

**BỘ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI
TRƯỜNG TRUNG CẤP NGHỀ CỬ CHI**

GIÁO TRÌNH

**MÔN HỌC/MÔ ĐUN: QUẢN TRỊ MẠNG
NGÀNH/NGHỀ: QUẢN TRỊ MẠNG MÁY TÍNH
TRÌNH ĐỘ: TRUNG CẤP**

(Ban hành kèm theo Quyết định số:48/QĐ-TCN, ngày 04 tháng 10 năm 2021 của Hiệu trưởng Trường Trung cấp nghề Cử Chi

Cử Chi, năm 2021

TUYÊN BỐ BẢN QUYỀN:

Tài liệu này thuộc loại sách giáo trình nên các nguồn thông tin có thể được phép dùng nguyên bản hoặc trích dùng cho các mục đích về đào tạo và tham khảo.

Mọi mục đích khác mang tính lệch lạc hoặc sử dụng với mục đích kinh doanh thiếu lành mạnh sẽ bị nghiêm cấm.

LỜI GIỚI THIỆU

Trong những năm qua, dạy nghề đã có những bước tiến vượt bậc cả về số lượng và chất lượng, nhằm thực hiện nhiệm vụ đào tạo nguồn nhân lực kỹ thuật trực tiếp đáp ứng nhu cầu xã hội. Cùng với sự phát triển của khoa học công nghệ trên thế giới, lĩnh vực Công nghệ thông tin nói chung và ngành Quản trị mạng ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình dạy nghề Quản trị mạng máy tính đã được xây dựng trên cơ sở phân tích nghề, phân kỹ năng nghề được kết cấu theo các môđun. Để tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình thực hiện, việc biên soạn giáo trình theo các môđun đào tạo nghề là cấp thiết hiện nay.

Quản trị mạng là môđun đào tạo chuyên môn nghề được biên soạn theo hình thức tích hợp lý thuyết và thực hành. Trong quá trình thực hiện, nhóm biên soạn đã tham khảo nhiều tài liệu Quản trị mạng trong và ngoài nước, kết hợp với kinh nghiệm trong thực tế rất mong nhận được sự đóng góp ý kiến của độc giả để giáo trình được hoàn thiện hơn.

Xin chân thành cảm!

Củ Chi, ngày ... tháng ... năm 2021

Tham gia biên soạn

1. Lê Bá Thi

MỤC LỤC

BÀI 1: TỔNG QUAN VỀ WINDOWS SERVER.....	6
1. MỤC TIÊU:	6
2. NỘI DUNG CHÍNH:	6
2.1. GIỚI THIỆU	6
2.2. CHUẨN BỊ CÀI ĐẶT WINDOWS SERVER.....	7
2.3. CÀI ĐẶT WINDOWS SERVER 2008	10
2.4. TỰ ĐỘNG HÓA QUÁ TRÌNH CÀI ĐẶT	16
BÀI TẬP.....	18
BÀI 2: DỊCH VỤ TÊN MIỀN (DNS).....	19
1. MỤC TIÊU:	19
2. NỘI DUNG CHÍNH:	19
2.1. TỔNG QUAN VỀ DNS	19
2.2. CÁCH PHÂN BỐ DỮ LIỆU QUẢN LÝ TRÊN TÊN MIỀN.....	22
2.3. CƠ CHẾ PHÂN GIẢI TÊN	23
2.4. MỘT SỐ KHÁI NIỆM CƠ BẢN.....	25
2.5. PHÂN LOẠI DOMAIN NAME SERVER.....	27
2.6. RESOURCE RECORD (RR).....	27
2.7. CÀI ĐẶT VÀ CẤU HÌNH DNS	30
BÀI TẬP.....	35
BÀI 3: ACTIVE DIRECTORY	38
1. MỤC TIÊU CỦA BÀI HỌC:.....	38
2. NỘI DUNG CHÍNH:	38
2.1 CÁC MÔ HÌNH MẠNG TRONG MÔI TRƯỜNG MICROSOFT	38
2.2. ACTIVE DIRECTORY	40
2.3. CÀI ĐẶT VÀ CẤU HÌNH ACTIVE DIRECTORY.....	44
BÀI TẬP.....	47
BÀI 4: QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM.....	48
1. MỤC TIÊU:	48
2. NỘI DUNG CHÍNH:	48
2.1. ĐỊNH NGHĨA TÀI KHOẢN NGƯỜI DÙNG VÀ TÀI KHOẢN NHÓM.....	48
2.2. CHỨNG THỰC VÀ KIỂM SOÁT TRUY CẬP	51
2.3 CÁC TÀI KHOẢN TẠO SẴN	52
2.4. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM CỤC BỘ	55
2.5 QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM TRÊN ACTIVE DIRECTORY	57
BÀI TẬP.....	65
BÀI 5: QUẢN LÝ ĐĨA	68
1. MỤC TIÊU:	68
2. NỘI DUNG CHÍNH:	68
2.1 CẤU HÌNH HỆ THỐNG TẬP TIN	68
2.2 CẤU HÌNH ĐĨA LƯU TRỮ.....	69
2.3 SỬ DỤNG CHƯƠNG TRÌNH DISK MANAGER	71
2.4. QUẢN LÝ VIỆC NÉN DỮ LIỆU	79

2.5. THIẾT LẬP HẠN NGÁCH ĐĨA (DISK QUOTA).....	79
2.6. MÃ HOÁ DỮ LIỆU BẰNG EFS	82
BÀI TẬP	82
BÀI 6: TẠO VÀ QUẢN LÝ THƯ MỤC DÙNG CHUNG.....	83
1. MỤC TIÊU:	83
2. NỘI DUNG CHÍNH:	83
2.1 TẠO THƯ MỤC DÙNG CHUNG.....	83
2.2. QUẢN LÝ CÁC THƯ MỤC DÙNG CHUNG.....	86
2.3. QUYỀN TRUY CẬP NTFS.....	87
2.4. DFS	93
BÀI TẬP THỰC HÀNH CỦA HỌC VIÊN.....	97
BÀI 7: DỊCH VỤ DHCP VÀ WINS.....	103
1. MỤC TIÊU:	103
2. NỘI DUNG CHÍNH:	103
2.1 DỊCH VỤ DHCP	103
2.2. DỊCH VỤ WINS.....	107
BÀI TẬP THỰC HÀNH CỦA HỌC VIÊN.....	116
BÀI 8: QUẢN TRỊ MÁY IN.....	125
1. MỤC TIÊU:	125
2. NỘI DUNG CHÍNH:	125
2.1. CÀI ĐẶT MÁY IN.....	125
2.2 QUẢN LÝ THUỘC TÍNH MÁY IN.....	126
2.3. CẤU HÌNH CHIA SẺ MÁY IN.....	127
2.4. CẤU HÌNH TAB ADVANCE	127
TÀI LIỆU THAM KHẢO.....	132

CHƯƠNG TRÌNH MÔ ĐUN

(Kèm theo Thông tư số: 03/2017/TT-BLĐXH ngày 01/03/2017

Của Bộ trưởng Bộ Lao động – Thương binh và Xã hội)

Tên mô đun: QUẢN TRỊ MẠNG

Mã số mô đun: MĐ 23

Thời gian mô đun: 75 giờ (Lý thuyết: 15 giờ; Thực hành: 55 giờ; Kiểm tra: 5 giờ)

I. VỊ TRÍ, TÍNH CHẤT CỦA MÔ ĐUN:

- Vị trí
 - + Mô đun được bố trí sau khi học sinh học xong các môn học chung, trước các môn học, mô đun đào tạo cơ sở nghề
- Tính chất
 - + Là môn học chuyên ngành đào tạo tự chọn.

II. MỤC TIÊU MÔ ĐUN:

- Về kiến thức
 - + Phân biệt sự khác nhau trong việc quản trị máy chủ (Server) và máy trạm (workstation);
 - + Phân biệt sự khác nhau giữa các mô hình mạng DOMAIN và WORKGROUP
 - + Trình bày được kiến trúc của Active Directory
 - + Trình bày được nguyên lý hoạt động của các dịch vụ: DNS, DHCP, NAT...;
- Về kỹ năng
 - + Cài đặt được hệ điều hành server;
 - + Tạo được tài khoản người dùng, tài khoản nhóm;
 - + Quản lý tài khoản người dùng, nhóm và sắp xếp hệ thống hoá các tác vụ quản trị tài khoản người dùng và tài khoản nhóm;
 - + Chia sẻ và cấp quyền truy cập tài nguyên dùng chung;
 - + Cài đặt và cấp hạn ngạch sử dụng đĩa;
 - + Lập cấu hình và quản trị in ấn của một máy phục vụ in mạng;
 - + Cài đặt và cấu hình các dịch vụ mạng: Active Directory, DNS, DHCP, WINS.
- Về năng lực tự chủ và trách nhiệm
 - + Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập;
 - + Rèn luyện ý thức kỷ luật trong học tập, tinh thần hợp tác, giúp đỡ lẫn nhau;
 - + Thực hiện được các thao tác an toàn trong lao động

Bài 1: TỔNG QUAN VỀ WINDOWS SERVER

Giới thiệu:

Bài này sẽ giới thiệu cho bạn các phiên bản của hệ điều hành Windows Server, yêu cầu phần cứng tối thiểu để cài đặt hệ điều hành này và các bước cài đặt Windows Server trên một máy tính.

1. Mục tiêu:

- Phân biệt được về họ hệ điều hành Windows Server;
- Cài đặt được hệ điều hành Windows Server.
- Thực hiện các thao tác an toàn với máy tính.

2. Nội dung chính:

2.1. Giới thiệu

Mục tiêu:

- Phân biệt được về họ hệ điều hành Windows Server

Windows Server 2008 là hệ điều hành được thiết kế nhằm tăng sức mạnh cho các mạng, ứng dụng và dịch vụ Web thế hệ mới. Với Windows Server 2008, bạn có thể phát triển, cung cấp và quản lý các trải nghiệm người dùng và ứng dụng phong phú, đem tới một hạ tầng mạng có tính bảo mật cao, và tăng cường hiệu quả về mặt công nghệ và giá trị trong phạm vi tổ chức của mình.

Windows Server 2008 kế thừa những thành công và thế mạnh của các hệ điều hành Windows Server thế hệ trước, đồng thời đem tới tính năng mới có giá trị và những cải tiến mạnh mẽ cho hệ điều hành cơ sở này. Công cụ Web mới, công nghệ ảo hóa, tính bảo mật tăng cường và các tiện ích quản lý giúp tiết kiệm thời gian, giảm bớt các chi phí, và đem tới một nền tảng vững chắc cho hạ tầng Công nghệ Thông tin (CNTT) của bạn.

Nền tảng chắc chắn dành cho doanh nghiệp Windows Server 2008 đem tới một nền tảng chắc chắn đáp ứng tất cả các yêu cầu về ứng dụng và chế độ làm việc cho máy chủ, đồng thời dễ triển khai và quản lý. Thành phần mới Server Manager cung cấp một console quản lý hợp nhất, đơn giản hóa và sắp xếp một cách hợp lý việc cài đặt, cấu hình và quản lý liên tục cho máy chủ. Windows PowerShell, một shell mới kiểu dòng lệnh, giúp quản trị viên tự động hóa các tác vụ thường trình về quản trị hệ thống trên nhiều máy chủ. Windows Deployment Services đem tới một phương tiện bảo mật cao, đơn giản hóa để nhanh chóng triển khai hệ điều hành này qua các bước cài đặt trên nền mạng. Thêm vào đó, các wizard Failover Clustering của Windows Server 2008, và việc hỗ trợ đầy đủ cho Giao thức Internet phiên bản 6 (gọi tắt là IPv6) cộng với khả năng quản lý hợp nhất Network Load Balancing khiến dễ dàng triển khai với tính sẵn có cao, thậm chí bởi những người có hiểu biết chung nhất về CNTT.

Windows Server 2008 có các phiên bản như sau:

- **Windows Server 2008 Standard (Bản tiêu chuẩn):** Với các khả năng ảo hóa và Web dựng sẵn và tăng cường, phiên bản này được thiết kế để tăng độ tin cậy và linh hoạt của cơ sở hạ tầng máy chủ của bạn đồng thời giúp tiết kiệm thời gian và giảm chi phí. Các công cụ mạnh mẽ giúp bạn kiểm soát máy chủ tốt hơn, và sắp xếp hợp lý các tác vụ cấu hình và quản lý. Thêm vào đó, các tính năng bảo mật được cải tiến làm tăng sức

manh cho hệ điều hành để giúp bạn bảo vệ dữ liệu và mạng, và tạo ra một nền tảng vững chắc và đáng tin cậy cho doanh nghiệp của bạn.

- **Windows Server 2008 Standard without Hyper-V:** Bản tiêu chuẩn nhưng không có Hyper-V.

- **Windows Server 2008 Enterprise** (Bản dùng cho Doanh nghiệp): đem tới một nền tảng cấp doanh nghiệp để triển khai các ứng dụng quan trọng đối với hoạt động kinh doanh. Phiên bản này giúp cải thiện tính sẵn có nhờ các khả năng clustering và cảm nóng bộ xử lý, giúp cải thiện tính bảo mật với các đặc tính được củng cố để quản lý nhận dạng, và giảm bớt chi phí cho cơ sở hạ tầng hệ thống bằng cách hợp nhất ứng dụng với các quyền cấp phép ảo hóa. Windows Server 2008 Enterprise mang lại nền tảng cho một cơ sở hạ tầng CNTT có độ năng động và khả năng mở rộng cao.

- **Windows Server 2008 Enterprise without Hyper-V:** Bản dùng cho doanh nghiệp nhưng không có Hyper-V

- **Windows Server 2008 Datacenter** (Bản dùng cho Trung tâm dữ liệu): đem tới một nền tảng cấp doanh nghiệp để triển khai các ứng dụng quan trọng đối với hoạt động kinh doanh và ảo hóa ở quy mô lớn trên các máy chủ lớn và nhỏ. Phiên bản này cải thiện tính sẵn có nhờ các khả năng clustering và phân vùng phần cứng động, giảm bớt chi phí cho cơ sở hạ tầng hệ thống bằng cách hợp nhất các ứng dụng với các quyền cấp phép ảo hóa không hạn chế, và mở rộng từ 2 tới 64 bộ xử lý. Windows Server 2008 Datacenter mang lại một nền tảng để từ đó xây dựng các giải pháp mở rộng và ảo hóa cấp doanh nghiệp.

- **Windows Server 2008 Datacenter without Hyper-v:** Bản dùng cho Trung tâm dữ liệu, không có Hyper-V.

- **Windows Web Server 2008** (Bản dùng cho Web): Được thiết kế để chuyên dùng như một Web server đơn mục đích, Windows Web Server 2008 đem tới một nền tảng vững chắc gồm các tính năng liên quan tới hạ tầng Web trong Windows Server 2008 thế hệ kế tiếp. Tích hợp với IIS 7.0 mới được cấu trúc lại, ASP.NET, và Microsoft .NET Framework, Windows Web Server 2008 cho phép mọi tổ chức triển khai nhanh chóng các Web page, Web site, ứng dụng và dịch vụ Web.

- **Windows Server 2008:** dành cho các hệ thống dựa trên bộ xử lý Itanium được tối ưu hóa cho các trung tâm dữ liệu lớn, các ứng dụng nghiệp vụ riêng, ứng dụng tùy biến mang lại độ sẵn sàng và khả năng mở rộng cao cho tới 64 bộ xử lý để đáp ứng nhu cầu cho các giải pháp khẩn khe và quan trọng.

2.2. Chuẩn bị cài đặt windows server

Mục tiêu:

- Nêu được cấu hình phần cứng tối thiểu để cài đặt windows server 2008.

2.2.1. Yêu cầu phần cứng

- Đối với windows Server 2008 yêu cầu về phần cứng như sau:

Thành phần	Yêu cầu
Bộ xử lý	Tối thiểu: 1 GHz (bộ xử lý x86) hoặc 1.4 GHz (bộ xử lý x64) Khuyến nghị: Tốc độ xử lý 2 GHz hoặc nhanh hơn

Thành phần	Yêu cầu
	Chú ý: Cần bộ xử lý Intel Itanium 2 cho Windows Server đối với các Hệ thống dựa trên kiến trúc Itanium.
Bộ nhớ	Tối thiểu: RAM 512 MB Khuyến nghị: RAM 2 GB hoặc lớn hơn Tối ưu: RAM 2 GB (Cài đặt toàn bộ) or RAM 1 GB (Cài Server Core) hoặc hơn Tối đa (hệ thống 32 bit): 4 GB (Bản Standard) hoặc 64 GB (Bản Enterprise và Datacenter) Tối đa (các hệ thống 64 bit): 32 GB (Bản Standard) hoặc 2 TB (Bản Enterprise, Datacenter, và Các hệ thống dựa trên kiến trúc Itanium)
Không gian ổ đĩa còn trống	Tối thiểu: 10 GB Khuyến nghị : 40 GB hoặc lớn hơn Chú ý: Các máy tính có RAM lớn hơn 16 GB sẽ cần nhiều không gian ổ đĩa trống hơn dành cho paging, hibernation, and dump files
Ổ đĩa	Ổ DVD-ROM
Màn hình	Super VGA (800 × 600) hoặc màn hình có độ phân giải cao hơn
Thành phần khác	Bàn phím, Chuột của Microsoft hoặc thiết bị trở tương thích

2.2.2. Tương thích phần cứng

Một bước quan trọng trước khi nâng cấp hoặc cài đặt mới Server của bạn là kiểm tra xem phần cứng của máy tính hiện tại có tương thích với sản phẩm hệ điều hành trong họ **Windows Server 2008**.

2.2.3. Cài đặt mới hoặc nâng cấp

Trong một số trường hợp hệ thống **Server** chúng ta đang hoạt động tốt, các ứng dụng và dữ liệu quan trọng đều lưu trữ trên **Server** này, nhưng theo yêu cầu chúng ta phải nâng cấp hệ điều hành **Server** hiện tại thành **Windows Server 2008**. Chúng ta cần xem xét nên nâng cấp hệ điều hành đồng thời giữ lại các ứng dụng và dữ liệu hay cài đặt mới hệ điều hành rồi sau cấu hình và cài đặt ứng dụng lại. Đây là vấn đề cần xem xét và lựa chọn cho hợp lý. Các điểm cần xem xét khi nâng cấp:

- Với nâng cấp (**upgrade**) thì việc cấu hình **Server** đơn giản, các thông tin của bạn được giữ lại như: người dùng (**users**), cấu hình (**settings**), nhóm (**groups**), quyền hệ thống (**rights**), và quyền truy cập (**permissions**)...
- Với nâng cấp bạn không cần cài lại các ứng dụng, nhưng nếu có sự thay đổi lớn về đĩa cứng thì bạn cần backup dữ liệu trước khi nâng cấp.
- Trước khi nâng cấp bạn cần xem hệ điều hành hiện tại có nằm trong danh sách các hệ điều hành hỗ trợ nâng cấp thành **Windows Server 2008** không ?

- Trong một số trường hợp đặc biệt như bạn cần nâng cấp một máy tính đang làm chức năng **Domain Controller** hoặc nâng cấp một máy tính đang có các phần mềm quan trọng thì bạn nên tham khảo thêm thông tin hướng dẫn của **Microsoft**.

Các hệ điều hành cho phép nâng cấp thành **Windows Server 2008**:

- Windows Server 2000.
- Windows Server 2003.

2.2.4. Phân chia ổ đĩa

Đây là việc phân chia ổ đĩa vật lý thành các **partition logic**. Khi chia **partition**, bạn phải quan tâm các yếu tố sau:

- **Lượng không gian cần cấp phát**: bạn phải biết được không gian chiếm dụng bởi hệ điều hành, các chương trình ứng dụng, các dữ liệu đã có và sắp phát sinh.

- Cấu hình đĩa đặc biệt: **Windows Server** hỗ trợ nhiều cấu hình đĩa khác nhau. Các lựa chọn có thể là **volume simple, spanned, striped, mirrored** hoặc là **RAID-5**.

- **Tiện ích phân chia partition**: nếu bạn định chia **partition** trước khi cài đặt, bạn có thể sử dụng nhiều chương trình tiện ích khác nhau, chẳng hạn như **FDISK** hoặc **PowerQuest Partition Magic**. Có thể ban đầu bạn chỉ cần tạo một **partition** để cài đặt **Windows Server**, sau đó sử dụng công cụ **Disk Management** để tạo thêm các **partition** khác.

2.2.5. Chọn hệ thống tập tin

Bạn nên chọn hệ thống tập tin **NTFS**, vì nó có các đặc điểm sau: chỉ định khả năng an toàn cho từng tập tin, thư mục; nén dữ liệu, tăng không gian lưu trữ; có thể chỉ định hạn ngạch sử dụng đĩa cho từng người dùng; có thể mã hoá các tập tin, nâng cao khả năng bảo mật.

2.2.6. Chọn chế độ sử dụng giấy phép

Bạn chọn một trong hai chế độ giấy phép sau đây:

- **Per server licensing**: là lựa chọn tốt nhất trong trường hợp mạng chỉ có một Server và phục cho một số lượng Client nhất định. Khi chọn chế độ giấy phép này, chúng ta phải xác định số lượng giấy phép tại thời điểm cài đặt hệ điều hành. Số lượng giấy phép tùy thuộc vào số kết nối đồng thời của các Client đến Server. Tuy nhiên, trong quá trình sử dụng chúng ta có thể thay đổi số lượng kết nối đồng thời cho phù hợp với tình hình hiện tại của mạng.

- **Per Seat licensing**: là lựa chọn tốt nhất trong trường hợp mạng có nhiều Server. Trong chế độ giấy phép này thì mỗi Client chỉ cần một giấy phép duy nhất để truy xuất đến tất cả các Server và không giới hạn số lượng kết nối đồng thời đến Server.

2.2.7. Chọn phương án kết nối mạng

2.2.7.1. Các giao thức kết nối mạng

Windows Server mặc định chỉ cài một giao thức **TCP/IP**, còn những giao thức còn lại như **IPX, AppleTalk** là những tùy chọn có thể cài đặt sau nếu cần thiết. Riêng giao thức **NetBEUI, Windows Server** không đưa vào trong các tùy chọn cài đặt mà chỉ cung cấp kèm theo đĩa **DVD-ROM** cài đặt.

2.2.7.2. Thành viên trong Workgroup hoặc Domain.

Nếu máy tính của bạn nằm trong một mạng nhỏ, phân tán hoặc các máy tính không được nối mạng với nhau, bạn có thể chọn cho máy tính làm thành viên của **workgroup**, đơn giản bạn chỉ cần cho biết tên **workgroup** là xong. Nếu hệ thống mạng của bạn làm việc theo cơ chế quản lý tập trung, trên mạng đã có một vài máy **Windows Server 2003** hoặc **Windows Server 2008** sử dụng **Active Directory** thì bạn có thể chọn cho máy tính tham gia **domain** này. Trong trường hợp này, bạn phải cho biết tên chính xác của **domain** cùng với tài khoản (gồm có **username** và **password**) của một người dùng có quyền bổ sung thêm máy tính vào **domain**. Ví dụ như tài khoản của người quản trị mạng (**Administrator**).

Các thiết lập về ngôn ngữ và các giá trị cục bộ. **Windows Server** hỗ trợ rất nhiều ngôn ngữ, bạn có thể chọn ngôn ngữ của mình nếu được hỗ trợ. Các giá trị **local** gồm có hệ thống số, đơn vị tiền tệ, cách hiển thị thời gian, ngày tháng.

2.3. Cài đặt windows server 2008

Mục tiêu:

- Cài đặt được windows server 2008.

2.3.1. Giai đoạn Preinstallation

Sau khi kiểm tra và chắc chắn rằng máy của mình đã hội đủ các điều kiện để cài đặt **Windows Server 2008**, bạn phải chọn một trong các cách sau đây để bắt đầu quá trình cài đặt.

2.3.1.1. Cài đặt từ hệ điều hành khác.

Nếu máy tính của bạn đã có một hệ điều hành và bạn muốn nâng cấp lên **Windows 2008 Server** hoặc là bạn muốn khởi động kép, đầu tiên bạn cho máy tính khởi động bằng hệ điều hành có sẵn này, sau đó tiến hành quá trình cài đặt **Windows Server 2008** bằng cách thi hành tập tin Setup.exe rồi chọn mục Upgrade.

2.3.1.2. Cài đặt trực tiếp từ đĩa DVD Windows Server 2008

Nếu máy tính của bạn hỗ trợ tính năng khởi động từ đĩa DVD, bạn chỉ cần đặt đĩa DVD vào ổ đĩa và khởi động lại máy tính. Lưu ý là bạn phải cấu hình **CMOS Setup**, chỉ định thiết bị khởi động đầu tiên là ổ đĩa **DVDROM**. Khi máy tính khởi động lên thì quá trình cài đặt tự động thi hành, sau đó làm theo những hướng dẫn trên màn hình để cài đặt **Windows 2008**.

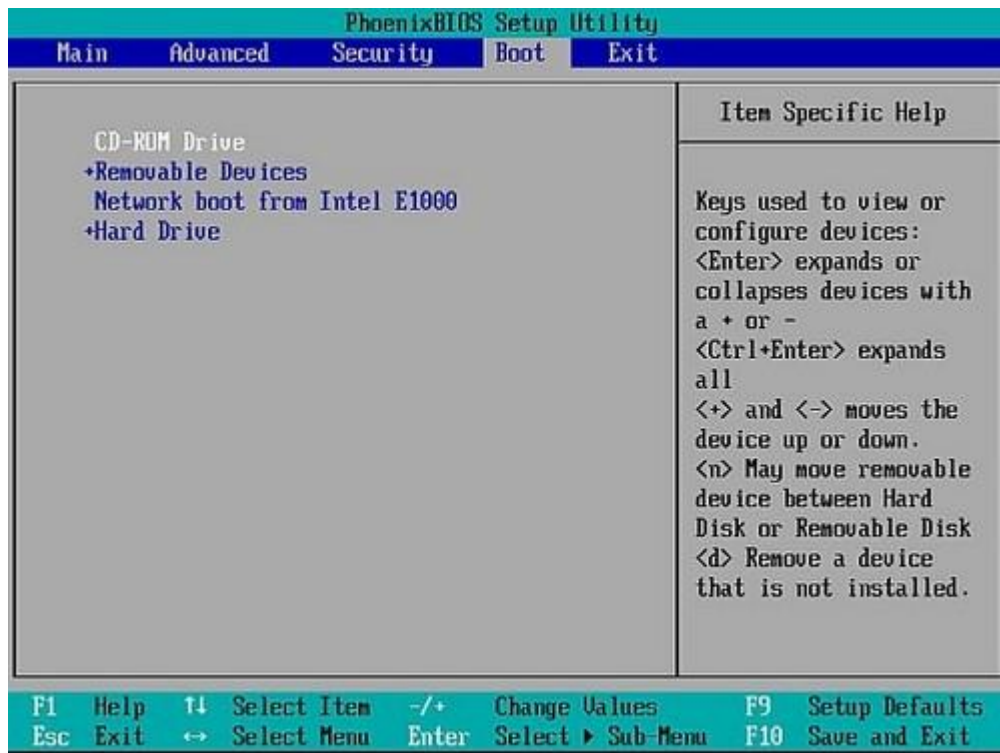
2.3.2. Giai đoạn Text-Based Setup

Trong quá trình cài đặt nên chú ý đến các thông tin hướng dẫn ở thanh trạng thái. Giai đoạn Text-based setup diễn ra một số bước như sau:

Bước 1: Cấu hình BIOS của máy tính để có thể khởi động từ ổ đĩa DVD-ROM

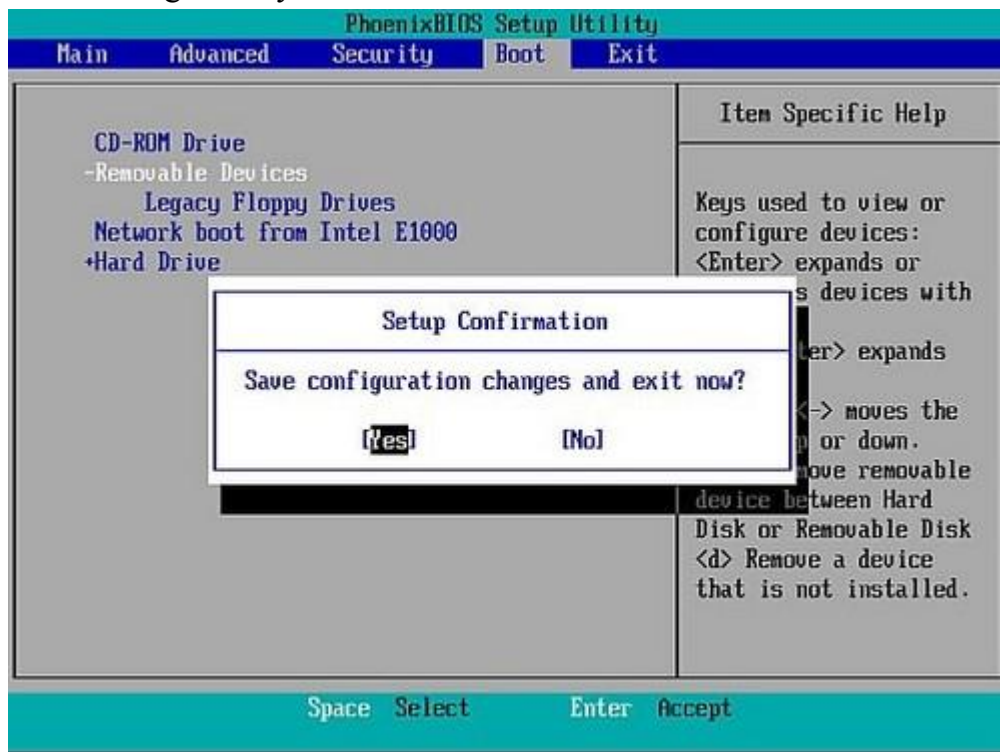
- Để thiết lập cho máy tính khởi động từ CD / DVD bạn khởi động máy tính và nhấn phím Del hoặc F2 tùy theo Mainboard máy tính của bạn (máy tính của tôi sử dụng phím F2).

Sau khi vào **BIOS** bạn di chuyển đến thẻ boot và chọn boot từ CD/DVD như hình 1.1



Hình 1.1: Thiết lập máy tính khởi động từ ổ đĩa CD/DVD.

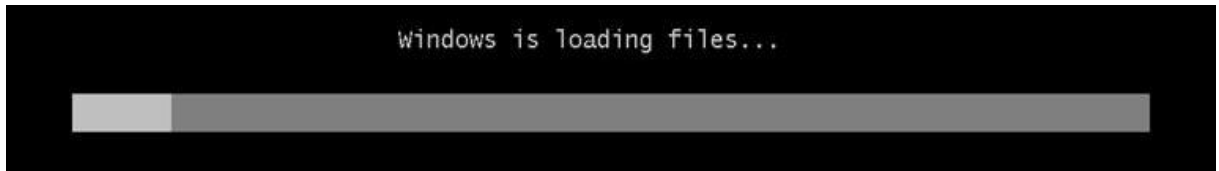
Bước 2: Sau khi hoàn tất bạn nhấn F10 để lưu cấu hình và thoát khỏi màn hình BIOS sau đó bạn khởi động lại máy tính.



Hình 1.2: Lưu cấu hình BIOS.

Bước 3: Bạn chèn đĩa cài đặt Windows 2008 Server vào ổ đĩa DVD-ROM.

Khi máy khởi động từ đĩa DVD-ROM sẽ xuất hiện một thông báo “Press any key to continue...” yêu cầu nhấn một phím bất kỳ để bắt đầu quá trình cài đặt. Cửa sổ sẽ xuất hiện như sau:



Hình 1.3. Load file.

Bước 4: Sau khi load xong, một màn hình **Start Windows** sẽ hiện ra.



Hình 1.4. Start Windows.

Bước 5: Tiếp đến màn hình cài đặt đầu tiên sẽ xuất hiện, ở đây bạn sẽ 3 phần để lựa chọn:

- + **Language to Install:** Ngôn ngữ cài đặt.
 - + **Time and currency format:** Định dạng ngày tháng và tiền tệ.
 - + **Keyboard or input method:** Kiểu bàn phím bạn sử dụng.
- Sau khi bạn lựa chọn hoàn tất, click Next.



Hình 1.5: Lựa chọn ngôn ngữ, định dạng ngày tháng và kiểu bàn phím

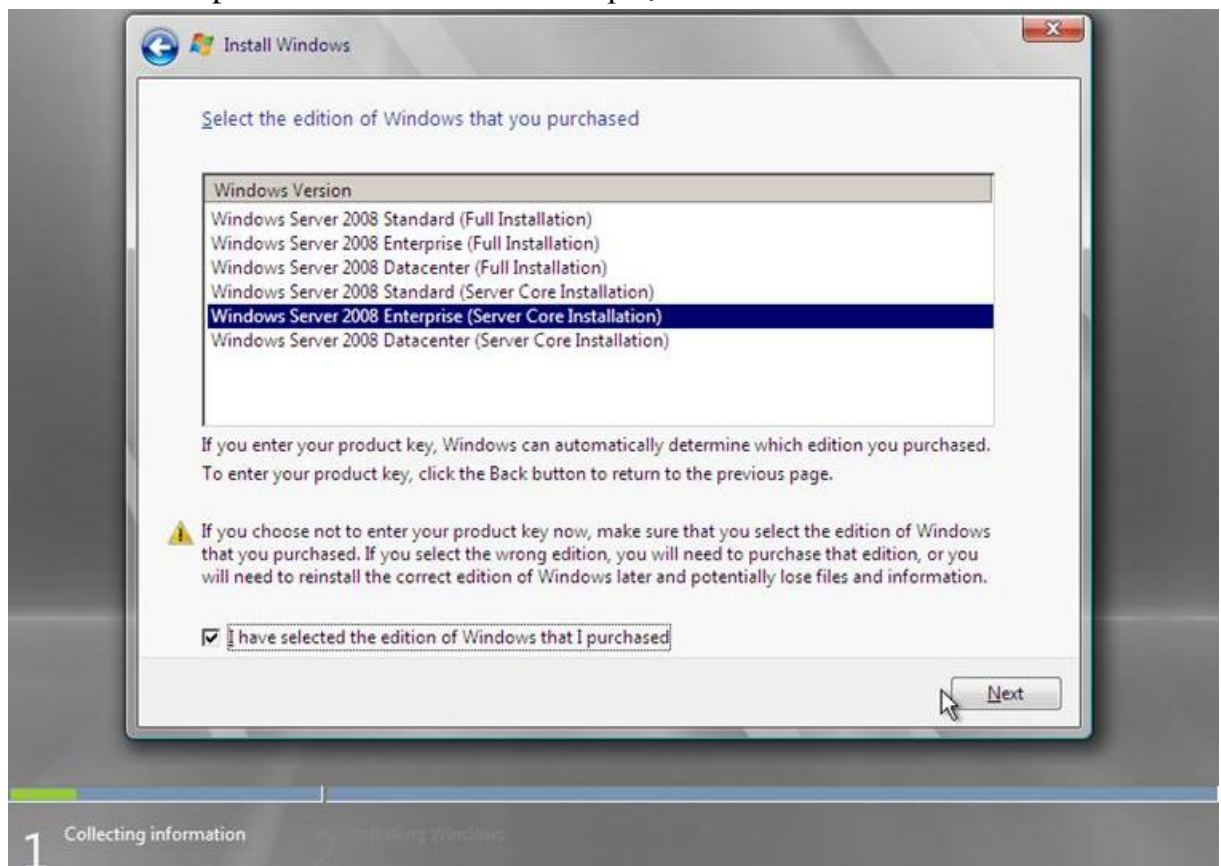
Bước 6: Xuất hiện cửa sổ tiếp theo, click nút **Install Now**



Hình 1.6: Install now

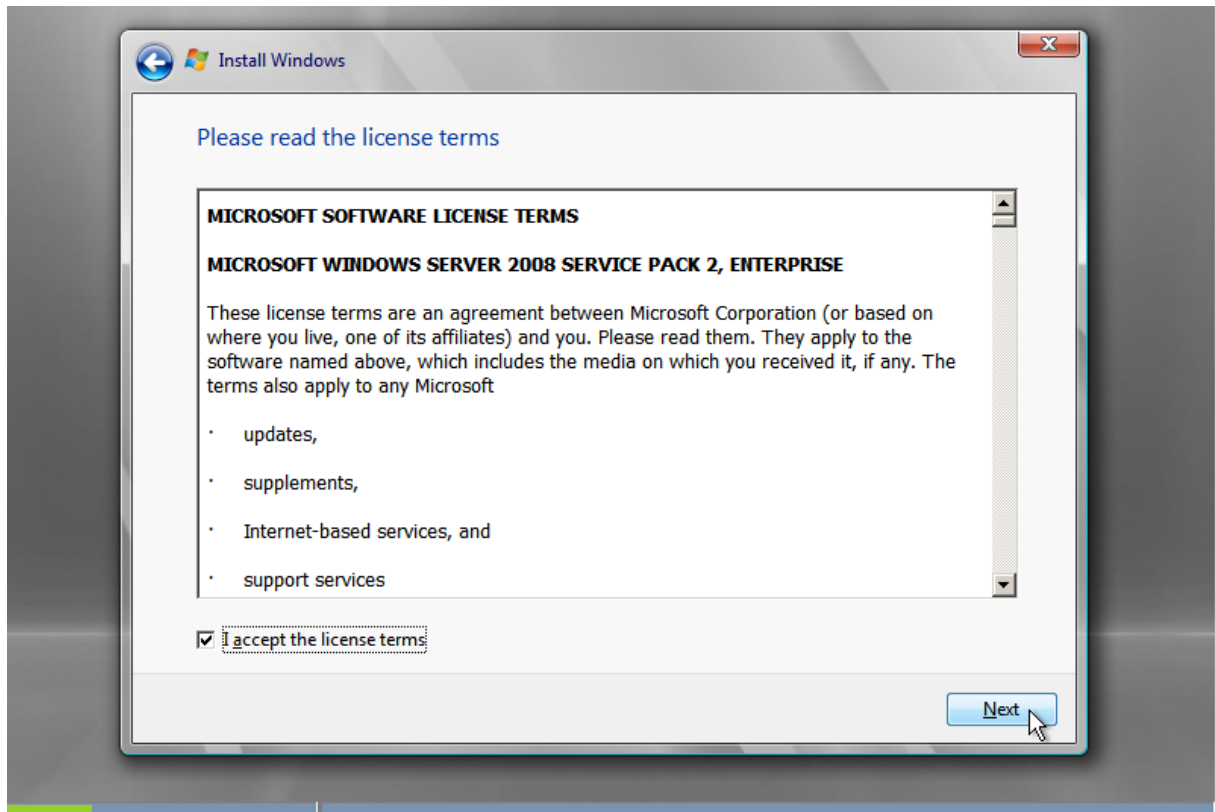
Bước 7: Tại khung **Type your product key for activation** bạn nhập key vào và click nút next để tiếp tục.

Bước 8: Tại khung các phiên bản **Windows Server 2008**, bạn chọn **Windows Server 2008 Enterprise (Full Installation)** và **đánh dấu chọn** chọn I have selected the edition of Windows that I purchased. Click **Next** để tiếp tục.



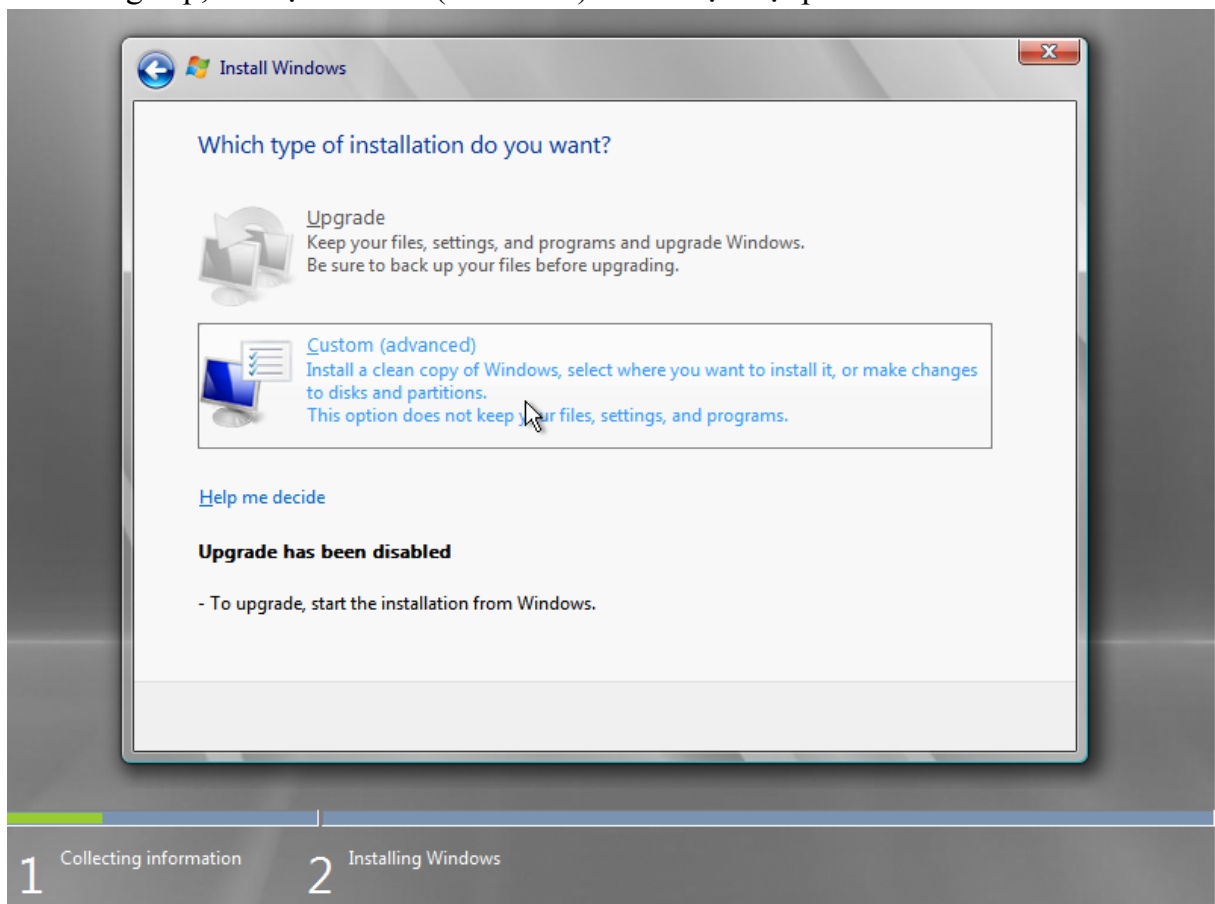
Hình 1.7: Lựa chọn phiên bản cài đặt

Bước 9: Tại bảng các điều khoản bạn click vào **I accept the license terms**, sau đó click **Next**.



Hình 1.8: Các điều khoản của Microsoft

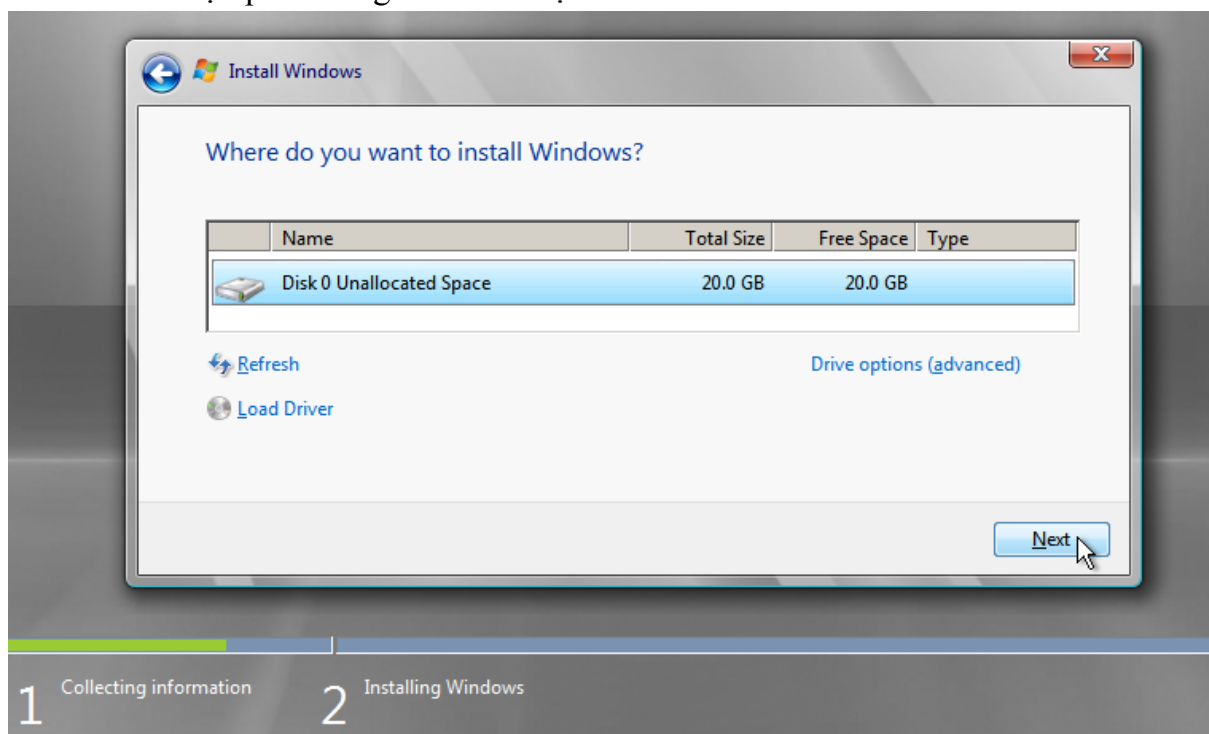
Bước 9: Tại bảng lựa chọn các kiểu cài đặt thích hợp bạn có thể chọn Upgrade nếu muốn nâng cấp, và chọn Custom(advanced) để cài đặt một phiên bản mới.



Hình 1.9: Chọn kiểu cài đặt

Bước 10: Sau đó chọn Drive Option nếu muốn thao tác lên ổ đĩa cứng như New, Delete, Format...v.v...

- Sau đó chọn phân vùng muốn cài đặt và click nút Next



Hình 1.10: Lựa chọn các thao tác trên đĩa cứng

2.3.3. Giai đoạn Graphical-Based Setup

Giai đoạn này Windows bắt đầu sao chép các tập tin từ DVD vào trong đĩa cứng, quá trình trình diễn ra khoản vài phút. .

- (1) Bắt đầu giai đoạn **Graphical**, trình cài đặt sẽ cài **driver** cho các thiết bị mà nó tìm thấy trong hệ thống.
- (2) Tại hộp thoại **Regional and Language Options**, cho phép chọn các tùy chọn liên quan đến ngôn ngữ, số đếm, đơn vị tiền tệ, định dạng ngày tháng năm,....Sau khi đã thay đổi các tùy chọn phù hợp, nhấn **Next** để tiếp tục.
- (3) Tại hộp thoại **Personalize Your Software**, điền tên người sử dụng và tên tổ chức. Nhấn **Next**.
- (4) Tại hộp thoại **Your Product Key**, điền vào 25 số **DVD-Key** vào 5 ô trống bên dưới. Nhấn **Next**
- (5) Tại hộp thoại **Licensing Mode**, chọn chế độ bản quyền là **Per Server** hoặc **Per Seat** tùy thuộc vào tình hình thực tế của mỗi hệ thống mạng
- (6) Tại hộp thoại **Computer Name and Administrator Password**, điền vào tên của **Server** và **Password** của người quản trị (**Administrator**).
- (7) Tại hộp thoại **Date and Time Settings**, thay đổi ngày, tháng, và múi giờ (**Time zone**) cho thích hợp
- (8) Tại hộp thoại **Networking Settings**, chọn **Custom settings** để thay đổi các thông số giao thức **TCP/IP**. Các thông số này có thể thay đổi lại sau khi quá trình cài đặt hoàn tất.
- (9) Tại hộp thoại **Workgroup or Computer Domain**, tùy chọn gia nhập

Server vào một **Workgroup** hay một **Domain** có sẵn. Nếu muốn gia nhập vào **Domain** thì đánh vào tên **Domain** vào ô bên dưới.

- (10) Sau khi chép đầy đủ các tập tin, quá trình cài đặt kết thúc.

2.4. Tự động hóa quá trình cài đặt

Mục tiêu:

- Thực hiện cài đặt windows server thông qua file tra lời tự động.

Nếu bạn dự định cài đặt hệ điều hành **Windows 2003 Server** trên nhiều máy tính, bạn có thể đến từng máy và tự tay thực hiện quá trình cài đặt như đã hướng dẫn trong chương trước. Tuy nhiên, chắc chắn công việc này sẽ vô cùng nhàm chán và không hiệu quả. Lúc này việc tự động hoá quá trình cài đặt sẽ giúp công việc của bạn trở nên đơn giản, hiệu quả và ít tốn kém hơn.

Có nhiều phương pháp hỗ trợ việc cài đặt tự động. Chẳng hạn, bạn có thể sử dụng phương pháp dùng ảnh đĩa (**disk image**) hoặc phương pháp cài đặt không cần theo dõi (**unattended installation**) thông qua một kịch bản (**script**) hay tập tin trả lời.

2.4.1. Giới thiệu kịch bản cài đặt

Kịch bản cài đặt là một tập tin văn bản có nội dung trả lời trước tất cả các câu hỏi mà trình cài đặt hỏi như: tên máy, **DVD-Key**,... Để trình cài đặt có thể đọc hiểu các nội dung trong kịch bản thì nó phải được tạo ra theo một cấu trúc được quy định trước. Để tạo ra được các kịch bản cài đặt, có thể dùng bất kỳ chương trình soạn thảo văn bản nào, chẳng hạn như **Notepad**. Tuy nhiên, kịch bản là một tập tin có cấu trúc nên trong quá trình soạn thảo có thể xảy ra các sai sót dẫn đến quá trình tự động hóa cài đặt không diễn ra theo ý muốn. Do đó, **Microsoft** đã tạo ra một tiện ích có tên là **Setup Manager (setupmgr.exe)** để giúp cho việc tạo ra kịch bản cài đặt được dễ dàng hơn. Sau khi có được kịch bản, có thể sử dụng **Notepad** để thêm, sửa lại một số thông tin để sử dụng kịch bản vào quá trình cài đặt tự động hiệu quả hơn.

2.4.2. Tự động hóa dùng tham biến dòng lệnh

Khi tiến hành cài đặt **Windows 2003 Server**, ngoài cách khởi động và cài trực tiếp từ đĩa **DVD-ROM**, còn có thể dùng một trong hai lệnh sau: **winnt.exe** dùng với các máy đang chạy hệ điều hành DOS, **windows 3.x** hoặc **Windows for workgroup**; **winnt32.exe** khi máy đang chạy hệ điều hành **Windows 9x**, **Windows NT** hoặc mới hơn. Hai lệnh trên được đặt trong thư mục **I386** của đĩa cài đặt. Sau đây là cú pháp cài đặt từ 2 lệnh trên:

```
winnt [/s:[sourcepath]] [/t:[tempdrive]] [/u:[answer_file]]  
[/udf:id [,UDB_file]]
```

Ý nghĩa các tham số:

- **/s**: Chỉ rõ vị trí đặt của bộ nguồn cài đặt (thư mục I386). Đường dẫn phải là dạng đầy đủ, ví dụ: e:\i386 hoặc \\server\i386. Giá trị mặc định là thư mục hiện hành.
- **/t**: Hướng chương trình cài đặt đặt thư mục tạm vào một ổ đĩa và cài **Windows** vào ổ đĩa đó. Nếu không chỉ định, trình cài đặt sẽ tự xác định.
- **/u**: Cài đặt không cần theo dõi với một tập tin trả lời tự động (kịch bản). Nếu sử dụng **/u** thì phải sử dụng **/s**.

- **/udf**: Chỉ định tên của **Server** và tập tin cơ sở dữ liệu chứa tên, các thông tin đặc trưng cho mỗi máy

- (unattend.udf).

```
winnt32 [/checkupgradeonly] [/s:sourcepath] [/tempdrive:drive_letter:]  
        [/unattend[num]:[answer_file]] [/udf:id [,UDB_file]]
```

Ý nghĩa của các tham số:

- **/checkupgradeonly**: Kiểm tra xem máy có tương thích để nâng cấp và cài đặt **Windows 2003 Server** hay không?

- **/tempdrive**: Tương tự như tham số /t

- **/unattend**: Tương tự như tham số /u

2.4.3. Sử dụng Setup Manager để tạo ra tập tin trả lời

Setup Manager là một tiện ích giúp cho việc tạo các tập tin trả lời sử dụng trong cài đặt không cần theo dõi. Theo mặc định, **Setup Manager** không được cài đặt, mà được đặt trong tập tin **Deploy.Cab**. Chỉ có thể chạy tiện ích **Setup Manager** trên các hệ điều hành **Windows 2000, Windows XP, Windows 2003**.

Tạo tập tin trả lời tự động bằng **Setup Manager**:

- (1). Giải nén tập tin **Deploy.cab** được lưu trong thư mục **Support\Tools** trên đĩa cài đặt **Windows 2003**.

- (2). Thi hành tập tin **Setupmgr.exe**

- (3). Hộp thoại **Setup Manager** xuất hiện, nhấn **Next** để tiếp tục.

- (4). Xuất hiện hộp thoại **New or Existing Answer File**. Hộp thoại này cho phép bạn chỉ định tạo ra một tập tin trả lời mới, một tập tin trả lời phản ánh cấu hình của máy tính hiện hành hoặc là chỉnh sửa một tập tin sẵn có. Bạn chọn **Create new** và nhấn **Next**.

- (5) Tiếp theo là hộp thoại **Type of Setup**. Chọn **Unattended Setup** và chọn **Next**.

- (6) Trong hộp thoại **Product**, chọn hệ điều hành cài đặt sử dụng tập tin trả lời tự động. Chọn **Windows Server 2003, Enterprise Edition**, nhấn **Next**.

- (7) Tại hộp thoại **User Interaction**, chọn mức độ tương tác với trình cài đặt của người sử dụng. Chọn **Fully Automated**, nhấn **Next**.

- (8) Xuất hiện hộp thoại **Distribution Share**, chọn **Setup from a DVD**, nhấn **Next**.

- (9) Tại hộp thoại **License Agreement**, đánh dấu vào **I accept the terms of ...**, nhấn **Next**.

- (10) Tại cửa sổ **Setup Manager**, chọn mục **Name and Organization**. Điền tên và tổ chức sử dụng hệ điều hành. Nhấn **Next**.

- (11) Chọn mục **Time Zone** \ chọn múi giờ (**GMT+7:00**) **Bangkok, Hanoi, Jarkata**. Nhấn **Next**.

- (12) Tại mục **Product Key**, điền **DVD-Key** vào trong 5 ô trống. Nhấn **Next**.

- (13) Tại mục **Licensing Mode**, chọn loại bản quyền thích hợp. Nhấn **Next**.

- (14) Tại mục **Computer Names**, điền tên của các máy dự định cài đặt. Nhấn **Next**.

- (15) Tại mục **Administrator Password**, nhập vào **password** của người quản trị. Nếu muốn mã hóa **password** thì đánh dấu chọn vào mục “**Encrypt the Administrator password...**”. Nhấn **Next**

- (16) Tại mục **Network Component**, cấu hình các thông số cho giao thức **TCP/IP** và cài thêm các giao thức. Nhấn **Next**.

- (17) Tại mục **Workgroup or Domain**, gia nhập máy vào **Workgroup** hoặc **Domain** có sẵn. Nhấn **Next**.

- (18) Cuối cùng, trong thư mục đã chỉ định, **Setup Manager** sẽ tạo ra ba tập tin. Nếu bạn không thay đổi tên thì các tập tin là:

+ **Unattend.txt**: đây là tập tin trả lời, chứa tất cả các câu trả lời mà **Setup Manager** thu thập được

+ **Unattend.udb**: đây là tập tin cơ sở dữ liệu chứa tên các máy tính sẽ được cài đặt. Tập tin này chỉ được tạo ra khi bạn chỉ định danh sách các tập tin và được sử dụng khi bạn thực hiện cài đặt không cần theo dõi.

+ **Unattend.bat**: chứa dòng lệnh với các tham số được thiết lập sẵn. Tập tin này cũng thiết lập các biến môi trường chỉ định vị trí các tập tin liên quan.

2.4.4. Sử dụng tập tin trả lời

Có nhiều cách để sử dụng các tập tin được tạo ra trong bước trên. Bạn có thể thực hiện theo một trong hai cách dưới đây:

2.4.4.1. Sử dụng đĩa DVD Windows 2003 Server có thể khởi động được

Sửa tập tin **Unattend.txt** thành **WINNT.SIF** và lưu lên đĩa mềm.

Đưa đĩa DVD **Windows 2000 Server** và đĩa mềm trên vào ổ đĩa, khởi động lại máy tính, đảm bảo ổ đĩa DVD là thiết bị khởi động đầu tiên. Chương trình cài đặt trên đĩa DVD sẽ tự động tìm đọc tập tin **WINNT.SIF** trên đĩa mềm và tiến hành cài đặt không cần theo dõi.

2.4.4.2. Sử dụng một bộ nguồn cài đặt Windows 2003 Server

Chép các tập tin đã tạo trong bước trên vào thư mục **I386** của nguồn cài đặt **Windows 2003 Server**. Chuyển vào thư mục **I386**.

Tuỳ theo hệ điều hành đang sử dụng mà sử dụng lệnh **WINNT.EXE** hoặc **WINNT32.EXE** theo cú pháp sau:

```
WINNT /s:e:\i386 /u:unattend.txt
```

Hoặc

```
WINNT32 /s:e:\i386 /unattend:unattend.txt
```

Nếu chương trình **Setup Manager** tạo ra tập tin **Unatend.UDB** do bạn đã nhập vào danh sách tên các máy tính, và giả định bạn định đặt tên máy tính này là **server01** thì cú pháp lệnh sẽ như sau:

```
WINNT /s:e:\i386 /u:unattend.txt /udf:server01,unattend.udf
```

Bài tập

1. Cài đặt hệ điều hành Windows Server.
2. Cài đặt hệ điều hành Windows Server sử dụng tập tin trả lời tự động.

HƯỚNG DẪN THỰC HIỆN

Tham khảo mục 3 và 4 trong bài học trên.

Bài 2: DỊCH VỤ TÊN MIỀN (DNS)

Giới thiệu:

Trong bài này giúp học sinh biết Tên miền là tên của một website hoạt động trên internet, đóng vai trò là một địa chỉ vật lý. Nó giống như là địa chỉ nhà hay zip code để giúp các thiết bị định tuyến về tinh dẫn đường, một trình duyệt cũng cần một tên miền để dẫn đường tới website của bạn.

Ví dụ như **Hostinger.com**, **Google.com**, **Facebook.com** là tên miền của các công ty Internet. Khi một công ty (hoặc một người) mua một tên miền, họ có thể chỉ định server nào mà tên miền trở tới.

1. Mục tiêu:

- Trình bày được cấu trúc cơ sở dữ liệu của hệ thống tên miền;
- Mô tả được sự hoạt động và phân cấp của hệ thống tên miền;
- Cài đặt và cấu hình hệ thống tên miền DNS.
- Thực hiện các thao tác an toàn với máy tính.

2. Nội dung chính:

2.1. Tổng quan về DNS

Mục tiêu:

- Trình bày được cấu trúc cơ sở dữ liệu của hệ thống tên miền;
- Mô tả được sự phân cấp của hệ thống tên miền;

2.1.1. Giới thiệu DNS

Mỗi máy tính trong mạng muốn liên lạc hay trao đổi thông tin, dữ liệu cho nhau cần phải biết rõ địa chỉ IP của nhau. Nếu số lượng máy tính nhiều thì việc nhớ những địa chỉ IP này rất là khó khăn. Vì vậy, **DNS (Domain Name System)** là giải pháp dùng tên thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng. Vì thế, người ta nghĩ ra cách làm sao ánh xạ địa chỉ IP thành tên máy tính.

Ban đầu do quy mô mạng ARPAnet (tiền thân của mạng Internet) còn nhỏ chỉ vài trăm máy, nên chỉ có một tập tin đơn HOSTS.TXT lưu thông tin về ánh xạ tên máy thành địa chỉ IP. Trong đó tên máy chỉ là 1 chuỗi văn bản không phân cấp (flat name). Tập tin này được duy trì tại 1 máy chủ và các máy chủ khác lưu giữ bản sao của nó. Tuy nhiên khi quy mô mạng lớn hơn, việc sử dụng tập tin HOSTS.TXT có các nhược điểm như sau:

- Lưu lượng mạng và máy chủ duy trì tập tin HOSTS.TXT bị quá tải do hiệu ứng “cổ chai”.
- Xung đột tên: Không thể có 2 máy tính có cùng tên trong tập tin HOSTS.TXT. Tuy nhiên do tên máy không phân cấp và không có gì đảm bảo để ngăn chặn việc tạo 2 tên trùng nhau vì không có cơ chế uỷ quyền quản lý tập tin nên có nguy cơ bị xung đột tên.
- Không đảm bảo sự toàn vẹn: việc duy trì 1 tập tin trên mạng lớn rất khó khăn. Ví dụ như khi tập tin HOSTS.TXT vừa cập nhật chưa kịp chuyển đến máy chủ ở xa thì đã có sự thay đổi địa chỉ trên mạng rồi.

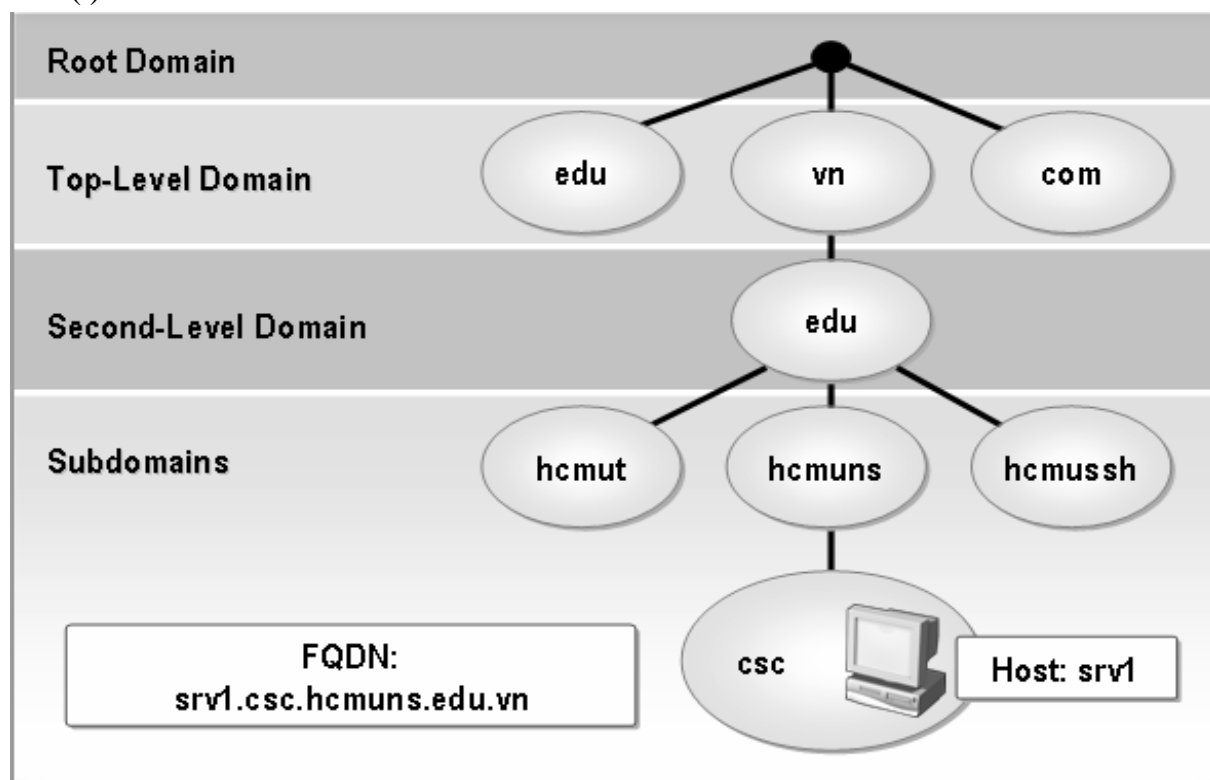
Tóm lại việc dùng tập tin HOSTS.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng. Do đó, dịch vụ DNS ra đời nhằm khắc phục các nhược

điểm này. Người thiết kế cấu trúc của dịch vụ DNS là Paul Mockapetris - USC's Information Sciences Institute, và các khuyến nghị RFC của DNS là RFC 882 và 883, sau đó là RFC 1034 và 1035 cùng với 1 số RFC bổ sung như bảo mật trên hệ thống DNS, cập nhật động các bản ghi DNS ...

Lưu ý: Hiện tại trên các máy chủ vẫn sử dụng được tập tin hosts.txt để phân giải tên máy tính thành địa chỉ IP (trong Windows tập tin này nằm trong thư mục WINDOWS\system32\drivers\etc)

Dịch vụ DNS hoạt động theo mô hình Client-Server: phần Server gọi là máy chủ phục vụ tên hay còn gọi là Name Server, còn phần Client là trình phân giải tên - Resolver. Name Server chứa các thông tin CSDL của DNS, còn Resolver đơn giản chỉ là các hàm thư viện dùng để tạo các truy vấn (query) và gửi chúng qua đến Name Server. DNS được thi hành như một giao thức tầng Application trong mạng TCP/IP.

DNS là 1 CSDL phân tán. Điều này cho phép người quản trị cục bộ quản lý phần dữ liệu nội bộ thuộc phạm vi của họ, đồng thời dữ liệu này cũng dễ dàng truy cập được trên toàn bộ hệ thống mạng theo mô hình **Client-Server**. Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân bản (**replication**) và lưu tạm (**caching**). Một **hostname** trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm(.).



Hình 2.1: Sơ đồ tổ chức DNS

Loại tên	Miêu tả	Ví dụ
Gốc (domain root)	Nó là đỉnh của nhánh cây của tên miền. Nó xác định kết thúc của domain (fully qualified domain names)	Đơn giản nó chỉ là dấu chấm (.) sử dụng tại cuối của tên ví như

Loại tên	Miêu tả	Ví dụ
	FQDNs).	"example.microsoft.com."
Tên miền cấp một (Top-level domain)	Là hai hoặc ba ký tự xác định nước/khu vực hoặc cáctổ chức	".com", xác định tên sử dụng trong xác định là tổ chức thương mại .
Tên miền cấp hai (Second-level domain)	Nó rất đa dạng trên internet, nó có thể là tên của một công ty, một tổ chức hay một cá nhân .v.v. đăng ký trên internet.	"microsoft.com.", là tên miền cấp hai đăng ký là công ty Microsoft.
Tên miền cấp nhỏ hơn	Chia nhỏ thêm ra của tên miền cấp hai xuống thường được sử dụng như chi "example.microsoft.com." là phần quản lý tài liệu ví dụ của microsof (Subdomain) nhánh, phong ban của một cơ quan hay một chủ đề nào đó.	

Cơ sở dữ liệu(CSDL) của **DNS** là một cây đảo ngược. Mỗi nút trên cây cũng lại là gốc của 1 cây con. Mỗi cây con là 1 phân vùng con trong toàn bộ CSDL **DNS** gọi là 1 miền (**domain**). Mỗi domain có thể phân chia thành các phân vùng con nhỏ hơn gọi là các miền con (**subdomain**).

Mỗi **domain** có 1 tên (**domain name**). Tên **domain** chỉ ra vị trí của nó trong CSDL **DNS**. Trong **DNS** tên miền là chuỗi tuần tự các tên nhãn tại nút đó đi ngược lên nút gốc của cây và phân cách nhau bởi dấu chấm.

Tên nhãn bên phải trong mỗi **domain name** được gọi là **top-level domain**. Trong ví dụ trước srv1.csc.hcmuns.edu.vn, vậy miền “.vn” là **top-level domain**. Bảng sau đây liệt kê **top-level domain**.

Tên miền	Mô tả
.com	Các tổ chức, công ty thương mại
.org	Các tổ chức phi lợi nhuận
.net	Các trung tâm hỗ trợ về mạng
.edu	Các tổ chức giáo dục
.gov	Các tổ chức thuộc chính phủ
.mil	Các tổ chức quân sự
.int	Các tổ chức được thành lập bởi các hiệp ước quốc tế

Bên cạnh đó, mỗi nước cũng có một **top-level domain**. Ví dụ **top-level domain** của Việt Nam là .vn, Mỹ là .us, ta có thể tham khảo thêm thông tin địa chỉ tên miền tại địa chỉ: <http://www.thrall.org/domains.htm>

Ví dụ về tên miền của một số quốc gia

Tên miền quốc gia	Tên quốc gia
.vn	Việt Nam
.us	Mỹ
.uk	Anh

Tên miền quốc gia	Tên quốc gia
.jp	Nhật Bản
.ru	Nga
.cn	Trung Quốc

2.1.2. Đặc điểm của DNS trong Windows Server

- **Conditional forwarder:** Cho phép **Name Server** chuyển các yêu cầu phân giải dựa theo tên domain trong yêu cầu truy vấn.
- **Stub zone:** hỗ trợ cơ chế phân giải hiệu quả hơn.
- Đồng bộ các **DNS zone** trong **Active Directory (DNS zone replication in Active Directory)**.
 - Cung cấp một số cơ chế bảo mật tốt hơn trong các hệ thống **Windows** trước đây.
 - Luân chuyển (**Round robin**) tất cả các loại **RR**.
 - Cung cấp nhiều cơ chế ghi nhận và theo dõi sự cố lỗi trên **DNS**.
 - Hỗ trợ giao thức **DNS Security Extensions (DNSSEC)** để cung cấp các tính năng bảo mật cho việc lưu trữ và nhân bản (**replicate**) **zone**.
 - Cung cấp tính năng **EDNS0 (Extension Mechanisms for DNS)** để cho phép **DNS Requestor** quản bá những **zone transfer packet** có kích thước lớn hơn 512byte.

2.2. Cách phân bố dữ liệu quản lý trên tên miền

Mục tiêu:

- Trình bày được sự phân bố dữ liệu quản lý trên tên miền.

Những **root name server** (.) quản lý những **top-level domain** trên **Internet**. Tên máy và địa chỉ **IP** của những **name server** này được công bố cho mọi người biết và chúng được liệt kê trong bảng sau. Những **name server** này cũng có thể đặt khắp nơi trên thế giới.

Tên máy tính	Địa chỉ IP
H.ROOT-SERVERS.NET	128.63.2.53
B.ROOT-SERVERS.NET	128.9.0.107
C.ROOT-SERVERS.NET	192.33.4.12
D.ROOT-SERVERS.NET	128.8.10.90
E.ROOT-SERVERS.NET	192.203.230.10
I.ROOT-SERVERS.NET	192.36.148.17
F.ROOT-SERVERS.NET	192.5.5.241
F.ROOT-SERVERS.NET	39.13.229.241
G.ROOT-SERVERS.NET	192.112.88.4
A.ROOT-SERVERS.NET	198.41.0.4

Thông thường một tổ chức được đăng ký một hay nhiều domain name. Sau đó, mỗi tổ chức sẽ cài đặt một hay nhiều name server và duy trì cơ sở dữ liệu cho tất cả những máy tính trong domain. Những name server của tổ chức được đăng ký trên Internet. Một trong những name server này được biết như là Primary Name Server. Nhiều Secondary Name Server được dùng để làm backup cho Primary Name Server. Trong trường hợp Primary bị lỗi, Secondary được sử dụng để phân giải tên.

Primary Name Server có thể tạo ra những subdomain và ủy quyền những subdomain này cho những Name Server khác.

2.3. Cơ chế phân giải tên

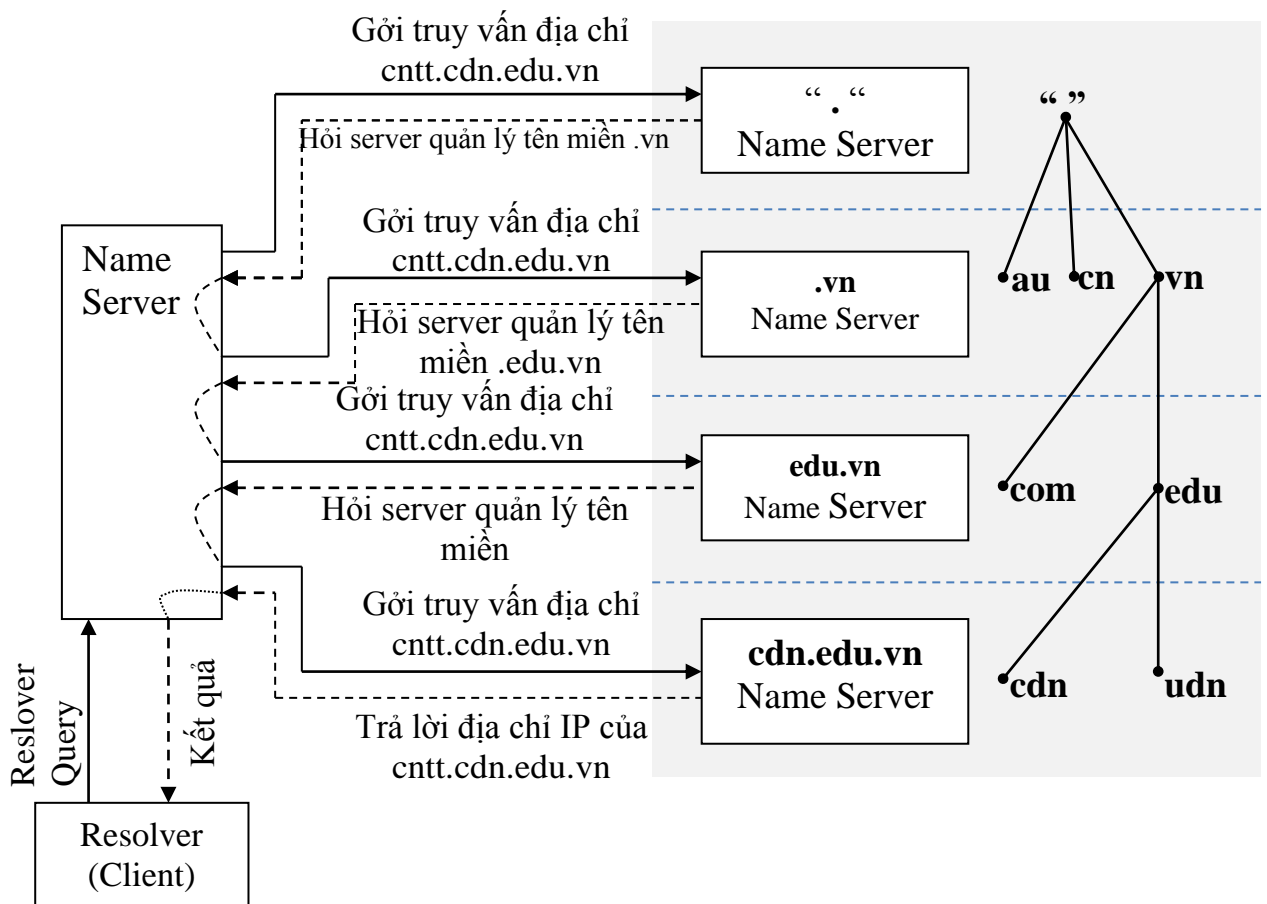
Mục tiêu:

- Trình bày được cơ chế phân giải tên máy tính thành địa chỉ IP và ngược lại;

2.3.1. Phân giải tên thành IP

Root name server : Là máy chủ quản lý các **name server** ở mức **top-level domain**. Khi có truy vấn về một tên miền nào đó thì **Root Name Server** phải cung cấp tên và địa chỉ **IP** của **name server** quản lý **top-level domain** (Thực tế là hầu hết các **root server** cũng chính là máy chủ quản lý **top-level domain**) và đến lượt các **name server** của **top-level domain** cung cấp danh sách các **name server** có quyền trên các **second-level domain** mà tên miền này thuộc vào. Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn.

Qua trên cho thấy vai trò rất quan trọng của **root name server** trong quá trình phân giải tên miền. Nếu mọi **root name server** trên mạng **Internet** không liên lạc được thì mọi yêu cầu phân giải đều không thực hiện được.



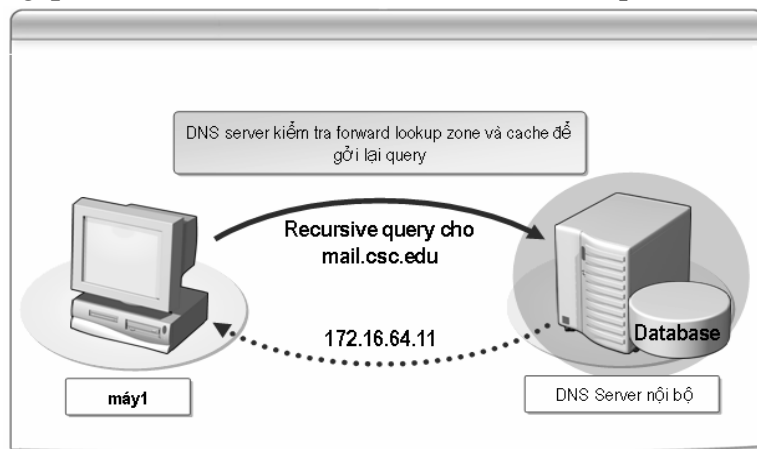
Hình 2.2: Mô tả quá trình phân giải `cntt.edu.vn` trên mạng **Internet**

Client sẽ gửi yêu cầu cần phân giải địa chỉ **IP** của máy tính có tên `cntt.DVDn.edu.vn` đến **name server** cục bộ. Khi nhận yêu cầu từ **Resolver**, **Name Server** cục bộ sẽ phân tích tên này và xét xem tên miền này có do mình quản lý hay không. Nếu như tên miền do **Server** cục bộ quản lý, nó sẽ trả lời địa chỉ **IP** của tên máy đó ngay cho **Resolver**. Ngược lại, server cục bộ sẽ truy vấn đến một **Root**

Name Server gần nhất mà nó biết được. **Root Name Server** sẽ trả lời địa chỉ IP của **Name Server** quản lý miền **vn**. Máy chủ **name server** cục bộ lại hỏi tiếp **name server** quản lý miền **vn** và được tham chiếu đến máy chủ quản lý miền **edu.vn**. Máy chủ quản lý **edu.vn** chỉ dẫn máy **name server** cục bộ tham chiếu đến máy chủ quản lý miền **DVDn.edu.vn**. Cuối cùng máy **name server** cục bộ truy vấn máy chủ quản lý miền **DVDn.edu.vn** và nhận được câu trả lời.

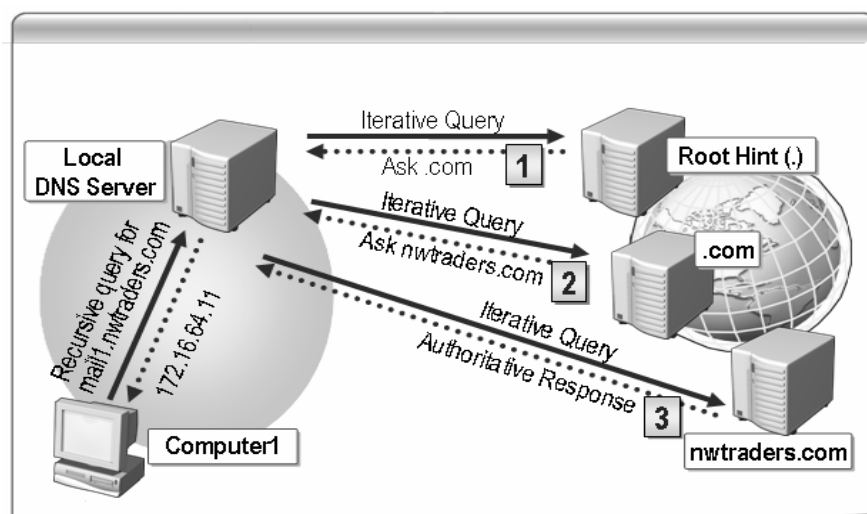
Các loại truy vấn : Truy vấn có thể ở 2 dạng :

- Truy vấn đệ quy (**recursive query**) : khi **name server** nhận được truy vấn dạng này, nó bắt buộc phải trả về kết quả tìm được hoặc thông báo lỗi nếu như truy vấn này không phân giải được. **Name server** không thể tham chiếu truy vấn đến một **name server** khác. **Name server** có thể gửi truy vấn dạng đệ quy hoặc tương tác đến **name server** khác nhưng phải thực hiện cho đến khi nào có kết quả mới thôi.



Hình 2.3: Truy vấn đệ quy (**recursive query**)

- Truy vấn tương tác (**Iterative query**): khi **name server** nhận được truy vấn dạng này, nó trả lời cho **Resolver** với thông tin tốt nhất mà nó có được vào thời điểm lúc đó. Bản thân **name server** không thực hiện bất cứ một truy vấn nào thêm. Thông tin tốt nhất trả về có thể lấy từ dữ liệu cục bộ (kể cả **cache**). Trong trường hợp **name server** không tìm thấy trong dữ liệu cục bộ nó sẽ trả về tên miền và địa chỉ IP của **name server** gần nhất mà nó biết.



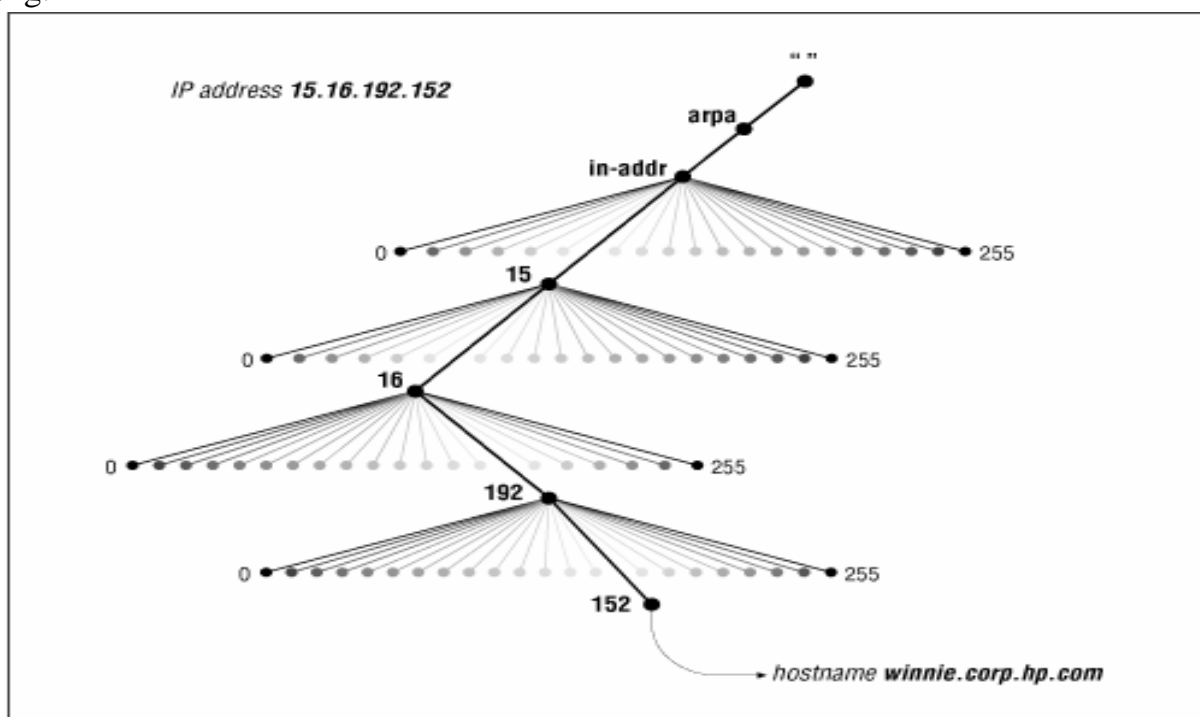
Hình 2.4: Truy vấn tương tác (**Iterative query**):

2.3.2. Phân giải IP thành tên máy tính

Ánh xạ địa chỉ **IP** thành tên máy tính được dùng để diễn dịch các tập tin log cho dễ đọc hơn. Nó còn dùng trong một số trường hợp chứng thực trên hệ thống **UNIX** (kiểm tra các tập tin `.rhost` hay `host.equiv`). Trong không gian tên miền đã nói ở trên dữ liệu -bao gồm cả địa chỉ **IP**- được lập chỉ mục theo tên miền. Do đó với một tên miền đã cho việc tìm ra địa chỉ **IP** khá dễ dàng.

Để có thể phân giải tên máy tính của một địa chỉ **IP**, trong không gian tên miền người ta bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ **IP**. Phần không gian này có tên miền là **in-addr.arpa**.

Mỗi nút trong miền **in-addr.arpa** có một tên nhãn là chỉ số thập phân của địa chỉ **IP**. Ví dụ miền **in-addr.arpa** có thể có 256 **subdomain**, tương ứng với 256 giá trị từ 0 đến 255 của byte đầu tiên trong địa chỉ **IP**. Trong mỗi **subdomain** lại có 256 **subdomain** con nữa ứng với byte thứ hai. Cứ như thế và đến byte thứ tư có các bản ghi cho biết tên miền đầy đủ của các máy tính hoặc các mạng có địa chỉ **IP** tương ứng.



Hình 2.5: Phân giải IP thành tên máy tính

Lưu ý khi đọc tên miền địa chỉ **IP** sẽ xuất hiện theo thứ tự ngược. Ví dụ nếu địa chỉ **IP** của máy `winnie.corp.hp.com` là `15.16.192.152`, khi ánh xạ vào miền `in-addr.arpa` sẽ là `152.192.16.15.in-addr.arpa`.

2.4. Một số khái niệm cơ bản

Mục tiêu:

- Trình bày được các khái niệm cơ bản.

2.4.1. Domain name và zone

Một miền gồm nhiều thực thể nhỏ hơn gọi là miền con (**subdomain**). Ví dụ, miền **ca** bao gồm nhiều miền con như **ab.ca**, **on.ca**, **qc.ca**,... . Bạn có thể ủy quyền một số miền con cho những **DNS Server** khác quản lý. Những miền và miền con mà **DNS**

Server được quyền quản lý gọi là **zone**. Như vậy, một **Zone** có thể gồm một miền, một hay nhiều miền con.

Các loại **zone**:

- **Primary zone**: Cho phép đọc và ghi cơ sở dữ liệu.
- **Secondary zone**: Cho phép đọc bản sao cơ sở dữ liệu.
- **Stub zone**: chứa bản sao cơ sở dữ liệu của **zone** nào đó, nó chỉ chứa chỉ một vài **RR(Resource Record)**.

2.4.2. Fully Qualified Domain Name (FQDN)

Mỗi nút trên cây có một tên gọi(không chứa dấu chấm) dài tối đa 63 ký tự. Tên riêng dành riêng cho gốc (**root**) cao nhất và biểu diễn bởi dấu chấm. Một tên miền đầy đủ của một nút chính là chuỗi tuần tự các tên gọi của nút hiện tại đi ngược lên nút gốc, mỗi tên gọi cách nhau bởi dấu chấm. Tên miền có xuất hiện dấu chấm sau cùng được gọi là tên tuyệt đối (**absolute**) khác với tên tương đối là tên không kết thúc bằng dấu chấm. Tên tuyệt đối cũng được xem là tên miền đầy đủ đã được chứng nhận (**Fully Qualified Domain Name – FQDN**).

2.4.3. Sự ủy quyền(Delegation)

Một trong các mục tiêu khi thiết kế hệ thống DNS là khả năng quản lý phân tán thông qua cơ chế ủy quyền (delegation). Trong một miền có thể tổ chức thành nhiều miền con, mỗi miền con có thể được ủy quyền cho một tổ chức khác và tổ chức đó chịu trách nhiệm duy trì thông tin trong miền con này. Khi đó, miền cha chỉ cần một con trỏ trỏ đến miền con này để tham chiếu khi có các truy vấn.

Không phải một miền luôn luôn tổ chức miền con và ủy quyền toàn bộ cho các miền con này, có thể chỉ có vài miền con được ủy quyền.

2.4.4. Forwarders

Là kỹ thuật cho phép Name Server nội bộ chuyển yêu cầu truy vấn cho các Name Server khác để phân giải các miền bên ngoài.

2.4.5. Stub zone

Là zone chứa bản sao cơ sở dữ liệu DNS từ master name server, Stub zone chỉ chứa các resource record cần thiết như : A, SOA, NS, một hoặc vài địa chỉ của master name server hỗ trợ cơ chế cập nhật Stub zone, chế chứng thực name server trong zone và cung cấp cơ chế phân giải tên miền được hiệu quả hơn, đơn giản hóa công tác quản trị.

2.4.6. Dynamic DNS

Dynamic DNS là phương thức ánh xạ tên miền tới địa chỉ IP có tần xuất thay đổi cao. Dịch vụ DNS động (Dynamic DNS) cung cấp một chương trình đặc biệt chạy trên máy tính của người sử dụng dịch vụ dynamic DNS gọi là Dynamic Dns Client. Chương trình này giám sát sự thay đổi địa chỉ IP tại host và liên hệ với hệ thống DNS mỗi khi địa chỉ IP của host thay đổi và sau đó update thông tin vào cơ sở dữ liệu DNS về sự thay đổi địa chỉ đó.

2.4.7. Active Directory-integrated zone

Sử dụng Active Directory-integrated zone có một số thuận lợi sau:

- DNS zone lưu trữ trong trong Active Directory, nhờ cơ chế này mà dữ liệu được bảo mật hơn.
- Sử dụng cơ chế nhân bản của Active Directory để cập nhật và sao chép cơ sở dữ liệu DNS.
- Sử dụng secure dynamic update.
- Sử dụng nhiều master name server để quản lý tên miền thay vì sử dụng một master name server.

2.5. Phân loại Domain Name Server

Mục tiêu:

- Trình bày được các loại tên Domain Server.

2.5.1. Primary Name Server

Mỗi miền phải có một Primary Name Server. Server này được đăng kí trên Internet để quản lý miền. Mọi người trên Internet đều biết tên máy tính và địa chỉ IP của Server này. Người quản trị DNS sẽ tổ chức những tập tin CSDL trên Primary Name Server. Server này có nhiệm vụ phân giải tất cả các máy trong miền hay zone.

2.5.2. Secondary Name Server

Mỗi miền có một Primary Name Server để quản lý CSDL của miền. Nếu như Server này tạm ngưng hoạt động vì một lý do nào đó thì việc phân giải tên máy tính thành địa chỉ IP và ngược lại xem như bị gián đoạn. Việc gián đoạn này làm ảnh hưởng rất lớn đến những tổ chức có nhu cầu trao đổi thông tin ra ngoài Internet cao. Nhằm khắc phục nhược điểm này, những nhà thiết kế đã đưa ra một Server dự phòng gọi là Secondary(hay Slave) Name Server. Server này có nhiệm vụ sao lưu tất cả những dữ liệu trên Primary Name Server và khi Primary Name Server bị gián đoạn thì nó sẽ đảm nhận việc phân giải tên máy tính thành địa chỉ IP và ngược lại. Trong một miền có thể có một hay nhiều Secondary Name Server. Theo một chu kỳ, Secondary sẽ sao chép và cập nhật CSDL từ Primary Name Server. Tên và địa chỉ IP của Secondary Name Server cũng được mọi người trên Internet biết đến.

2.5.3. Caching Name Server

Caching Name Server không có bất kỳ tập tin CSDL nào. Nó có chức năng phân giải tên máy trên những mạng ở xa thông qua những Name Server khác. Nó lưu giữ lại những tên máy đã được phân giải trước đó và được sử dụng lại những thông tin này nhằm mục đích:

- Làm tăng tốc độ phân giải bằng cách sử dụng cache.
- Giảm bớt gánh nặng phân giải tên máy cho các Name Server.
- Giảm việc lưu thông trên những mạng lớn.

2.6. Resource Record (RR)

RR là mẫu thông tin dùng để mô tả các thông tin về cơ sở dữ liệu DNS, các mẫu tin này được lưu trong các file cơ sở dữ liệu DNS (\systemroot\system32\dns).

2.6.1. SOA(Start of Authority)

Trong mỗi tập tin CSDL phải có một và chỉ một record SOA (start of authority). Record SOA chỉ ra rằng máy chủ Name Server là nơi cung cấp thông tin tin cậy từ dữ liệu có trong zone.

Cú pháp của record SOA.

**[tên-miền] IN SOA [tên-server-dns] [địa-chỉ-email](
serial number;
refresh number;
retry number;
experi number;
Time-to-live number)**

- **Serial:** Áp dụng cho mọi dữ liệu trong zone và là 1 số nguyên. Trong ví dụ, giá trị này bắt đầu từ 1 nhưng thông thường người ta sử dụng theo định dạng thời gian như 2012032501. Định dạng này theo kiểu YYYYMMDDNN, trong đó YYYY là năm, MM là tháng, DD là ngày và NN số lần sửa đổi dữ liệu zone trong ngày. Bất kể là theo định dạng nào, luôn luôn phải tăng số này lên mỗi lần sửa đổi dữ liệu zone. Khi máy chủ Secondary liên lạc với máy chủ Primary, trước tiên nó sẽ hỏi số serial. Nếu số serial của máy Secondary nhỏ hơn số serial của máy Primary tức là dữ liệu zone trên Secondary đã cũ và sau đó máy Secondary sẽ sao chép dữ liệu mới từ máy Primary thay cho dữ liệu đang có hiện hành.

- **Refresh:** Chỉ ra khoảng thời gian máy chủ Secondary kiểm tra dữ liệu zone trên máy Primary để cập nhật nếu cần. Trong ví dụ trên thì cứ mỗi 3 giờ máy chủ Secondary sẽ liên lạc với máy chủ Primary để cập nhật dữ liệu nếu có. Giá trị này thay đổi tùy theo tần suất thay đổi dữ liệu trong zone.

- **Retry:** nếu máy chủ Secondary không kết nối được với máy chủ Primary theo thời hạn mô tả trong refresh (ví dụ máy chủ Primary bị shutdown vào lúc đó thì máy chủ Secondary phải tìm cách kết nối lại với máy chủ Primary theo một chu kỳ thời gian mô tả trong retry. Thông thường giá trị này nhỏ hơn giá trị refresh.

- **Expire:** Nếu sau khoảng thời gian này mà máy chủ Secondary không kết nối được với máy chủ Primary thì dữ liệu zone trên máy Secondary sẽ bị quá hạn. Một khi dữ liệu trên Secondary bị quá hạn thì máy chủ này sẽ không trả lời mọi truy vấn về zone này nữa. Giá trị expire này phải lớn hơn giá trị refresh và giá trị retry.

- **TTL:** Viết tắt của time to live. Giá trị này áp dụng cho mọi record trong zone và được đính kèm trong thông tin trả lời một truy vấn. Mục đích của nó là chỉ ra thời gian mà các máy chủ Name Server khác cache lại thông tin trả lời. Việc cache thông tin trả lời giúp giảm lưu lượng truy vấn DNS trên mạng.

2.6.2. NS (Name Server)

Record tiếp theo cần có trong zone là NS (name server) record. Mỗi Name Server cho zone sẽ có một NS record.

Cú pháp:

[domain_name] IN NS [DNS-Server_name]

Ví dụ: Record NS sau:

qtm.com. IN NS dnserver.qtm.com.

qtm.com. IN NS server.qtm.com.

chỉ ra 2 name servers cho miền qtm.com

2.6.3. A (Address) và CNAME (Canonical Name)

Record A (Address) ánh xạ tên máy (hostname) vào địa chỉ IP. Record CNAME (canonical name) tạo tên bí danh alias trở vào một tên canonical. Tên canonical là tên host trong record A hoặc lại trở vào 1 tên canonical khác.

Cú pháp record A:

[tên-máy-tính] IN A [địa-chỉ-IP]

Ví dụ: record A trong tập tin db.qtm // Multi-homed hosts
server.qtm.com. IN A 172.29.14.1 server.qtm.com. IN A 172.29.14.1
diehard.qtm.com. IN A 172.29.14.4 server.qtm.com. IN A 192.253.253.1

2.6.4. AAAA

Ánh xạ tên máy (hostname) vào địa chỉ IP version 6

Cú pháp:

[tên-máy-tính] IN AAAA [địa-chỉ-IPv6]

Ví dụ

Server IN AAAA 1243:123:456:789:1:2:3:456ab

2.6.5. SRV

Cung cấp cơ chế định vị dịch vụ, Active Directory sử dụng Resource Record này để xác định domain controllers, global catalog servers, Lightweight Directory Access Protocol (LDAP) servers.

Các field trong SVR:

- Tên dịch vụ service.
- Giao thức sử dụng.
- Tên miền (domain name).
- TTL và class.
- Priority.
- Weight (hỗ trợ load balancing).
- Port của dịch vụ.
- Target chỉ định FQDN cho host hỗ trợ dịch vụ.

2.6.6. MX (Mail Exchange)

DNS dùng record MX trong việc chuyển mail trên mạng Internet. Ban đầu chức năng chuyển mail dựa trên 2 record: record MD (mail destination) và record MF (mail forwarder) records. MD chỉ ra đích cuối cùng của một thông điệp mail có tên miền cụ thể. MF chỉ ra máy chủ trung gian sẽ chuyển tiếp mail đến được máy chủ đích cuối cùng. Tuy nhiên, việc tổ chức này hoạt động không tốt. Do đó, chúng được tích hợp lại thành một record là MX. Khi nhận được mail, trình chuyển mail (mailer) sẽ dựa vào record MX để quyết định đường đi của mail. Record MX chỉ ra một mail exchanger cho một miền - mail exchanger là một máy chủ xử lý (chuyển mail đến mailbox cục bộ hay làm gateway chuyển sang một giao thức chuyển mail khác như UUCP) hoặc chuyển tiếp mail đến một mail exchanger khác (trung gian) gần với mình nhất để đến tới máy chủ đích cuối cùng hơn dùng giao thức SMTP (Simple Mail Transfer Protocol).

Để tránh việc gửi mail bị lặp lại, record MX có thêm 1 giá trị bổ sung ngoài tên miền của mail exchanger là 1 số thứ tự tham chiếu. Đây là giá trị nguyên không dấu 16-bit (0-65535) chỉ ra thứ tự ưu tiên của các mail exchanger.

Cú pháp record MX:

[domain_name] IN MX [priority] [mail-host]

Ví dụ record MX sau :

qtm.com. INMX 10 mailserver.qtm.com.

Chỉ ra máy chủ mailserver.qtm.com là một mail exchanger cho miền qtm.com với số thứ tự tham chiếu 10.

Chú ý: các giá trị này chỉ có ý nghĩa so sánh với nhau.

Ví dụ khai báo 2 record MX:

qtm.com. IN MX 1 listo.qtm.com.

qtm.com. IN MX 2 hep.qtm.com.

Trình chuyển thư mailer sẽ thử phân phát thư đến mail exchanger có số thứ tự tham chiếu nhỏ nhất trước. Nếu không chuyển thư được thì mail exchanger với giá trị kế sau sẽ được chọn. Trong trường hợp có nhiều mail exchanger có cùng số tham chiếu thì mailer sẽ chọn ngẫu nhiên giữa chúng.

2.6.7. PTR (Pointer)

Record PTR (pointer) dùng để ánh xạ địa chỉ IP thành Hostname.

Cú pháp:

[Host-ID.{Reverse_Lookup_Zone}] IN PTR [tên-máy-tính]

Ví dụ:

Các record PTR cho các host trong mạng 192.249.249:

1.14.29.172.in-addr.arpa. IN PTR server.qtm.com.

2.7. Cài đặt và cấu hình DNS

Mục tiêu:

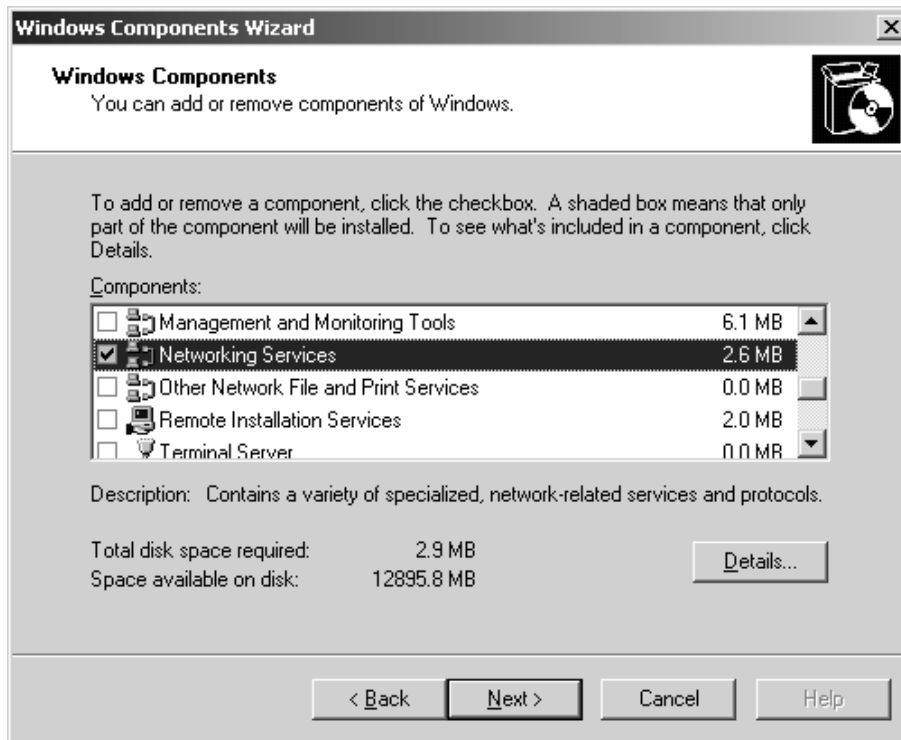
- Thực hiện được quá trình cài đặt và cấu hình DNS.

Có nhiều cách cài đặt dịch vụ **DNS** trên môi trường **Windows** như: Ta có thể cài đặt **DNS** khi ta nâng cấp máy chủ lên **domain controllers** hoặc cài đặt **DNS** trên máy **stand-alone Windows 2003 Server**.

2.7.1. Các bước cài đặt dịch vụ DNS

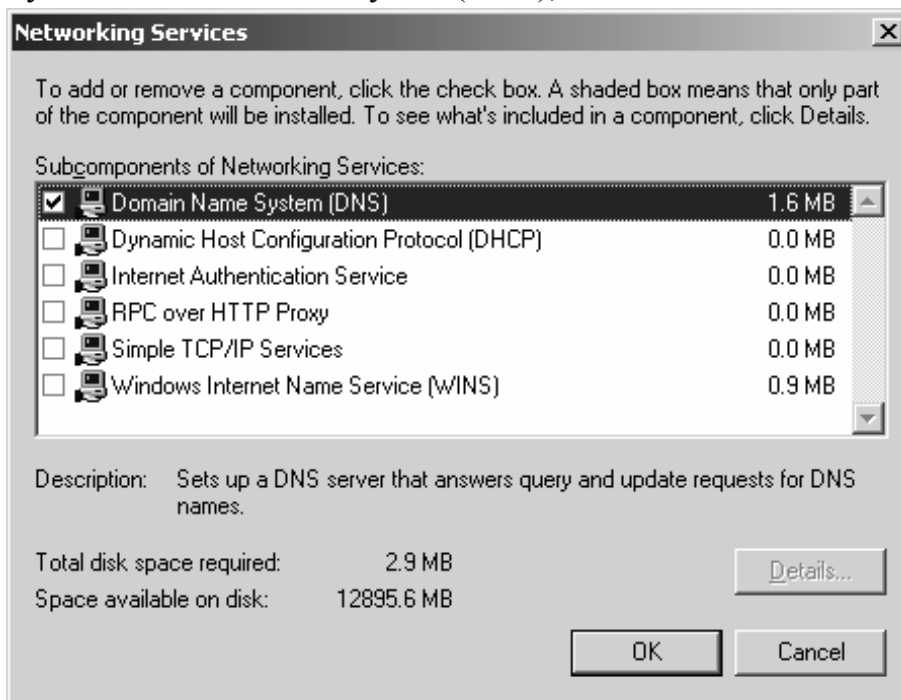
Khi cài đặt dịch vụ DNS trên Windows 2003 Server đòi hỏi máy này phải được cung cấp địa chỉ IP tĩnh, sau đây là một số bước cơ bản nhất để cài đặt dịch vụ DNS trên Windows 2003 stand-alone Server.

- Chọn Start | Control Panel | Add/Remove Programs.
- Chọn Add or Remove Windows Components trong hộp thoại Windows components.
- Từ hộp thoại ở bước 2 ta chọn **Network Services** sau đó chọn nút **Details**



Hình 2.6: Các bước cài đặt dịch vụ DNS

- Chọn tùy chọn Domain Name System(DNS), sau đó chọn nút OK



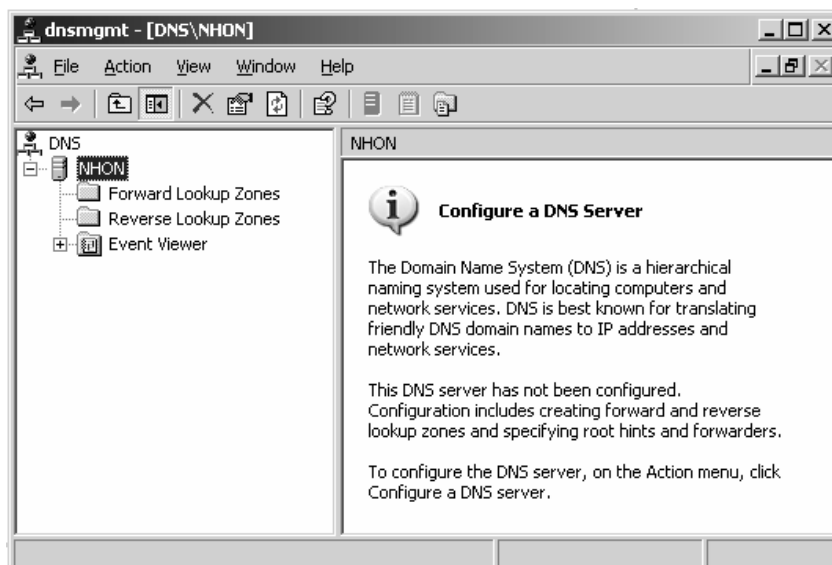
Hình 2.6.1: Các bước cài đặt dịch vụ DNS

- Chọn Next sau đó hệ thống sẽ chép các tập tin cần thiết để cài đặt dịch vụ (bạn phải đảm bảo có đĩa DVDROM Windows 2003 trên máy cục bộ hoặc có thể truy xuất tài nguyên này từ mạng). Chọn nút Finish để hoàn tất quá trình cài đặt.

2.7.2. Cấu hình dịch vụ DNS

Sau khi ta cài đặt thành công dịch vụ DNS, ta có thể tham khảo trình quản lý dịch vụ này như sau:

- Ta chọn Start | Programs | Administrative Tools | DNS. Nếu ta không cài DNS cùng với quá trình cài đặt Active Directory thì không có zone nào được cấu hình mặc định.



Hình 2.7: Cấu hình dịch vụ DNS

- Event Viewer: Đây trình theo dõi sự kiện nhật ký dịch vụ DNS, nó sẽ lưu trữ các thông tin về: cảnh giác (alert), cảnh báo (warnings), lỗi (errors).

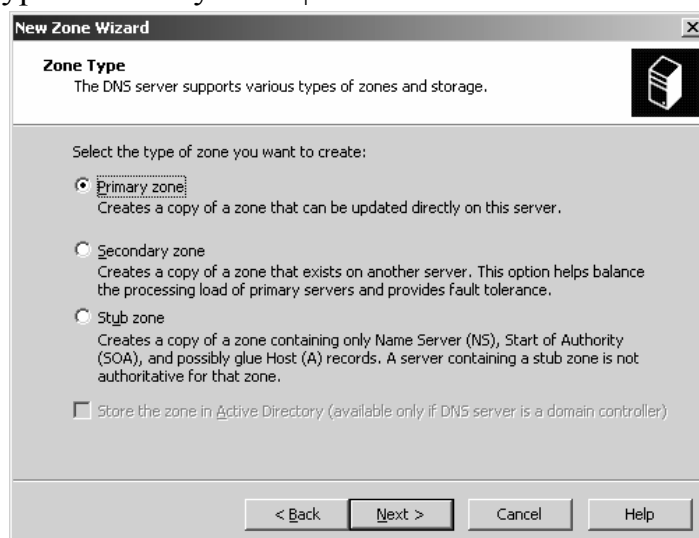
- Forward Lookup Zones: Chứa tất cả các zone thuận của dịch vụ DNS, zone này được lưu tại máy DNS Server.

- Reverse Lookup Zones: Chứa tất cả các zone nghịch của dịch vụ DNS, zone này được lưu tại máy DNS Server.

2.7.2.1. Tạo Forward Lookup Zones

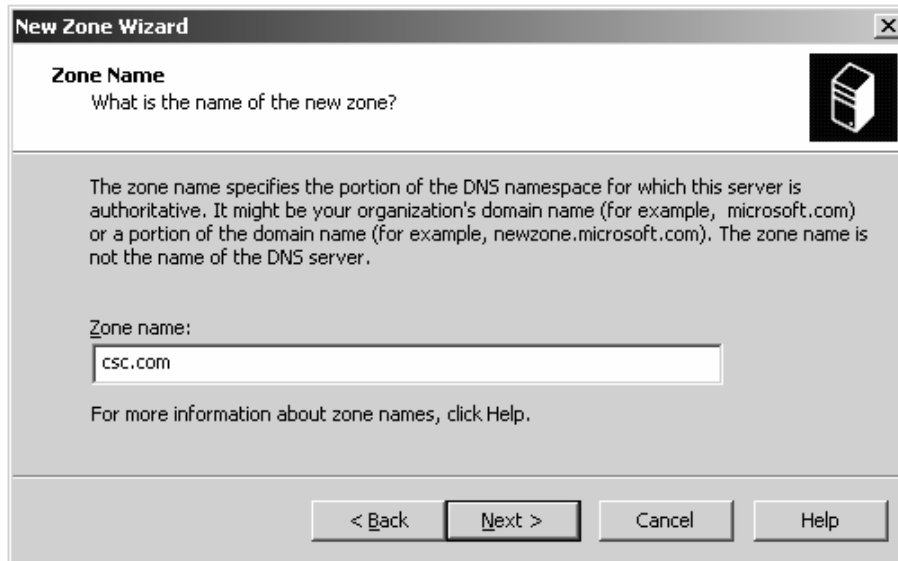
Forward Lookup Zone để phân giải địa chỉ Tên máy (hostname) thành địa chỉ IP. Để tạo zone này ta thực hiện các bước sau:

- Chọn nút Start | Administrative Tools | DNS.
- Chọn tên DNS server, sau đó Click chuột phải chọn New Zone. Chọn Next trên hộp thoại Welcome to New Zone Wizard.
- Chọn Zone Type là Primary Zone | Next.



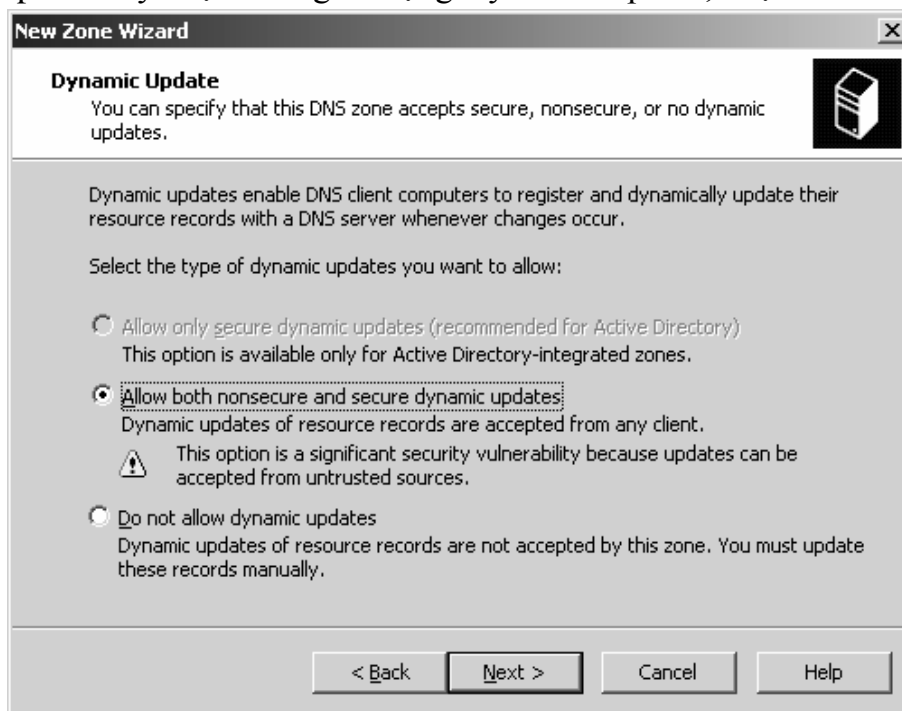
Hình 2.7.1: Cấu hình dịch vụ DNS

- Chọn Forward Lookup Zone | Next
- Chỉ định Zone Name để khai báo tên Zone (Ví dụ: csc.com), chọn Next.



Hình 2.7.2: Cấu hình dịch vụ DNS

- Từ hộp thoại Zone File, ta có thể tạo file lưu trữ cơ sở dữ liệu cho Zone(zonename.dns) hay ta có thể chỉ định Zone File đã tồn tại sẵn (tất cả các file này được lưu trữ tại %systemroot%\system32\dns), tiếp tục chọn Next.
- Hộp thoại Dynamic Update để chỉ định zone chấp nhận Secure Update, nonsecure Update hay chọn không sử dụng Dynamic Update, chọn Next.



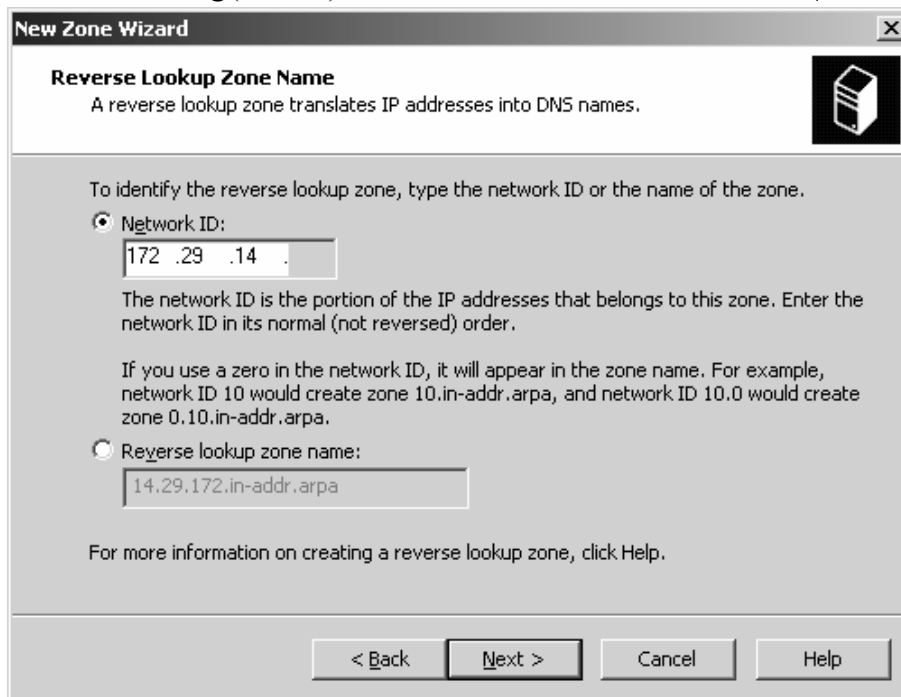
Hình 2.7.3: Cấu hình dịch vụ DNS

- Chọn Finish để hoàn tất.

2.7.2.2. Tạo Reverse Lookup Zone

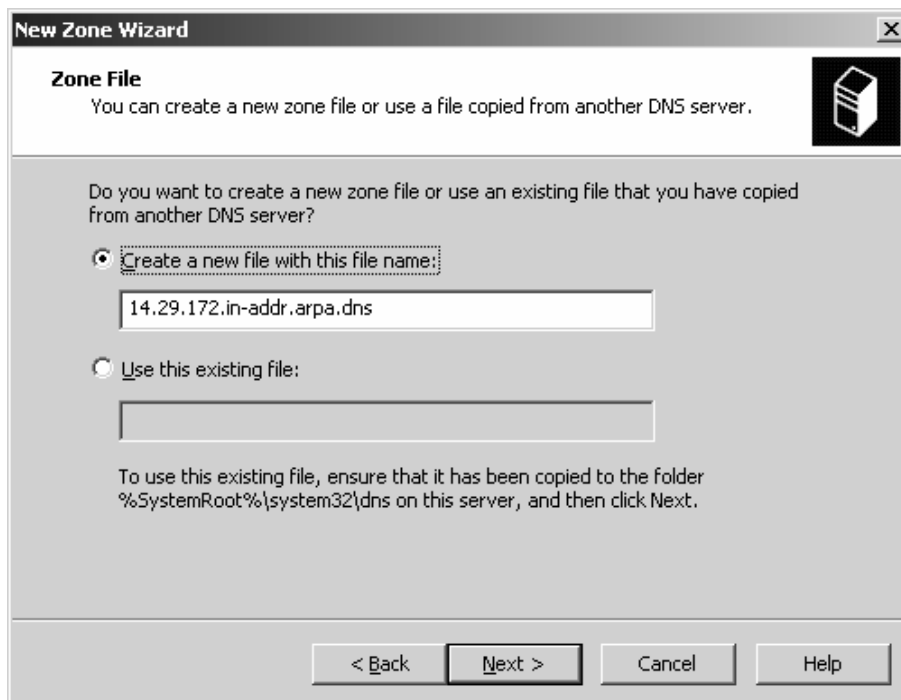
Sau khi ta hoàn tất quá trình tạo Zone thuận ta sẽ tạo Zone nghịch (Reverse Lookup Zone) để hỗ trợ cơ chế phân giải địa chỉ IP thành tên máy(hostname).

- Để tạo Reverse Lookup Zone ta thực hiện trình tự các bước sau: Chọn Start | Programs | Administrative Tools | DNS. Chọn tên của DNS server, Click chuột phải chọn New Zone
- Chọn Next trên hộp thoại Welcome to New Zone Wizard. Chọn Zone Type là Primary Zone | Next. Chọn Reverse Lookup Zone | Next.
- Gõ phần địa chỉ mạng(NetID) của địa chỉ IP trên Name Server | Next.



Hình 2.7.4: Cấu hình dịch vụ DNS

- Tạo mới hay sử dụng tập tin lưu trữ cơ sở dữ liệu cho zone ngược, sau đó chọn Next.



Hình 2.7.5: Cấu hình dịch vụ DNS

- Hộp thoại Dynamic Update để chỉ định zone chấp nhận Secure Update, nonsecure Update hãy chọn sử dụng Dynamic Update, chọn Next. Chọn Finish để hoàn tất.

Bài tập

1. Cài đặt dịch vụ DNS.
2. Cấu hình dịch vụ DNS.

HƯỚNG DẪN THỰC HIỆN

1. Cài đặt dịch vụ DNS

Khi cài đặt dịch vụ DNS trên Windows 2003 Server đòi hỏi máy này phải được cung cấp địa chỉ IP tĩnh, máy tính phải kết nối với HUB/SWITCH, sau đây là một số bước cơ bản nhất để cài đặt dịch vụ DNS trên Windows 2003 stand-alone Server.

- Chọn Start | Control Panel | Add/Remove Programs.
- Chọn Add or Remove Windows Components trong hộp thoại Windows components.
- Từ hộp thoại ở bước 2 **Windows components** ta chọn **Network Services** sau đó chọn nút **Details**
 - + Chọn mục **Domain Name System(DNS)**, sau đó chọn nút **OK**
 - + Chọn **Next** sau đó hệ thống sẽ chép các tập tin cần thiết để cài đặt dịch vụ (bạn phải đảm bảo có đĩa **DVDROM Windows 2003** trên máy cục bộ hoặc có thể truy xuất tài nguyên này từ mạng). Chọn nút **Finish** để hoàn tất quá trình cài đặt.

2. Cấu hình dịch vụ DNS

Sau khi ta cài đặt thành công dịch vụ **DNS**, ta có thể tham khảo trình quản lý dịch vụ này như sau:

Ta chọn **Start | Programs | Administrative Tools | DNS**. Nếu ta không cài **DNS** cùng với quá trình cài đặt **Active Directory** thì không có **zone** nào được cấu hình mặc định.

- **Event Viewer:** Đây trình theo dõi sự kiện nhật ký dịch vụ **DNS**, nó sẽ lưu trữ các thông tin về: cảnh giác (**alert**), cảnh báo (**warnings**), lỗi (**errors**).
- **Forward Lookup Zones:** Chứa tất cả các **zone** thuận của dịch vụ **DNS**, **zone** này được lưu tại máy **DNS Server**.
- **Reverse Lookup Zones:** Chứa tất cả các **zone** nghịch của dịch vụ **DNS**, **zone** này được lưu tại máy **DNS Server**.

2.1. Tạo Forward Lookup Zones

Forward Lookup Zone để phân giải địa chỉ Tên máy (**hostname**) thành địa chỉ **IP**. Để tạo **zone** này ta thực hiện các bước sau:

- Chọn nút Start | Administrative Tools | DNS.
- Chọn tên DNS server, sau đó Click chuột phải chọn New Zone. Chọn Next trên hộp thoại Welcome to New Zone Wizard.
- Chọn Zone Type là Primary Zone | Next.
- Chọn Forward Lookup Zone | Next
- Chỉ định Zone Name để khai báo tên Zone (Ví dụ: csc.com), chọn Next.

- Từ hộp thoại Zone File, ta có thể tạo file lưu trữ cơ sở dữ liệu cho Zone(zonename.dns) hay ta có thể chỉ định Zone File đã tồn tại sẵn (tất cả các file này được lưu trữ tại %systemroot%\system32\dns), tiếp tục chọn Next.

- Hộp thoại Dynamic Update để chỉ định zone chấp nhận Secure Update, nonsecure Update hay chọn không sử dụng Dynamic Update, chọn Next.

Chỉ định **Dynamic Update**, chọn **Finish** để hoàn tất.

2.2. Tạo Reverse Lookup Zone

Sau khi ta hoàn tất quá trình tạo Zone thuận ta sẽ tạo Zone nghịch (**Reverse Lookup Zone**) để hỗ trợ cơ chế phân giải địa chỉ IP thành tên máy(**hostname**).

Để tạo **Reverse Lookup Zone** ta thực hiện trình tự các bước sau: Chọn **Start | Programs | Administrative Tools | DNS**. Chọn tên của **DNS server**, Click chuột phải chọn **New Zone**

Chọn Next trên hộp thoại Welcome to New Zone Wizard. Chọn Zone Type là Primary Zone | Next. Chọn Reverse Lookup Zone | Next.

Gõ phần địa chỉ mạng(**NetID**) của địa chỉ IP trên **Name Server | Next**.

Tạo mới hay sử dụng tập tin lưu trữ cơ sở dữ liệu cho **zone** ngược, sau đó chọn **Next**.

Hộp thoại **Dynamic Update** để chỉ định zone chấp nhận **Secure Update**, **nonsecure Update** hay chọn không sử dụng **Dynamic Update**, chọn **Next**. Chọn **Finish** để hoàn tất.

2.3. Thêm tên miền (domain name)

Tại cửa sổ quản lý domain chọn vào server và bấm chuột phải hiện lên menu và chọn "*New Domain...*" để điền một domain mới .

Sau khi bấm vào "*New Domain*" nó sẽ xuất hiện cửa sổ cho phép bạn điền tên miền mà server được phép quản lý.

Sau khi điền bấm "*OK*" để kết thúc

2.4. Thêm một host mới

Tại cửa sổ quản lý DNS chọn zone đã tạo và bấm chuột phải chọn "*new host*"

Xuất hiện cửa sổ cho phép ta khai báo host mới

Bạn điền tên của host mà muốn tạo. Tên của host sẽ được tự động điền thêm phần domain để thành tên đầy đủ của host.

Ví dụ: như trên đây là vùng quản lý zone (*location*) là ktm.vnn.vn.

+ Vậy khi bạn điền *Name* là www và *IP address* là 203.162.0.100 thì sẽ tương ứng với định nghĩa domain www.ktm.vnn.vn. trở đến địa chỉ IP 203.162.0.100 www.ktm.vnn.vn. IN A 203.162.0.100

2.5. Tạo một bản ghi web (tạo bí danh)

Tại cửa sổ quản lý Domain và tên miền vừa tạo và bấm chuột phải và chọn "*New Alias*" để tạo một CNAME đến một host.

Bấm vào "*New Alias...*" sẽ xuất hiện cửa sổ cho phép khai báo Alias

Tại phần "*Alias name*" điền tên tạo alias và tại phần "*Fully qualified name for target host*" điền tên đầy đủ của một host mà muốn tạo bí danh (thường được sử dụng cho

webhosting) Ví dụ : www.ktm.vnn.vn. IN CNAME ktm.vnn.vn. Ta sẽ có trang web www.ktm.vnn.vn đặt trên server web có tên là ktm.vnn.vn.

2.6. Tạo một bản ghi thư điện tử (MX)

Tại cửa sổ quản lý DNS tại tên miền muốn tạo bản ghi MX bấm chuột phải

Sau khi bấm vào "New Mail Exchanger.." sẽ xuất hiện cửa sổ cho phép tạo các thông số cho bản ghi mx

Điền tại "Host or domain" điền tên hoặc để trống tên này kết hợp với phần zone "Parent domain" để tạo thành domain đầy đủ của bản ghi thư điện tử. Tại "Mail server" điền tên của server thư điện tử và tại "Mail server priority" điền mức độ ưu tiên của server thư điện tử (độ lớn càng nhỏ mức ưu tiên càng cao)

Ví dụ trên hình ta có: mail.ktm.vnn.vn IN MX 10 mr-hn.vnn.vn. Ta có tên miền thư điện tử mail.ktm.vnn.vn. (ta có thể tạo được các hộp thư abc@mail.ktm.vnn.vn) được chứa tại server thư điện tử mr-hn.vnn.vn với mức ưu tiên là 10

2.7. Chuyển quyền quản lý tên miền (delegate)

Tại cửa sổ quản lý DNS tại domain muốn chuyển quyền quản lý bấm chuột phải.

Bấm vào "New Delegation.." để hiện cửa sổ cho phép chuyển quyền quản lý tên miền

Điền phần domain mà bạn muốn chuyển quyền quản lý vào "Delegated domain" Ví dụ ở đây điền là abc nghĩa là bạn muốn chuyển quyền quản lý domain abc.ktm.vnn.vn. Bấm "Next" để tiếp tục

Hiện cửa sổ điền vào "Server name" tên của dns server sẽ được phép quản lý tên miền abc.ktm.vnn.vn. Bấm "Resolve" để xác định địa chỉ IP của dns server. Sau đó bấm "Ok" để kết thúc. Ví dụ abc.ktm.vnn.vn. IN NS vdc-hn01.vnn.vn. Tương ứng tên miền abc.ktm.vnn.vn sẽ được chuyển quyền về dns server vdc-hn01.vnn.vn để quản lý.

Bài 3: ACTIVE DIRECTORY

Giới thiệu

Dịch vụ thư mục đã là một phần của một hệ thống liên kết mở (OSI), Trong những năm 1980, ITU và ISO tiến tới một bộ các tiêu chuẩn – X.500, các dịch vụ thư mục, bước đầu để hỗ trợ các yêu cầu của các nhà cung cấp dịch vụ nhắn tin và Tra cứu tên mạng.

Giao thức thư mục nhẹ, LDAP, dựa trên các dịch vụ thư mục thông tin của X.500 nhưng sử dụng TCP/IP stack và một chuỗi mã hóa chương trình của giao thức X.500 DAP, cho nó liên quan nhiều hơn trên Internet.

1. Mục tiêu của bài học:

- Trình bày được cấu trúc của Active Directory trên windows server;
- Cài đặt và cấu hình được máy điều khiển vùng.
- Thực hiện các thao tác an toàn với máy tính.

2. Nội dung chính:

2.1 Các mô hình mạng trong môi trường Microsoft

Mạng máy tính là một hệ thống gồm nhiều máy tính và các thiết bị được kết nối với nhau bởi đường truyền vật lý theo một kiến trúc (Network Architecture) nào đó nhằm thu thập, trao đổi dữ liệu và chia sẻ tài nguyên cho nhiều người sử dụng.

Một máy tính trên mạng có thể thuộc một trong ba loại như sau:

- + **Máy trạm (Client):** Không cung cấp tài nguyên mà chỉ sử dụng tài nguyên từ mạng.
- + **Máy chủ (Server):** Cung cấp tài nguyên và các dịch vụ cho các máy trên mạng.
- + **Peer:** Sử dụng tài nguyên và đồng thời cũng cung cấp tài nguyên cho mạng.

Dựa vào cách mà các máy tính được nối vào mạng cũng như cách mà chúng tương tác với mạng và với nhau, mạng máy tính được chia làm ba mô hình cơ bản như sau:

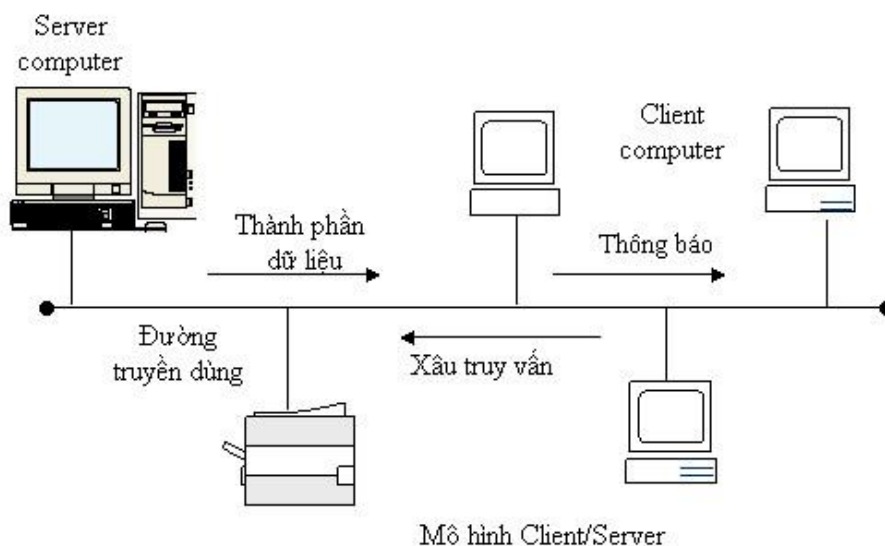
- **Mô hình trạm-chủ (Client-Server):** Các máy trạm được nối với các máy chủ, nhận quyền truy cập mạng và tài nguyên mạng từ các máy chủ. Đối với Windows NT các máy được tổ chức thành các miền (**domain**). An ninh trên các domain được quản lý bởi một số máy chủ đặc biệt gọi là **domain controller**. Trên domain có một master domain controller được gọi là **PDC (Primary Domain Controller)** và một **BDC (Backup Domain Controller)** để đề phòng trường hợp PDC gặp sự cố.

- **Mô hình phân mềm Client/Server:** là mô hình giải pháp phân mềm cho việc khắc phục tình trạng quá tải trên mạng và vượt qua những ngăn cách về sự khác nhau trong cấu trúc vật lý cũng như hệ điều hành của các hệ thống máy tính khác nhau trên mạng.

Mỗi phần mềm xây dựng theo mô hình Client/Server sẽ được chia làm hai phần: phần hoạt động trên máy phục vụ gọi là phần phía Server và phần hoạt động trên trạm làm việc gọi là phần phía Client. Với mô hình này các trạm làm việc cũng được gọi là các Client (hay máy Client) còn các máy phục vụ gọi là các Server. Nhiệm vụ của mỗi phần được quy định như sau:

Phần phía Server quản lý các giao tiếp môi trường bên ngoài tại Server và với các Client, tiếp nhận các yêu cầu dưới dạng các xâu ký tự (query string), phân tích các query string, xử lý dữ liệu và gửi kết quả trả lời về phía các Client.

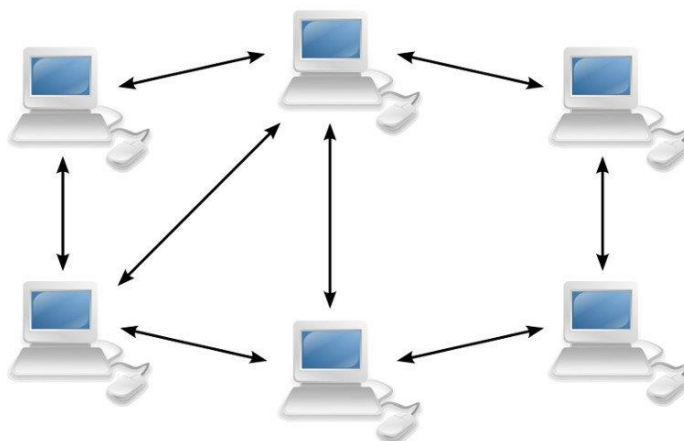
Phần phía Client tổ chức giao tiếp với người dùng, với môi trường bên ngoài tại trạm làm việc và với phía Server, tiếp nhận yêu cầu của người dùng, thành lập các query string gửi về phía Server, tiếp nhận kết quả và tổ chức trình diễn chúng.



Hình 3.1: Mô hình mạng Client/Server

Mạng ngang hàng (P2P): là mạng mà trong đó hai hay nhiều máy tính chia sẻ tập tin và truy cập các thiết bị như máy in mà không cần đến máy chủ hay phần mềm máy chủ. Mạng ngang hàng thường được tổ chức thành các nhóm làm việc workgroup. Mô hình này không có quá trình đăng nhập tập trung, nếu đã đăng nhập vào mạng bạn có thể sử dụng tất cả tài nguyên trên mạng. Truy cập vào các tài nguyên phụ thuộc vào người đã chia sẻ các tài nguyên đó, do vậy bạn có thể phải biết mật khẩu để có thể truy cập được tới các tài nguyên được chia sẻ.

Mạng p2p được tạo ra bởi hai hay nhiều máy tính được kết nối với nhau và chia sẻ tài nguyên mà không phải thông qua một máy chủ dành riêng. Mạng p2p có thể là kết nối tại chỗ – hai máy tính nối với nhau qua cổng USB để truyền tập tin. P2p cũng có thể là cơ sở hạ tầng thường trực kết nối 5-6 máy tính với nhau trong một văn phòng nhỏ bằng cáp đồng. Hay nó cũng có thể là một mạng có quy mô lớn hơn nhiều, dùng các giao thức và ứng dụng đặc biệt để thiết lập những mối quan hệ trực tiếp giữa người dùng trên internet.



Hình 3.2: Mô hình mạng máy tính Peer-to-peer.

Mô hình lai (Hybrid): Mô hình này là sự kết hợp giữa Client-Server và Peer-to-Peer. Phần lớn các mạng máy tính trên thực tế thuộc mô hình này.

Trong các mô hình mạng nói trên, mỗi mô hình có những ưu, nhược điểm riêng đối với từng chỉ tiêu đánh giá như: tính bảo mật thông tin, sự cài đặt, khả năng mở rộng mạng.... Sự so sánh giữa các mô hình mạng trên đối với một số chỉ tiêu đánh giá phổ biến được cho trong bảng sau:

Mô hình mạng	Client-Server	Peer-to-Peer	Hybrid
Chỉ tiêu đánh giá			
Độ an toàn và tính bảo mật thông tin.	Có độ an toàn và bảo mật thông tin cao nhất. Quản trị mạng có thể điều chỉnh quyền truy nhập thông tin.	Độ an toàn và bảo mật kém, phụ thuộc vào mức truy nhập được chia sẻ.	Độ an toàn và bảo mật cao gần như Client-Server.
Khả năng cài đặt.	Khó cài đặt.	Dễ cài đặt.	Khó cài đặt.
Đòi hỏi về phần cứng và phần mềm.	Đòi hỏi có máy chủ, hệ điều hành mạng và các phần cứng bổ sung.	Không cần máy chủ, hệ điều hành mạng, phần cứng bổ sung rất ít.	Như Client-Server.
Quản trị mạng.	Phải có quản trị mạng.	Không cần có quản trị mạng.	Như Client-Server.
Xử lý và lưu trữ tập trung.	Có.	Không.	Không.
Chi phí cài đặt.	Cao.	Thấp.	Cao.

Trong mô hình mạng có máy chủ (server) không phải mọi máy chủ đều hoạt động như nhau mà chúng được dành riêng để thực hiện những nhiệm vụ chuyên biệt nhằm hỗ trợ các máy trạm trên mạng, một máy chủ có thể thực hiện toàn bộ các nhiệm vụ này hoặc cũng có thể có một số máy chủ sẽ thực hiện một nhiệm vụ riêng biệt nào đó, ví dụ như: Web server, FTP server, File server, Printer server...

2.2. Active Directory

Mục tiêu:

- Trình bày được cấu trúc của Active Directory trên windows server

2.2.1. Giới thiệu

AD (Active Directory) là dịch vụ thư mục chứa các thông tin về các tài nguyên trên mạng, có thể mở rộng và có khả năng tự điều chỉnh cho phép bạn quản lý tài nguyên mạng hiệu quả. Để có thể làm việc tốt với Active Directory, chúng ta sẽ tìm hiểu khái quát về Active Directory, sau đó khảo sát các thành phần của dịch vụ này.

Các đối tượng AD bao gồm dữ liệu của người dùng (user data), máy in (printers), máy chủ (servers), cơ sở dữ liệu (databases), các nhóm người dùng (groups), các máy tính (computers), và các chính sách bảo mật (security policies).

Ngoài ra một khái niệm mới được sử dụng là *container* (tạm dịch là tập đối tượng). Ví dụ Domain là một tập đối tượng chứa thông tin người dùng, thông tin các máy trên mạng, và chứa các đối tượng khác.

2.2.2 Chức năng của Active Directory

- Lưu giữ một danh sách tập trung các tên tài khoản người dùng, mật khẩu tương ứng và các tài khoản máy tính.
- Cung cấp một **Server** đóng vai trò chứng thực (**authentication server**) hoặc **Server** quản lý đăng nhập (**logon Server**), **Server** này còn gọi là **domain controller** (máy điều khiển vùng).
- Duy trì một bảng hướng dẫn hoặc một bảng chỉ mục (**index**) giúp các máy tính trong mạng có thể dò tìm nhanh một tài nguyên nào đó trên các máy tính khác trong vùng
- Cho phép chúng ta tạo ra những tài khoản người dùng với những mức độ quyền (**rights**) khác nhau như: toàn quyền trên hệ thống mạng, chỉ có quyền **backup** dữ liệu hay **shutdown Server** từ xa...
- Cho phép chúng ta chia nhỏ miền của mình ra thành các miền con (**subdomain**) hay các đơn vị tổ chức **OU (Organizational Unit)**. Sau đó chúng ta có thể ủy quyền cho các quản trị viên bộ phận quản lý từng bộ phận nhỏ.

2.2.3. Directory Services

2.2.3.1. Giới thiệu Directory Services

Directory Services (dịch vụ danh bạ) là hệ thống thông tin chứa trong **NTDS.DIT** và các chương trình quản lý, khai thác tập tin này. Dịch vụ danh bạ là một dịch vụ cơ sở làm nền tảng để hình thành một hệ thống **Active Directory**. Một hệ thống với những tính năng vượt trội của **Microsoft**.

2.2.3.2. Các thành phần trong Directory Services

Đầu tiên, bạn phải biết được những thành phần cấu tạo nên dịch vụ danh bạ là gì? Bạn có thể so sánh dịch vụ danh bạ với một quyển sổ lưu số điện thoại. Cả hai đều chứa danh sách của nhiều đối tượng khác nhau cũng như các thông tin và thuộc tính liên quan đến các đối tượng đó.

- **Object** (đối tượng).
 - + Trong hệ thống cơ sở dữ liệu, đối tượng bao gồm các máy in, người dùng mạng, các server, các máy trạm, các thư mục dùng chung, dịch vụ mạng, ... Đối tượng chính là thành tố căn bản nhất của dịch vụ danh bạ.
- **Attribute** (thuộc tính).
 - + Một thuộc tính mô tả một đối tượng. Ví dụ, mật khẩu và tên là thuộc tính của đối tượng người dùng mạng. Các đối tượng khác nhau có danh sách thuộc tính khác nhau, tuy nhiên, các đối tượng khác nhau cũng có thể có một số thuộc tính giống nhau. Lấy ví dụ như một máy in và một máy trạm cả hai đều có một thuộc tính là địa chỉ **IP**.
- **Schema** (cấu trúc tổ chức).
 - + Một **schema** định nghĩa danh sách các thuộc tính dùng để mô tả một loại đối tượng nào đó. Ví dụ, cho rằng tất cả các đối tượng máy in đều được định nghĩa bằng

các thuộc tính tên, loại **PDL** và tốc độ. Danh sách các đối tượng này hình thành nên **schema** cho lớp đối tượng “máy in”. **Schema** có đặc tính là tùy biến được, nghĩa là các thuộc tính dùng để định nghĩa một lớp đối tượng có thể sửa đổi được. Nói tóm lại **Schema** có thể xem là một danh bạ của cái danh bạ **Active Directory**.

- **Container** (vật chứa).

+ Vật chứa tương tự với khái niệm thư mục trong **Windows**. Một thư mục có thể chứa các tập tin và các thư mục khác. Trong **Active Directory**, một vật chứa có thể chứa các đối tượng và các vật chứa khác. Vật chứa cũng có các thuộc tính như đối tượng mặc dù vật chứa không thể hiện một thực thể thật sự nào đó như đối tượng. Có ba loại vật chứa là:

+ **Domain**: khái niệm này được trình bày chi tiết ở phần sau.

+ **Site**: một **site** là một vị trí. **Site** được dùng để phân biệt giữa các vị trí cục bộ và các vị trí xa xôi. Ví dụ, công ty XYZ có tổng hành dinh đặt ở **San Fransisco**, một chi nhánh đặt ở **Denver** và một văn phòng đại diện đặt ở **Portland** kết nối về tổng hành dinh bằng **Dialup Networking**. Như vậy hệ thống mạng này có ba **site**.

+ **OU (Organizational Unit)**: là một loại vật chứa mà bạn có thể đưa vào đó người dùng, nhóm, máy tính và những **OU** khác. Một **OU** không thể chứa các đối tượng nằm trong domain khác. Nhờ việc một **OU** có thể chứa các **OU** khác, bạn có thể xây dựng một mô hình thứ bậc của các vật chứa để mô hình hoá cấu trúc của một tổ chức bên trong một domain. Bạn nên sử dụng **OU** để giảm thiểu số lượng domain cần phải thiết lập trên hệ thống.

- **Global Catalog**.

+ Dịch vụ **Global Catalog** dùng để xác định vị trí của một đối tượng mà người dùng được cấp quyền truy cập. Việc tìm kiếm được thực hiện xa hơn những gì đã có trong **Windows NT** và không chỉ có thể định vị được đối tượng bằng tên mà có thể bằng cả những thuộc tính của đối tượng.

+ Giả sử bạn phải in một tài liệu dày 50 trang thành 1000 bản, chắc chắn bạn sẽ không dùng một máy in **HP Laserjet 4L**. Bạn sẽ phải tìm một máy in chuyên dụng, in với tốc độ 100ppm và có khả năng đóng tài liệu thành quyển. Nhờ **Global Catalog**, bạn tìm kiếm trên mạng một máy in với các thuộc tính như vậy và tìm thấy được một máy **Xerox Docutech 6135**. Bạn có thể cài đặt **driver** cho máy in đó và gửi **print job** đến máy in. Nhưng nếu bạn ở **Portland** và máy in thì ở **Seattle** thì sao? **Global Catalog** sẽ cung cấp thông tin này và bạn có thể gửi **email** cho chủ nhân của máy in, nhờ họ in giùm.

Một ví dụ khác, giả sử bạn nhận được một thư thoại từ một người tên **Betty Doe** ở bộ phận kế toán. Đoạn thư thoại của cô ta bị cắt xén và bạn không thể biết được số điện thoại của cô ta. Bạn có thể dùng **Global Catalog** để tìm thông tin về cô ta nhờ tên, và nhờ đó bạn có được số điện thoại của cô ta.

Khi một đối tượng được tạo mới trong **Active Directory**, đối tượng được gán một con số phân biệt gọi là **GUID (Global Unique Identifier)**. **GUID** của một đối tượng luôn luôn cố định cho dù bạn có di chuyển đối tượng đi đến khu vực khác.

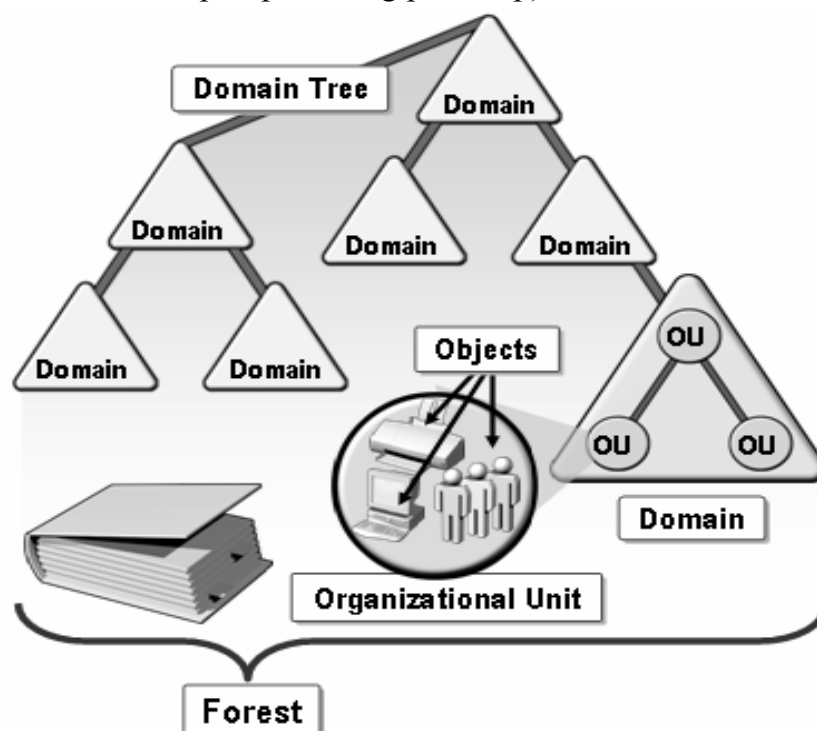
2.2.4. Các thành phần của AD

Mục tiêu:

- Trình bày được các thành phần của Active Directory.

2.2.4.1. Cấu trúc AD logic

Gồm các thành phần: domains (vùng), organization units (đơn vị tổ chức), trees (hệ vùng phân cấp) và forests (tập hợp hệ vùng phân cấp).



Hình 3.4: Cấu trúc AD logic

- **Organizational Units.**

+ **Organizational Unit** hay **OU** là đơn vị nhỏ nhất trong hệ thống **AD**, nó được xem là một vật chứa các đối tượng (**Object**) được dùng để sắp xếp các đối tượng khác nhau phục vụ cho mục đích quản trị của bạn. **OU** cũng được thiết lập dựa trên **subnet IP** và được định nghĩa là “một hoặc nhiều **subnet** kết nối tốt với nhau”. Việc sử dụng **OU** có hai công dụng chính sau:

+ Trao quyền kiểm soát một tập hợp các tài khoản người dùng, máy tính hay các thiết bị mạng cho một nhóm người hay một phụ tá quản trị viên nào đó (sub-administrator), từ đó giảm bớt công tác quản trị cho người quản trị toàn bộ hệ thống.

+ Kiểm soát và khóa bớt một số chức năng trên các máy trạm của người dùng trong **OU** thông qua việc sử dụng các đối tượng chính sách nhóm (**GPO**), các chính sách nhóm này chúng ta sẽ tìm hiểu ở các chương sau.

- **Domain**

+ **Domain** là đơn vị chức năng nòng cốt của cấu trúc **logic Active Directory**. Nó là phương tiện để qui định một tập hợp những người dùng, máy tính, tài nguyên chia sẻ có những qui tắc bảo mật giống nhau từ đó giúp cho việc quản lý các truy cập vào các **Server** dễ dàng hơn. **Domain** đáp ứng ba chức năng chính sau:

+ Đóng vai trò như một khu vực quản trị (**administrative boundary**) các đối tượng, là một tập hợp các định nghĩa quản trị cho các đối tượng chia sẻ như: có

chung một cơ sở dữ liệu thư mục, các chính sách bảo mật, các quan hệ ủy quyền với các **domain** khác.

- + Giúp chúng ta quản lý bảo mật các tài nguyên chia sẻ.

- + Cung cấp các **Server** dự phòng làm chức năng điều khiển vùng (**domain controller**), đồng thời đảm bảo các thông tin trên các **Server** này được đồng bộ với nhau.

- **Domain Tree**

- + **Domain Tree** là cấu trúc bao gồm nhiều **domain** được sắp xếp có cấp bậc theo cấu trúc hình cây. **Domain** tạo ra đầu tiên được gọi là **domain root** và nằm ở gốc của cây thư mục. Tất cả các **domain** tạo ra sau sẽ nằm bên dưới **domain root** và được gọi là **domain con (child domain)**. Tên của các **domain con** phải khác biệt nhau. Khi một **domain root** và ít nhất một **domain con** được tạo ra thì hình thành một cây **domain**. Khái niệm này bạn sẽ thường nghe thấy khi làm việc với một dịch vụ thư mục. Bạn có thể thấy cấu trúc sẽ có hình dáng của một cây khi có nhiều nhánh xuất hiện.

- **Forest**

- + **Forest** (rừng) được xây dựng trên một hoặc nhiều **Domain Tree**, nói cách khác **Forest** là tập hợp các **Domain Tree** có thiết lập quan hệ và ủy quyền cho nhau. Ví dụ giả sử một công ty nào đó, chẳng hạn như **Microsoft**, thu mua một công ty khác. Thông thường, mỗi công ty đều có một hệ thống **Domain Tree** riêng và để tiện quản lý, các cây này sẽ được hợp nhất với nhau bằng một khái niệm là rừng

- + Trong ví dụ trên, công ty mcmse.com thu mua được techtutorials.com và xyzabc.com và hình thành rừng từ gốc mcmse.com

2.2.5 Cấu trúc AD vật lý

Gồm: sites và domain controllers.

- Địa bàn (site): là tập hợp của một hay nhiều mạng con kết nối với nhau, tạo điều kiện truyền thông qua mạng dễ dàng, ấn định ranh giới vật lý xung quanh các tài nguyên mạng.

- Điều khiển vùng (domain controllers): là máy tính chạy Windows Server chứa bản sao dữ liệu vùng. Một vùng có thể có một hay nhiều điều khiển vùng. Mỗi sự thay đổi dữ liệu trên một điều khiển vùng sẽ được tự động cập nhật lên các điều khiển khác của vùng.

2.3. Cài đặt và cấu hình Active Directory

Mục tiêu:

- Cài đặt và cấu hình được máy điều khiển vùng.
- Gia nhập máy trạm vào máy điều khiển vùng (join domain)

2.3.1. Nâng cấp Server thành Domain Controller(DC)

Theo mặc định, tất cả các máy **Windows Server 2003** khi mới cài đặt đều là **Server độc lập (standalone server)**. Chương trình **DCPRMO** chính là **Active Directory Installation Wizard** và được dùng để nâng cấp một máy không phải là **DC (Server Stand-alone)** thành một máy **DC** và ngược lại giáng cấp một máy **DC** thành một **Server** bình thường. Chú ý đối với **Windows Server 2003** thì bạn có thể đổi tên máy tính khi đã nâng cấp thành **DC**.

Trước khi nâng cấp **Server** thành **Domain Controller**, bạn cần khai báo đầy đủ các thông số **TCP/IP**, đặc biệt là phải khai báo **DNS Server** có địa chỉ chính là địa chỉ IP của **Server** cần nâng cấp. Nếu bạn có khả năng cấu hình dịch vụ **DNS** thì bạn nên cài đặt dịch vụ này trước khi nâng cấp **Server**, còn ngược lại thì bạn chọn cài đặt **DNS** tự động trong quá trình nâng cấp. Có hai cách để bạn chạy chương trình **Active Directory Installation Wizard**: bạn dùng tiện ích **Manage Your Server** trong **Administrative Tools** hoặc nhấp chuột vào **Start \ Run**, gõ lệnh **DCPROMO**.

- Các bước cài đặt.

+ Chọn menu **Start \ Run**, nhập **DCPROMO** trong hộp thoại **Run**, và nhấn nút **OK**.

+ Khi đó hộp thoại **Active Directory Installation Wizard** xuất hiện. Bạn nhấn **Next** Chương trình xuất hiện hộp thoại cảnh báo: **DOS, Windows 95** và **WinNT SP3** trở về trước sẽ bị loại ra khỏi miền **Active Directory** dựa trên **Windows Server 2003**. Bạn chọn **Next** để tiếp tục

+ Trong hộp thoại **Domain Controller Type**, chọn mục **Domain Controller for a New Domain** và nhấn chọn **Next**. (Nếu bạn muốn bổ sung máy điều khiển vùng vào một **domain** có sẵn, bạn sẽ chọn **Additional domain controller for an existing domain**.)

Đến đây chương trình cho phép bạn chọn một trong ba lựa chọn sau: chọn **Domain in new forest** nếu bạn muốn tạo **domain** đầu tiên trong một rừng mới, chọn **Child domain in an existing domain tree** nếu bạn muốn tạo ra một **domain** con dựa trên một cây **domain** có sẵn, chọn **Domain tree in an existing forest** nếu bạn muốn tạo ra một cây **domain** mới trong một rừng đã có sẵn.

Hộp thoại **New Domain Name** yêu cầu bạn tên **DNS** đầy đủ của **domain** mà bạn cần xây dựng

Hộp thoại **NetBIOS Domain Name**, yêu cầu bạn cho biết tên **domain** theo chuẩn **NetBIOS** để tương thích với các máy **Windows NT**. Theo mặc định, tên **Domain NetBIOS** giống phần đầu của tên **Full DNS**, bạn có thể đổi sang tên khác hoặc chấp nhận giá trị mặc định. Chọn **Next** để tiếp tục

Hộp thoại **Database and Log Locations** cho phép bạn chỉ định vị trí lưu trữ **database Active Directory** và các tập tin **log**. Bạn có thể chỉ định vị trí khác hoặc chấp nhận giá trị mặc định. Tuy nhiên theo khuyến cáo của các nhà quản trị mạng thì chúng ta nên đặt tập tin chứa thông tin giao dịch (**transaction log**) ở một đĩa cứng vật lý khác với đĩa cứng chứa cơ sở dữ liệu của **Active Directory** nhằm tăng hiệu năng của hệ thống. Bạn chọn **Next** để tiếp tục

Hộp thoại **Shared System Volume** cho phép bạn chỉ định vị trí của thư mục **SYSVOL**. Thư mục này phải nằm trên một **NTFS5 Volume**. Tất cả dữ liệu đặt trong thư mục **Sysvol** này sẽ được tự động sao chép sang các **Domain Controller** khác trong miền. Bạn có thể chấp nhận giá trị mặc định hoặc chỉ định vị trí khác, sau đó chọn **Next** tiếp tục. (Nếu **partition** không sử dụng định dạng **NTFS5**, bạn sẽ thấy một thông báo lỗi yêu cầu phải đổi hệ thống tập tin).

DNS là dịch vụ phân giải tên kết hợp với **Active Directory** để phân giải tên các máy tính trong miền. Do đó để hệ thống **Active Directory** hoạt động được thì trong miền phải có ít nhất một **DNS Server** phân giải miền mà chúng ta cần thiết lập. Theo đúng lý thuyết thì chúng ta phải cài đặt và cấu hình dịch vụ **DNS** hoàn chỉnh trước khi nâng cấp **Server**, nhưng do hiện tại các bạn chưa học về dịch vụ này nên chúng ta chấp nhận cho hệ thống tự động cài đặt dịch vụ này. Chúng ta sẽ tìm hiểu chi tiết dịch vụ **DNS** ở giáo trình “Dịch Vụ Mạng”. Trong hộp thoại xuất hiện bạn chọn lựa chọn thứ hai để hệ thống tự động cài đặt và cấu hình dịch vụ **DNS**.

Trong hộp thoại **Permissions**, bạn chọn giá trị **Permission Compatible with pre-Windows 2000 servers** khi hệ thống có các **Server** phiên bản trước **Windows 2000**, hoặc chọn **Permissions compatible only with Windows 2000 servers or Windows Server 2003** khi hệ thống của bạn chỉ toàn các **Server Windows 2000** và **Windows Server 2003**.

Trong hộp thoại **Directory Services Restore Mode Administrator Password**, bạn sẽ chỉ định mật khẩu dùng trong trường hợp **Server** phải khởi động vào chế độ **Directory Services Restore Mode**. Nhấn chọn **Next** để tiếp tục.

Hộp thoại **Summary** xuất hiện, trình bày tất cả các thông tin bạn đã chọn. Nếu tất cả đều chính xác, bạn nhấn **Next** để bắt đầu thực hiện quá trình cài đặt, nếu có thông tin không chính xác thì bạn chọn **Back** để quay lại các bước trước đó.

Hộp thoại **Configuring Active Directory** cho bạn biết quá trình cài đặt đang thực hiện những gì. Quá trình này sẽ chiếm nhiều thời gian. Chương trình cài đặt cũng yêu cầu bạn cung cấp nguồn cài đặt **Windows Server 2003** để tiến hành sao chép các tập tin nếu tìm không thấy.

Sau khi quá trình cài đặt kết thúc, hộp thoại **Completing the Active Directory Installation Wizard** xuất hiện. Bạn nhấn chọn **Finish** để kết thúc.

Cuối cùng, bạn được yêu cầu phải khởi động lại máy thì các thông tin cài đặt mới bắt đầu có hiệu lực. Bạn nhấn chọn nút **Restart Now** để khởi động lại. Quá trình thăng cấp kết thúc.

2.3.2. Gia nhập máy trạm vào Domain

Một máy trạm gia nhập vào một **domain** thực sự là việc tạo ra một mối quan hệ tin cậy (**trust relationship**) giữa máy trạm đó với các máy **Domain Controller** trong vùng. Sau khi đã thiết lập quan hệ tin cậy thì việc chứng thực người dùng **logon** vào mạng trên máy trạm này sẽ do các máy điều khiển vùng đảm nhiệm. Nhưng chú ý việc gia nhập một máy trạm vào miền phải có sự đồng ý của người quản trị mạng cấp miền và quản trị viên cục bộ trên máy trạm đó. Nói cách khác khi bạn muốn gia nhập một máy trạm vào miền, bạn phải đăng nhập cục bộ vào máy trạm với vai trò là **administrator**, sau đó gia nhập vào miền, hệ thống sẽ yêu cầu bạn xác thực bằng một tài khoản người dùng cấp miền có quyền **Add Workstation to Domain** (bạn có thể dùng trực tiếp tài khoản **administrator** cấp miền).

- Các bước cài đặt

- + Đăng nhập cục bộ vào máy trạm với vai trò người quản trị (có thể dùng trực tiếp tài khoản **administrator**).

+ Nhấp phải chuột trên biểu tượng My Computer, chọn **Properties**, hộp thoại **System Properties** xuất hiện, trong **Tab Computer Name**, bạn nhấp chuột vào nút **Change**. Hộp thoại nhập liệu xuất hiện bạn nhập tên miền của mạng cần gia nhập vào mục **Member of Domain**

+ Máy trạm dựa trên tên miền mà bạn đã khai báo để tìm đến **Domain Controller** gần nhất và xin gia nhập vào mạng, **Server** sẽ yêu cầu bạn xác thực với một tài khoản người dùng cấp miền có quyền quản trị.

Sau khi xác thực chính xác và hệ thống chấp nhận máy trạm này gia nhập vào miền thì hệ thống xuất hiện thông báo thành công và yêu cầu bạn **reboot** máy lại để đăng nhập vào mạng.

Đến đây, bạn thấy hộp thoại **Log on to Windows** mà bạn dùng mỗi ngày có vài điều khác, đó là xuất hiện thêm mục **Log on to**, và cho phép bạn chọn một trong hai phần là: **NETCLASS**, **This Computer**. Bạn chọn mục **NETCLASS** khi bạn muốn đăng nhập vào miền, nhớ rằng lúc này bạn phải dùng tài khoản người dùng cấp miền. Bạn chọn mục **This Computer** khi bạn muốn **logon** cục bộ vào máy trạm nào và nhớ dùng tài khoản cục bộ của máy.

Bài tập

1. Cài đặt và cấu hình Active Directory (AD).
2. Gia nhập máy trạm vào Domain controller.

BÀI 4: QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM

Giới thiệu

Sử dụng được các công cụ tạo và quản trị tài khoản người dùng và nhóm cục bộ, tổ chức và quản lý người dùng cục bộ, ta dùng công cụ **Local Users and Groups**. Với công cụ này bạn có thể tạo, xóa, sửa các tài khoản người dùng, cũng như thay đổi mật mã.

1. Mục tiêu:

- Mô tả được tài khoản người dùng, tài khoản nhóm, các thuộc tính của người dùng;
- Tạo và quản trị được tài khoản người dùng, tài khoản nhóm.
- Thực hiện các thao tác an toàn với máy tính.

2. Nội dung chính:

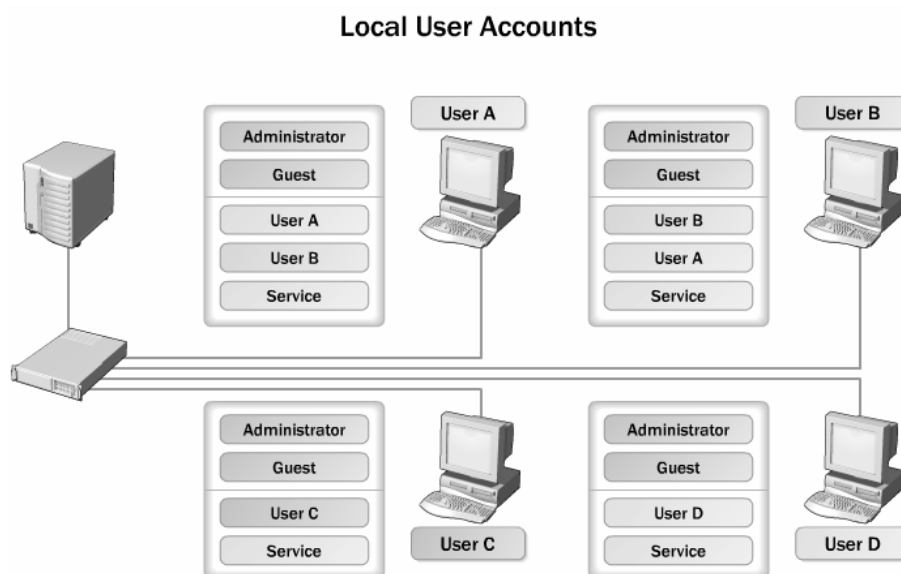
2.1. Định nghĩa tài khoản người dùng và tài khoản nhóm

2.1.1. Tài khoản người dùng

Tài khoản người dùng (**user account**) là một đối tượng quan trọng đại diện cho người dùng trên mạng, chúng được phân biệt với nhau thông qua chuỗi nhận dạng **username**. Chuỗi nhận dạng này giúp hệ thống mạng phân biệt giữa người này và người khác trên mạng từ đó người dùng có thể đăng nhập vào mạng và truy cập các tài nguyên mạng mà mình được phép.

2.1.1.1 Tài khoản người dùng cục bộ

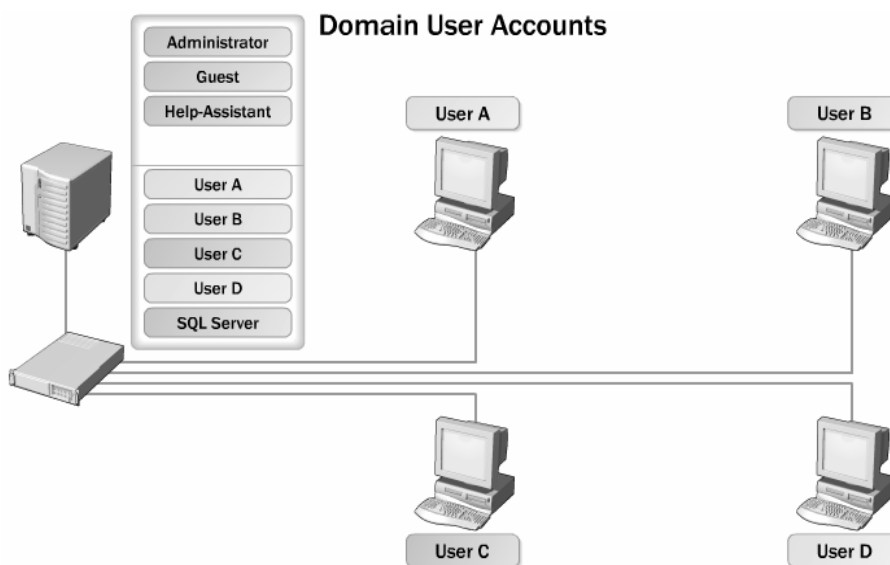
Tài khoản người dùng cục bộ (**local user account**) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép logon, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy domain controller hoặc máy tính chứa tài nguyên chia sẻ. Bạn tạo tài khoản người dùng cục bộ với công cụ Local Users and Group trong Computer Management (COMPMGMT.MSC). Các tài khoản cục bộ tạo ra trên máy stand-alone server, member server hoặc các máy trạm đều được lưu trữ trong tập tin cơ sở dữ liệu SAM (Security Accounts Manager). Tập tin SAM này được đặt trong thư mục `\Windows\system32\config`



Hình 4.1: Tài khoản người dùng cục bộ

2.1.1.2 Tài khoản người dùng miền

Tài khoản người dùng miền (**domain user account**) là tài khoản người dùng được định nghĩa trên **Active Directory** và được phép đăng nhập (**logon**) vào mạng trên bất kỳ máy trạm nào thuộc vùng. Đồng thời với tài khoản này người dùng có thể truy cập đến các tài nguyên trên mạng. Bạn tạo tài khoản người dùng miền với công cụ **Active Directory Users and Computer (DSA.MSC)**. Khác với tài khoản người dùng cục bộ, tài khoản người dùng miền không chứa trong các tập tin cơ sở dữ liệu **SAM** mà chứa trong tập tin **NTDS.DIT**, theo mặc định thì tập tin này chứa trong thư mục **\Windows\NTDS**.



Hình 4.2 Tài khoản người dùng miền

- Yêu cầu về tài khoản người dùng
 - + Mỗi **username** phải từ 1 đến 20 ký tự (trên **Windows Server 2003** thì tên đăng nhập có thể dài đến 104 ký tự, tuy nhiên khi đăng nhập từ các máy cài hệ điều hành **Windows NT 4.0** về trước thì mặc định chỉ hiểu 20 ký tự).
 - + Mỗi **username** là chuỗi duy nhất của mỗi người dùng có nghĩa là tất cả tên của người dùng và nhóm không được trùng nhau.
 - + **Username** không chứa các ký tự sau: “ / \ [] : ; | = , + * ? < >
 - + Trong một **username** có thể chứa các ký tự đặc biệt bao gồm: dấu chấm câu, khoảng trắng, dấu gạch ngang, dấu gạch dưới. Tuy nhiên, nên tránh các khoảng trắng vì những tên như thế phải đặt trong dấu ngoặc khi dùng các kịch bản hay dòng lệnh.

2.1.2. Tài khoản nhóm

Tài khoản nhóm (**group account**) là một đối tượng đại diện cho một nhóm người nào đó, dùng cho việc quản lý chung các đối tượng người dùng. Việc phân bổ các người dùng vào nhóm giúp chúng ta dễ dàng cấp quyền trên các tài nguyên mạng như thư mục chia sẻ, máy in. Chú ý là tài khoản người dùng có thể đăng nhập vào mạng nhưng tài khoản nhóm không được phép đăng nhập mà chỉ dùng để quản lý. Tài khoản nhóm được chia làm hai loại: nhóm bảo mật (**security group**) và nhóm phân phối (**distribution group**)

2.1.2.1. Nhóm bảo mật

Nhóm bảo mật là loại nhóm được dùng để cấp phát các quyền hệ thống (rights) và quyền truy cập (permission). Giống như các tài khoản người dùng, các nhóm bảo mật đều được chỉ định các SID. Có ba loại nhóm bảo mật chính là: local, global và universal. Tuy nhiên nếu chúng ta khảo sát kỹ thì có thể phân thành bốn loại như sau: local, domain local, global và universal.

Local group (nhóm cục bộ) là loại nhóm có trên các máy stand-alone Server, member server, Win2K Pro hay WinXP. Các nhóm cục bộ này chỉ có ý nghĩa và phạm vi hoạt động ngay tại trên máy chứa nó thôi.

Domain local group (nhóm cục bộ miền) là loại nhóm cục bộ đặc biệt vì chúng là local group nhưng nằm trên máy Domain Controller. Các máy Domain Controller có một cơ sở dữ liệu Active Directory chung và được sao chép đồng bộ với nhau do đó một local group trên một Domain Controller này thì cũng sẽ có mặt trên các Domain Controller anh em của nó, như vậy local group này có mặt trên miền nên được gọi với cái tên nhóm cục bộ miền. Các nhóm trong mục Built-in của Active Directory là các domain local.

Global group (nhóm toàn cục hay nhóm toàn mạng) là loại nhóm nằm trong Active Directory và được tạo trên các Domain Controller. Chúng dùng để cấp phát những quyền hệ thống và quyền truy cập vượt qua những ranh giới của một miền. Một nhóm global có thể đặt vào trong một nhóm local của các server thành viên trong miền. Chú ý khi tạo nhiều nhóm global thì có thể làm tăng tải trọng công việc của Global Catalog.

Universal group (nhóm phổ quát) là loại nhóm có chức năng giống như global group nhưng nó dùng để cấp quyền cho các đối tượng trên khắp các miền trong một rừng và giữa các miền có thiết lập quan hệ tin cậy với nhau. Loại nhóm này tiện lợi hơn hai nhóm global group và local group vì chúng dễ dàng lồng các nhóm vào nhau. Nhưng chú ý là loại nhóm này chỉ có thể dùng được khi hệ thống của bạn phải hoạt động ở chế độ Windows 2000 native functional level hoặc Windows Server 2003 functional level có nghĩa là tất cả các máy Domain Controller trong mạng đều phải là Windows Server 2003 hoặc Windows 2000 Server.

2.1.2.2. Nhóm phân phối

Nhóm phân phối là một loại nhóm phi bảo mật, không có SID và không xuất hiện trong các ACL (Access Control List). Loại nhóm này không được dùng bởi các nhà quản trị mà được dùng bởi các phần mềm và dịch vụ. Chúng được dùng để phân phối thư (e-mail) hoặc các tin nhắn (message). Bạn sẽ gặp lại loại nhóm này khi làm việc với phần mềm MS Exchange.

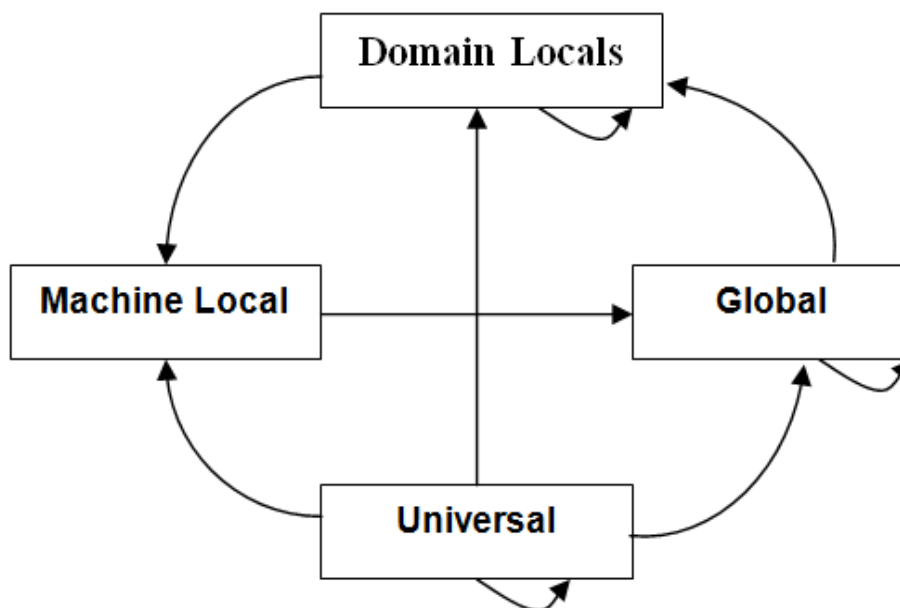
- **Quy tắc gia nhập nhóm**

+ Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong nhóm Machine Local.

+ Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong chính loại nhóm của mình.

+ Nhóm Global và Universal có thể đặt vào trong nhóm Domain local.

+ Nhóm Global có thể đặt vào trong nhóm Universal.



Hình 4.3: Qui tắc gia nhập nhóm

2.2. Chứng thực và kiểm soát truy cập

2.2.1. Các giao thức chứng thực:

- Chứng thực trong Windows Server 2003 là quy trình gồm hai giai đoạn: đăng nhập tương tác và chứng thực mạng.

- Khi người dùng đăng nhập vùng bằng tên và mật mã, quy trình đăng nhập tương tác sẽ phê chuẩn yêu cầu truy cập của người dùng.

- Với tài khoản cục bộ, thông tin đăng nhập được chứng thực cục bộ và người dùng được cấp quyền truy cập máy tính cục bộ.

- Với tài khoản miền, thông tin đăng nhập được chứng thực trên Active Directory và người dùng có quyền truy cập các tài nguyên trên mạng.

- Windows Server 2003 hỗ trợ nhiều giao thức chứng thực mạng, nổi bật nhất là :

Kerberos V5 : Là giao thức chuẩn Internet dùng để chứng thực người dùng và hệ thống.

NT LAN Manager (NTLM) : Là giao thức chứng thực chính của Windows NT.

Secure Socket Layer/Transport Layer Security (SSL/TLS) : Là cơ chế chứng thực chính được dùng khi truy cập vào máy phục vụ Web an toàn.

2.2.2. Số nhận diện bảo mật SID:

- Tuy hệ thống Windows Server 2003 dựa vào tài khoản người dùng (user account) để mô tả các quyền hệ thống (Rights) và quyền truy cập (Permission) nhưng thực sự bên trong hệ thống mỗi tài khoản được đặc trưng bởi một con số nhận dạng bảo mật SID (Security Identifier).

- SID là thành phần nhận dạng không trùng lặp, được hệ thống tạo ra đồng thời với tài khoản và dùng riêng cho hệ thống xử lý, người dùng không quan tâm đến các giá trị này.

- SID bao gồm phần SID vùng cộng thêm với một RID của người dùng không trùng lặp.

- SID có dạng chuẩn “S-1-5-21-D1-D2-D3-RID“, khi đó tất cả các SID trong miền đều có cùng giá trị D1, D2, D3, nhưng giá trị RID là khác nhau.

- Hai mục đích chính của việc hệ thống sử dụng SID là :

Để dàng thay đổi tên tài khoản người dùng mà các quyền hệ thống và quyền truy cập không thay đổi.

Khi xóa một tài khoản thì SID của tài khoản đó không còn giá trị nữa, nếu chúng ta có tạo một tài khoản mới cùng tên với tài khoản vừa xóa thì các quyền cũ cũng không sử dụng được bởi vì khi tạo tài khoản mới thì giá trị SID của tài khoản này là một giá trị mới.

2.3 Các tài khoản tạo sẵn

2.3.1. Tài khoản người dùng tạo sẵn

Tài khoản người dùng tạo sẵn (**Built-in**) là những tài khoản người dùng mà khi ta cài đặt **Windows Server 2003** thì mặc định được tạo ra. Tài khoản này là hệ thống nên chúng ta không có quyền xóa đi nhưng vẫn có quyền đổi tên (chú ý thao tác đổi tên trên những tài khoản hệ thống phức tạp một chút so với việc đổi tên một tài khoản bình thường do nhà quản trị tạo ra). Tất cả các tài khoản người dùng tạo sẵn này đều nằm trong **Container Users** của công cụ **Active Directory User and Computer**. Sau đây là bảng mô tả các tài khoản người dùng được tạo sẵn:

Tên tài khoản	Mô tả
Administrator	Administrator là một tài khoản đặc biệt, có toàn quyền trên máy tính hiện tại. Bạn có thể đặt mật khẩu cho tài khoản này trong lúc cài đặt Windows Server 2003 . Tài khoản này có thể thi hành tất cả các tác vụ như tạo tài khoản người dùng, nhóm, quản lý các tập tin hệ thống và cấu hình máy in...
Guest	Tài khoản Guest cho phép người dùng truy cập vào các máy tính nếu họ không có một tài khoản và mật mã riêng. Mặc định là tài khoản này không được sử dụng, nếu được sử dụng thì thông thường nó bị giới hạn về quyền, ví dụ như là chỉ được truy cập Internet hoặc in ấn.
ILS_Anonymous_User	Là tài khoản đặc biệt được dùng cho dịch vụ ILS . ILS hỗ trợ cho các ứng dụng điện thoại có các đặc tính như: caller ID , video conferencing , conference calling , và faxing . Muốn sử dụng ILS thì dịch vụ IIS phải được cài đặt.
IUSR_computer-name	Là tài khoản đặc biệt được dùng trong các truy cập giấu tên trong dịch vụ IIS trên máy tính có cài IIS .
IWAM_computer-name	Là tài khoản đặc biệt được dùng cho IIS khởi động các tiến trình của các ứng dụng trên máy có cài IIS .
Krbtgt	Là tài khoản đặc biệt được dùng cho dịch vụ trung tâm phân phối khóa (Key Distribution Center)
TSInternetUser	Là tài khoản đặc biệt được dùng cho Terminal Services .

2.3.2. Tài khoản nhóm Domain Local tạo sẵn

Nhưng chúng ta đã thấy trong công cụ **Active Directory User and Computers**, **container Users** chứa nhóm **universal**, nhóm **domain** local và nhóm **global** là do hệ thống đã mặc định quy định trước. Nhưng một số nhóm **domain** local đặc biệt được đặt trong **container Built-in**, các nhóm này không được di chuyển sang các **OU** khác, đồng thời nó cũng được gán một số quyền cố định trước nhằm phục vụ cho công tác quản trị. Bạn cũng chú ý rằng là không có quyền xóa các nhóm đặc biệt này.

Tên nhóm	Mô tả
Administrators	Nhóm này mặc định được ấn định sẵn tất cả các quyền hạn cho nên thành viên của nhóm này có toàn quyền trên hệ thống mạng. Nhóm Domain Admins và Enterprise Admins là thành viên mặc định của nhóm Administrators .
Account Operators	Thành viên của nhóm này có thể thêm, xóa, sửa được các tài khoản người dùng, tài khoản máy và tài khoản nhóm. Tuy nhiên họ không có quyền xóa, sửa các nhóm trong container Built-in và OU .
Domain Controllers	Nhóm này chỉ có trên các Domain Controller và mặc định không có thành viên nào, thành viên của nhóm có thể đăng nhập cục bộ vào các Domain Controller nhưng không có quyền quản trị các chính sách bảo mật.
Backup Operators	Thành viên của nhóm này có quyền lưu trữ dự phòng (Backup) và phục hồi (Retore) hệ thống tập tin. Trong trường hợp hệ thống tập tin là NTFS và họ không được gán quyền trên hệ thống tập tin thì thành viên của nhóm này chỉ có thể truy cập hệ thống tập tin thông qua công cụ Backup . Nếu muốn truy cập trực tiếp thì họ phải được gán quyền.
Guests	Là nhóm bị hạn chế quyền truy cập các tài nguyên trên mạng. Các thành viên nhóm này là người dùng vắng lai không phải là thành viên của mạng. Mặc định các tài khoản Guest bị khóa
Print Operator	Thành viên của nhóm này có quyền tạo ra, quản lý và xóa bỏ các đối tượng máy in dùng chung trong Active Directory.
Server Operators	Thành viên của nhóm này có thể quản trị các máy server trong miền như: cài đặt, quản lý máy in, tạo và quản lý thư mục dùng chung, backup dữ liệu, định dạng đĩa, thay đổi giờ...
Users	Mặc định mọi người dùng được tạo đều thuộc nhóm này, nhóm này có quyền tối thiểu của một người dùng nên việc truy cập rất hạn chế.
Replicator	Nhóm này được dùng để hỗ trợ việc sao chép danh bạ trong Directory Services , nhóm này không có thành viên mặc định.

Tên nhóm	Mô tả
Incoming Forest Trust Builders	Thành viên nhóm này có thể tạo ra các quan hệ tin cậy hướng đến, một chiều vào các rừng. Nhóm này không có thành viên mặc định.
Network Configuration Operators	Thành viên nhóm này có quyền sửa đổi các thông số TCP/IP trên các máy Domain Controller trong miền.
Pre-Windows 2000 Compatible Access	Nhóm này có quyền truy cập đến tất cả các tài khoản người dùng và tài khoản nhóm trong miền, nhằm hỗ trợ cho các hệ thống WinNT cũ.
Remote Desktop User	Thành viên nhóm này có thể đăng nhập từ xa vào các Domain Controller trong miền, nhóm này không có thành viên mặc định.
Performace Log Users	Thành viên nhóm này có quyền truy cập từ xa để ghi nhận lại những giá trị về hiệu năng của các máy Domain Controller , nhóm này cũng không có thành viên mặc định.
Performace Monitor Users	Thành viên nhóm này có khả năng giám sát từ xa các máy Domain Controller .

Ngoài ra còn một số nhóm khác như DHCP Users, DHCP Administrators, DNS Administrators... các nhóm này phục vụ chủ yếu cho các dịch vụ, chúng ta sẽ tìm hiểu cụ thể trong từng dịch vụ ở giáo trình “Dịch Vụ Mạng”. Chú ý theo mặc định hai nhóm Domain Computers và Domain Controllers được dành riêng cho tài khoản máy tính, nhưng bạn vẫn có thể đưa tài khoản người dùng vào hai nhóm này.

2.3.3. Tài khoản nhóm Global tạo sẵn

Tên nhóm	Mô tả
Domain Admins	Thành viên của nhóm này có thể toàn quyền quản trị các máy tính trong miền vì mặc định khi gia nhập vào miền các member server và các máy trạm (Win2K Pro, WinXP) đã đưa nhóm Domain Admins là thành viên của nhóm cục bộ Administrators trên các máy này.
Domain Users	Theo mặc định mọi tài khoản người dùng trên miền đều là thành viên của nhóm này. Mặc định nhóm này là thành viên của nhóm cục bộ Users trên các máy server thành viên và máy trạm.
Group Policy Creator Owners	Thành viên nhóm này có quyền sửa đổi chính sách nhóm của miền, theo mặc định tài khoản administrator miền là thành viên của nhóm này.

Tên nhóm	Mô tả
Enterprise Admins	Đây là một nhóm universal , thành viên của nhóm này có toàn quyền trên tất cả các miền trong rừng đang xét. Nhóm này chỉ xuất hiện trong miền gốc của rừng thôi. Mặc định nhóm này là thành viên của nhóm administrators trên các Domain Controller trong rừng.
Schema Admins	Nhóm universal này cũng chỉ xuất hiện trong miền gốc của rừng, thành viên của nhóm này có thể chỉnh sửa cấu trúc tổ chức (schema) của Active Directory .

2.3.4. Các nhóm tạo sẵn đặc biệt

Ngoài các nhóm tạo sẵn đã trình bày ở trên, hệ thống **Windows Server 2003** còn có một số nhóm tạo sẵn đặt biệt, chúng không xuất hiện trên cửa sổ của công cụ **Active Directory User and Computer**, mà chúng chỉ xuất hiện trên các **ACL** của các tài nguyên và đối tượng. Ý nghĩa của nhóm đặc biệt này là:

- **Interactive**: đại diện cho những người dùng đang sử dụng máy tại chỗ.
- **Network**: đại diện cho tất cả những người dùng nối kết mạng đến một máy tính khác.
- **Everyone**: đại diện cho tất cả mọi người dùng.
- **System**: đại diện cho hệ điều hành.
- **Creator owner**: đại diện cho những người tạo ra, những người sở hữu một tài nguyên nào đó như: thư mục, tập tin, tác vụ in ấn (**print job**)...
- **Authenticated users**: đại diện cho những người dùng đã được hệ thống xác thực, nhóm này được dùng như một giải pháp thay thế an toàn hơn cho nhóm **everyone**.
- **Anonymous logon**: đại diện cho một người dùng đã đăng nhập vào hệ thống một cách nặc danh, chẳng hạn một người sử dụng dịch vụ **FTP**.
- **Service**: đại diện cho một tài khoản mà đã đăng nhập với tư cách như một dịch vụ.
- **Dialup**: đại diện cho những người đang truy cập hệ thống thông qua **Dial-up Networking**.

2.4. Quản lý tài khoản người dùng và nhóm cục bộ

2.4.1. Công cụ quản lý tài khoản người dùng cục bộ

Muốn tổ chức và quản lý người dùng cục bộ, ta dùng công cụ **Local Users and Groups**. Với công cụ này bạn có thể tạo, xóa, sửa các tài khoản người dùng, cũng như thay đổi mật mã. Có hai phương thức truy cập đến công cụ **Local Users and Groups**:

- Dùng như một MMC (Microsoft Management Console) snap-in.
- Dùng thông qua công cụ Computer Management.

Các bước dùng để chèn Local Users and Groups snap-in vào trong MMC:

- + Chọn **Start \ Run**, nhập vào hộp thoại **MMC** và ấn phím **Enter** để mở cửa sổ **MMC**.
- + Chọn **Console \ Add/Remove Snap-in** để mở hộp thoại **Add/Remove Snap-in**

+ Nhấp chuột vào nút Add để mở hộp thoại Add Standalone Snap-in. Chọn Local Users and Groups và nhấp chuột vào nút Add. Hộp thoại Choose Target Machine xuất hiện, ta chọn Local Computer và nhấp chuột vào nút Finish để trở lại hộp thoại Add Standalone Snap-in.

+ Nhấp chuột vào nút Close để trở lại hộp thoại Add/Remove Snap-in.

+ Nhấp chuột vào nút OK, ta sẽ nhìn thấy Local Users and Groups snap-in đã chèn vào MMC như hình sau.

+ Lưu Console bằng cách chọn Console \ Save, sau đó ta nhập đường dẫn và tên file cần lưu trữ. Để tiện lợi cho việc quản trị sau này ta có thể lưu console ngay trên Desktop.

+ Nếu máy tính của bạn không có cấu hình MMC thì cách nhanh nhất để truy cập công cụ Local Users and Groups thông qua công cụ Computer Management. Nhấp phải chuột vào My Computer và chọn Manage từ pop-up menu và mở cửa sổ Computer Management. Trong mục System Tools, ta sẽ nhìn thấy mục Local Users and Groups

+ Cách khác để truy cập đến công cụ Local Users and Groups là vào Start \ Programs\Administrative Tools \ Computer Management

2.4.2. Các thao tác cơ bản trên tài khoản người dùng cục bộ

2.4.2.1. Tạo tài khoản mới

Trong công cụ **Local Users and Groups**, ta nhấp phải chuột vào **Users** và chọn **New User**, hộp thoại **New User** hiển thị bạn nhập các thông tin cần thiết vào, nhưng quan trọng nhất và bắt buộc phải có là mục **Username**.

2.4.2.2. Xóa tài khoản

Bạn nên xóa tài khoản người dùng, nếu bạn chắc rằng tài khoản này không bao giờ cần dùng lại nữa. Muốn xóa tài khoản người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần xóa, nhấp phải chuột và chọn **Delete** hoặc vào thực đơn **Action \ Delete**.

Chú ý: khi chọn **Delete** thì hệ thống xuất hiện hộp thoại hỏi bạn muốn xóa thật sự không vì tránh trường hợp bạn xóa nhầm. Bởi vì khi đã xóa thì tài khoản người dùng này không thể phục hồi được.

2.4.2.3. Khóa tài khoản

Khi một tài khoản không sử dụng trong thời gian dài bạn nên khóa lại vì lý do bảo mật và an toàn hệ thống. Nếu bạn xóa tài khoản này đi thì không thể phục hồi lại được do đó ta chỉ tạm khóa. Trong công cụ **Local Users and Groups**, nhấp đôi chuột vào người dùng cần khóa, hộp thoại **Properties** của tài khoản xuất hiện.

Trong **Tab General**, đánh dấu vào mục **Account is disabled**.

2.4.2.4. Đổi tên tài khoản

Bạn có thể đổi tên bất kỳ một tài khoản người dùng nào, đồng thời bạn cũng có thể điều chỉnh các thông tin của tài khoản người dùng thông qua chức năng này. Chức năng này có ưu điểm là khi bạn thay đổi tên người dùng nhưng **SID** của tài khoản vẫn không thay đổi. Muốn thay đổi tên tài khoản người dùng bạn mở công cụ

Local Users and Groups, chọn tài khoản người dùng cần thay đổi tên, nhấp phải chuột và chọn **Rename**.

2.4.2.5. Thay đổi mật khẩu

Muốn đổi mật mã của người dùng bạn mở công cụ Local Users and Groups, chọn tài khoản người dùng cần thay đổi mật mã, nhấp phải chuột và chọn Reset password.

2.5 Quản lý tài khoản người dùng và nhóm trên Active Directory

2.5.1. Tạo mới tài khoản người dùng

Bạn có thể dùng công cụ Active Directory User and Computers trong Administrative Tools ngay trên máy Domain Controller để tạo các tài khoản người dùng miền. Công cụ này cho phép bạn quản lý tài khoản người dùng từ xa thậm chí trên các máy trạm không phải dùng hệ điều hành Server như WinXP, Win2K Pro. Muốn thế trên các máy trạm này phải cài thêm bộ công cụ Admin Pack. Bộ công cụ này nằm trên Server trong thư mục \Windows\system32\ADMINPAK.MSI. Tạo một tài khoản người dùng trên Active Directory, ta làm các bước sau:

+ Chọn Start\ Programs\ Administrative Tools\ Active Directory Users and Computers.

+ Cửa sổ Active Directory Users and Computers xuất hiện, bạn nhấp phải chuột vào mục Users, chọn New \ User

+ Hộp thoại New Object-User xuất hiện như hình sau, bạn nhập tên mô tả người dùng, tên tài khoản logon vào mạng. Giá trị Full Name sẽ tự động phát sinh khi bạn nhập giá trị First Name và Last Name, nhưng bạn vẫn có thể thay đổi được. Chú ý: giá trị quan trọng nhất và bắt buộc phải có là logon name (username). Chuỗi này là duy nhất cho một tài khoản người dùng theo như định nghĩa trên phần lý thuyết. Trong môi trường Windows 2000 và 2003, Microsoft đưa thêm một khái niệm hậu tố UPN (Universal Principal Name), trong ví dụ này là “@netclass.edu.vn”. Hậu tố UPN này gắn vào sau chuỗi username dùng để tạo thành một tên username đầy đủ dùng để chứng thực ở cấp rừng hoặc chứng thực ở một miền khác có quan hệ tin cậy với miền của người dùng đó, trong ví dụ này thì tên username đầy đủ là tuan@netclass.edu.vn”. Ngoài ra trong hộp thoại này cũng cho phép chúng ta đặt tên username của tài khoản người dùng phục vụ cho hệ thống cũ (pre-Windows 2000). Sau khi việc nhập các thông tin hoàn thành bạn nhấp chuột vào nút Next để tiếp tục.

+ Hộp thoại thứ hai xuất hiện, cho phép bạn nhập vào mật khẩu (password) của tài khoản người dùng và đánh dấu vào các lựa chọn liên quan đến tài khoản như: cho phép đổi mật khẩu, yêu cầu phải đổi mật khẩu lần đăng nhập đầu tiên hay khóa tài khoản. Các lựa chọn này chúng ta sẽ tìm hiểu chi tiết ở phần tiếp theo.

+ Hộp thoại cuối cùng xuất hiện và nó hiển thị các thông tin đã cấu hình cho người dùng. Nếu tất cả các thông tin đã chính xác thì bạn nhấp chuột vào nút Finish để hoàn thành, còn nếu cần chỉnh sửa lại thì nhấp chuột vào nút Back để trở về các hộp thoại trước.

2.5.2. Các thuộc tính của tài khoản người dùng

Muốn quản lý các thuộc tính của các tài khoản người ta dùng công cụ Active Directory Users and Computers (bằng cách chọn Start\ Programs\ Administrative

Tools\ Active Directory Users and Computers), sau đó chọn thư mục Users và nhấp đôi chuột vào tài khoản người dùng cần khảo sát. Hộp thoại Properties xuất hiện, trong hộp thoại này chứa 12 Tab chính, ta sẽ lần lượt khảo sát các Tab này. Ngoài ra bạn có thể gom nhóm (dùng hai phím Shift, Ctrl) và hiệu chỉnh thông tin của nhiều tài khoản người dùng cùng một lúc.

- Các thông tin mở rộng của người dùng

Tab **General** chứa các thông tin chung của người dùng trên mạng mà bạn đã nhập trong lúc tạo người dùng mới. Đồng thời bạn có thể nhập thêm một số thông tin như: số điện thoại, địa chỉ mail và trang địa chỉ trang Web cá nhân...

Tab **Address** cho phép bạn có thể khai báo chi tiết các thông tin liên quan đến địa chỉ của tài khoản người dùng như: địa chỉ đường, thành phố, mã vùng, quốc gia...

Tab **Telephones** cho phép bạn khai báo chi tiết các số điện thoại của tài khoản người dùng

Tab **Organization** cho phép bạn khai báo các thông tin người dùng về: chức năng của công ty, tên phòng ban trực thuộc, tên công ty ...

- Tab Account

Tab **Account** cho phép bạn khai báo lại username, quy định giờ logon vào mạng cho người dùng, quy định máy trạm mà người dùng có thể sử dụng để vào mạng, quy định các chính sách tài khoản cho người dùng, quy định thời điểm hết hạn của tài khoản...

Điều khiển giờ logon vào mạng: bạn nhấp chuột vào nút Logon Hours, hộp thoại Logon Hours xuất hiện. Mặc định tất cả mọi người dùng đều được phép truy cập vào mạng 24 giờ mỗi ngày, trong tất cả 7 ngày của tuần. Khi một người dùng logon vào mạng thì hệ thống sẽ kiểm tra xem thời điểm này có nằm trong khoảng thời gian cho phép truy cập không, nếu không phù hợp thì hệ thống sẽ không cho vào mạng và thông báo lỗi Unable to log you on because of an account restriction. Bạn có thể thay đổi quy định giờ logon bằng cách chọn vùng thời gian cần thay đổi và nhấp chuột vào nút lựa chọn Logon Permitted, nếu ngược lại không cho phép thì nhấp chuột vào nút lựa chọn Logon Denied. Sau đây là hình ví dụ chỉ cho phép người dùng làm việc từ 7h sáng đến 5h chiều, từ thứ 2 đến thứ 6.

Chú ý: mặc định người dùng không bị logoff tự động khi hết giờ đăng nhập nhưng bạn có thể điều chỉnh điều này tại mục Automatically Log Off Users When Logon Hours Expire trong Group Policy phần Computer Configuration\ Windows Settings\Security Settings\ Local Policies\ Security Option. Ngoài ra bạn cũng có cách khác để điều chỉnh thông tin logoff này bằng cách dùng công cụ Domain Security Policy hoặc Local Security Policy tùy theo bối cảnh.

Chọn lựa máy trạm được truy cập vào mạng: bạn nhấp chuột vào nút Log On To, bạn sẽ thấy hộp thoại Logon Workstations xuất hiện. Hộp thoại này cho phép bạn chỉ định người dùng có thể logon từ tất cả các máy tính trong mạng hoặc giới hạn người dùng chỉ được phép logon từ một số máy tính trong mạng. Ví dụ như người quản trị mạng làm việc trong môi trường bảo mật nên tài khoản người dùng này chỉ được chỉ định logon vào mạng từ một số máy tránh tình trạng người dùng giả dạng quản trị để

tấn công mạng. Muốn chỉ định máy tính mà người dùng được phép logon vào mạng, bạn nhập tên máy tính đó vào mục Computer Name và sau đó nhấp chuột vào nút Add

Bảng mô tả chi tiết các tùy chọn liên quan đến tài khoản người dùng:

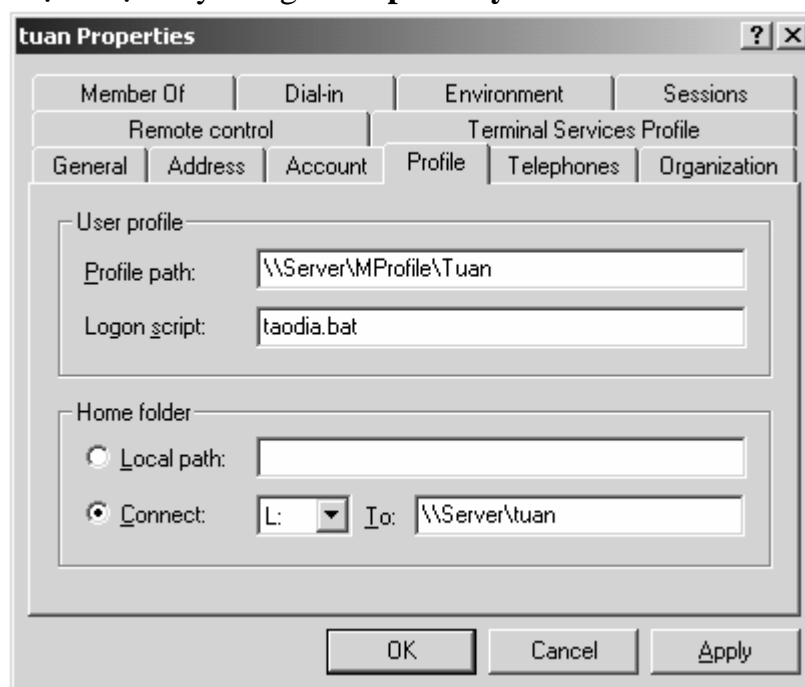
Tùy chọn	Ý nghĩa
User must change password at next logon	Người dùng phải thay đổi mật khẩu lần đăng nhập kế tiếp, sau đó mục này sẽ tự động bỏ chọn.
User cannot change password	Nếu được chọn thì ngăn không cho người dùng tùy ý thay đổi mật khẩu.
Password never expires	Nếu được chọn thì mật khẩu của tài khoản này không bao giờ hết hạn.
Store password using reversible encryption	Chỉ áp dụng tùy chọn này đối với người dùng đăng nhập từ các máy Apple .
Account is disabled	Nếu được chọn thì tài khoản này tạm thời bị khóa, không sử dụng được.
Smart card is required for interactive login	Tùy chọn này được dùng khi người dùng đăng nhập vào mạng thông qua một thẻ thông minh (smart card), lúc đó người dùng không nhập username và password mà chỉ cần nhập vào một số PIN .
Account is trusted for delegation	Chỉ áp dụng cho các tài khoản dịch vụ nào cần giành được quyền truy cập vào tài nguyên với vai trò những tài khoản người dùng khác
Account is sensitive and cannot be delegated	Dùng tùy chọn này trên một tài khoản khách vắng lai hoặc tạm để đảm bảo rằng tài khoản đó sẽ không được đại diện bởi một tài khoản khác.
Use DES encryption types for this account	Nếu được chọn thì hệ thống sẽ hỗ trợ Data Encryption Standard (DES) với nhiều mức độ khác nhau.
Do not require Kerberos preauthentication	Nếu được chọn hệ thống sẽ cho phép tài khoản này dùng một kiểu thực hiện giao thức Kerberos khác với kiểu của Windows Server 2003 .

Mục cuối cùng trong Tab này là quy định thời gian hết hạn của một tài khoản người dùng. Trong mục Account Expires, nếu ta chọn Never thì tài khoản này không bị hết hạn, nếu chọn End of: ngày tháng hết hạn thì đến ngày này tài khoản này bị tạm khóa.

- Tab Profile

Tab Profile cho phép bạn khai báo đường dẫn đến **Profile** của tài khoản người dùng hiện tại, khai báo tập tin **logon script** được tự động thi hành khi người dùng đăng nhập hay khai báo **home folder**. Chú ý các tùy chọn trong **Tab Profile** này chủ yếu phục vụ cho các máy trạm trước **Windows 2000**, còn đối với các máy trạm từ

Win2K trở về sau như: **Win2K Pro, WinXP, Windows Server 2003** thì chúng ta có thể cấu hình các lựa chọn này trong **Group Policy**.



Hình 4.4: Tab Profile

Trước tiên chúng ta hãy tìm hiểu khái niệm **Profile**. **User Profiles** là một thư mục chứa các thông tin về môi trường của **Windows Server 2003** cho từng người dùng mạng. **Profile** chứa các qui định về màn hình **Desktop**, nội dung của menu **Start**, kiểu cách phối màu sắc, vị trí sắp xếp các **icon**, biểu tượng chuột...

Mặc định khi người dùng đăng nhập vào mạng, một **profile** sẽ được mở cho người dùng đó. Nếu là lần đăng nhập lần đầu tiên thì họ sẽ nhận được một **profile** chuẩn. Một thư mục có tên giống như tên của người dùng đăng nhập sẽ được tạo trong thư mục **Documents and Settings**. Thư mục **profile** người dùng được tạo chứa một tập tin **ntuser.dat**, tập tin này được xem như là một thư mục con chứa các liên kết thư mục đến các biểu tượng nền của người dùng. Trong **Windows Server 2003** có ba loại **Profile**:

- + **Local Profile**: là **profile** của người dùng được lưu trên máy cục bộ và họ tự cấu hình trên **profile** đó.

- + **Roaming Profile**: là loại **Profile** được chứa trên mạng và người quản trị mạng thêm thông tin đường dẫn **user profile** vào trong thông tin tài khoản người dùng, để tự động duy trì một bản sao của tài khoản người dùng trên mạng.

- + **Mandatory Profile**: người quản trị mạng thêm thông tin đường dẫn **user profile** vào trong thông tin tài khoản người dùng, sau đó chép một **profile** đã cấu hình sẵn vào đường dẫn đó. Lúc đó các người dùng dùng chung **profile** này và không được quyền thay đổi **profile** đó.

Kịch bản đăng nhập (**logon script** hay **login script**) là những tập tin chương trình được thi hành mỗi khi người dùng đăng nhập vào hệ thống, với chức năng là cấu hình môi trường làm việc của người dùng và phân phát cho họ những tài nguyên mạng như ổ đĩa, máy in (được ánh xạ từ **Server**). Bạn có thể dùng nhiều ngôn ngữ

kịch bản để tạo ra **logon script** như: lệnh **shell** của **DOS/NT/Windows, Windows Scripting Host (WSH), VBScript, Jscript...**

Đối với **Windows Server 2003** thì có hai cách để khai báo **logon script** là: khai báo trong thuộc tính của tài khoản người dùng thông qua công cụ **Active Directory User and Computers**, khai báo thông qua **Group Policy**. Nhưng chú ý trong cả hai cách, các tập tin **script** và mọi tập tin cần thiết khác phải được đặt trong thư mục chia sẻ **SYSVOL**, nằm trong **\Windows\SYSVOL\sysvol**, nếu các tập tin script này phục vụ cho các máy tiền **Win2K** thì phải đặt trong thư mục **\Windows\Sysvol\sysvol\domainname\scripts**. Để các tập tin **script** thi hành được bạn nhớ cấp quyền cho các người dùng mạng có quyền **Read** và **Excute** trên các tập tin này.

Thư mục cá nhân (**home folder hay home directory**) là thư mục dành riêng cho mỗi tài khoản người dùng, giúp người dùng có thể lưu trữ các tài liệu và tập tin riêng, đồng thời đây cũng là thư mục mặc định tại dấu nhắc lệnh. Muốn tạo một thư mục nhân cho người dùng thì trong mục **Connect** bạn chọn ổ đĩa hiển thị trên máy trạm và đường dẫn mà đĩa này cần ánh xạ đến (chú ý là các thư mục dùng chung đảm bảo đã chia sẻ). Trong ví dụ này bạn chỉ thư mục cá nhân cho tài khoản Tuan là “\\server\tuan”, nhưng bạn có thể thay thế tên tài khoản bằng biến môi trường người dùng như: “\\server\%username%”.

- **Tab Member Of**

Tab Member Of cho phép bạn xem và cấu hình tài khoản người dùng hiện tại là thành viên của những nhóm nào. Một tài khoản người dùng có thể là thành viên của nhiều nhóm khác nhau và nó được thừa hưởng quyền của tất cả các nhóm này. Muốn gia nhập vào nhóm nào bạn nhấp chuột vào nút **Add**, hộp thoại chọn nhóm sẽ hiện ra.

Trong hộp thoại chọn nhóm, nếu bạn nhớ tên nhóm thì có thể nhập trực tiếp tên nhóm vào và sau đó nhấp chuột vào nút **Check Names** để kiểm tra có chính xác không, bạn có thể nhập gần đúng để hệ thống tìm các tên nhóm có liên quan. Đây là tính năng mới của **Windows Server 2003** tránh tình trạng tìm kiếm và hiển thị hết tất cả các nhóm hiện có trong hệ thống. Nếu bạn không nhớ tên nhóm thì chấp nhận nhấp chuột vào nút **Advanced** và **Find Now** để tìm hết tất cả các nhóm

Nếu bạn muốn tài khoản người dùng hiện tại thoát ra khỏi một nhóm nào đó thì bạn chọn nhóm sau đó nhấp chuột vào nút **Remove**.

- **Tab Dial-in**

Tab **Dial-in** cho phép bạn cấu hình quyền truy cập từ xa của người dùng cho kết nối **dial-in** hoặc **VPN**, chúng ta sẽ khảo sát chi tiết ở chương **Routing and Remote Access 2.5.3. Tạo mới tài khoản nhóm**

Bạn tạo và quản lý tài khoản nhóm trên Active Directory thông qua công cụ Active Directory Users and Computers. Trước khi tạo nhóm bạn phải xác định loại nhóm cần tạo, phạm vi hoạt động của nhóm như thế nào. Sau khi chuẩn bị đầy đủ các thông tin bạn thực hiện các bước sau:

Chọn Start \ Programs \ Administrative Tools \ Active Directory Users and Computers để mở công cụ Active Directory Users and Computers lên. Nhấp phải chuột vào mục Users, chọn New trên pop-up menu và chọn Group.

Hộp thoại New Object – Group xuất hiện, bạn nhập tên nhóm vào mục Group name, trường tên nhóm cho các hệ điều hành trước Windows 2000 (pre-Windows 2000) tự động phát sinh, bạn có thể hiệu chỉnh lại cho phù hợp.

2.5.4. Các tiện ích dòng lệnh quản lý tài khoản người dùng và tài khoản nhóm

Windows Server 2003 cung cấp nhiều công cụ dòng lệnh mạnh mẽ, có thể được dùng trong các tập tin xử lý theo lô (**batch**) hoặc các tập tin kịch bản (**script**) để quản lý tài khoản người dùng như thêm, xóa, sửa. **Windows 2003** còn hỗ trợ việc nhập và xuất các đối tượng từ **Active Directory**. Hai tiện ích **dsadd.exe** và **admod.exe** với đối số **user** cho phép chúng ta thêm và chỉnh sửa tài khoản người dùng trong **Active Directory**. Tiện ích **csvde.exe** được dùng để nhập hoặc xuất dữ liệu đối tượng thông qua các tập tin kiểu **CSV (comma-separated values)**. Đồng thời hệ thống mới này vẫn còn sử dụng hai lệnh **net user** và **net group** của **Windows 2000**.

Lệnh net user

- Chức năng: tạo thêm, hiệu chỉnh và hiển thị thông tin của các tài khoản người dùng.

- Cú pháp:

```
net user [username [password | *] [options]] [/domain]
net user username {password | *} /add [options] [/domain]
net user username [/delete] [/domain]
```

- Ý nghĩa các tham số:

+ Không tham số: dùng để hiển thị danh sách của tất cả các tài khoản người dùng trên máy tính

+ [**Username**]: chỉ ra tên tài khoản người dùng cần thêm, xóa, hiệu chỉnh hoặc hiển thị. Tên của tài khoản người dùng có thể dài đến 20 ký tự.

+ [**Password**]: ấn định hoặc thay đổi mật mã của tài khoản người dùng. Một mật mã phải có chiều dài tối thiểu bằng với chiều dài quy định trong chính sách tài khoản người dùng. Trong **Windows 2000** thì chiều dài của mật mã có thể dài đến 127 ký tự, nhưng trên hệ thống **Win9X** thì chỉ hiểu được 14 ký tự, do đó nếu bạn đặt mật mã dài hơn 14 ký tự thì có thể tài khoản này không thể **logon** vào mạng từ máy trạm dùng **Win9X**.

+ [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.

+ [**/add**]: thêm một tài khoản người dùng vào trong cơ sở dữ liệu tài khoản người dùng.

+ [**/delete**]: xóa một tài khoản người dùng khỏi cơ sở dữ liệu tài khoản người dùng.

+ [/active:{no | yes}]: cho phép hoặc tạm khóa tài khoản người dùng. Nếu tài khoản bị khóa thì người dùng không thể truy cập các tài nguyên trên máy tính. Mặc định là cho phép (active).

+ [/comment:"text"]: cung cấp mô tả về tài khoản người dùng, mô tả này có thể dài đến 48 ký tự.

+ [/countrycode:nnn]: chỉ định mã quốc gia và mã vùng.

+ [/expires:{date | never}]: quy định ngày hết hiệu lực của tài khoản người dùng.

+ [/fullname:"name"]: khai báo tên đầy đủ của người dùng.

+ [/homedir:path]: khai báo đường dẫn thư mục cá nhân của tài khoản, chú ý đường dẫn này đã tồn tại.

+ [/passwordchg:{yes | no}]: chỉ định người dùng có thể thay đổi mật mã của mình không, mặc định là có thể.

+ [/passwordreq:{yes | no}]: chỉ định một tài khoản người dùng phải có một mật mã, mặc định là có mật mã.

+ [/profilepath:[path]]: khai báo đường dẫn **Profile** của người dùng, nếu không hệ thống sẽ tự tạo một profile chuẩn cho người dùng lần **logon** đầu tiên.

+ [/scriptpath:path]: khai báo đường dẫn và tập tin **logon script**. Đường dẫn này có thể là đường dẫn tuyệt đối hoặc đường dẫn tương đối (ví dụ: %systemroot%\System32\Repl\Import\Scripts).

+ [/times:{times | all}]: quy định giờ cho phép người dùng logon vào mạng hay máy tính cục bộ. Các thứ trong tuần được đại diện bởi ký tự : M, T, W, Th, F, Sa, Su. Giờ ta dùng AM, PM để phân biệt buổi sáng hoặc chiều. Ví dụ sau chỉ cho phép người dùng làm việc trong giờ hành chính từ thứ 2 đến thứ 6: "M,7AM-5PM; T,7AM-5PM; W,7AM-5PM; Th,7AM-5PM; F,7AM-5PM;"

+ [/workstations:{computername[,...] | *}]: chỉ định các máy tính mà người dùng này có thể sử dụng để logon vào mạng. Nếu **/workstations** không có danh sách hoặc danh sách là ký tự "*" thì người dùng có thể sử dụng bất kỳ máy nào để vào mạng.

Lệnh net group

- Chức năng: tạo mới thêm, hiển thị hoặc hiệu chỉnh nhóm toàn cục trên **Windows 2000 Server**

- Cú pháp:

```
net group [groupname [/comment:"text"]] [/domain]
```

```
net group groupname {/add [/comment:"text"] | /delete} [/domain]
```

```
net group groupname username[ ...] {/add | /delete} [/domain]
```

- Ý nghĩa các tham số:

+ Không tham số: dùng để hiển thị tên của Server và tên của các nhóm trên Server đó.

+ [**Groupname**]: chỉ định tên nhóm cần thêm, mở rộng hoặc xóa.

+ [/comment:"text"]: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn, nội dung này có thể dài đến 48 ký tự.

+ [/domain]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.

+ [username[...]]: danh sách một hoặc nhiều người dùng cần thêm hoặc xóa ra khỏi nhóm, các tên này cách nhau bởi khoảng trắng.

+ [/add]: thêm một nhóm hoặc thêm một người dùng vào nhóm.

+ [/delete]: xóa một nhóm hoặc xóa một người dùng khỏi nhóm.

2.5.5. Các lệnh hỗ trợ dịch vụ Active Directory trong môi trường Windows Server 2003

Trên hệ thống **Windows Server 2003**, **Microsoft** phát triển thêm một số lệnh nhằm hỗ trợ tốt hơn cho dịch vụ **Directory** như: **dsadd**, **dsrcm**, **dsmove**, **dsget**, **dsmod**, **dsquery**. Các lệnh này thao tác chủ yếu trên các đối tượng **computer**, **contact**, **group**, **ou**, **user**, **quota**.

- **Dsadd**: cho phép bạn thêm một **computer**, **contact**, **group**, **ou** hoặc **user** vào trong dịch vụ **Directory**.

- **Dsrcm**: xóa một đối tượng trong dịch vụ **Directory**.

- **Dsmove**: di chuyển một đối tượng từ vị trí này đến vị trí khác trong dịch vụ **Directory**.

- **Dsget**: hiển thị các thông tin lựa chọn của một đối tượng **computer**, **contact**, **group**, **ou**, **server** hoặc **user** trong một dịch vụ **Directory**.

- **Dsmod**: chỉnh sửa các thông tin của **computer**, **contact**, **group**, **ou** hoặc **user** trong một dịch vụ **Directory**.

- **Dsquery**: truy vấn các thành phần trong dịch vụ **Directory**.

Ví dụ:

- Tạo một **user** mới: dsadd user "CN=HV10, CN=Users, DC=netclass, DC=edu, DC=vn" -samid hv10 -pwd 123

- Xóa một **user**: dsrcm "CN=HV10, CN=Users, DC=netclass, DC=edu, DC=vn"

- Xem các **user** trong hệ thống: dsquery user

- Gia nhập **user** mới vào nhóm: dsmod group "CN=hs, CN=Users, DC=netclass, DC=edu, DC=vn" -addmbr "CN=HV10, CN=Users, DC=netclass, DC=edu, DC=vn"

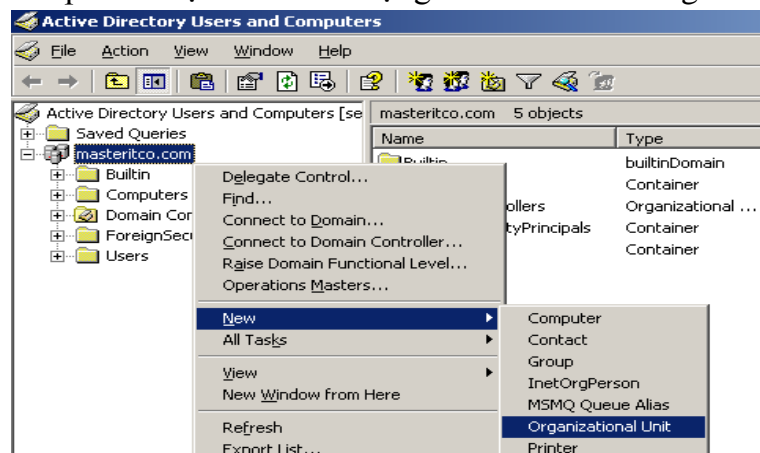
Bài tập

1. Trên máy Domain Controller tạo OU có tên HCM.
2. Trong OU HCM tạo 2 nhóm có tên là Ke Toan và Nhan Su.
3. Trong mỗi nhóm tạo 3 user.
4. Tìm kiếm, di chuyển và khóa một vài tài khoản người dùng bất kỳ.
5. Chỉ cho phép các user logon vào mạng từ 7:00am-6:00pm.
6. Tạo Home Folder cho các user.
7. Cho phép user chỉ lưu trữ 500MB trên Home Folder.
8. Thực hiện Account Lock-Out(cho phép user nhập sai 2 lần)
9. Cài đặt Adminpak.msi xuống máy client.

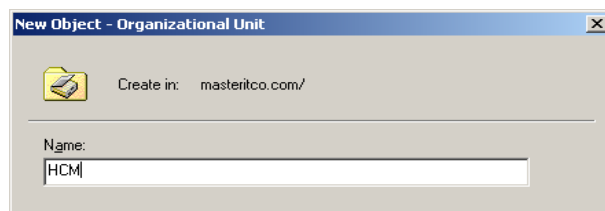
Hướng dẫn thực hiện:

1. Tạo OU có tên HCM:

☞ Tại server: Start / Programs / Administrative Tools / Active Directory Users and Computers/ click nút phải chuột trên biểu tượng server / New / Organizational Unit

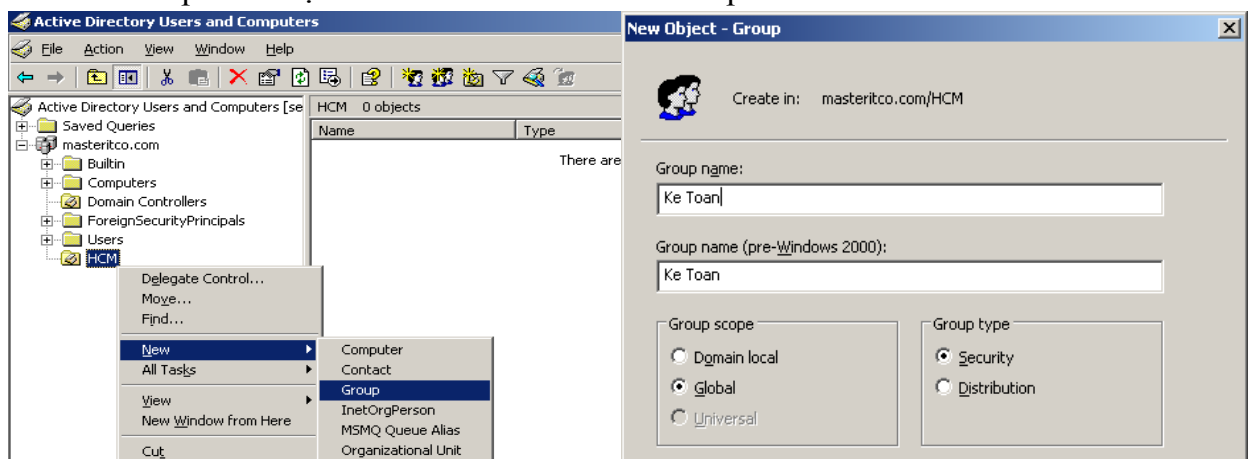


☞ Đặt tên cho OU



2. Trong OU HCM tạo 2 nhóm có tên là Ke Toan và Nhan Su:

☞ Click nút phải chuột trên OU HCM / New / Group



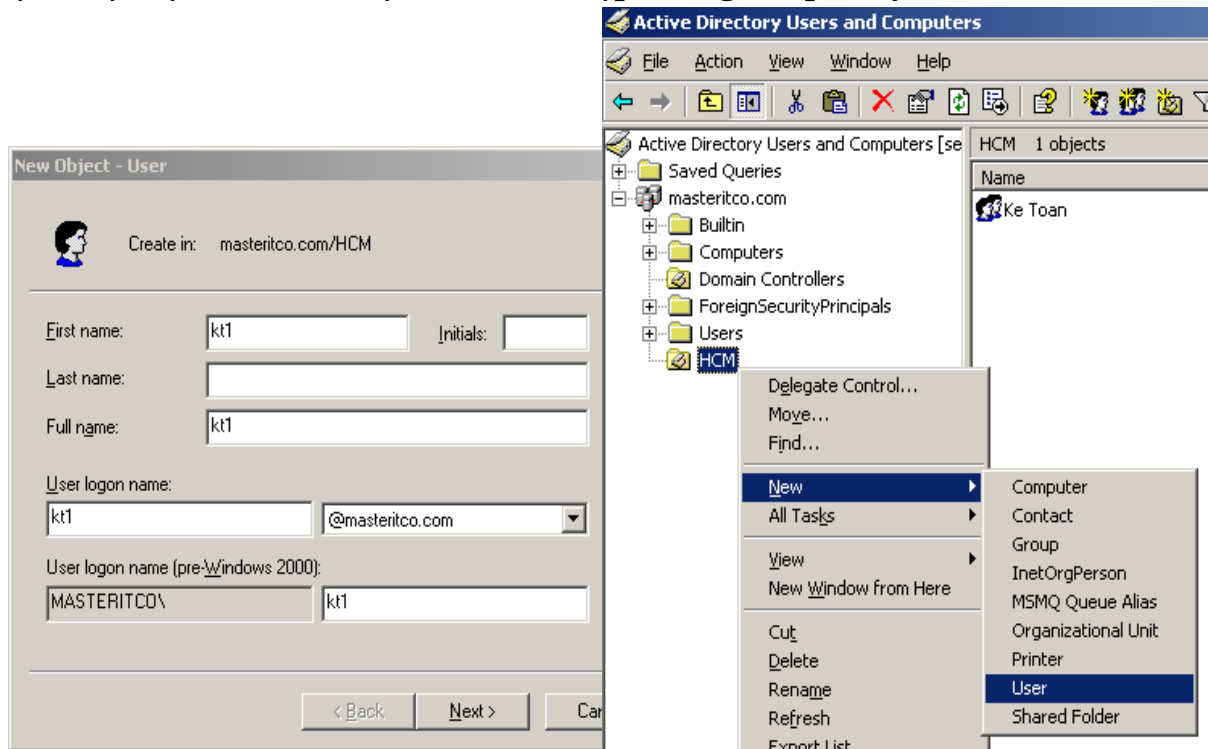
Group Name: Ke Toan /Group scope: Global /Group type: Security

☞ Tương tự tạo Group “Nhan Su”

3. Trong mỗi nhóm tạo 3 user:

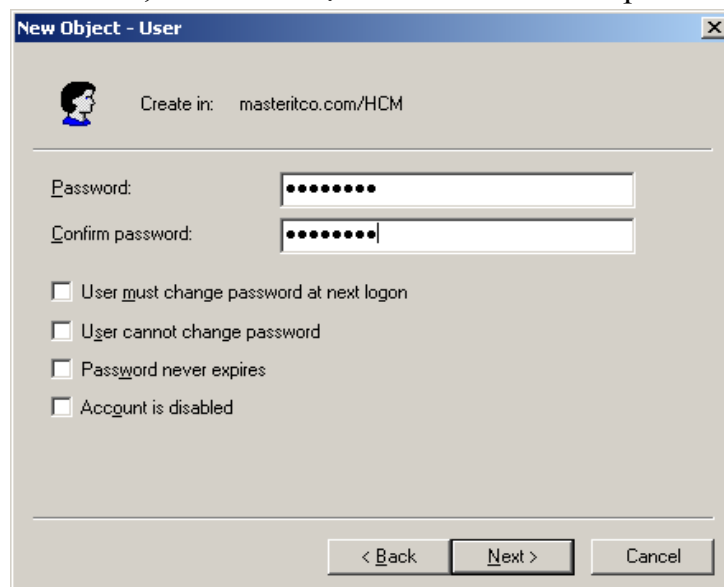
a). Tạo Users

(Chú ý: Sau khi tạo xong các User hãy nhập các thông tin về các User đó như: Số điện thoại, địa chỉ, email, địa chỉ Web, nhập tên người quản lý....)



☞ Click nút phải chuột trên OU HCM / New / User / điền thông tin cho user kt1

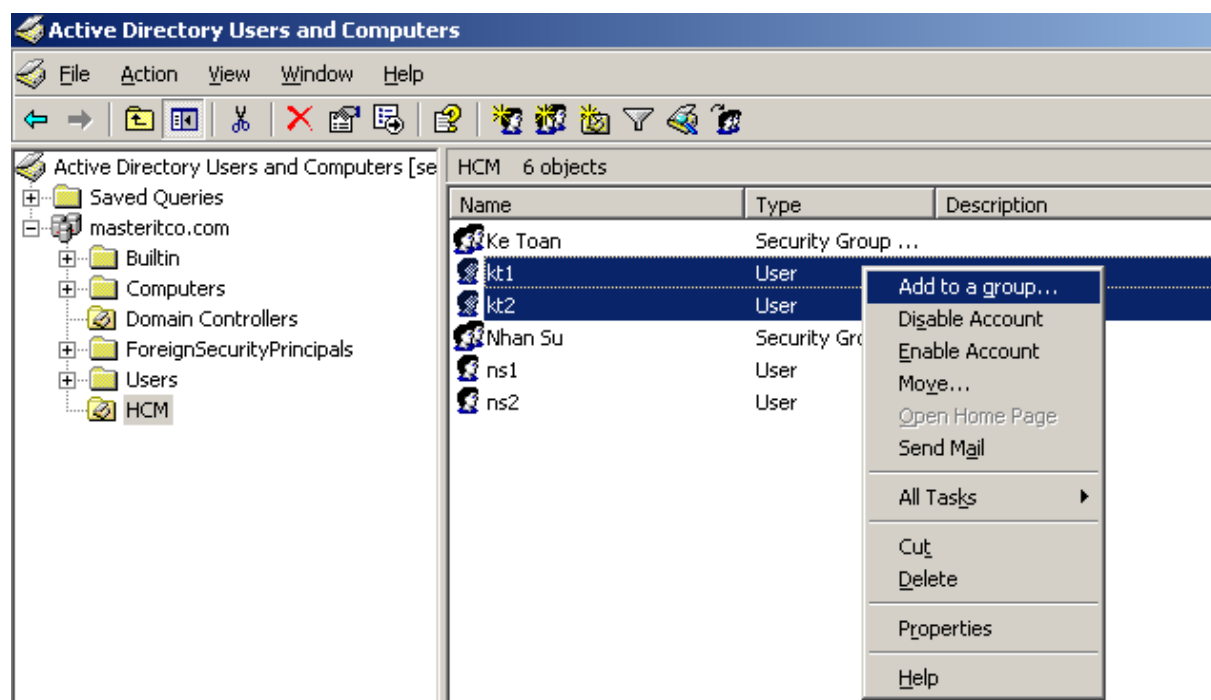
☞ Đặt password cho user, đánh dấu mục Password never expires



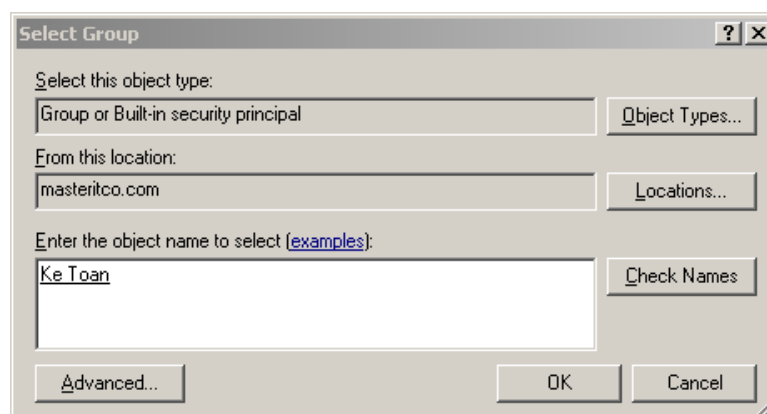
☞ Lặp lại tương tự cho các user KT2, KT3, NS1, NS2, NS3

b). Thiết lập Users thuộc Group:

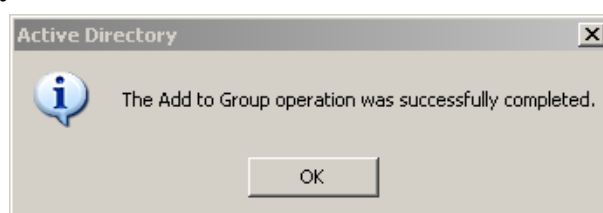
☞ Chọn 3 user KT1, KT2 và KT3 / click nút phải chuột trên 3 user / Add to a group



☛ Gõ tên nhóm “Ke Toan” / Check Names / xuất hiện gạch chân trên group “Ke Toan”



☛ Thông báo kết quả



☛ Làm tương tự với các user NS1, NS2 và NS3 để đưa vào nhóm “Nhan Su”

Bài 5: QUẢN LÝ ĐĨA

Giới thiệu:

Trong bài này giới thiệu cho học sinh phân biệt được các loại định dạng đĩa cứng; Công nghệ lưu trữ mới Dynamic storage; Mô tả được kỹ thuật nén và mã hoá dữ liệu

1. Mục tiêu:

- Phân biệt được các loại định dạng đĩa cứng;
- Công nghệ lưu trữ mới Dynamic storage;
- Mô tả được kỹ thuật nén và mã hoá dữ liệu.
- Thực hiện các thao tác an toàn với máy tính.

2. Nội dung chính:

2.1 Cấu hình hệ thống tập tin

Hệ thống tập tin quản lý việc lưu trữ và định vị các tập tin trên đĩa cứng. **Windows Server 2003** hỗ trợ ba hệ thống tập tin khác nhau: **FAT16**, **FAT32** và **NTFS**. Nếu bạn định sử dụng các tính năng như bảo mật cục bộ, nén và mã hoá các tập tin thì bạn nên dùng **NTFS**. Bảng sau trình bày khả năng của từng hệ thống tập tin trên **Windows Server 2003**:

Khả năng	FAT16	FAT32	NTFS
Hệ điều hành hỗ trợ	Hầu hết các hệ điều hành	Windows 95/98/2000/XP/2003/ Vista/ 7/ 2008	Windows 2000,2000/XP/2003/ Vista/7/2008
Hỗ trợ tên tập tin dài	256 ký tự trên Windows	256 ký tự	256 ký tự
Sử dụng hiệu quả đĩa	Không	Có	Có
Hỗ trợ nén đĩa	Không	Không	Có
Hỗ trợ hạn ngạch	Không	Không	Có
Hỗ trợ mã hoá	Không	Không	Có
Hỗ trợ bảo mật cục bộ	Không	Không	Có
Hỗ trợ bảo mật trên mạng	Có	Có	Có
Kích thước Volume tối đa được hỗ trợ	4GB	32GB	1024GB

Trên **Windows Server 2003/Windows 2000/NT**, bạn có thể sử dụng lệnh **CONVERT** để chuyển đổi hệ thống tập tin từ **FAT16**, **FAT32** thành **NTFS**. Cú pháp của lệnh như sau:

```
CONVERT [ổ đĩa:] /fs:ntfs
```

2.2 Cấu hình đĩa lưu trữ

2.2.1. Basic storage

Bao gồm các partition primary và extended. Partition tạo ra đầu tiên trên đĩa được gọi là partition primary và toàn bộ không gian cấp cho partition được sử dụng trọn vẹn. Mỗi ổ đĩa vật lý có tối đa bốn partition. Bạn có thể tạo ba partition primary và một partition extended. Với partition extended, bạn có thể tạo ra nhiều partition logical.

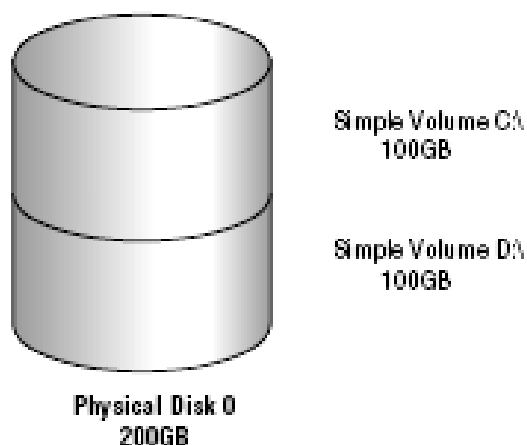
2.2.2. Dynamic storage

Đây là một tính năng mới của Windows Server 2003. Đĩa lưu trữ dynamic chia thành các volume dynamic. Volume dynamic không chứa partition hoặc ổ đĩa logic, và chỉ có thể truy cập bằng Windows Server 2003 và Windows 2000. Windows Server 2003/ Windows 2000 hỗ trợ năm loại volume dynamic: simple, spanned, striped, mirrored và RAID-5. Ưu điểm của công nghệ Dynamic storage so với công nghệ Basic storage:

- Cho phép ghép nhiều ổ đĩa vật lý để tạo thành các ổ đĩa logic (Volume).
- Cho phép ghép nhiều vùng trống không liên tục trên nhiều đĩa cứng vật lý để tạo ổ đĩa logic.
- Có thể tạo ra các ổ đĩa logic có khả năng dung lỗi cao và tăng tốc độ truy xuất...

2.2.2.1 Volume simple.

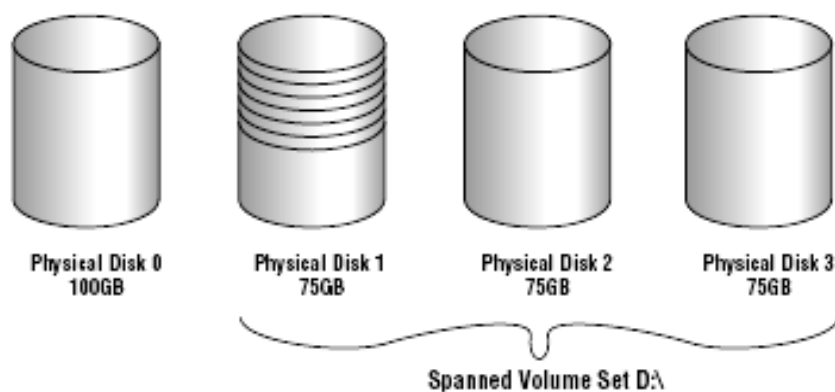
Chứa không gian lấy từ một đĩa **dynamic** duy nhất. Không gian đĩa này có thể liên tục hoặc không liên tục. Hình sau minh họa một đĩa vật lý được chia thành hai **volume** đơn giản.



Hình 5.1 Volume simple.

2.2.2.2 Volume spanned.

Bao gồm một hoặc nhiều đĩa **dynamic** (tối đa là 32 đĩa). Sử dụng khi bạn muốn tăng kích cỡ của **volume**. Dữ liệu ghi lên **volume** theo thứ tự, hết đĩa này đến đĩa khác. Thông thường người quản trị sử dụng **volume spanned** khi ổ đĩa đang sử dụng trong **volume** sắp bị đầy và muốn tăng kích thước của **volume** bằng cách bổ sung thêm một đĩa khác.

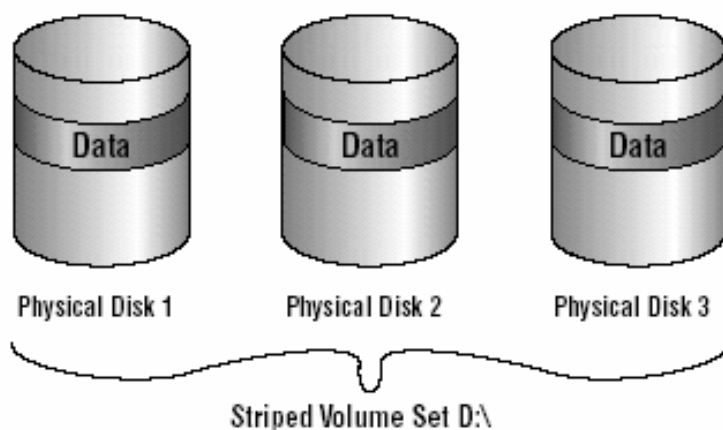


Hình 5.1 Volume Spanned.

Do dữ liệu được ghi tuần tự nên **volume** loại này không tăng hiệu năng sử dụng. Nhược điểm chính của **volume spanned** là nếu một đĩa bị hỏng thì toàn bộ dữ liệu trên **volume** không thể truy xuất được.

2.2.2.3 Volume striped

Lưu trữ dữ liệu lên các dãy (**strip**) bằng nhau trên một hoặc nhiều đĩa vật lý (tối đa là 32). Do dữ liệu được ghi tuần tự lên từng dãy, nên bạn có thể thi hành nhiều tác vụ **I/O** đồng thời, làm tăng tốc độ truy xuất dữ liệu. Thông thường, người quản trị mạng sử dụng **volume striped** để kết hợp dung lượng của nhiều ổ đĩa vật lý thành một đĩa **logic** đồng thời tăng tốc độ truy xuất.

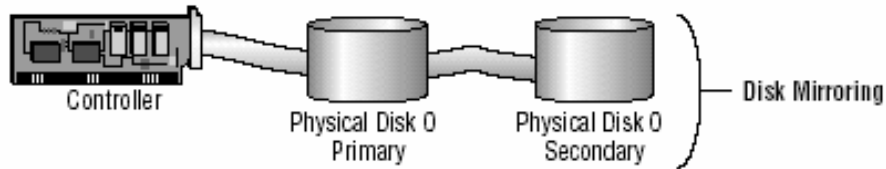


Hình 5.3: volume striped

Nhược điểm chính của **volume striped** là nếu một ổ đĩa bị hỏng thì dữ liệu trên toàn bộ **volume** mất giá trị.

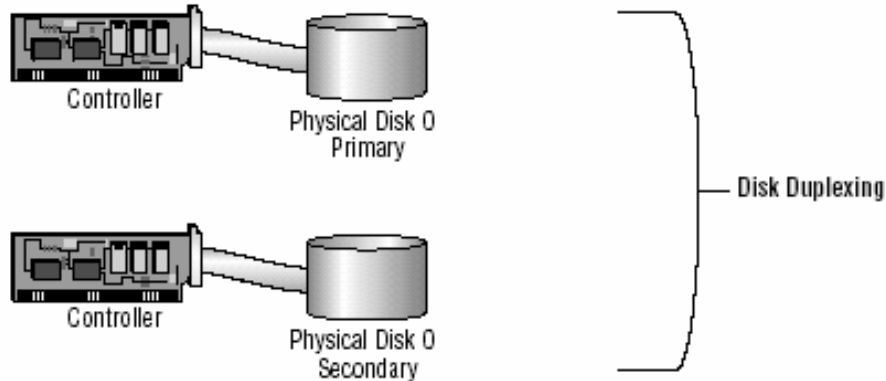
2.2.2.4 Volume mirrored.

Là hai bản sao của một **volume** đơn giản. Bạn dùng một ổ đĩa chính và một ổ đĩa phụ. Dữ liệu khi ghi lên đĩa chính đồng thời cũng sẽ được ghi lên đĩa phụ. **Volume** dạng này cung cấp khả năng dung lỗi tốt. Nếu một đĩa bị hỏng thì ổ đĩa kia vẫn làm việc và không làm gián đoạn quá trình truy xuất dữ liệu. Nhược điểm của phương pháp này là bộ điều khiển đĩa phải ghi lần lượt lên hai đĩa, làm giảm hiệu năng.



Hình 5.4: Volume mirrored

Để tăng tốc độ ghi đồng thời cũng tăng khả năng dung lỗi, bạn có thể sử dụng một biến thể của **volume mirrored** là **duplexing**. Theo cách này bạn phải sử dụng một bộ điều khiển đĩa khác cho ổ đĩa thứ hai.

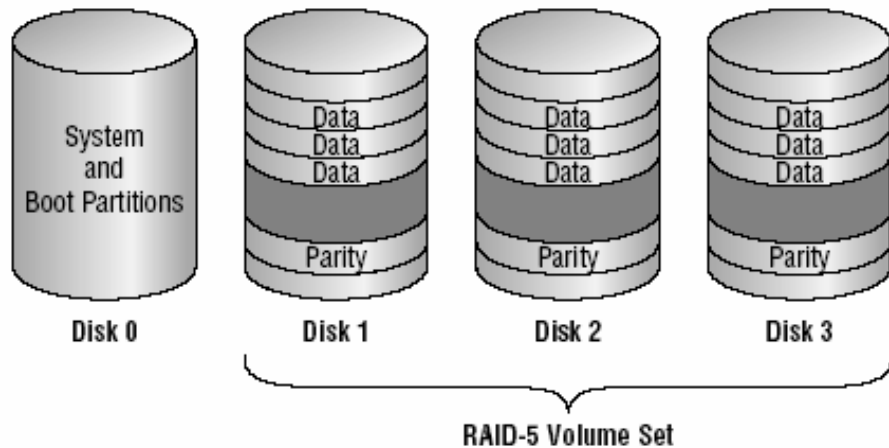


Hình 5.4.1: Volume mirrored

Nhược điểm chính của phương pháp này là chi phí cao. Để có một **volume 4GB** bạn phải tốn đến **8GB** cho hai ổ đĩa.

2.2.2.5 Volume RAID-5

Tương tự như **volume striped** nhưng **RAID-5** lại dùng thêm một dãy (**strip**) ghi thông tin kiểm lỗi **parity**. Nếu một đĩa của **volume** bị hỏng thì thông tin **parity** ghi trên đĩa khác sẽ giúp phục hồi lại dữ liệu trên đĩa hỏng. **Volume RAID-5** sử dụng ít nhất ba ổ đĩa (tối đa là 32).



Hình 5.5: Volume RAID-5

Ưu điểm chính của kỹ thuật này là khả năng dung lỗi cao và tốc độ truy xuất cao bởi sử dụng nhiều kênh I/O.

2.3 Sử dụng chương trình Disk Manager

Disk Manager là một tiện ích giao diện đồ họa phục vụ việc quản lý đĩa và volume trên môi trường Windows 2000 và Windows Server 2003. Để có thể sử dụng

được hết các chức năng của chương trình, bạn phải đăng nhập vào máy bằng tài khoản Administrator. Vào menu Start \ Programs \ Administrative Tools \ Computer Management. Sau đó mở rộng mục Storage và chọn Disk Management. Cửa sổ Disk Management xuất hiện.

2.3.1. Xem thuộc tính của đĩa

Nhấp phải chuột lên ổ đĩa vật lý muốn biết thông tin và chọn Properties.

- + Số thứ tự của ổ đĩa vật lý
- + Loại đĩa (basic, dynamic, DVD-ROM, DVD, đĩa chuyển đời được, hoặc unknown)
- + Trạng thái của đĩa (online hoặc offline)
- + Dung lượng đĩa
- + Lượng không gian chưa cấp phát
- + Loại thiết bị phần cứng
- + Nhà sản xuất thiết bị
- + Tên của adapter
- + Danh sách các volume đã tạo trên đĩa

2.3.2. Xem thuộc tính của volume hoặc đĩa cục bộ

Trên một ổ đĩa **dynamic**, bạn sử dụng các **volume**. Ngược lại trên một ổ đĩa **basic**, bạn sử dụng các đĩa cục bộ (**local disk**). **Volume** và đĩa cục bộ đều có chức năng như nhau, do vậy các phần sau dựa vào đĩa cục bộ để minh họa. Để xem thuộc tính của một đĩa cục bộ, bạn nhấp phải chuột lên đĩa cục bộ đó và chọn **Properties**.

2.3.2.1 Tab General.

Cung cấp các thông tin như nhãn đĩa, loại, hệ thống tập tin, dung lượng đã sử dụng, còn trống và tổng dung lượng. Nút **Disk Cleanup** dùng để mở chương trình **Disk Cleanup** dùng để xóa các tập tin không cần thiết, giải phóng không gian đĩa.

2.3.2.2 Tab Tools.

Bấm nút **Check Now** để kích hoạt chương trình **Check Disk** dùng để kiểm tra lỗi như khi không thể truy xuất đĩa hoặc khởi động lại máy không đúng cách. Nút **Backup Now** sẽ mở chương trình **Backup Wizard**, hướng dẫn bạn các bước thực hiện việc sao lưu các tập tin và thư mục trên đĩa. Nút **Defragment Now** mở chương trình **Disk Defragment**, dùng để dồn các tập tin trên đĩa thành một khối liên tục, giúp ích cho việc truy xuất đĩa.

2.3.2.3 Tab Hardware

Liệt kê các ổ đĩa vật lý **Windows Server 2003** nhận diện được. Bên dưới danh sách liệt kê các thuộc tính của ổ đĩa được chọn.

2.3.2.4 Tab Sharing

Cho phép chia sẻ hoặc không chia sẻ ổ đĩa cục bộ này. Theo mặc định, tất cả các ổ đĩa cục bộ đều được chia sẻ dưới dạng ẩn (có dấu \$ sau tên chia sẻ).

2.3.2.5 Tab Security

Chỉ xuất hiện khi đĩa cục bộ này sử dụng hệ thống tập tin **NTFS**. Dùng để thiết lập quyền truy cập lên đĩa. Theo mặc định, nhóm **Everyone** được toàn quyền trên thư mục gốc của đĩa.

2.3.2.6 Tab Quota

Chỉ xuất hiện khi sử dụng **NTFS**. Dùng để quy định lượng không gian đĩa cấp phát cho người dùng.

2.3.2.7 Shadow Copies

Shadow Copies là dịch vụ cho phép người dùng truy cập hoặc khôi phục những phiên bản trước đây của những tập tin đã lưu, bằng cách dùng một tính năng ở máy trạm gọi là **Previous Versions**.

2.3.3. Bổ sung thêm một ổ đĩa mới

2.3.3.1 Máy tính không hỗ trợ tính năng “hot swap”

Bạn phải tắt máy tính rồi mới lắp ổ đĩa mới vào. Sau đó khởi động máy tính lại. Chương trình **Disk Management** sẽ tự động phát hiện và yêu cầu bạn ghi một chữ ký đặc biệt lên ổ đĩa, giúp cho **Windows Server 2003** nhận diện được ổ đĩa này. Theo mặc định, ổ đĩa mới được cấu hình là một đĩa **dynamic**.

2.3.3.2 Máy tính hỗ trợ “hot swap”

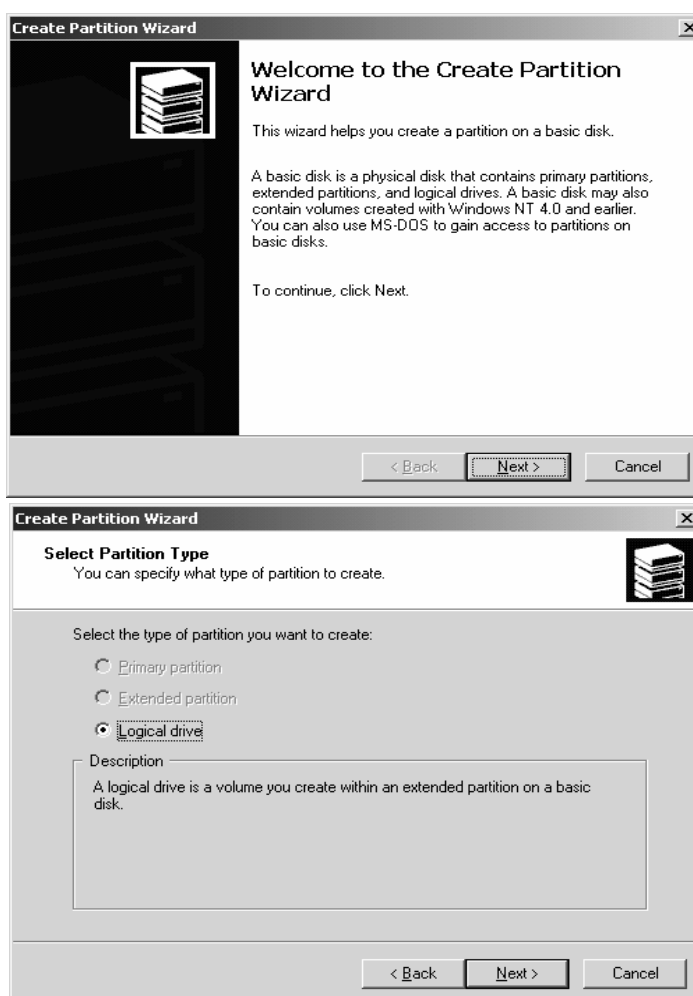
Bạn chỉ cần lắp thêm ổ đĩa mới vào theo hướng dẫn của nhà sản xuất mà không cần tắt máy. Rồi sau đó dùng chức năng **Action** □ **Rescan Disk** của **Disk Manager** để phát hiện ổ đĩa mới này.

2.3.4. Tạo partition volume mới

Nếu bạn còn không gian chưa cấp phát trên một đĩa **basic** thì bạn có thể tạo thêm **partition** mới, còn trên đĩa **dynamic** thì bạn có thể tạo thêm **volume** mới. Phần sau hướng dẫn bạn sử dụng **Create Partition Wizard** để tạo một **partition** mới:

Nhấp phải chuột lên vùng trống chưa cấp phát của đĩa **basic** và chọn **Create Logical Drive**.

Xuất hiện hộp thoại **Create Partition Wizard**. Nhấn nút **Next** trong hộp thoại này.



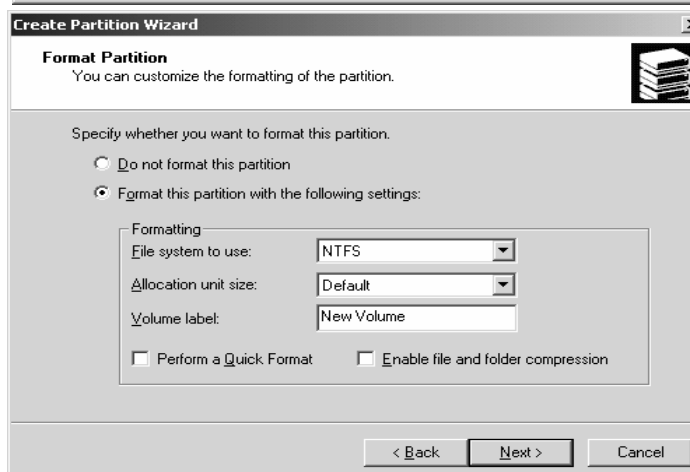
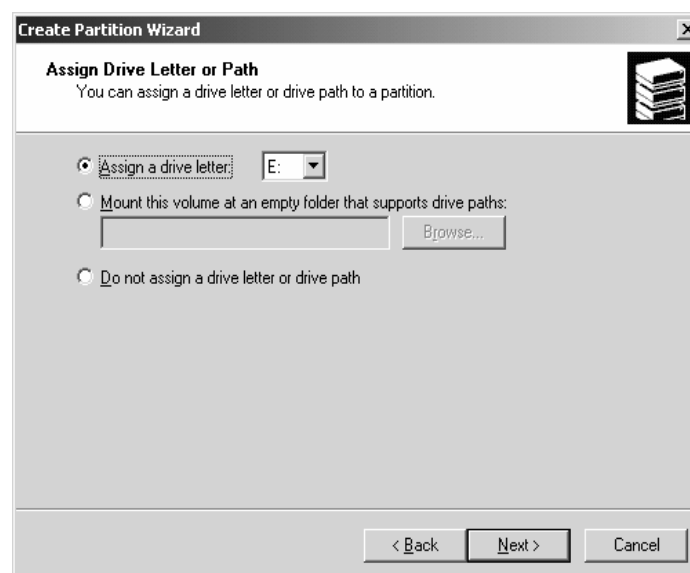
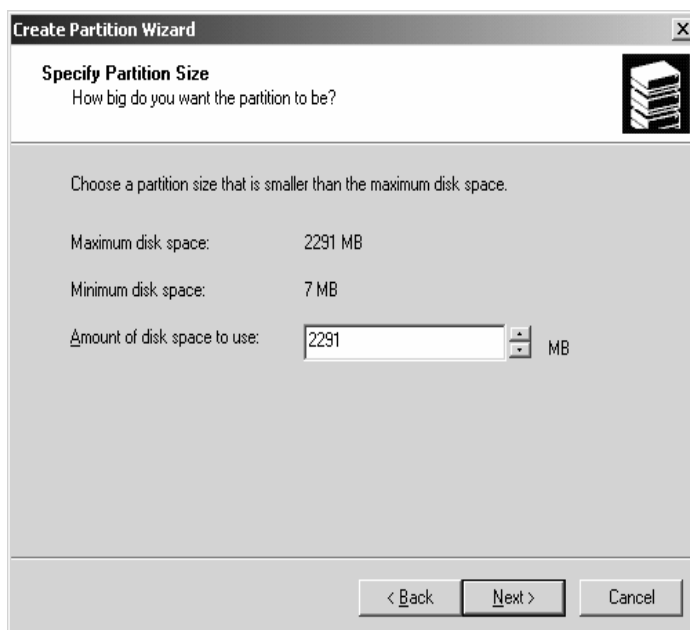
Tiếp theo, hộp thoại **Specify Partition Size** yêu cầu bạn cho biết dung lượng định cấp phát. Sau khi chỉ định xong, nhấn **Next**.

Trong hộp thoại **Select Partition Type**, chọn loại **partition** mà bạn định tạo. Chỉ có những loại còn khả năng tạo mới được phép chọn (tùy thuộc vào ổ đĩa vật lý của bạn). Sau khi chọn loại **partition** xong nhấn **Next** để tiếp tục.

Trong hộp thoại **Assign Drive Letter or Path**, bạn có thể đặt cho **partition** này một ký tự ổ đĩa, hoặc gắn (**mount**) vào một thư mục rỗng, hoặc không làm đặt gì hết. Khi bạn chọn kiểu gắn vào một thư mục rỗng thì bạn có thể tạo ra vô số **partition** mới. Sau khi đã quyết định xong, nhấn **Next** để tiếp tục.

Hộp thoại **Format Partition** yêu cầu bạn quyết định có định dạng **partition** này không. Nếu có thì dùng hệ thống tập tin là gì? đơn vị cấp phát là bao nhiêu? nhãn của **partition** (**volume label**) là gì? có định dạng nhanh không? Có nén tập tin và thư mục không? Sau khi đã chọn xong, nhấn **Next** để tiếp tục.

Hộp thoại **Completing the Create Partition Wizard** tóm tắt lại các thao tác sẽ thực hiện, bạn phải kiểm tra lại xem đã chính xác chưa, sau đó nhấn **Finish** để bắt đầu thực hiện.



2.3.5. Thay đổi ký tự ổ đĩa hoặc đường dẫn.

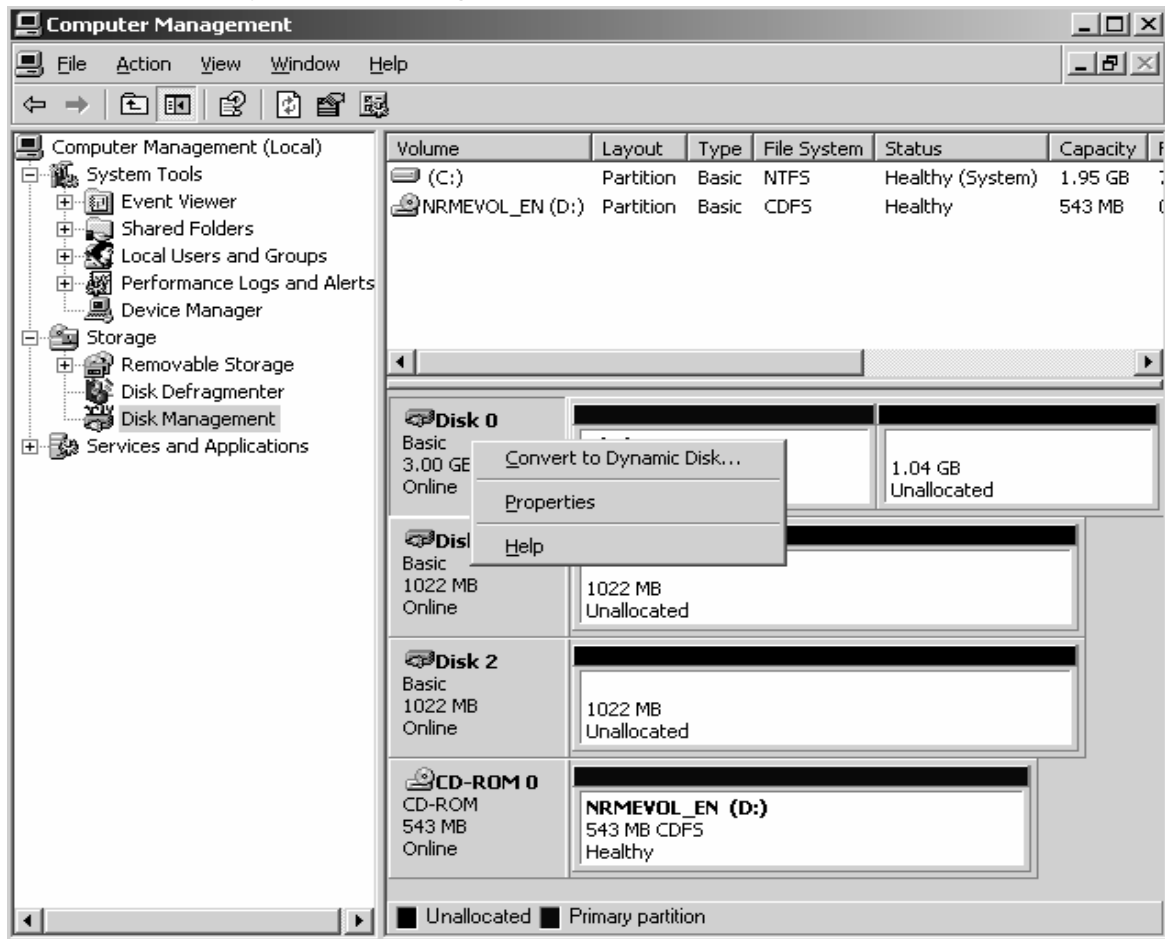
Muốn thay đổi ký tự ổ đĩa cho **partition/volume** nào, bạn nhấp phải chuột lên **volume** đó và chọn **Change Drive Letter and Path**. Hộp thoại **Change Drive Letter and Path** xuất hiện.

Trong hộp thoại này, nhấn nút **Edit** để mở tiếp hộp thoại **Edit Drive Letter and Path**, mở danh sách **Assign a drive letter** và chọn một ký tự ổ đĩa mới định đặt cho **partition/volume** này. Cuối cùng đồng ý xác nhận các thay đổi đã thực hiện.

2.3.6. Xoá partition/volume

Để tổ chức lại một ổ đĩa hoặc huỷ các dữ liệu có trên một **partition/volume**, bạn có thể xoá nó đi. Để thực hiện, trong cửa sổ **Disk Manager**, bạn nhấp phải chuột lên **partition/volume** muốn xoá và chọn **Delete Partition** (hoặc **Delete Volume**). Một hộp thoại cảnh báo xuất hiện, thông báo dữ liệu trên **partition** hoặc **volume** sẽ bị xoá và yêu cầu bạn xác nhận lại lần nữa thao tác này.

2.3.7. Cấu hình Dynamic Storage



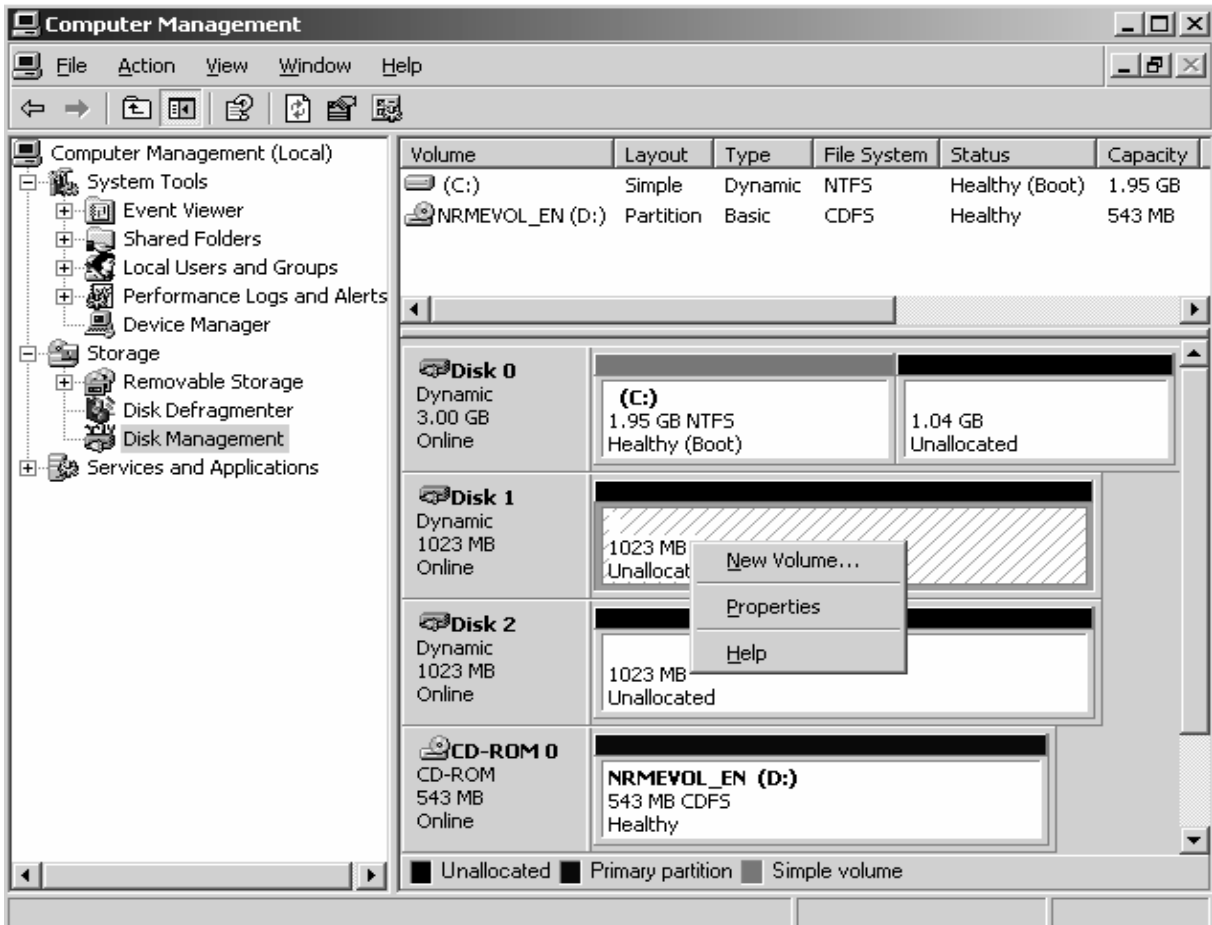
Hình 5.6: Cấu hình Dynamic Storage

2.3.7.1 Chuyển chế độ lưu trữ.

Để sử dụng được cơ chế lưu trữ **Dynamic**, bạn phải chuyển đổi các đĩa cứng vật lý trong hệ thống thành **Dynamic Disk**. Trong công cụ **Computer Management \ Disk Management**, bạn nhấp phải chuột trên các ổ đĩa bên của sổ bên phải và chọn **Convert to Dynamic Disk....** Sau đó đánh dấu vào tất cả các đĩa cứng vật lý cần chuyển đổi chế độ lưu trữ và chọn **OK** để hệ thống chuyển đổi. Sau khi chuyển đổi

xong hệ thống sẽ yêu cầu bạn **restart** máy để áp dụng chế độ lưu trữ mới.

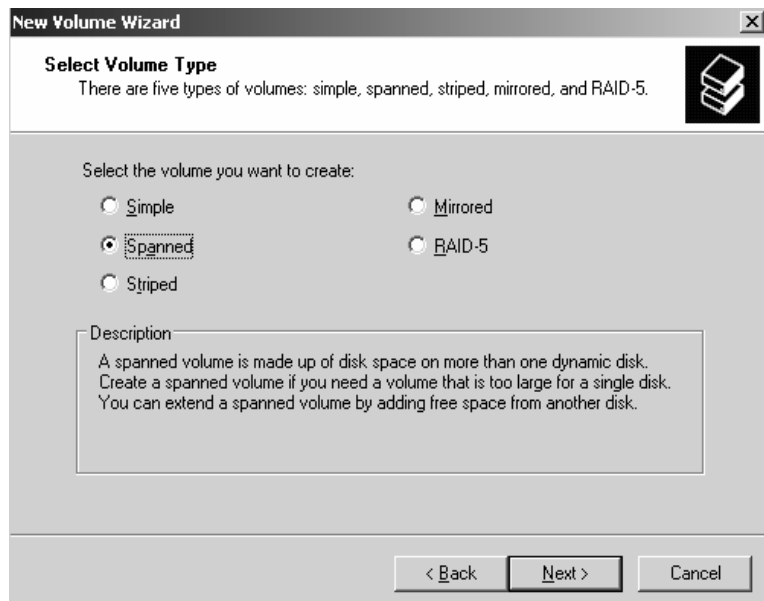
2.3.7.2 Tạo Volume Spanned.



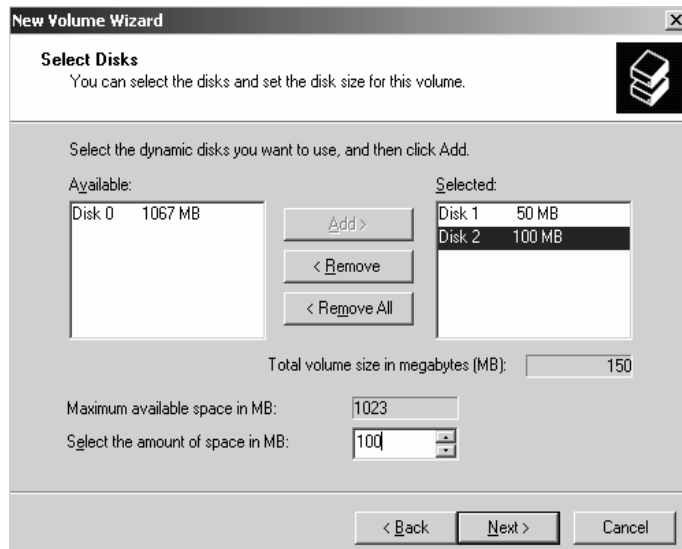
Hình 5.7: Tạo Volume Spanned

Trong công cụ **Disk Management**, bạn nhấp phải chuột lên vùng trống của đĩa cứng cần tạo **Volume**, sau đó chọn **New Volume**.

Tiếp theo, bạn chọn loại **Volume** cần tạo. Trong trường hợp này chúng ta chọn **Spanned**.



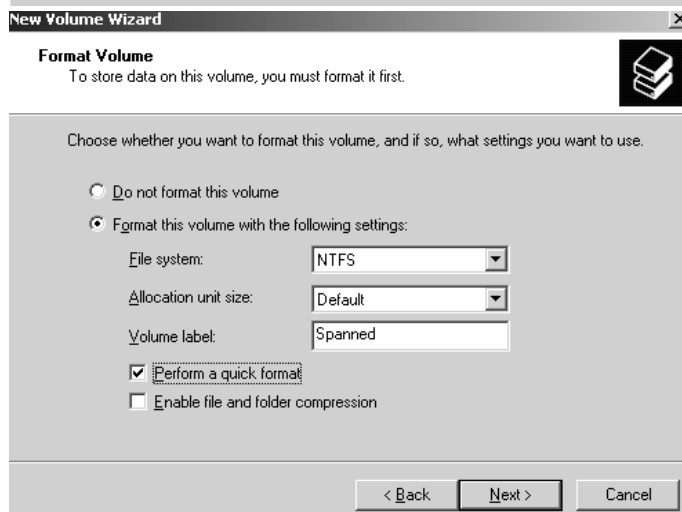
Bạn chọn những đĩa cứng dùng để tạo **Volume** này, đồng thời bạn cũng nhập kích thước mà mỗi đĩa giành ra để tạo **Volume**. Chú ý đối với loại **Volume** này thì kích thước của các đĩa giành cho **Volume** có thể khác nhau.



Bạn gán ký tự ổ đĩa cho **Volume**.



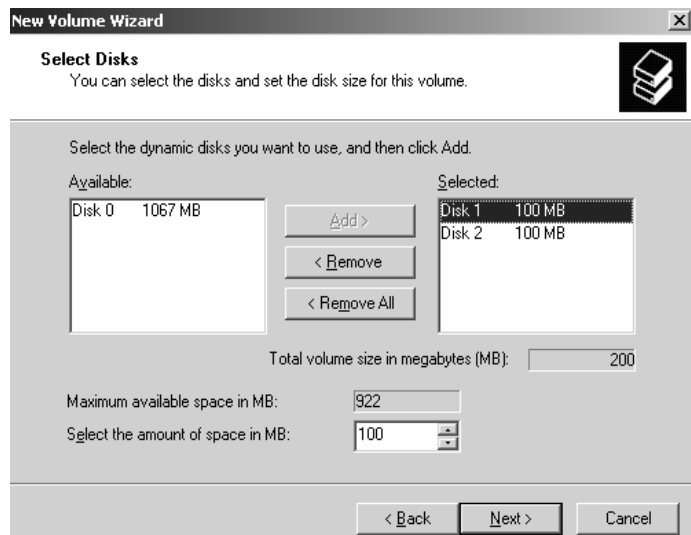
Bạn định dạng **Volume** mà bạn vừa tạo để có thể chứa dữ liệu.



Đến đây đã hoàn thành việc tạo **Volume**, bạn có thể lưu trữ dữ liệu trên **Volume** này theo cơ chế đã trình bày ở phần lý thuyết.

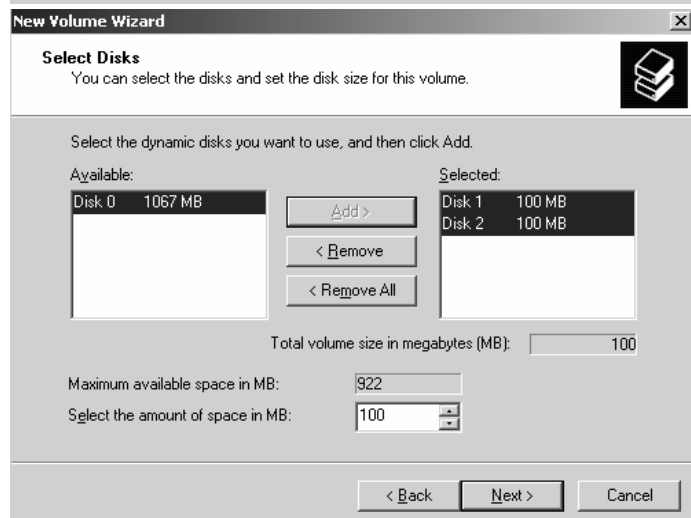
3.7.3 Tạo Volume Striped

Các bước tạo **Volume Striped** cũng tương tự như việc tạo các **Volume** khác nhưng chú ý là kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng tổng các kích thước của các phần trên.

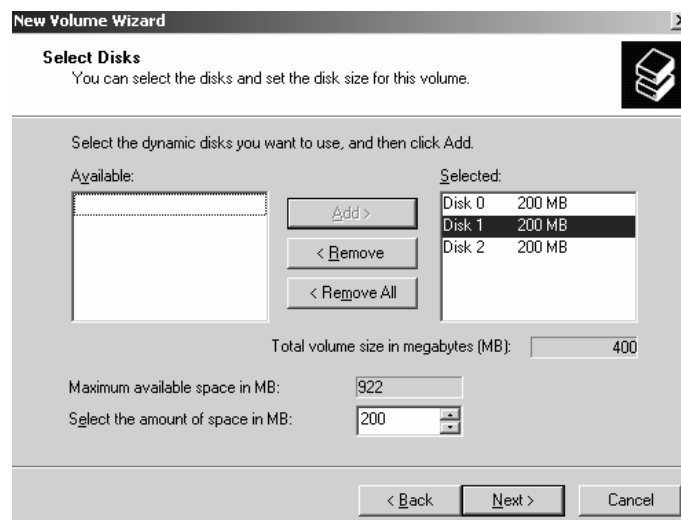


2.3.7.4 Tạo Volume Mirror.

Các bước tạo **Volume Mirror** cũng tương tự như trên, chú ý kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng chính kích thước của mỗi phần trên.



3.7.5 Tạo Volume Raid-5.



Các bước tạo **Volume Raid-5** cũng tương tự như trên nhưng chú ý là loại **Volume** yêu cầu tối thiểu đến 3 đĩa cứng. Kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng 2/3 kích thước của mỗi phần cộng lại.

2.4. Quản lý việc nén dữ liệu

Nén dữ liệu là quá trình lưu trữ dữ liệu dưới một dạng thức chiếm ít không gian hơn dữ liệu ban đầu. **Windows Server 2003** hỗ trợ tính năng nén các tập tin và thư mục một cách tự động và trong suốt. Các chương trình ứng dụng truy xuất các tập tin nén một cách bình thường do hệ điều hành tự động giải nén khi mở tập tin và nén lại khi lưu tập tin lên đĩa. Khả năng này chỉ có trên các **partition NTFS**. Nếu bạn chép một tập tin/thư mục trên một **partition** có tính năng nén sang một **partition FAT** bình thường thì hệ điều hành sẽ giải nén tập tin/ thư mục đó trước khi chép đi.

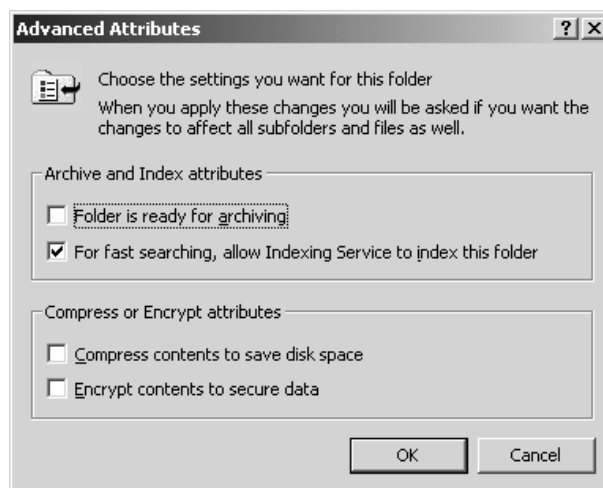
Để thi hành việc nén một tập tin/thư mục, bạn sử dụng chương trình **Windows Explorer** và thực hiện theo các bước sau:

- Trong cửa sổ **Windows Explorer**, duyệt đến tập tin/thư mục định nén và chọn tập tin/thư mục đó.

- Nhấp phải chuột lên đối tượng đó và chọn **Properties**.

- Trong hộp thoại **Properties**, nhấn nút **Advanced** trong **tab General**.

- Trong hộp thoại **Advanced Properties**, chọn mục “**Compress contents to save disk space**” và nhấn chọn **OK**.



- Nhấn chọn **OK** trong hộp thoại **Properties** để xác nhận thao tác. Nếu bạn định nén một thư mục, hộp thoại **Confirm Attribute Changes** xuất hiện, yêu cầu bạn lựa chọn hoặc là chỉ nén thư mục này thôi (**Apply changes to this folder only**) hoặc nén cả các thư mục con và tập tin có trong thư mục (**Apply changes to this folder, subfolders and files**). Thực hiện lựa chọn của bạn và nhấn **OK**.



Để thực hiện việc giải nén một thư mục/tập tin, bạn thực hiện tương tự theo các bước ở trên và bỏ chọn mục **Compress contents to save disk space** trong hộp thoại **Advanced Properties**.

2.5. Thiết lập hạn ngạch đĩa (disk quota).

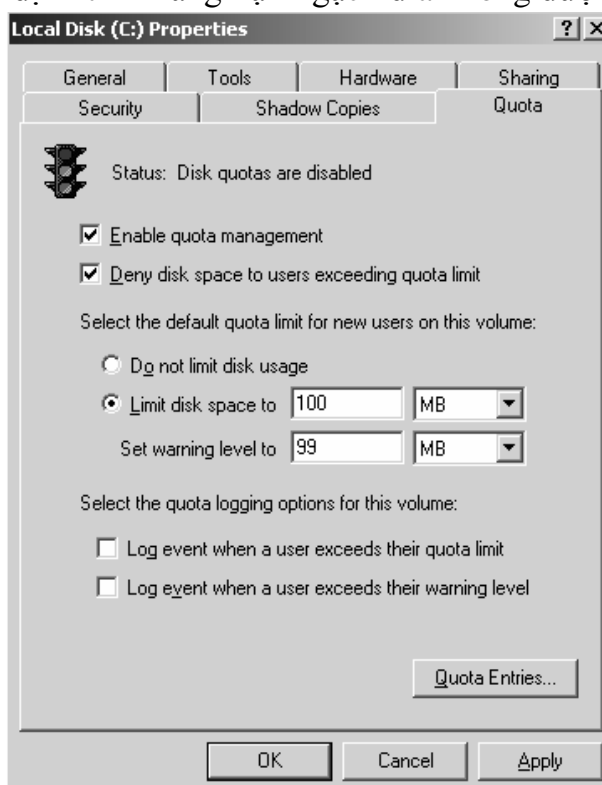
Hạn ngạch đĩa được dùng để chỉ định lượng không gian đĩa tối đa mà một người dùng có thể sử dụng trên một **volume NTFS**. Bạn có thể áp dụng hạn ngạch đĩa cho tất cả người dùng hoặc chỉ đối với từng người dùng riêng biệt.

Một số vấn đề bạn phải lưu ý khi thiết lập hạn ngạch đĩa:

- Chỉ có thể áp dụng trên các volume **NTFS**.
- Lượng không gian chiếm dụng được tính theo các tập tin và thư mục do người dùng sở hữu.
 - Khi người dùng cài đặt một chương trình, lượng không gian đĩa còn trống mà chương trình thấy được tính toán dựa vào hạn ngạch đĩa của người dùng, không phải là lượng không gian còn trống trên **volume**.
 - Được tính toán trên kích thước thật sự của tập tin trong trường hợp tập tin/thư mục được nén.

2.5.1. Cấu hình hạn ngạch đĩa.

Bạn cấu hình hạn ngạch đĩa bằng hộp thoại **Volume Properties** đã giới thiệu trong phần trên. Bạn cũng có thể mở hộp thoại này bằng cách nhấp phải chuột lên ký tự ổ đĩa trong **Windows Explorer** và chọn **Properties**. Trong hộp thoại này nhấp chọn **tab Quota**. Theo mặc định tính năng hạn ngạch đĩa không được kích hoạt.



Hình 5.8: Cấu hình hạn ngạch đĩa

Các mục trong hộp thoại có ý nghĩa như sau:

- + **Enable quota management**: thực hiện hoặc không thực hiện quản lý hạn ngạch đĩa.
- + **Deny disk space to users exceeding quota limit**: người dùng sẽ không thể tiếp tục sử dụng đĩa khi vượt quá hạn ngạch và nhận được thông báo **out of disk space**.
- + **Select the default quota limit for new users on this volume**: định nghĩa các giới hạn sử dụng. Các lựa chọn bao gồm “không định nghĩa giới hạn” (**Do not limit**

disk space), “giới hạn cho phép” (**Limit disk space to**) và “giới hạn cảnh báo” (**Set warning level to**).

+ **Select the quota logging options for this volume:** có ghi nhận lại các sự kiện liên quan đến sử dụng hạn ngạch đĩa. Có thể ghi nhận khi người dùng vượt quá giới hạn cho phép hoặc vượt quá giới hạn cảnh báo.

Biểu tượng đèn giao thông trong hộp thoại có các trạng thái sau:

- + Đèn đỏ cho biết tính năng quản lý hạn ngạch không được kích hoạt.
- + Đèn vàng cho biết **Windows Server** đang xây dựng lại thông tin hạn ngạch.
- + Đèn xanh cho biết tính năng quản lý đang có tác dụng.

2.5.2. Thiết lập hạn ngạch mặc định.

Khi bạn thiết lập hạn ngạch mặc định áp dụng cho các người dùng mới trên volume, chỉ những người dùng chưa bao giờ tạo tập tin trên volume đó mới chịu ảnh hưởng. Có nghĩa là những người dùng đã sở hữu các tập tin/thư mục trên volume này đều không bị chính sách hạn ngạch quy định. Như vậy, nếu bạn dự định áp đặt hạn ngạch cho tất cả các người dùng, bạn phải chỉ định hạn ngạch ngay từ khi tạo lập volume.

Để thực hiện, bạn mở hộp thoại **Volume Properties** và chọn tab **Quota**. Đánh dấu chọn mục **Enable quota management** và điền vào các giá trị giới hạn sử dụng và giới hạn cảnh báo.

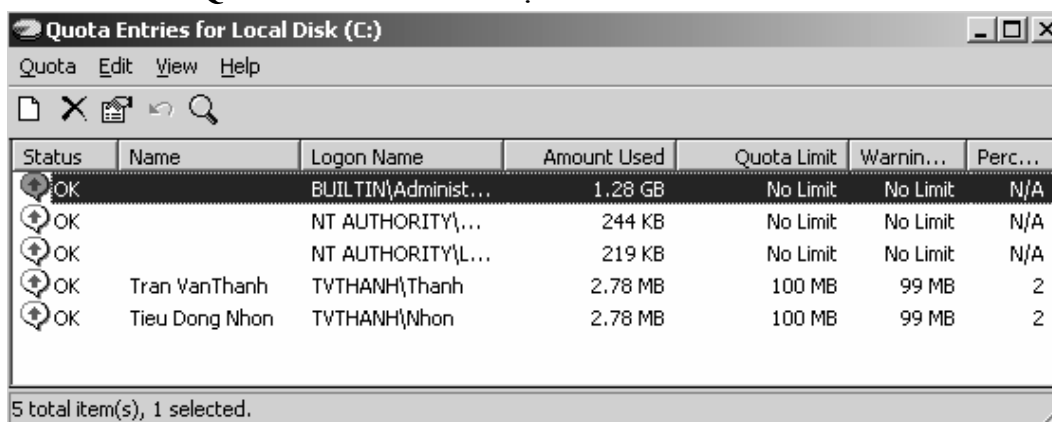
2.5.3. Chỉ định hạn ngạch cho từng cá nhân.

Trong một vài trường hợp, bạn cần phải chỉ định hạn ngạch cho riêng một người nào đó, chẳng hạn có thể là các lý do sau:

+ Người dùng này sẽ giữ nhiệm vụ cài đặt các phần mềm mới, và như vậy họ phải có được lượng không gian đĩa trống lớn.

+ Hoặc là người dùng đã tạo nhiều tập tin trên **volume** trước khi thiết lập hạn ngạch, do vậy họ sẽ không chịu tác dụng. Bạn phải tạo riêng một giới hạn mới áp dụng cho người đó.

Để thiết lập, nhấn nút **Quota Entries** trong tab **Quota** của hộp thoại **Volume Properties**. Cửa sổ **Quota Entries** xuất hiện.

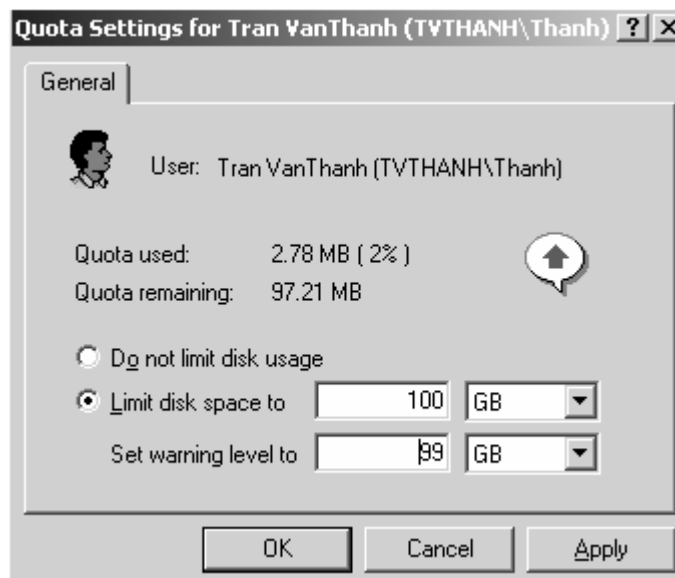


Status	Name	Logon Name	Amount Used	Quota Limit	Warnin...	Perc...
OK		BUILTIN\Administ...	1.28 GB	No Limit	No Limit	N/A
OK		NT AUTHORITY\...	244 KB	No Limit	No Limit	N/A
OK		NT AUTHORITY\L...	219 KB	No Limit	No Limit	N/A
OK	Tran VanThanh	TVTHANH\Thanh	2.78 MB	100 MB	99 MB	2
OK	Tieu Dong Nhon	TVTHANH\Nhon	2.78 MB	100 MB	99 MB	2

5 total item(s), 1 selected.

Hình 5.9: Chỉ định hạn ngạch cho từng cá nhân

Chỉnh sửa thông tin hạn ngạch của một người dùng: nhấn đúp vào mục của người dùng tương ứng, hộp thoại **Quota Setting** xuất hiện cho phép bạn thay đổi các giá trị hạn ngạch.



Hình 5.10: Chỉnh sửa thông tin hạn ngạch

Bổ sung thêm một mục quy định hạn ngạch: trong cửa sổ **Quota Entries**, vào menu **Quota** chọn mục **New Quota Entry** / xuất hiện hộp thoại **Select Users**, bạn chọn người dùng rồi nhấn **OK** / xuất hiện hộp thoại **Add New Quota Entry**, bạn nhập các giá trị hạn ngạch thích hợp và nhấn **OK**.

2.6. Mã hoá dữ liệu bằng EFS

EFS (Encrypting File System) là một kỹ thuật dùng trong **Windows Server 2003** dùng để mã hoá các tập tin lưu trên các **partition NTFS**. Việc mã hoá sẽ bổ sung thêm một lớp bảo vệ an toàn cho hệ thống tập tin. Chỉ người dùng có đúng khoá mới có thể truy xuất được các tập tin này còn những người khác thì bị từ chối truy cập. Ngoài ra, người quản trị mạng còn có thể dùng tác nhân phục hồi (**recovery agent**) để truy xuất đến bất kỳ tập tin nào bị mã hoá. Để mã hoá các tập tin, tiến hành theo các bước sau:

Mở cửa sổ Windows Explorer: Trong cửa sổ **Windows Explorer**, chọn các tập tin và thư mục cần mã hoá. Nhấp phải chuột lên các tập tin và thư mục, chọn **Properties**. Trong hộp thoại **Properties**, nhấn nút **Advanced**.

Hộp thoại **Advanced Properties** xuất hiện, đánh dấu mục **Encrypt contents to secure data** và nhấn **OK**.

Trở lại hộp thoại **Properties**, nhấn **OK**, xuất hiện hộp thoại **Confirm Attribute Changes** yêu cầu bạn cho biết sẽ mã hoá chỉ riêng thư mục được chọn (**Apply changes to this folder only**) hoặc mã hoá toàn bộ thư mục kể cả các thư mục con (**Apply changes to this folder, subfolders and files**). Sau đó nhấn **OK**.

Để thôi không mã hoá các tập tin, bạn thực hiện tương tự theo các bước trên nhưng bỏ chọn mục **Encrypt contents to secure data**.

Bài tập

1. Thiết lập lại hạn ngạch đĩa cho từng thành viên

Bài 6: TẠO VÀ QUẢN LÝ THƯ MỤC DÙNG CHUNG

Giới thiệu

Tài nguyên chia sẻ là các tài nguyên trên mạng mà người dùng có thể truy xuất và sử dụng thông qua mạng. Muốn chia sẻ một thư mục dùng chung trên mạng, phải logon vào hệ thống với vai trò người quản trị (Administrators) hoặc là thành viên của nhóm Server Operators.

1. Mục tiêu:

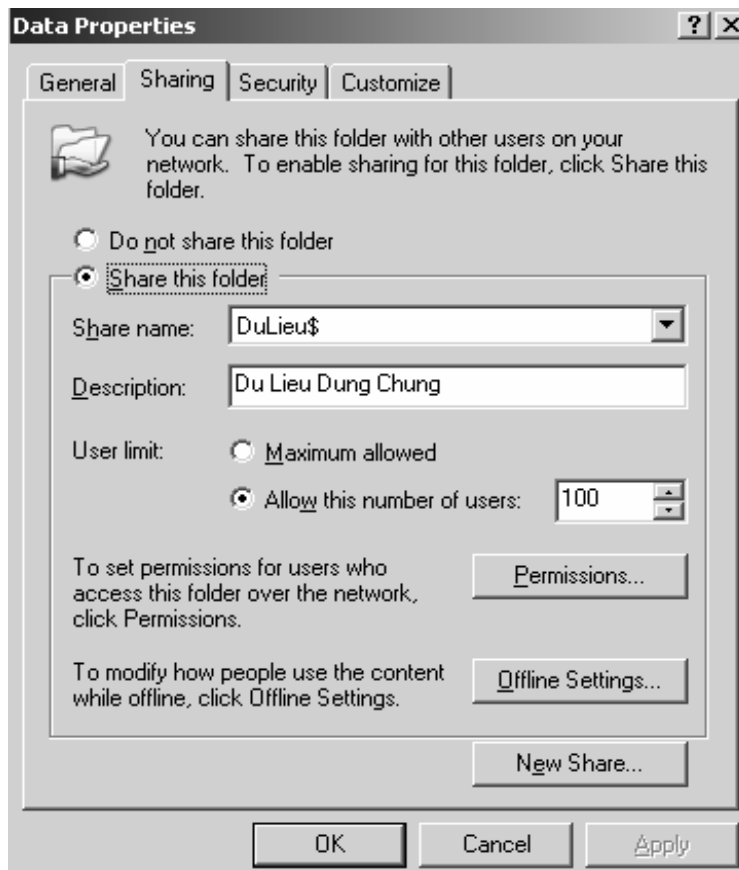
- Trình bày các loại quyền truy cập dữ liệu;
- Tạo và quản lý các thư mục dùng chung trên mạng.
- Thực hiện các thao tác an toàn với máy tính.

2. Nội dung chính:

2.1 Tạo thư mục dùng chung

2.1.1. Chia sẻ thư mục dùng chung

Các tài nguyên chia sẻ là các tài nguyên trên mạng mà các người dùng có thể truy xuất và sử dụng thông qua mạng. Muốn chia sẻ một thư mục dùng chung trên mạng, bạn phải **logon** vào hệ thống với vai trò người quản trị (**Administrators**) hoặc là thành viên của nhóm **Server Operators**, tiếp theo trong **Explorer** bạn nhấp phải chuột trên thư mục đó và chọn **Properties**, hộp thoại **Properties** xuất hiện, chọn **Tab Sharing**.



Ý nghĩa của các mục trong **Tab Sharing**:

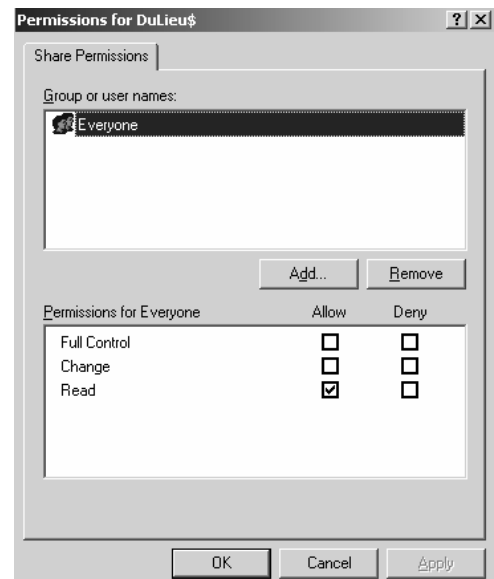
Mục	Ý nghĩa
Do not share this folder	Chỉ định thư mục này chỉ được phép truy cập cục bộ

Mục	Ý nghĩa
Share this folder	Chỉ định thư mục này được phép truy cập cục bộ và truy cập qua mạng
Share name	Tên thư mục mà người dùng mạng nhìn thấy và truy cập
Comment	Cho phép người dùng mô tả thêm thông tin về thư mục dùng chung này
User Limit	Cho phép bạn khai báo số kết nối tối đa truy xuất vào thư mục tại một thời điểm
Permissions	Cho phép bạn thiết lập danh sách quyền truy cập thông qua mạng của người dùng
Offline Settings	Cho phép thư mục được lưu trữ tạm tài liệu khi làm việc dưới chế độ Offline .

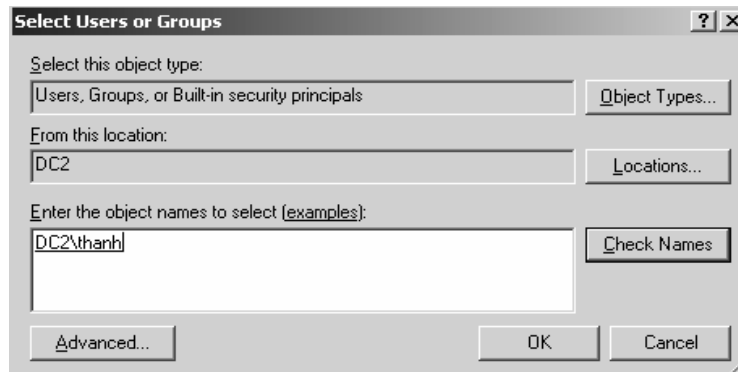
2.1.2. Cấu hình Share Permissions

Bạn muốn cấp quyền cho các người dùng truy cập qua mạng thì dùng **Share Permissions**. **Share Permissions** chỉ có hiệu lực khi người dùng truy cập qua mạng chứ không có hiệu lực khi người dùng truy cập cục bộ. Khác với **NTFS Permissions** là quản lý người dùng truy cập dưới cấp độ truy xuất đĩa. Trong hộp thoại **Share Permissions**, chứa danh sách các quyền sau:

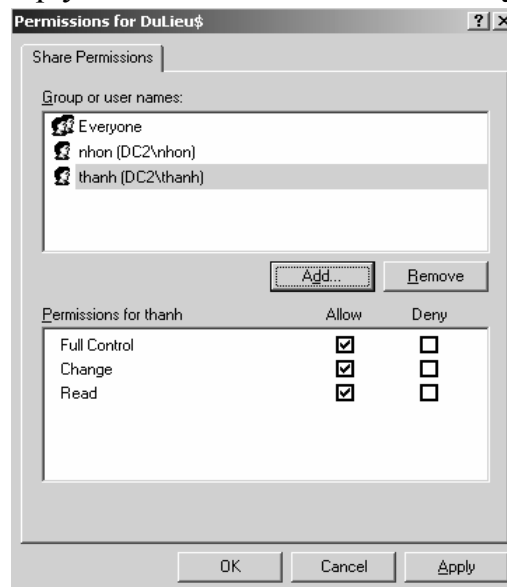
- **Full Control**: cho phép người dùng có toàn quyền trên thư mục chia sẻ.
- **Change**: cho phép người dùng thay đổi dữ liệu trên tập tin và xóa tập tin trong thư mục chia sẻ.
- **Read**: cho phép người dùng xem và thi hành các tập tin trong thư mục chia sẻ. Bạn muốn cấp quyền cho người dùng thì nhấp chuột vào nút **Add**.



Hộp thoại chọn người dùng và nhóm xuất hiện, bạn nhấp đôi chuột vào các tài khoản người dùng và nhóm cần chọn, sau đó chọn **OK**.



Trong hộp thoại xuất hiện, muốn cấp quyền cho người dùng bạn đánh dấu vào mục **Allow**, ngược lại khóa quyền thì đánh dấu vào mục **Deny**.



2.1.3. Chia sẻ thư mục dùng lệnh netshare

Chức năng: tạo, xóa và hiển thị các tài nguyên chia sẻ. Cú pháp:

net share sharename

net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]

net share sharename [/users:number | unlimited] [/remark:"text"]

net share {sharename | drive:path} /delete

Ý nghĩa các tham số:

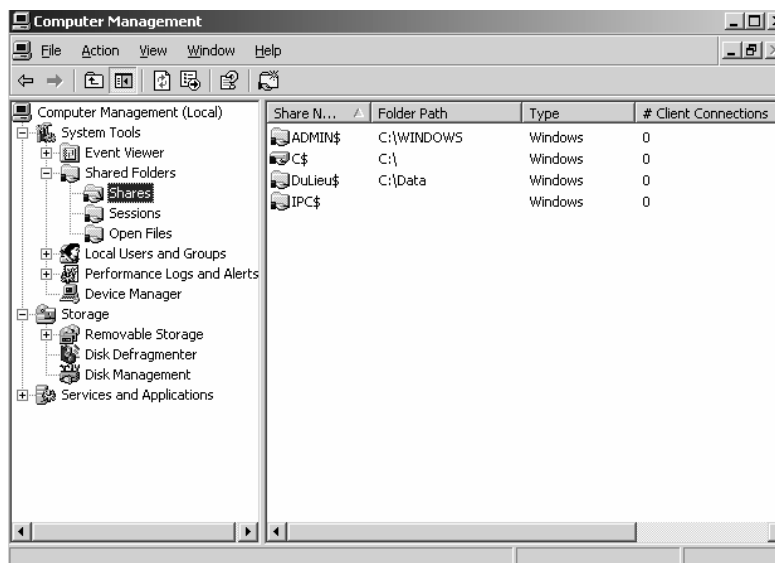
- [Không tham số]: hiển thị thông tin về tất cả các tài nguyên chia sẻ trên máy tính cục bộ
- [**Sharename**]: tên trên mạng của tài nguyên chia sẻ, nếu dùng lệnh **net share** với một tham số **sharename** thì hệ thống sẽ hiển thị thông tin về tài nguyên dùng chung này.
- [**drive:path**]: chỉ định đường dẫn tuyệt đối của thư mục cần chia sẻ.
- [**/users:number**]: đặt số lượng người dùng lớn nhất có thể truy cập vào tài nguyên dùng chung này.
- [**/unlimited**]: không giới hạn số lượng người dùng có thể truy cập vào tài nguyên dùng chung này.
- [**/remark:"text"**]: thêm thông tin mô tả về tài nguyên này.

- /delete: xóa thuộc tính chia sẻ của thư mục hiện tại.

2.2. Quản lý các thư mục dùng chung

2.2.1. Xem các thư mục dùng chung

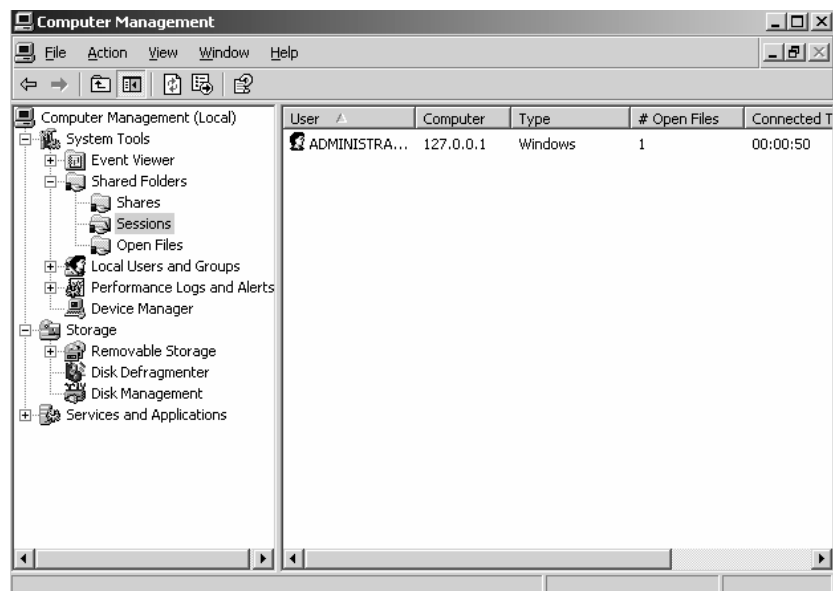
Mục **Shared Folders** trong công cụ **Computer Management** cho phép bạn tạo và quản lý các thư mục dùng chung trên máy tính. Muốn xem các thư mục dùng chung trên máy tính bạn chọn mục **Shares**. Nếu thư mục dùng chung nào có phần cuối của tên chia sẻ (**share name**) là dấu \$ thì tên thư mục dùng chung này được ẩn đi và không tìm thấy khi bạn tìm kiếm thông qua **My Network Places** hoặc duyệt các tài nguyên mạng.



2.2.2. Xem các phiên làm việc trên thư mục dùng chung

Muốn xem tất cả các người dùng đang truy cập đến các thư mục dùng chung trên máy tính bạn chọn mục **Session**. Mục **Session** cung cấp các thông tin sau:

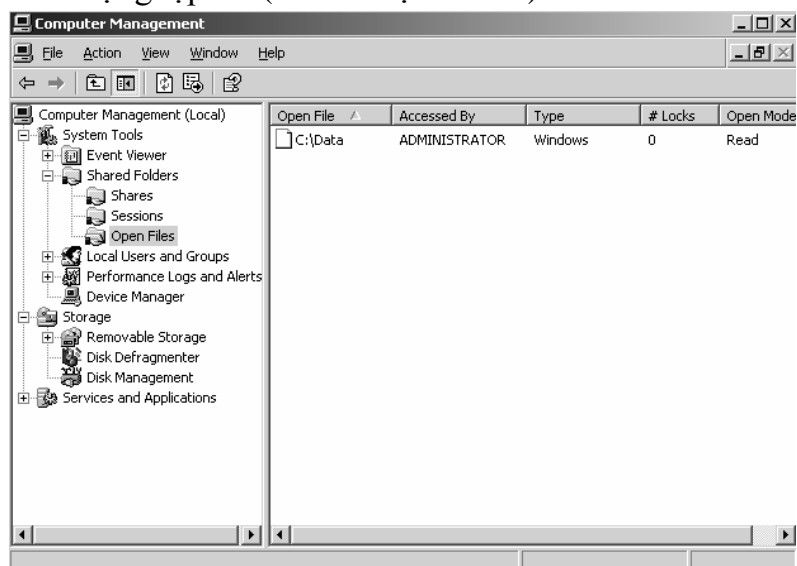
- Tên tài khoản người dùng đang kết nối vào tài nguyên chia sẻ.
- Tên máy tính có người dùng kết nối từ đó.
- Hệ điều hành mà máy trạm đang sử dụng để kết nối.
- Số tập tin mà người dùng đang mở.
- Thời gian kết nối của người dùng.
- Thời gian chờ xử lý của kết nối.
- Phải là truy cập của người dùng **Guest** không?



2.2.3. Xem các tập tin đang mở trong các thư mục dùng chung

Muốn xem các tập tin đang mở trong các thư mục dùng chung bạn nhấp chuột vào mục **Open Files**. Mục **Open Files** cung cấp các thông tin sau:

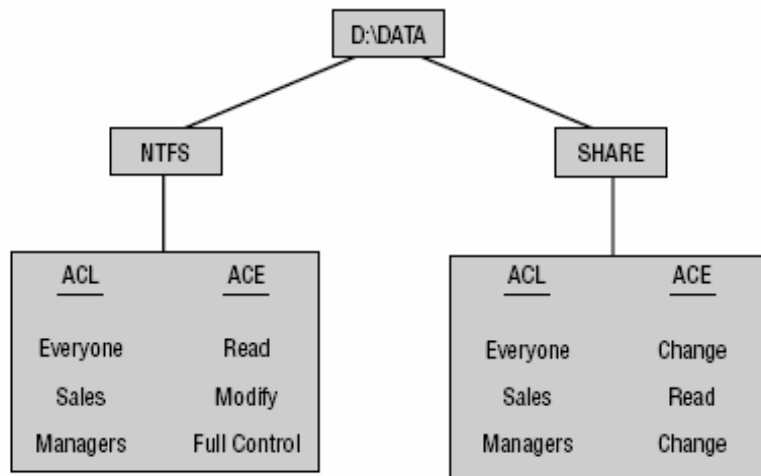
- Đường dẫn và tập tin hiện đang được mở.
- Tên tài khoản người dùng đang truy cập tập tin đó.
- Hệ điều hành mà người dùng sử dụng để truy cập tập tin.
- Trạng thái tập tin có đang bị khoá hay không.
- Trạng thái mở sử dụng tập tin (**Read** hoặc **Write**).



2.3. Quyền truy cập ntfs

Có hai loại hệ thống tập được dùng cho **partition** và **volume** cục bộ là **FAT** (bao gồm **FAT16** và **FAT32**). **FAT partition** không hỗ trợ bảo mật nội bộ, còn **NTFS partition** thì ngược lại có hỗ trợ bảo mật; có nghĩa là nếu đĩa cứng của bạn định dạng là **FAT** thì mọi người đều có thể thao tác trên các file chứa trên đĩa cứng này, còn ngược lại là định dạng **NTFS** thì tùy theo người dùng có quyền truy cập không, nếu người dùng không có quyền thì không thể nào truy cập được dữ liệu trên đĩa. Hệ thống **Windows Server 2003** dùng các **ACL (Access Control List)** để quản lý các

quyền truy cập của đối tượng cục bộ và các đối tượng trên **Active Directory**. Một **ACL** có thể chứa nhiều **ACE (Access Control Entry)** đại diện cho một người dùng hay một nhóm người.



2.3.1. Các quyền truy cập của NTFS

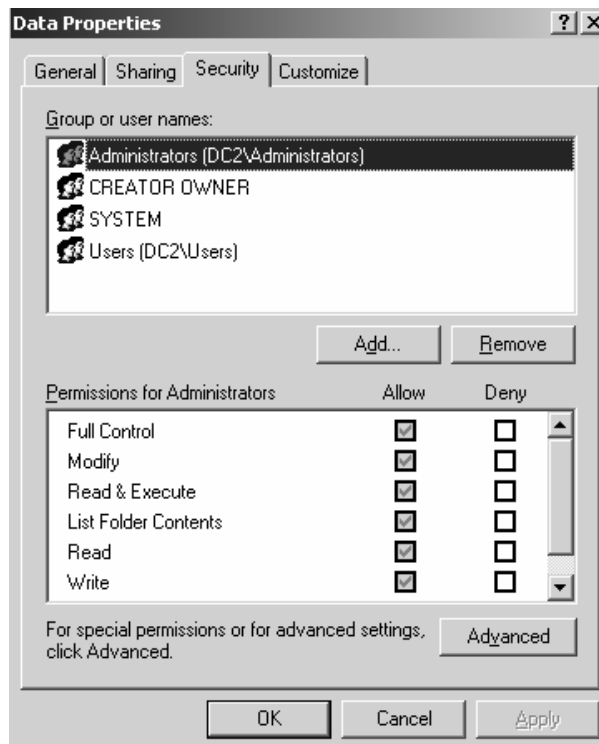
Tên quyền	Chức năng
Traverse Folder/Execute File	Duyệt các thư mục và thi hành các tập tin chương trình trong thư mục
List Folder/Read Data	Liệt kê nội dung của thư mục và đọc dữ liệu của các tập tin trong thư mục
Read Attributes	Đọc các thuộc tính của các tập tin và thư mục
Read Extended Attributes	Đọc các thuộc tính mở rộng của các tập tin và thư mục
Create File/Write Data	Tạo các tập tin mới và ghi dữ liệu lên các tập tin này
Create Folder/Append Data	Tạo thư mục mới và chèn thêm dữ liệu vào các tập tin
Write Attributes	Thay đổi thuộc tính của các tập tin và thư mục
Write Extended Attributes	Thay đổi thuộc tính mở rộng của các tập tin và thư mục
Delete Subfolders and Files	Xóa thư mục con và các tập tin
Delete	Xóa các tập tin
Read Permissions	Đọc các quyền trên các tập tin và thư mục
Change Permissions	Thay đổi quyền trên các tập tin và thư mục
Take Ownership	Tước quyền sở hữu của các tập tin và thư mục

2.3.2. Các mức quyền truy cập được dùng trong NTFS

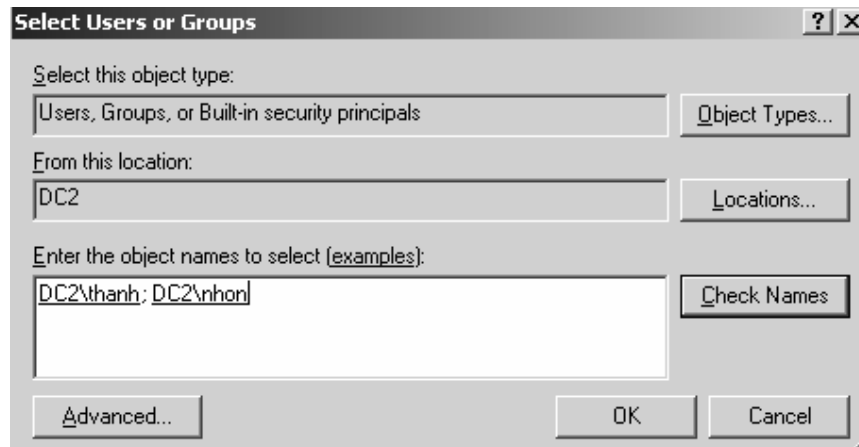
Tên quyền	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder /Execute File	X	X	X	X		
List Folder /Read Data	X	X	X	X	X	
Read Attributes	X	X	X	X	X	
Read Extended Attributes	X	X	X	X	X	
Create File /Write Data	X	X				
Create Folder /Append Data	X	X				X
Write Attributes	X	X				X
Write Extended Attributes	X	X				X
Delete Subfolders and Files	X					
Delete	X	X				
Read Permissions	X	X	X	X	X	X
Change Permissions	X					
Take Ownership	X					

2.3.3. Gán quyền truy cập NTFS trên thư mục dùng chung

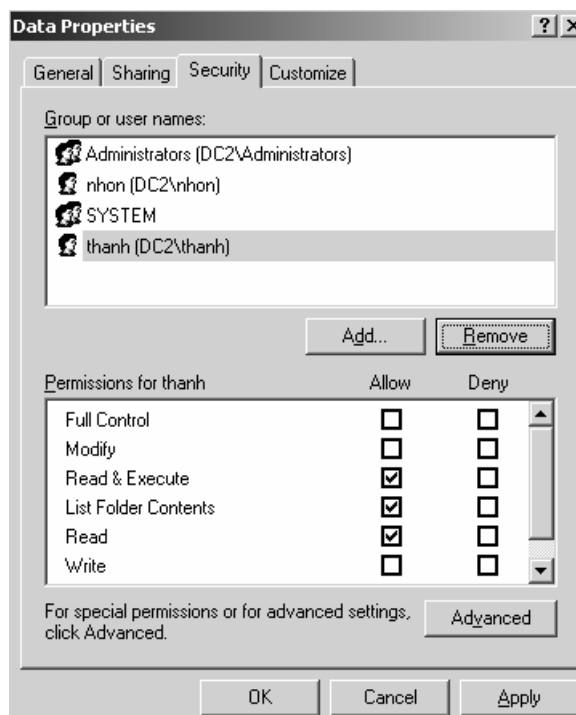
Bạn muốn gán quyền **NTFS**, thông qua **Windows Explorer** bạn nhấp phải chuột vào tập tin hay thư mục cần cấu hình quyền truy cập rồi chọn **Properties**. Hộp thoại **Properties** xuất hiện. Nếu ổ đĩa của bạn định dạng là **FAT** thì hộp thoại chỉ có hai **Tab** là **General** và **Sharing**. Nhưng nếu đĩa có định dạng là **NTFS** thì trong hộp thoại sẽ có thêm một **Tab** là **Security**. Tab này cho phép ta có thể quy định quyền truy cập cho từng người dùng hoặc một nhóm người dùng lên các tập tin và thư mục. Bạn nhấp chuột vào **Tab Security** để cấp quyền cho các người dùng.



Muốn cấp quyền truy cập cho một người dùng, bạn nhấp chuột vào nút **Add**, hộp thoại chọn lựa người dùng và nhóm xuất hiện, bạn chọn người dùng và nhóm cần cấp quyền, nhấp chuột vào nút **Add** để thêm vào danh sách, sau đó nhấp chuột vào nút **OK** để trở lại hộp thoại chính.

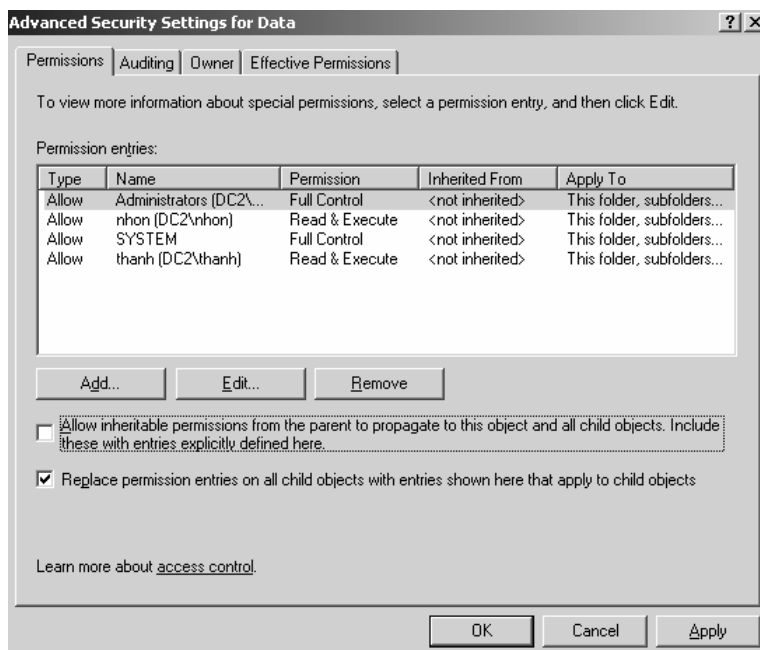


Hộp thoại chính sẽ xuất hiện các người dùng và nhóm mà bạn mới thêm vào, sau đó chọn người dùng và nhóm để cấp quyền. Trong hộp thoại đã hiện sẵn danh sách quyền, bạn muốn cho người dùng đó có quyền gì thì bạn đánh dấu vào phần **Allow**, còn ngược lại muốn cấm quyền đó thì đánh dấu vào mục **Deny**.

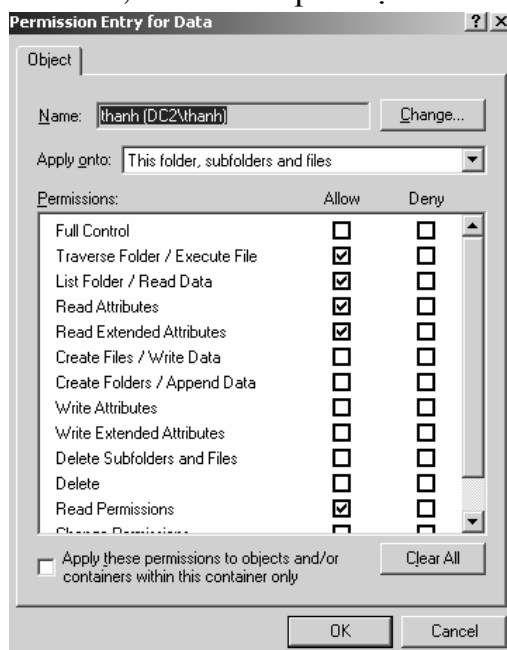


2.3.4. Kế thừa và thay thế quyền của đối tượng con.

Trong hộp thoại chính trên, chúng ta có thể nhấp chuột vào nút **Advanced** để cấu hình chi tiết hơn cho các quyền truy cập của người dùng. Khi nhấp chuột vào nút **Advanced**, hộp thoại **Advanced Security Settings** xuất hiện, trong hộp thoại, nếu bạn đánh dấu vào mục **Allow inheritable permissions from parent to propagate to this object and child objects** thì thư mục hiện tại được thừa hưởng danh sách quyền truy cập từ thư mục cha, bạn muốn xóa những quyền thừa hưởng từ thư mục cha bạn phải bỏ đánh dấu này. Nếu danh sách quyền truy cập của thư mục cha thay đổi thì danh sách quyền truy cập của thư mục hiện tại cũng thay đổi theo. Ngoài ra nếu bạn đánh dấu vào mục **Replace permission entries on all child objects with entries shown here that apply to child objects** thì danh sách quyền truy cập của thư mục hiện tại sẽ được áp dụng xuống các tập tin và thư mục con có nghĩa là các tập tin và thư mục con sẽ được thay thế quyền truy cập giống như các quyền đang hiển thị trong hộp thoại.



Trong hộp thoại này, **Windows Server 2003** cũng cho phép chúng ta kiểm tra và cấu hình lại chi tiết các quyền của người dùng và nhóm, để thực hiện, bạn chọn nhóm hay người dùng cần thao tác, sau đó nhấp chuột vào nút **Edit**.



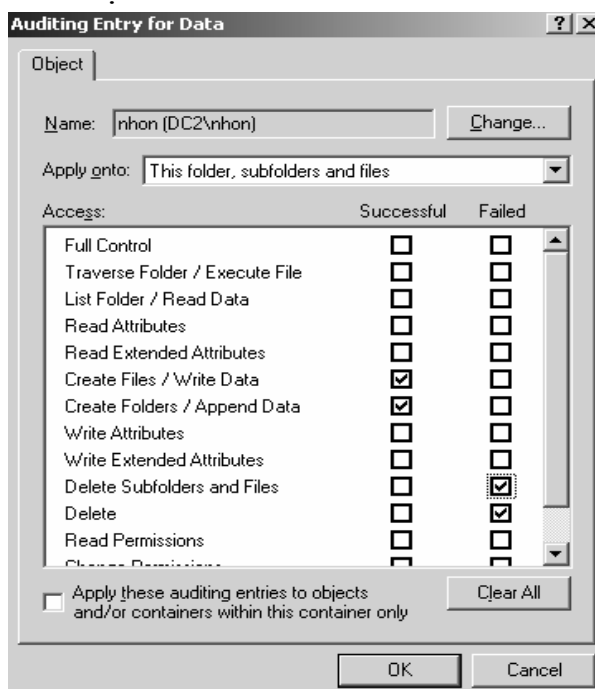
2.3.5. Thay đổi quyền khi di chuyển thư mục và tập tin.

Khi chúng ta sao chép (**copy**) một tập tin hay thư mục sang một vị trí mới thì quyền truy cập trên tập tin hay thư mục này sẽ thay đổi theo quyền trên thư mục cha chứa chúng, nhưng ngược lại nếu chúng ta di chuyển (**move**) một tập tin hay thư mục sang bất kỳ vị trí nào thì các quyền trên chúng vẫn được giữ nguyên.

2.3.6. Giám sát người dùng truy cập thư mục

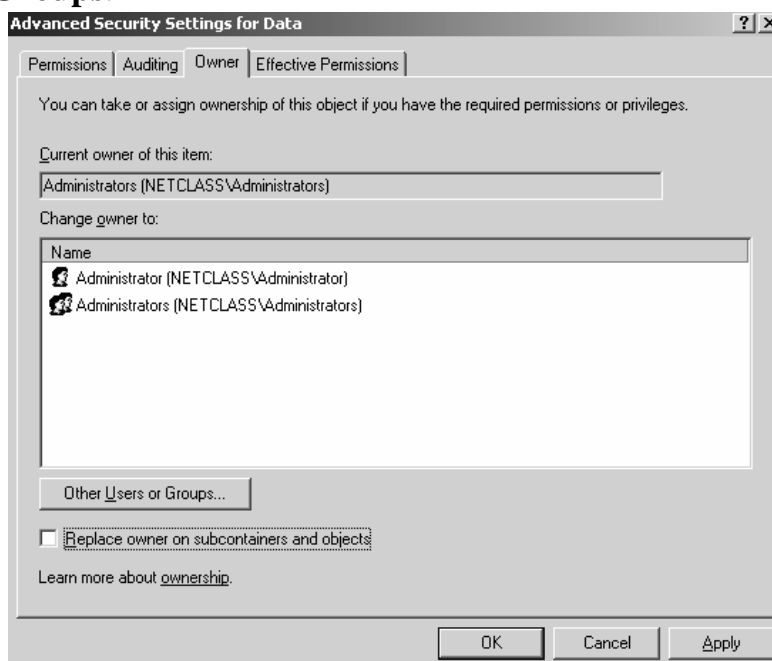
Bạn muốn giám sát và ghi nhận lại các người dùng thao tác trên thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Auditing**, nhấp chuột vào nút **Add** để chọn người dùng cần giám sát, sau đó bạn muốn giám sát việc truy xuất

thành công thì đánh dấu vào mục **Successful**, ngược lại giám sát việc truy xuất không thành công thì đánh dấu vào mục **Failed**.



2.3.7. Thay đổi người sở hữu thư mục

Bạn muốn xem tài khoản người và nhóm người dùng sở hữu thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Owner**. Đồng thời bạn cũng có thể thay đổi người và nhóm người sở hữu thư mục này bằng cách nhấp chuột vào nút **Other Users or Groups**.



2.4. DFS

DFS (Distributed File System) là hệ thống tổ chức sắp xếp các thư mục, tập tin dùng chung trên mạng mà **Server** quản lý, ở đó bạn có thể tập hợp các thư mục dùng chung nằm trên nhiều **Server** khác nhau trên mạng với một tên chia sẻ duy nhất. Nhờ hệ thống này mà người dùng dễ dàng tìm kiếm một tài nguyên dùng chung nào

đó trên mạng... **DFS** có hai loại **root**: **domain root** là hệ thống **root** gắn kết vào **Active Directory** được chứa trên tất cả **Domain Controller**, **Stand-alone root** chỉ chứa thông tin ngay tại máy được cấu hình. Chú ý **DFS** không phải là một **File Server** mà nó là chỉ là một “bảng mục lục” chỉ đến các thư mục đã được tạo và chia sẻ sẵn trên các **Server**. Để triển khai một hệ thống **DFS** trước tiên bạn phải hiểu các khái niệm sau:

- Gốc **DFS (DFS root)** là một thư mục chia sẻ đại diện cho chung cho các thư mục chia sẻ khác trên các **Server**.
- Liên kết **DFS (DFS link)** là một thư mục nằm trong **DFS root**, nó ánh xạ đến một tài nguyên chia sẻ các **Server** khác.

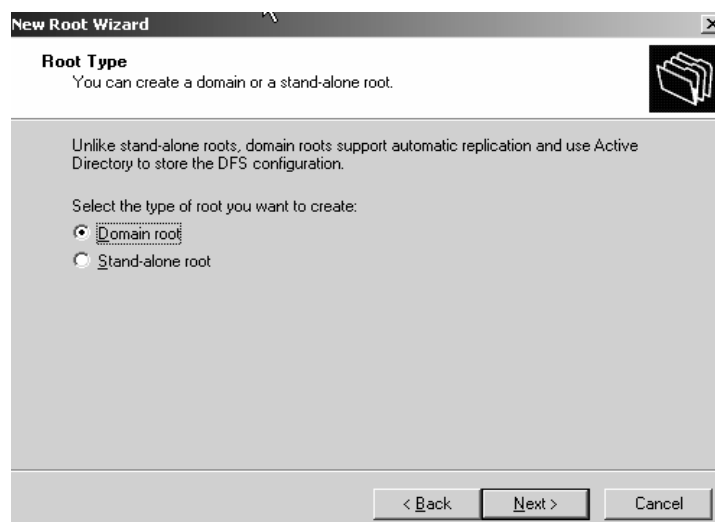
2.4.1. So sánh hai loại DFS

Stand-alone DFS	Fault-tolerant DFS
<ul style="list-style-type: none"> - Là hệ thống DFS trên một máy Server Stand-alone, không có khả năng dung lỗi. - Người dùng truy xuất hệ thống DFS thông qua đường dẫn \\servername\dfsname. 	<ul style="list-style-type: none"> - Là hệ thống DFS dựa trên nền Active Directory nên có chính dung lỗi cao. - Hệ thống DFS sẽ tự động đồng bộ giữa các Domain Controller và người dùng có thể truy xuất đến DFS thông qua đường dẫn \\domainname\dfsname.

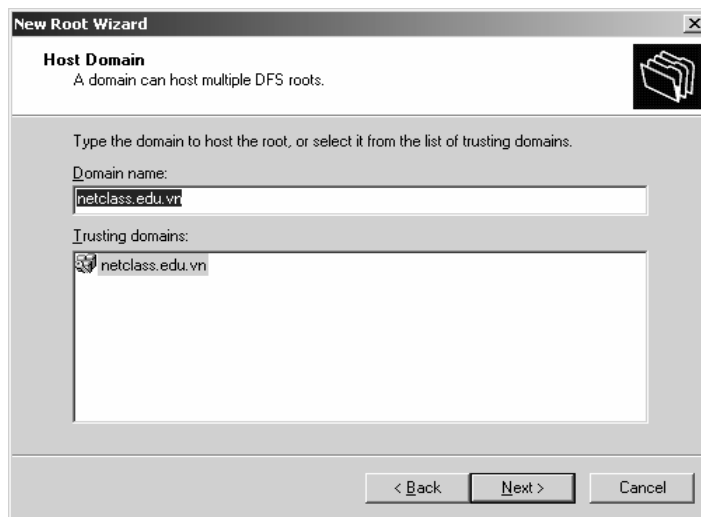
2.4.2. Cài đặt Fault-tolerant DFS

Để tạo một hệ thống **Fault-tolerant DFS** bạn làm theo các bước sau:

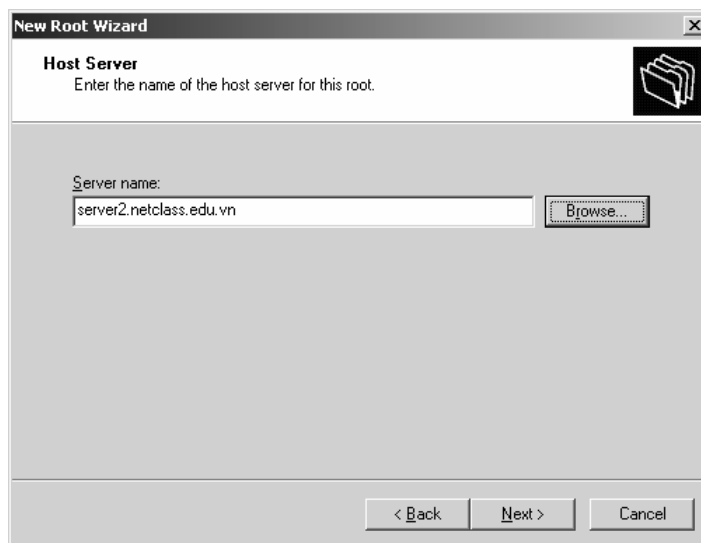
Bạn nhấp chuột vào **Start** □ **Programs** □ **Administrative Tools** □ **Distributed File System**. Hộp thoại **Welcome** xuất hiện, bạn nhấn **Next** để tiếp tục. Hộp thoại **Root Type** xuất hiện, bạn chọn mục **Domain Root**, nhấn **Next** để tiếp tục.



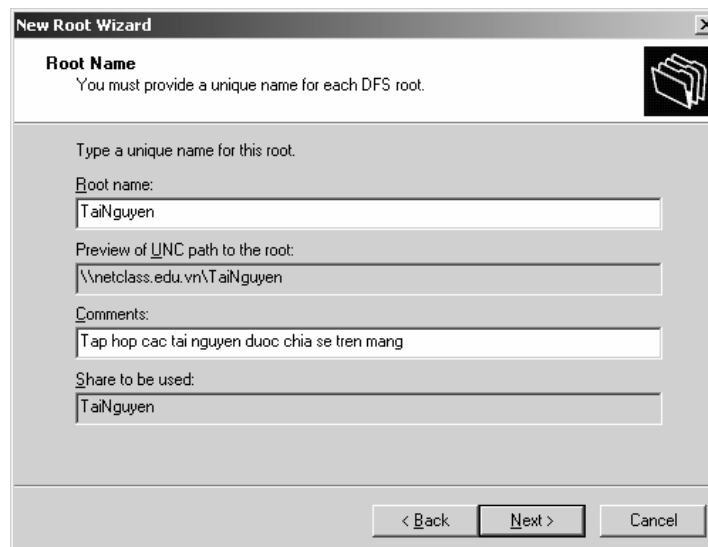
Hệ thống yêu cầu bạn chọn tên miền (**domain name**) kết hợp với hệ thống **DFS** cần tạo.



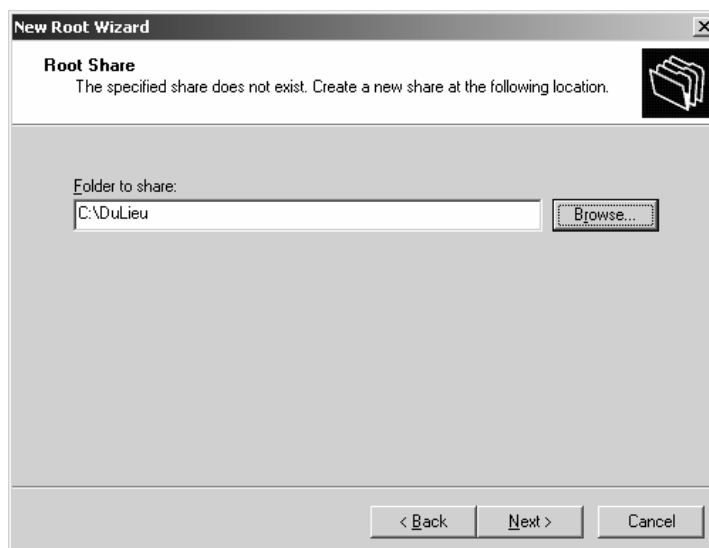
Tiếp theo bạn khai báo tên của **Domain Controller** chứa **root DFS** cần tạo.



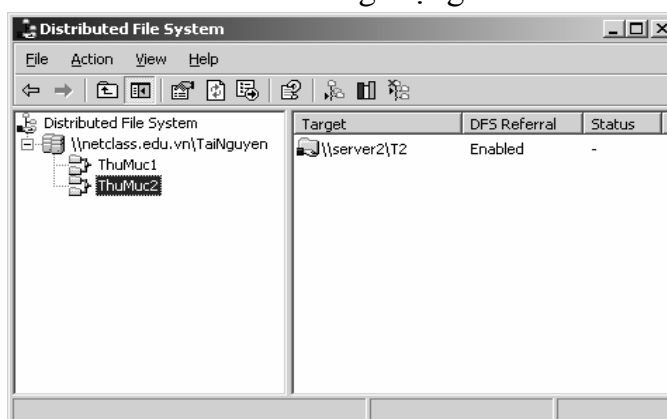
Đến đây bạn khai báo tên chia sẻ gốc (**Root Name**) của hệ thống **DFS**, đây chính là tên chia sẻ đại diện cho các tài nguyên khác trên mạng. Bạn nhập đầy đủ các thông tin chọn **Next** để tiếp tục.



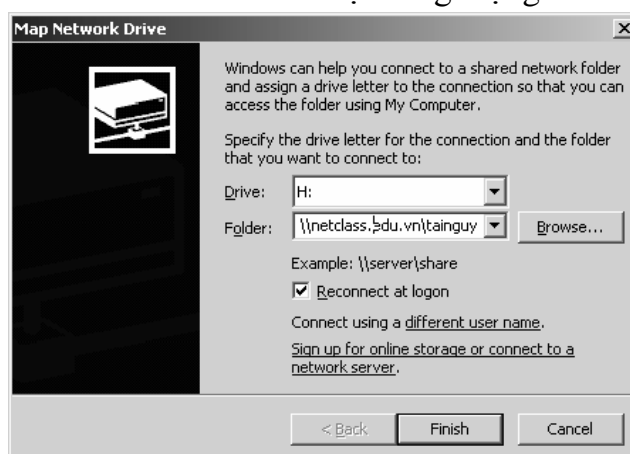
Trong hộp thoại xuất hiện, bạn khai báo tên thư mục chia sẻ gốc của hệ thống **DFS**.



Sau khi cấu hình hệ thống **DFS** hoàn tất, tiếp theo bạn tạo các liên kết đến các tài nguyên dùng chung trên các **Server** khác trong mạng.



Để sử dụng hệ thống **DFS** này, tại máy trạm bạn ánh xạ (**map**) thư mục chia sẻ gốc thành một ổ đĩa mạng. Trong ổ đĩa mạng này bạn có thể nhìn thấy tất cả các thư mục chia sẻ trên các **Server** khác nhau trên hệ thống mạng.



Tương tự như **Fault-tolerant DFS**, bạn có thể tạo ra một **Stand-alone DFS** trên một máy **Server Stand-alone**, tất nhiên là hệ thống đó không có khả năng dung lỗi có nghĩa là khi **Server** chứa **DFS Root** hỏng thì các máy trạm sẽ không tìm thấy các tài nguyên chia sẻ trên các **Server** khác. Nhưng hệ thống **Stand-alone DFS** được sử dụng rộng rãi vì nó đơn giản, tiện dụng.

Bài tập thực hành của học viên

1. Tạo thư mục có tên Personal trên ổ đĩa bất kỳ.
2. Chia sẻ và phân quyền truy cập thư mục này.

Hướng dẫn trả lời:

1. Tạo thư mục có tên Personal trên ổ đĩa bất kỳ.

Mở ổ đĩa cần tạo folder để share, ở đây tôi chọn là ổ C, các bạn có thể tùy chọn một ổ đĩa khác bất kỳ, **right click** chọn **new**, chọn **folder**, và đặt tên cho folder này là **personal**



2. Chia sẻ và phân quyền truy cập thư mục này.

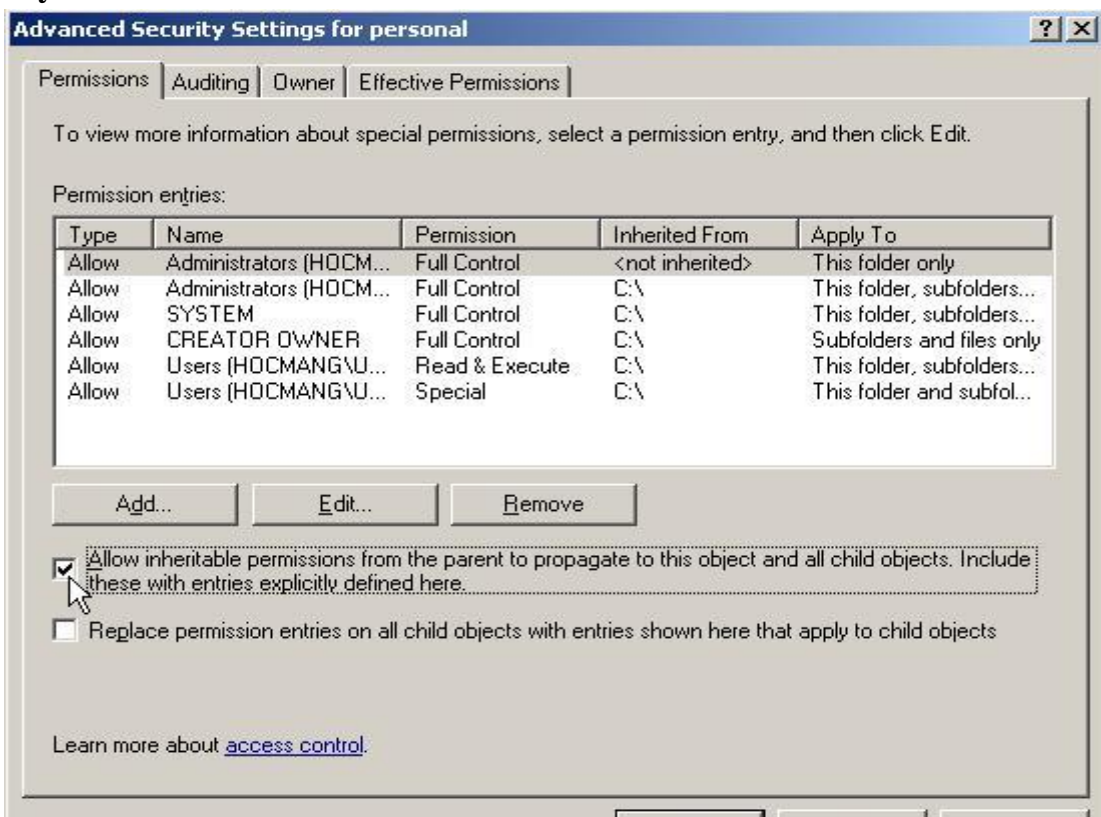
Ta sẽ cấu hình một số thuộc tính của **folder** này, right click vào **folder** này, chọn **properties**, hộp thoại **personal properties** xuất hiện:



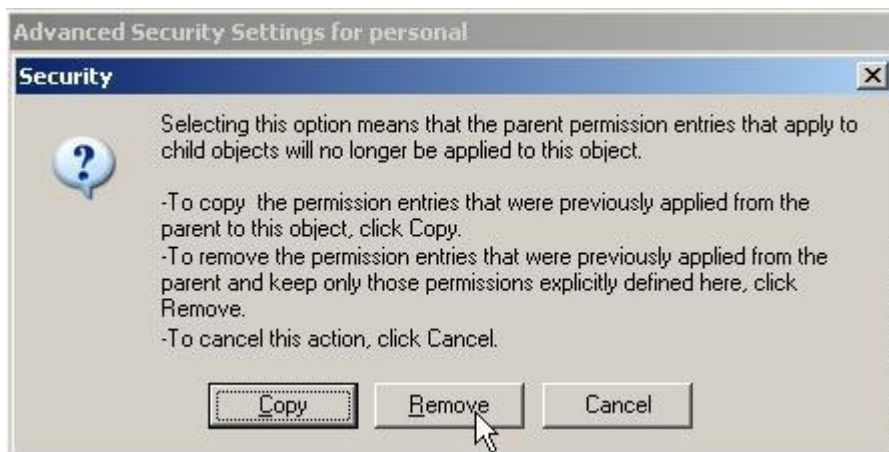
Click vào tab **Security** để cấu hình **NTFS permission** trên folder này. Trên tab Security, click nút **Advanced**



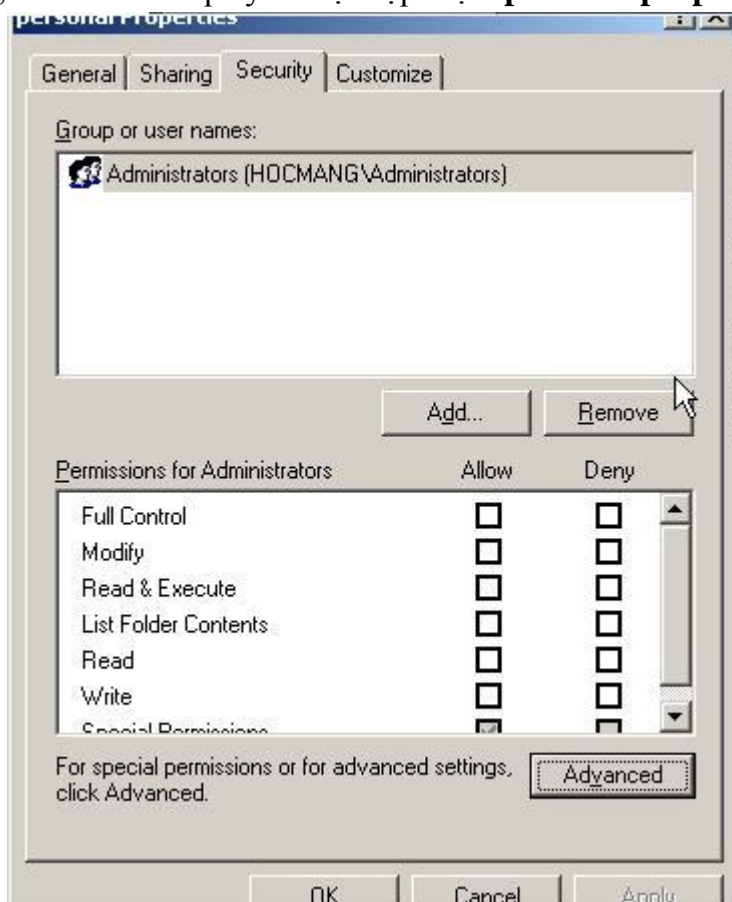
Trong hộp thoại **Advanced Security Setting for personal**, bạn ngắt quyền thừa hưởng bằng cách loại bỏ dấu check ra khỏi mục **Allow inheritable permissions from the parent to propagate to this object and all child object. Include these with entries explicitly defined here.**



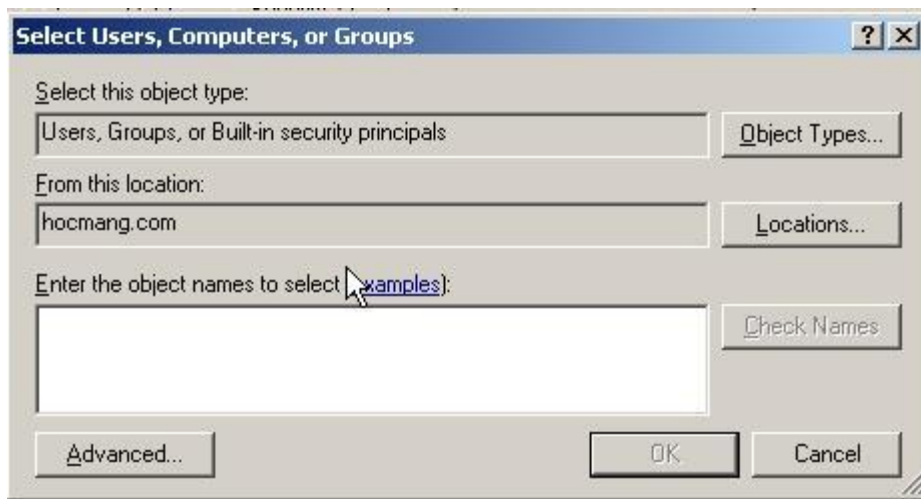
Trên hộp thoại **Security**, click nút **Remove** để loại bỏ tất cả các quyền thừa hưởng



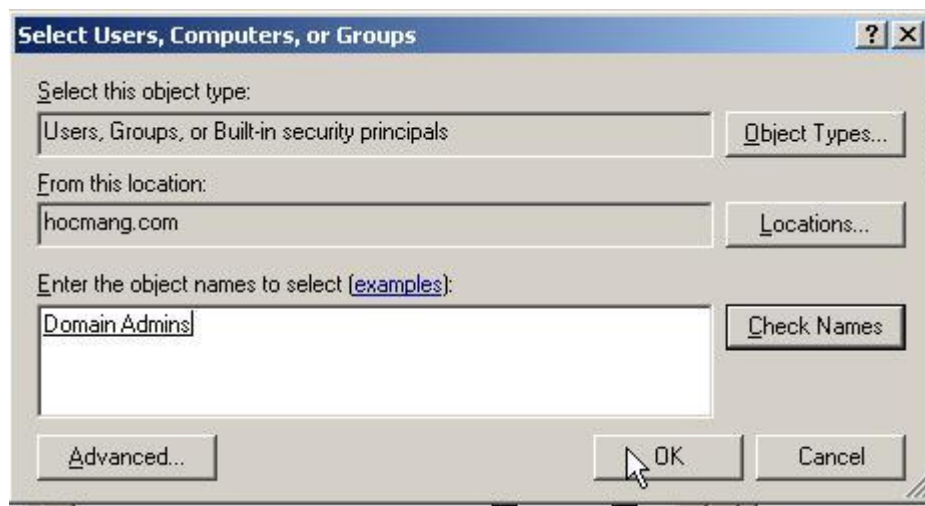
Xong nhấn **apply**, nhấn **OK** để quay về hội hộp thoại **personal properties**



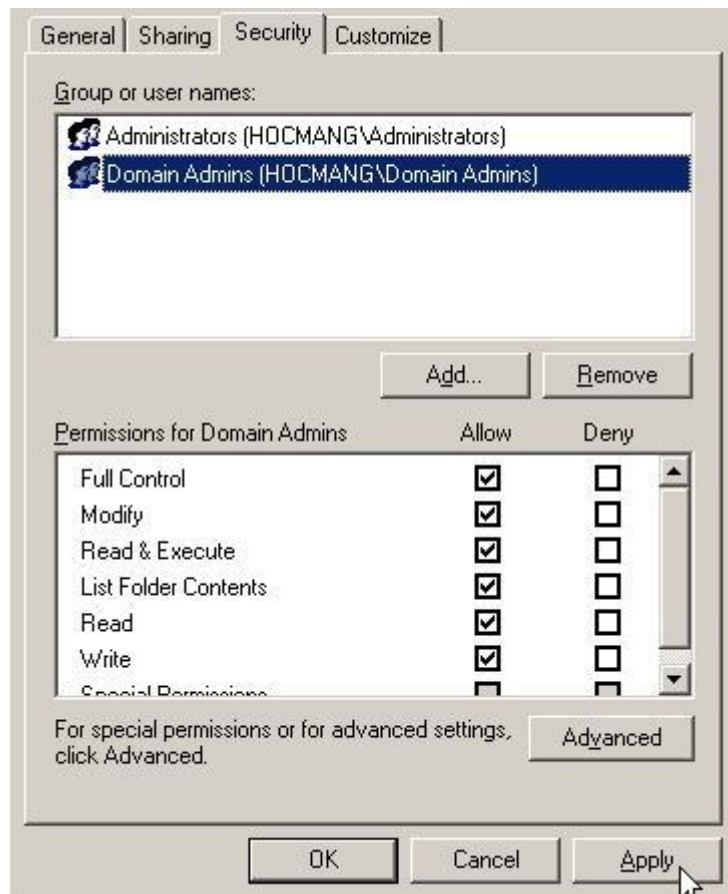
Trong hộp này các bạn nhấn **add**, sẽ xuất hiện hộp thoại **Select user, computer, or groups**



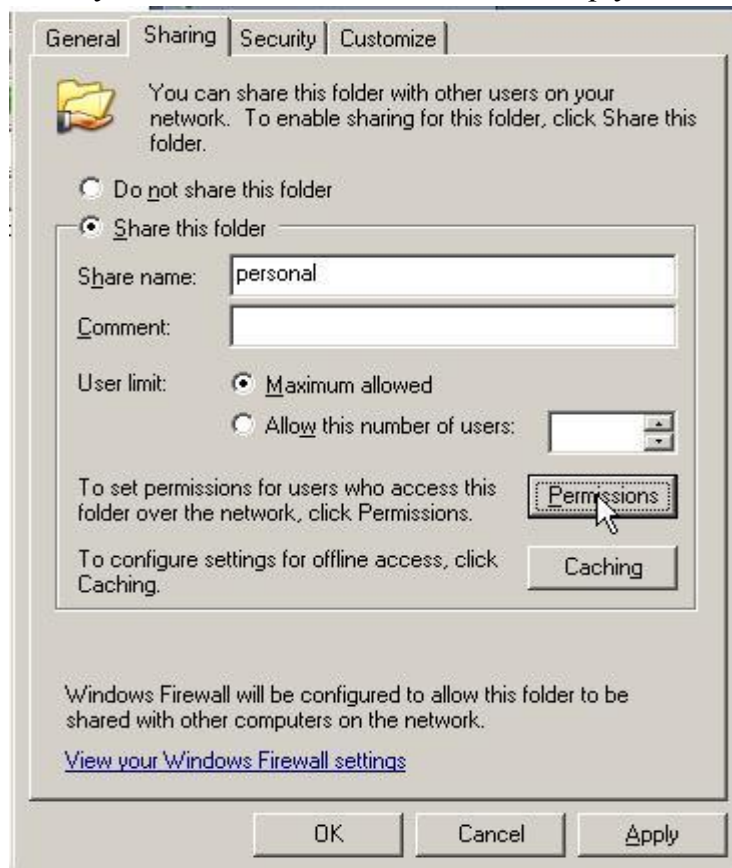
Nhập vào hộp text **Enter the object names to select (examples):** group **Domain Admins** rồi click vào nút **check names**. Group **Domain Admins** sẽ được gạch dưới, click **ok**



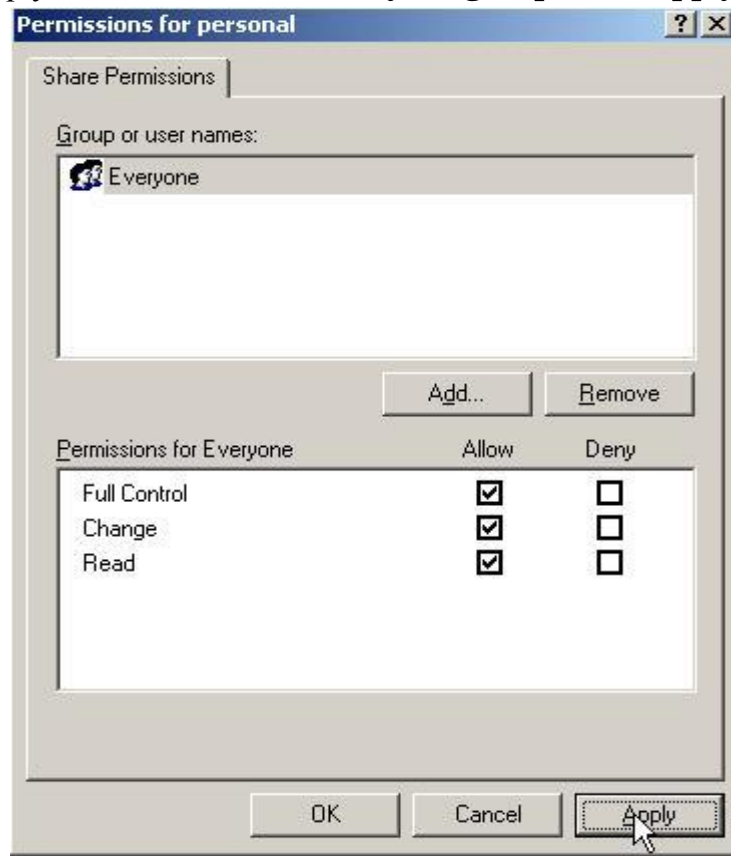
Trong hộp thoại **Personal Properties**, cấp quyền **Full Control** cho group **Domain Admins** bạn mới thêm vào. Click **apply**



Sau đó di chuyển qua tab **sharing**, trên tab **sharing**, đánh dấu chọn vào mục **share this folder** để share folder này. Click vào nút **Permission** để ấn quyền share cho folder



Trong hộp thoại **permission for personal**, đánh dấu chọn vào mục **Full Control** trong cột **Allow** để cấp quyền **full control** cho **everyone group**. Click **apply** rồi click **ok**.



Click apply và rồi click ok để đóng hộp thoại Personal Properties

Bài 7: DỊCH VỤ DHCP VÀ WINS

Giới thiệu

Theo định nghĩa của Microsoft thì "*Dynamic Host Configuration Protocol (DHCP) là một chuẩn IP được thiết kế để giảm tính phức tạp cho các cấu hình địa chỉ IP quản trị*". Một server DHCP có thể được cài đặt với các thông số thiết lập phù hợp theo mạng cung cấp. Các thông số thiết lập đó là một tập hợp các tham số như gateway, DNS, subnet mask và một loạt địa chỉ IP. Khi đã dùng DHCP trên mạng, quản trị viên không cần phải cấu hình các thiết lập riêng biệt cho từng client. DHCP sẽ tự động phân phối chúng.

WINS (là từ viết tắt của Windows Internet Name Service) là dịch vụ phân giải tên, có chức năng là phân giải tên máy tính thành địa chỉ IP cho phép các máy tính trên mạng tìm thấy nhau và truyền tải thông tin... được triển khai trong Internal Network Domain, nó sẽ phục vụ các Computer trong Network giải quyết để tìm NetBIOS names lẫn nhau..

1. Mục tiêu:

- Mô tả được sự hoạt động của dịch vụ DHCP và WINS;
- Cài đặt và cấu hình được dịch vụ DHCP và WINS.
- Thực hiện các thao tác an toàn với máy tính.

2. Nội dung chính:

2.1 Dịch vụ DHCP

Mục tiêu:

- *Trình bày được khái niệm DHCP.*
- *Cài đặt được dịch vụ DHCP.*
- *Cấu hình được máy phục vụ DHCP.*

2.1.1. DHCP (Dynamic Host Configitaton Protocol) là gì, tại sao phải dùng DHCP?

Một máy tính hay thiết bị khác phải được cấu hình theo một tham số trước khi có thể hoạt động trên một mạng. Ta phải cấu hình các tham số như tên lĩnh vực và địa chỉ IP của hệ khách, địa chỉ IP của hệ phục vụ DNS để phân giải tên của hệ chủ và mặt nạ con. Không có các tham số cấu hình này, một máy tính hay thiết bị khác không thể tương tác với các thiết bị khác trên mạng. Ngày nay hầu hết các mạng TCP/IP đều sử dụng DHCP để tự động cấp các địa chỉ IP và các tham số cho hệ khách. Khi đã cài đặt DHCP, bạn sẽ dựa vào máy phục vụ DHCP để cung cấp thông tin cơ bản cần thiết cho hoạt động nối mạng TCP/IP: địa chỉ IP, mặt nạ mạng con, bộ định tuyến mặt định, máy phục vụ DNS chính và phụ, máy phục vụ WINS chính và phụ, tên vùng DNS.

DHCP được thiết kế nhằm đơn giản hoá các tác vụ quản trị của vùng AD. DHCP được dùng để gán thông tin cấu hình. cho máy khách mạng, như vậy không những tiết kiệm được thời gian trong giai đoạn lập cấu hình. hệ thống mà còn cung cấp cơ chế tập trung cập nhật cấu hình.. DHCP cho phép chi phối hoạt động gán địa chỉ IP tại điểm tập trung.

2.1.2. Các bước cài đặt DHCP

- a. Vào **Start**→**Settings**→**Control Panel** bạn nhấn chuột vào **Add/Remove Programs**

- b. Trong hộp thoại **Add/Remove Programs** bạn nhấn chuột vào **Add/Remove Windows Components**.
- c. Trong hộp thoại ta di chuyển con trỏ tới **Networking Services** và sau đó bạn nhấn chuột vào nút **Details....**
- d. Bạn nhấn chuột vào ô **Dynamis Host Configutation Protocol (DHCP)** rồi **Ok** cuối cùng là bạn chọn **Next** 2 lần.
- e. Bây giờ bạn đã cài đặt xong dịch vụ DHCP.

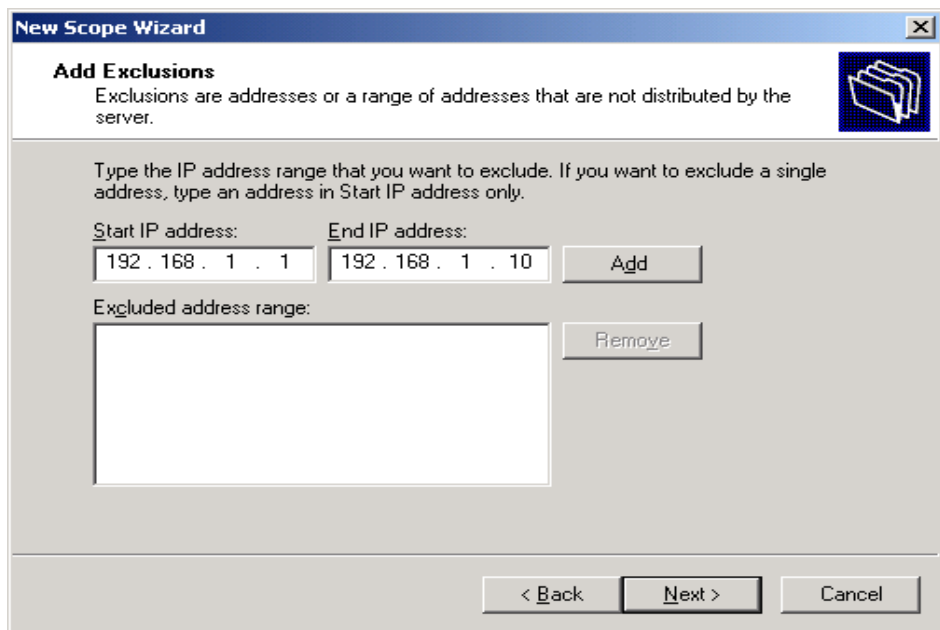
2.1.3. Cấu hình dịch vụ DHCP

- a. Vào **Start**→**Settings**→ **Programs**→**Administrative Tools**→**DHCP**. Hộp thoại xuất hiện bạn nhấn chuột vào **Action**, bạn chọn **New Scope...** Hộp thoại New Scope Wizard xuất hiện, bạn nhấn **Next**.
- b. Hộp thoại xuất hiện bạn nhập tên máy vào mục **Name** và nhấn **Next**.
- c. Hộp thoại xuất hiện bạn nhập địa chỉ số IP cấp phát tự động cho các máy trạm vào các ô sau: **Start Address** (địa chỉ IP đầu tiên), **End Address** (địa chỉ IP cuối cùng) và **Subnet Mask** cho khoảng IP tương ứng. Nhấn **Next** để tiếp quá trình cấu hình. dịch vụ này

The screenshot shows the 'New Scope Wizard' dialog box with the 'IP Address Range' step selected. The title bar reads 'New Scope Wizard'. Below the title bar, the text says 'IP Address Range' and 'You define the scope address range by identifying a set of consecutive IP addresses.' There is a folder icon on the right. The main area contains the instruction 'Enter the range of addresses that the scope distributes.' followed by input fields for 'Start IP address' (192.168.1.1) and 'End IP address' (192.168.1.100). Below that, it explains 'A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.' There are input fields for 'Length' (24) and 'Subnet mask' (255.255.255.0). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

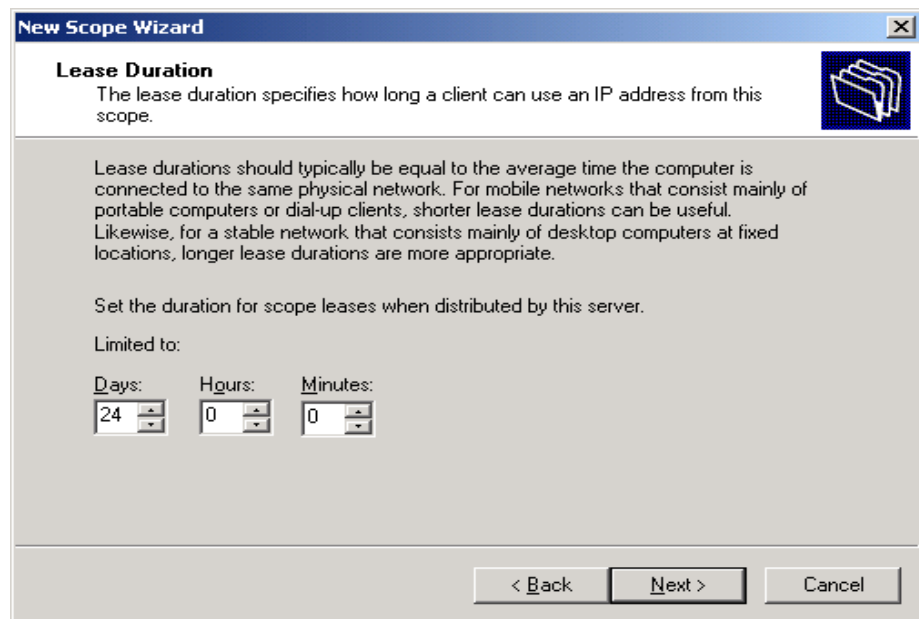
Hình 7.1 Trang IP Address Range, nhập phạm vi các địa chỉ IP sẽ cung cấp

- d. Hộp thoại xuất hiện bạn nhập địa chỉ số IP cấp phát cho những máy mà bạn định nhập tình loại ra trong số IP động như sau: **Start Address** (địa chỉ IP đầu tiên), **End Address** (địa chỉ IP cuối cùng) rồi nhấn **Add** và bạn cũng có thể từng địa chỉ vào mục **Start Address** sau đó nhấn **Add** nếu bạn đã nhập xong thì nhấn **Next**.



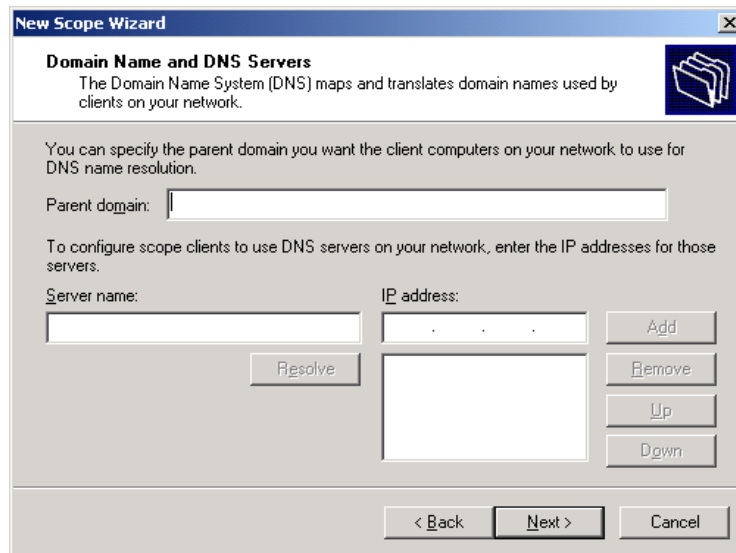
Hình 7.2 Phạm vi các IP đặc biệt không được phân phối

- e. Hộp thoại xuất hiện bạn nhập chỉ ra thời gian mà địa chỉ IP động sử dụng, lúc đầu máy quy định cho bạn là 8 ngày, bạn có thể sửa đổi vào các mục sau: Days (số ngày), Hours (giờ) và Minutes (phút). Nếu bạn muốn không giới hạn thì chọn tất cả là 0. Chọn rồi nhấn Next.



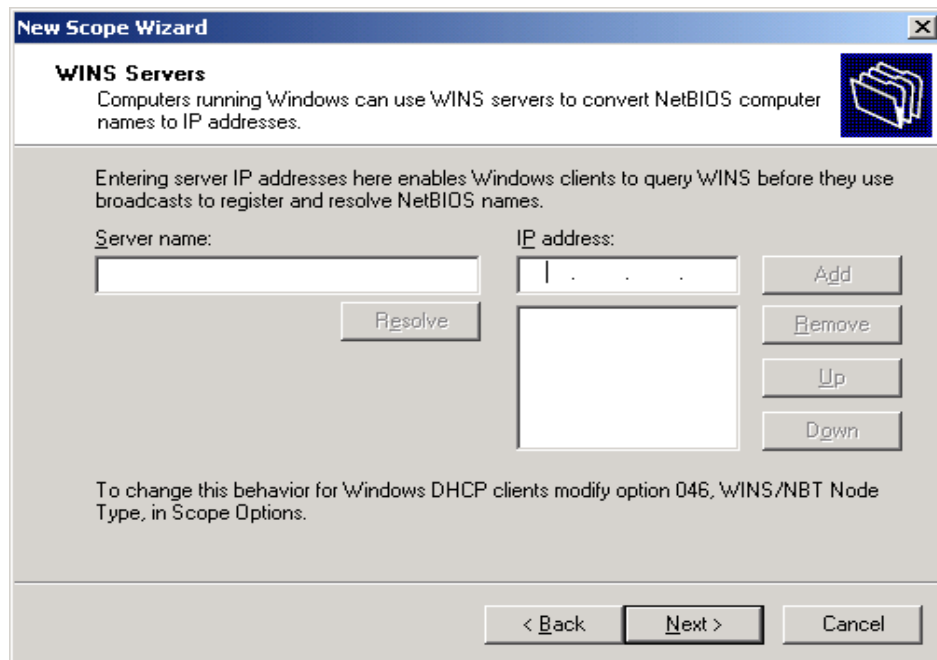
Hình 7.3 Thời hạn máy khách có thể sử dụng địa chỉ IP

- f. Hộp thoại xuất hiện hỏi bạn là muốn chỉ ra các dịch vụ khác cho các máy trạm như: DNS, WINS, ...nếu bạn muốn thì chọn Yes rồi nhấn Next để tiếp tục cấu hình., ngược lại thì chọn No.
- g. Hộp thoại xuất hiện bạn nhập chỉ vào IP Address của Router (Default Gateway) rồi nhấn Add, Next.
- h. Hộp thoại xuất hiện bạn nhập tên Domain và Server của DNS vào hai mục *Parent Domain* và *Server name*, địa chỉ IP của máy DNS vào *IP Address*, nhấn Add, Next.



Hình 7.4 Nhập Domain và Server name

- i. Hộp thoại xuất hiện để bạn nhập tên server của WINS vào *Server name*, địa chỉ IP vào *IP Address*, nhấn *Add*, *Next*.

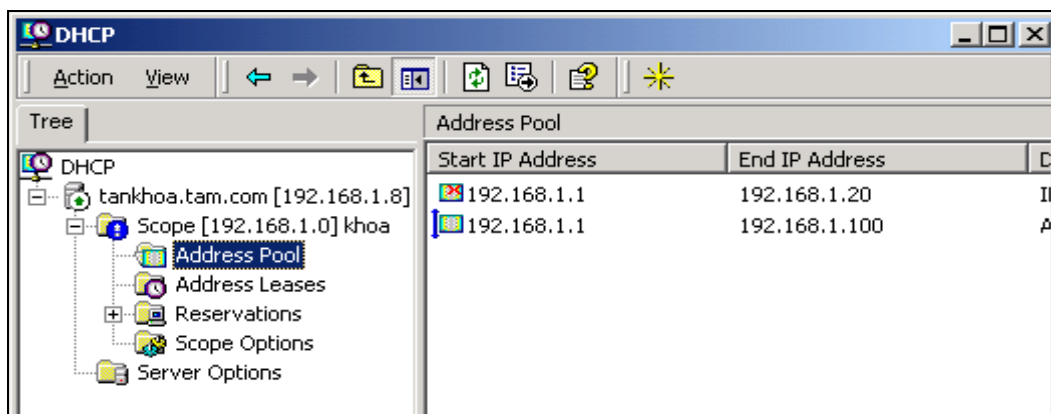


Hình 7.5 Tên máy phục vụ (Server name) có cài dịch vụ WINS

- j. Trong hộp thoại New Scope Wizard muốn khởi động DHCP ngay hãy chọn *Yes*, nhấn *Next* và *Finish*..

2.1.4. Kiểm tra dịch vụ DHCP trên Server

Để kiểm tra dịch vụ DHCP cấu hình có bị lỗi không bạn mở cửa sổ DHCP lên nếu bạn thấy biểu tượng có màu xanh là bạn đã cấu hình đúng.



Hình 7.6 Address Pool có màu xanh lá cây khi đặt dịch vụ DHCP đúng

2.1.5. Cấu hình IP động cho máy Client

Mục tiêu: bạn đã cấu hình xong dịch vụ DHCP, phần này sẽ hướng dẫn bạn cấu hình tất cả máy client để nhận IP Address và đăng ký với DHCP server.

1.5.1. Cách cấu hình địa chỉ động trong cửa sổ *Local Area Connection Properties*

- + Bước 1: Đăng nhập vào một máy cài Win2kPro
- + Bước 2: Trong cửa sổ *Control Panel*, chọn *Network and Dial-Up Connection*.
- + Bước 3: Nhấp phải chuột vào mục *Local Area Connection*, chọn *Properties*.
- + Bước 4: Trong hộp thoại *Internet Protocol (TCP/IP) Properties*, chọn *Obtain an IP Address automatically*.

1.5.2. Cách kiểm tra địa chỉ IP được cấp phát cho máy tính

Thực hiện kiểm tra địa chỉ động được cấp phát như sau:

- + Bước 1: Vào *Start-> Run*, nhập *cmd* rồi *Enter*, cửa sổ DOS xuất hiện.
- + Bước 2: Gõ *ipconfig /all | more*.

Gõ lệnh *ping* địa chỉ IP của một máy bất kỳ để kiểm tra thông mạng.

2.2. Dịch vụ WINS

Mục tiêu:

- Trình bày được khái niệm dịch vụ WINS.
- Cài đặt được dịch vụ WINS.
- Cấu hình được máy phục vụ WINS.

2.2.1. Giới thiệu dịch vụ WINS

Microsoft Windows Internet Nameing Service (WINS) là dịch vụ phân giải tên, có chức năng phân giải tên máy tính thành địa chỉ IP cho phép các máy tính trên mạng tìm thấy nhau và truyền tải thông tin. WINS hoạt động tốt nhất trong môi trường máy khách /máy phục vụ (Client/Server), nơi máy khách WINS gửi yêu cầu phân giải tên máy phục vụ WINS, đến phiên mình máy phục vụ WINS sẽ phân giải yêu cầu và hồi đáp. Máy tính sử dụng NetBIOS để truyền tải yêu cầu và hồi đáp. Máy tính sử dụng NetBIOS cung cấp API cho phép máy tính trên mạng giao tiếp với nhau. Khi cài đặt giao thức mạng TCP/IP trên máy phục vụ hay máy khách, NetBIOS over TCP/IP (NBT) cũng đồng thời được cài đặt NBT là dịch vụ thuộc tầng Session, cho phép chương trình ứng dụng NetBIOS dựa vào WINS hay tập tin LMHOSTS cục bộ để phân giải tên máy tính thành địa chỉ IP. Trên mạng chạy hệ điều hành trước Windows 2000, WINS là dịch vụ phân giải tên chủ yếu. Ở mạng Windows 2000, vai trò này thuộc về DNS, WINS có vai trò khác, đó là cho phép

hệ thống trước Windows 2000 duyệt danh sách tài nguyên trên mạng và cho phép hệ thống Windows 2000 định vị tài nguyên NetBIOS. Trong Microsoft Windows 2000, WINS không được tự động cài đặt khi bạn cài hệ điều hành. Muốn dùng WINS bạn phải cài đặt .

2.2.2. Cài đặt WINS

Các bước cài đặt:

- + Bước 1: Nhấp Stars->Setting->Control Panel
- + Bước 2: Nhấp đúp biểu tượng Add/Remove Programs.
- + Bước 3: Nhấp Add/Remove Windows Components, nhấp next.
- + Bước 4: Trong phần Components Networking Services chọn WINS.

2.2.3. Cấu hình máy chủ và máy khách với WINS

Để kích hoạt cơ chế phân giải tên **WINS** trên mạng, bạn phải lập cấu hình. máy phục vụ và máy khách **WINS**, nhớ khai báo địa chỉ IP của các máy phục vụ **WINS** trên mạng cho máy khách biết. Dựa vào địa chỉ IP này máy khách có thể giao tiếp với máy phục vụ **WINS** ở bất cứ đâu trên mạng, cho dù máy phục vụ đang thường trú trên mạng con khác. Máy khách **WINS** còn giao tiếp thông qua phương pháp broadcast, trong đó máy khách phát rộng thông điệp đến những máy khác trên đoạn mạng cục bộ đang yêu cầu cấp địa chỉ IP. Do thông điệp được phát rộng nên máy phục vụ **WINS** coi như “ngồi chơi xơi nước”. Máy khách nào không cài **WINS** nhưng có hỗ trợ loại hình phát rộng thông điệp cũng có thể vận dụng phương pháp này phân giải tên máy tính thành địa chỉ IP.

Khi máy khách giao tiếp với máy phục vụ **WINS**, chúng thiết lập phiên giao tiếp có ba phiên chủ yếu:

- + **Đăng ký tên:** Suốt tiến trình đăng ký tên, máy khách cung cấp tên máy tính và địa chỉ IP của nó cho máy phục vụ và yêu cầu máy phục vụ đưa thông tin này vào cơ sở dữ liệu WINS,

- + **Gia hạn tên:** Tên đăng ký không có hiệu lực vĩnh viễn. Thay vào đó, máy khách chỉ được phép sử dụng tên trong một giai đoạn cụ thể, gọi là thời gian thuê bao (lease). Máy khách còn được quy định thời gian bắt buộc phải gia hạn tên thuê bao, gọi là chu kỳ gia hạn (renewal interval). Máy khách phải đăng ký lại với máy phục vụ WINS theo chu kỳ gia hạn đã ấn định.

- + **Giải phóng tên:** Nếu máy khách không thể gia hạn tên thuê bao, tên đăng ký sẽ được giải phóng, cho phép hệ thống khác trên cùng mạng có cơ hội sử dụng tên máy tính hay địa chỉ IP này. Tên cũng được giải phóng khi bạn đóng máy khách **WINS** bất kỳ.

- + **Các phương pháp phân giải tên**

Khi máy khách thiết lập phiên giao tiếp với máy phục vụ WINS, máy khách có thể yêu cầu cung cấp dịch vụ phân giải tên. Áp dụng phương pháp nào để phân giải tên máy tính thành địa chỉ IP còn tùy thuộc vào cấu hình mạng. Có bốn phương pháp phân giải tên máy tính khả dụng:

- + **B-node:** Phát rộng thông điệp nhằm phân giải tên máy tính thành địa chỉ IP. Những máy tính cần phân giải tên sẽ phát rộng thông điệp đến từng máy chủ trên mạng cục bộ, yêu cầu cấp địa chỉ IP cho máy tính cụ thể.

+ **P-node**: Dùng máy phục vụ WINS phân giải tên máy tính thành địa chỉ IP. Như đã giải thích trước phiên máy khách gồm ba phần: đăng ký tên, gia hạn tên, và giải phóng tên. Khi cần phân giải tên máy tính thành địa chỉ IP, máy khách gửi thông điệp truy vấn máy phục vụ, đến phiên mình, máy phục vụ sẽ hồi đáp cho máy khách.

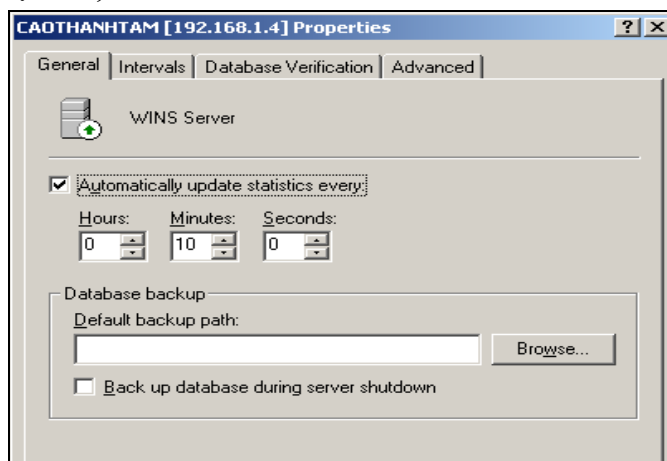
+ **M-node (Modified Node)**: Kết hợp giữa B-node và P-node, với M-node, máy khách WINS trước tiên sẽ thử dùng B-node phân giải tên. Nếu thất bại, máy khách lại dùng đến P-node. Do B-node được sử dụng trước, nên phương pháp này cũng gặp trở lại ở mức độ sử dụng dải thông mạng, hệt như B-node.

+ **H-node (Hybrid Node)**: Cũng kết hợp B-node và P-node nhưng ở đây máy khách WINS sẽ thử áp dụng P-node phân giải tên. Trường hợp thất bại, máy khách sẽ cố phát rộng thông điệp với B-node. Vì P-node là phương pháp chính nên H-node cung cấp hiệu suất thi hành tối ưu trên hầu hết mạng. H-node cũng là phương pháp mặc định cho hoạt động phân giải tên WINS.

2.2.3.1 Cấu hình máy phục vụ WINS

Khi cài đặt máy phục vụ **WINS** máy phục được lập cấu hình. với các xác lập mặc định, bạn có thể thay đổi xác lập mặc định:

1. Trong **console WINS**, nhấp nút phải chuột vào máy phục vụ cần làm việc, chọn **properties** mở hộp thoại sau,



Hình 7.7 Cấu hình máy phục vụ WINS

2. Thay đổi giá trị thuộc tính trên các trang **General**, **Interval**, **Database Verification**, **Advance**(tìm hiểu sau).

3. Nhấp **OK** khi xong việc.

2.2.3.2. Cấu hình máy khách WINS

1. Trên desktop, nhấp chuột phải vào My Network Place chọn Properties, nhấp phải vào Local Connection chọn Properties.

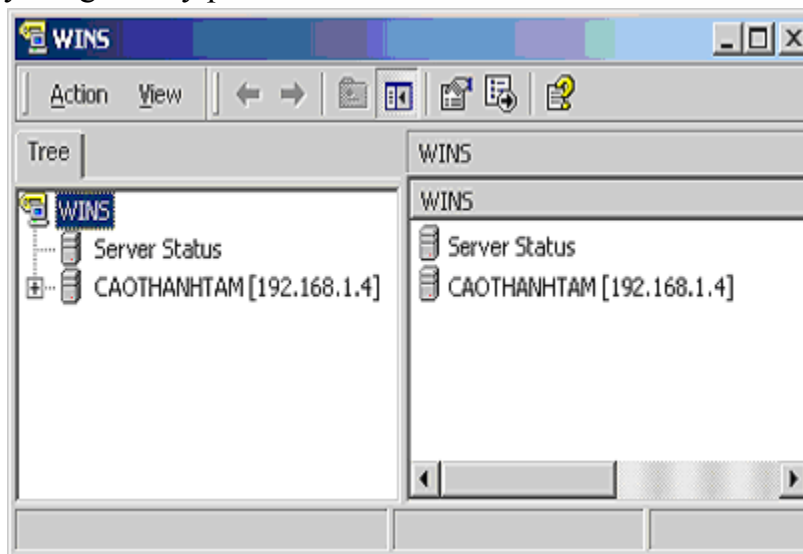
2. Nhấp đôi vào Internet Protocol(TCI/IP), Nhấp vào Advance, chọn WINS.

3. Chọn tiếp **Add**, nhập vào **IP** của **WINS server**, nhấp **Add**..

2.2.3.4. Bổ sung máy chủ WINS

Khi cài đặt máy phục vụ mới, máy này được lập cấu hình. với các xác lập mặc định. Bạn có thể xem và thay đổi xác lập mặc định bất cứ lúc nào thông qua **console WINS**. **Console WINS** truy cập từ thư mục **Administrative Tools (common)**, là nơi bạn quản lý

các máy phục vụ WINS trên mạng. Cửa sổ chính của console WINS; được chia thành hai khung. Khung bên trái liệt kê máy phục vụ WINS trong vùng theo địa chỉ IP, kể cả máy tính cục bộ, nếu đây cũng là máy phục vụ WINS.



Hình 7.8 Cấu hình máy phục vụ WINS

Nếu một máy phục vụ WINS cần lập cấu hình không có tên trong console WINS, tiến hành bổ sung vào console như sau:

- + Bước 1: Nhấp nút phải chuột vào **WINS** bên khung trái, chọn **Add Server**.
- + Bước 2: Gõ địa chỉ **IP** hay tên máy tính của máy phục vụ **WINS** được quản lý
- + Bước 3: Nhấp **OK**. Khung bên trái xuất hiện thêm mục nhập dành cho máy phục vụ WINS này.

2.2.3.5. Khởi động và ngừng WINS

Công tác quản lý máy phục vụ WINS được thực hiện qua Windows Internet Naming Service. Tương tự mọi dịch vụ khác, bạn có thể khởi động, ngừng hẳn hay tạm dừng tiếp tục chạy WINS trong thư mục Servers của Computer Management hay từ dòng lệnh.

Để quản lý máy phục vụ WINS thông qua Computer Management nhấp nút phải chuột vào WINS, chọn All Task, Start, Stop, Pause, Resume, Restart tùy tình huống. Cũng có thể quản lý WINS trong console WINS: Nhấp nút phải chuột vào “máy phục vụ” sẽ được quản lý trong console WINS chọn All Tasks, chọn tiếp Start, Stop, Pause, Resume, Restart, tùy tình huống.

2.2.3.6. Xem thống kê trên máy chủ:

Chức năng thống kê máy phục vụ cung cấp thông tin tóm tắt cho WINS, thuận tiện cho việc giám sát và xử lý lỗi ở WINS, để xem chỉ cần nhấp nút chuột vào máy phục vụ WINS trong console WINS, chọn **Display Server Statistics**

- + **Server Start Time:** Thời điểm WINS khởi động trên máy phục vụ.
- + **Database Initialized:** Thời điểm cơ sở dữ liệu WINS được khởi tạo.
- + **Statistics Last Cleared:** Thời điểm thông tin thống kê máy phục vụ được xóa lần cuối.
- + **Last Periodic Replication:** Thời điểm cơ sở dữ liệu WINS được sao chép lần cuối, dựa trên tần số sao chép quy định trong hộp thoại Pull Partner Properties.

+ **Last Manual Replication:** Thời điểm cơ sở dữ liệu WINS được nhà quản trị sao chép lần cuối.

+ **Last Net Update Replication:** Thời điểm cơ sở dữ liệu WINS được sao chép lần cuối dựa trên thông tin về hoạt động đẩy (push).

+ **Last Address Change Replication:** Thời điểm cơ sở dữ liệu WINS được sao chép lần cuối dựa trên thông điệp thay đổi địa chỉ.

+ **Total Queries:** Tổng số vấn tin (yêu cầu) máy phục vụ nhận được kể từ lần khởi động cuối cùng. Records Found cho biết số yêu cầu được giải quyết thành công. Records Not Found chỉ ra số yêu cầu thất bại.

+ **Total Release:** Tổng số thông điệp nhận được, cho biết có một chương trình ứng dụng NetBIOS đã giải phóng tên đăng ký của nó và tự đóng lại. Records Found chỉ ra số lần giải phóng thành công. Records Not Found biểu thị số lần giải phóng thất bại.

+ **Unique Registrations:** Tổng số thông điệp đăng ký tên nhận được từ máy khách WINS (và đã được duyệt). Conflicts nêu rõ số trường hợp trùng tên gặp phải đối với mỗi tên máy tính. Renewals cho biết số lần gia hạn nhận được cho từng tên máy tính không trùng lặp.

+ **Group Registrations:** Tổng số thông điệp đăng ký tên nhận được từ nhóm. Conflicts chỉ ra số lần trùng lặp đối với tên nhóm. Renewals cho biết số lần nhận được gia hạn cho tên nhóm.

+ **Total Registrations:** Tổng số thông điệp đăng ký tên nhận được từ máy khách.

+ **Last Periodic Scavenging:** Lần xoá cuối cùng xảy ra dựa trên tần số gia hạn ấn định trong hộp thoại **WINS Server Configuration**.

+ **Last Extinction Scavenging:** Lần xoá cuối cùng dựa trên tần số xoá trắng quy định trong hộp thoại **WINS Sever Configuration**.

+ **Last Verification Scavenging:** Lần xoá cuối cùng xảy ra dựa trên tần số kiểm tra định rõ trong hộp thoại **WINS Server Configuration**.

2.2.3.7. Cập nhật thông tin thống kê WINS

Mặc định, những thống kê WINS được cập nhật cứ 10 phút/ lần. Nếu muốn bạn có thể thay đổi tần số cập nhật hay ngừng hẳn đặc tính tự động cập nhật:

+ Trong **console WINS**, nhấp nút phải chuột vào máy phục vụ cần làm việc, chọn **properties**.

+ Nhấp thẻ(tab) **General**.

+ Ấn định tần số cập nhật: chọn **Automatically Update Statistics Every**, rồi gõ giá trị biểu thị tần số cập nhật.

+ Ngừng tự động cập nhật: xoá chọn **Automatically Update Statistics Every**. Nhấp **OK**

2.2.3.8. Quản lý hoạt động đăng ký, gia hạn và giải phóng tên

Tên máy tính được đăng ký trong cơ sở dữ liệu **WINS** theo khoảng thời gian cụ thể, gọi là thời gian thuê bao. Bằng cách quy định tần số gia hạn, xoá trắng và kiểm tra, bạn sẽ kiểm soát được nhiều phương diện của thuê bao tên.

+ Trong **console WINS**, nhấp chuột phải chọn máy phục vụ cần quản lý, chọn **properties**.

+ Chuyển sang trang **Interval**

+ **Renewal Interval:** Định rõ thời gian có hiệu lực của tên thuê bao, qua đó máy khách WINS bắt buộc phải gia hạn tên máy tính của mình. Thông thường máy khách sẽ cố gia hạn khi 50% thời hạn thuê bao đã trôi qua, giá trị tối thiểu là 40 phút. Giá trị mặc định là 6 ngày, có nghĩa máy tính sẽ cố gia hạn tên thuê bao 7 ngày/lần. Tên máy tính nào không gia hạn sẽ bị đánh dấu và được giải phóng (released).

+ **Extinction Interval:** Quy định thời hạn tên máy tính có thể bị đánh dấu là biến mất (extinct). Khi tên máy tính đã được giải phóng, bước kế tiếp là đánh dấu nó đã biến mất. Giá trị này phải lớn hơn hay bằng giá trị Renewal Interval, tức 4 ngày.

+ **Verification Interval:** Định rõ thời hạn sau đó một máy phục vụ WINS phải kiểm tra những tên cũ mà nó không sở hữu. Nếu tên không còn hoạt động, chúng có thể bị xoá, giá trị tối thiểu là 24 ngày. Thường thì, tên máy tính được đăng ký ở máy phục vụ WINS khác sẽ có chủ sở hữu khác, vì thế chúng được xếp vào hạng mục này.

2.2.3.9. Ghi nhận các sự kiện vào nhật ký sự kiện của Windows

Sự kiện **WINS** tự động được ghi nhận vào nhật ký sự kiện hệ thống. Mặc dù không thể vô hiệu hoá đặc tính này, bạn vẫn được phép kích hoạt tạm thời chế độ ghi nhật ký chi tiết, nhằm giúp xử lý lỗi **WINS**, cách làm như sau:

+ Trong Console WINS, nhấp nút phải chuột vào máy phục vụ cần làm việc, chọn Properties.

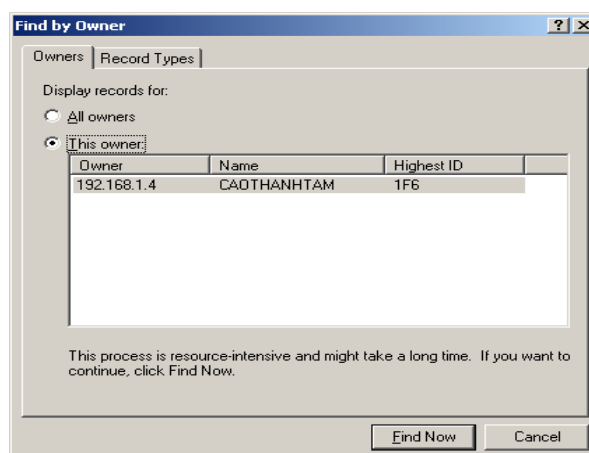
+ Mở trang Advanced, chọn Log Detail Events To These Windows Event Logs,

2.2.3.10. Chọn số hiệu phiên bản cho cơ sở dữ liệu WINS

Số hiệu phiên bản (version ID) dành cho cơ sở dữ liệu **WINS** tự động cập nhật khi thực hiện thay đổi cho cơ sở dữ liệu. Nếu cơ sở dữ liệu **WINS** đột nhiên bị hỏng, buộc phải phục hồi cơ sở dữ liệu qua mạng, bạn sẽ cần truy cập máy phục vụ **WINS** chính, định **version ID** ở giá trị cao hơn giá trị tương ứng trên mọi đối tác ở xa, muốn xem và thay đổi số hiệu phiên bản hiện hành:

+ Trong **Console WINS**, nhấp phải chuột vào **Active Registrations**, chọn **Find Owner** mở hộp thoại cùng tên.

+ Trên trang **Owners**, cột **Highest ID** chỉ rõ số hiệu phiên bản cao nhất đang dùng trên máy phục vụ. Giá trị này được ấn định theo dạng thức thập lục phân với giá trị tối đa là 2^{31}

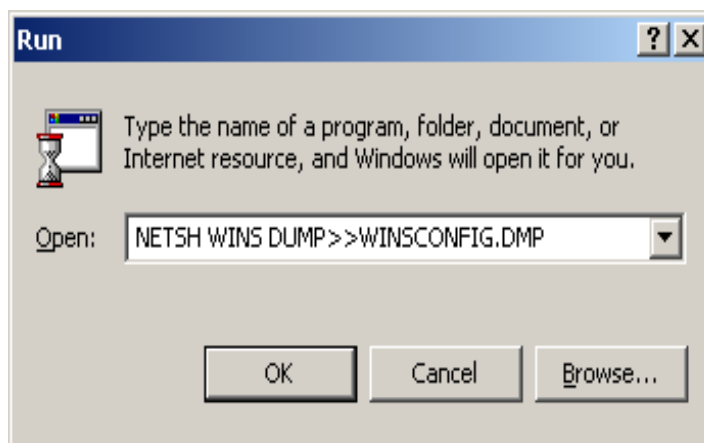


Hình 7.9 Cấu hình máy phục vụ WINS

- + Lưu ý giá trị **version** cao nhất, nhấp cancel .
- + Nhấp phải chuột vào mục nhập dành cho máy phục vụ **WINS** chính ở khung trái, chọn **Properties**.
- + Trên trang **Advance**, gõ giá trị mới vào trường **Starting Version ID**. Phải gõ giá trị này cho đúng thập lục phân và nhấp **OK**.

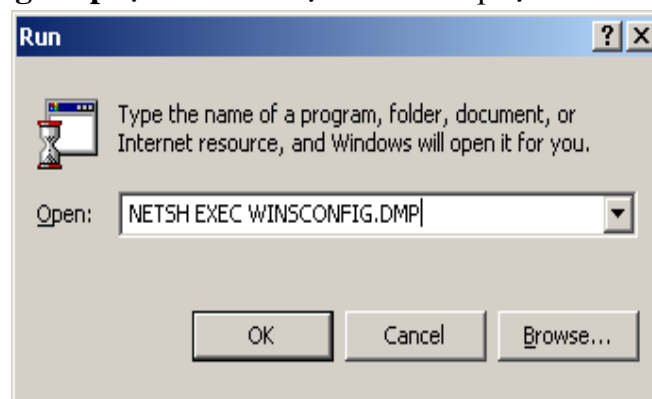
2.2.3.11. Lưu và phục hồi cấu hình WINS

Sau khi lập cấu hình **WINS** cần thiết hãy lưu thông tin cấu hình để sau này có thể phục hồi nó trên máy phục vụ **WINS**. Muốn thế, gõ **netsh WINS dump>>winsconfig.dmp** tại dấu nhắc lệnh,



Hình 7.10 Cấu hình máy phục vụ WINS

Ở ví dụ này, winsconfig.dmp là tên kịch bản cấu hình sẽ tạo. Tạo xong kịch bản, gõ **netsh exec winsconfig.dmp** tại dấu nhắc lệnh nếu cần phục hồi cấu hình.



Hình 7.11 Cấu hình máy phục vụ WINS

2.2.3.12. Quản lý cơ sở dữ liệu WINS

Bạn phải tích cực quản lý **WINS** hầu duy trì tính hiệu quả của hoạt động phân giải tên trên mạng. Những mục tiếp theo trình bày các tác vụ quản lý thông thường.

- Khảo sát kết quả ánh xạ trong cơ sở dữ liệu WINS

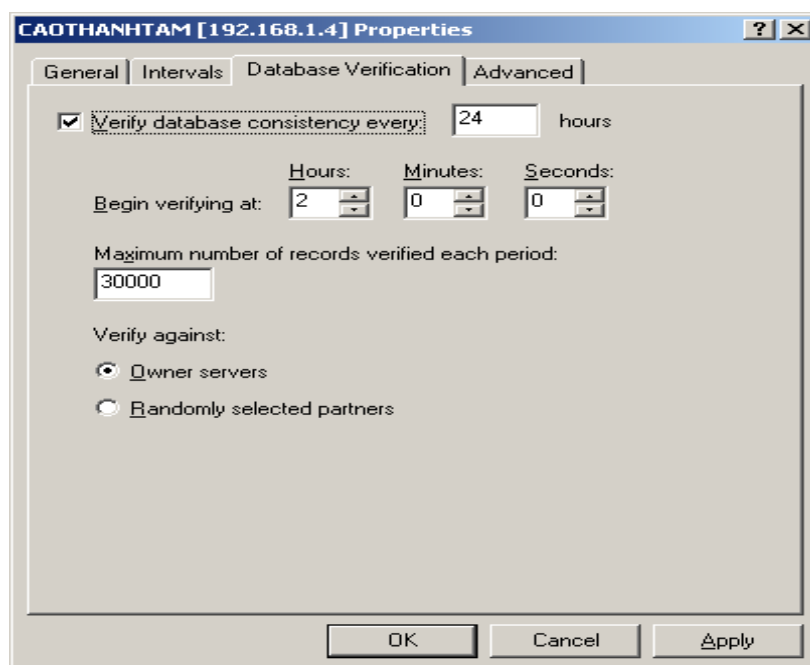
Khi thư mục **Active Registrations** được chọn ở khung bên trái, khung bên phải của console **WINS** sẽ liệt kê những mẫu tin bạn đã chọn xem. Mỗi mục nhập biểu thị một mẫu tin trong cơ sở dữ liệu **WINS**. Bên trái mục nhập xuất hiện một trong hai biểu tượng. Biểu tượng nhiều máy tính nêu rõ kết quả ánh xạ là tên nhóm, vùng, nhóm Internet. Ánh xạ còn cho biết thêm những thông tin sau đây:

- + **Record Name:** Tên **NetBIOS** hoàn chỉnh của máy tính, nhóm, hay dịch vụ đăng ký trong cơ sở dữ liệu .
- + **Type:** Loại mẫu tin phối hợp với kết quả ánh xạ này, như **00h Workstation**.
- + **IP Adress:** Địa chỉ IP phối hợp với kết quả ánh xạ.
- + **State:** Trạng thái của mẫu tin, chẳng hạn **Active** (hoạt động) hay **Released** (được giải phóng)
- + **Owner:** Địa chỉ IP của máy phục vụ WINS sở hữu mẫu tin.
- + **Version:** Số hiệu phiên bản của cơ sở dữ liệu nguồn, tức nơi mẫu tin tạo thành.
- + **Expiration:** Ngày/giờ hết hiệu lực kết quả ánh xạ, các ánh xạ tĩnh có xác lập Expiration là **Infinite**, có nghĩa chúng có hiệu lực vô thời hạn (trừ khi bị chùng hay xóa đi).

- Kiểm tra tính nhất quán của cơ sở dữ liệu WINS

Áp dụng cách sau để kiểm tra tính nhất quán của cơ sở dữ liệu:

- + Nhấp nút phải chuột lên máy phục vụ cần xử lý trong **console WINS**, chọn **Properties**,



Hình 7.12 Cấu hình máy phục vụ WINS

- + Trên trang **Database Verification**, chọn **Verify Database Consistency Every...** Gõ tần số kiểm tra ví dụ 24 giờ /lần hay 48 giờ /lần.

- + Ở trường **Begin Verify At**, gõ thời điểm bắt đầu kiểm tra, dựa vào chu kỳ 24 giờ. Nếu cần, định rõ giá trị **Maximum Number Of Records Verified Each Priod**. Giá trị mặc định là 30000.

Có thể kiểm tra mẫu tin dựa vào các máy phục vụ chủ sở hữu hay dựa vào những đối tác được chọn ngẫu nhiên. Phương pháp chọn ngẫu nhiên cho kết quả chính xác nhất trên mạng rất lớn, nơi bạn không thể kiểm tra toàn bộ mẫu tin trong chỉ một lần. Còn không thì hãy chọn **Owner Server** để kiểm tra mẫu tin trên máy phục vụ được chỉ định là chủ sở hữu mẫu tin.

- + Nhấp **OK** khi xong việc.

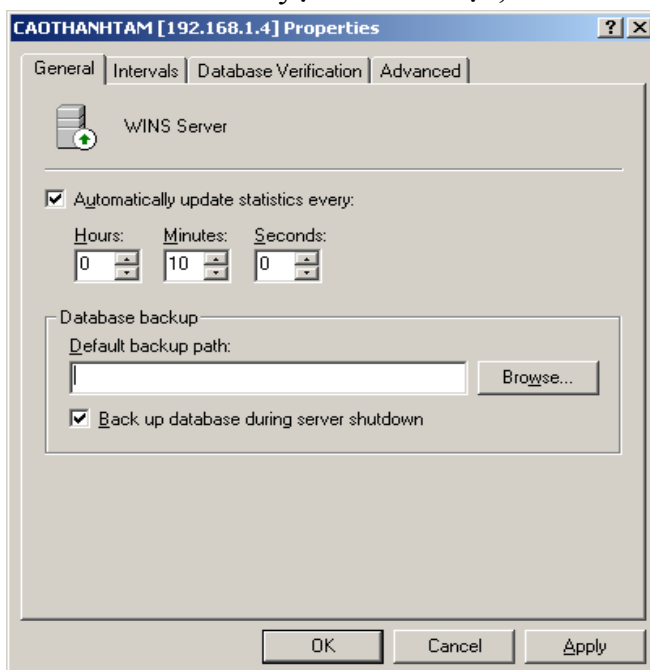
2.2.3.13. Sao lưu và phục hồi cơ sở dữ liệu WINS

- Lập cấu hình cho WINS tự động sao lưu

Mặc định cơ sở dữ liệu **WINS** không được sao lưu. Nếu cơ sở dữ liệu gặp sự cố, bạn sẽ vô phương phục hồi. Nhằm bảo toàn cơ sở dữ liệu trước những sự cố bất kỳ, hãy thiết lập chế độ sao lưu tự động hay tự mình thực hiện sao lưu theo định kỳ.

+ Nhấp phải chuột vào máy phục vụ mong muốn trong **console WINS**, chọn **Properties**.

+ Trên **General**, gõ đường dẫn thư mục sẽ chứa bản sao lưu vào trường **Default Backup Path**. Nhấp **Browse** nếu muốn duyệt tìm thư mục,



Hình 7.13 Cấu hình máy phục vụ WINS

+ Chọn **Backup Database During Server Shutdown** nhằm đảm bảo cơ sở dữ liệu được sao lưu mỗi khi máy phục vụ **WINS** ngừng vận hành.

+ Nhấp **OK**, cơ sở dữ liệu sẽ tự động được sao lưu cứ 3 giờ/lần.

- Phục hồi cơ sở dữ liệu

Điều kiện để phục hồi là phải có sẵn bản sao lưu hoàn chỉnh của cơ sở dữ liệu WINS.

+ Chọn máy phục vụ cần làm việc trong **console WINS**

+ Nhấp menu **Action**, chọn **All Tasks->Stop**.

+ Chọn **Restore Database** cũng từ menu **Action**.

+ Trong **Browse For Folder**, chọn thư mục con **wins_back**, vốn chứa bản sao lưu mới nhất, rồi nhấp **OK**.

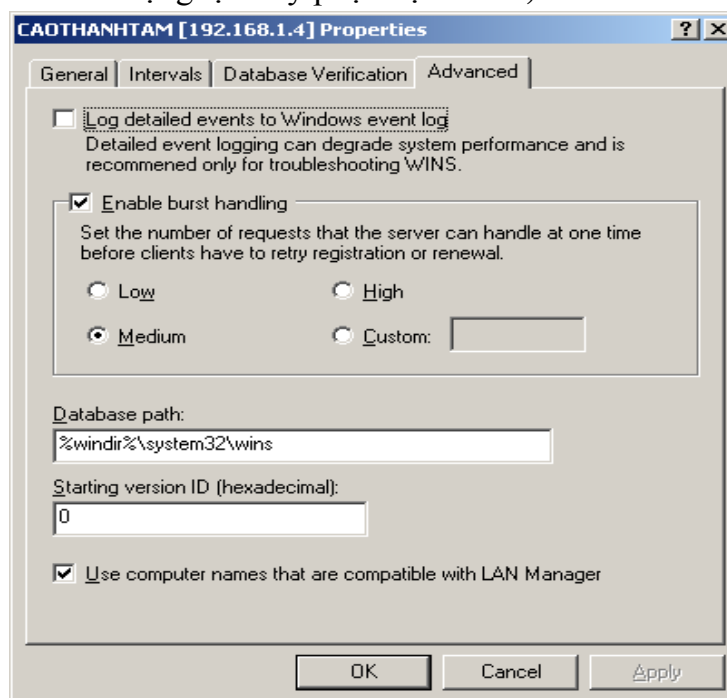
+ Nếu phục hồi thành công, cơ sở dữ liệu **WINS** sẽ được trả về trạng thái tại thời điểm sao lưu. Chọn **Action→AllTasks→Start**.

+ Trường hợp phục hồi thất bại, có lẽ bạn phải xoá mọi tập tin **WINS** và lại tạo dựng từ đầu.

- Xoá trống WINS và bắt đầu với cơ sở dữ liệu mới

Nếu **WINS** không phục hồi từ bản sao lưu hay không khởi động bình thường, giải pháp là xoá trắng mọi mẫu tin và nhật ký **WINS**, sau đó xây dựng tất cả từ cơ sở dữ liệu mới. Theo các bước sau:

- + Trong **Console WINS**, chọn **Properties** từ menu tắt của máy phục vụ cần làm việc.
- + Trên trang **Advanced**, lưu ý đường dẫn thư mục ở trường **Database Path**, nhấp **OK** đóng hộp thoại lại.
- + Chọn **Action**→**AllTasks**→**Stop** ngừng vận hành máy phục vụ.
- + Mở **Microsoft Windows Explorer**, xoá tất cả tập tin trong thư mục cơ sở dữ liệu **WINS**.
- + Trong **Console WINS** nhấp nút phải chuột vào máy phục vụ đang định phục hồi, chọn **AllTasks**→**Start** khởi động lại máy phục vụ **WINS**,



Hình 7.14 Cấu hình máy phục vụ WINS

Bài tập thực hành của học viên

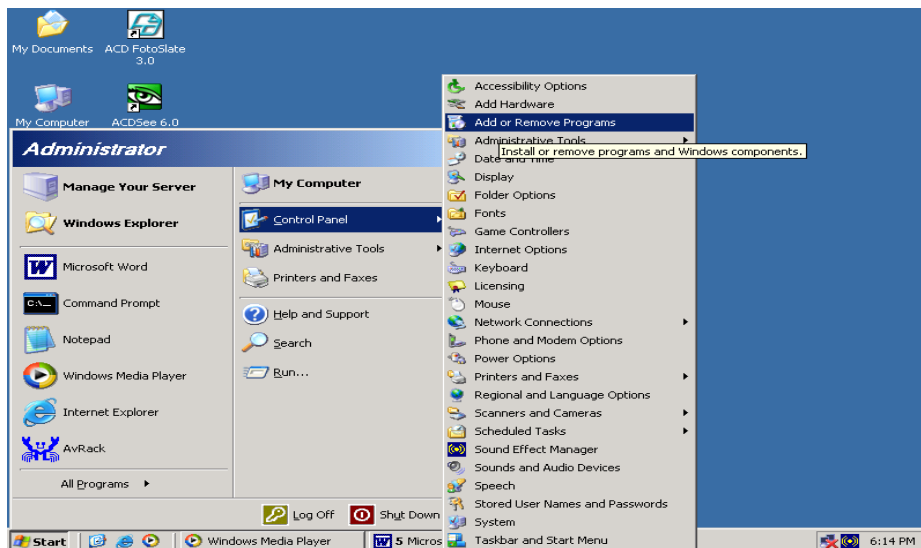
1. Cài đặt và cấu hình dịch vụ DHCP.
2. Cài đặt và cấu hình dịch vụ WINS

Hướng dẫn thực hiện:

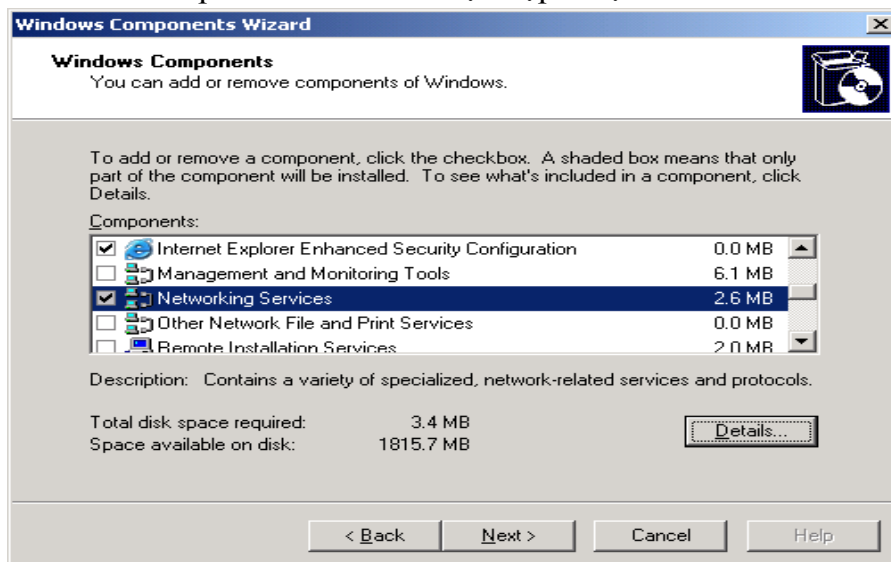
1. Cài đặt và cấu hình dịch vụ DHCP

a). CÀI ĐẶT DHCP

Các máy khách sẽ nhận địa chỉ IP một cách tự động từ dịch vụ cấp phát địa chỉ động DHCP. Dịch vụ này được cài đặt trên máy chủ như sau:

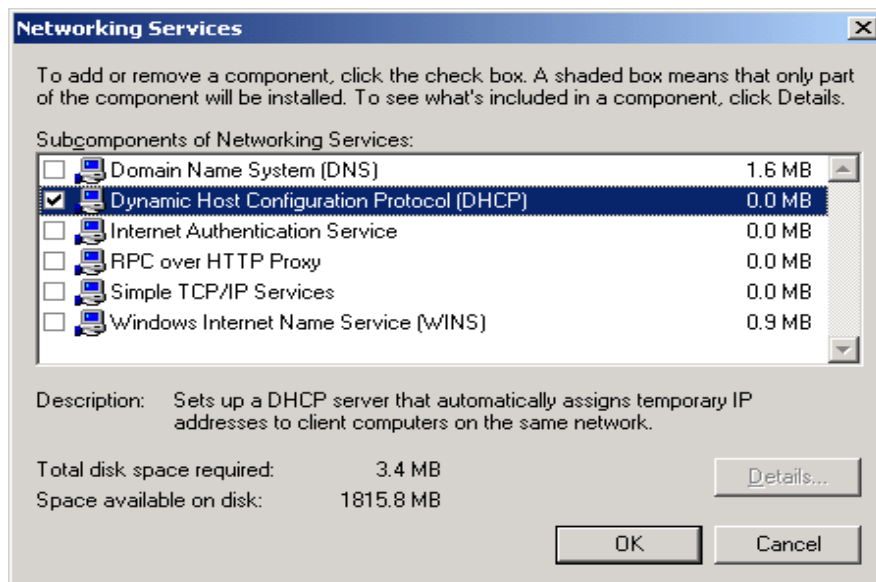


Start / control panel / Add or remove programs(Start/ Settings / control panel / Add or remove programs), xuất hiện hộp thoại Add or remove programs click biểu tượng Add/remove Windows Components. Sẽ xuất hiện hộp thoại sau:

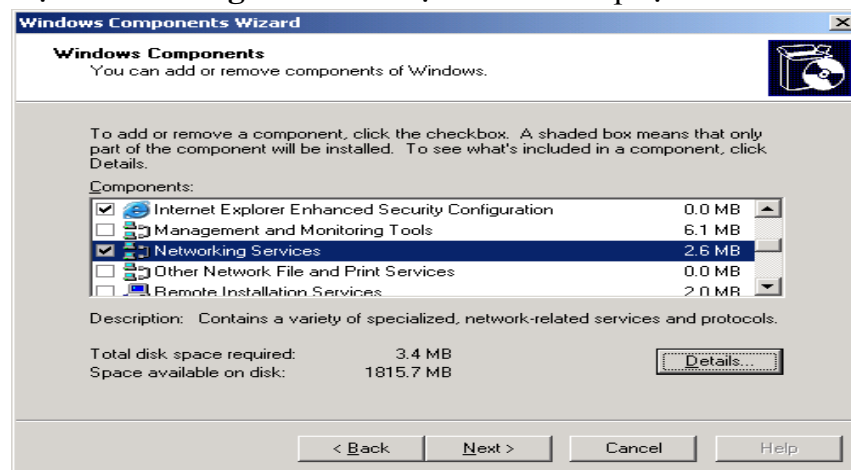


Di chuyển thanh sáng đến mục **Networking Service** và nhấn nút **Details** sẽ xuất hiện cửa sổ **Networking Services**.

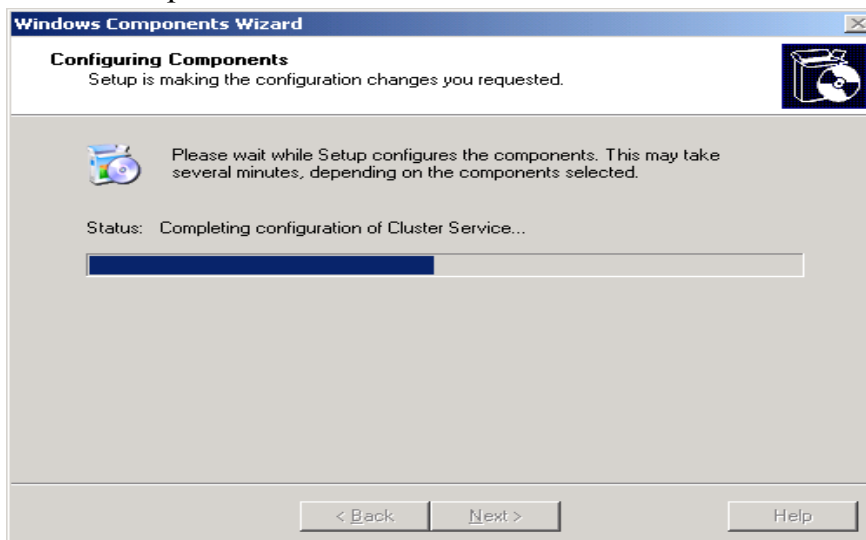
Trong cửa sổ Networking Services đánh dấu chọn mục Dynamic Host Configuration Protocol (DHCP) và nhấn OK.



Trở lại hộp thoại **Networking Services** chọn **Next** để tiếp tục.



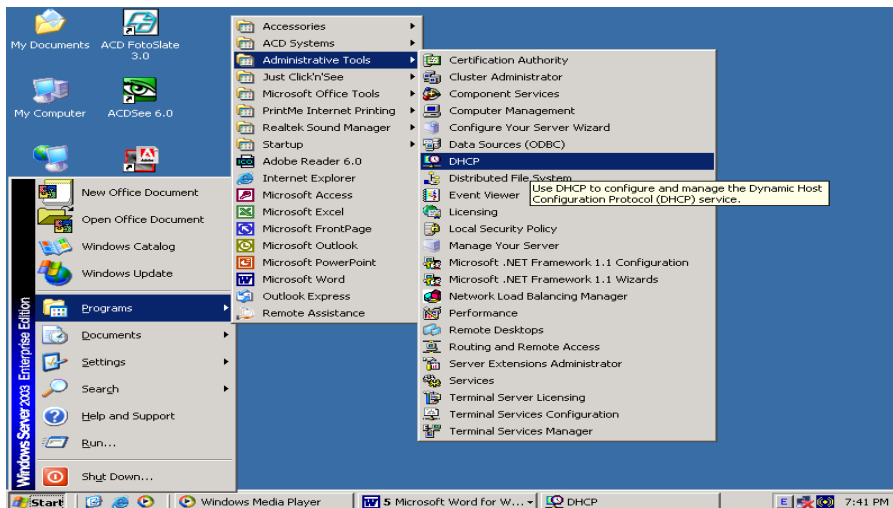
Windows sẽ cấu hình và cài đặt các thành phần của dịch vụ **DHCP**. Trong quá trình cài đặt Windows đòi hỏi phải Insert đĩa DVD Windows Server 2003 vào.



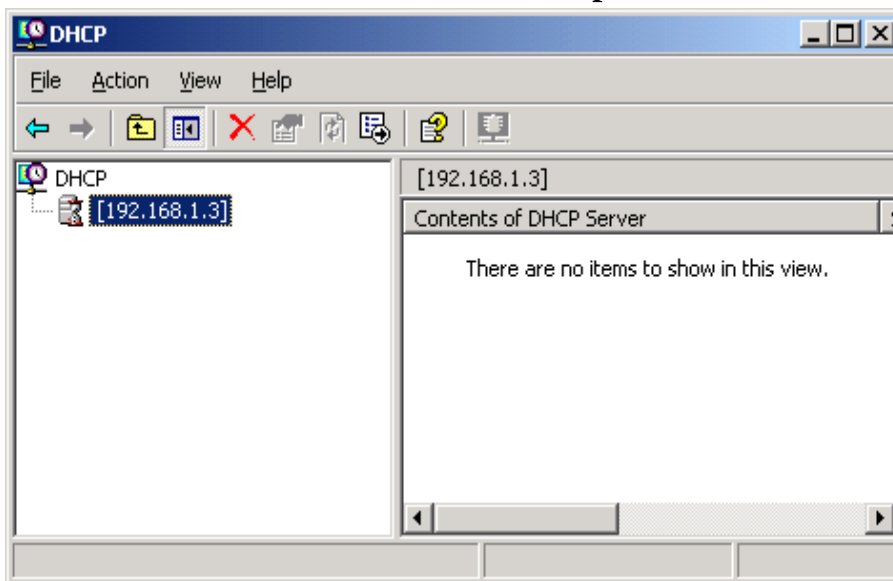
Đến khi hộp thoại Completing The Windows Components Wizard, chọn Finish để hoàn tất.

b). CẤU HÌNH DỊCH VỤ DHCP

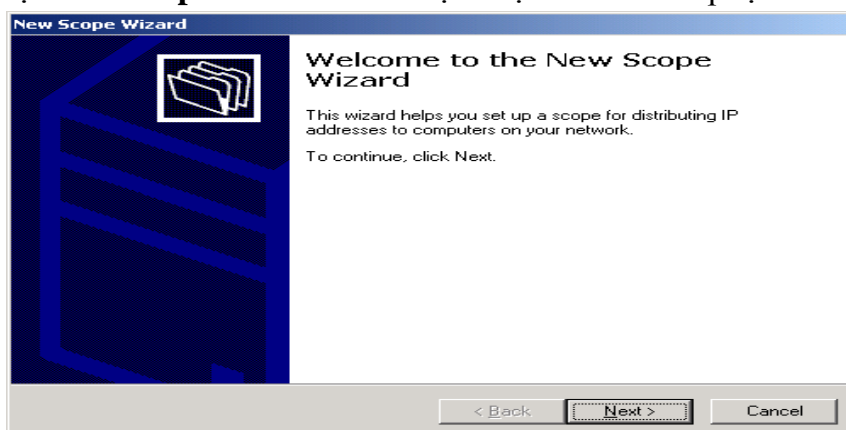
Từ menu Start / Programs/ Administrative Tools / DHCP. Cửa sổ DHCP xuất hiện.



Trong cửa sổ DHCP. Chọn menu **Action / New Scope**.



Hộp thoại **New Scope Wizard** xuất hiện chọn **Next** để tiếp tục.

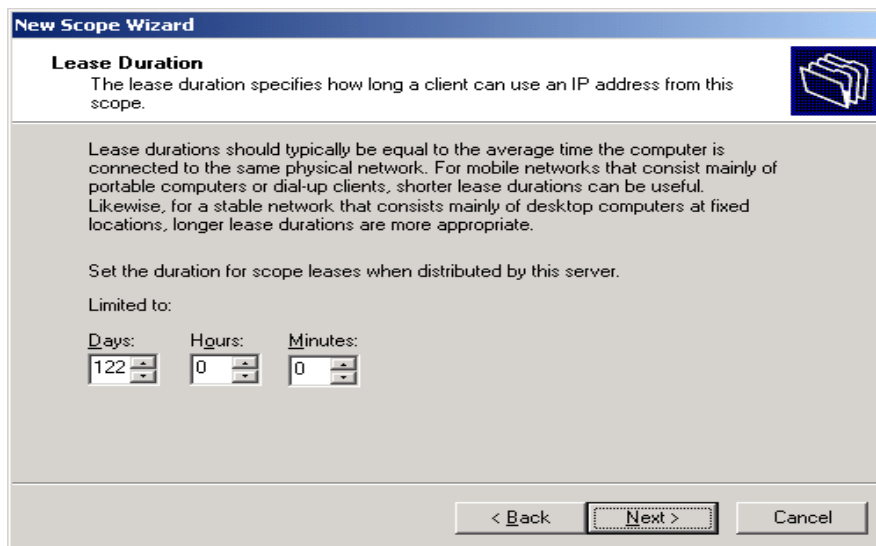


Hộp thoại **Scope Name** xuất hiện, nhập tên và chú thích cho **Scope**. Sau đó chọn **Next**.

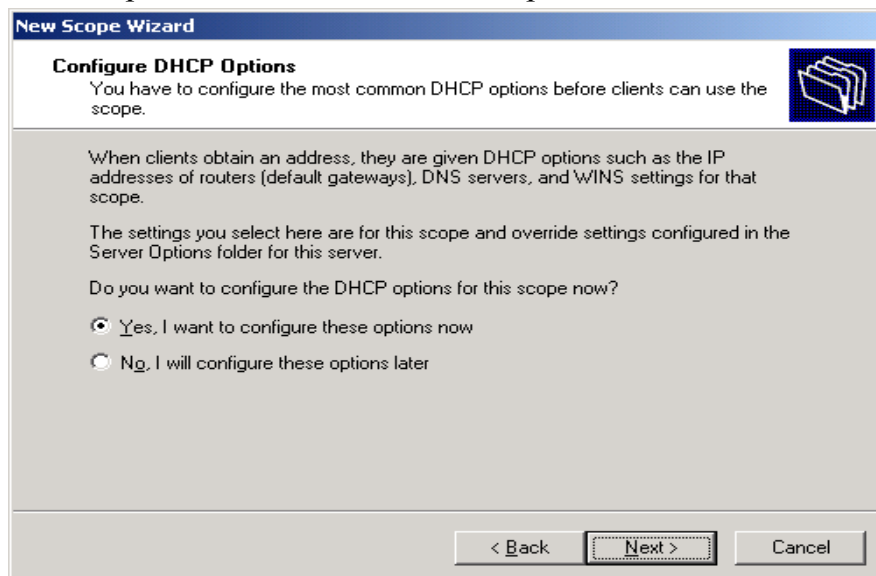
Hộp thoại IP Address Range xuất hiện. Nhập địa chỉ bắt đầu và địa chỉ kết thúc cho dãy địa chỉ cấp phát, đồng thời nhập địa chỉ Subnet mask. Rồi chọn **Next** để sang bước tiếp theo.

Hộp thoại Add Exclusions dùng để xác định dãy địa chỉ cần loại bỏ ra khỏi danh sách địa chỉ cấp phát của bước trên.

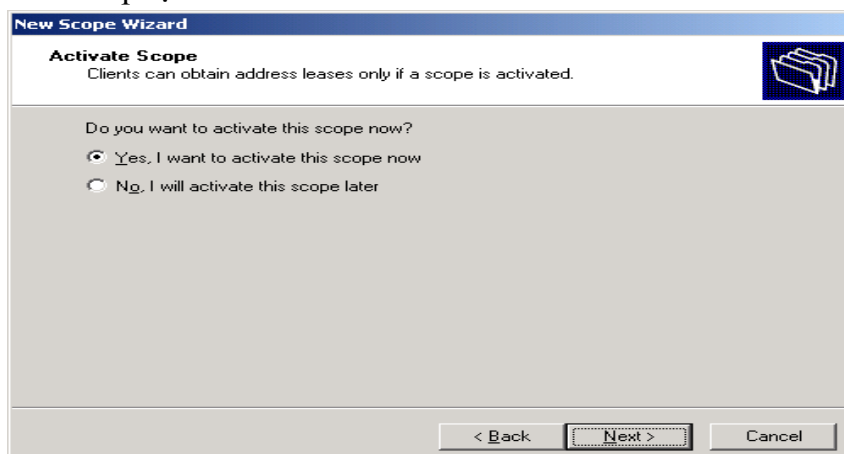
Trong hộp thoại **Lease Duration**, cho biết thời gian mà các máy Client có thể sử dụng các địa chỉ IP này. Mặc định ở đây là 8 ngày. Chọn Next để tiếp tục.



Hộp thoại Configure DHCP Options xuất hiện. Ta có thể chọn Yes, I want to configure these option now (để thiết lập thêm các cấu hình tùy chọn khác), hoặc chọn No, I will configure these options later (để hoàn tất việc cấu hình cho Scope). Chọn No, I will configure these options later, nhấn Next để tiếp tục.



Trong hộp thoại **Activate scope** hỏi ta có muốn kích hoạt **Scope** này không. Vì Scope chỉ có thể cấp phát địa chỉ khi được kích hoạt. Chọn Yes, I want to activate this scope now. Nhấn Next để tiếp tục.



Hộp thoại **Completing The New Scope Wizard** thông báo việc thiết lập cấu hình cho scope đã hoàn tất, nhấn Finish để kết thúc.

2. Cài đặt và cấu hình dịch vụ WINS

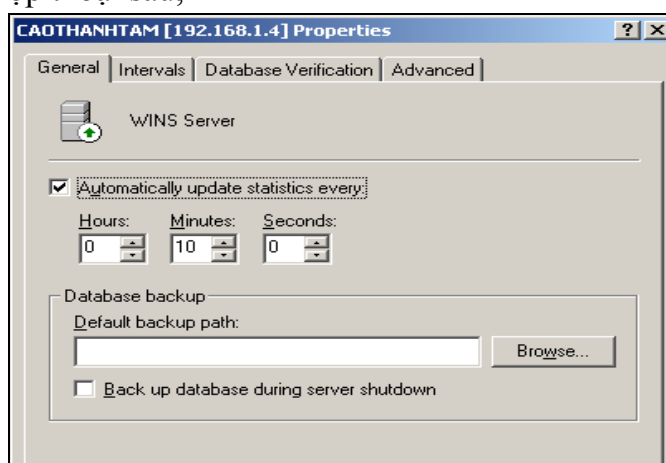
a). Cài đặt WINS

- + Bước 1: Click Start->Setting->Control Panel
- + Bước 2: Click đúp biểu tượng Add/Remove Programs.
- + Bước 3: Click Add/Remove Windows Components, Click Next.
- + Bước 4: Di chuyển thanh sáng đến mục **Networking Service** và nhấn nút **Details** sẽ xuất hiện cửa sổ **Networking Services**.
- + Bước 5: Trong cửa sổ **Networking Services** đánh dấu chọn mục **Windows Internet Name Service(WINS)** và nhấn **OK**.
- + Bước 6: Trở lại hộp thoại **Networking Services** chọn **Next** để tiếp tục.
- + Bước 7: Trong quá trình cài đặt Windows đòi hỏi phải Insert đĩa DVD Windows Server 2003 vào.
- + Bước 8: Đến khi hộp thoại **Completing The Windows Components Wizard**, chọn **Finish** để hoàn tất.

b). Cấu hình máy phục vụ WINS

Khi cài đặt máy phục vụ **WINS** máy phục được lập cấu hình. với các xác lập mặc định, bạn có thể thay đổi xác lập mặc định:

Trong **console WINS**, nhấp nút phải chuột vào máy phục vụ cần làm việc, chọn **properties** mở hộp thoại sau,



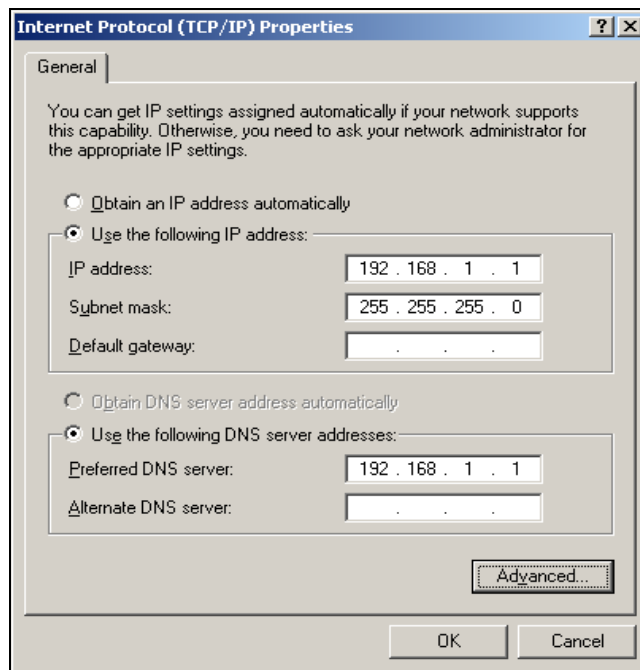
Thay đổi giá trị thuộc tính trên các trang General, Interval, Database Verification, Advance.

Click **OK** khi xong việc.

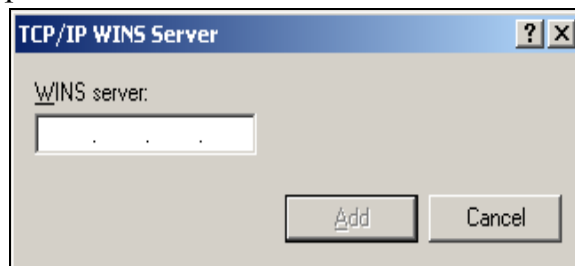
c). Cấu hình máy khách WINS

Trên **desktop**, Click chuột phải vào **My Network Place** chọn **Properties**, Click phải vào **Local Connection** chọn **Properties**.

Click đôi vào **Internet Protocol(TCP/IP)**, Click vào **Advanced**, chọn **WINS**.

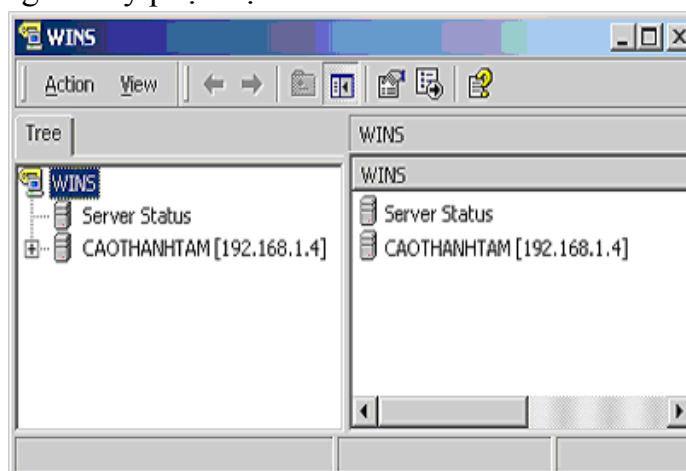


Chọn tiếp **Add**, nhập vào **IP** của **WINS server**, Click **Add**..



d). Bổ sung máy chủ WINS

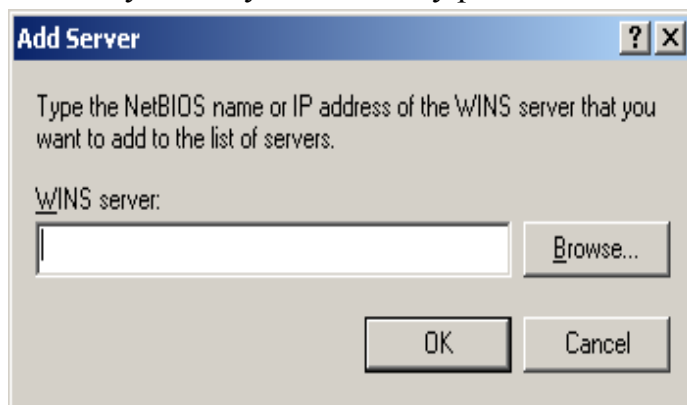
Khi cài đặt máy phục vụ mới, máy này được lập cấu hình với các xác lập mặc định. Bạn có thể xem và thay đổi xác lập mặc định bất cứ lúc nào thông qua **console WINS**. **Console WINS** truy cập từ thư mục **Administrative Tools (common)**, là nơi bạn quản lý các máy phục vụ WINS trên mạng. Cửa sổ chính của console WINS; được chia thành hai khung. Khung bên trái liệt kê máy phục vụ WINS trong vùng theo địa chỉ IP, kể cả máy tính cục bộ, nếu đây cũng là máy phục vụ WINS.



Nếu một máy phục vụ WINS cần lập cấu hình không có tên trong console WINS, tiến hành bổ sung vào console như sau:

+ Bước 1: Click nút phải chuột vào **WINS** bên khung trái, chọn **Add Server**.

+ Bước 2: Gõ địa chỉ **IP** hay tên máy tính của máy phục vụ **WINS** được quản lý



+ Bước 3: Click **OK**. Khung bên trái xuất hiện thêm mục nhập dành cho máy phục vụ WINS này

e). Khởi động và ngừng WINS:

Công tác quản lý máy phục vụ WINS được thực hiện qua Windows Internet Naming Service. Tương tự mọi dịch vụ khác, bạn có thể khởi động, ngừng hẳn hay tạm dừng tiếp tục chạy WINS trong thư mục Servers của Computer Management hay từ dòng lệnh.

Để quản lý máy phục vụ WINS thông qua Computer Management Click nút phải chuột vào WINS, chọn All Task, Start, Stop, Pause, Resume, Restart tùy tình huống. Cũng có thể quản lý WINS trong console WINS: Click nút phải chuột vào “máy phục vụ” sẽ được quản lý trong console WINS chọn All Tasks, chọn tiếp Start, Stop, Pause, Resume, Restart, tùy tình huống.

Bài 8: QUẢN TRỊ MÁY IN

Giới thiệu

Nhiều năm trở lại đây, máy in đã trở thành thứ không quá đắt đối với chi phí của bạn. Tuy nhiên có nhiều giải pháp để có thể biết được ai đang thực hiện việc in ẩn trên máy in trong mạng của bạn.

Ví dụ: văn phòng trả tài khoản của công ty có một máy in để in các bản kiểm tra. Bạn có thể cấu hình máy in theo kiểu này để không cho những người có tài khoản người dùng trong miền có thể in nó. Ngoài ra việc biết một người dùng trái phép đã dùng nó để in và kiểm tra các bản kiểm tra xem người dùng hợp lệ có được in hay không là một vấn đề hết sức quan trọng.

1. Mục tiêu:

- Mô tả về mô hình và thuật ngữ được sử dụng cho tác vụ in ẩn trong Windows;
- Cài đặt một máy in logic trên một máy chủ in ẩn;
- Chuẩn bị một máy chủ in ẩn cho các máy trạm;
- Kết nối một máy trạm in ẩn đến một máy in logic trên máy chủ in ẩn;
- Quản trị hàng đợi in ẩn và các đặc tính máy in;
- Xử lý sự cố các lỗi về máy in.
- Thực hiện các thao tác an toàn với máy tính.

2. Nội dung chính:

2.1. Cài đặt máy in

Mục tiêu:

- *Cài đặt được máy in cho server và qua mạng.*

Trước khi bạn có thể truy xuất vào thiết bị máy in vật lý thông qua hệ điều hành **Windows Server 2003** thì bạn phải tạo ra một máy in **logic**. Nếu máy in của bạn có tính năng **Plug and Play** thì máy in đó sẽ được nhận diện ra ngay khi nó được gắn vào máy tính dùng hệ điều hành **Windows Server 2003**. Tiện ích **Found New Hardware Wizard** sẽ tự động bật lên. Tiện ích này sẽ hướng dẫn cho bạn từng bước để cài đặt máy in. Nếu hệ điều hành nhận diện không chính xác thì bạn dùng đĩa **DVD** được hãng sản xuất cung cấp kèm theo máy để cài đặt.

Ngoài ra, bạn cũng có thể tự mình thực hiện tạo ra một máy in **logic** bằng cách sử dụng tiện ích **Add Printer Wizard**. Để có thể tạo ra một máy in **logic** trong **Windows Server 2003** thì trước hết bạn phải đăng nhập vào hệ thống với vai trò là một thành viên của nhóm **Administrators** hay nhóm **Power Users** (trong trường hợp đây là một **Server** thành viên) hay nhóm **Server Operators** (trong trường hợp đây là một **domain controller**).

Bạn có thể tạo ra một máy in logic cục bộ tương ứng với một máy in vật lý được gắn trực tiếp vào máy tính cục bộ của mình hoặc tương ứng với một máy in mạng (máy in mạng được gắn vào một máy tính khác trong mạng hay một thiết bị **Print Server**). Muốn thao tác bằng tay để tạo ra một máy in cục bộ hay một máy in mạng, chúng ta lần lượt thực hiện các thao tác sau đây:

Nhấp chuột chọn **Start**, rồi chọn **Printers And Faxes**.

Nhấp chuột vào biểu tượng **Add Printer**, tiện ích **Add Printer Wizard** sẽ được khởi động. Nhấp chuột vào nút **Next** để tiếp tục.

Hộp thoại **Local Or Network Printer** xuất hiện. Bạn nhấp vào tùy chọn **Local Printer Attached To This Computer** trong trường hợp bạn có một máy in vật lý gắn trực tiếp vào máy tính của mình. Nếu trường hợp ta đang tạo ra một máy in **logic** ứng với một máy in mạng thì ta nhấp vào tùy chọn **A Printer Attached To Another Computer**. Nếu máy in được gắn trực tiếp vào máy tính, bạn có thể chọn thêm tính năng **Automatically Detect And Install My Plug And Play Printer**. Tùy chọn này cho phép hệ thống tự động quét máy tính của bạn để phát hiện ra các máy in **Plug and Play**, và tự động cài đặt các máy in đó cho bạn. Khi đã hoàn tất việc chọn lựa, nhấp chuột vào nút **Next** để sang bước kế tiếp.

Nếu máy in vật lý đã được tự động nhận diện bằng tiện ích **Found New Hardware Wizard**. Tiện ích này sẽ hướng dẫn bạn tiếp tục cài đặt **driver** máy in qua từng bước.

Hộp thoại **Print Test Page** xuất hiện. Nếu thiết bị máy in được gắn trực tiếp vào máy tính của bạn, bạn nên in thử một trang kiểm tra để xác nhận rằng mọi thứ đều được cấu hình chính xác. Ngược lại, nếu máy in là máy in mạng thì bạn nên bỏ qua bước này. Nhấp chuột vào nút **Next** để sang bước kế tiếp.

Hộp thoại **Completing The Add Printer Wizard** hiện ra. Hộp thoại này đem đến cho chúng ta một cơ hội để xác nhận rằng tất cả các thuộc tính máy in đã được xác lập chính xác. Nếu bạn phát hiện có thông tin nào không chính xác, hãy nhấp chuột vào nút **Back** để quay lại sửa chữa thông tin cho đúng.

Còn nếu nhận thấy mọi thứ đều ổn cả thì bạn nhấp chuột vào nút **Finish**.

Một biểu tượng máy in mới sẽ hiện ra trong cửa sổ **Printer And Faxes**. Theo mặc định, máy in sẽ được chia sẻ.

2.2 Quản lý thuộc tính máy in

2.2.1. Cấu hình Layout

Trong hộp thoại **Printing Preferences**, chọn **Tab Layout**. Sau đó trong mục **Orientation**, bạn chọn cách thức in trang theo chiều ngang hay chiều dọc. Trong mục **Page Order**, bạn chọn in từ trang đầu đến trang cuối của tài liệu hoặc in theo thứ tự ngược lại. Trong mục **Pages Per Sheet**, bạn chọn số trang tài liệu sẽ được in trên một trang giấy.

2.2.2. Giấy và chất lượng in

Cũng trong hộp thoại **Printing Preferences**, để qui định giấy và chất lượng in, chúng ta chọn **Tab Paper/Quality**. Các tùy chọn trong **Tab Paper/Quality** phụ thuộc vào đặc tính của máy in. Ví dụ, máy in chỉ có thể cung cấp một tùy chọn là **Paper Source**. Còn đối với máy in **HP OfficeJet Pro Cxi**, chúng ta có các tùy chọn là: **Paper Source, Media, Quality Settings** và **Color**

2.2.3. Các thông số mở rộng

Nhấp chuột vào nút **Advanced** ở góc dưới bên phải của hộp thoại **Printing Preferences**. Hộp thoại **Advanced Options** xuất hiện cho phép bạn điều chỉnh các thông số mở rộng. Chúng ta có thể có các tùy chọn của máy in như: **Paper/Output,**

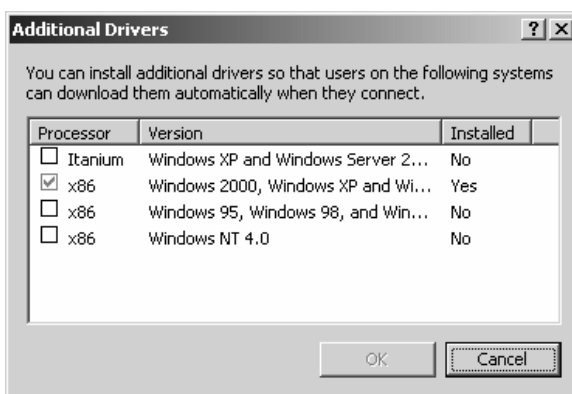
Graphic, Document Options, và Printer Features. Các thông số mở rộng có trong hộp thoại **Advanced Options** phụ thuộc vào driver máy in mà bạn đang sử dụng.

2.3. Cấu hình chia sẻ máy in

Nhấp phải chuột lên máy in, chọn **Properties**. Hộp thoại **Properties** xuất hiện, bạn chọn **Tab Sharing**. Để chia sẻ máy in này cho nhiều người dùng, bạn nhấp chuột chọn **Share this printer**. Trong mục **Share name**, bạn nhập vào tên chia sẻ của máy in, tên này sẽ được nhìn thấy trên mạng. Bạn cũng có thể nhấp chọn mục **List In The Directory** để cho phép người dùng có thể tìm kiếm máy in thông qua **Active Directory** theo một vài thuộc tính đặc trưng nào đó.

Ngoài ra, trong **Tab Sharing**, ta có thể cấu hình **driver** hỗ trợ cho các máy trạm sử dụng máy in trong trường hợp máy trạm không phải là **Windows Server 2003**. Đây là một tính năng cần thiết vì nó cho phép chỉ định các **driver** hỗ trợ in để các máy trạm có thể tải về một cách tự động. Mặc định, **driver** duy nhất được nạp vào là **driver** của hãng **Intel** cho các máy trạm là **Windows 2000, Windows Server 2003, và Windows XP**. Để cung cấp thêm các **driver** cho máy trạm khác, bạn nhấp chuột vào nút **Additional Drivers** nằm phía dưới **Tab Sharing**. Hộp thoại **Additional Drivers** xuất hiện. **Windows Server 2003** hỗ trợ các **driver** thêm vào cho các **Client** là một trong những hệ điều hành sau:

- Itanium Windows XP hay Windows Server 2003.
- x86 Windows 2000, Windows XP, hay Windows Server 2003 (mặc định).
- x86 Windows 95, Windows 98, hay Windows Millennium Edition.
- x86 Windows NT 4



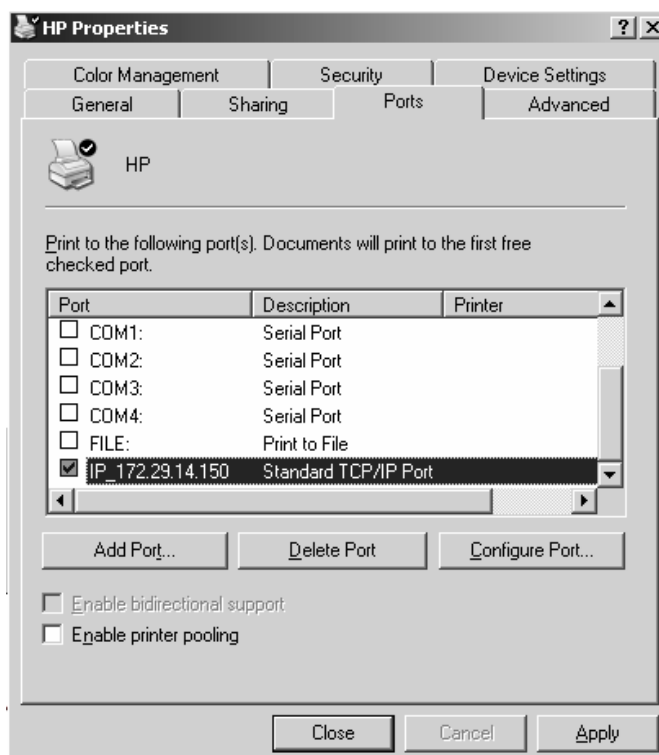
Hình 8.1 chọn driver để cài đặt

2.4. Cấu hình Tab Advance

2.4.1. Cấu hình các thông số trong Tab Port

Trong hộp thoại **Properties**, bạn chọn **Tab Port** để cấu hình tất cả các **port** đã được định nghĩa cho máy in sử dụng. Một **port** được định nghĩa như một **interface** sẽ cho phép máy tính giao tiếp với thiết bị máy in. **Windows Server 2003** hỗ trợ các **port** vật lý (**local port**) và các **port TCP/IP** chuẩn (**port logic**).

Port vật lý chỉ được sử dụng khi ta gắn trực tiếp máy in vào máy tính. Trong trường hợp **Windows Server 2003** đang được triển khai trong một nhóm làm việc nhỏ, hầu như bạn phải gắn máy in vào **port LPT1**.



Hình 8.2 cấu hình máy in

Port TCP/IP chuẩn được sử dụng khi máy in có thể kết nối trực tiếp vào mạng (trên máy in có hỗ trợ **port RJ45**) và máy in này có một địa chỉ **IP** để nhận dạng. Ưu điểm của máy in mạng là tốc độ in nhanh hơn máy in cục bộ và máy in có thể đặt bất kỳ nơi nào trong hệ thống mạng. Khi đó bạn cần chỉ định một port **TCP/IP** và khai báo địa chỉ **IP** của máy in mạng. Cùng với việc xóa và cấu hình lại một **port** đã tồn tại, bạn cũng có thể thiết lập **printer pooling** và điều hướng các công việc in ấn đến một máy in khác.

2.4.2. Printer Pooling

Printer pool được sử dụng nhằm phối hợp nhiều máy in vật lý với một máy in **logic**, được minh họa như hình bên dưới. Lợi ích của việc sử dụng **printer pool** là máy in rảnh đầu tiên sẽ thực hiện thao tác in ấn cho bạn. Tính năng này rất hữu dụng trong trường hợp ta có một nhóm các máy in vật lý được chia sẻ cho một nhóm người dùng, ví dụ như là nhóm các thư ký

Để cấu hình một **printer pool**, bạn nhấp chuột vào tùy chọn **Enable Printer Pooling** nằm ở phía dưới **Tab Port** trong hộp thoại **Properties**. Sau đó, kiểm tra lại tất cả các **port** mà ta dự định gắn các máy in vật lý trong **printer pool** vào. Nếu ta không chọn tùy chọn **Enable Printer Pooling** thì ta chỉ có một port duy nhất cho mỗi máy in. Chú ý tất cả các máy in vật lý trong một **printer pool** phải sử dụng cùng một **driver** máy in.

2.4.3. Điều hướng tác vụ in đến một máy in khác

Nếu một máy in vật lý của bạn bị hư, bạn có thể chuyển tất cả các tác vụ in ấn của máy in bị hư sang một máy in khác. Để làm được điều này, trước hết bạn phải đảm bảo máy in mới phải có **driver** giống với máy in cũ. Sau đó, trong **Tab Port**, bạn nhấp chuột vào nút **Add Port**, chọn **Local port** rồi chọn tiếp **New Port**. Hộp thoại

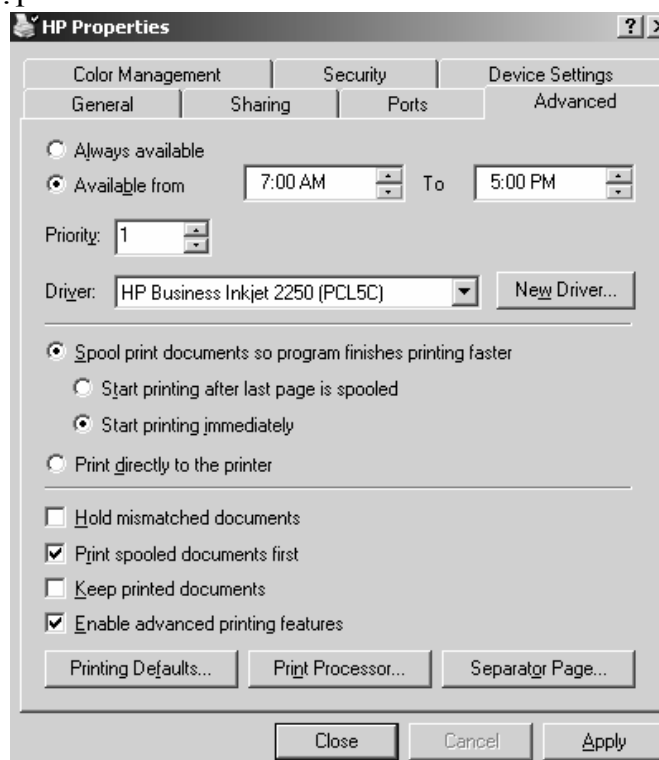
Port Name xuất hiện, gõ vào tên **UNC** của máy in mới theo định dạng: **\\computername\printer_sharename**.

2.4.4. Cấu hình tab advanced

2.4.4.1. Các thông số của Tab Advanced

Trong hộp thoại **Properties**, bạn nhấp chuột vào **Tab Advanced** để điều khiển các đặc tính của máy in. Bạn có thể cấu hình các thuộc tính sau:

- Khả năng của máy in
- Độ ưu tiên của máy in
- Driver mà máy in sẽ sử dụng
- Các thuộc tính đồng tác (**spooling**) của máy in
- Cách thức in tài liệu
- Chế độ in mặc định
- Sử dụng bộ xử lý in ấn nào
- Các trang độc lập



Hình 8.3 cấu hình máy in

2.4.4.2. Khả năng sẵn sàng phục vụ của máy in

Thông thường, chúng ta cần kiểm tra khả năng sẵn sàng phục vụ của máy in trong trường hợp chúng ta có nhiều máy in cùng sử dụng một thiết bị in. Mặc định thì tùy chọn **Always Available** luôn được bật lên. Do đó, người dùng có thể sử dụng máy in 24 tiếng một ngày. Để giới hạn khả năng phục vụ của máy in, bạn chọn **Available From** và chỉ định khoảng thời gian mà máy in sẽ phục vụ. Ngoài khoảng thời gian này, máy in sẽ không phục vụ cho bất kỳ người dùng nào.

2.4.4.3. Độ ưu tiên (Printer Priority)

Khi bạn đặt độ ưu tiên, bạn sẽ định ra bao nhiêu công việc sẽ được gửi trực tiếp vào thiết bị in. Ví dụ, bạn có thể sử dụng tùy chọn này khi 2 nhóm người dùng cùng

chia sẻ một máy in và bạn cần điều khiển độ ưu tiên đối với các thao tác in ấn trên thiết bị in này. Trong **Tab Advanced** của hộp thoại **Properties**, bạn sẽ đặt độ ưu tiên bằng các giá trị từ 1 đến 99, với 1 là có độ ưu tiên thấp nhất và 99 là có độ ưu tiên cao nhất.

Ví dụ: giả sử có một máy in được phòng kế toán sử dụng. Những người quản lý trong phòng kế toán luôn luôn muốn tài liệu của họ sẽ được ưu tiên in ra trước các nhân viên khác. Để cấu hình cho việc sắp xếp thứ tự này, ta tạo ra một máy in tên là **MANAGERS** gắn vào **port LPT1** với độ ưu tiên là 99. Sau đó, cũng trên **port LPT1**, ta tạo thêm một máy in nữa tên là **WORKERS** với độ ưu tiên là 1. Sau đó, ta sẽ sử dụng **Tab Security** trong hộp thoại **Properties** để giới hạn quyền sử dụng máy in **MANAGERS** cho những người quản lý. Đối với các nhân viên còn lại trong phòng kế toán, ta cho phép họ sử dụng máy in **WORKERS** (chúng ta sẽ tìm hiểu rõ hơn về **Security** trong phần sau). Khi các tác vụ in xuất phát từ máy in **MANAGERS**, nó sẽ đi vào hàng đợi của của máy in vật lý với độ ưu tiên cao hơn là các tác vụ xuất phát từ máy in **WORKERS**. Do đó, tài liệu của những người quản lý sẽ được ưu tiên in trước.

2.4.4.4. Print Driver

Mục **Driver** trong **Tab Advanced** cho phép bạn chỉ định driver sẽ dùng cho máy in. Nếu bạn đã cấu hình nhiều máy in trên một máy tính thì bạn có thể chọn bất kỳ **driver** nào trong các **driver** đã cài đặt. Thao tác thực hiện như sau: Nhấp chuột vào nút **New Driver** để khởi động **Add Printer Driver Wizard**. **Add Printer Driver Wizard** cho phép bạn thực hiện cập nhật cũng như thêm driver mới.

2.4.4.5. Spooling

Khi bạn cấu hình tùy chọn **spooling**, bạn cần chỉ định rõ các tác vụ in ấn sẽ được đẩy ra đường ống máy in hay được gửi trực tiếp đến thiết bị máy in. **Spooling** có nghĩa là các thao tác in ấn sẽ được lưu trữ xuống đĩa thành một hàng đợi trước khi các thao tác in này được gửi đến máy in. Có thể xem **spooling** giống như là bộ điều phối in ấn nếu như tại một thời điểm có nhiều người dùng cùng lúc gửi yêu cầu đến máy in. Theo chế độ mặc định, tùy chọn **spooling** sẽ được bật lên sẵn.

2.4.4.6. Print Options

Phía dưới **Tab Advance** có chứa bốn tùy chọn in ấn. Đó là các tùy chọn:

- **Hold Mismatched Documents**: tùy chọn này hữu dụng trong trường hợp bạn sử dụng chế độ nhiều biểu mẫu trong một máy in. Mặc định thì tùy chọn này sẽ không được bật lên. Các tác vụ sẽ được in theo chế độ **first-in-first-out (FIFO)**. Nếu bạn bật tùy chọn này lên, hệ thống sẽ chọn ưu tiên in trước những tác vụ có chung một biểu mẫu.

- **Print Spooled Documents First**: tùy chọn này qui định rằng các tác vụ in ấn được điều hướng xong trước các loại tác vụ lớn khác. Điều này có nghĩa là các tác vụ in ấn sẽ có độ ưu tiên lớn hơn các loại tác vụ khác trong quá trình điều hướng. Mặc định thì tùy chọn này luôn được bật lên giúp gia tăng hiệu quả làm việc của máy in.

- **Keep Printed Documents**: tùy chọn này qui định rằng các tác vụ in ấn phải được xóa khỏi hàng đợi điều hướng in ấn khi các tác vụ này đã hoàn tất quá trình in.

Thông thường, bạn muốn xóa các tác vụ in ấn ngay khi nó bắt đầu in bởi vì nếu chúng ta tiếp tục lưu trữ các tác vụ này trong hàng đợi điều hướng và đợi cho đến khi chúng được in xong mới xóa thì sẽ phải tốn dung lượng ổ đĩa cho việc lưu trữ. Mặc định thì tùy chọn này sẽ không được bật lên.

- - **Enable Advanced Printing Features:** tùy chọn này qui định rằng bất kì các tính năng mở rộng nào mà máy in của bạn có hỗ trợ ví dụ như **Page Order** và **Pages Per Sheet** nên được bật lên. Mặc định thì tùy chọn này luôn được bật lên. Chỉ trong trường hợp xảy ra các vấn đề về tương thích thì bạn có thể tắt tùy chọn này. Ví dụ như bạn đang sử dụng **driver** cho một thiết bị máy in tương tự nhưng nó không hỗ trợ tất cả các tính năng của máy in. Trong trường hợp đó, bạn nên tắt tùy chọn này đi.

2.4.4.7. Printing Defaults

Nút **Printing Defaults** nằm ở góc trái phía dưới của **Tab Advance**. Nếu bạn nhấp chuột vào nút **Printing Defaults**, hộp thoại **The Printing Preferences** sẽ xuất hiện. Đây cũng chính là hộp thoại sẽ xuất hiện khi bạn nhấp chuột vào nút **Printing Preferences** trong **Tab General**

2.4.4.8. Print Processor

Bộ xử lý in ấn được sử dụng để qui định **Windows Server 2003** có cần phải thực hiện các xử lý bổ sung trong công việc in ấn hay không. Bộ xử lý in ấn **WinPrint** mặc định được cài đặt và được **Windows Server 2003** sử dụng. Bộ xử lý in ấn **WinPrint** có thể hỗ trợ một vài kiểu dữ liệu.

Theo mặc định thì hầu hết các ứng dụng trên nền **Window** sử dụng chuẩn **EMF (enhanced metafile)** để gửi các tác vụ đến máy in. Chuẩn **EMF** dùng kiểu dữ liệu **RAW**. Kiểu dữ liệu này sẽ báo với bộ xử lý in ấn là tác vụ này không cần phải sửa đổi độ ưu tiên khi in. Điều này là do nhà sản xuất phần mềm qui định.

Bảng danh sách các kiểu dữ liệu được bộ xử lý in ấn trong **Windows Server 2003** hỗ trợ:

Kiểu dữ liệu	Mô tả
RAW	Không làm thay đổi tài liệu in ấn
RAW (FF appended)	Không làm thay đổi tài liệu in ấn ngoại trừ việc thêm vào một kí tự form-feed
RAW (FF Auto)	Không làm thay đổi tài liệu in ấn ngoại trừ việc kiểm tra xem có cần thêm vào một kí tự form-feed hay không
NT EMF 1.00x	Thường điều hướng các tài liệu được gửi từ các máy tính Window khác
TEXT	Phiên dịch tất cả các kiểu dữ liệu văn bản đơn giản và máy in sẽ thực hiện in bằng cách sử dụng các lệnh văn bản chuẩn.

2.4.4.9. Separator Pages

Separator pages được sử dụng tại thời điểm bắt đầu của mỗi tài liệu nhằm mục đích định dạng rõ người dùng nào đã thực hiện việc in tài liệu này. Nếu như máy in

không được chia sẻ thì chế độ **Separator pages** vô hình chung sẽ gây ra lãng phí giấy in. Nếu trong trường hợp máy in được chia sẻ cho nhiều người dùng thì chế độ **Separator pages** sẽ hữu dụng trong việc phân phối các tác vụ in ấn đã hoàn tất.

Để thêm một **Separator page**, bạn thực hiện như sau: nhấp chuột vào nút **Separator page** nằm ở góc phải phía dưới **Tab Advance**. Hộp thoại **Separator page** hiện ra, bạn nhấp chuột vào nút **Browse** để chọn tập tin **Separator page** nào bạn muốn sử dụng.

TÀI LIỆU THAM KHẢO

- (1) Quản trị mạng Windows Server 2008, Nhà xuất bản Phương Đông, Năm 2009, Phương Lan và Tô Thanh Hải (Tập 1, 2)
- (2) Làm chủ Microsoft Windows 2003 Server, Nhà xuất bản thống kê, Năm 2005. Phạm Hoàng Dũng (Tập 1, 2, 3)
- (3) Microsoft Windows 2000s - Cài Đặt & Quản Trị , Nhà xuất bản Mũi Cà mau, Phạm Thế Bảo.
- (4) MCSE Training Kit, Published by Microsoft Press, 2003.
- (5) <http://technet.microsoft.com/en-us/library/dd349801%28v=ws.10%29.aspx>