng,.v.v.v.



Hình 7.9: *Tạo bộ lưu trữ người dùng trên trang Profile. Bộ lưu trữ cho phép bạn lập cấu hình môi trường mạng cho người dùng.*

Logon Scrept Đường dẫn đến kịch bản đăng nhập của người dùng. *Kịch bản đăng nhập* (logon Scrept) là tập tin batch, sẽ chạy mỗi lần người dùng đăng nhập. Bạn dùng kịch bản đăng nhập tập hợp những lệnh sẽ được thi hành mỗi khi người dùng đăng nhập.

Local Path Là thư mục do người sử dụng để lưu trữ tập tin. Tại đây, bạn chỉ định một thư mục cụ thể cho tập tin người dùng. Nếu thư mục khả dụng với mạng, người dùng được phép truy cập thư mục từ máy tính bất kỳ trên mạng.

- Biến môi trường hệ thống (*system environment variable*) Thường tỏ ra hữu dụng khi khi bạn tiến hành thiết lập môi trường của người dùng, nhất là lúc làm việc với kịch bản đăng nhập. Bạn sử dụng biến môi trường để định rõ thông tin đường dẫn. Dưới đây là những biến môi trường thông dụng nhất:

  - %***SystemRoot***% Thư mục gốc của hệ điều hành Microsoft Windows 2000, như C:\WIN2000. Hãy dùng biến này với trang Profile của hộp thoại thuộc tính người dùng với kịch bản đăng nhập.

  - %***UserName***% Tên tài khoản đăng nhập, được dùng với trang Profile của hộp thoại thuộc tính người dùng và với kịch bản đăng nhập.

  - %***HomeDrive***% Mẫu tự ổ đĩa của thư mục cá nhân thuộc về người dùng, như C:, dùng với kịch bản đăng nhập.

  - %***HomePath***% Đường dẫn hoàn chỉnh dẫn đến thư mục cá nhân của người dùng, nằm trên ổ đĩa gốc tương ứng. Sử dụng biến này với kịch bản đăng nhập.

  - ***Processor_Architecture%*** Kiến trúc bộ vi sử lý của máy tính, như x86, được dùng với kịch bản đăng nhập

- Kịch bản đăng nhập (logon script) chứa các lệnh sẽ thi hành mỗi lần người dùng đăng nhập. Có thể dùng kịch bản đăng nhập để định giờ hệ thống, đường dẫn ổ đĩa mạng, máy in mạng, .v.v. Mặc dù được phép sử dụng kịch bản đăng nhập để thi hành lệnh nhưng không nên ấn định biến môi trường vào chúng. Các xác lập môi trường do kịch bản định rõ sẽ không được duy trì ở mức người dùng kế tiếp. Cũng không nên định rõ chương trình ứng dụng sẽ chạy ở thời điểm đăng nhập thông qua kịch bản đăng nhập, mà hãy dùng cách đặt lối tắt thích hợp vào thư mục Startup của người dùng. Thông thường, kịch bản đăng nhập có chứa lệnh của Windows 2000. Tuy thế kịch bản đăng nhập có thể là:

- Tập tin Windows Script Host với phần mở rộng .VBS, .JS, hay phần mở rộng hợp lệ khác.
- Tập tin .BAT
- Chương trình có thể thi hành với phần mở rộng .EXE.

• Chỉ định thư mục cá nhân: Windows 2000 cho phép bạn chỉ định *thư mục cá nhân* (home directory) cho từng tài khoản người dùng. Người dùng sử dụng thư mục này để lưu giữ và truy xuất thông tin cá nhân. Nhiều chương trình ứng dụng dùng thư mục cá nhân làm thư mục mặc định cho các hoạt động File Open và Save As, giúp người dùng dễ dàng tìm thấy tài nguyên của mình. Dấu nhắc lệnh cũng sử dụng thư mục cá nhân làm thư mục hiện hành lúc ban đầu. Thư mục cá nhân thường trú trên ở đĩa cứng cục bộ của người dùng, hoặc trên ổ đĩa mạng dùng chung. Trên ổ đĩa cục bộ, chỉ có thể truy cập thư mục từ một trạm làm việc đơn lẻ. Ngược lại bạn truy cập ổ đĩa mạng dùng chung từ máy tính bất kỳ trên mạng, tạo nên môi trường làm việc năng động hơn. Không nhất thiết phải tạo trước thư mục cá nhân của người dùng. Active Directory Users And Computers sẽ tự động tạo cho bạn. Nhưng giả như có rắc rối xảy ra*, Active Directory Users And Computers* sẽ hướng dẫn bạn tạo thư mục.

Cách định rõ thư mục cá nhân cục bộ:

1. Mở hộp thoại Properties dành cho người dùng trong *Active Directory Users And Computers,* nhấp tab Properties .

2. Nhấp nút Properties, gõ đường dẫn vào thư mục cá nhân ở trường phối hợp. Ví dụ: **C:\Home\%UserName%.**

Cách định rõ thư mục cá nhân trên mạng:

1. Vẫn mở hộp thoại thuộc tính của người dùng trong *Active Directory Users And Computers* nhấp tab Profile.

2. Nhấp nút tab Connect, chọn mẫu từ ổ đĩa của thư mục cá nhân. Nhằm đảm bảo tính nhất quán, nên dùng chung mẫu từ ổ đĩa cho tất cả người dùng. Ngoài ra cũng phải chọn mẫu từ ổ đĩa nào đó không xung đột với ổ đĩa vật lý hay ổ đĩa ánh xạ hiện hành.(ổ Z chẳng hạn.)

3. Gõ đường dẫn hoàn chỉnh đến thư mục cá nhân, dựa vào quy ước UNC như \\GAMMA\USER_DIRS\%UserName%. Mục đích của việc kèm tên máy phục vụ vào đường dẫn là nhằm người dùng có thể truy cập thư mục từ máy tính bất kỳ trên mạng.

❖ Định giới hạn và các tuỳ chọn tài khoản.

Windows 2000 cung cấp nhiều cách giúp kiểm soát và quản lý tài khoản người dùng và khả năng truy cập của họ. Bạn có thể định rõ số giờ đăng nhập, Trạm làm việc

được phép đăng nhập, các đặc quyền quay số,..

- Quản lý số giờ đăng nhập: Trong Windows 2000 cho phép bạn quyết định thời điểm user được phép đăng nhập vào mạng, bằng cách ấn định số giờ đăng nhập mạng hợp lệ. Mục đích để kiểm soát tài khoản người dùng và tăng khả năng bảo mật của hệ thống, ngăn chặn những truy cập bất hợp pháp vào hệ thống. Khi hết thời gian đăng nhập hợp lệ, việc tiếp theo sẽ tuỳ thuộc vào chính sách tài khoản áp dụng cho họ. Thông thường một trong hai tình huống sau đây sẽ xảy ra cho người dùng:

  - **Bắt buộc ngắt kết nối**. Không thể truy cập được tất cả các tài nguyên mạng.
  - **Không bị ngắt kết nối**: Người dùng sẽ không bị ngắt kết nối khi sử dụng hết số giờ đăng nhập. Có điều, Windows 2000 sẽ không cho phép họ thiết lập thêm bất kỳ kết nối nào vào mạng.

Lập cấu hình số giờ đăng nhập:

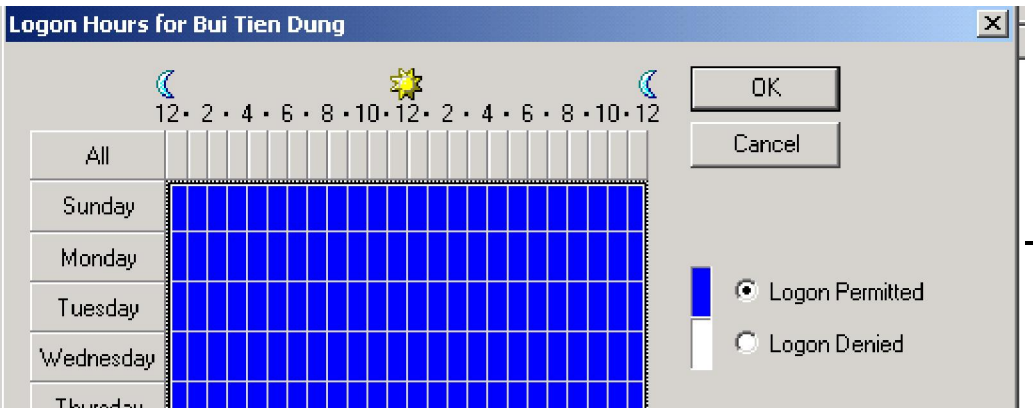
1. Mở hộp thoại thuộc tính người dùng trong Active Directory Users And Computers. Nhấp tab Account.

2. Nhấp nút logon Hours. ấn định khoảng đăng nhập hợp lệ và không hợp lệ, thông qua hộp thoại minh hoạ ở Hình 7.10. Các đặc tính Logon Hours được liệt kê ở bảng 7.1

Trong hộp thoại này, mỗi giờ trong ngày được hiển thị trong một ô có thể bật / tắt. Giờ được phép đăng nhập được biểu thị bằng ô màu đen (Ô được bật) ngược lại giờ bị cấm biểu thị bằng ô màu trắng. Muốn thay đổi xác lập cho giờ cụ thể, bạn nhấp ô tương ứng. Chọn Logon Permitted hoặc Logon Denied.

Bảng 7.1

Đặc tính	Chức năng
All	Cho phép chọn tất cả giai đoạn thời gian
Dãy nút ngày trong tuần	Cho phép chọn toàn bộ số giờ trong tuần cụ thể.
Dãy nút giờ	Cho phép chọn giờ cụ thể cho tất cả các ngày trong tuần
Logon Permitted	ấn định số giờ được phép đăng nhập
Logon Denied	Ấn ®Þnh sè giê bÞ cÊm ®¨ng nhËp



H×nh 7.10: *Ấn định số giờ đăng nhập cho người dùng*

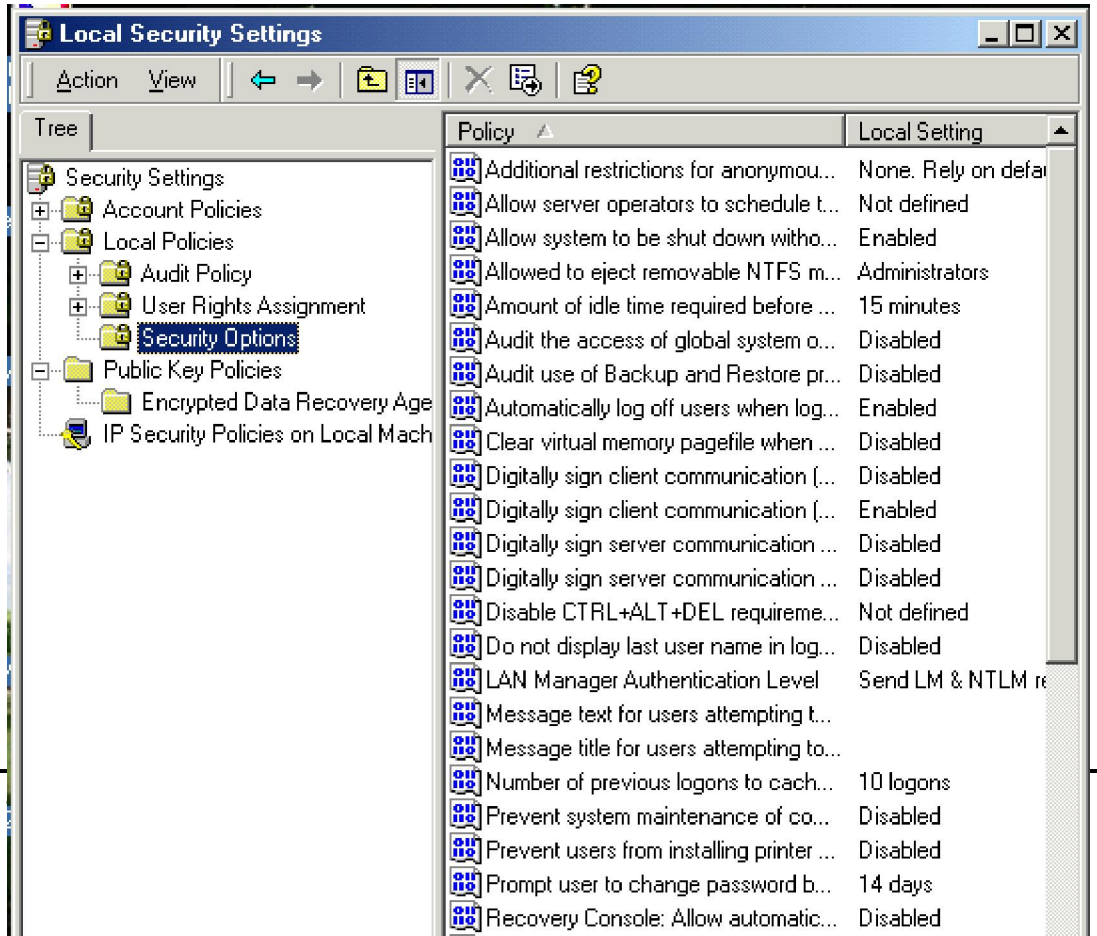
Bắt buộc ngắt kết nối khi hết hạn đăng nhập:

1. Truy cập thư mục chứa chính sách nhóm cần xử lý .

2. Mở rộng Computer Configuration, Windows Settings. Trong Security Settings, mở rộng Local Policies rồi chọn Security Option (Hình 7.11)

3. Nhấp đúp *Automatically Log Off Users When Logon Time Expries*. Hộp thoại Properties dành chochính sách hiển thị.

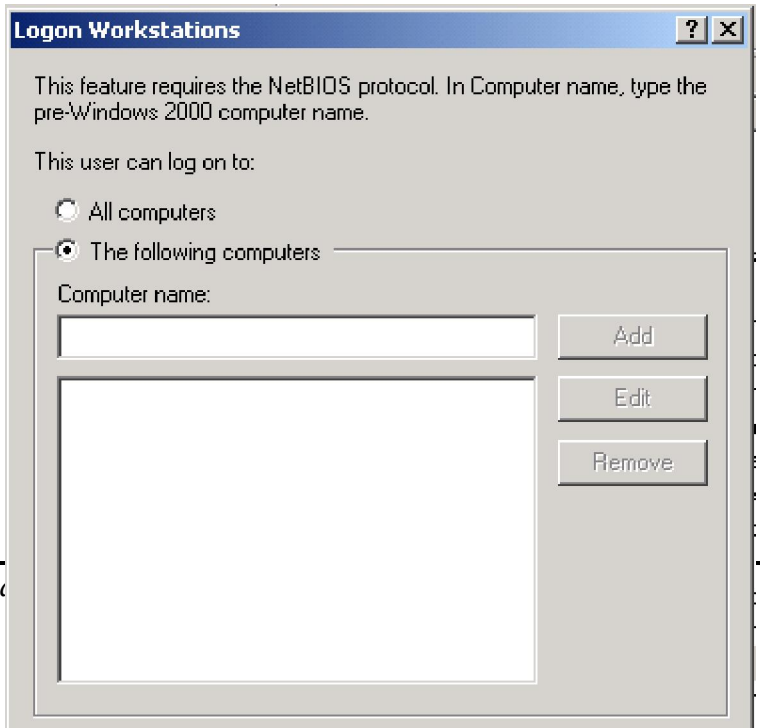
4. Đánh dấu chọn *Define This Policy Setting,* nhấp tiếp Enabledáp dụng chính sách giới hạn số giờ đăng nhập. Nhấp OK.



Hình 7.11: *Truy cập Security Options Trong Policy*.

❖ **Quy định số trạm làm việc cho phép đăng nhập**: Windows 2000 mặc định một người có tài khoản bất kỳ, kể cả tài khoản Guest để đăng nhập tài nguyên mạng từ bất kỳ trạm nào trong vùng. Như vậy không an toàn cho việc bảo mật. Để đảm bảo an toàn trong Windows NT và 2000 đưa ra chức năng ấn định số trạm làm việc cho phép đăng nhập .

- Mở hộp thoại Properties dành cho người dùng trong Active Directory Users And Computers. Nhấp tab Account.
- Nhấp nut Log On To mở hộp thoại Logon Workstations.
- Nhấp nút the Following Computers xem hình 7.11.Gõ tên trạm làm việc bạn muốn cho phép đăng nhập, rồi nhấp Add. Lặp lại chỉ định này để chỉ định thêm trạm làm việc khác.
- Nếu phạm sai lầm, nhấp mục nhập sai và nhấp Edit hay Remove tuỳ ý.



Hình 7.12: *Nhằm giới hạn truy cập ở trạm làm việc, hãy định rõ những trạm làm việc được phép đăng nhập.*

❖ **Cập nhật tài khoản người dùng**

- Đổi tên tài khoản người dùng:

▫ Truy cập Active Directory And Computers.

▫ Nhấp nut phải mouse vào tên tài khoản, chọn Rename. Gõ tên mới cho tài khoản khi được nhắc.

- Thay đổi các thông tin khác: bao gồmcác thông tin sau:

▫ **Display Name** Đổi tên hiển thị của tài khoản người dùng trong *Active Directory And Computers*

▫ **User Profile Path:**Thay đổi đường dẫn bộ lưu trữ trong Active Directory And Computers, rồi đổi tên thư mục tương ứng trên ổ đĩa.

▫ **Logon script Name:** Nếu dùng kịch bản đăng nhập riêng biệt cho từng người dùng, hãy đổi tên kịch bản đăng nhập trong Active Directory And Computers, sau đó đổi tên kịch bản đăng nhập trên đĩa.

▫ **Home Directory:** Thay đổi đường dẫn của thư mục cá nhân trong Active Directory And Computers, rồi đổi tên đăng nhập tương ứng trên đĩa.

- Sao chép tài khoản người dùng vùng: Sẽ rất chán ngán nếu phải tạo tài khoản người dùng vùng từ đầu, chúng ta có thể cải thiện tình hình bằng cách dùng tài khoản hiện có làm khuôn mẫu. Theo các bước sau:

1. Nhấp nút phải chuột vào tài khoản cần sao chép trong Active Directory And Computers, chọn Copy mở hộp thoại copy Oject – Users.

2. Tạo tài khoản làm khuôn mẫu cho mọi tài khoản người dùng khác. Sau đó cập nhật thuộc tính của tài khoản, nếu thấy thích hợp.

Khi sao chép tài khoản, Active Directory And Computers sẽ không giữ lại toàn bộ thông tin từ tài khoản hiện có mà chỉ sao chép những thông mà bạn cần đến, đồng thời loại bỏ những thông tin nào phải được cập nhật. Những thông tin thuộc tính được giữ lại

bao gồm.

- Thành phố, quốc gia, mã bưu cục trên trang Address
- Tên công ty và phòng ban trên trang Organziation
- Nhóm tuỳ chọn tài khoản (Account Options) trên trang Account.
- Số giờ đăng nhập và số trạm làm việc được phép đăng nhập.
- Ngày hết hạn tài khoản.
- Quan hệ thành viên nhóm của tài khoản
- Tập hợp xác lập bộ lưu trữ.
- Các đặc quyền quay số.

• Huỷ bỏ tài khoản người dùng: Việc huỷ bỏ tài khoản tác động đên toàn vùng, nên Windows 2000 không cho phép bạn xoá tài khoản nhóm hay tài khoản người dùng cài sẵn . Chúng ta có thể xoá các loạ tài khoản khác bằng cách chọn chúng và ấn Del, hoặc chọn Del từ menu tắt (hiển thị khi bấm nút phải chuột). Nhấp OK và nhấp Yes xác nhận xoá.

Với Active Directory And Computers, áp dụng một trong hai phương pháp sau đẻ xoá bỏ nhiều tài khoản cùng lúc:

- Nhấn- giữ phím CTRL, nhấp nút trái mouse trên từng tài khoản muốn chọn.
- Nhấn- giữ phím SHIFT, chon tên tài khoản đầu tiên,rồi nhấp tên tài khoản cuối cùng trong dãy.

• Thay đổi và tái lập mật mã: Đây là công việc thường xuyên của nhà quản trị, nhất là khi người dùng quên mất mật mã hoặc lúc mật mã hết hạn sử dụng. Cách thay đổi hay tái lập mật mã:

- Truy cập Active Directory And Computers hoặc Local Users And Group tuỳ thuộc vào loại tài khoản.
- Nhấp nút phải Mouse vào tên tài khoản, chon Reset Password hay Set Passwordsét tình hình cụ thể.
- Gõ mật mã mới cho người dùng và xác nhận mật mã này.
- Nhấp đúp tên tài khoản, xoá chọn Account is Disable hoặc Account Is Locked Out, xét tình huống cụ thể.. Trong Active Directory And Computers, bạn truy cập hai tuỳ chọn nêu trên từ trong Account.

• Vô hiệu hoá tài khoản người dùng: vì nhiều nguyên nhân mà chúng ta phải vô hiệu hoá tài khoản. Dưới đây là những công việc cần trong trường hợp tài khoản bị vô hiệu hoá, bị khoá, hay hết hạn sử dụng:

- Tài khoản bị vô hiệu hoá:

1. Truy cập Active Directory And Computers.

2. Nhấp nut phải mouse vào tên tài khoản, chọn Enable Account

- Tài khoản bị khoá:

1. Truy cập Active Directory And Computers.

2. Nhấp đúp tên tài khoản, xoá chọn Account Is Locked Out. Tong Active Directory And Computers, tuỳ chọn này hiện trên trang Account.

- Tài khoản hết hạn dùng: chỉ riêng tài khoản vùng mới có ngày hết hạn. Tìa khoản cục bộn luôn luôn có hiệu lực. Khi tài khoản vùng hết hạn sử dụng bạn:

1. Truy cập Active Directory And Computers.

2. Nhấp đúp tài khoản, nhấp tab Account.

3. Ở phân mục Account Expires, chọn End Of và nhấp mũi tên xuống trên hộp danh sách tương ứng. Một bảnh lịch xuất hiện, cho phép bạn ấn định thời hạn sử dụng mới.

- Xử lý lỗi đăng nhập: Ngoài những nguyên nhân thông thường buộc phải vô hiệu hoá tài khoản, một vài xác lập hệ thống cũng có thể gây nên lỗi truy cập cụ thể là:

- Người dùng nhận được thông điệp cho biết không thể đăng nhập theo cách tương tác Anh ta đã không được cấp quyền Log On Locally (Đăng nhập cục bộ), mà cũng không là thànhviên của nhóm có quyền đăng nhập này. Có thể người dùng cố gắng đăng nhập máy phục vụ hay máy điều khiển vùng. Nếu thế, đừng quên rằng quyền Log On Locally áp dụng cho tất cả máy điều khiển trong vùng. Ngược lại, quyền này chỉ áp dụng cho các trạm làm việc đơn lẻ. Trường hợp người dùng phải được cấp quyền truy cập hệ thống cục bộ, hãy ấn định quyền Log On Locally.

- Người dùng nhận được thông điệp cho biết hệ thống không cho phép truy cập. Nếu đã kiểm tra tên tài khoản, mật mã, tại sao lại không kiểm tra dạng thức tài khoản. biết đâu người dùng đang cố truy cập vùng tài khoản cục bộ. Còn không thì có lẽ máy phục vụ danh mục phục vụ toàn cục hiện không khả dụng, do đó chỉ riêng người có đặc quyền quản trị mới được phếp đăng nhập vùng.

- Người dùng có bộ lưu trữ quy định nhưng máy tính chứa bộ lưu trữ đó lại không khả dụng: Khi người dùng có bộ lưu trữ quy định, máy tính lưu bộ lưu từ đó phải ở tình trạng truy cập được trong suốt tiến trình đăng nhập. Ngược lại người dùng này sẽ không cách nào đăng nhập được.

- Người dùng nhận thông điệp cho biết tài khoản đã được lập cấu hình nhằm ngăn không cho họ đăng nhập trạm làm việc. Người dùng đang cố gắng đăng nhập vào một trạm làm việc mà không nằm trong số những trạm làm việc anh ta được phép đăng nhập. Nếu thực sự cần truy cập trạm làm việc này, hãy thay đổi thông tin về trạm làm việc đăng nhập như đã mô tả ở phần trên.

3. THIẾT LẬP VÀ QUẢN LÝ TÀI KHOẢN NHÓM.

Cũng tương tự như tài khoản người dùng tài khoản nhóm cũng cần được tuân thủ các chính sách về tên tài khoản, mật mã, chính sách tài khoản... tất cả các chính sách này hoàn toàn tương tư như của tài khoản người dùng do đó chúng ta không mô tả ở đây.

Bạn dùng tài khoản nhóm vào việc quản lý đặc quyền cho nhiều người dùng. Tài khoản nhóm toàn cục được thiết lập trong Active Directory Users And Computers. Khi cần tạo tài khoản nhóm cục bộ, hãy truy cập Local And Groups.

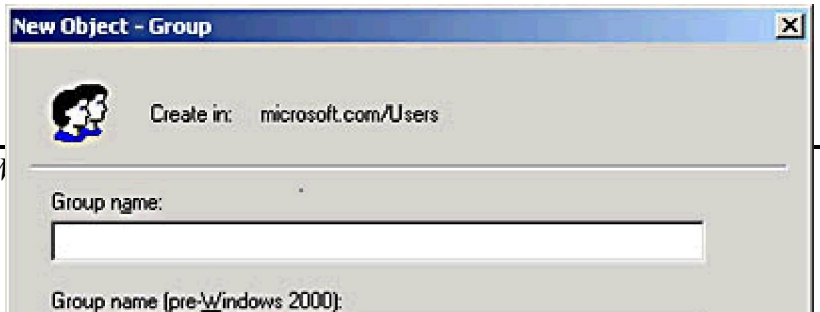
Khi bắt đầu thiết lập tài khoản nhóm, hãy nhớ rằng tài khoản nhóm chỉ nên chứa các dạng người dùng tương tự nhau. Như vậy bạn có thể có:

- Nhóm toàn cục cho các phòng ban trong phạm vi tổ chức: Thông thường những nhân viên ở cùng phòng ban, họ sẽ cần truy cập tài nguyên tương tự nhau. Vì lẽ đó có thể thiết lập nhóm quản lý theo phòng ban, như Development, Sale, Marketing, v.v.
- Nhóm cho người dùng các chương trình ứng dụng cụ thể: Thường thì người dùng sẽ truy cập một chương trình ứng dụngvà tài nguyên liên quan đến chương trình ứng dụng nào đó. Nếu tạo nhóm đặc trưng cho từng chương trình ứng dụng, bạn có thể đảm bảo người dùng dễ dàng truy cập tài nguyên và tài nguyên chương trình ứng dụng cần thiết.
- Nhóm cho các vai trò trong phạm vi tổ chức: Cách thứ ba là tổ chức nhóm theo vai trò của người dùng trong phạm vi tổ chức. Lấy ví dụ, điều hành viên sẽ cần quyền truy cập khác với giám sát viên và người dùng thông thường. phương pháp tạo nhóm này giúp đảm bảo quyền truy cập thích hợp được cấp cho ai thật sự cần đến.

3.1. Thiết lập tài khoản nhóm cục bộ.

Thiết lập tài khoản nhóm cục bộ theo các bước sau:

1. Khởi động Active Directory Users And Computers. Nhấp nút phải chuột vào địa điểm tiếp cận tài khoản mới. Chọn New -> Group mở hộp thoại New Object- Group (Xem hình minh hoạ sau đây)



Hình 7.13: *Hộp thoại New Object-Group cho phép bạn bổ xung nhóm toàn cục mới vào vùng*

2. **Đặt tên nhóm.** Tên tài khoản nhóm toàn cục phải theo đúng quy ước áp dụng cho tên hiển thị của tài khoản người dùng. Tên này không phân biệt chữ hoa và chữ thường và dài tối đa 64 kí tự.

3. 20 kí tự đầu tiên của tên nhóm được dùng để ấn định tên nhóm của Windows NT 4.0 trở vè trước. Tên nhóm không được trùng lặp trong vùng.

4. Chọn phạm vi nhóm: Domain Local, Global, hay Universal.

5. Chọn loại nhóm: Security hay Distribution.

6. Nhấp OK thiết lập nhóm. Khi nhóm đã hình thành, sau này có thể bổ xung thành viên và ấn định thêm thuộc tính.

*** Tạo nhóm cục bộ và chỉ định thành viên.**

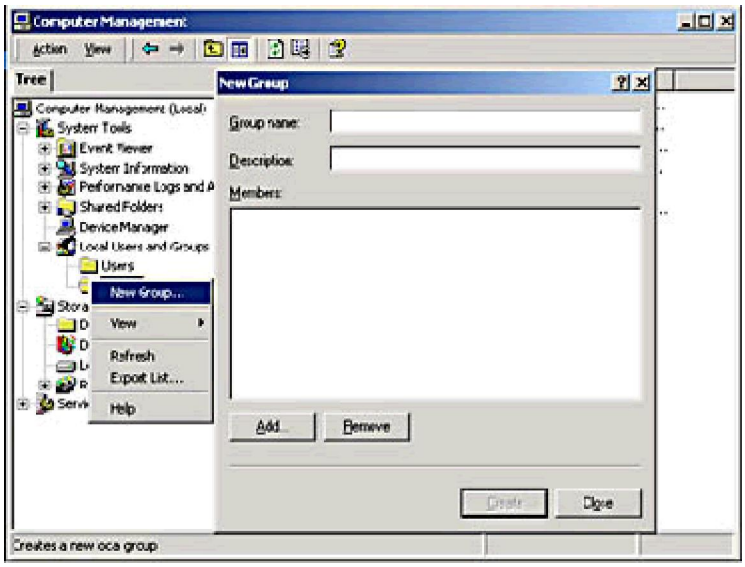
Nhóm cục bộ được thiết lập với Local Users And Group. áp dụng thủ tục dưới đây để truy cập tiện ích này và tạo tài khoản nhóm cụ bộ:

1. Chọn Start -> Programs -> Administractive Tools-> computers Management. Hoặc chọn Conputer Management từ thư mục Administrative Tools.

2. Nhấp nut phải chuột vào mục nhập Mycomputer Management bên khung trái, chọn Connect To Another Computer từ menu tắt. Chọn hệ thống có tài khoản cục bộ cần quản lý. Máy điều khiển vùng (domain controler) không chứa người dùng và nhóm cục bộ.

3. Mở rộng System Tools (nhấp nút +), chọn Local Users And Groups.

4. Nhấp nut phải mouse vào Group, chọn New -> Group mở hộp thoại New Group(xem hình 7.13)



Hình 7.14: *Hộp thoại New Group cho phép bổ xung nhóm cục bộ mới vào máy tính*

Sau khi gõ tên và thông tin mô tả nhóm nhấp Add đưa tên vào nhóm. Hộp thoại Select Users Or Groups hiển thị như đã minh hoạ ở phần trên. Bạn kết nạp các thànhviên vào nhóm dựa vào các tuỳ chọn sau:

- **Look In** Cho phép truy cập tên tài khoản từ vùng và máy tính khác. Nhấp *Look In* sẽ hiển thị danh sách liệt kê tên máy tính hiện hành, các vùng được uỷ quyền, và nhiều tài nguyên cần thiết. Chọn Entire Directory xem tất cả tên tài khoản chứa trong thư mục.
- **Name** Cột name hiện tên tất cả các tài khoản khả dụng trực thuộc vùng hay tài nguyên hiện đang được chọn.
- **Add** Bổ xung tên đã chọn vào danh sách.
- **Check Names** Chứng thực tên nhóm và tên người dùng đã gõ vào danh sách. Đây là việc làm hữu ích nếu bạn tự gõ vào bàn phím và muốn đảm bảo nó luôn khả dụng.

5. Sau khi chọn tên tài khoản để đưa vào nhóm, nhấp OK.

6. Hộp thoại **New Group** được cập nhật để phản ánh các chọn lựa vừa thực hiện. Trường hợp có phạm sai lầm, hãy chọn tên và nhấp Remove.

7. Nhấp **Create** khi hoàn thành việc bổ xung hay loại bỏ thành viên nhóm.

3.3. Quản lý quan hệ thành viên nhóm cục bộ

Khi đã thiết lập tài khoản nhóm thì bạn cần quản lý quan hệ thành viên nhóm

thông qua tiện ích Active Directory Uer And Computers. Khi làm việc với nhóm hãy ghi nhớ những yếu tố sau:

- Tất cả người dùng trong vùng đều là thành viên của nhóm Domian Users, đồng thời nhóm chính của họ cũng là Domain Users.
- Toàn bộ trạm làm việc và dịch vụ thành viên mới thuộc vùng đều là thành viên nhóm Domains Computers, nhóm chính của chúng cũng là Domains Users.
- Tất cả máy điều khiển vùng mới đều là thành viên nhóm Domains Controllers, nhóm chính của chúng cũng là Domains Controllers.

Active Directory Users And Conputers cung cấp nhiều cách giúp quản lý quan hệ thành viên nhóm. Bạn có thể:

- Quản lý từng thành viên cá thể.
- Quản lý nhiều thành viên đồng thời.
- Ấn định nhóm chính cho từng người dùng và máy tính.

3.3.1. Quản lý từng thành viên cá thể

Bạn có thể bổ xung hay xoá bỏ tài khoản khỏi nhóm bất kỳ theo cách sau:

- Nhấp đúp mục nhập dành cho người dùng, máy tính hoặc nhóm trong Active Directory Users And Conputers. Hộp thoại Properties dành cho tài khoản xuất hiện.
- Nhấp tab Member Of.
- Nhấp Add đưa tài khoản vào nhóm. Thao tác này mở hộp thoại Select Groups cũng chính là hộp thoại Select Users Or Groups đã giới thiệu ở phần trên. Chọn nhóm sẽ tiếp nhận tài khoản hiện đang được chọn.
- Muốn loại bỏ tài khoản nhóm, hãy chọn tài khoản và bấm Remove.
- Nhấp OK.

3.3.2 Quản lý nhiều thành viên đồng thời.

Phương pháp thứ hai giúp quản lý quan hệ thành viên nhóm là bổ xung hay loại bỏ cùng lúc nhiều tài khoản thôngqua hộp thoại Properties:

1. Nhấp đúp mục nhập dành cho người dùng hoặc máy tính trong Active Directory Users And Computers. Hộp thoại tính xuất hiện.

2. Chuyển sang trang Member Of.

3. Nhấp Add nếu cần bổ xung tài khoản vào nhóm. Trong hộp thoại Select Users Or Groups vừa mở ra, bạn chọn người dùng, máy tính, và nhóm sẽ kết nạp vào nhóm hiện đang được chọn.

4. Muốn loại bỏ thành viên nào đó ra khỏi nhóm, chỉ việc chọn thnàh viên này và nhấp Remove.

5. Nhấp OK.

3.3.3. Ấn định nhóm chính cho người dùng và máy tính

Nhóm chính (primary group) do những người truy cập Windows 2000 qua Services For Macintosh sử dụng. Khi người dùng Macintosh tạo tập tin hay thư mục trên hệ thống Windows 2000, nhóm chính được chỉ định cho số tập tin, thư mục này. Mọi tài khoản và máy tính đều phải có nhóm chính, bất luận tài khoản có truy cập hệ thống Wondows 2000 qua Macintosh hay không. Đây phải là nhóm có phạm vi toàn cục hay tổng thể, chẳng hạn nhóm Domain Users hay nhóm Doamin Computers toàn cục.

Áp dụng thủ tục sau đây để ấn định nhóm chính:

1. Nhấp đúp mục nhập ứng với người dùng, máy tính, hoặc nhóm trong Active Directory Users And Conputers.

2. Chuyển sang trang Member Of trong hộp thoại thuộc tính tài khoản.

3. Chọn nhóm có phạm vi toàn cục hay tổng thể từ danh sách Member Of.

4. Nhấp Set Primary Group.

Tất cả người dùng bắt buộc phải là thành viên của ít nhất một nhóm chính. Bạn không thể huỷ bỏ quan hệ thành viên trong một nhóm chính và trước tiên không kết nạp người dùng vào nhóm chính khác. Theo các bước sau:

1. Chọn nhóm khác, cũng có phạm vi toàn cục hay tổng thể từ danh sách Member Of rồi nhấp Set Primary Group.

2. Nhấp nhóm chính cũ từ danh sách Member Of, nhấp tiếp nút Remove. Quan hệ thành viên với nhóm cũ giờ đây bị thu hồi.

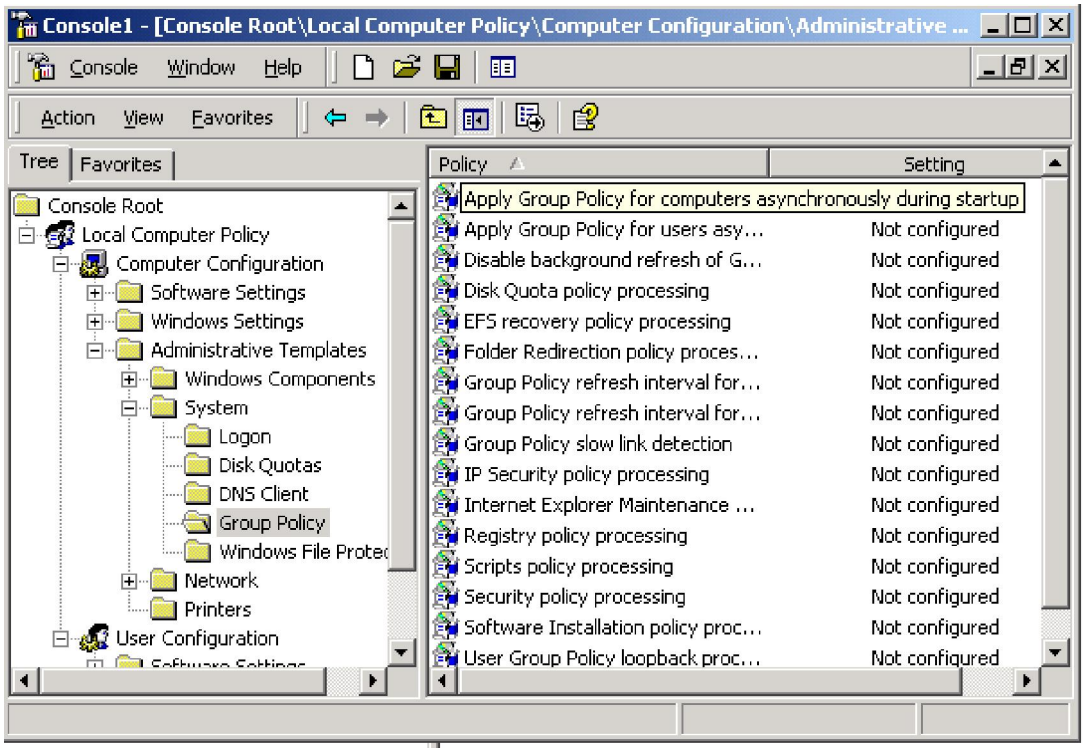
4. QUẢN LÝ CÁC CHÍNH SÁCH NHÓM

4.1. Các chính sách nhóm về Group Policy

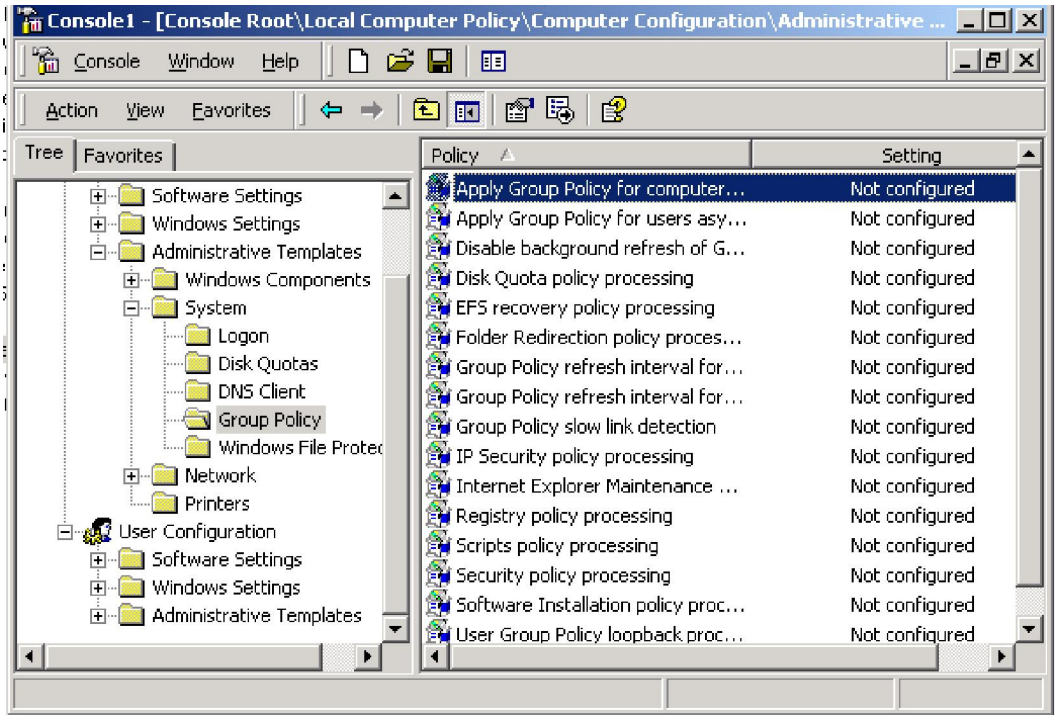
Các chính sách để kiểm soát Group Policy được tìm thấy bên dưới *Administractive Templates* của cả hai đốt trong *Users Configuration* và *Computer Configuretion*. Hình 7.14 và 7.15 các tuỳ chọn trong *Users Configuration* và *Computer Configuretion* dành cho Group Policy. Sau đây là những thông tin tóm lược về các tuỳ chọn cấu hình quan trọng nhất:

Group Policy refresh interval for users/computers/domaincontrollers Các chính sách riêng này quyết định đến các đối tượng chính sách nhóm GPO được làm tươi

đến mức nào ở chế độ nền (background) trong khi các người dùng hoặc máy đang làm việc. Các thông số này cho phép bạn thay đổi các *gián cách thời gian làm tươi ở chế độ nền mặc định* (default background refresh interval), và cho phép điều chỉnh thời gian lệch (offset time).



Hình 7.14: *Các thiết định User Configuration đối với Group Policy*.

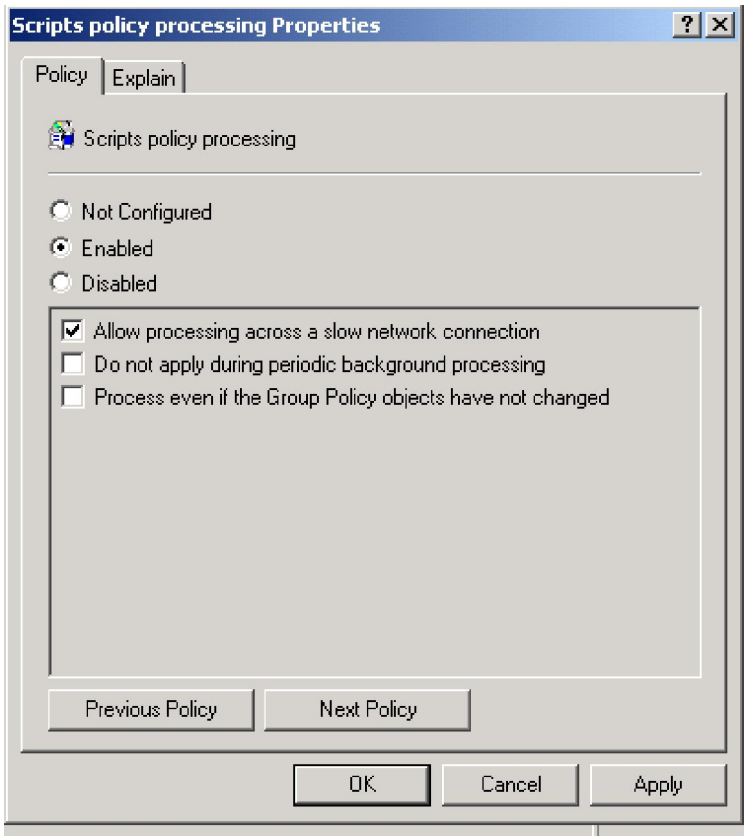


Hình 7.15: *Các thiết định Computer Configuration đối với Group Policy*

Disable background refresh Nếu bạn đưa vào áp dụng thiết định này các chính sách sẽ chỉ được làm tươi vào lúc khởi động máy và người dùng đăng nhập mà thôi. Điều này có thể có ích vì những lý do hiệu năng, bởi vì việc để cho 1500 máy cứ 90 phút lại làm tươi các chính sách một lần có thể gây tắc nghẽn trên mạng, nhất là mạng Ethernet.

Apply Group Policy for uers/computers synchonousiy during start-up Bạn nên dưa vào áp dụng này để ngăn không cho người dùng đăng nhập chừng nào tất cả các chính sách còn chưa được áp dụng hết. Nếu không các chính sách sẽ được áp dụng ở chế độ background, và người dùng vẫn có thể đăng nhập trong khai các thiết định chính sách vẫn còn đang thay đổi.

Các chính sách về sử lý chính sách: Các chính sách này với cái tên như **Registry Policy Processing và Folder Redirection Policy Processing,** có thể được dùng để tuỳ biến cách sử lý của các thành phần GPO khác nhau. Mỗi chính sách này(xem hình 7.16) đều có mặt ít nhất hai trong số ngững tuỳ chọn sau đây:



Hình 7.16: *Các tuỳ chọn về chính sách hạn ngạch đĩa*

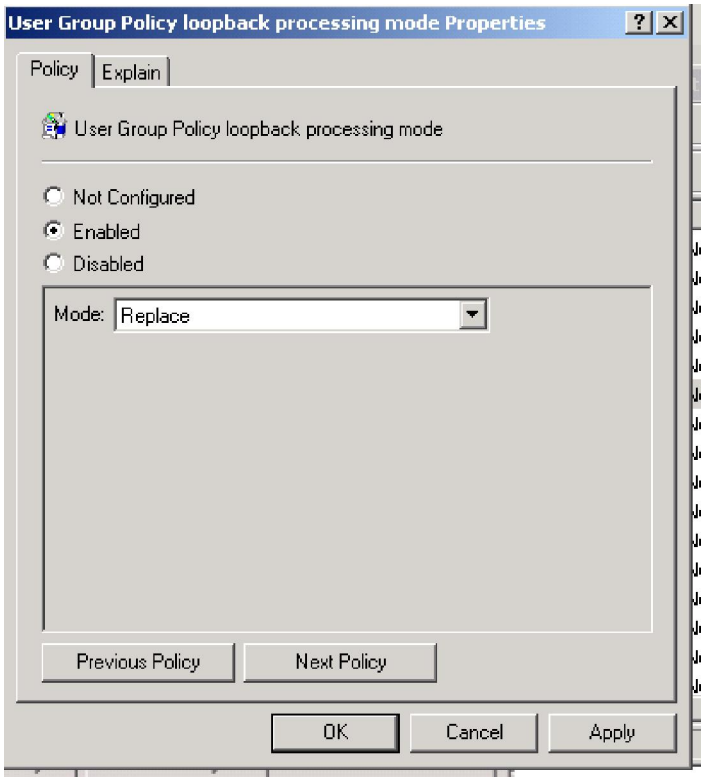
Allow process across a slow network conection Đối với các mối liên kết mạng chậm, một số chính sách có thể được tắt đi để tăng cường hiệu năng (bạn có thể định nghĩa một "slow conection" hay "slow link" là gì bằng cách dùng thiết định **Group Policy slow link detection**). Tuy nhiên, các thiết định về bảo mật và về việc sử lý chính sách đối với Registry luôn luôn được áp dụng, và không thể bị tắt đi.

Do not apply during periodic background processing Chỉ định các thành phần nào làm tươi định kỳ. Các chính sách cài đặt phần mềm và định hướng lại folder sẽ không bao giờ được làm tươi trong khi một người dùng đăng nhập, cho nên tuỳ chọn này sẽ không dùng được cho chúng.

Process even if the Group Policy Object have not changed Để tồn tại tài nguyên mạng và tài nguyên hệ thống, theo mặc định các GPO không được làm tươi nếu không có gì thay đổi cả. Tuy nhiên để tăng cường tính bảo mật và đề phòng người dùng thay đổi các thiết đặt chính sách bạn hãy thực thi chính sách này để đảm bảo rằng tất cả các thiết định đều được áp dụng lại vào mỗi kỳ làm tươi. Chý ý rằng khi áp dụng chính sách này thì hiệu năng của mạng sẽ giảm đi đáng kể đấy.

User Group Policy loopback processing mode Mặc định các chính sách cấu hình

người dùng được xử lý sau các chính sách cấu hình máy, và các chính sách người dùng sẽ được ưu tiên hơn nếu có mâu thuẫn. Cũng theo mặc định, bất luận người dùng đăng nhập vào máy nào họ đều nhận được các chính sách của họ. Nhưng đôi lúc điều này không thích hợp, và các chính sách cần được áp dụng theo các GPO giành cho máy, ví dụ nếu bạn đăng nhập vào một server để thực hiện việc quản trị, thì thật không thích hợp nếu các úng dụng chính của văn phòng được cài đặt vào đúng lúc đó. Một ví dụ khác: khi muốn áp dụng chính sách nghiêm ngặt hơn cho các máy được đặt ở chỗ công cộng, hẳn là bạn cần để chính sách máy lấn át người dùng. Có hai chế độ khác nhau để kiểm xoát cách sử lý này: chế độ Merge và chế độ Replace (xem hình7.17).



Hình 7.17: *Chính sách User Group Policy loopback processing mode*

Chế độ Merge Xử lý các chính sách người dùng trước, rồi đến các chính sách máy. Như vậy chính sách máy sẽ phủ quyết chính sách người dùng mâu thuẫn với chúng.

Chế độ Replace Bất chấp các chính sách người dùng, và chỉ xử lý các chính sách máy mà thôi.

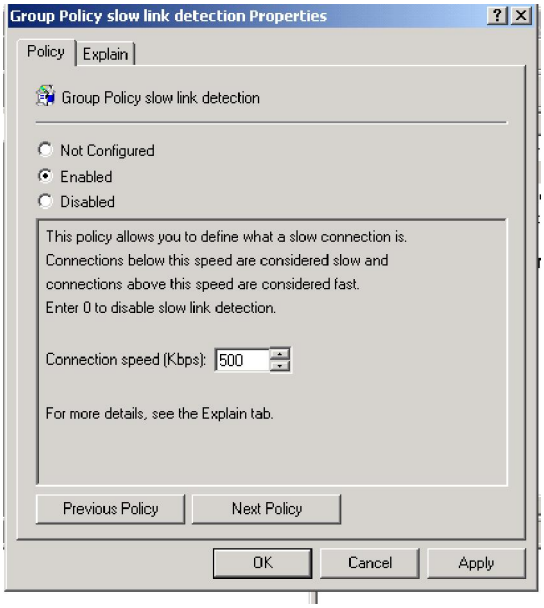
4.2. Chính sách nhóm ngang qua các đường liên kết chậm

Chính sách nhóm vẫn làm việc ngang qua các đường liên kết chậm, như các nối kết dial- up chẳng hạn. tuyết hơn nữa, các chính sách được áp dụng bất kể nhười dùng đăng nhập bằng Dial-Up Networking hay đăng nhập với các giấy giới thiệu (credential)

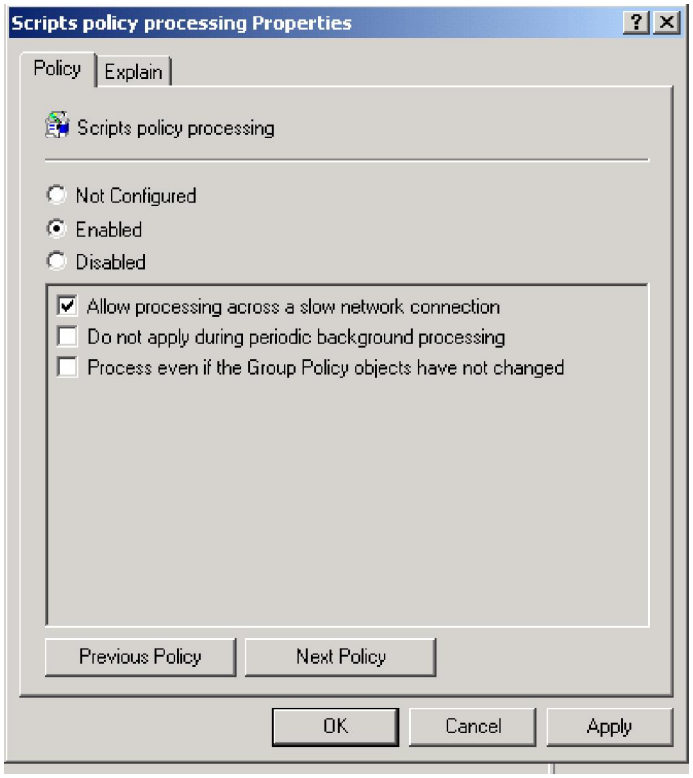
đã được lưu trữ trước rồi khởi động một mối liên kết. Tuy nhiên việc áp dụng chính sách nhóm ngang qua các đường liên kết chậm có thể đặt ra những vấn để về hiệu năng hoạt động của mạng, cho nên Win2K có kèm những thiết định để định rõ thế nào là slow link, và để quy định cách áp dụng các chính sách ngang qua các đường liên kết chậm đã phát hiện được.

Định nghĩa mặc định về một đường liên kết chậm, trong chừng mực các chính sách nhóm có liên quan, là một đường liên kết mà tốc độ dưới 500kilobits/giây. Hệ thống thực hiện một cuộc trắc nghiệm bằng cách dùng tiện ích Ping để xác định tốc độ cảu mối liên kết. Nếu thời gian hồi đáp của Ping là trên 2000 miligiây, thì mối liên kết được coi là nhanh, tuy nhiên bạn có thể thay đổi thiết định định nghĩa về slow link. Thiết định chính sách này, tên là **Group Policy Slow Link Detection** có trong cả *Users configuration* lẫn *Computers Configuration*, bên dưới *Administrative Templates\System\Group Policy* (khung thoại thuộc tín của nó trong hình 7.18) Bạn nhập số muốn chỉ định vào Conection speed (Kbps), hoặc nhập số 0 vào để dislable việc phát hiện slow link. Nếu bạn dislable việc phát hiện slow link, tất cả các chính sách sẽ được áp dụng, bất kể tốc độ kết nối là bao nhiêu.

Các thiết định về cách sử lý chính sách của từng thành phần chính sách (có tên kiểu như Folder Redection Policy Processing chẳng hạnvà nằm trong cùng một đường dẫn với thiết định slow link detection bên dưới *Users configuration* lẫn *Computers Configuration\Administrative Templates\System\Group Policy*) cho phép bạn chỉ định có phần nào của đối tượng chính sách được sử lý ngang qua một đường liên kết chậm hay không. Một lần nữa, đây không phải là tuỳ chọn các chính sách dựa trên Registry hoặc dành cho các thiết bị bảo mật, chúng luôn luôn được xử lý, ngay cả ngang qua các slow link. Những thiết định khác thì theo mặc định, sẽ không được áp dụng ngang qua các slow link



Hình 7.18: *Khung thoại đặc tính Group Policy Slow Link Detection*



Hình 7.19: *Một ví dụ về các tuỳ chọn về sử lý chính sách*

Ví dụ, để làm cho các login script chạy ngang qua các slow link bạn mở chính sách tên là Script policy processing. Bạn enlable chính sách này, như trong hình 7.19 duyệt vào ô Allow processing across a slow network connection, rồi nhấp OK. Nếu thấy cần, bạn cứ lặp lại các thao tác đó đối với các thiết định xử lý chính sách khác.

CHƯƠNG 6

QUẢN LÝ VÀ CHIA SẺ TÀI NGUYÊN MẠNG

---

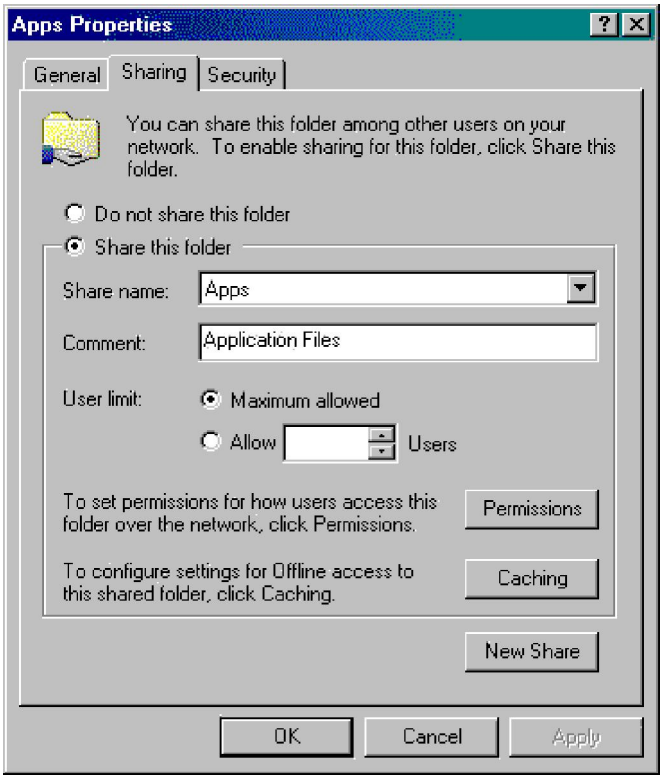
1. CƠ SỞ CỦA VIỆC CHIA SẺ DÙNG CHUNG TẬP TIN

Chức năng cốt lõi của một máy chủ bất kì là chia sẻ dùng chung các tập tin. Khi máy chủ chia sẻ một *folder* ra toàn mạng tức là nó cho phép ánh xạ (map) một mẫu tự ổ đĩa mới từ các máy khác trong mạng đến *folder* đó. ánh xạ một ổ đĩa đến một *folder* còn gọi là nối kết (*connect*) ổ đĩa đó với *folder* này. Bằng cách nối kết này người dùng có thể dùng mạng để truy cập các tài nguyên từ mạng, hay còn gọi là chia sẻ (*share*) tài nguyên mạng.

2. THIẾT LẬP CÁC FOLDER DÙNG CHUNG (SHARE)

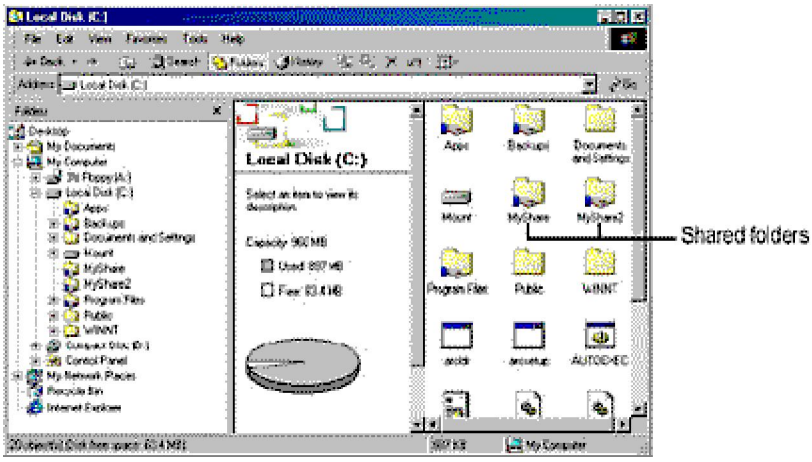
2.1. Tạo ra các share bằng Explorer

- Nhấn chuột vào **Start → Explorer** để kích hoạt **Explorer Window**.



Hình 9.1: *The Sharing tab of a folder's Properties dialog box*

- Nhấn chuột phải vào *folder* muốn chia sẻ sử dụng chung → chọn **Sharing** để mở trang đặc tính của *folder* đó. (Xem hình 9.1)
- Nhấn chuột vào nút **Share this folder**.
- Trong trường **Share name** bạn gõ vào tên của *share* mà bạn muốn phổ biến ra toàn mạng.
- Nút **Permissions** cho phép bạn quy định những quyền truy cập đối với *share* này.
- Mục **Caching** cho phép người dùng có thể truy cập vào tập tin mà không cần đăng nhập.
- Nút **New share** cho phép bạn tạo tiếp những *share* khác nếu bạn muốn.
- Nút **User limit** cho phép bạn hạn chế bớt số người truy nhập *share* này đồng thời.
- Sau khi đã thiết lập xong các thuộc tính của *share* bạn nhấn **OK**, khi đó *folder* đó sẽ được chia sẻ sử dụng chung ra toàn mạng. Trong cửa sổ Window Explorer bạn sẽ nhìn thấy các folder này với hình một bàn tay đỡ bên dưới như trong hình 9.2



Hình 9.2: *Shared folders in Windows Explorer*

2.2. Tạo các share từ xa dùng Console Computer Manage

- Kích hoạt khung thoại **Computer Management** bằng cách kích chuột vào **Start → Programs → Administrative Tools → Computer Management**.
- Thực hiện việc kết nối với máy tính ở xa bằng cách nhắp chuột phải hình tượng **Coputer management (local)** rồi chọn **Connect to another computer**.
- Tiếp theo bạn mở khung thoại **Create shared folder** bằng chách nhắp vào **Action → New file share**.

- Chọn *folder* bạn muốn chia sẻ dùng chung trong mục **Folder to share**.
- Gõ vào tên của *share* trong mục **Share name**.
- Nhấp chuột vào **Next** để tiếp tuc, khung thoại tiếp theo cho phép bạn quy định quyền truy cập đối với *share* này.
- Sau khi thiết lập xong các quyền truy cập bạn nhấp chuột vào **OK** để kết thúc.

3. QUẢN LÝ CÁC QUYỀN TRUY CẬP

3.1. Quyền truy cập cấp share

Cần phải quy định quyền truy cập *share* sao cho chúng được nới lỏng hơn so với quyền truy cập các tập tin (file) và *folder* con trong chúng.

Để quy định *share permission* bạn nhắp phải vào tên *share* ấy rồi chọn **properties** → nhắp **sharing** → và mở trang **share permission** ra. Trang này sẽ có một khung thoại cho phép bạn quy định quyền truy cập cho *share*. Các quyền truy cập cấp *share* bao gồm:

- **Full Control**: Cho phép bạn thực hiện tất cả mọi công việc trên các tập tin và *folder* trên *share* này.
- **Change**: Cho phép thay đổi, thi hành và xoá các tập tin và *folder* trong *share* này.
- **Read**: Chỉ cho phép đọc và chạy chương trình.

3.2. Quyền truy cập cấp thư mục và tập tin

3.2.1. Các kiểu quyền truy cập

Có thể phân các mức quyền truy cập (*permission*) theo 2 loại:

Permission mức nguyên tử (*atomic level*)

Permission mức phân tử (*molecular level*).

Permission mức nguyên tử là những mẩu *permission* nhỏ nhất có thể. *Permission* mức phân tử là kiểu kết hợp của các *permission* mức nguyên tử lại với nhau. Quan hệ giữa các *permision* mức phân tử và nguyên tử được thể hiện trong bảng sau:

Bảng 9.1: Quan hệ giữa permission phân tử và permission nguyên tử

QTC phân tử **QTC ngyên tử**	Write	Read	List contents	Read & excute	modify	Full control
Traverse folder / Excute file			*	*	*	*
List folder / read data		*	*	*	*	*
Read attributes		*	*	*	*	*
Read extended attributes		*	*	*	*	*
Create file / write data	*				*	*
Create folder / Append data	*				*	*
Write attributes	*				*	*
Write extended attributes	*				*	*
Delete subfolder & files						*
Delete					*	*
Read permission	*	*	*	*	*	*
Change permission						*
Take ownership						*

3.2.2. Các Permission Nguyên tử

- **Traverse folder/Excute file**: Cho phép bạn duyệt xem qua một folder và chạy (*Excute*) các files có đuôi .exe, .com ở trong đó.
- **Lits folder/read data**: cho phép bạn liệt kê các thư mục và tập tin trong một *folder*. Nó cũng cho phép bạn xem nội dung tập tin trong *folder* đó.
- **Read attributes:** Cho phép bạn nhìn thấy các thuộc tính cơ bản của các tập tin.
- **Read extended attributes:** Cho phép bạn nhìn thấy các thuộc tính mở rộng.
- **Create file/write data:** Cho phép bạn đặt một tập tin vào trong một *folder* cũng

như ghi đè lên những dữ liệu hiện có của một tập tin.

- **Create folder/Append data**: **Create folder** cho phép tạo *folder* con trong một *folder*, **Append data** cho phép thêm dữ liệu vào cuối của tập tin hiện có.
- **Write Attributes**: Cho phép thay đổi các thuộc tính cơ bản của một tập tin.
- **Write extended attributes**: cho phép thay đổi các thuộc tính mở rộng của một tập tin.
- **Delete subfolder and files**: cho phép xóa bỏ nội dung của một *folder*.
- **Delete**: cho phép xoá bỏ một *folder*.
- **Read permission**: cho phép xem các *permission* NTFS có liên kết với tập tin hay *folder* đó.
- **Change permission**: cho phép thay đổi các *permission* được ấn định cho một *folder* hay tập tin.
- **Take ownership**: cho phép chiếm quyền sử dụng đối với một tập tin hay *folder*.

3.2.3. Các Permission Phân tử

- **Read**: cho phép xem được nội dung và các *permission* của một đối tượng (tập tin hay *folder*).
- **Write**: Cho phép bạn tạo tập tin hay *folder* con trong một *folder*. Nó cũng cho phép ghi các dữ liệu vào trong các tập tin hiện có.
- **Read and Excute**: *Permission* này cũng giống như **Read**, tuy nhiên nó còn cho phép thi hành các tập tin khả thi.
- **List folder contents**: Giống như **Read and Excute** nhưng nó chỉ được áp dụng cho các *folder* mà thôi.
- **Modify**: Là sự kết hợp của **Read, Excute, Write** và **Delete**.
- **Full control**: là sự kết hợp của tất cả các *permission* trên.

3.2.4. Thiết lập quyền sử dụng đối với các tập tin và thư mục

Để thiết lập quyền sử dụng đối với một tập tin hay thư mục bạn nhắp chuột phải vào đối tượng đó, chọn **properties** rồi mở trang **security**. Trong khung **Name** ở phía bên trên của trang này cho thấy tên các nhóm hoặc người dùng được phép truy cập vào đối tượng này. Khung bên dưới miêu tả những quyền truy cập được phân bổ cho nhóm hay người dùng tương ứng trong khung trên.

Để cho phép thêm một người dùng hay một nhóm nào đó quyền truy cập vào đối tượng bạn nhắp chuột vào **Add** để mở khung thoại trong đó bạn có thể chọn tên người

dùng hay nhóm mà bạn muốn gán cho quyền truy cập. Bạn chọn tên người đó rồi nhắp chuột vào **Add** một lần nữa để thêm vào, bạn sẽ thấy tên người bạn vừa chọn được thêm vào trong khung bên dưới. Sau khi đã chọn hết các người dùng mà bạn muốn thêm vào, bạn nhắp chuột vào **OK** để xác nhận cuối cùng.

Để loại bỏ quyền truy cập của một người hay nhóm nào đó bạn chỉ việc chọn tên người đó rồi nhắp chuột vào **remove** để xoá đi.

Để thiết lập quyền truy cập cho một người nào đó bạn chọn tên người đó ở khung bên trên rồi nhắp chuột vào các *permission* bên dưới để thiết lập quyền truy cập mà bạn muốn gán cho người này.

Trong khung bên dưới của trang này chỉ có các *permission* phân tử, có những trường hợp bạn có thể muốn thiết lập một quyền truy cập đặc biệt không theo một chuẩn nào trong khung này cho một người hay nhóm người sử dụng, bạn có thể nhắp vào mục **Advance** để mở khung thoại **Access Control Setting**. Trong trang này bạn nhắp chuột vào mục **View/Edit** để mở khung thoại **Permission Entry**, khung thoại này sẽ cho phép bạn gán cho người sử dụng những *permission* nguyên tử.

3.2.5. Sử dụng Deny Permission (quyền cấm)

Deny permission (quyền cấm) được sử dụng để tăng độ an toàn cho việc thiết lập quyền truy cập. Nó được thiết lập nhằm đảm bảo không một cá nhân hay nhóm người sử dụng nào có thể vô tình được trao một quyền truy cập nào đó mà đáng ra người đó không được hưởng.

3.2.6. Sử dụng quyền sở hữu (Ownership)

Mỗi *folder* hay tập tin đều có một chủ nhân (*owner*). Chủ nhân của tập tin được ngầm định là người tạo ra tập tin đó. Nếu đó là một tập tin hệ thống, chủ nhân của tập tin được ngầm định là nhóm *administrator* của miền (*domain*). Đối với những tập tin hay *folder* bình thường nhóm *administrators* cũng có đặc quyền chiếm láy quyền sở hữu của các đối tượng đó. Chủ nhân của một đối tượng có quyền thiết lập và phân bổ lại các quyền truy cập đối với đối tượng đó.

Nếu bạn là một *administrator* thì bạn có thể chiếm lấy quyền sở hữu đối với một đối tượng nào đó bằng cách nhắp chuột phải vào đối tượng đó, chọn **properties** rồi mở trang **security**. Trong trang **security** bạn nhắp vào nút **Advance** rồi chọn trang **Owner**. Trong khung **Change owner to** sẽ có các tài khoản **Adminitrator** và **Administrators**, bạn nên chọn **Administrator**, sau đó nhắp chuột vào ô **Replace owner on subcontainer and object** rồi nhấn **OK**. Như vậy là bạn đã chiếm lấy quyền sở hữu đối với đối tượng đó rồi đấy. Bây giờ ở trên trang **Security** bạn có thể nhắp chuột vào **Add** để thêm đề mục **Administrator** vào danh sách tên những người được quyền truy cập đối với đối tượng

này.

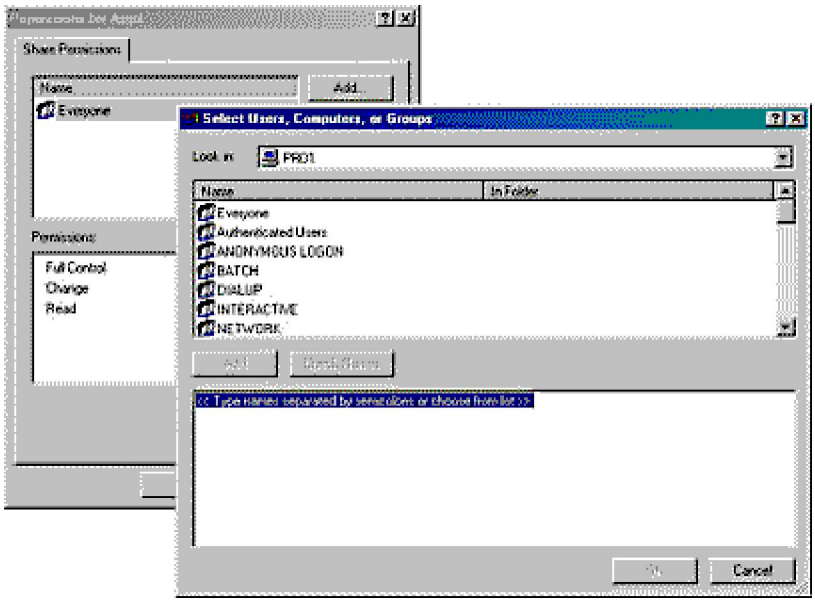
Thực hành: Gán các permission cho các share

Để gán các permission cho các tài khoản người dùng hay nhóm, bạn làm theo các bước như sau:

1. On the Sharing tab of the Properties dialog box of the shared folder, click Permissions.

2. In the Permissions dialog box, ensure that the Everyone group is selected and then click Remove.

3. In the Permissions dialog box, click Add (Xem hình 9.4).



Hình 9.4: *Setting permissions for a shared folder*

4. In the Select Users, Computers, Or Groups dialog box, click the user accounts and groups to which you want to assign permissions.

5. Click Add to add the user account or group to the shared folder. Repeat this step for all user accounts and groups to which you want to assign permissions.

6. Click OK.

7. In the Permissions dialog box for the shared folder, click the user account or group, and then, under Permissions, select the Allow check box or the Deny check box for the appropriate permissions for the user account or group.

4. CÁC SHARE ẨN

Các *share* ẩn là những *share* có đặc tính giống như các *share* bình thương tuy

nhiên chúng không được nhìn thấy ở trên mạng. Để tạo ra một *share* ẩn bạn chỉ việc làm giống như khi bạn tạo một *share* bình thường, chỉ khác là bạn cần thêm kí hiệu dollar ($) vào sau tên của *share* (Share name).

Để gọi ra các *share* ẩn này bạn phải gõ đầy đủ tên của *share* đó vào trong khung thoại **Map Network Drive**. Bạn cũng có thể nhìn thấy các *share* ẩn thông qua công cụ **Console Computer management**.

5. CÁC COMMON SHARE

Các *common share* là những *share* thông thường được *Windows 2000* tạo sẵn, hầu hết tất cả các *share* này là những *share* ẩn.

- **Các share dạng C$, D$.**

Đây là các *share* ổ đĩa, loại *share* này được gọi là các *share* quản trị (*administrative share)*. Bạn không có quyền thay đổi các quyền truy cập của các *share* này nhưng lại có thể chấm dứt việc chia sẻ chúng.

- **Print$:** *Share* này chứa các *driver* của máy in mạng.
- **IPC$:** Là *share* được dùng để liên lạc truyền thông giữa các máy chủ với nhau.
- **REPL$:** Là *share* được dùng cho quá trình dịch vụ sao chép (*replication services*) giữa các máy chủ trong mạng.
- **NETLOGON$:** *Share* này được dùng liên đới với việc xử lý các yêu cầu đăng nhập từ người dùng mạng.

6. CÁC PHƯƠNG PHÁP KẾT NỐI VÀO SHARE

- Nhắp chuột phải vào **My Network Place** rồi chọn **Map Network Drive**. Bạn có thể gõ vào tên *folder* trong mục **Folder** hoặc có thể dùng **Browser** để tìm *folder* mà bạn cần. Nhấn chuột vào **Finish** khi bạn kết thúc quá trình tìm kiếm.
- Rà duyệt mạng từ **My network places**.
- Tìm kiếm *share* đó trong **Active Directory**.
- Sử dụng công cụ dòng lệnh **netuse** (thường được sử dụng cho các mạng WAN).

Nối kết với folder đã share bằng cách sử dung Run command:

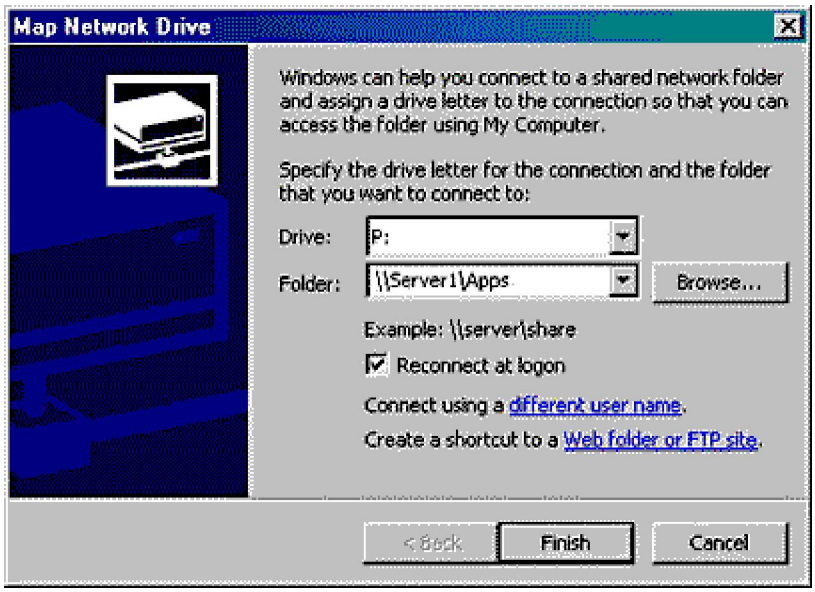
1. Click the Start button, click Run, and then type *computer_name* in the Open box.

Windows 2000 displays shared folders for the computer.

2. Double-click the shared folder to which you want to connect.

Nối kết với folder đã share bằng cách sử dung My Network Places:

1. Double-click the My Network Places icon.
2. Locate the computer on which the shared folder is located.
3. Double-click the shared folder to which you want to connect.



Hình 9.5: *The Map Network Drive wizard*

CHƯƠNG 7

CÀI ĐẶT CÁC GIAO THỨC VÀ DỊCH VỤ MẠNG

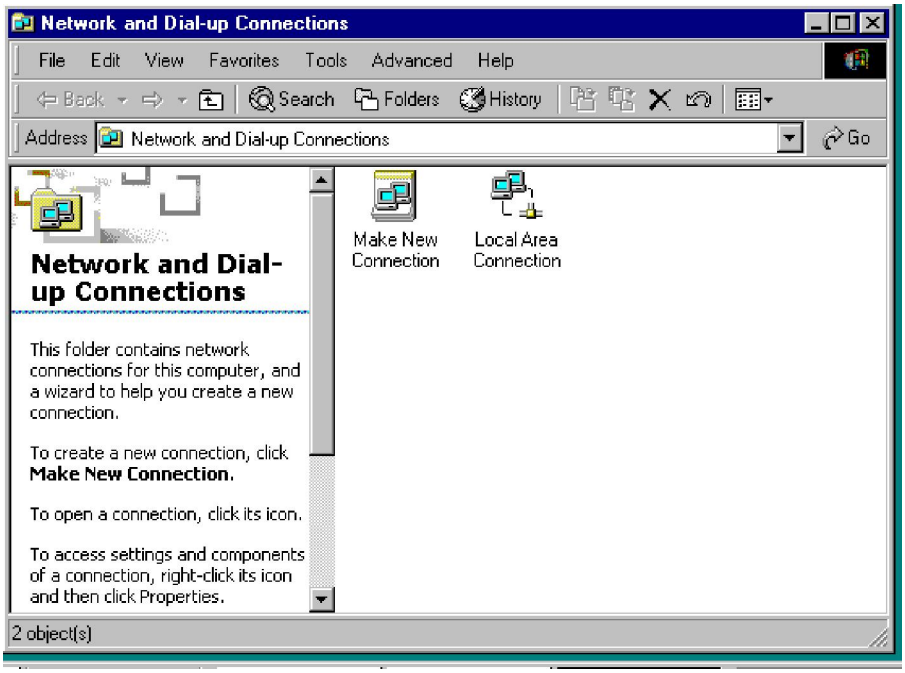
---

1. CẤU HÌNH (CONFIGURATING) TCP/IP

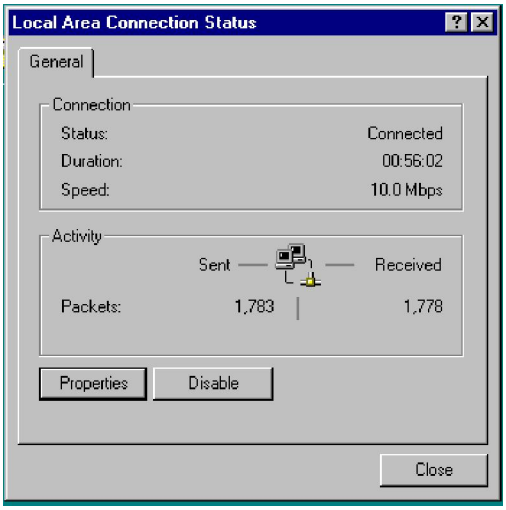
1.1. Thiết lập cấu hình TCP/IP

Một mạng LAN sẽ được tự động cấu hình sau khi bạn cài đặt card mạng. Các kết nối sẽ được cấu hình dựa trên các thông số ngầm định. Bạn cần phải cấu hình lại các đặc tính của các kết nối sao cho phù hợp với yêu cầu của mạng.

Để kích hoạt màn hiển thị cấu trúc TCP/IP nhắp chuột vào **Start** → **Setting** → **Network and dial-up connection** ta sẽ có màn hiển thị như sau.

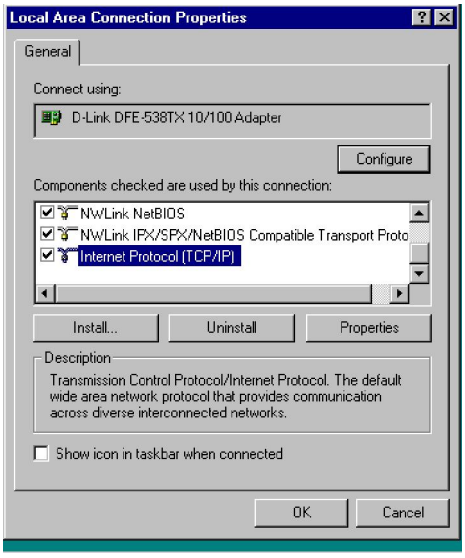


Nhắp chuột vào **Local Area Connection** để mở màn hình cấu trúc mạng LAN

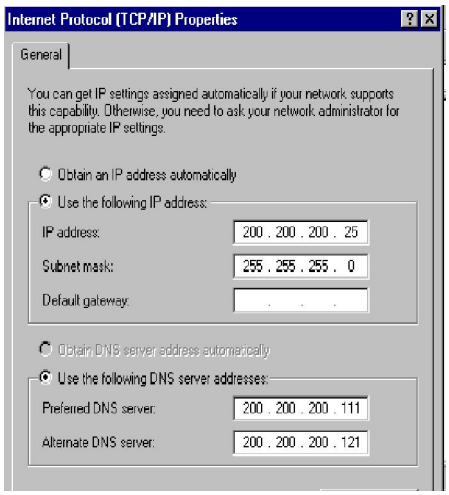


Tiếp theo nhắp chuột vào **Properties** để mở màn hình **Local Area Connection Properties**. Trang **General** của màn hình này liệt kê tất cả máy khách, dịch vụ và các giao thức đã được cài đặt cho card dùng cho mối kết nối này. Thường thì trong danh sách này đã có sắn giao thức TCP/IP, tuy nhiên nếu vì một lí do nào đó mà giao thức này chưa được cài đặt sắn thì ta vẫn có thể cài đặt giao thức này bằng cách nhắp chuột vào **Istall** → chọn **Protocol**→ **Add** → chọn **Internet Protocol (TCP/IP)** → **OK**.

Để cấu trúc lại TCP/IP thì từ trang **Local Area Connection Properties** Chọn **Internet Protocol (TCP/IP)** và nhắp chuột vào **Properties** để mở màn hình **Internet Protocol (TCP/IP) Properties.**



Trang **General** của màn hình **Internet Protocol (TCP/IP) Properties** cho phép bạn thiết lập địa chỉ IP và các thông tin về *DNS server*. Bạn có thể tự đưa vào địa chỉ IP hoặc nhận được tự động nhờ dịch vụ *Dynamic Host Configuration Protocol (DHCP)* hay *Automatic Private IP Addressing*.



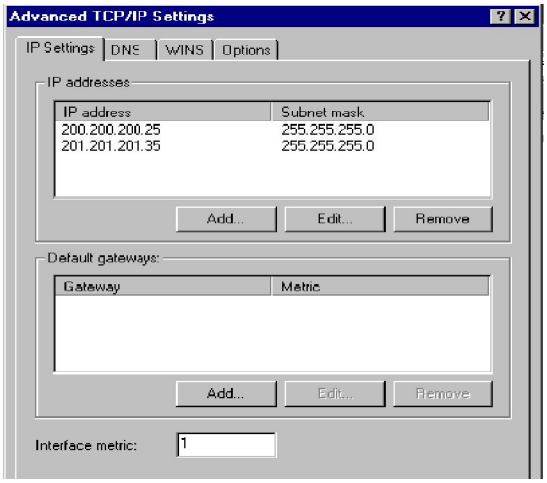
Nếu bạn chọn phương thức lấy địa chỉ IP tự động máy sẽ cố gắng lấy một địa chỉ từ *DHCP server*, nếu không được thì máy sẽ lấy từ *Automatic Private IP Address*. Địa chỉ mạng lấy tự động ngầm định là một địa chỉ lớp B: 169.254.y.z và sẽ mặc định lớp B *submask*.

Bạn cũng cần phải cung cấp *DNS server* để dùng vào việc đặt tên. *DNS server* thực ra là một cơ sở dữ liệu để gắn tên mỗi máy tính với một địa chỉ IP. Dùng tên máy tính sẽ dễ dàng hơn cho người sử dụng, nhưng tên máy tính lại không thể dùng cho việc thông tin giữa các máy tính với nhau. Máy tính chỉ có thể hiểu được địa chỉ IP mà thôi.

Để đặt thêm các đặc tính khác của TCP/IP bạn nhắp chuột vào **Advanced** để mở trang **Advanced Properties**.

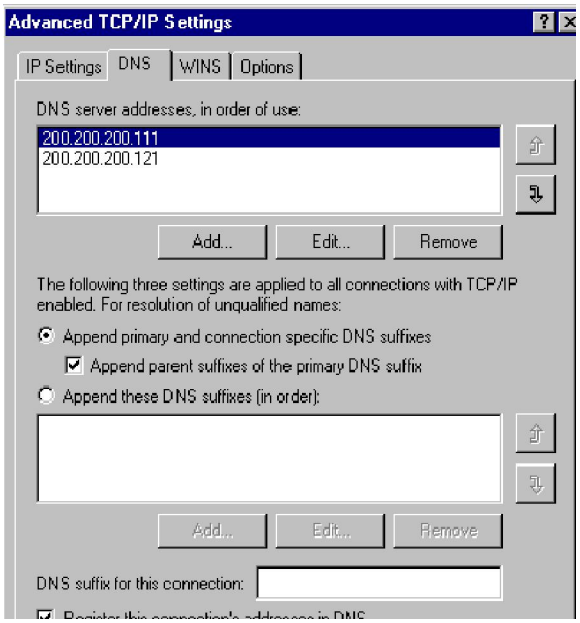
Avanced Properties - IP Setting

Trang này cho phép thêm nhiều địa chỉ IP khác nhau cho cùng một card mạng. Bạn làm như thế khi bạn muốn máy của bạn có thể được kết nối với các mạng khác nhau. Ví dụ bạn thiết lập 2 mạng trên cùng một đường cáp, 2 mạng này hoàn toàn không nhìn thấy nhau. Nếu bạn muốn một máy tính có thể liên lạc được với những máy chủ của cả 2 mạng đó thì bạn phải cung cấp cho nó địa chỉ của cả 2 mạng.



Avanced Properties - DNS Setting

Bạn có thể thiết lập thêm các các đặc tính của DNS thông qua trang **DNS properties**. Bạn cũng có thể thêm vào hay loại bỏ bớt các *DNS server* trong trang này.



Ở chế độ ngầm định thì mục **Append Primary and Connecion Speciffic DNS sufixes** sẽ được chọn. Sau đó máy sẽ tự động thêm tên miền vào sau tên của máy tính. Ví dụ tên miền của bạn là OPS.MYCOM.COM và tên máy tính của bạn là Comp33, như vậy tên DNS của máy bạn sẽ là:

COMP33.OPS.MYCOM.COM

Tuy nhiên bạn cũng có thể tự thiết lập một tên DNS riêng. Ví dụ nếu bạn chọn **Append these DNS sufixes (in order)** và bạn gõ vào:

DEV.MYCOM.COM

Như vậy tên DNS của máy tính bạn sẽ là

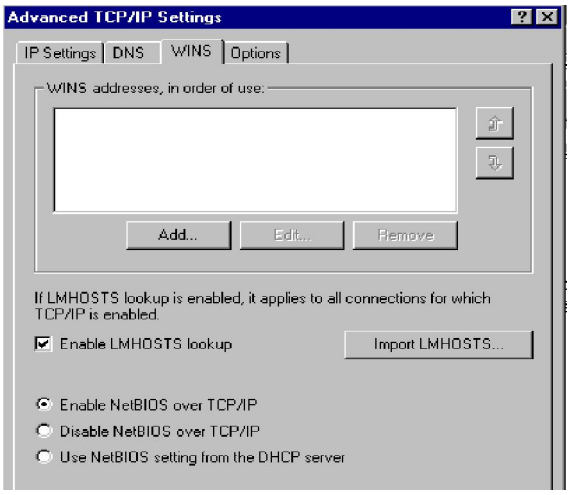
COMP33.DEV.MYCOM.COM

Nếu bạn chọn **Parent Suffixes of the primary DNS Suffix**. Khi đó tên DNS sẽ được thiết lập với phần đuôi là đuôi của mạng parent suffix. Như ở VD trên thì tên sẽ là:

COMP33.MYCOM.COM

Avanced Properties - WINS Setting

Window Internet Name Services (WINS) được sử dụng để giải quyết mối tương thích giữa tên NetBIOS với đ/c IP. Trang WINS cho phép bạn quản lý việc phân giải các tên NetBIOS cũng như việc hỗ trợ của NetBIOS cho các kết nối.



1.2. Troubleshooting TCP/IP

Windows 2000 cung cấp một số tiện ích để kiểm tra và khắc phục sự cố cho TCP/IP. Bảng sau sẽ miêu tả các tiện ích đó.

Option	Description
Ping	Xác thực cấu hình và kiểm tra các kết nối.
Arp	Hiển thị địa chỉ IP và địa chỉ vật lý của máy cục bộ.
Ipconfig	Hiển thị cấu hình TCP/IP hiện tại.
Nbtstat	Hiển thị các số liệu và các kết nối sử dụng NetBIOS over TCP/IP
Netstat	Sử dụng các số liệu của giao thức TCP/IP và các mối kết nối.
Route	Hiển thị và chỉnh sửa bảng định tuyến cục bộ.
Hostname	Hiển thị tên của máy chủ nơi mà bạn thực hiện lệnh đó.
Telnet	Cung cấp một sự mô phỏng với một máy chủ TCP/IP có chạy Telnet.
Finger	Lấy các thông tin từ một máy tính ở xa.
Tracert	Kiểm tra tuyến đường tới một hệ thống ở xa.

Tiếp theo sau chúng ta sẽ tìm hiểu kĩ hơn một chút về các tiện ích này.

1.3. Sử dụng Các Tiện ích (utilities) của TCP/IP

Trong phần này chúng ta sẽ bàn về các tiện ích (công cụ) để kiểm nghiệm cấu hình TCP/IP. Các công cụ này được chạy trong cửa sổ **Command Prompt**.

1.3.1. Hostname

Công cụ này có tác dụng gọi tên của máy mà bạn đang chạy lệnh này. Cú pháp của lệnh này như sau:

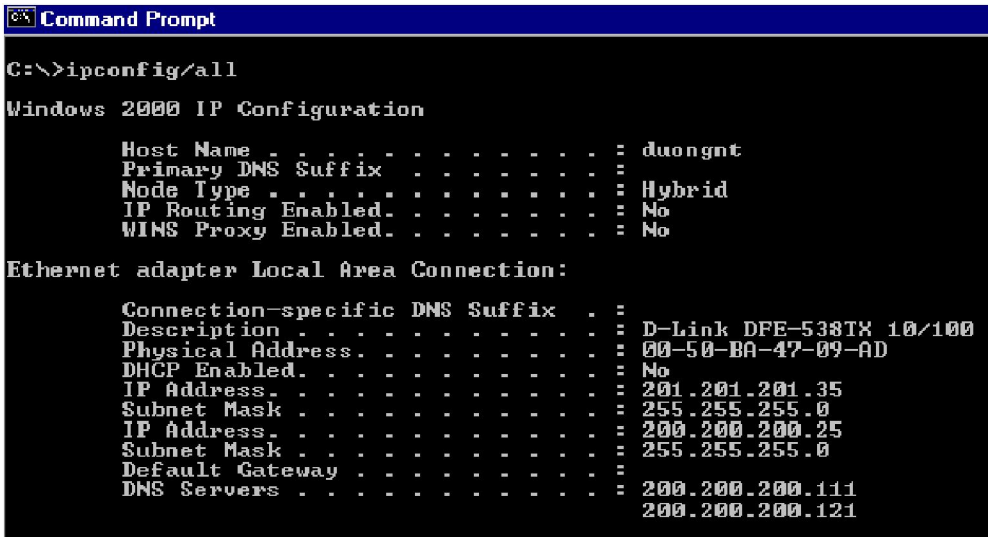
hostname ↵

1.3.2. Ipconfig

Lệnh này cho phép bạn xem cấu hình của TCP/IP hiện tại. Lệnh **ipconfig** hiện thị một bảng tóm tắt cấu hình TCP/IP bao gồm địa chỉ IP, *subnetmask*, và địa chỉ *gateway* mặc định. Nếu bạn thêm tuỳ chọn **/all** thì máy sẽ hiển thị thêm các tính năng khác nữa. Ví dụ từ dấu nhắc lệnh gõ vào lệnh

ipconfig / all ↵

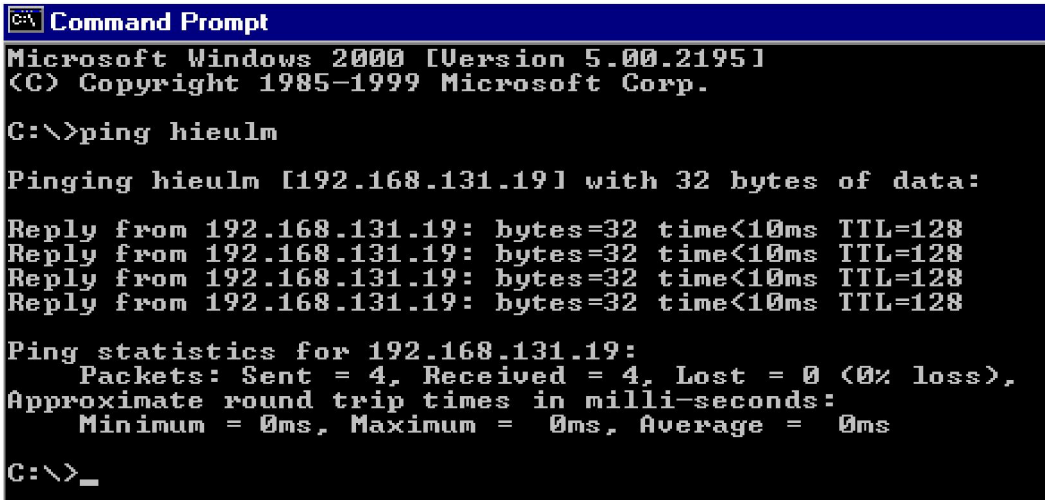
Bạn sẽ thấy một màn hình tương tự như trong hình sau.



Trong hình trên dòng đầu tiên cho bạn biết về tên máy chủ (*hotsname*). Dòng *Note Type* chỉ cách thức mà máy dùng để chuyển một tên NetBIOS thành một địa chỉ IP. Dòng *IP Routing Enabled* cho bạn biết máy này có đóng vai trò như một *IP router* không.

1.3.3. Ping

Ping là một lệnh cho phép bạn kiểm tra xem cấu hình TCP/IP có hoạt động tốt không bằng cách gửi một thông điệp ngắn đến một nốt mạng TCP/IP khác, hỏi rằng "cậu có ở đó không?". Nếu máy đó có ở đó nó sẽ trả lời đối với ping, và ping sẽ chuyển thông tin đó ngược trở lại cho bạn. Một ví dụ vè ping được thể hiện trong hình sau:



1.3.4. Nestat

Lệnh này cho phép bạn xem tất cả các thông tin về các mối kết nối sử dụng các giao thức của TCP/IP.

1.3.5. Using Ipconfig and Ping

Bạn có thể kết hợp cả hai lệnh ipconfig và ping để xác định cấu hình máy tính và các kết nối của router. Các bước sau đây chỉ cho bạn cách sử dụng các dụng cụ này:

1. Lệnh ipconfig được dùng để xác nhận rằng cấu hình TCP/IP đã được thiết lập.

2. Lệnh ping được dùng tương phản với loopback address (127.0.0.1) để xác nhận rằng TCP/IP được cài đặt đúng và bao trùm card mạng của bạn.

3. Lệnh ping được dùng với IP address của máy cục bộ để xác nhận IP address đó là duy nhất.

4. Lệnh ping được dùng với IP address của gateway (ngầm định) để xác nhận máy tính có thể liên lạc được với mạng cục bộ.

5. Lệnh ping được dùng với IP address của máy chủ xa để xác nhận máy tính có thể liên lạc được qua router.

2. DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

DHCP tối thiểu hoá quá trình quản trị địa chỉ IP bằng cách tự động gán các đ/c IP cho các máy khách khi chúng khởi động. Ngoài việc cung cấp cho các máy khách các đ/c IP và các subnetmask DHCP còn có khả năng cung cấp cho chúng các gateway mặc định, đ/c của DNS server và đ/c WINS server.

***Cài đặt và định cấu hình cho các DHCP server.**

DHCP server là máy mà có khả năng cung cấp các đ/c IP cho các máy khách khi chúng có yêu cầu truy cập vào mạng. Để làm được điều này các máy tram phải có cài đặt

thêm các phần mềm DHCP client. Các máy Win2000 profesional có kèm sắn DHCP client của chúng.

Cài đặt dịch vụ DHCP

Để cài đặt được dịch vụ DHCP hệ thống phải thoả mãn các yêu cầu sau:

- Có 1 đ/c IP tĩnh (cố định) để dùng cho DHCP server.
- Biết được một quỹ đ/c IP chưa dùng để cung cấp cho máy khách.

Để cài đặt DHCP server cần trải qua các bước sau:

1. Mở control panel.
2. Mở Add/Remove program.
3. Nhắp Add/Remove Windows Component

3. WINDOW INTERNET NAME SERVICES (WINS)

WINS là một dịch vụ dùng để giải đáp tên (Name Resollution) cho các máy chạy NetBIOS (Network Basis Input Output System). NetBIOS là một giao diện lập trình ứng dụng mạng (API) được Microsoft lập ra và được sử dụng rộng rãi trong các version cũ của window. Trước khi WINS ra đời thì việc phân giải tên do phần mềm LMHOSTS đảm nhiệm. LMHOSTS thực ra là một tập tin ASCII trong đó có chứa những địa chỉ IP và những tên của NetBIOS (gồm 15 kí tự) để dùng cho việc phân giải tên trong mạng. Tuy nhiên do nhiều hạn chế của LMHOSTS nên từ năm 1994 Microsoft cho trình làng phần mềm WINS.

***Cài đặt WINS Server**

Cần lưu ý là chỉ có WinNT server hoặc Win2000 server là có thể dùng để làm WINS server. Thực ra không cần thiết phải đặt cho mỗi mạng con một WINS server riêng, tuy nhiên cần có một máy thứ 2 chạy secondary WINS server để đảm bảo khả năng chịu lỗi. Cũng không nên đặt WINS server và Domain controler lên cùng một máy để tránh quá tải. Các bước để thiết lập một WINS server như sau.

1. Mở *Control Panel* ra.
2. Mở *Add/Remove Programs*
3. Nhắp vào Add/Remove Window components để mở Window components Wizard.
4. Nhắp Next .
5. chọn Networking Services rồi nhắp Details.
6. Chọn ô Window Internet Name Services
7. Nhắp OK.

8. Nhắp Next và đợi máy định cấu hình WINS.

9. Nhắp Finish trong Completting the Window Components Wizard để kết thúc.

WINS sẽ tự động active ngay mà không cần khởi động lại máy cũng như không cần bạn phải trao quyền cho nó. Các máy khách WINS sẽ tự động đăng kí với WINS server, nhưng những máy chạy các hệ điều hành cũ không có dịch vụ WINS thì bạn phải đăng kí với WINS server. Để làm điều này trước hết bạn mở cửa sổ WINS từ menu Addministrator Tools. Nhắp phải vào Active Registrations rồi chọn New Static Mapping. Trong trang này bạn điền vào tên NetBIOS của máy tính, Tầm NetBIOS, type of mapping và địa chỉ IP của máy tính.

CHƯƠNG 8

NỐI KẾT CÁC MÁY KHÁCH VÀO MẠNG WINDOW 2000 SERVER

---

1. CÁC KHÁCH HÀNG WINDOWS 2000

Mặc dầu Windows 9x đã được sử dụng khoảng 5 năm, nhưng thế giới máy tính vẫn là hỗn hợp các hệ điều hành. Microsoft Windows For Workgroup vẫn được sử dụng rộng rãi, thường có các khách hàng Windows 9x. Điều này là do nhiều tổ chức bị ràng buộc với phần cứng cũ không thể chạy các phiên bản mới hơn. Một số tổ chức không muốn chi phí để nâng cấp và huấn luyện nhân viên theo hệ điều hành mới.

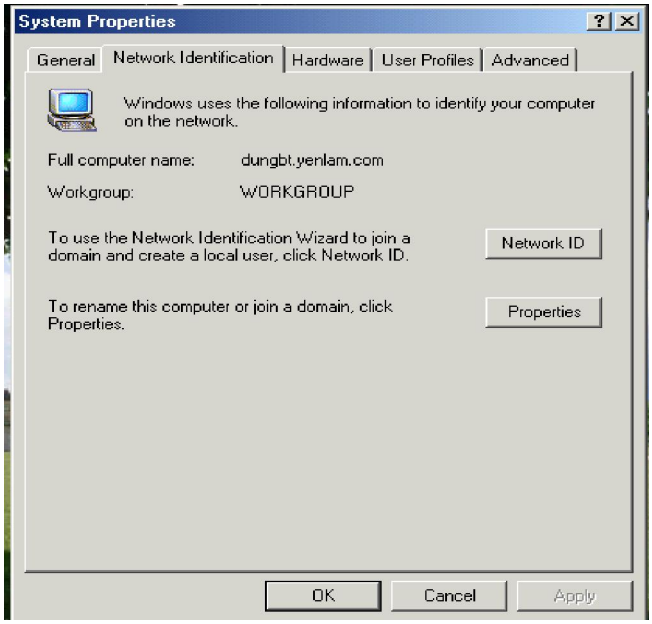
Tuy nhiên, khách hàng MS_DOS trên mạng Microsoft (dùng cho cả khách hàng mạng sử dụng MS_DOS và Windows 3.1) không còn được hỗ trợ nữa. Các thay đổi chính trong Microsoft Networking, do sử dụng Active Directory coi các khách hàng cũ này là không tương thích, trừ khi bạn chạy Windows 2000 Server trong chế độ tương thích NetBIOS, khi đó máy tính Windows 2000 Server sẽ hoạt động như máy chủ Windows NT 4.0 thay vì Windows 2000 Server. Chỉ có khách hàng Windows 2000 Professional là có khả năng nói chuyện với Windows 2000 Server theo chế độ chuẩn.

Bạn cần cách thức lập cấu hình một khoảng rộng các khách hàng mạng Microsoft. Chương này trình bày 4 loại khách hàng:

- Windows 2000 Professional.
- Windows NT Workstaion
- Windows 95 và Windows 98
- Windows For Workgroups 3.11

2. WINDOWS 2000 PROFESSIONAL LÀ KHÁCH HÀNG MẠNG

Phần này sẽ trình bày sự sử dụng Windows 2000 Professional, hệ điều hành để bàn mới nhất của Microsoft, làm khách hàng mạng. Nếu bạn cài đặt Windows 2000 Server, hầu như chắc chắn bạn sẽ có khách hàng Windows 2000 trên mạng.



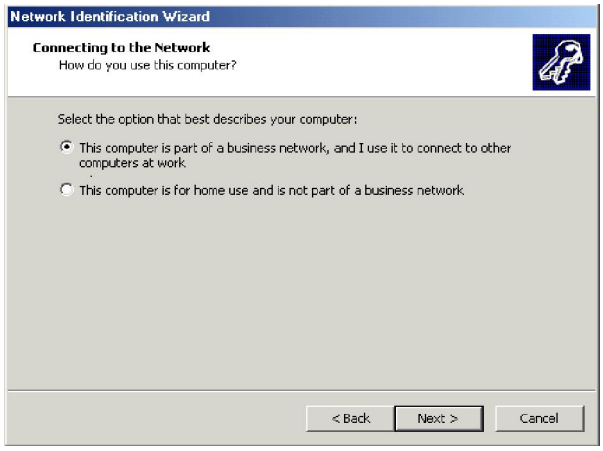
Hình 11.1: *Tab Network Identification được dùng để nhận biết và chỉnh sửa tên và nhóm làm việc vcủa máy tínhWindows 2000 Professional hoặc để nối vào vùng.*

Để xác lập Windows 2000 Professional làm khách hàng Windows 2000 Server bạn cần thực hiện các bước sau:

1. Từ Desktop của Windows 2000 Professional, bạn chọn biểu tượng Mycomputer và nhấp phải chuột. Điều này sẽ mở menu tương ứng. Bạn hãy chọn Properties và chọn tab Network Identification như hình 11.1

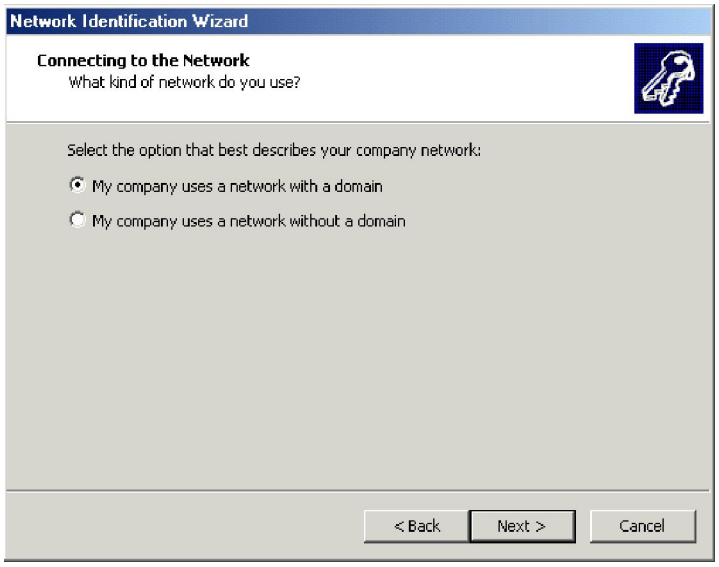
2. Nhấp nút Network ID khởi động Identification Wizard, hướng dẫn bạn lập cấu hình mạng. Bạn nhấp Next để tiếp tục

3. Tuỳ chọn thứ nhất đối với Network Identification Wizard là xem có cần máy tính đó tham gia vào mạng không.



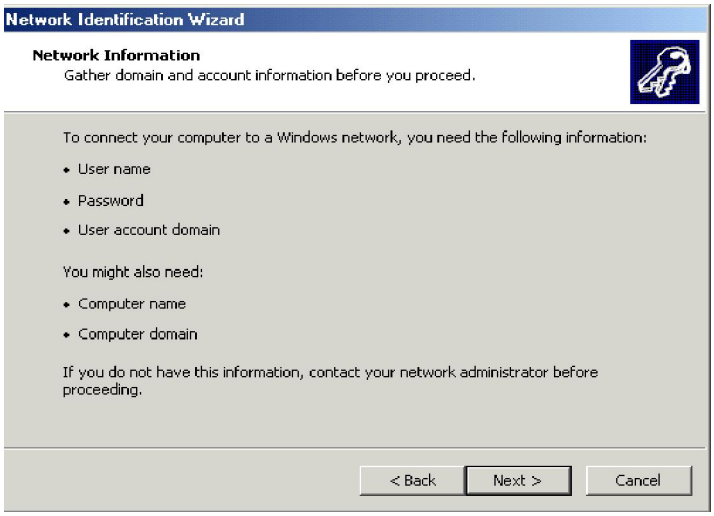
Hình 11.2: *Xác định việc lập cấu hình mạng dựa trên sử dụng của bạn*

4. Kế tiếp, Wizard cần biết bạn muốn nối kết vào vùng hay đơn giản chỉ tham gia vào mạng theo quan hệ ngang cấp.



Hình11.3: *Xác định kiểu mạng bạn cần, dựa trên sử dụng của bạn.*

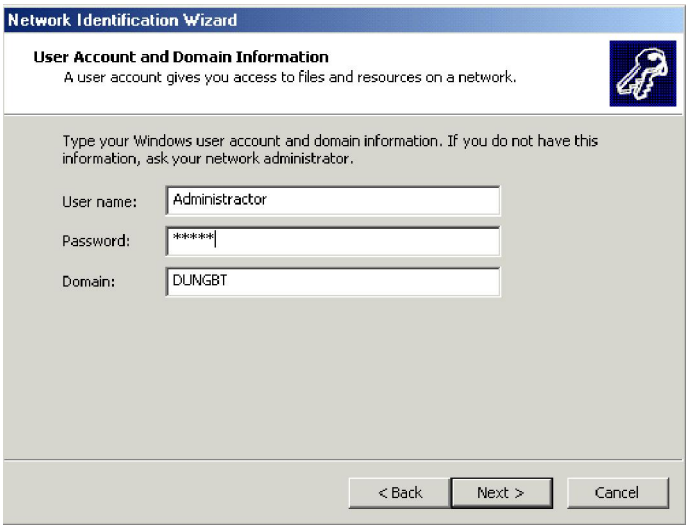
5. Hộp thoại Network Infomation hình 11.4, thông báo bạn cần thông tin vùng và tài khoản người dùng để tiếp tục .



Hình 11.4: *Bạn cần thông tin này để tiếp tục nối vào vùng*

6. Trong hộp thoại User Account and Domain Information hình 8.5, bạn nhấp thông tin đã chọn cho bước trước. Nếu bạn không có tài khoản trong vùng, bạn cần bổ xung tài khoản. Do ở đây người đăng nhập máy tính Windows 2000 Professtional là

Administractor tại chỗ, hộp thoại nêu ra User ID là Administrator, sau đó bạn cần nhập password của bạn và tên vùng bạn muốn nối vào. Nhấp Next để tiếp tục

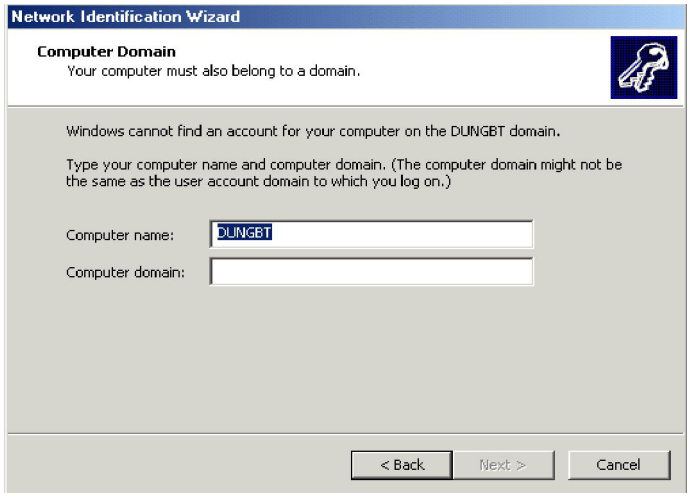


Hình 8.5: *Bạn hãy nhập tài khoản người dùng và thông tin vùng trước khi tiếp tục*

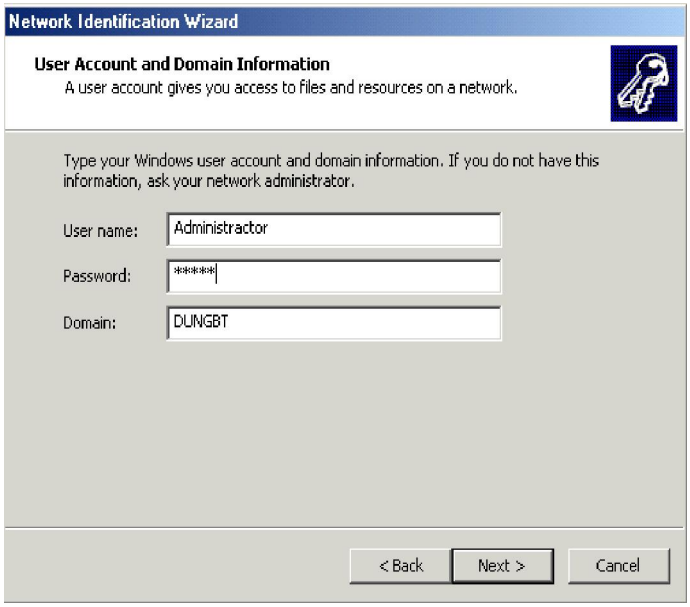
7. Kế tiếp, hộp thoại Computer Domain hình 11.6 xác nhận tên máy tính chẳng hạn là Dungbt, không có tài khoản trong vùng DUNGBT chẳng hạn,. Nếu máy tính của bạn có tài khoản trong vùng khác, đây là nơi để nhập tên vùng. Trong trường hợp này bạn cần tạo tài khoản máy tính trong vùng DUNGBT, do đó bạn nên nhấp nút Next.

8. Để nối kết vào vùng, bạn phải nhập ID người dùngcó phép bổ xung máy tính vào vùng đó, cùng password Hình 6-7. Bạn hãy nhấp OK để tiếp tục.

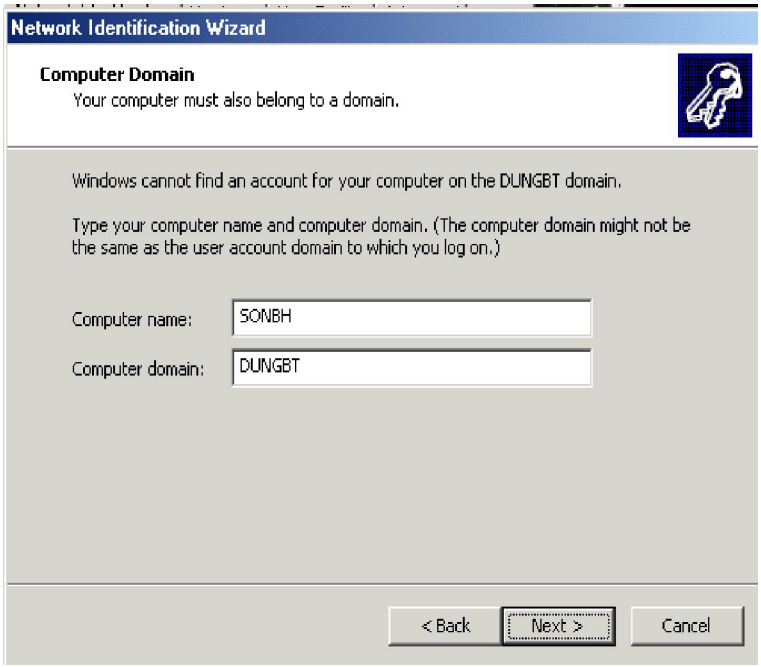
9. Kế tiếp, Network Identification Wizard cho phép bạn bổ xung tài khoản người dùng cho máy tính tại chỗ. Bởi vì bạn muốn xác lập tài khoản để sử dụng riêng, không phải là Administrator, bạn chọn để bổ xung người dùng SONBH cho máy tính Dungbt và cho vùng WORKGROUP. Điều này được nêu trên hình 11.8



Hình 11-6 Với Windows 2000 Professional, máy tính của bạn cũng phải là thành viên của vùng.



Hình 11-7: *Màn hình Domain User Name and Password*



Hình 11.8: *Bổ xung tài khoản người dùng*

10. Bạn có thể xác lập Access Level cho người dùng mới từ hộp thoại Access Level, bạn hãy nhấp Next để tiếp tục.

11. Sau khi xác lập Access Level, bạn hoàn tất Network Identification Wizard. Bạn hãy nhấp Finish đóng Wizard này.

Sau khi nhấp Finish bạn sẽ được nhắc khởi động lại PC để các thay đổi có hiệu lực. Khi đó hộp thoại SystemProperties phản ánh các thay đổi bạn đã thực hiện. Sau khi bạn nhấp OK, Wizard này đòi hỏi, bạn có muốn khởi động lại máy không, nếu bạn thực hiện điều đó, bạn sẽ được phép đăng nhập vùng này.

3. WINDOWS NT WORKSTATION 4.0 LÀ KHÁCH HÀNG MẠNG

Windows NT Workstaion phiên bản 4.0 hoặc cũ hơn, coi vùng Windows 2000 Server của bạn và các máy chủ theo các tên NetBIOS tương ứng, xuất hiện như máy chủ và vùng NT. Trong cả vùng Windows NT Server 4.0 (REINSTEIN) và vùng Windows 2000 Server(w2k) được nêu trong Network Neighborhood

Tính tương thích ngược này được cìa đặt theo mặc định trên Windows 2000 Server, tuy nhiên, nếu được kết cấu hạ tầng của bạn chuyển đến Active Directory Sevice gốc, tuỳ chọn này có thể không khả dụng, bạn cần cài đặt Windows 2000 Professional làm hệ điều hành Destop của mình.

Để bổ xung Windows NT Workstaion vào vùng Windows 2000, bạn cần thực hiện các bước sau:

1. Cài đặt Microsoft Networking bằng cách mở Networking gồm cả sự cài đặt thẻ mạch mạng Ethernet và giao thức trong Windows NT 4.0 vượt ra ngoài phạm vi chương này ở đây giả thiết mạng đã được cài đặt sẵn.

2. Nhấp đúp biểu tượng Network và chọn Tab Identification. Bạn sẽ thấy tên và vùng hoặc nhóm làm việc đã chọn khi bạn cài đặt Windows NT Workstation 4.0

3. Bạn hãy nhấp nút Change. Hộp thoại kết quả, cho phép bạn đổi từ nhóm làm việc hiện hữu hoặc tên vùng sang vùng Windows 2000 mới. Do tính tương thích ngược của Windows 2000, vùng Windows 2000 mới sẽ xuất hiện đối với hệ thống Windows NT Workstation 4.0 như một vùng NT 4.0.Để thây đổi các vùng, bạn cần ID người dùng và password đối với tài khoản có cho phép bổ xung máy tính cho vùng. Sau khi nhập tên vùng mới, bạn hãy nhấp OK. Sau khi hoàn tất sự thay đổi này, bạn sẽ nhận được thông báo chào mừng bạn ở vùng mới, bạn hãy nhấp OK.

4. Nhấp OK trên hộp thoại tính chất Network, sau đó khởi động lại máy tính để đăng nhập vùng mới.

4. WINDOWS 95 VÀ WINDOWS 98 LÀ KHÁCH HÀNG MẠNG

Windows 95 và Windows 98 là các hệ điều hành Plug and Play. Chúng được thiết kế tìm phần cứng cho máy tính của bạn và lập cấu hình một cách thích hợp. Sự tự lập cấu

hình được mở rộng sang thiếit lập mạng. Nếu hệ điều hành phát hiện thẻ mạch mạng, sẽ cố gắng chạy tải trình điều khiển và chạy trình khách hàng mạng.

Windows 98 có tính tự lập cấu hình rất cao, đơn giản không cho bạn xoá trình điều khiển đối với thẻ mạch mạng. Nếu thẻ mạch mạng được cài đặt thẻ đó thường được phát hiện và trình điều khiển được thiết lập lại khi bạn khởi động lại máy tính. Vì những lý do đó, ở đây sẽ không cần trình bày sự lập cấu hình trình khách hàng dối với Windows 95 và Windows 98, phần lớn công việc được thực hiện độc lập dù bạn muốn hay không.

Với thời gian, bạn sẽ cần bổ xung trình điều khiển thẻ mạch mạng thay, thay đổi giao thức,hoặc lập lại cấu hình một vài đặc tính mạng, do vậy phần này sẽ trình bày các quy trình đó.

4.1. Cài đặt mặng Windows 95 và 98

Nếu bạn đã cài đặt thẻ mạch mạng, có lẽ thẻ mạch đó được phát hiện khi bạn cài đặt Windows 95 hoặc 98 trừ khi đó là thẻ mạch mới không có trong danh sách của phần mềm đó.

Windows 95 cung cấp tuỳ chọn để tìm thẻ mạch mạng, nếu bạn kiểm ô kiểm Network Adapter. Setup Wizard sẽ quuét hệ thống của bạn để tìm thẻ mạch đó, và có lẽ sẽ tìm được. Windows 98 tìm thẻ mạch này một cáh tự động.

Vài thẻ mạch mạng có tính năng riêng có thể gây nhầm lẫn cho các chương trình Setup.Bạn cần đảm bảo xác nhận thẻ mạch của mình trong quá trình Setup.

Sau khi xác lập Windows 95 hoặc 98, bạn hãy dùng Network trong Control Panel để thực hiện các các thay đổ về cấu hình mạng. Nêu ra Network khi xuất hiện trong Windows 95 và 98.

4.2. Lập cấu hình các thành phần mạng

Windows 98 có khả năng tự xác lập phần cứng, abnj sẽ không cần bổ xung bằng tay trình điều khiển thẻ mạch mạng trừ khi bạn sử dụng phần cứng mới, Windows 2000 không thể nhận biết. Windows 95 là hệ điều hành cũ do đó bạn cần cài đặt các trình điều khiển mạng sau khi cài đặt phần cứng mới.

Nếu Windows 95 và 98 không tìm được thẻ mạch mới và không caig đặt trình điều khiển đúng, hoặc bạn cần cài đặt các trình điều khiển cập nhật cho thẻ mạch mạng, bạn hãy bổ xung trình điều khiển thẻ mạch mạng như sau:

Bổ xung trình điều khiển cho thẻ mạch mạng

Bước thứ nhất trong việc lập cấu hình mạng Windows 9x là càI đặt thẻ mạch mạng:

1. Mở Network và chọn Tab Configuration.

2. Nhấn Add để mở hộp thoại Select Network Component Type Chọn Adapter trong hộp thoại danh sách Click the Type of Network Component You Want to Install. Sau đó nhấp Add để mở hộp thoại Select Network adapters

3. Trong hộp thoại Select Network adapters, bạn thực hiện một trong hai việc dưới đây:

- Nếu bạn cài đặt sản phẩm được liệt kê, hãy chọn một mục trong hộp danh sách Manufacturer, sau đó chọn sản phẩm trong danh sách Network Adapters.

- Nếu bạn cài đặt sản phẩm không được liệt kê, hoặc sản phẩm của bạn có trình điều khiển mới, hãy nhấp Have Disk. Khi được nhắc, bạn hãy chọn đương dẫn đến nơi chứa các trình điều khiển đó, thường là trên đĩa mềm trong ổ A:

Windows cài sẵn trình điều khiển cho thẻ mạch mạng Clent for Microsoft Networks, và các giao thức mạng mặc định .

4. Nếu bạn không thích các giao thức mặc định Windows đã chọn bạn có thể xoá giao thức. Bạn hãy chọn giao thức trong danh sách The Flowing Network Components Are Installed, sau đó nhấp Remove.

5. Để bổ xung giao thức cho cấu hình:

a) Bạn hãy nhấp Add trong hộp thoại Network

b) Chọn Protocol trong hộp thoại Select Network Component Type, sau đó nhấp Add để mở hộp thoại Select Network Protocol

c) Chọn nhà sản xuất trong danh sách Manufacturers

d) Chọn giao thức trong dang sách Network Protocol. Nếu bạn chọn giao thức đòi hỏi cấu hình, bạn sẽ thấy hộp thoại cần thiết khi thoát khỏi Network. Bạmn hãy nhập các tính chất thích hợp trong các hộp thoại đó.

6. Nếu bạn đã cài đặt nhiều khách hàng mạng, bạn hãy kiểm chứng khách hàng được chọn trong hộp danh sách Primary Network Logon. Khi Windows95 hoặc 98 khởi động, sẽ sử dụng trình khách hàng chuyên biệt trong trường này để thực hiện sự nỗ lực đăng nhập lên mạng.

7. Bạn hãy chọn tab Identification. Tab này có các trường hợp sau:

- *Computer Name*: Nói chung mục này thương trùng với tên người dùng mạng

- *Workgroup:* giá trị này tương hợp với tên nhóm làm việchoặc vùng máy tính đăng nhập. Nếu máy tính đăng nhập một vùng trường này phải có tên vùng đó.

Computer Description. ở đây bạn có thể nhập thông báo ngắnđể nhận biết may

tính. Mô tả này xuất hiện với tên máy tính trong các danh sách duyệt.

8. Bạn hãy trở lại tab Configuration và kiểm tra các tính chất của trình khách hàng Microsoft Network. Nhấp đúp Client for Microsoft Network để mở hộp thoại Microsoft Network Properties. Hộp thoại này có các trương hợp sau:

- *Logon to Windowns NT Domain.*Nếu bạn kiểm trường này, Windows 95 hoặc 98 sẽ đăng nhập vùng thay vì nhóm làm việc.
- *Windows NT Domain.* Nếu trường Logon to Windows NT Domain được kiểm, trường này phải chuyên biệt tên vùng Windows 2000 Server máy tính được đang nhập . Giá trị của trường này phải phải tương hợp với giá trị của trường Workgroup trên tab Identification.
- *Quick Logon.*Nếu nut này được chọn, Windows 9x sẽ không nối kết lâu dài khi người dùng đăng nhập. Nối kết lâu dài chỉ được thiết lập khi người dùng cố gắng truy cập nguồn tài nguyên dùng chung. Quá trình đăng nhập tốn ít thời gian hơn với tuỳ chọn này, nhưng người dùng sẽ bị chậm khi kết nối tài nguyên dùng chung.
- *Logon and Restore Network Conections.*Nếu nút này được chọn, Windows 9x cố gắng thiết lập lại mọi kết nối lâu dàikhi người dùng đăng nhập.Tuỳ chọn này có thể kéo dài quá trình đăng nhập, nhưng sẽ cải thiện tính đáp ứg khi người dùng được đăng nhập.

9. Nếu máy tính này sẽ chia sẻ các tập tin hoặc các máy in của miình trên mạng, bạn nhấp File And Print Sharing để mở hộp thoại File And Print Sharing có chứa các ô kiểm:

- I Want to Be Able to Give Other Access to My Files.
- I Want to Be Able to Allow Others to Print to My Printer(s)

Nếu bạn chọn một trong hai ô kiểm đó, tuỳ chọn File and Printer Sharing for Microsoft Network được bổ xung vào danh sách các thành phần mạng đã cài đặt.

10. Sau khi bạn lập cấu hình các thẻ mạch mạng, giao thức và các khách hàng, theo yêu cầu, bạn hãy thoats khỏi Network. Trong hầu hết các trường hợp bạn phải khỏi động lại để kích hoạt các thay đổi.

4.3. Đăng nhập

Khi Windows khởi động lại, sẽ cố gắng nối vào mạng, nếu bạn chuyên biệt vùng, bạn được nhắc gõ Password của mình để đăng nhập mạng Microsoft. Windows 9x ghi nhớ tên người dùng mạng của bạn ở các phiên làm việc, nhưng bạn phải nhập Password mỗi khi đăng nhập.

Quy chiếu các ổ đĩa đến tài nguyên dùng chung

Nếu bạn thông thạo Windows 2000, bạn có lẽ đã biết các tính năng kết nối và trình duyệt của Windows 9x. Trước hết Windows 2000 sử dụng giao diện người dùng của Windows 9x. Để quy chiếu chia sẻ tập tin mạng bạn hãy thực hiện các bước sau:

1. Duyệt các nguồn tài nguyên mạngtrong Network Neighborhood hoặc trong Windows NT Explorer.

2. Sau khi tìm được chia sẻ bạn muốn kết nối, hãy nhấp phải chia sẻ đó để mở hộp thoại tương ứng.

3. Chọn Map Network Drive từ menu đó để mở hộp thoại Map Network Drive. Hộp thoại này có hai trương mục nhập dữ liệu:

- *Drive* Bạn hãy nhập kí tự ổ đĩa cần quy chiếu.
- *Reconnect at Logon* Hãy kiểm ô này để thiết lập kết nối lâu dài. Tuỳ theo các xác lập trong hộp thoại Client for Microsoft Network Properties, các kết nối lâu dài được thiết lập lại khi bạn đăng nhập (Quick Logon) hoặc khi lần đầu bạn nối vào nguồn tài nguyên (Logon and Restore Network Connectional)

4. Nhấp OK để quy chiếu ổ đĩa.

Nối kết các máy in chia sẻ

Sự xác lập máy in được quản lý bằng Wizard được dùng để bổ xung máy in cho cấu hình của bạn. Để bổ xung máy in bạn cần làm các bước sau:

1. Bạn hãy mở hồ sơ Printer trong My Computer.

2. Nhấp đúp Add Printer để khởi động Add Printer Wizard

3. Khi được đề nghị chuyên biệt cách thức nối máy in vào máy tính, bạn hãy chọn Network Printer.

4. Khi được hỏi để chọn đường dẫn hoặc tên dãy thứ tự, bạn hãy nhấp ô Browse để mở ô trình duyệt, ở đó bạn có thể xem và chọn máy in chia sẻ.

5. Hoàn tất xác lập máy in như máy in thông thường.

6. Windows 9x có thể nhận biết kiểu máy in bằng cách tìm kiếm Windows 95 hoặc 98 đã được cài đặt trên máy dịch vụ in, chúng có thể được truy nhập bằng Windows 9x, và không cần cài đặt các trình điều khiển trên máy tính tại chỗ. Nếu các trình điều khiển càn thiết không được cài đặt trên máy dịch vụ in, các trình điều khiển đó được cài đặt trên máy tính tại chỗ.

5. TẠO KHẢ NĂNG HOẠT ĐỘNG CHO WINDOWS FOR WORKGROUP

Windows For Workgroup có thể được dùng để xây dựng các mạng đồng cấp hỗ trợ sự chia sẻ tậptin vào máy in. Các trình tiện ích được gộp trong Windows For Workgroup đã có tính chất mạng. Print Manager có thể chia sẻ các máy in tại chỗ và nối đến các máy in chia sẻ trên mạng. File Manager có thể chia sẻ các tập tin và nối đến các tập tin chia sẻ. Mặc dầu bạn có thể tạo mạng với Windows 3.1, nhưng các tiện ích trong Windows 3.1 không thể tham gia vào mạng với cùng mức độ các tiện ích trong Windows For Workgroups.

Mọi thứ bạn cần lập cấu hình khách hàng Windows For Workgroup 3.11 đều được gộp trong sản phẩm này, phần này sẽ trình bày về phương pháp cài đặt phần mềm mạng, nối vào vùng và truy cập tài nguyên vùng.

5.1. Cài đặt phần mềm mạng Windows For Workgroups

Khi Windows For Workgroups được càI trên máy tính mạng, setup thường càI đặt phần mềm mạng và lập cấu hình Windows For Workgroups để tham gia vào nhóm làm việc.

Nếu máy tính Windows For Workgroups đã tham gia nhóm làm việc, phần mềm mạng cũng được càI đặt, bạn có thể bỏ qua phần này và đọc tiếp phần "nối kết vào vùng".

Phần này trình bày các quy trình từng bước bổ xung phần mềm mạng vào bản sao Windows For Workgroups đã càI đặt. Để bổ xung phần mềm mạng vào Windows For Workgroups bạn cần thực hiện các bước sau:

1. Chạy tiện ích Windows setup. Biểu tượng Windows setup thường được lưu trong nhóm chương trình chính. Trong hộp thoại Windows Setup, trường Network nêu ra No Network Installed.

2. Chọn lệnh Change Network Settings trong menu Options. Hộp thoại Network Setup hiển thị (hình 6.19). Hộp thoại này là tiêu đIểm của hầu hết các quy trình lập cấu hình mạng Windows For Workgroups.Trong không có tính năng mạng nào được kích hoạt.

3. Để cài đặt sự hỗ trợ mạng, bạn hãy nhấp Networks để hiển thị hộp thoại Networks

4. Để cài đặt các giao thức, bạn hãy nhấp nút Install Microsoft Windows Network và nhấp OK. (Nếu mạng của bạn có Netwere và các mạng được hỗ trợ khác, bạn cần chọn Other và tuân theo các quy trình cho kiểu mạng đó). Bạn trở lại hộp thoại Networks Setup lúc này cho biết Setup sẽ cài đặt Microsoft Windows Network (phiên bản 3.11). Nhấp OK để tiếp tục.

5. Setup cố gắng tìm các thẻ mạch trong PC,, sẽ tìm được các thẻ mạch cũ, nhưng không tìm được các trình đIều khiển cần thiết để hỗ trợ các thẻ mạch mới.

6. Nếu bạn phải chọn trình đIều khiển thẻ mạch mạng, bạn thực hiện đIều đó từ danh sách trong hộp thoại Add Network Adapter, được nêu trên. Trên hình này NE 2000 được chọn.

7. Tiếp đến chuỗi các ô cho phép bạn chọn các xác lập đối với thẻ mạch mạng của bạn. Trong trường hợp NE 2000, sự ngắt và cổng I/D đã được xác nhận. Nếu bạn chọn sự ngắt chuyên biệt cho nguồn tàI nguyên khác, Setup sẽ cảnh báo. Nêu ra sự cảnh báo khi Interup 3 được chọn.

8. Sau khi chuyên biệt các xác lập thẻ mạch, Setup đưa ra hộp thoại Microsoft Windows Network Name ở đây bạn phảI chọn:

- *Tên người dùng* Mục này phảI tương hợp tên người dùng được nhận biết bởi vùng người này sẽ truy nhập.
- *Nhóm làm việc.*Đây có thể là nhóm Windows For Workgroups (mặc định là WORKGROUP) hoặc có thể là vùng. Bạn nên tránh dùng tên mặc định là WORKGROUP, đặc biệt nếu là mạng của bạnđược nối vào WAN.
- *Tên máy tính.* Tên này phải là duy nhất cho máy tính đó trên mạng. Các tên nhóm và tên máy tính có thể đến 15 ký tựvà có thể gộp các ký tự sau: ! # $ ( ) - _. @ ^ ’ ~. Các khoảng trống giữa các ký tựlà không được phép.

9. Nhấp OK khi các tên mạng đã được chọn. Setup đã bắt đầu cài đặt các tập tin. Bạn hãy lắp các đĩa và chuyên biệt vị trí các tập tin khi được nhắc. Setup sẽ chỉnh sửa các tập tin Autoxec.BAT, SYSTEM, INI, và PROTOCOL.INI

10. Sau khi các tập tin được cài đặt, mày tính phải được khởi động lại để kích hoạt phâme mềm mạng, bạn sẽ có tuỳ chọn Restart Your Computer Now, bạn hãy nhấp Restart Your Computer Now để kích hoạt mạng.

11. Khi khởi động lại Windows, bạn sẽ thấy hộp thoại Wellcom to Windows For Workgroups. Hộp thoại này có hai trường hợp:

- *Logon name*. Tên này tương hợp với tên đã chọn trong bước 8.
- *Password*. Bạn cần nhập password cho người dùng này sẽ nhập đẻ truy nhập mạng nhóm làm việc.

12. Kế tiếp, bạn sẽ thấy thông báo ô ‘There is no password list file for user name. Do you want ti create one now ? ’ Bạn nhấp OK.

13. Hộp thoại Confirm User Password yêu cầu bạn nhấp Password lần thứ hai. Bạn

gõ lại và nhấp OK.

Windows For Workgroups mã hoá Password bạn đã nhập và lưu nó trong tập tin *username*.PWL ở thư mục Windows. Lần kế tiếp người dùng đăng nhập Windows For Workgroups, passwor yêu cầu được đối chiếu vớ Password trong tập tin PWL. Nếu Password trống được nhập vào, sẽ không có Password xuất hiện khi Windowns For Workgroups khởi động.

Máy tính lúc nàyđược xác lập thâm gia trên mạng nhưng không đăng nhập vào vùng.

5.2. Nối kết vào vùng

Sau khi máy tính Windows For Workgroups được lập cấu hình để đăng nhập mạng, bạn có thể tạo khả năng cho máy tính đó đăng nhập vào vùng. Banj hãy khởi động tiện ích Network trong Control Panel. Hộp thoại Microsoft Windows Network có thể được lập cấu hình cho nhiều xác lập mạng Windows For Workgroups. Để lập cấu hình cho Windows For Workgroups đăng nhập vào vùng, bạn thưc hiện các bước sau:

1. Nhấp nút Startup để hiển thị hộp thoại Startup Settings, trong đó có các ô kiểm:

- *Log On at Startup.* Việc kiểm ô này sẽ cho bạn đăng nhập tự động khi Windows For Workgroups khởi động.

- *Enable Network DDE.* Nếu bạn sử dụng DDE mạng với các ứng dụng của bạn, bạn hãy kiểm ô này, bạn chỉ cần kiểm ô này nếu nếu cần sử dụng DDE mạng bởi vì tuỳ chọn này hoạt động sẽ cần đến 50KB.

- *Ghosted Conections.* Chọn tuỳ chọn này sẽ tiết kiệm thời gian khi khởi đầu do chưa thiết lập các nối kết đến các nguồn tài nguyên cho đến khi sử dụng chúng các kí tự ổ đĩa được kết nối cho cácthiết lập lâu dài.

- *Enable WinPopup.* WinPupop là tiện ích hiển thị thông báo sẽ hiển thị các thông báo cho mạng Windows. Nếu bạn định gửi thông báo cho nhiều người dùng, bạn hãy kích hoạt tuỳ chọn này. Winpupop còn nhận các thông báo xác nhận từ các máy tính dịch vụ in trong vùng.

2. Kiểm ô Log On to Windows NT or LAN Manager Domain để kích hoạt Windows For Workgroups đăng nhập Windows NT khi khởi động.

3. Nhấp tên vùng đăng nhập trong ô Domain Name

4. Nhấp Set password để nhập Password đăng nhập

5. Nếu bạn không muốn nhận thông báo xác nhận sự đăng nhập thành công, bạn hãy kiểm ô Don’t Display Message On Successful Logon.

6. Nhấp OK. Bạn được nhắc khởi động lại máy tính.

7. Khi Windows For Workgroups khởi động lại, bạn nhân được hộp thoại Domain Name Logon. Bạn hãy nhập Password cho vùng đã chọn.

8. Nếu bạn chọn Save This password in Your Password List, Windows For Worgroups sẽ mã hoá Password của vùng này và lưu vào trong tập tin PWL của người dùng đó.

9. Tiếp sau sự đăng nhập vùng thành công, Windows For Workgroups gửi thông báo xác nhận tương tự như.

5.3. Nối vào các thư mục chia sẻ

Một việc bạn cần thực hiện sau khi lập cấu hình mạng là nối vào các chia sẻ tập tin trên máy dịch vụ. Để yhưc hiện việc này bạn cần:

1. Chạy File Manager
2. Chọn lệnh Conect Network Drive trong menu Disk.
3. Chọn ký tự ổ đĩa và duyệt qua mạng đêt tìm thư mục chia sẻ
4. Chọn điã được kết nối lại khi khởi động
5. Nhấp OK

Sự nối kết đĩa này có thể được dùng như ổ đĩa ảo.

5.4. Nối kết các máy ing dùng chung

Khác với Windows 2000, các máy tính Windows For Workgroups không thể đọc các trình điều khiển in từ máy dịch vụ in. Trước khi máy tính Windows For Workgroups có thể sử dụng máy in dùng chung ở máy dịch vụ in Windows NT, các trình điều khiển phải được cài đặt trên máy tính đó. Sau đay ta sẽ trình bày phương pháp kết nối:

1. Bạn hãy mở Print Manager và chọn máy in cần kết nối, máy in này được cài đặt một cách tự động cho cổng tại chỗ khi trình điều khiển được cài đặt. Bạn hãy nhấp Connect trong cửa sổ Printes để mở hộp thoại Connect.
2. Chọn cổng còn trống trong hộp danh sách Ports.
3. Nhấp OK, máy in lúc này đã được cài đặt ở cổng đã chọn.

Để kích hoạt máy in này để in trên mạng bạn phải nối máy in đó vào máy in dùng chung. Điều này được thực hiên trong Print Mánger.

Để in trên máy in mạng, bạn thực hiện các bước sau:

1. Khởi động Print Manager
2. Chọn máy in có tên (không chia sẻ).

3. Chọn Connec Network Printer tù menu Printer, hộp thoại này xuất hiện.

4. Duyệt máy in có thể được dùng chung và chọn máy đó đểnlưu đường dẫn trong ô Path hoặc đường dẫn bàng tay

5. Kiểm Reconnect at Startup nếu kết nối máy in được thiết lạp lại mỗi khi Windows For Workgroups khởi động

6. Nhấp OK

7. Nhấp OK để trở về Printer Manager. Danh sách máy in nêu ra đương dẫn tài nguyên nối máy in đó.

6. SỬ DỤNG CÁC LỆNH KHÁCH HÀNG MẠNG

Lệnh NET chấp nhận nhiều biển thể lệnh điều khiển các chức năng, chẳng hạn đăng nhập, đăng xuất và các nối kết nguồn tài nguyên. Các lệnh này có thể dùng một cách tương tác, nhưng có lẽ rất giá trị khi được gộp trong các Script đăng nhập.

Phần này trình bày vài lệnh NET hứu dụng nhất. Danh sách các lệnh NET có thể có tong Windows Help, tuy nhiên không phải mọi lệnh liệt kê trong Help đều được hỗ trợ ở trình khách hàng.

Để liệt kê các lệnh NET khả dụng trong ở dòng nhắc lệnh, bạn hãy nhập lệnh NET HELP. Để nhận được sự giải thích chi tiết về từng lệnh, bạn hãy nhập NET HELP COMMAND, trong đó COMMAND là lệnh bạn muốn biết chi tiết. Từ dòng lệnh này cũng có thể gõ NET / ? để xem các tuỳ chọn.

Lệnh NET HELP

NET HELP Hiển thị tóm tắt các tuỳ chọn lệnh NET. Bạn có thể hiển thị chi tiết về lệnh bất kỳ bằng cách gõ gộp lệnh đó trong tuỳ chọn. Ví dụ để xem xét về lệnh LOGON bạn hãy gõ**:**

NET HELP LOGON

Lệnh NET LOGON khởi động hộp thoại đăng nhập. Được nhập một cách độc lập, NET LOGON nhắc bạn về tên người dùng và Password ở dạng tham số ví dụ, isaac muốn đăng nhập vùng mặc định hoặc nhóm làm việc với password là apple**:**

NET LOGON ISAAC APPLE

Vùng khác có thể đước chọn với tuỳ chọn/domain: domainname.

Ví dụ: NET LOGON MARIE RADIUM/ DOMAIN: MALAPROP.

Lệnh NET LOGOFF

Lệnh NET LOGOFF ngắt kết nối đăng nhập mạng cảu bạn. Nếu bạn gộp tuỳ chọn /YES, bạn sẽ không được đề nghị xác nhận yêu cầu đăng xuất của bạn

Lệnh NET USER

Các đĩa và các máy in được kết nối và ngắt kết nối với lệnh NET USER. Để nối ổ C: và chia sẻ APPS trên MALA PROP1, bạn hãy dùng lệnh:

NET USER C:\\ MALAPROP1\APPS

Lệnh kế tiếp sẽ nối LPT1: vào máy in WIDGETS1 trên MALAPROP 1:

NET USER LPT1:\\MALOPROP1\WIDGEST 1

Bạn hãy bổ xung tuỳ chọn /PERSISTENT: YESđể chuyên biệt các nối kết cần được thực hiện khi Workstation Connection khởi động.

Để xem danh sách các nguồn tài nguyên được nối kết của bạn, hãy nhập lệnh NET USER không kèm theo các tuỳ chọn.

Lệnh NET VIEW

Lệnh NET VIEW dùng để liệt kê các máy tính và các nguồn tài nguyên dùng chung. Nhập NET VIEW không có các tuỳ chọn sẽ liệt kê các máy tính chia sẻ nguồn tài nguyên trong vùng của bạn. Bạn hãy gộp tên máy tính để liệt kê các nguồn tài nguyên dùng chung trên máy tính đó. NET VIEW \\ DUNGBT liệt kê các nguồn tài nguyên dùng chung trên DUNGBT.

Lệnh NET TIME

NET TIME Cung cấp phương tiện đồng bộ hoá đồng hồ của máy tính với đồng hồ trên máy tính khác. Nói chung bạn nên đồng bộ hoá các đồng hồ trong môi trường chia sẻ để người dùng có thể chắc chắn các dấu thời gian và ngày tháng đều có ý nghĩa. Để đồng bộ háo đồng hồ khách hàng với máy tính DUNGBT bạn nên dùng lệnh:

NET TIME \\ DUNGBT / SET / YES.

Tham số YES thực thi lệnh NET TIME không cần xác nhận.

Lệnh NET STOP

Lệnh NET STOP dỡ tải các dịch vụ. Để dở tải popup, bạn hãy nhập lệnh:

NET STOP POPUP.

Bạn có thể dừng Redirector mặc định, ngắt kết nối mạng, bằng cáh nhập lệnh sau:

NET STOP WORKSTATION

Lệnh NET PASSWORD

Bạn hãy thay đổi password của mình bằng lệnh NET PASSWORD. Cần chú ý người dùng có thể có nhiều password ở vài vị trí, kể cả tập tin danh sách password trong cơ sở dữ liệu khách hàng và cơ sở dữ liệu tên người dùng trên vùng hoặc trạm làm việc.

Được nhập không có các tham số, lệnh này nhắc bạn về các password cũ và mới.

Bạn cũng có thể gộp các password cũ và mới theo tham số. Để thay đổi passwod trong thông tin danh sách khách hàng, cú pháp của lệnh này như sau:

NET PASSWORD oldpassword newpassword

Để thay đổi password trên máy tính, bạn hãy gộp tên máy tính đó theo tham số tên người dùng:

NET PASSWORD \\ WIDGEST1 MABLE oldpassword newpassword

Để chuyên biệt vùng bạn hãy dùng tuỳ chọn / DOMAIN.

NET PASSWORD / DOMAIN: MALAPROP oldpassword newpassword.

MỤC LỤC