

# MỤC LỤC

<b>NỘI DUNG.....</b>	<b>TRANG</b>
<b>LỜI NÓI ĐẦU .....</b>	<b>3</b>
<b>TÀI LIỆU THAM KHẢO .....</b>	<b>4</b>
<b>BÀI 1: TỔNG QUAN VỀ WINDOWS SERVER .....</b>	<b>5</b>
I. GIỚI THIỆU .....	5
II. CHUẨN BỊ CÀI ĐẶT HỆ THỐNG MẠNG.....	5
III. CÀI ĐẶT HỆ THỐNG MẠNG .....	5
<b>BÀI 2: ACTIVE DIRECTORY .....</b>	<b>15</b>
I. GIỚI THIỆU.....	15
II. CÁC THÀNH PHẦN CỦA ACTIVE DIRECTORY.....	15
III. CÀI ĐẶT VÀ CẤU HÌNH MÁY ĐIỀU KHIỂN VÙNG .....	17
<b>BÀI 3: DỊCH VỤ DNS .....</b>	<b>26</b>
I. GIỚI THIỆU.....	26
II. CÀI ĐẶT VÀ CẤU HÌNH .....	27
II.1. Cài đặt dịch vụ DNS .....	27
II.2. Tạo Zone trong DNS.....	28
II.3. Khảo sát một số thuộc tính cơ bản của Zone .....	28
II.4. Tạo các Resource Record .....	29
<b>BÀI 4: QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM .....</b>	<b>33</b>
I. ĐỊNH NGHĨA TÀI KHOẢN NGƯỜI DÙNG VÀ TÀI KHOẢN NHÓM .....	33
I.1 Tài khoản người dùng (user account) .....	33
I.2. Tài khoản nhóm (Group account) .....	34
II. TẠO MỚI TÀI KHOẢN NGƯỜI DÙNG.....	34
III. CÁC THÔNG TIN MỞ RỘNG CỦA TÀI KHOẢN NGƯỜI DÙNG .....	36
IV. TẠO MỚI TÀI KHOẢN NHÓM.....	39
<b>BÀI 5: DỊCH VỤ DHCP.....</b>	<b>41</b>
I. GIỚI THIỆU DỊCH VỤ DHCP .....	41
II. HOẠT ĐỘNG CỦA DHCP .....	41
III. CÀI ĐẶT DỊCH VỤ DHCP .....	41
IV. CHỨNG THỰC DỊCH VỤ DHCP TRONG ACTIVE DIRECTORY .....	42
V. CẤU HÌNH DỊCH VỤ DHCP.....	43
VI. CẤU HÌNH CÁC TÙY CHỌN DHCP .....	47

VII. CẤU HÌNH ĐỊA CHỈ DÀNH RIÊNG .....	48
<b>BÀI 6: DỊCH VỤ WINS .....</b>	<b>50</b>
I. GIỚI THIỆU DỊCH VỤ WINS.....	50
II. CÀI ĐẶT DỊCH VỤ WINS.....	50
III. CẤU HÌNH TỰY CHỌN WINS SERVER CHO DHCP .....	50
IV. CẤU HÌNH MÁY KHÁCH SỬ DỤNG DỊCH VỤ WINS .....	51
<b>BÀI 7: DỊCH VỤ ROUTING VÀ NAT.....</b>	<b>52</b>
I. ROUTING .....	52
I.1. Khái niệm.....	52
I.2. Cấu hình dịch vụ Routing And Remote Access .....	52
II. NAT .....	54
II.1. Giới thiệu .....	54
II.2. Cấu hình dịch vụ NAT .....	54
<b>BÀI 8: DỊCH VỤ PROXY.....</b>	<b>56</b>
I. GIỚI THIỆU VỀ FIREWALL.....	56
II. GIỚI THIỆU DỊCH VỤ WEB PROXY .....	56
III. CẤU HÌNH WEB PROXY SỬ DỤNG WINGATE.....	57
<b>BÀI 9: QUẢN TRỊ MÁY IN .....</b>	<b>64</b>
I. CÀI ĐẶT MÁY IN .....	64
II. QUẢN LÝ THUỘC TÍNH MÁY IN.....	64
III. CẤU HÌNH CHIA SẺ MÁY IN.....	66
IV. CẤU HÌNH THÔNG SỐ PORT .....	66
<b>BÀI 10: BẢO MẬT HỆ THỐNG .....</b>	<b>70</b>
I. SHARE PERMISSION .....	70
II. ROAMING USER - HOMEDIR & PROFILE.....	71
III. ORGANIZATION UNIT .....	72
IV. FOLDER REDIRECTED.....	74

## LỜI NÓI ĐẦU

*Giáo trình “**Mạng căn bản**” được biên soạn dành cho học sinh trung cấp nghề và sinh viên cao đẳng nghề với mục tiêu cung cấp cho người học các kiến thức tổng quan về quản trị mạng Windows Server.*

*Giáo trình được trình bày rõ ràng, hướng dẫn chi tiết từng bước cài đặt và cấu hình các dịch vụ trên Windows Server 2003 nhằm giúp người học dễ thực hành và hình thành kỹ năng của một người quản trị mạng Windows Server.*

*Trong quá trình biên soạn, chắc chắn giáo trình còn nhiều thiếu sót. Tác giả rất mong nhận được ý kiến đóng góp của quý thầy/cô và các em học sinh, sinh viên.*

**TÁC GIẢ**

Phan Hữu Phước

## TÀI LIỆU THAM KHẢO

1. Trần Văn Thành, Giáo trình Mạng Máy Tính, Đại học Quốc Gia Tp. HCM
2. Trần Văn Thành, Giáo trình Quản trị Windows Server 2003, Đại học Quốc Gia Tp. HCM
3. Giáo trình Quản Trị Windows Server 2003, Trung tâm Tin học Đại học Khoa học Tự nhiên Tp. HCM
4. Giáo trình Quản trị mạng, NXB Thống Kê
5. Giáo trình Quản trị mạng, Đại học Khoa học Kỹ thuật Tp. HCM

# BÀI 1: TỔNG QUAN VỀ WINDOWS SERVER

## I. GIỚI THIỆU

Hệ điều hành Windows 2003 Server có 4 phiên bản được sử dụng rộng rãi chính là: Windows Server 2003 Standard Edition, Enterprise Edition, Datacenter Edition, Web Edition.

- Kết chùm các Server để san sẻ tải (Network Load Balancing Clusters) và cài đặt nóng RAM (hot swap).
- Windows Server 2003 hỗ trợ hệ điều hành WinXP tốt hơn.
- Tính năng cơ bản của Mail Server được tính hợp sẵn.
- Cung cấp miễn phí hệ cơ sở dữ liệu thu gọn MSDE (Microsoft Database Engine) được cắt xén từ SQL Server 2000.
- Hỗ trợ môi trường quản trị Server thông qua dòng lệnh phong phú hơn

...

## II. CHUẨN BỊ CÀI ĐẶT HĐH MẠNG

### Yêu cầu phần cứng

- CPU
- RAM
- HDD

**Tương thích phần cứng:** \i386\winnt32 /checkupgradeonly

### Cài đặt mới hoặc nâng cấp

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 2003 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 chứa trong thư mục \Docs trên đĩa CD Windows Server 2003 Enterprise.

Các hệ điều hành cho phép nâng cấp thành Windows Server 2003 Enterprise Edition:

- Windows NT Server 4.0 với Service Pack 5 hoặc lớn hơn.
- Windows NT Server 4.0, Terminal Server Edition, với Service Pack 5 hoặc lớn hơn.
- Windows NT Server 4.0, Enterprise Edition, với Service Pack 5 hoặc lớn hơn.
- Windows 2000 Server.
- Windows 2000 Advanced Server.
- Windows Server 2003, Standard Edition.

## III. CÀI ĐẶT HĐH MẠNG

### Giai đoạn Preinstallation.

Sau khi kiểm tra và chắc chắn rằng máy của mình đã hội đủ các điều kiện để cài đặt Windows 2003 Server, bạn phải chọn một trong các cách sau đây để bắt đầu quá trình cài đặt.

### 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 2003 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 2003 Server.

Tùy theo hệ điều hành đang sử dụng là gì, bạn có thể sử dụng hai lệnh sau trong thư mục I386:

- WINNT32.EXE nếu là Windows 9x hoặc Windows NT.
- WINNT.EXE nếu là hệ điều hành khác.

### **Cài đặt trực tiếp từ đĩa CD Windows 2003.**

Nếu máy tính của bạn hỗ trợ tính năng khởi động từ đĩa CD, bạn chỉ cần đặt đĩa CD 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 CDROM. 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 2003.

### **Cài đặt Windows 2003 Server từ mạng.**

Để có thể cài đặt theo kiểu này, bạn phải có một Server phân phối tập tin, chứa bộ nguồn cài đặt Windows 2003 Server và đã chia sẻ thư mục này. Sau đó tiến hành theo các bước sau:

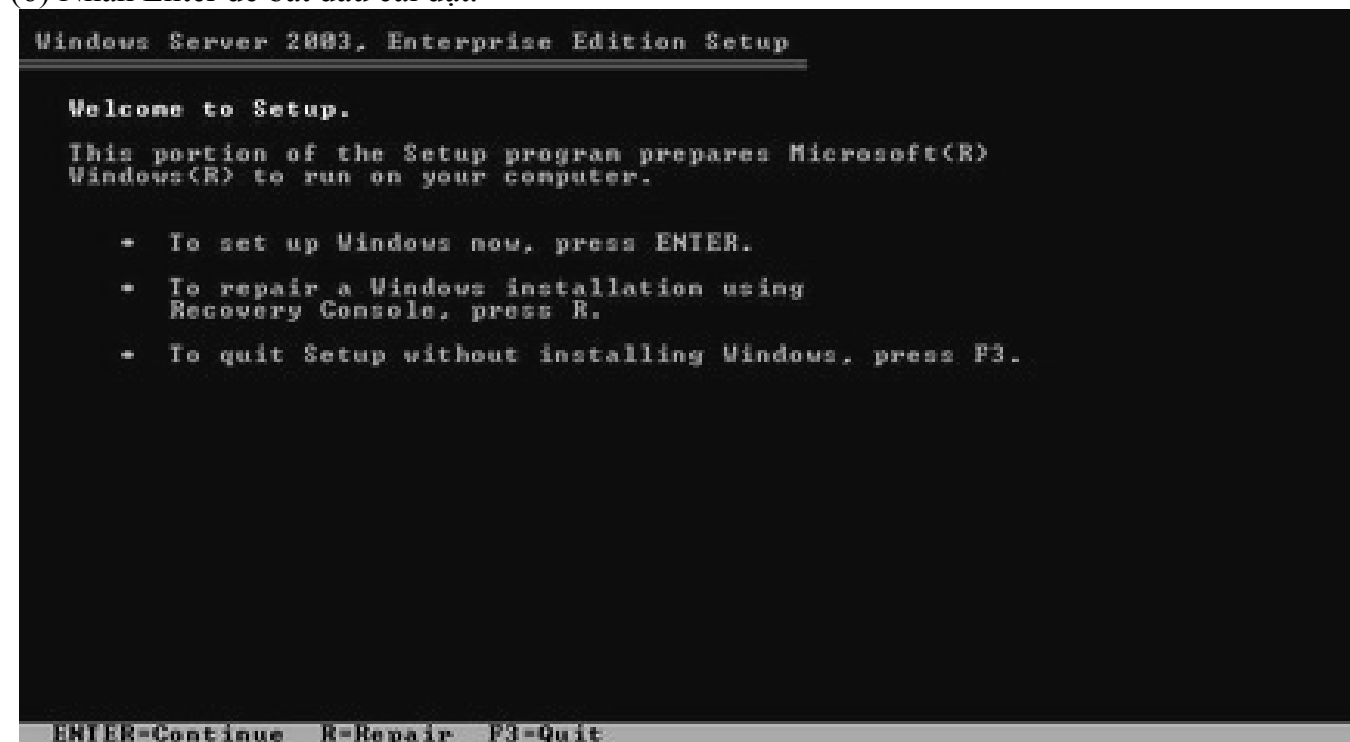
- Khởi động máy tính định cài đặt.
- Kết nối vào máy Server và truy cập vào thư mục chia sẻ chứa bộ nguồn cài đặt.
- Thi hành lệnh WINNT.EXE hoặc WINNT32.EXE tùy theo hệ điều hành đang sử dụng trên máy.
- Thực hiện theo hướng dẫn của chương trình cài đặt.

### **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:

- (1) Cấu hình BIOS của máy tính để có thể khởi động từ ổ đĩa CD
- (2) Đưa đĩa cài đặt Windows 2003 Server vào ổ đĩa CD-ROM và khởi động lại máy.
- (3) Khi máy khởi động từ đĩa CD-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.
- (4) Nếu máy có ổ đĩa SCSI thì phải nhấn phím F6 để chỉ Driver của ổ đĩa đó.
- (5) Trình cài đặt tiến hành chép các tập tin và driver cần thiết cho quá trình cài đặt.
- (6) Nhấn Enter để bắt đầu cài đặt.



- (7) Nhấn phím F8 để chấp nhận thỏa thuận bản quyền và tiếp tục quá trình cài đặt. Nếu nhấn ESC, thì chương trình cài đặt kết thúc.

## Windows Licensing Agreement

### END-USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE

MICROSOFT WINDOWS SERVER 2003, STANDARD EDITION  
MICROSOFT WINDOWS SERVER 2003, ENTERPRISE EDITION

PLEASE READ THIS END-USER  
LICENSE AGREEMENT ("EULA") CAREFULLY. BY  
INSTALLING OR USING THE SOFTWARE THAT  
ACCOMPANIES THIS EULA ("SOFTWARE"), YOU AGREE  
TO THE TERMS OF THIS EULA. IF YOU DO NOT  
AGREE, DO NOT USE THE SOFTWARE AND, IF  
APPLICABLE, RETURN IT TO THE PLACE OF  
PURCHASE FOR A FULL REFUND.

THIS SOFTWARE DOES NOT TRANSMIT ANY  
PERSONALLY IDENTIFIABLE INFORMATION FROM YOUR  
SERVER TO MICROSOFT COMPUTER SYSTEMS WITHOUT  
YOUR CONSENT.

1. GENERAL. This EULA is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation ("Microsoft"). This EULA governs the Software, which includes computer software (including online and electronic documentation) and any associated media and printed materials. This EULA applies to updates, supplements, add-on components, and Internet-based services components of

F8-I agree ESC-I do not agree PAGE DOWN-Next Page

(8) Chọn một vùng trống trên ổ đĩa và nhấn phím C để tạo một Partition mới chứa hệ điều hành.

## Windows Server 2003, Enterprise Edition Setup

The following list shows the existing partitions and  
unpartitioned space on this computer.

Use the UP and DOWN ARROW keys to select an item in the list.

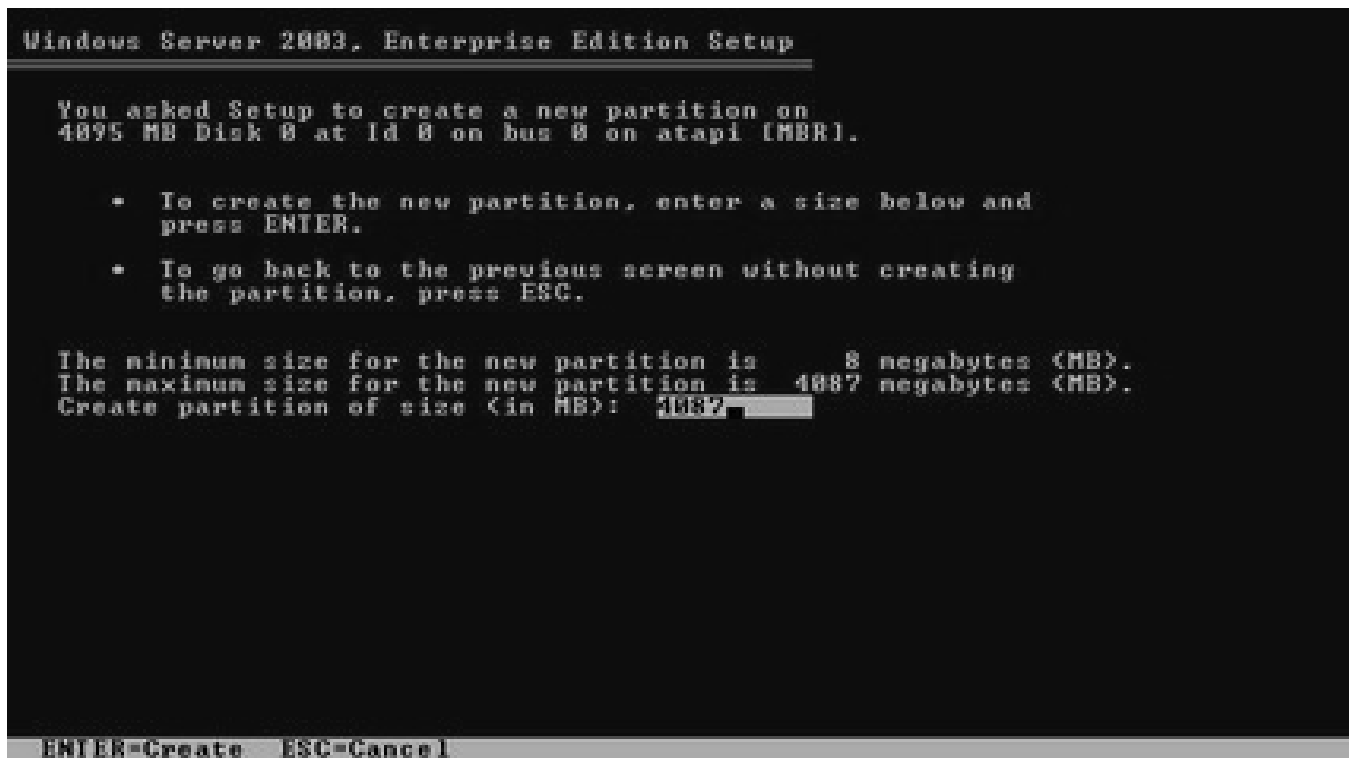
- To set up Windows on the selected item, press ENTER.
- To create a partition in the unpartitioned space, press C.
- To delete the selected partition, press D.

4095 MB Disk 0 at Id 0 on bus 0 on atapi [MBR]

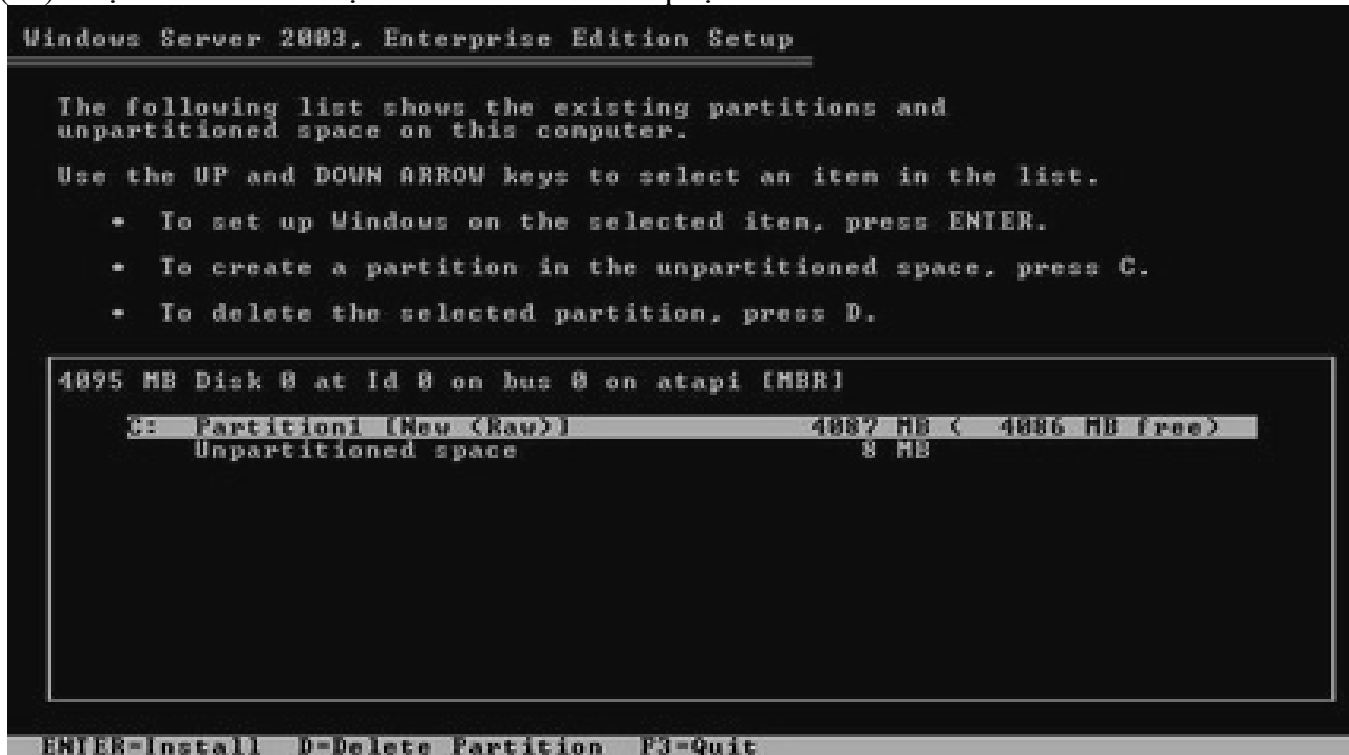
Unpartitioned space	4095 MB

ENTER=Install C=Create Partition F3=Quit

(9) Nhập vào kích thước của Partition mới và nhấn Enter.

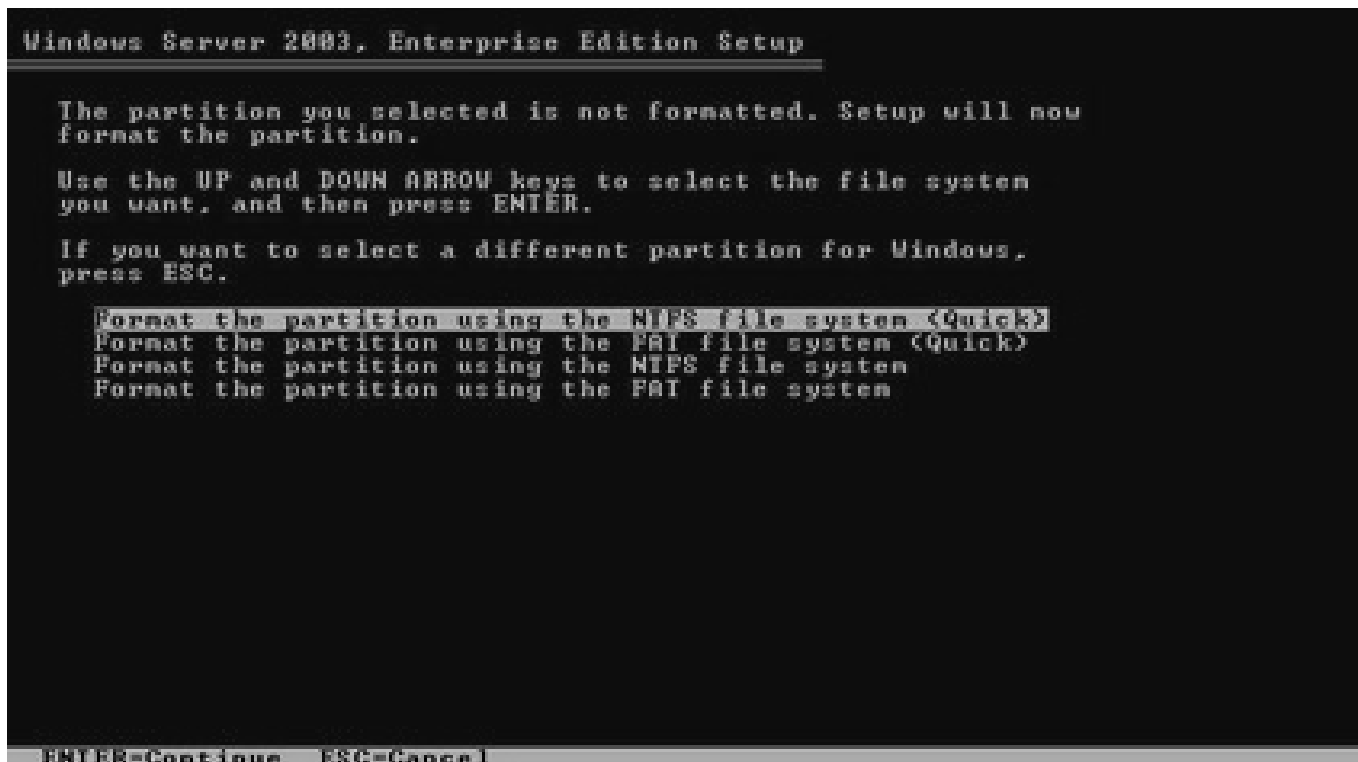


(10) Chọn Partition vừa tạo và nhấn Enter để tiếp tục.

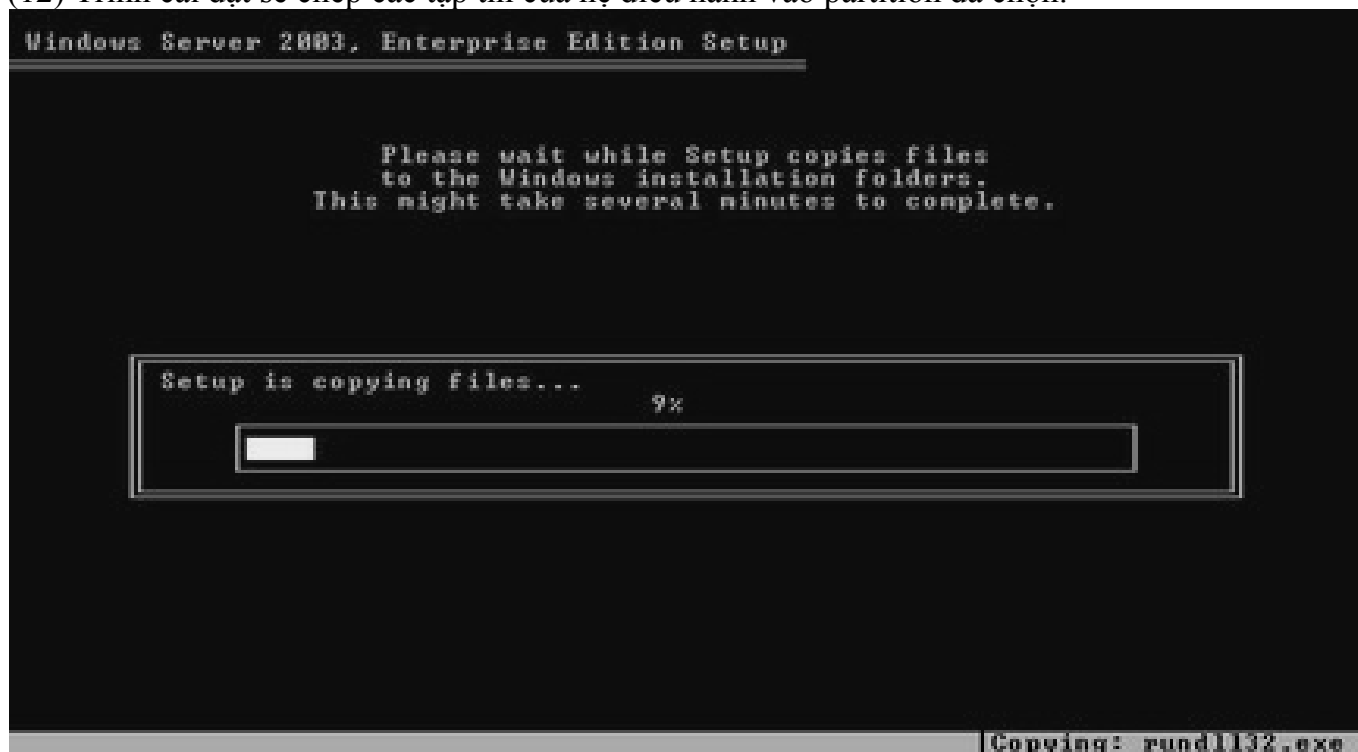


(11) Chọn kiểu hệ thống tập tin (FAT hay NTFS) để định dạng cho partition. Nhấn Enter để tiếp tục.





(12) Trình cài đặt sẽ chép các tập tin của hệ điều hành vào partition đã chọn.



(13) Khởi động lại hệ thống để bắt đầu giai đoạn Graphical Based. Trong khi khởi động, không nhấn bất kỳ phím nào khi hệ thống yêu cầu “Press any key to continue...”

#### **Giai đoạn Graphical-Based Setup.**

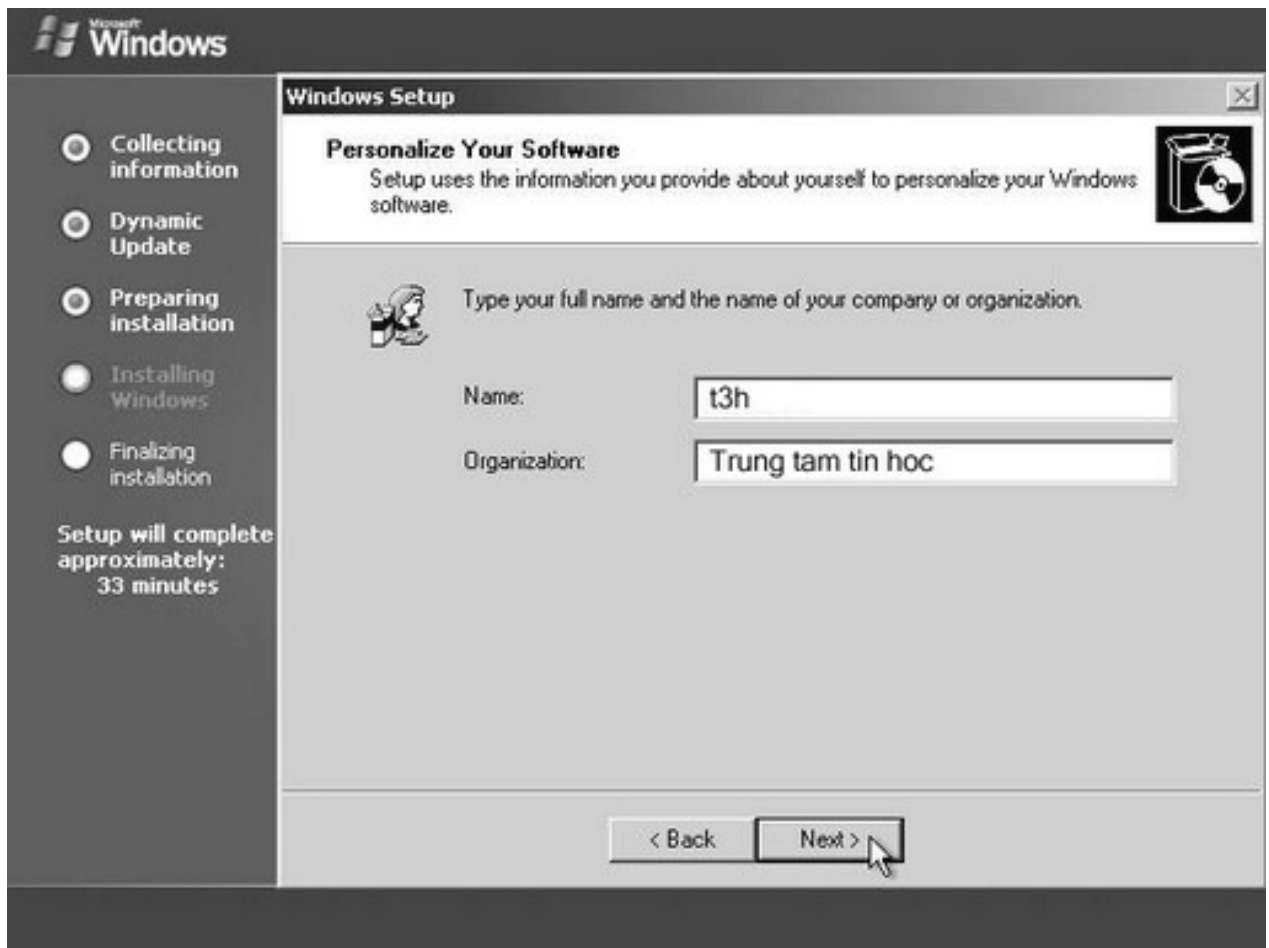
(1) Bắt đầu giai đoạn Graphical, trình cài đặt sẽ cài driver cho các thiết bị mà nó tìm thấy trong hệ thống.



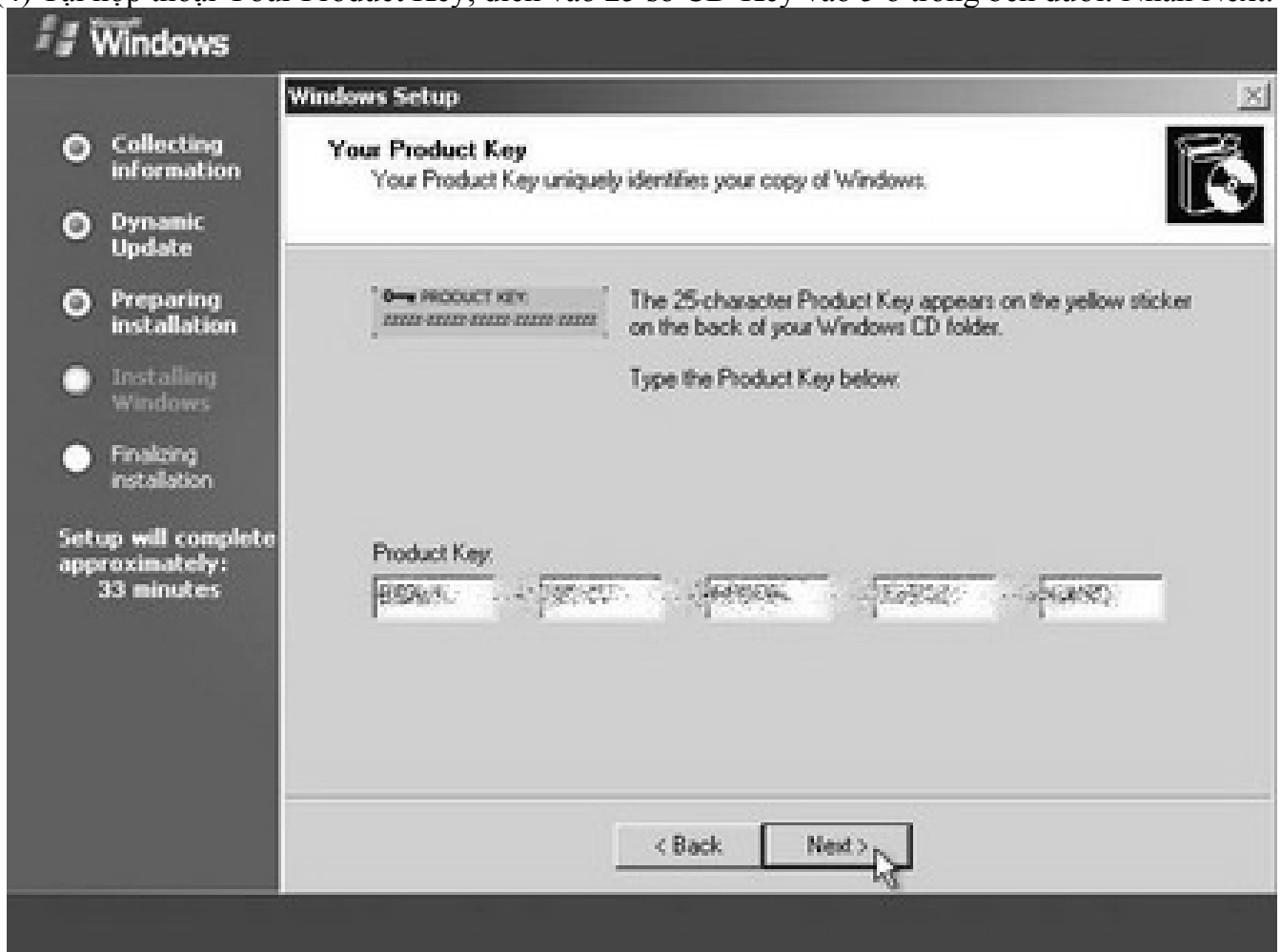
(2) Tại hộp thoại Regional and Language Options, cho phép chọn các tùy chọn liên quan đến ngôn ngữ, số đếm, đơn vị tiền tệ, định dạng ngày tháng năm,...Sau khi đã thay đổi các tùy chọn phù hợp, nhấn Next để tiếp tục.



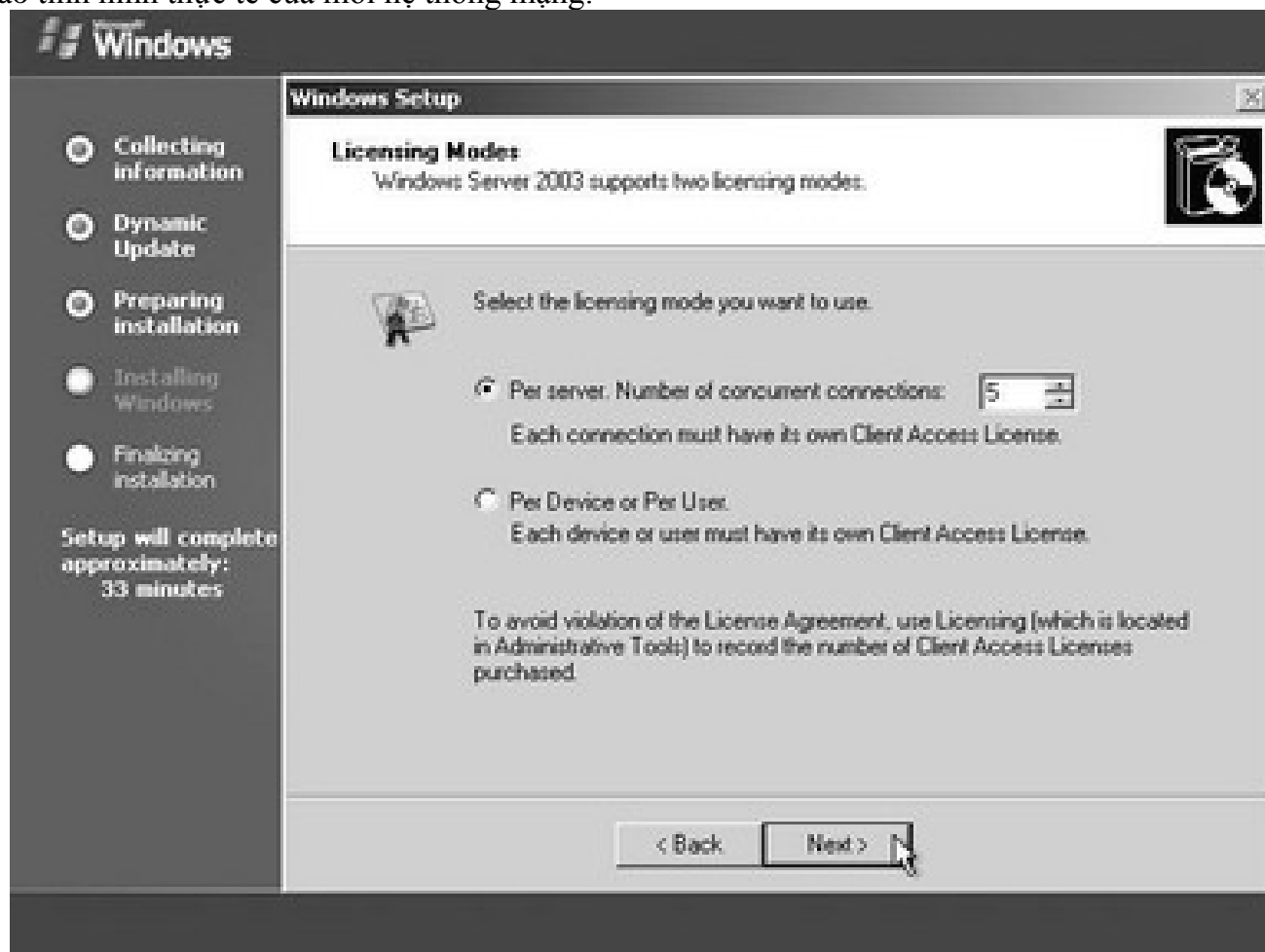
(3) Tại hộp thoại Personalize Your Software, điền tên người sử dụng và tên tổ chức. Nhấn Next.



(4) Tại hộp thoại Your Product Key, điền vào 25 số CD-Key vào 5 ô trống bên dưới. Nhấn Next.



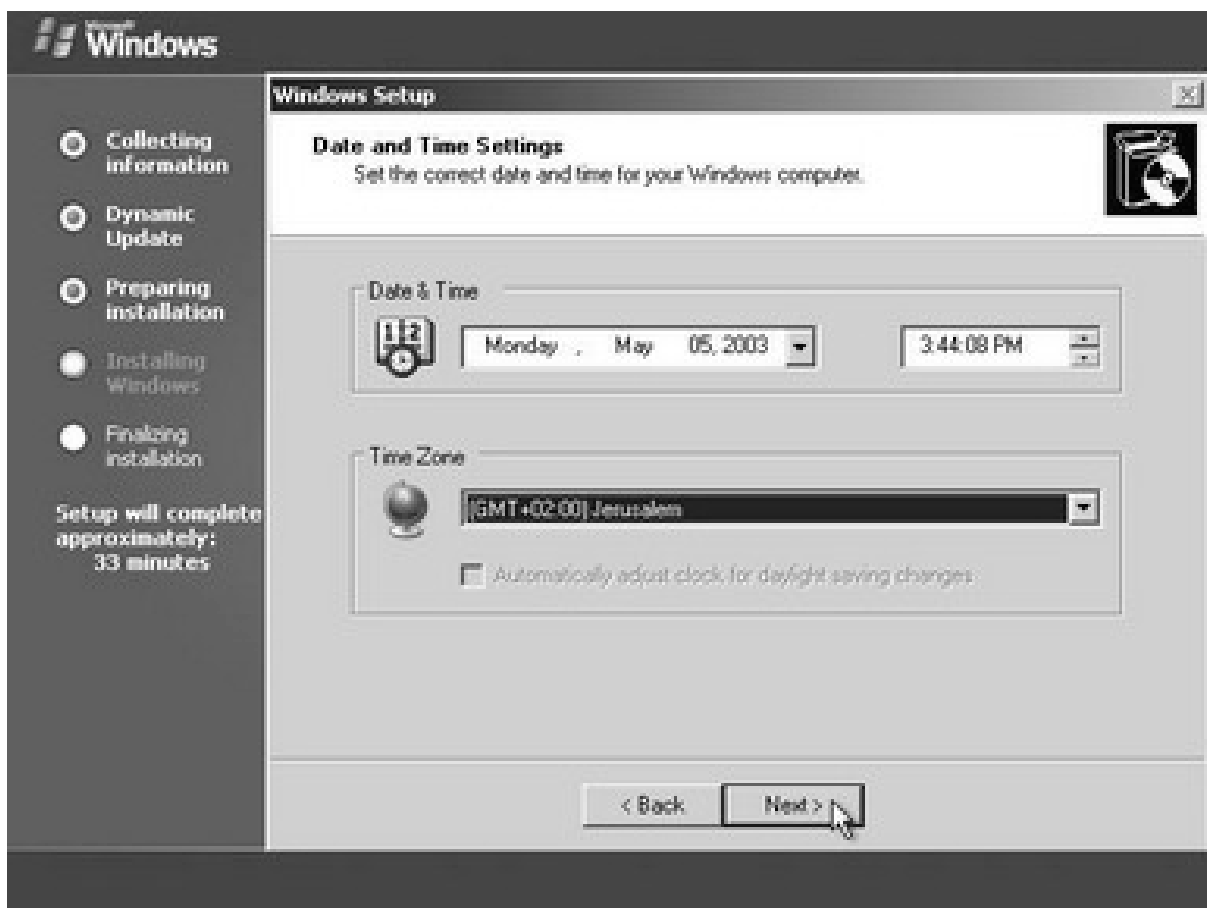
(5) Tại hộp thoại Licensing Mode, chọn chế độ bản quyền là Per Server hoặc Per Seat tùy thuộc vào tình hình thực tế của mỗi hệ thống mạng.



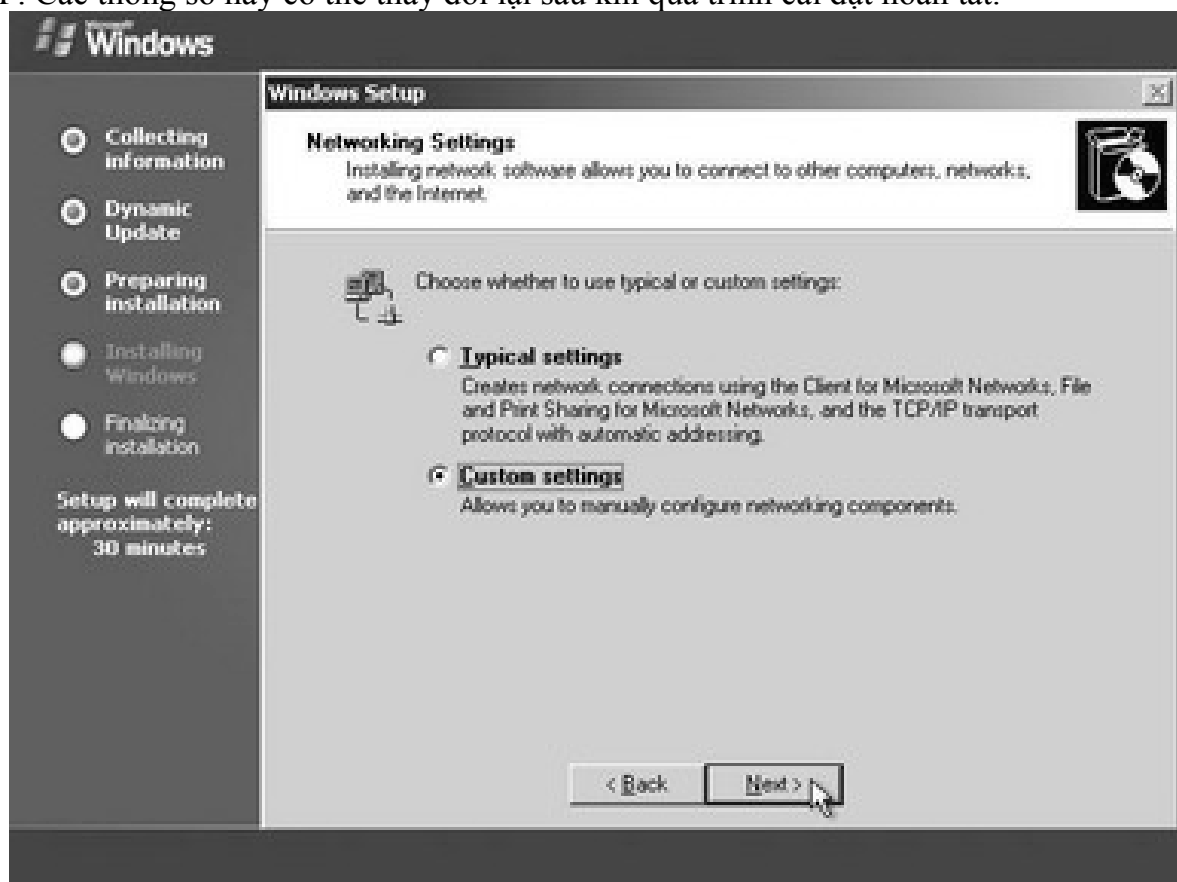
(6) Tại hộp thoại Computer Name and Administrator Password, điền vào tên của Server và Password của người quản trị (Administrator).



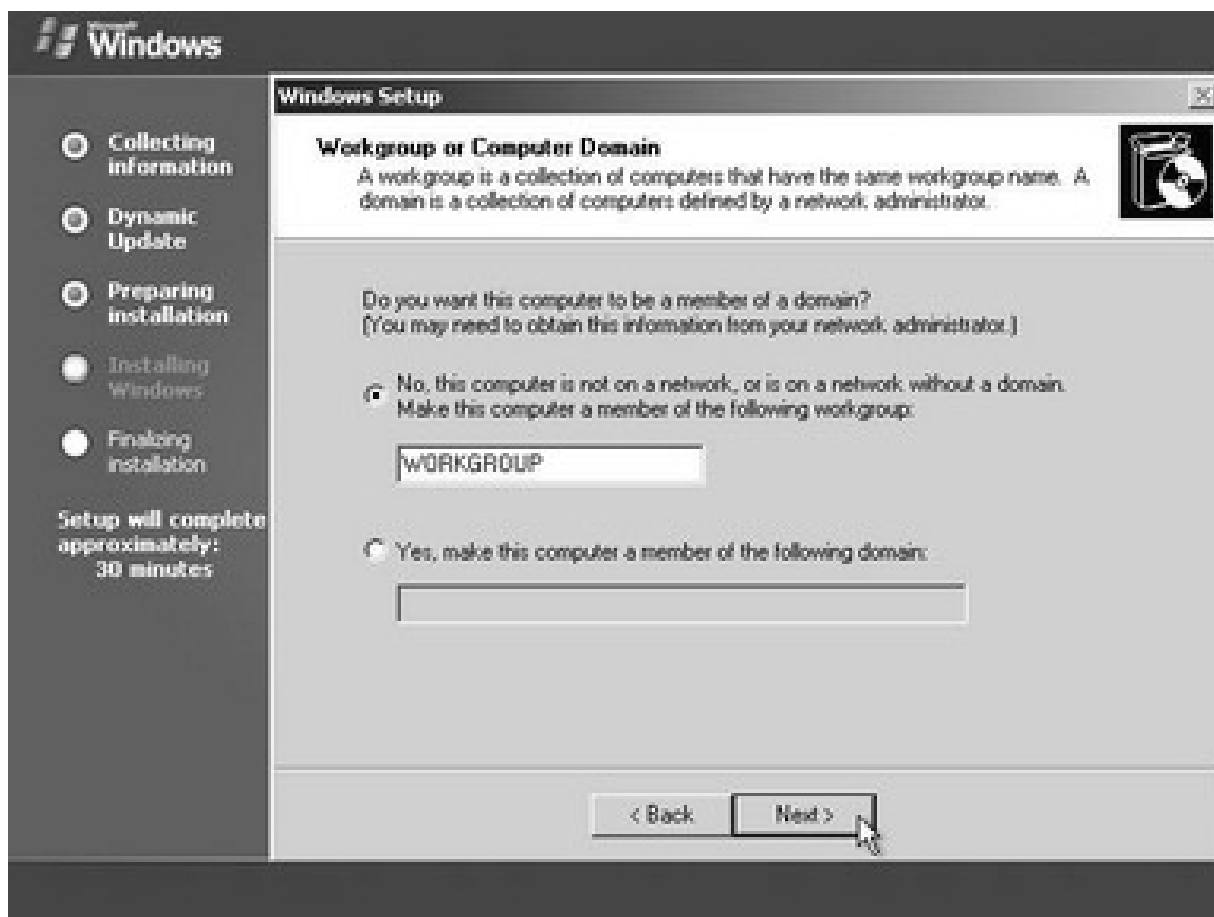
(7) Tại hộp thoại Date and Time Settings, thay đổi ngày, tháng, và múi giờ (Time zone) cho thích hợp.



(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.

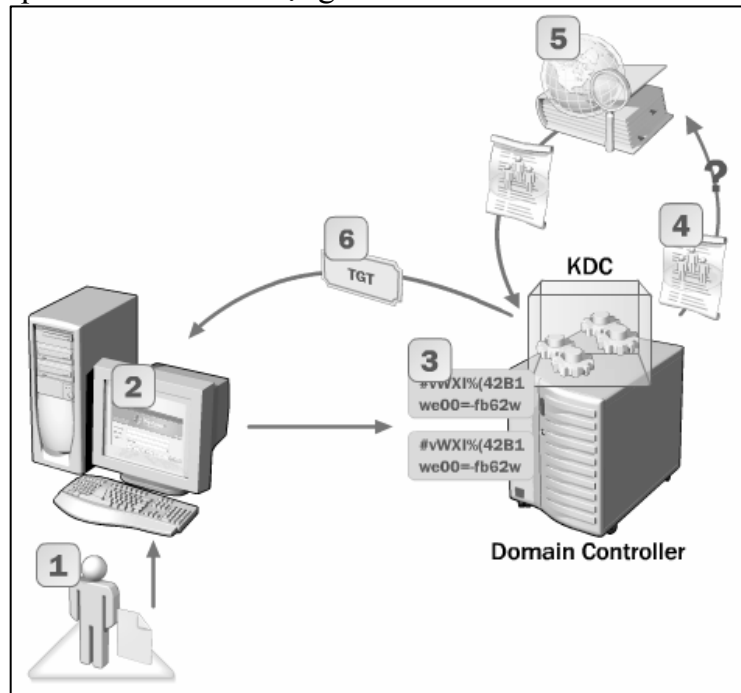


(10) Sau khi chép đầy đủ các tập tin, quá trình cài đặt kết thúc.

## BÀI 2: ACTIVE DIRECTORY

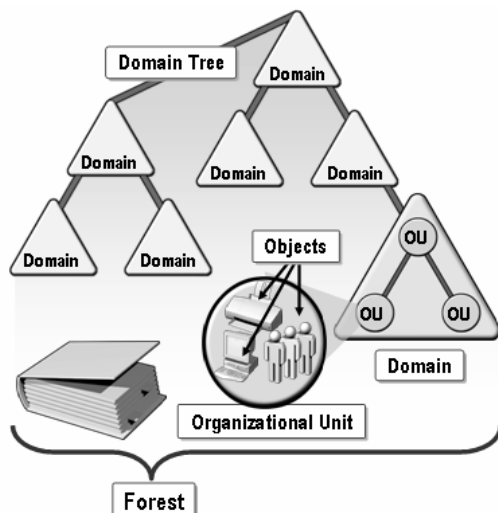
### I. GIỚI THIỆU

Active Directory là một cơ sở dữ liệu của các tài nguyên trên mạng (còn gọi là đối tượng) cũng như các thông tin liên quan đến các đối tượng đó





- 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.

### II. CÁC THÀNH PHẦN CỦA ACTIVE DIRECTORY



**a. 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.

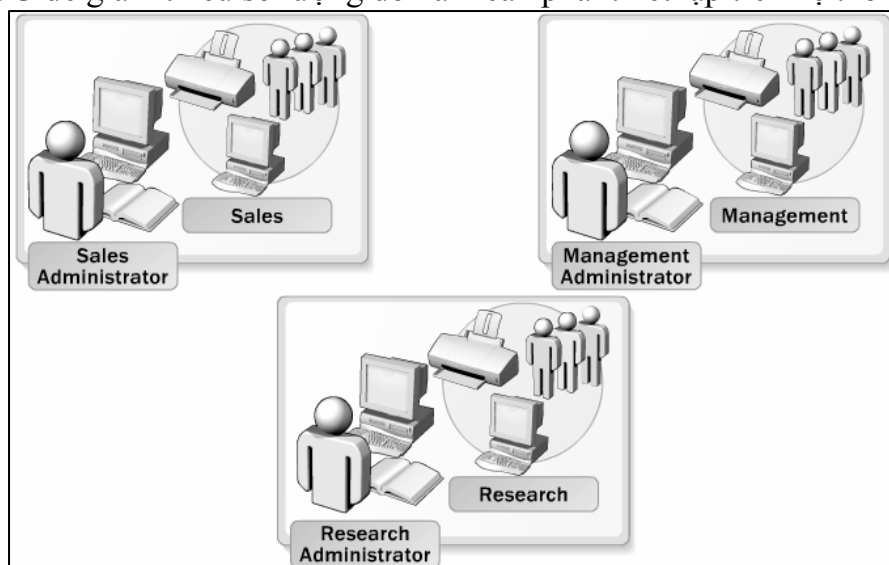
			
ColorPrinter1		KimYoshida	
Attributes	Values	Attributes	Values
IP address	172.16.0.0	Name	Kim Yoshida
Name	ColorPrinter1	Building	117
Building	117	Floor	1
Location	1342		

**b. 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.

**c. 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.

**d. 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 chúng ta 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, chúng ta 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. Chúng ta nên sử dụng OU để giảm thiểu số lượng domain cần phải thiết lập trên hệ thống.



#### e. 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.

- 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 chúng ta có di chuyển đối tượng đi đến khu vực khác.

### III. CÀI ĐẶT VÀ CẤU HÌNH MÁY ĐIỀU KHIỂN VÙNG

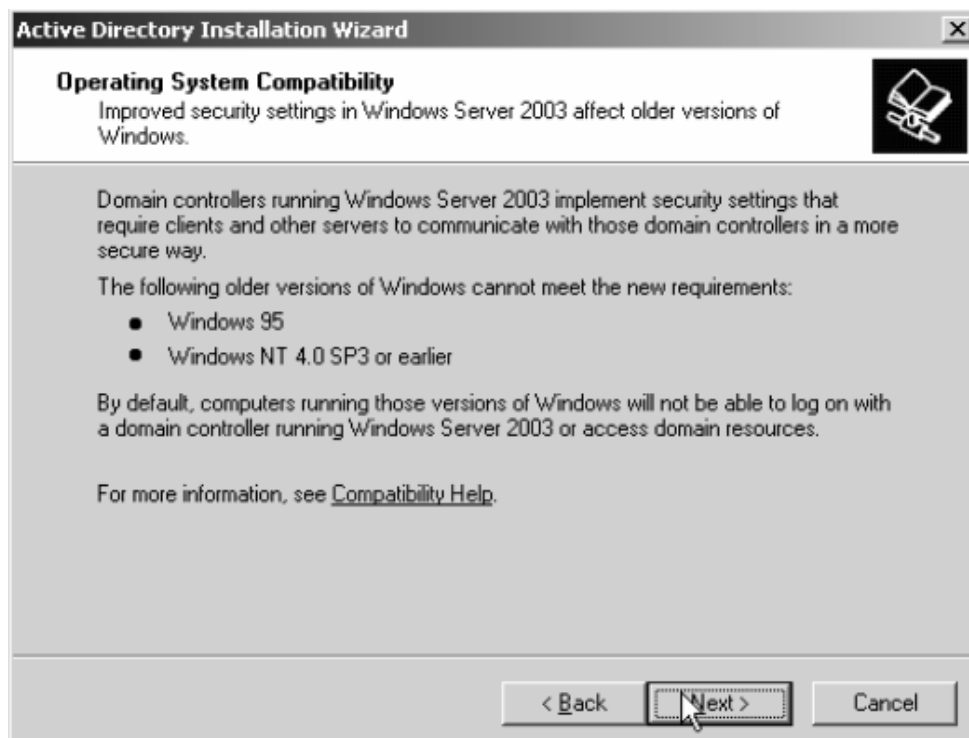
#### Nâng cấp Server thành Domain Controller

Chọn menu Start, nhập dcpromo trong hộp thoại Run và click OK

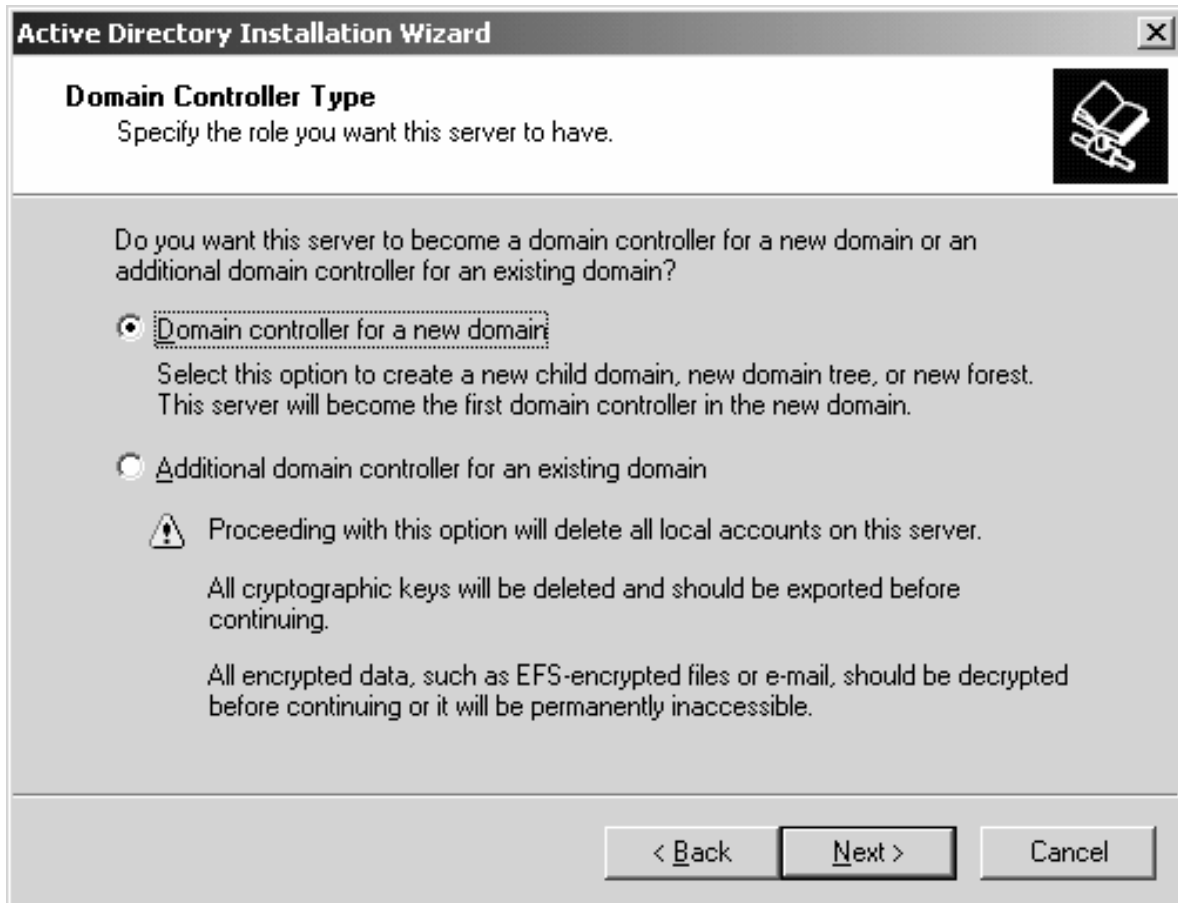
Khi đó, hộp thoại Active Directory Installation Wizard xuất hiện, chọn Next tiếp tục



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. Chọn Next để tiếp tục.

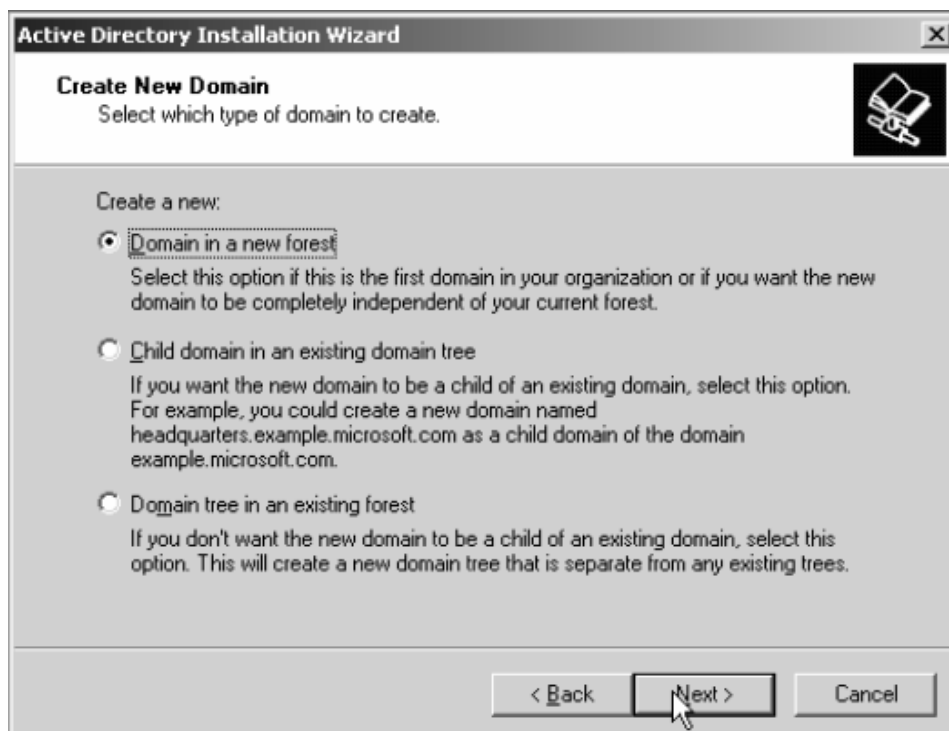


Trong hộp thoại Domain Controller Type, chọn mục Domain Controller for a New Domain và chọn Next. (Nếu muốn bổ sung máy điều khiển vùng vào một domain có sẵn thì chọn Additional domain controller for an existing domain.)

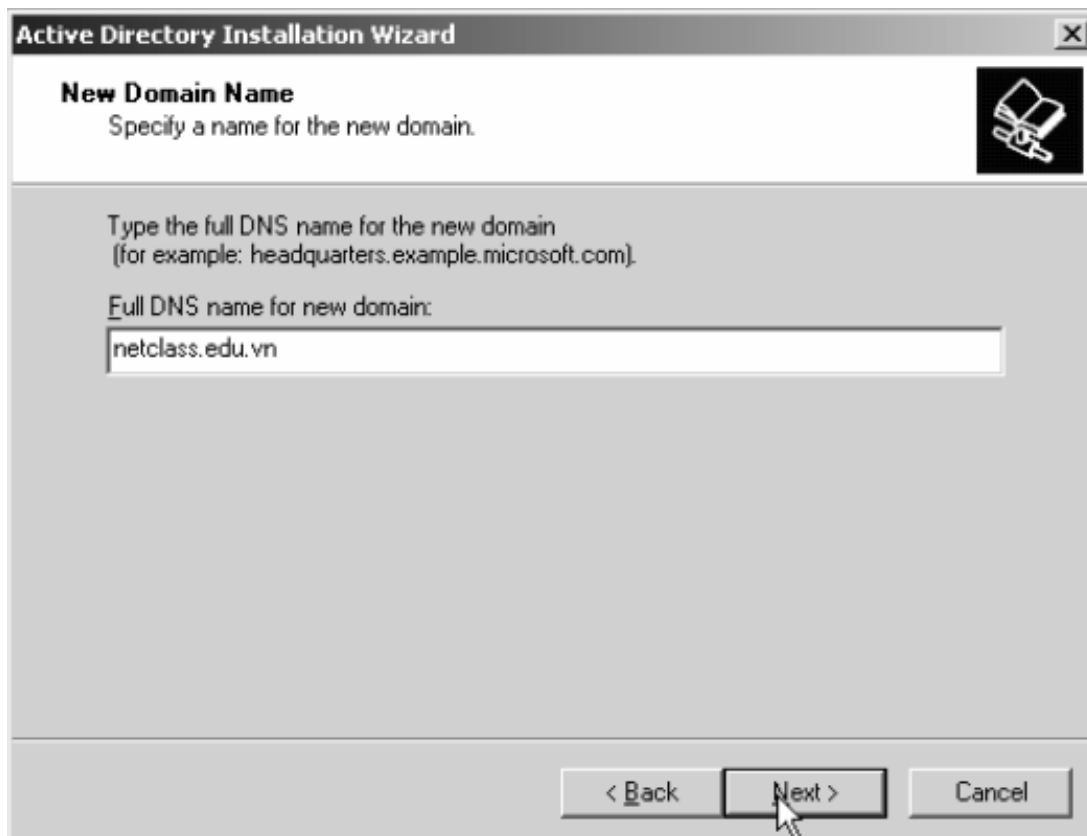


Đến đây chương trình cho phép chọn một trong ba lựa chọn sau:

- Domain in new forest: tạo domain đầu tiên trong một rừng mới
- Child domain in an existing domain tree: tạo ra một domain con dựa trên một cây domain có sẵn
- Domain tree in an existing forest: tạo ra một cây domain mới trong một rừng đã có sẵn.



Hộp thoại New Domain Name yêu cầu nhập tên DNS đầy đủ của domain cần xây dựng.



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'New Domain Name' with the instruction 'Specify a name for the new domain.' Below this, it says 'Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).' A text box labeled 'Full DNS name for new domain:' contains the text 'netclass.edu.vn'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Hộp thoại NetBIOS Domain Name: nhập 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, có thể đổi sang tên khác hoặc chấp nhận giá trị mặc định. Chọn Next để tiếp tục.



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'NetBIOS Domain Name' with the instruction 'Specify a NetBIOS name for the new domain.' Below this, it says 'This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.' A text box labeled 'Domain NetBIOS name:' contains the text 'NETCLASS'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Hộp thoại Database and Log Locations: chỉ định vị trí lưu trữ database Active Directory và các tập tin log. Có thể chỉ định vị trí khác hoặc chấp nhận giá trị mặc định. Tuy nhiên

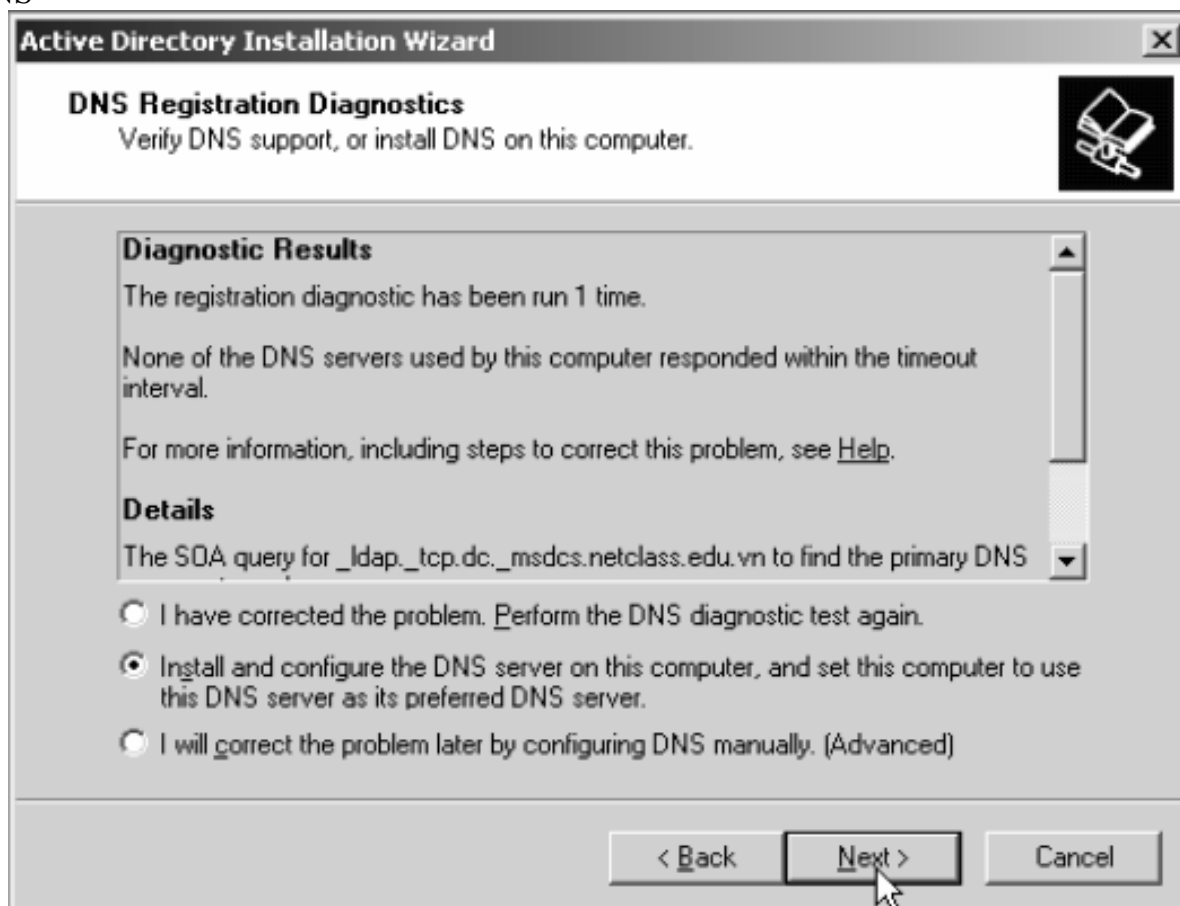
theo khuyến cáo của các nhà quản trị mạng thì chúng ta nên đặt tập tin chứa thông tin giao dịch (transaction log) ở một đĩa cứng vật lý khác với đĩa cứng chứa cơ sở dữ liệu của Active Directory nhằm tăng hiệu năng của hệ thống. Chọn Next để tiếp tục.

The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Database and Log Folders' step. The title bar reads 'Active Directory Installation Wizard'. Below the title bar, the section is titled 'Database and Log Folders' with a subtitle 'Specify the folders to contain the Active Directory database and log files.' and a folder icon. The main area contains instructions: 'For best performance and recoverability, store the database and the log on separate hard disks.' and the question 'Where do you want to store the Active Directory database?'. Below this, there is a 'Database folder:' label, a text box containing 'C:\WINDOWS\NTDS', and a 'Browse...' button. Another question follows: 'Where do you want to store the Active Directory log?'. Below this, there is a 'Log folder:' label, a text box containing 'C:\WINDOWS\NTDS', and another 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Hộp thoại Shared System Volume: 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. 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 thì sẽ xuất hiện một thông báo lỗi yêu cầu phải đổi hệ thống tập tin).

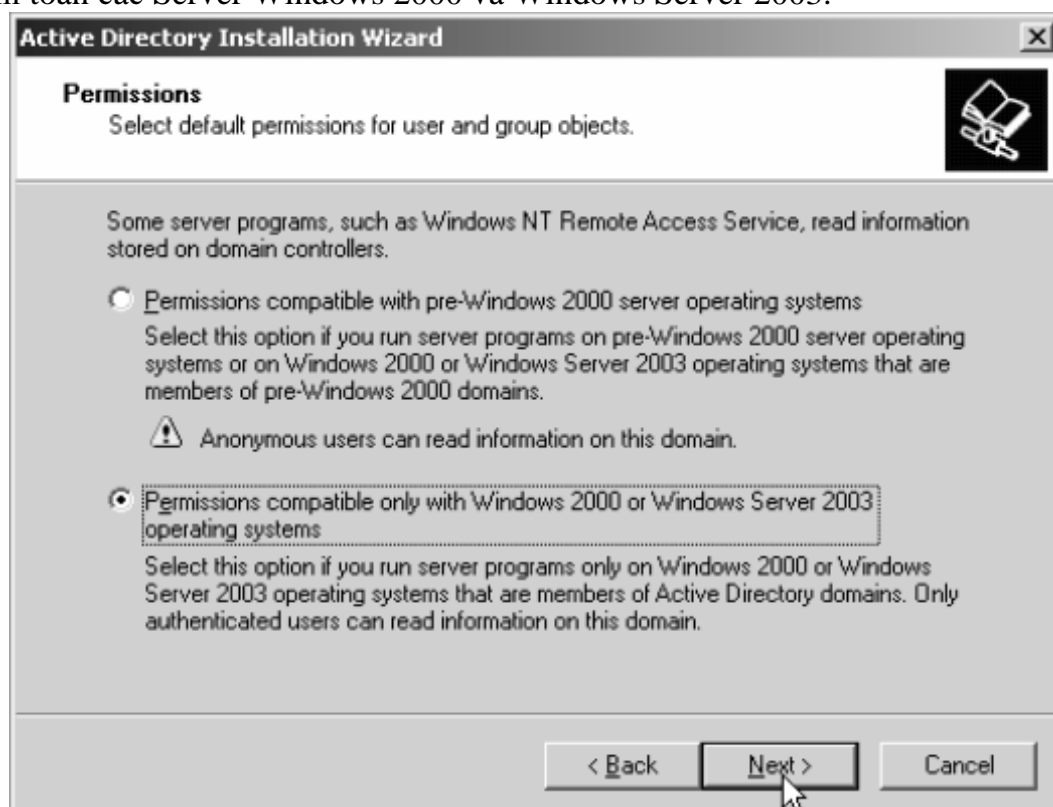
The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Shared System Volume' step. The title bar reads 'Active Directory Installation Wizard'. Below the title bar, the section is titled 'Shared System Volume' with a subtitle 'Specify the folder to be shared as the system volume.' and a folder icon. The main area contains instructions: 'The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.' and 'The SYSVOL folder must be located on an NTFS volume.' It then asks 'Enter a location for the SYSVOL folder.' Below this, there is a 'Folder location:' label, a text box containing 'C:\WINDOWS\SYSVOL', and a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Trong hộp thoại xuất hiện bạn chọn lựa chọn thứ hai để hệ thống tự động cài đặt và cấu hình dịch vụ DNS

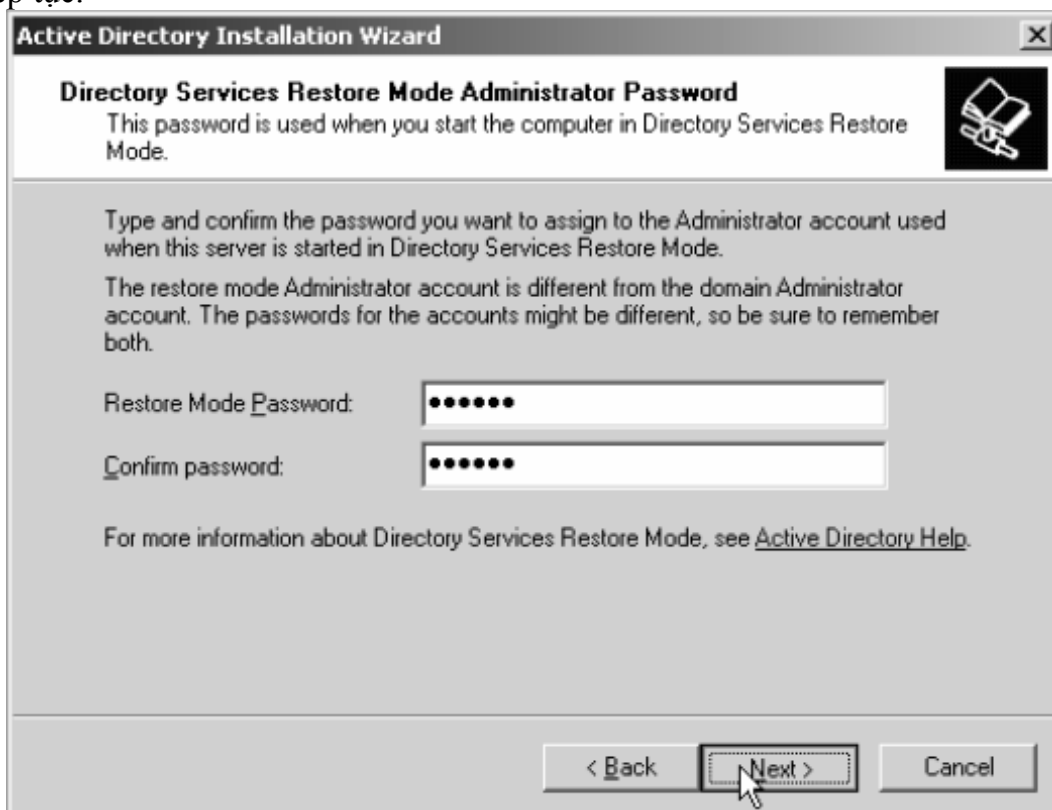


Trong hộp thoại Permissions:

- Permission Compatible with pre-Windows 2000 servers: khi hệ thống có các Server phiên bản trước Windows 2000
- Permissions compatible only with Windows 2000 servers or Windows Server 2003 khi hệ thống chỉ toàn các Server Windows 2000 và Windows Server 2003.

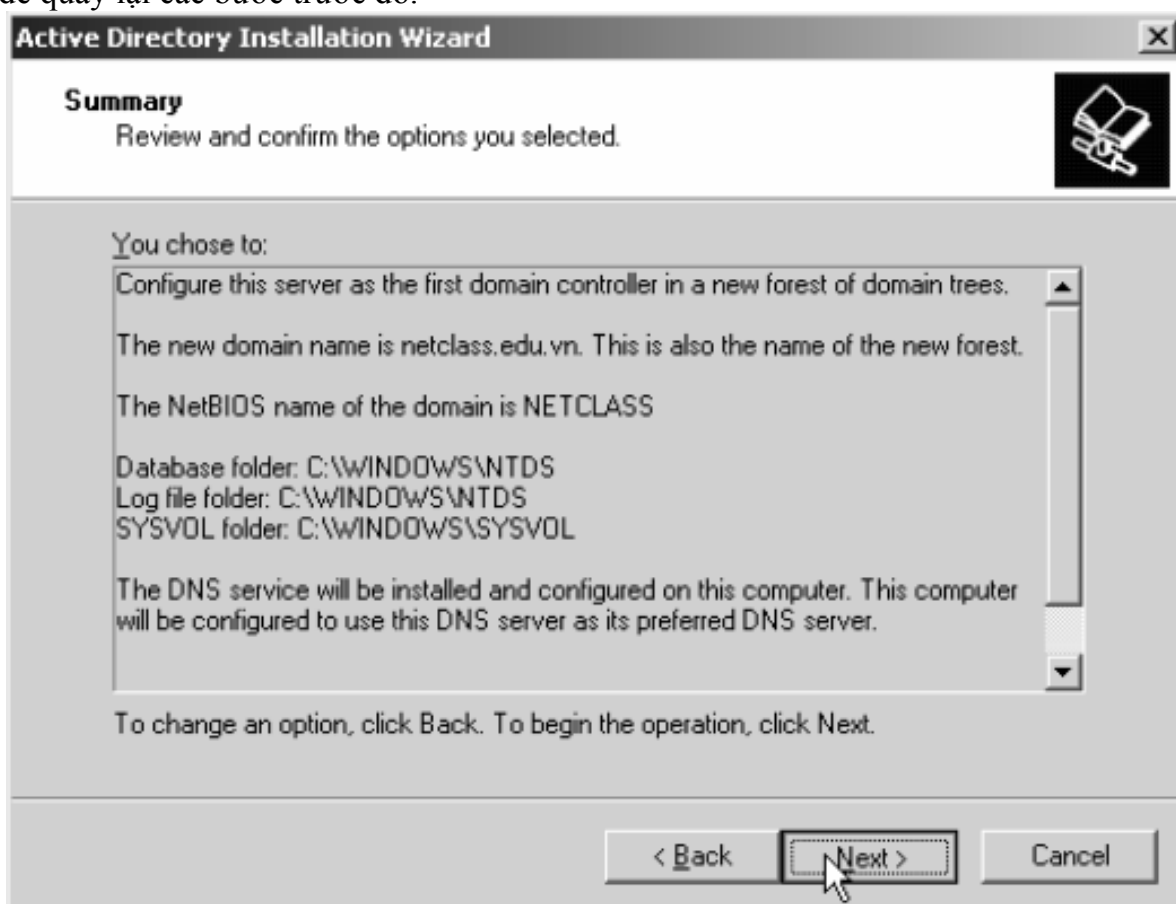


Trong hộp thoại Directory Services Restore Mode Administrator Password, nhập mật khẩu dùng trong trường hợp Server phải khởi động vào chế độ Directory Services Restore Mode. Nhấn chọn Next để tiếp tục.



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar says 'Active Directory Installation Wizard'. The main heading is 'Directory Services Restore Mode Administrator Password'. Below the heading, it says 'This password is used when you start the computer in Directory Services Restore Mode.' There is a small icon of a book with a hand pointing to it. The main text area contains instructions: 'Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode. The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.' Below this, there are two password input fields. The first is labeled 'Restore Mode Password:' and the second is labeled 'Confirm password:'. Both fields contain six dots. At the bottom, there is a link: 'For more information about Directory Services Restore Mode, see [Active Directory Help](#).' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

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



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar says 'Active Directory Installation Wizard'. The main heading is 'Summary'. Below the heading, it says 'Review and confirm the options you selected.' There is a small icon of a book with a hand pointing to it. The main text area contains a list of options chosen: 'You chose to: Configure this server as the first domain controller in a new forest of domain trees. The new domain name is netclass.edu.vn. This is also the name of the new forest. The NetBIOS name of the domain is NETCLASS Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.' At the bottom, there is a note: 'To change an option, click Back. To begin the operation, click Next.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Hộp thoại Configuring Active Directory cho biết quá trình cài đặt đang thực hiện những gì. Quá trình này sẽ chiếm nhiều thời gian.



### **Gia nhập máy trạm vào Domain**

Click chuột phải trên biểu tượng My Computer, chọn Properties, hộp thoại System Properties xuất hiện

Trong Tab Computer Name, click chuột vào nút Change. Hộp thoại nhập liệu xuất hiện, nhập tên miền của mạng cần gia nhập vào mục Member of Domain.



**Computer Name Changes** [?] [X]

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name:  
PC01

Full computer name:  
PC01.

[More...]

Member of

☒ Domain:  
netclass.edu.vn

☐ Workgroup:  
WORKGROUP

[OK] [Cancel]

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



**Computer Name Changes** [?] [X]

Enter the name and password of an account with permission to join the domain.

User name: administrator [v] [X]

Password: [.....]

[OK] [Cancel]



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 khởi động máy lại để đăng nhập vào mạng.

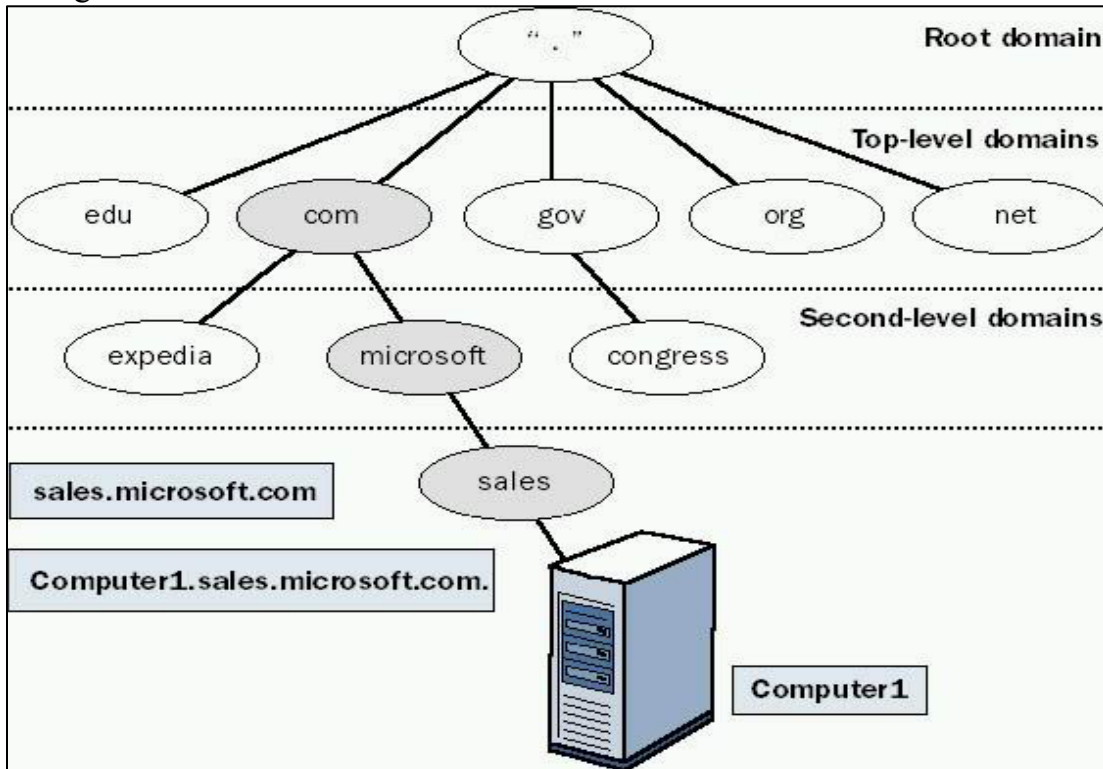


# BÀI 3: DỊCH VỤ DNS

## I. GIỚI THIỆU

DNS là một hệ thống phân cấp (hierachical) được dùng để xác định các máy tính trong mạng nội bộ cũng như trên internet. DNS có các đặc điểm sau:

- Có chức năng xác định một máy tính dựa vào tên gọi nhớ thay cho địa chỉ IP.
- Có cơ chế quản lý và lưu trữ thông tin về danh sách các tên và địa chỉ IP tương ứng với các tên này một cách phân tán.
- Phân giải tên thành địa chỉ IP, các máy tính/thiết bị sẽ sử dụng địa chỉ IP này để thực hiện truyền thông với nhau.



Mỗi máy tính cung cấp dịch vụ DNS (name server) sẽ chịu trách nhiệm về một phần của DNS namespace (zone). Mỗi zone bao gồm một domain hoặc một domain và một số subdomains.

### Các loại name server:

- Primary name server: Quản lý database của zone mà nó phụ trách.
- Secondary name server: chứa bản sao database của zone mà nó phụ trách.
- Caching-only server: Không chứa database của bất kỳ zone nào, Caching-only server chỉ có khả năng đại diện DNS client truy vấn thông tin từ các name server khác và cache lại nội dung này.
- Stub name server: các server này chứa thông tin về stub zone. Stub zone chứa danh sách các name server của một zone (master zone). Nhiệm vụ chính của stub server là giúp cho các name server của zone cha biết được danh sách cập nhật các name server trên các zone con.

### Các loại resource record:

Resource records là nội dung chủ yếu trong database của DNS server. Có các loại resource records như sau:

- Host (A) record: giúp ánh xạ domain name (tên máy tính) với một địa chỉ IP.
- Alias (CNAME) record: giúp ánh xạ nhiều tên vào một máy tính cụ thể.
- MX record: giúp xác định mailserver cho một domain.
- PTR record: loại resource record này có ý nghĩa trái với loại resource record A. PTR record cho biết một địa chỉ IP tương ứng với domain nào.

- SRV resource record: loại resource record này giúp xác định vị trí của một số dịch vụ. Một số ứng dụng đặc biệt có thể “hiểu” được SRV record sẽ truy vấn name server để xác định dịch vụ cần tìm kiếm đang ở trên máy tính nào, dịch vụ đang lắng nghe trên port nào...
- SOA record(Start Of Authority): DNS server đầu tiên có quyền trả lời yêu cầu DNS đến Client
- NS record (Name Server) : Máy chủ quản lý DNS zone

## II. CÀI ĐẶT VÀ CẤU HÌNH

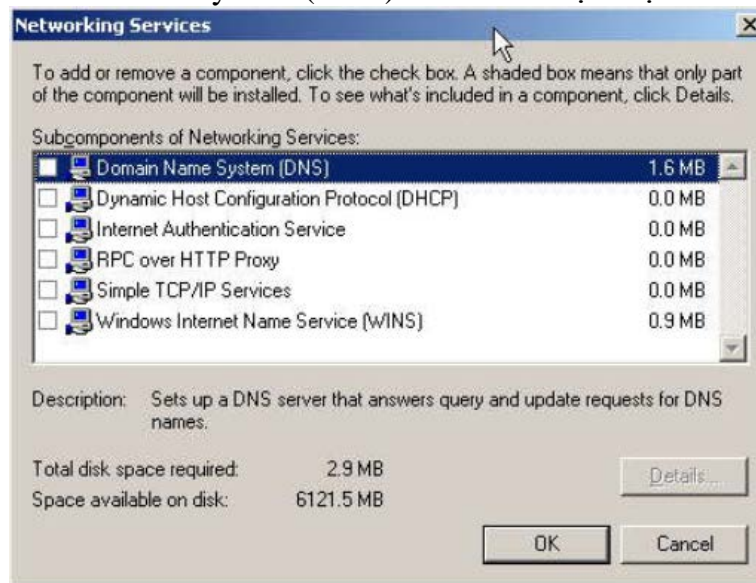
### II.1. Cài đặt dịch vụ DNS

B1: Mở Add/Remove Programs trong Control Panel

B2: chọn Add/Remove Windows Components

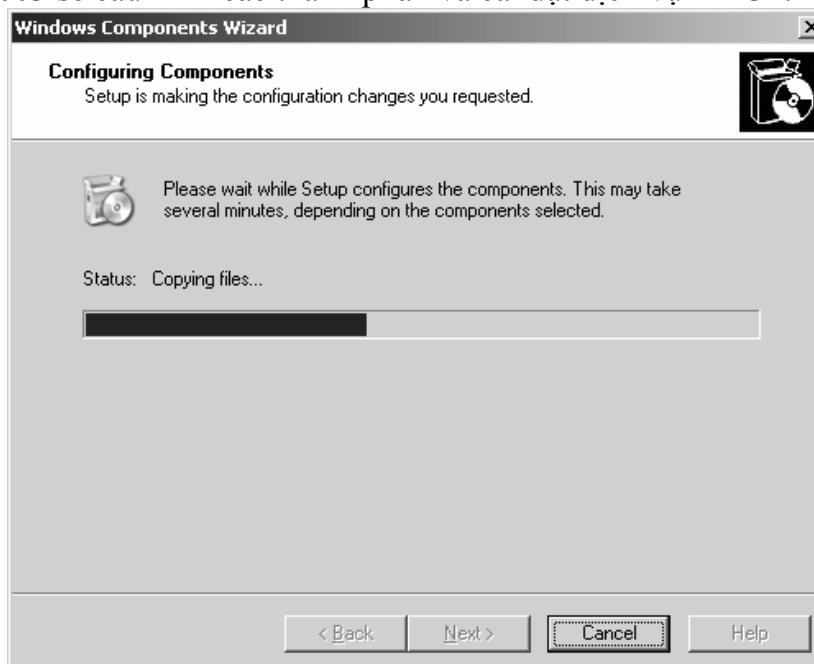
B3: Trong hộp thoại Windows Components Wizard, click chuột lên Network Services, chọn Details

B4: Đánh dấu chọn Domain Name system (DNS) và click chuột chọn OK



Trở lại hộp thoại Windows Components Wizard, nhấn chọn Next.

Windows Server 2003 sẽ cấu hình các thành phần và cài đặt dịch vụ DHCP.



Cuối cùng, trong hộp thoại Completing the Windows Components Wizard, nhấn chọn Finish để kết thúc.

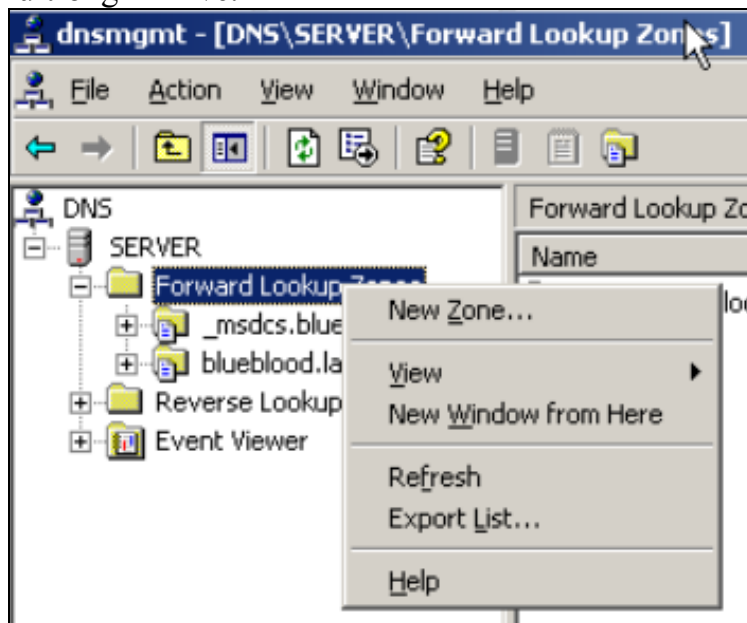
## II.2. Tạo Zone trong DNS

DNS có 2 loại zone:

- o Forward Lookup zone: zone chịu trách nhiệm chuyển domain name (tên miền) thành địa chỉ IP.
- o Reverse Lookup Zone: chịu trách nhiệm trái với Forward Lookup Zone, chuyển địa chỉ IP thành domain name

B1. Mở chương trình cấu hình DNS server trong mục Administrative Tools.

B2. Chọn New zone như trong hình vẽ.



B3: Chọn loại zone muốn tạo. 3 loại zone ở đây tương ứng với 3 loại Name Server (đã được trình bày ở trên). Ở ví dụ này, ta chọn Primary zone.

B4: Chọn tên file chứa cơ sở dữ liệu của zone.

B5. Chọn cách thức DNS server cập nhật những thay đổi của resource record. Ví dụ về thay đổi resource record là: một máy trong mạng thay đổi địa chỉ IP nên dẫn đến phải thay đổi A record của máy tính tương ứng. DNS có thể tự động điều chỉnh cho phù hợp với những thay đổi này (dynamic update) hoặc người quản trị phải can thiệp thủ công. Ở đây ta chọn chế độ cập nhật thay đổi một cách thủ công.

B6. Chọn finish để hoàn thành việc tạo zone.

## II.3. Khảo sát một số thuộc tính cơ bản của Zone

Khi vừa tạo ra, mỗi zone có một số record mặc định.

**SOA record:** chứa một số thông tin cơ bản mô tả cho zone.

Các thuộc tính của một SOA record.

The screenshot shows the 'khntn.edu Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The 'Serial number' is 1, 'Primary server' is server.blueblood.lan, and 'Responsible person' is hostmaster.blueblood.lan. The 'Refresh interval' is 15 minutes, 'Retry interval' is 10 minutes, 'Expires after' is 1 days, and 'Minimum (default) TTL' is 1 hours. The 'TTL for this record' is 0:1:0:0. Buttons for 'Increment', 'Browse...', 'OK', 'Cancel', and 'Apply' are visible.

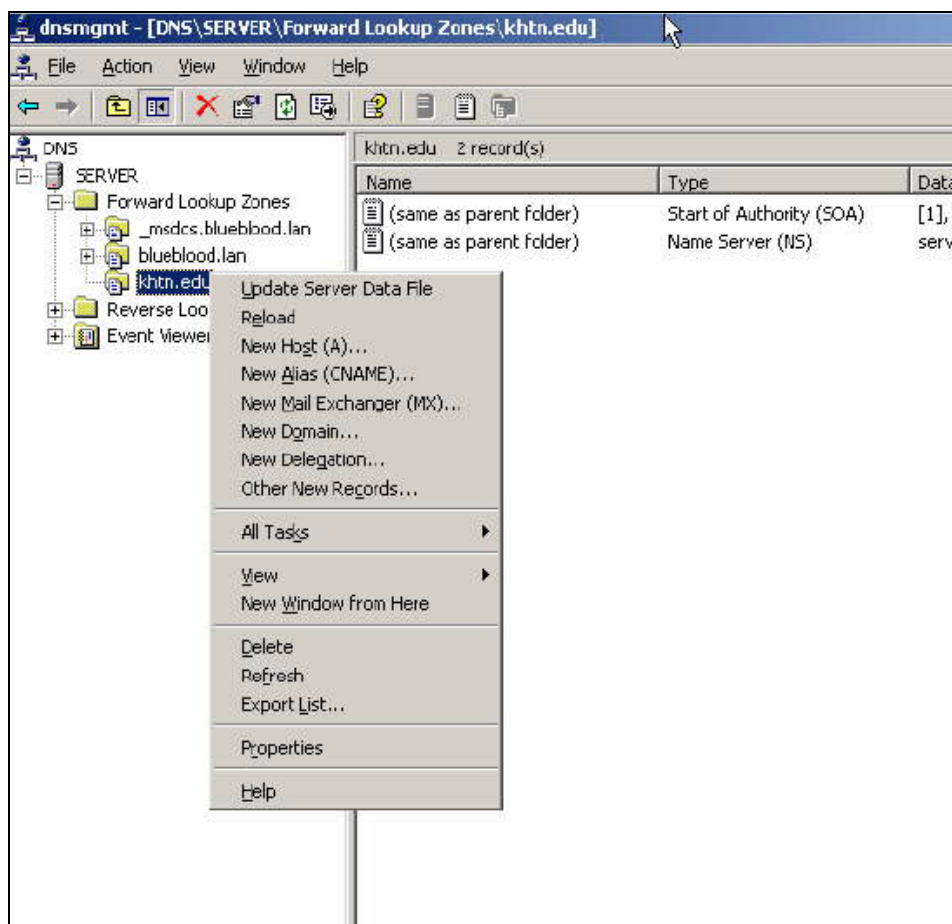
- Serial number: dùng để xác định version của thông tin trên primary server. Mỗi khi có thay đổi trên Primary server, số này sẽ được tăng lên 1, secondary server sẽ dựa trên thông tin này để quyết định việc cập nhật lại thông tin.
- Refresh interval: cứ sau một khoảng thời gian được chỉ ra ở thuộc tính này, secondary server sẽ đồng bộ hóa dữ liệu của nó với primary server.
- Retry interval: nếu secondary server không nhận được phản hồi từ primary server, sau khoảng thời gian được xác định ở thuộc tính này, secondary sẽ thử thực hiện đồng bộ hóa lại.
- Expires after: Nếu sau khoảng thời gian xác định ở thuộc tính này mà secondary vẫn không đồng bộ hóa dữ liệu được với primary server, secondary sẽ tạm dừng trả lời những truy vấn của DNS client.
- TTL: DNS server có cache lại những thông tin về domain name mà bản thân nó có được do truy vấn những DNS server khác. Giá trị TTL (Time to live) xác định khoảng thời gian mà những thông tin cache này có hiệu lực. Sau khoảng thời gian xác định ở thuộc tính này, DNS server sẽ xóa những thông tin nó đã cache.

**NS records:** những loại record này xác định các name server có trong domain.

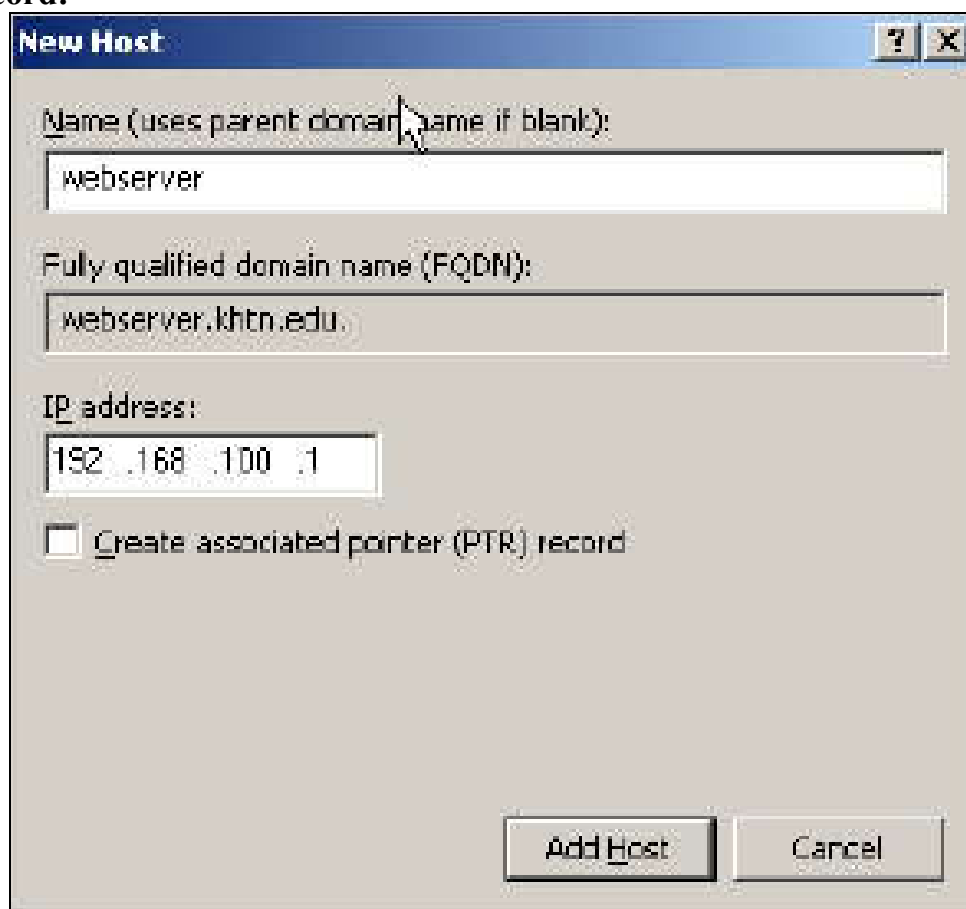
#### II.4. Tạo các Resource Record

Click chuột phải lên domain sẽ chứa resource record ta muốn tạo.

Chọn loại record cần tạo.



### Tạo Host record:



Trong ví dụ trên, máy tính có địa chỉ IP là 192.168.100.1 có domain name là webserver.khtn.edu. Ta có thể tạo PTR record tương ứng ở cửa sổ này.

### Tạo Alias record

**New Resource Record**

Alias (CNAME)

Alias name (uses parent domain if left blank):

Fully qualified domain name (FQDN):

Fully qualified domain name (FQDN) for target host:

OK Cancel

Trong ví dụ trên, máy tính có tên webserver.khtn.edu còn có thể được truy cập tới bằng tên [www.khtn.edu](http://www.khtn.edu)

### Tạo MX record

**New Resource Record**

Mail Exchanger (MX)

Host or child domain:

By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.

Fully qualified domain name (FQDN):

Fully qualified domain name (FQDN) of mail server:

Mail server priority:

OK Cancel

Trong ví dụ trên, emails gửi tới địa chỉ xyz@khtn.edu sẽ được chuyển tới mail server có domain name là mailserver.khtn.edu



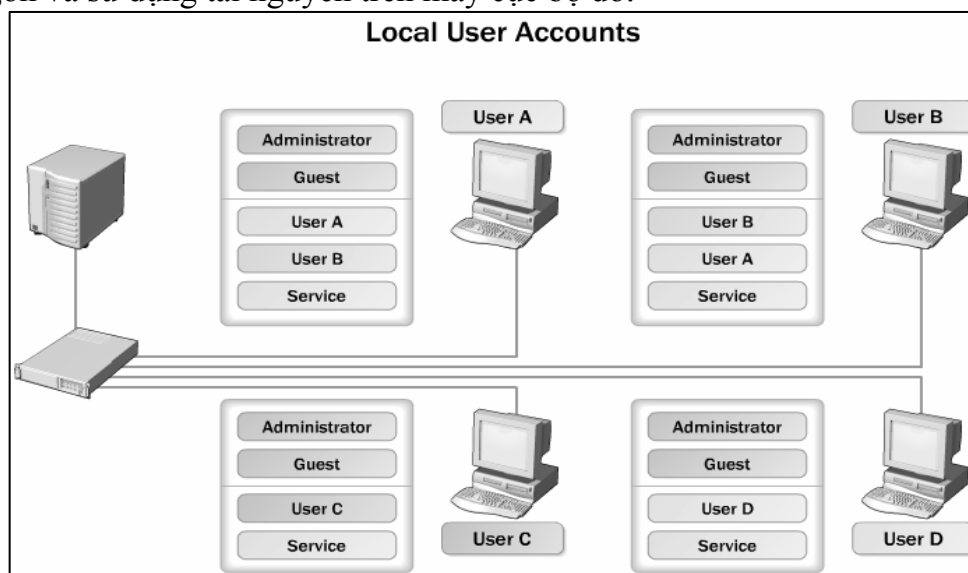


# BÀI 4: QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM

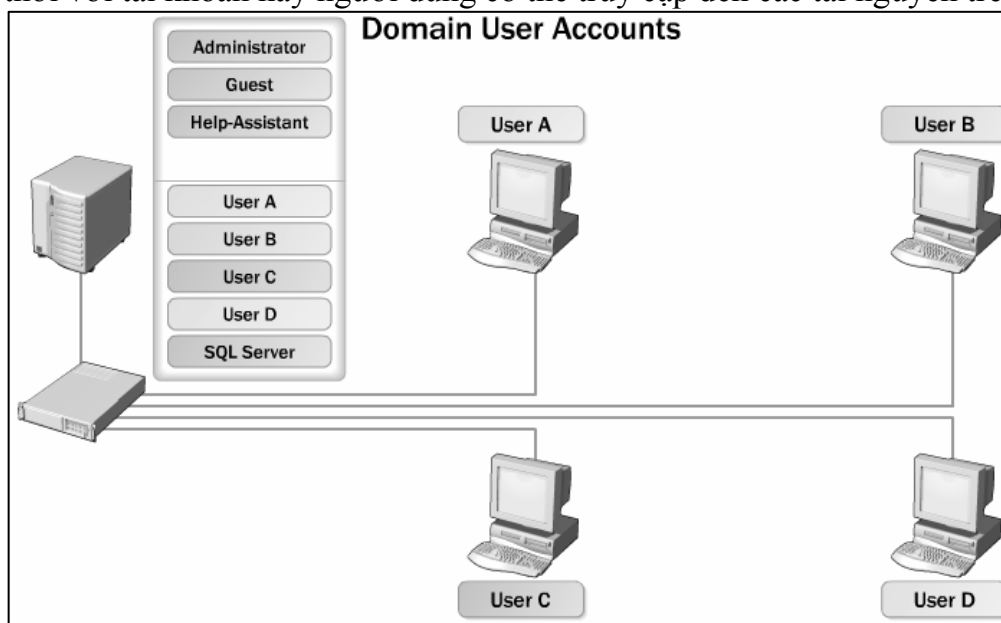
## I. ĐỊNH NGHĨA TÀI KHOẢN NGƯỜI DÙNG VÀ TÀI KHOẢN NHÓM

### I.1 Tài khoản người dùng (user account)

- Là một đối tượng quan trọng đại diện cho người dùng trên mạng
- Được phân biệt với nhau thông qua chuỗi nhận dạng username, từ đó người dùng có thể truy cập vào các tài nguyên mạng mà người dùng được phép.
- Tài khoản người dùng cục bộ (local user account): tài khoản được định nghĩa trên máy cục bộ, chỉ có thể logon và sử dụng tài nguyên trên máy cục bộ đó.



- 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.



### Yêu cầu về tài khoản người dùng

- Mỗi username phải có từ 1 đến 20 ký tự
- Không thể có 2 username giống nhau
- Không chứa các ký tự sau: \* / \ [ ] ; : | = , + “ ? < >
- Có thể chứa dấu chấm câu (.), gạch ngang, gạch nối

## I.2. Tài khoản nhóm (Group account)

- Một đối tượng đại diện cho một nhóm người nào đó, dùng cho việc quản lý chung các đối tượng người dùng

- 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.**

### Nhóm bảo mật (Security Group)

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): được định nghĩa 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): 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.

### Nhóm phân phối (Distribution group)

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). Gặp lại loại nhóm này khi làm việc với phần mềm MS Exchange.

## II. TẠO MỚI TÀI KHOẢN NGƯỜI DÙNG

B1: Trong cửa sổ Active Directory User and Computer, click chuột phải trên mục Users, chọn New -> User. Xuất hiện hộp thoại New User

**New Object - User**

Create in: netclass.com/Users

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

< Back Next > Cancel

B2: Nhập các thông tin họ tên, user logon name (username), Chọn Next, xuất hiện hộp thoại định nghĩa mật khẩu cho tài khoản

**New Object - User**

Create in: netclass.com/Users

Password:

Confirm password:

☐ User must change password at next logon

☒ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

B3: Nhập mật khẩu cần tạo cho tài khoản người dùng và các tùy chọn

- User must change password at next logon: bắt buộc người dùng phải đổi mật khẩu sau khi đăng nhập vào mạng lần đầu tiên
- User cannot change password: người dùng không có quyền thay đổi mật khẩu
- Password never expires: mật khẩu không bị giới hạn thời gian
- Account is disabled: tài khoản bị tắt, không thể đăng nhập vào mạng.

Chọn Next tiếp tục



**New Object - User**

Create in: netclass.com/Users

When you click Finish, the following object will be created:

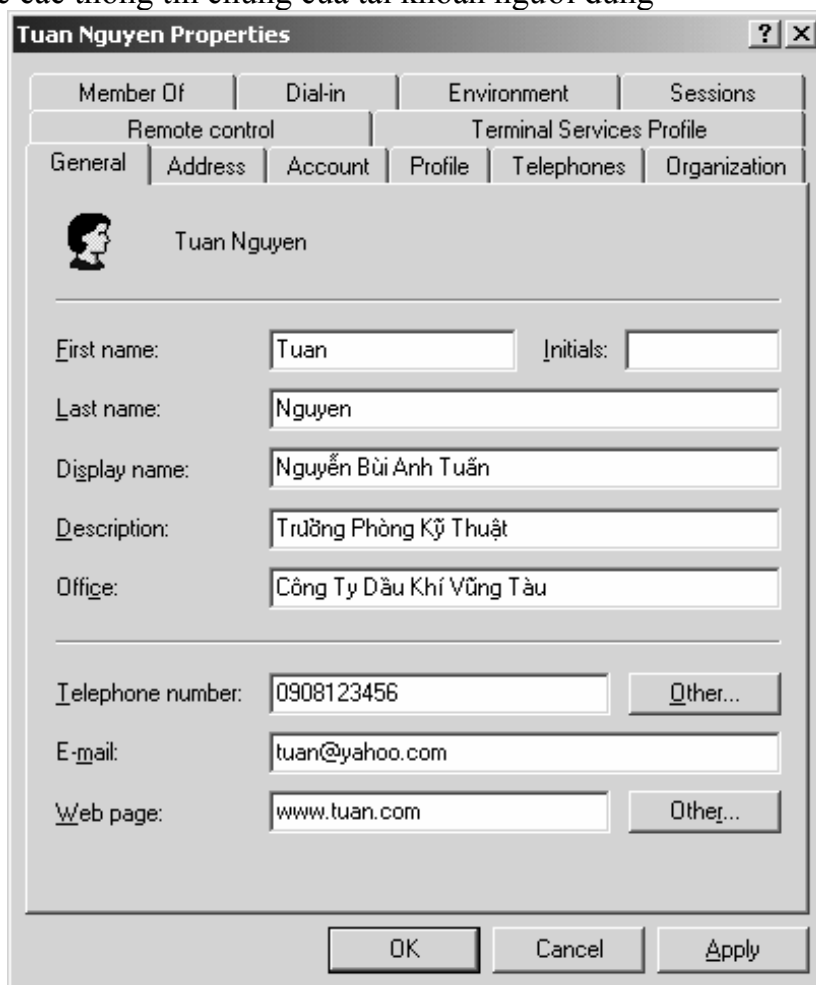
Full name: Tuan Nguyen  
 User logon name: tuan@netclass.com  
 The user cannot change the password.  
 The password never expires.

< Back Finish Cancel

B4: Chọn Finish hoàn tất tạo tài khoản người dùng mới

### III. CÁC THÔNG TIN MỞ RỘNG CỦA TÀI KHOẢN NGƯỜI DÙNG

**Tab General:** Chức các thông tin chung của tài khoản người dùng



**Tuan Nguyen Properties**

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

Tuan Nguyen

First name: Tuan Initials:   
 Last name: Nguyen  
 Display name: Nguyễn Bùi Anh Tuấn  
 Description: Trưởng Phòng Kỹ Thuật  
 Office: Công Ty Dầu Khí Vũng Tàu

Telephone number: 0908123456 Other...  
 E-mail: tuan@yahoo.com  
 Web page: www.tuan.com Other...

OK Cancel Apply

**Tab Address:** Khai báo chi tiết các thông tin liên lạc với người dùng

**Tuan Nguyen Properties** [?] [X]

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

Street: 123 Nguyễn Văn Cù, Quận 5.

P.O. Box:

City: Thành Phố Hồ Chí Minh

State/province: TP

Zip/Postal Code: 08

Country/region: VIET NAM

OK Cancel Apply

**Tab Telephone:** khai báo chi tiết số điện thoại liên hệ của người dùng

**Tuan Properties** [?] [X]

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

Telephone numbers

Home: 84-8-8451245 Other...

Pager: Other...

Mobile: 0918123456 Other...

Fax: 84-8-8451246 Other...

IP phone: 84-8-8451247 Other...

Notes:

OK Cancel Apply

**Tab Organization:** Khai báo các thông tin người dùng về: chức năng của công ty, tên phòng ban, tên công ty

**ntuan Properties** [?] [X]

Member Of | Dial-in | Environment | Sessions

Remote control | Terminal Services Profile

General | Address | Account | Profile | Telephones | Organization

Title: Kinh Doanh

Department: Phòng Kinh Doanh

Company: Công Ty Dầu Khí Vũng Tàu

Manager

Name: [ ]

Change... View Clear

Direct reports:

[ ]

OK Cancel Apply

**Tab account:** 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...

**Tuan Nguyen Properties** [?] [X]

Member Of | Dial-in | Environment | Sessions

Remote control | Terminal Services Profile

General | Address | Account | Profile | Telephones | Organization

User login name: tuan @netclass.com

User login name (pre-Windows 2000): NETCLASS\tuan

Logon Hours... Log On To...

☐ Account is locked out

Account options:

☐ User must change password at next logon

☒ User cannot change password

☒ Password never expires

☐ Store password using reversible encryption

Account expires

☒ Never

☐ End of: Tuesday, May 20, 2003

OK Cancel Apply

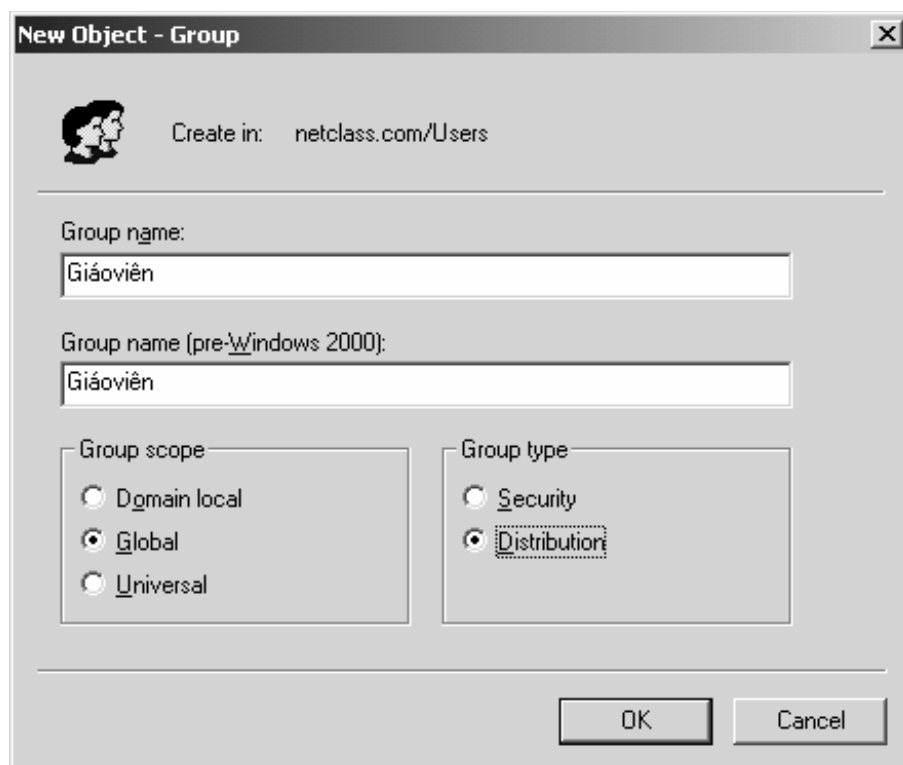
Tab Member Of: Khai báo tài khoản người dùng là thành viên của các tài khoản nhóm nào



#### IV. TẠO MỚI TÀI KHOẢN NHÓM

Trước khi tạo tài khoản nhóm, 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, thực hiện các bước sau:

B1: Click phải chuột vào mục Users, chọn New -> Group. Xuất hiện hộp thoại New Object – Group



B2: 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.

B3: Chọn OK hoàn tất.



# BÀI 5: DỊCH VỤ DHCP

## I. GIỚI THIỆU DỊCH VỤ DHCP

DHCP (Dynamic Host Configuration Protocol) được phát triển để hỗ trợ cho vấn đề theo dõi và cấp phát địa chỉ IP cho mỗi thiết bị trên mạng có dùng giao thức TCP/IP. Để làm một DHCP Server, máy phục vụ Windows Server 2003 phải đáp ứng các điều kiện sau:

- Đã cài dịch vụ DHCP
  - Mỗi Interface phải được cấu hình bằng một địa chỉ IP tĩnh
  - Người quản trị đã chuẩn bị sẵn danh sách các địa chỉ IP định cấp phát cho các máy client.
- Dịch vụ DHCP cho phép chúng ta cấp phát động các thông số cấu hình mạng cho các máy trạm (client). Các hệ điều hành của Microsoft và các hệ điều hành khác như Unix hoặc Macintosh đều hỗ trợ cơ chế nhận các thông số động, có nghĩa là trên các hệ điều hành này phải có một DHCP Client. Cơ chế sử dụng các thông số mạng được cấp phát động có ưu điểm hơn so với cơ chế khai báo tĩnh các thông số mạng như:
- Khắc phục được tình trạng đụng địa chỉ IP và giảm chi phí quản trị cho hệ thống mạng.
  - Giúp cho các nhà cung cấp dịch vụ (ISP) tiết kiệm được số lượng địa chỉ IP thật (Public IP).
  - Phù hợp cho các máy tính thường xuyên di chuyển qua lại giữa các mạng.
  - Kết hợp với hệ thống mạng không dây (Wireless) cung cấp các điểm Hotspot như: nhà ga, sân bay, trường học...

## II. HOẠT ĐỘNG CỦA DHCP

Giao thức DHCP làm việc theo mô hình Client/Server.

- Khi máy client khởi động, máy sẽ gửi broadcast gói tin DHCPDISCOVER, yêu cầu một server phục vụ mình. Gói tin này cũng chứa địa chỉ MAC của máy client.
- Các máy Server trên mạng khi nhận được gói tin yêu cầu đó, nếu còn khả năng cung cấp địa chỉ IP, đều gửi lại cho máy Client gói tin DHCPOFFER, đề nghị cho thuê một địa chỉ IP trong một khoảng thời gian nhất định, kèm theo là một subnet mask và địa chỉ của Server. Server sẽ không cấp phát địa chỉ IP vừa đề nghị cho những Client khác trong suốt quá trình thương thuyết.
- Máy Client sẽ lựa chọn một trong những lời đề nghị (DHCPOFFER) và gửi broadcast lại gói tin DHCPREQUEST chấp nhận lời đề nghị đó. Điều này cho phép các lời đề nghị không được chấp nhận sẽ được các Server rút lại và dùng để cấp phát cho Client khác.
- Máy Server được Client chấp nhận sẽ gửi ngược lại một gói tin DHCPACK như là một lời xác nhận, cho biết là địa chỉ IP đó, subnet mask đó và thời hạn cho sử dụng đó sẽ chính thức được áp dụng. Ngoài ra Server còn gửi kèm theo những thông tin cấu hình bổ sung như địa chỉ của gateway mặc định, địa chỉ DNS Server, ...

## III. CÀI ĐẶT DỊCH VỤ DHCP

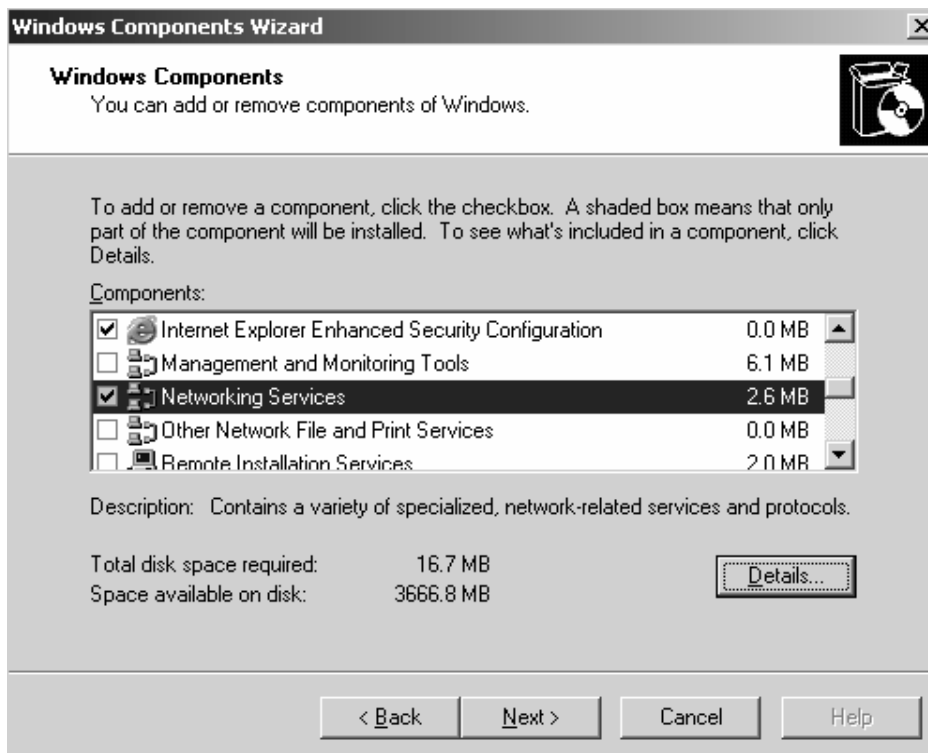
Vào menu Start → Setting → Control Panel

Trong cửa sổ Control Panel, click đôi chuột vào Add/Remove Programs

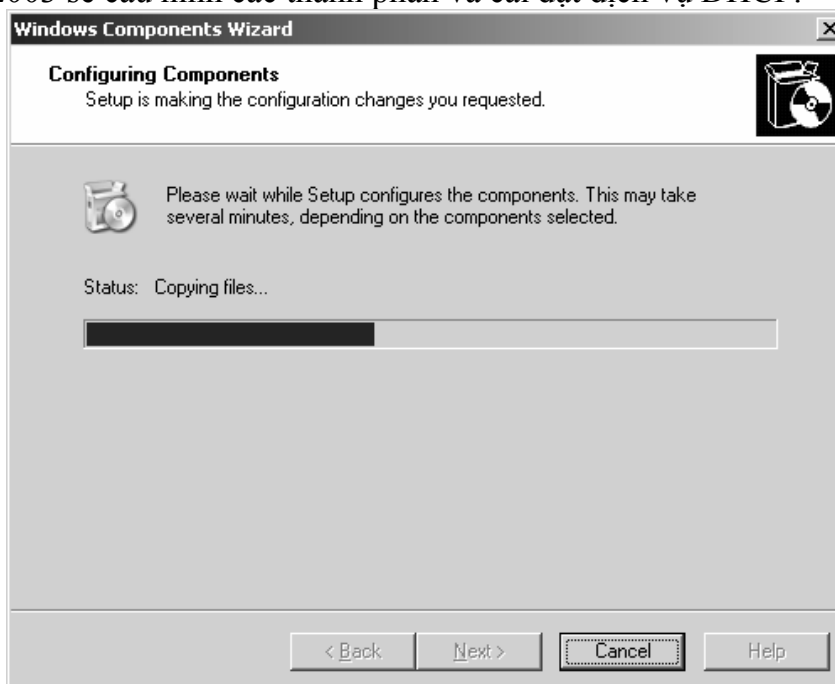
Trong hộp thoại Add/Remove Programs, chọn Add/Remove Windows Components

Trong hộp thoại Windows Components Wizard, click chuột lên Network Services, chọn Details

Trong hộp thoại Network Services, đánh dấu chọn Dynamic Host Configuration Protocol (DHCP) và click chuột chọn OK



Trở lại hộp thoại Windows Components Wizard, nhấn chọn Next.  
Windows Server 2003 sẽ cấu hình các thành phần và cài đặt dịch vụ DHCP.



Cuối cùng, trong hộp thoại Completing the Windows Components Wizard, nhấn chọn Finish để kết thúc.

#### IV. CHỨNG THỰC DỊCH VỤ DHCP TRONG ACTIVE DIRECTORY

Windows Server 2003 chạy dịch vụ DHCP trên đó lại làm việc trong một domain (có thể là một Server thành viên bình thường hoặc là một máy điều khiển vùng), dịch vụ muốn có thể hoạt động bình thường thì phải được chứng thực bằng Active Directory.

Mục đích của việc chứng thực này là để không cho các Server không được chứng thực làm ảnh hưởng đến hoạt động mạng. Chỉ có những Windows 2003 DHCP Server được chứng thực mới được phép hoạt động trên mạng. Giả sử có một nhân viên nào đó cài đặt dịch vụ DHCP và cấp những thông tin TCP/IP không chính xác. DHCP Server của nhân viên này không thể hoạt động được (do không được quản trị mạng cho phép) và do đó không ảnh hưởng đến hoạt động trên

mạng. Chỉ có Windows 2003 DHCP Server mới cần được chứng thực trong Active Directory. Còn các DHCP server chạy trên các hệ điều hành khác như Windows NT, UNIX, ... thì không cần phải chứng thực.

Trong trường hợp máy Windows Server 2003 làm DHCP Server không nằm trong một domain thì cũng không cần phải chứng thực trong Active Directory. Bạn có thể sử dụng công cụ quản trị DHCP để tiến hành việc chứng thực một DHCP Server. Các bước thực hiện như sau:

Chọn menu Start / Administrative Tools / DHCP.

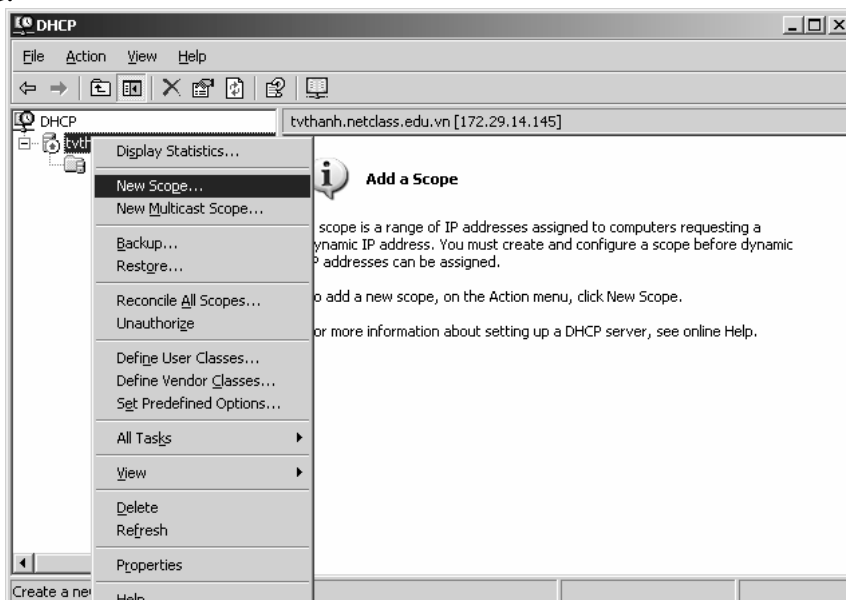
Trong ô bên trái của cửa sổ DHCP, tô sáng Server bạn định chứng thực. Chọn menu Action / Authorize. Đợi một hoặc hai phút sau, chọn lại menu Action / Refresh. Bây giờ DHCP đã được chứng thực, bạn để ý biểu tượng kế bên tên Server là một mũi tên màu xanh hướng lên (thay vì là mũi tên màu đỏ hướng xuống).

## V. CẤU HÌNH DỊCH VỤ DHCP

Sau khi đã cài đặt dịch vụ DHCP, bạn sẽ thấy biểu tượng DHCP trong menu Administrative Tools. Thực hiện theo các bước sau để tạo một scope cấp phát địa chỉ:

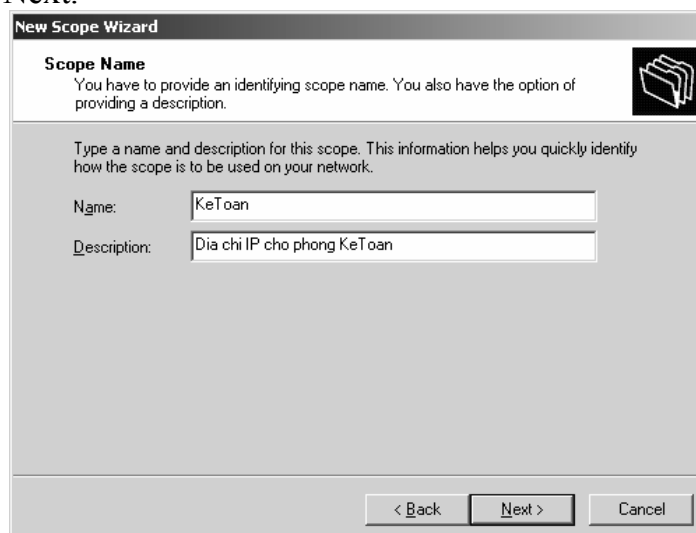
Chọn menu Start / Programs / Administrative Tools / DHCP.

Trong cửa sổ DHCP, nhấp phải chuột lên biểu tượng Server của bạn và chọn mục New Scope trong popup menu.

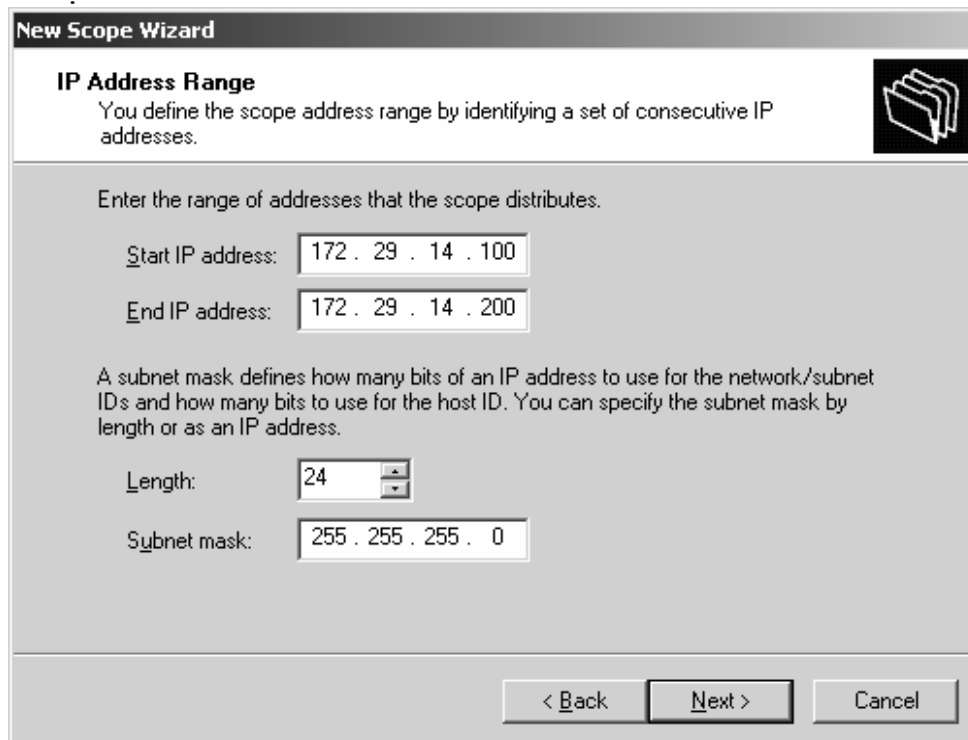


Hộp thoại New Scope Wizard xuất hiện. Nhấn chọn Next.

Trong hộp thoại Scope Name, bạn nhập vào tên và chú thích, giúp cho việc nhận diện ra scope này. Sau đó nhấn chọn Next.

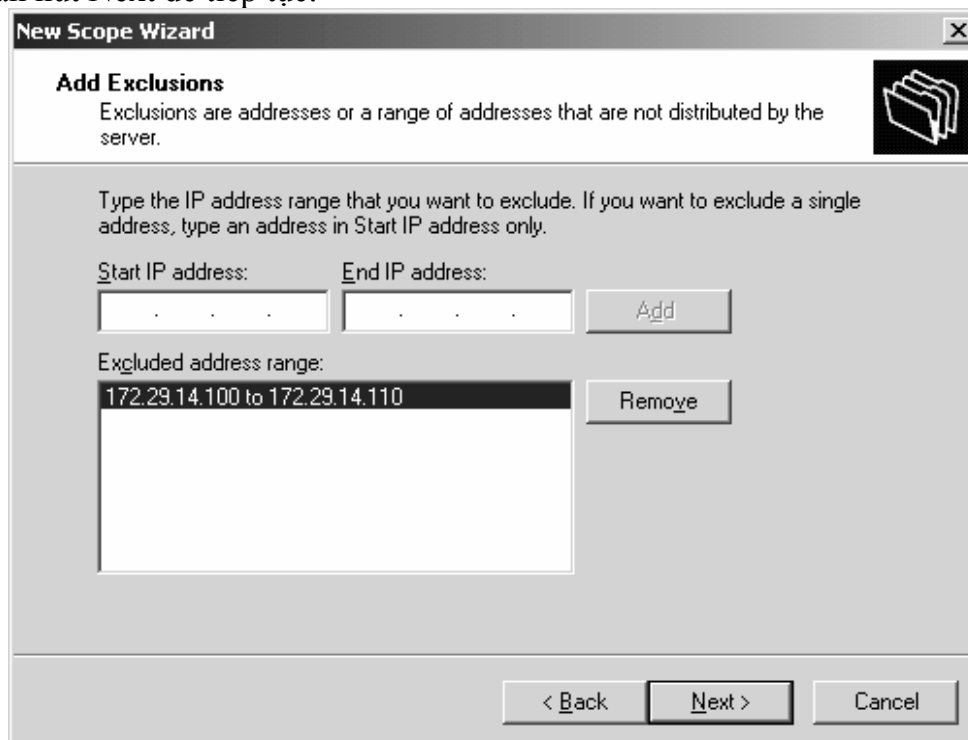


Hộp thoại IP Address Range xuất hiện. Bạn nhập vào địa chỉ bắt đầu và kết thúc của danh sách địa chỉ cấp phát. Sau đó bạn chỉ định subnet mask bằng cách cho biết số bit 1 hoặc nhập vào chuỗi số. Nhấn chọn Next.



The screenshot shows the 'New Scope Wizard' dialog box with the 'IP Address Range' tab selected. The title bar reads 'New Scope Wizard'. Below the title bar, the tab is labeled 'IP Address Range'. A small icon of a folder with a document is on the right. The main text says: 'You define the scope address range by identifying a set of consecutive IP addresses.' Below this, it says: 'Enter the range of addresses that the scope distributes.' There are two input fields: 'Start IP address:' with the value '172 . 29 . 14 . 100' and 'End IP address:' with the value '172 . 29 . 14 . 200'. Below these, it says: '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 two input fields: 'Length:' with the value '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

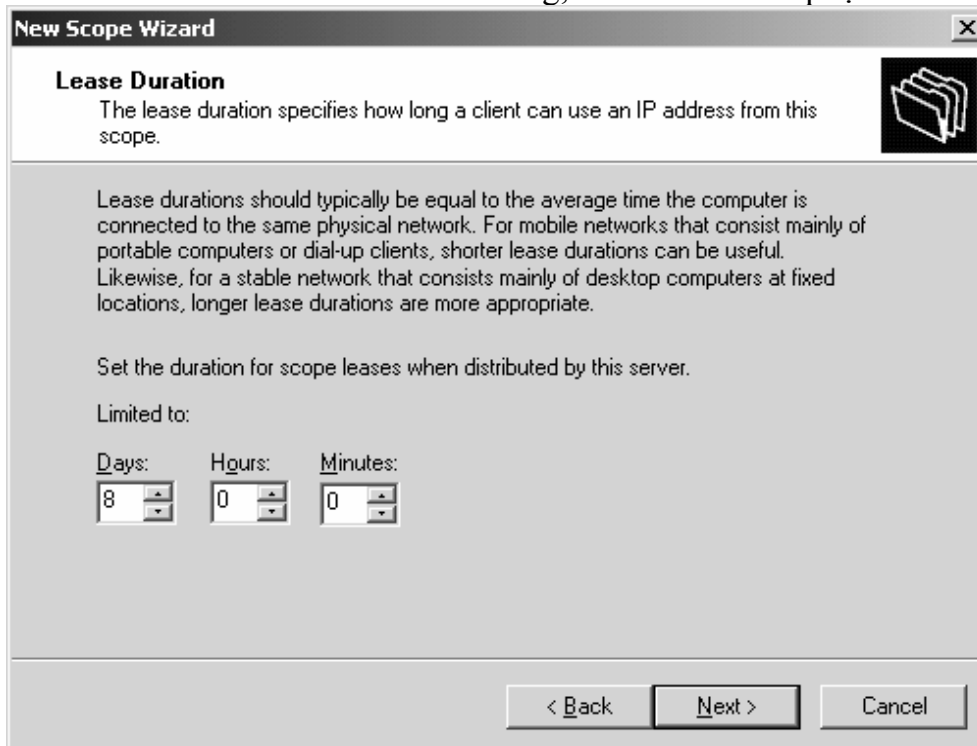
Trong hộp thoại Add Exclusions, bạn cho biết những địa chỉ nào sẽ được loại ra khỏi nhóm địa chỉ đã chỉ định ở trên. Các địa chỉ loại ra này được dùng để đặt cho các máy tính dùng địa chỉ tĩnh hoặc dùng để dành cho mục đích nào đó. Để loại một địa chỉ duy nhất, bạn chỉ cần cho biết địa chỉ trong ô Start IP Address và nhấn Add. Để loại một nhóm các địa chỉ, bạn cho biết địa chỉ bắt đầu và kết thúc của nhóm đó trong Start IP Address và Stop IP Address, sau đó nhấn Add. Nút Remove dùng để huỷ một hoặc một nhóm các địa chỉ ra khỏi danh sách trên. Sau khi đã cấu hình xong, bạn nhấn nút Next để tiếp tục.



The screenshot shows the 'New Scope Wizard' dialog box with the 'Add Exclusions' tab selected. The title bar reads 'New Scope Wizard'. Below the title bar, the tab is labeled 'Add Exclusions'. A small icon of a folder with a document is on the right. The main text says: 'Exclusions are addresses or a range of addresses that are not distributed by the server.' Below this, it says: 'Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.' There are two input fields: 'Start IP address:' and 'End IP address:'. Below these, there is a list of excluded address ranges. The first entry is '172.29.14.100 to 172.29.14.110'. To the right of the list, there are two buttons: 'Add' and 'Remove'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Trong hộp thoại Lease Duration tiếp theo, bạn cho biết thời gian các máy trạm có thể sử dụng địa chỉ này. Theo mặc định, một máy Client sẽ cố làm mới lại địa chỉ khi đã sử dụng được phân nửa

thời gian cho phép. Lượng thời gian cho phép mặc định là 8 ngày. Bạn có thể chỉ định lượng thời gian khác tùy theo nhu cầu. Sau khi đã cấu hình xong, nhấn Next để tiếp tục.



**New Scope Wizard**

**Lease Duration**  
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

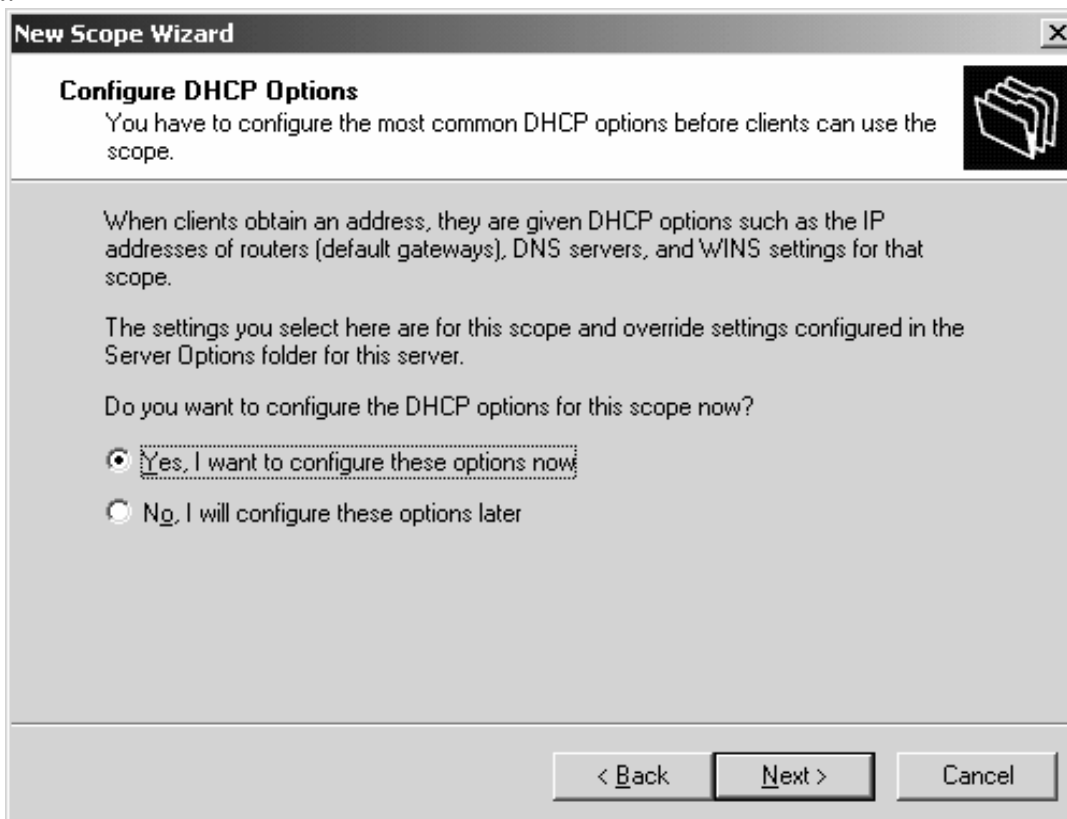
Set the duration for scope leases when distributed by this server.

Limited to:

Days: 8 Hours: 0 Minutes: 0

< Back Next > Cancel

Hộp thoại Configure DHCP Options xuất hiện. Bạn có thể đồng ý để cấu hình các tùy chọn phổ biến (chọn Yes, I want to configure these options now) hoặc không đồng ý, để việc thiết lập này thực hiện sau (chọn No, I will configure these options later). Bạn để mục chọn đồng ý và nhấn chọn Next.



**New Scope Wizard**

**Configure DHCP Options**  
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

< Back Next > Cancel

Trong hộp thoại Router (Default Gateway), bạn cho biết địa chỉ IP của default gateway mà các máy DHCP Client sẽ sử dụng và nhấn Add. Sau đó nhấn Next.



**New Scope Wizard**

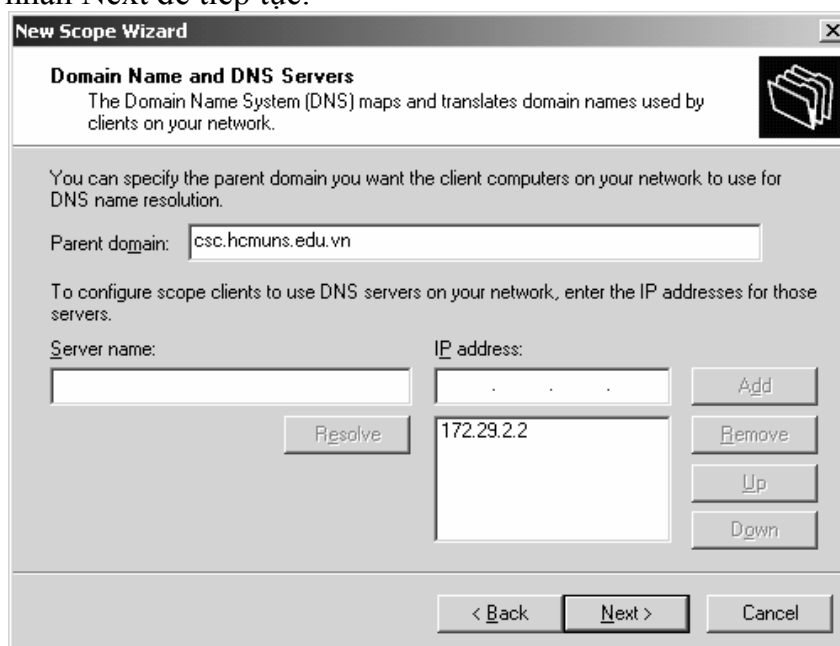
**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

< Back Next > Cancel

Trong hộp thoại Domain Name and DNS Server, bạn sẽ cho biết tên domain mà các máy DHCP client sẽ sử dụng, đồng thời cũng cho biết địa chỉ IP của DNS Server dùng phân giải tên. Sau khi đã cấu hình xong, nhấn Next để tiếp tục.



**New Scope Wizard**

**Domain Name and DNS Servers**  
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

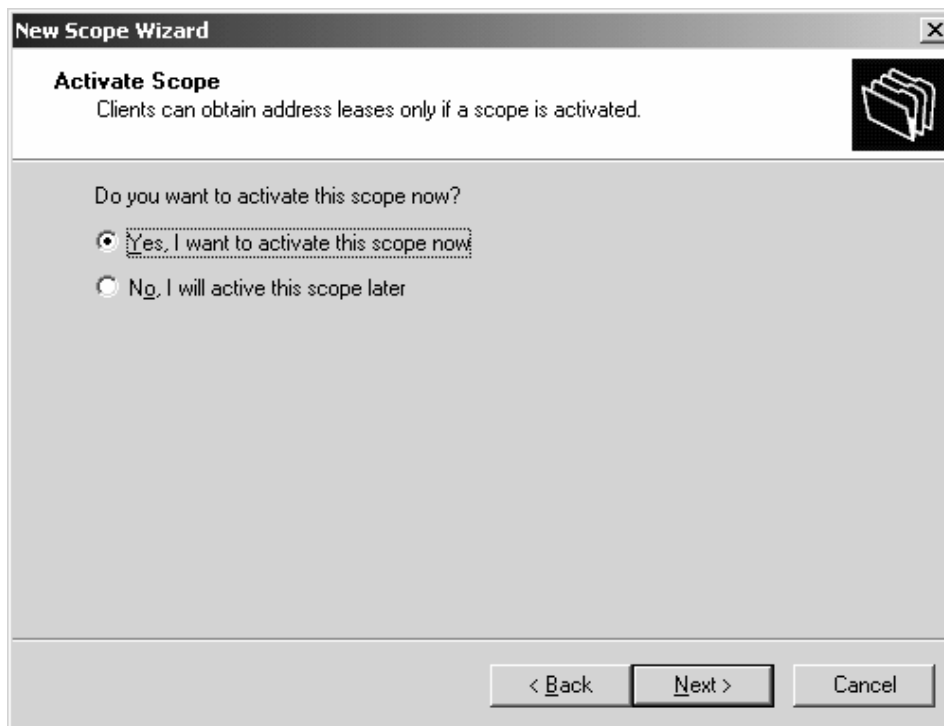
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

< Back Next > Cancel

Trong hộp thoại WINS SERVER tiếp theo, bạn có thể cho biết địa chỉ của WINS Server chính và phụ dùng phân giải các tên NetBIOS thành địa chỉ IP. Sau đó nhấn chọn Next. (Hiện nay dịch vụ WINS ít được sử dụng, do đó bạn có thể bỏ qua bước này, không nhập thông tin gì hết.) Tiếp theo, hộp thoại Activate Scope xuất hiện, hỏi bạn có muốn kích hoạt scope này hay không. Scope chỉ có thể cấp địa chỉ cho các máy Client khi được kích hoạt. Nếu bạn định cấu hình thêm các thông tin tùy chọn cho scope thì chưa nên kích hoạt bây giờ. Sau khi đã lựa chọn xong, nhấn chọn Next.



Trong hộp thoại Complete the New Scope Wizard, nhấn chọn Finish để kết thúc.

## VI. CẤU HÌNH CÁC TÙY CHỌN DHCP

Các tùy chọn DHCP là các thông tin phụ gửi kèm theo địa chỉ IP khi cấp phát cho các máy Client. Bạn có thể chỉ định các tùy chọn ở hai mức độ: scope và Server. Các tùy chọn mức scope chỉ áp dụng cho

riêng scope đó, còn các tùy chọn mức Server sẽ áp đặt cho tất cả các scope trên toàn Server. Tùy chọn mức scope sẽ che phủ tùy chọn mức server cùng loại nếu có.

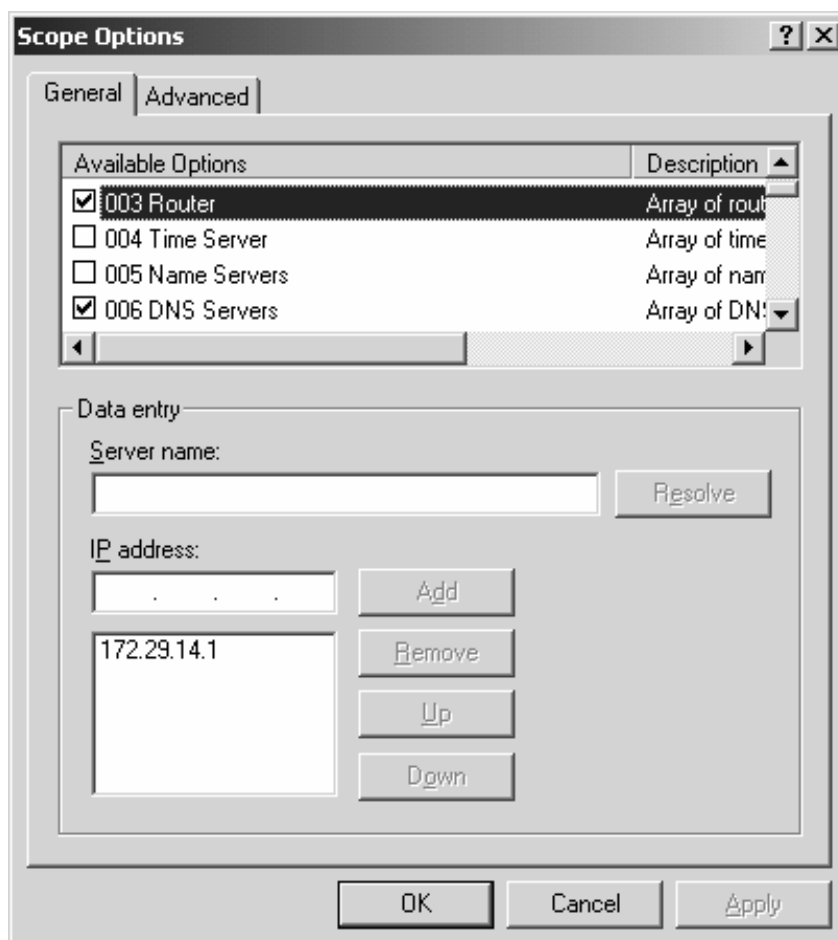
Các bước thực hiện:

Chọn menu Start / Programs / Administrative Tools / DHCP.

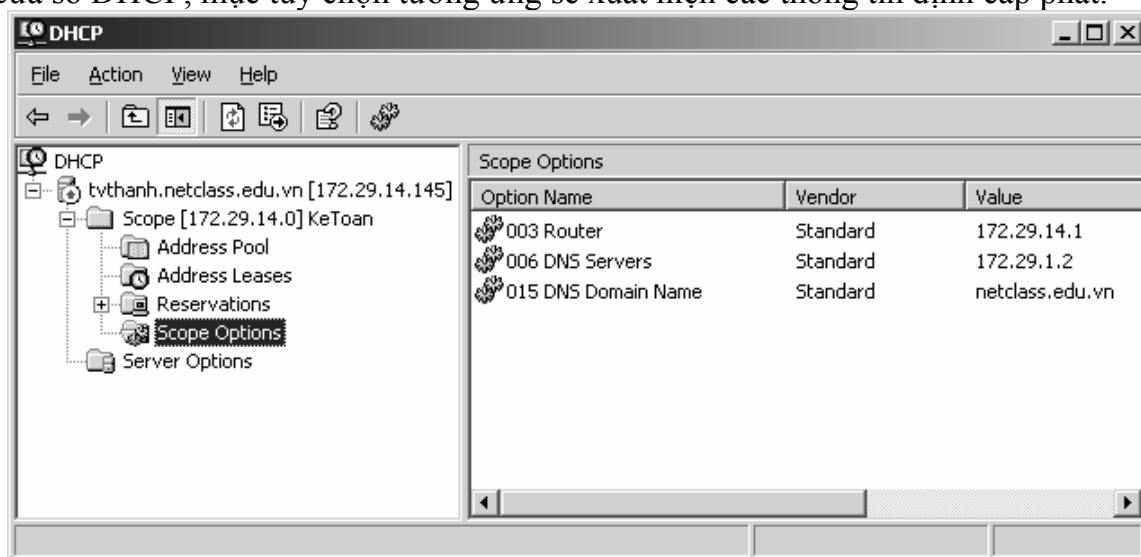
Trong cửa sổ DHCP, ở ô bên trái, mở rộng mục Server để tìm Server Options hoặc mở rộng một scope nào đó để tìm Scope Options.

Nhấn phải chuột lên mục tùy chọn tương ứng và chọn Configure Options.

Hộp thoại cấu hình các tùy chọn xuất hiện (mức Server hoặc scope đều giống nhau). Trong mục Available Options, chọn loại tùy chọn bạn định cấp phát và nhập các thông cấu hình kèm theo. Sau khi đã chọn xong hoặc chỉnh sửa các tùy chọn xong, nhấn OK để kết thúc.



Trong cửa sổ DHCP, mục tùy chọn tương ứng sẽ xuất hiện các thông tin định cấp phát.



## VII. CẤU HÌNH ĐỊA CHỈ DÀNH RIÊNG

Giả sử hệ thống mạng của bạn sử dụng việc cấp phát địa chỉ động, tuy nhiên trong đó có một số máy tính bắt buộc phải sử dụng một địa chỉ IP cố định trong một thời gian dài. Bạn có thể thực hiện được điều này bằng cách dành một địa chỉ IP cho riêng máy đó. Việc cấu hình này được thực hiện trên từng scope riêng biệt.

Các bước thực hiện:

Chọn menu Start / Programs / Administrative Tools / DHCP.

Trong ô bên trái của cửa sổ DHCP, mở rộng đến scope bạn định cấu hình, chọn mục Reservation, chọn menu Action / New Reservation.

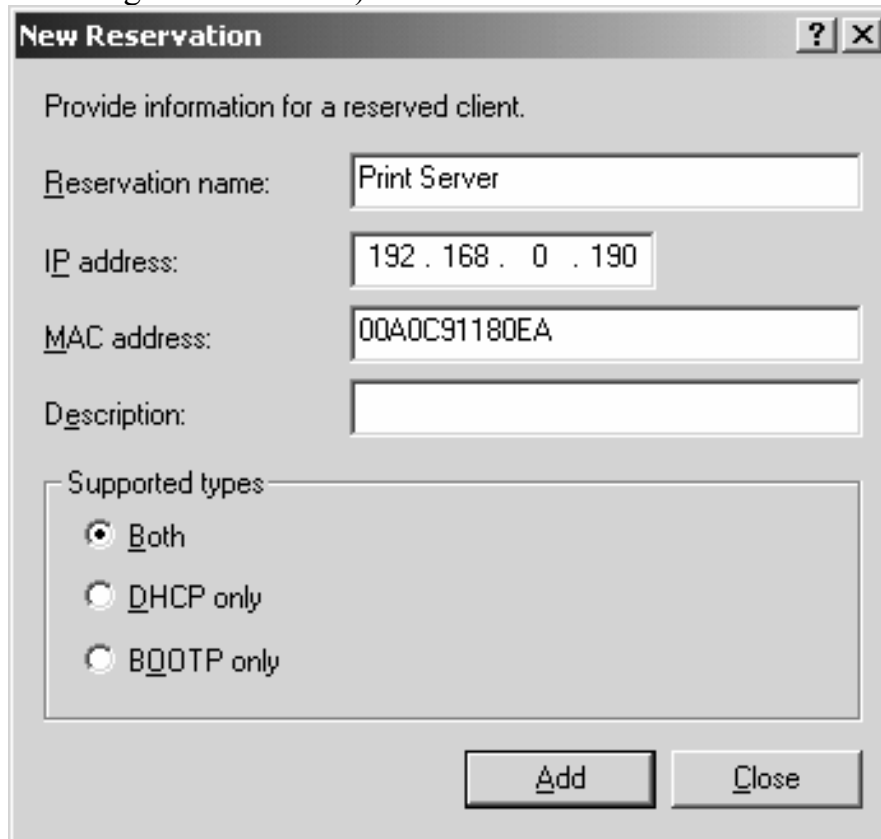
Xuất hiện hộp thoại New Reservation. Đặt tên cho mục dành riêng này trong ô Reservation Name, có thể là tên của máy tính được cấp địa chỉ đó. Trong mục IP Address, nhập vào địa chỉ IP



định cấp cho máy đó. Tiếp theo, trong mục MAC Address, nhập vào địa chỉ MAC của máy tính đó (là một chuỗi liên tục 12 ký số thập lục phân). Bạn có thể ghi một dòng mô tả về địa chỉ vào mục Description. Supported Types có ý nghĩa:

DHCP only: chỉ cho phép máy client DHCP yêu cầu địa chỉ này bằng cách sử dụng giao thức DHCP.

BOOTP only: chỉ cho phép máy client DHCP yêu cầu địa chỉ này bằng cách sử dụng giao thức BOOTP (là tiền thân của giao thức DHCP).



**New Reservation** [?] [X]

Provide information for a reserved client.

Reservation name: Print Server

IP address: 192 . 168 . 0 . 190

MAC address: 00A0C91180EA

Description:

Supported types

☒ Both

☐ DHCP only

☐ BOOTP only

[Add] [Close]

Both: máy client DHCP có thể dùng giao thức DHCP hoặc BOOTP để yêu cầu địa chỉ này. Lặp lại thao tác trên cho các địa chỉ dành riêng khác. Cuối cùng nhấn chọn Close.

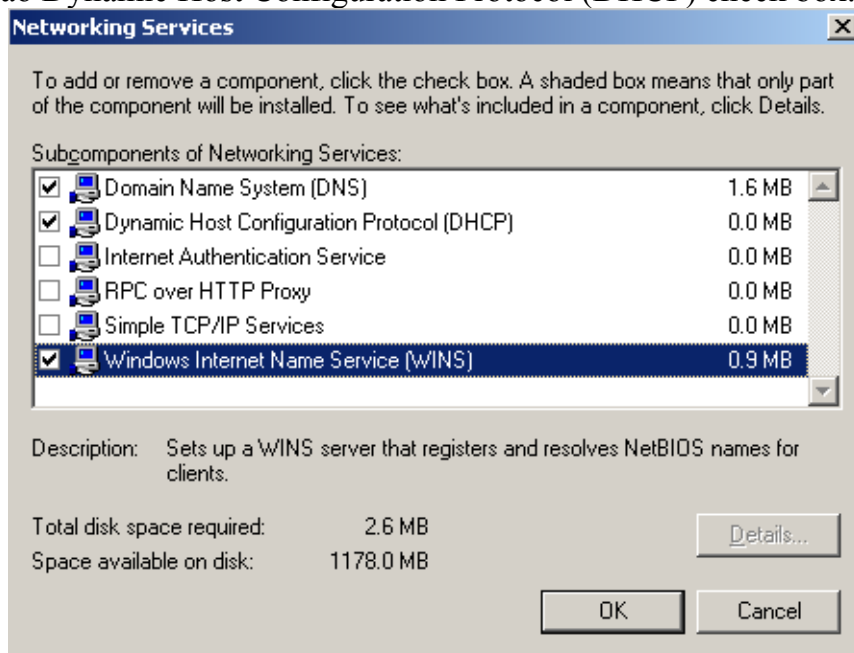
## BÀI 6: DỊCH VỤ WINS

### I. GIỚI THIỆU DỊCH VỤ WINS

Windows Internet Name Service (WINS) được sử dụng để giải quyết NetBIOS names ra IP Addresses (đơn giản vì chúng ta đang dùng Network TCP/IP, Network giao tiếp theo số- IP address, Computer name chỉ là yếu tố phụ, và là thói quen xác lập giao tiếp, vì tên dễ nhớ hơn số) My Network Places hoạt động tìm kiếm các Network Computer dựa trên Service Windows Browser. Và dịch vụ Windows Browser giải quyết tên dựa trên nền tảng Broadcast (broadcast-based service), nếu mạng triển khai WINS server thì Windows Browser trên các máy tính sẽ phụ thuộc vào WINS server để thu thập thông tin về các máy tính phân tán khắp các phân đoạn của mạng. Ngoài ra, dịch vụ WINS cũng được yêu cầu triển khai khi các VPN clients muốn có được danh sách các máy tính trong nội bộ mạng. Mục đích cài WINS server trong là để hỗ trợ giải quyết NetBIOS name và dịch vụ Windows Browser cho các VPN clients.

### II. CÀI ĐẶT DỊCH VỤ WINS

1. Click Start, Control Panel. Click Add or Remove Programs.
2. Trong Add or Remove Programs, click Add/Remove Windows Components
3. Trên Windows Components page, kéo xuống danh sách Components và chọn Networking Services entry. Click Details.
4. Trong Network Services dialog box, check vào Windows Internet Name Service (WINS) check box. Check tiếp vào Dynamic Host Configuration Protocol (DHCP) check box. Click OK.



5. Click Next trên Windows Components page.
  6. Click OK trên Insert Disk dialog box. Trong Files Needed dialog box, đưa đường dẫn đến I386 folder trong mục Copy files from text box và click OK.
  7. Click Finish trên Completing the Windows Components Wizard page.
  8. Đóng Add or Remove Programs.
- WINS server đã sẵn sàng phục vụ nhu cầu đăng kí NetBIOS name ngay lập tức mà không cần bất cứ cấu hình thêm nào.

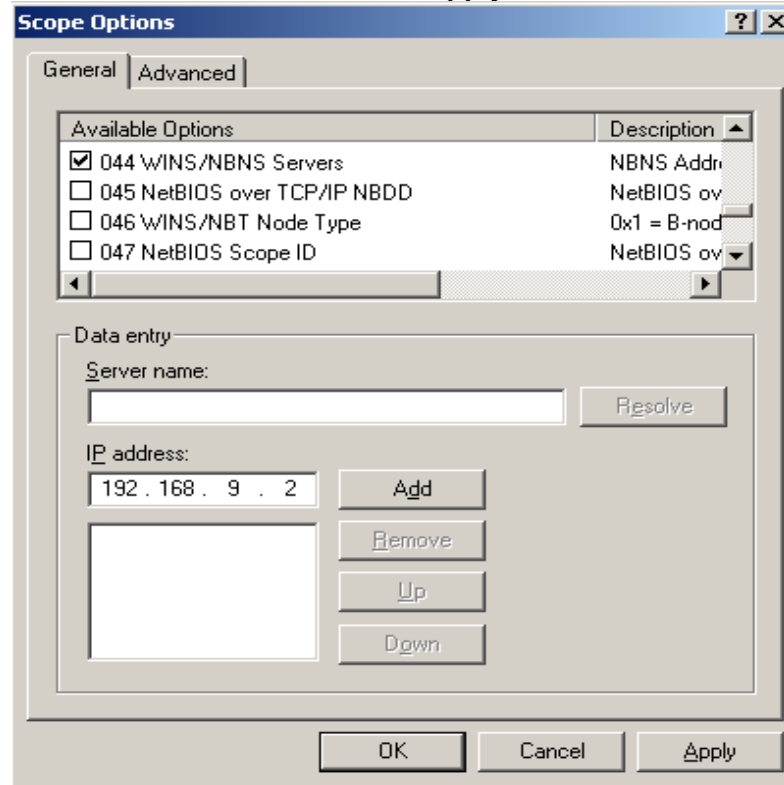
### III. CẤU HÌNH TÙY CHỌN WINS SERVER CHO DHCP

B1: Mở DHCP

B2: Click chuột phải lên Scope Option của Scope cần cấu hình, chọn Configure Options

B3: Đánh dấu chọn WINS/NBNS Server

B4: Nhập địa chỉ IP của WINS Server, chọn Add, Apply và OK



#### IV. CẤU HÌNH MÁY KHÁCH SỬ DỤNG DỊCH VỤ WINS

B1: Click chuột phải lên My Network Places trên Desktop, chọn Properties

B2: Click chuột phải vào biểu tượng kết nối cần cấu hình, chọn Properties

B3: Chọn TCP/IP, chọn Properties

B4: Chọn Advance, chọn WINS

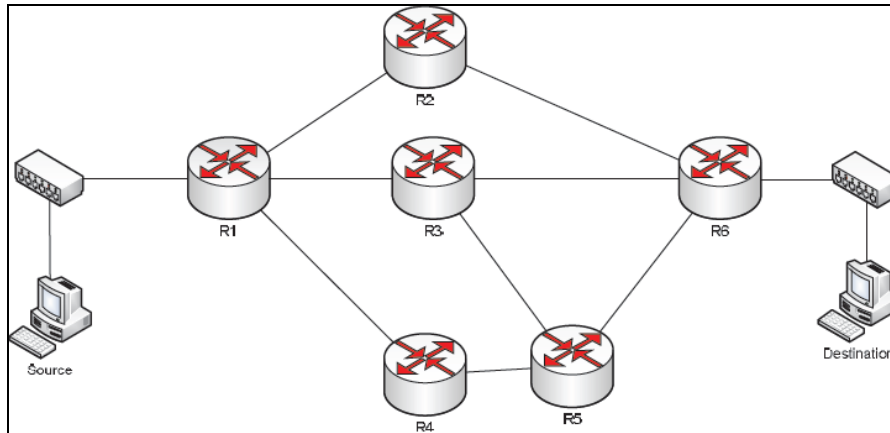
B5: Chọn Add, nhập địa chỉ IP của WINS Server rồi chọn Add

# BÀI 7: DỊCH VỤ ROUTING VÀ NAT

## I. ROUTING

### I.1. Khái niệm

Routing: việc lựa chọn “đường đi” để chuyển gói tin từ một máy tính/thiết bị nguồn đến máy tính/thiết bị đích.



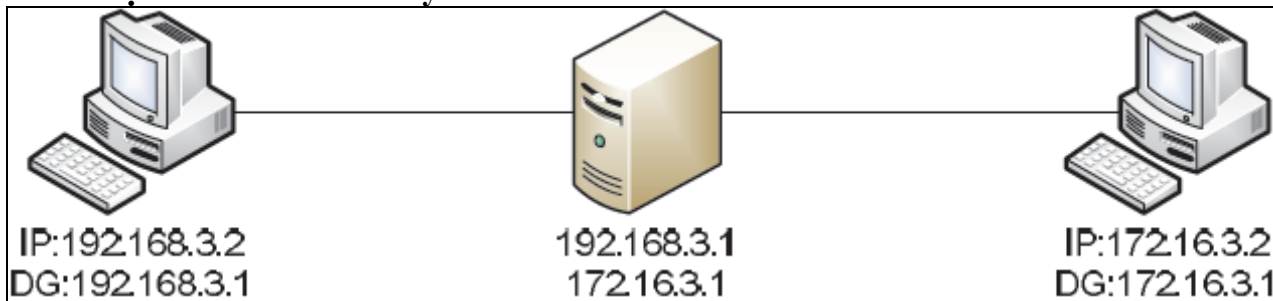
Quá trình lựa chọn đường đi để một gói tin từ máy Source đến máy Destination và chuyển gói tin đi theo con đường đó được gọi là quá trình routing. Việc lựa chọn đường đi và chuyển gói tin đi được thực hiện ở: máy tính Source, các thiết bị Router (Ri) nằm trên đường đi được lựa chọn.

### Dịch vụ Routing And Remote Access (RRAS)

Hệ điều hành Microsoft Windows 2003 Server cung cấp sẵn dịch vụ RRAS. RRAS có nhiều chức năng trong đó có chức năng cho phép một máy tính hoạt động như một router (gọi là Router mềm).

### I.2. Cấu hình dịch vụ Routing And Remote Access

Cấu hình địa chỉ IP cho các máy tính theo sơ đồ sau:



#### Kiểm tra:

Từ máy tính có địa chỉ IP 192.168.3.2, ping địa chỉ IP 17.16.3.2

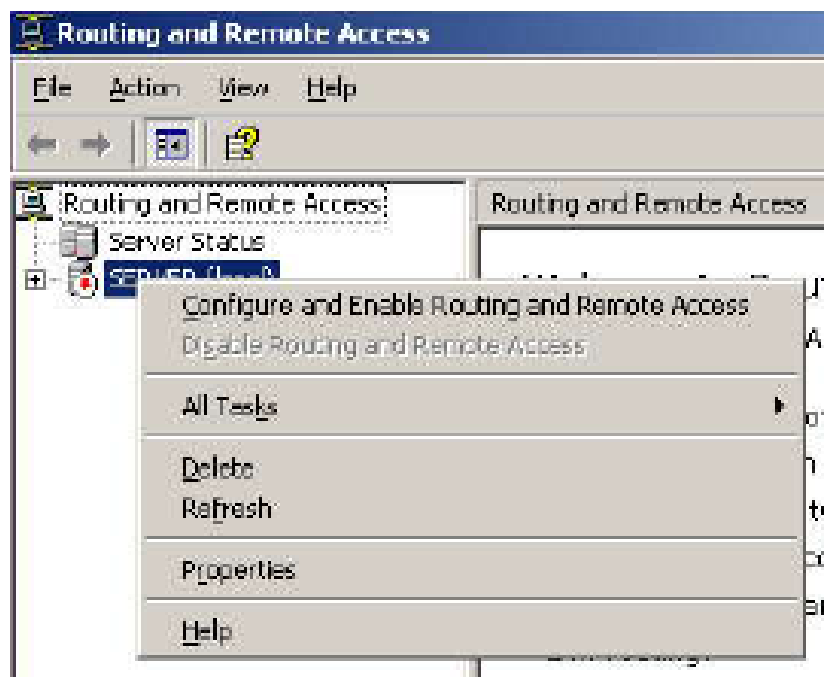
#### Kết quả:

không tìm thấy địa chỉ IP 172.16.3.2

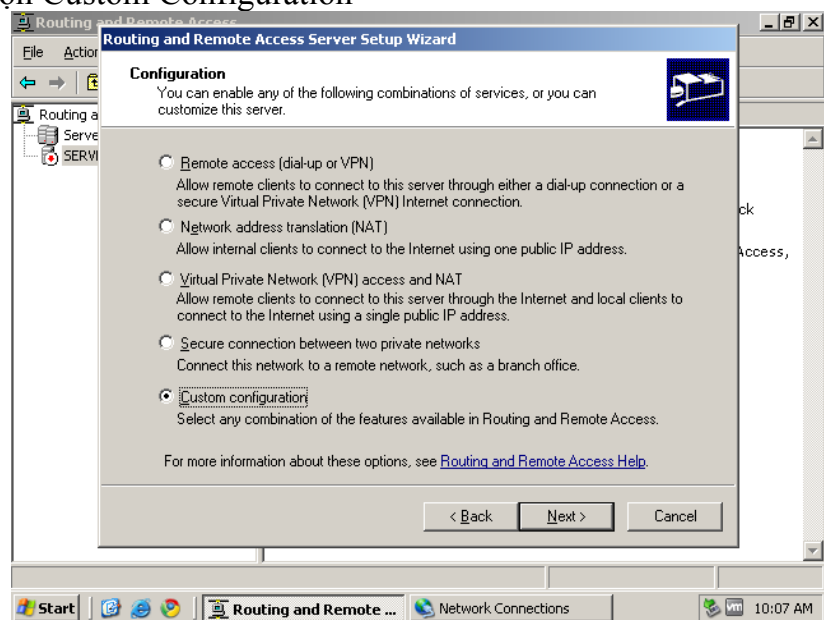
#### Cấu hình cho Server:

B1: Vào Start -> Administrative Tools -> Routing And Remote Access

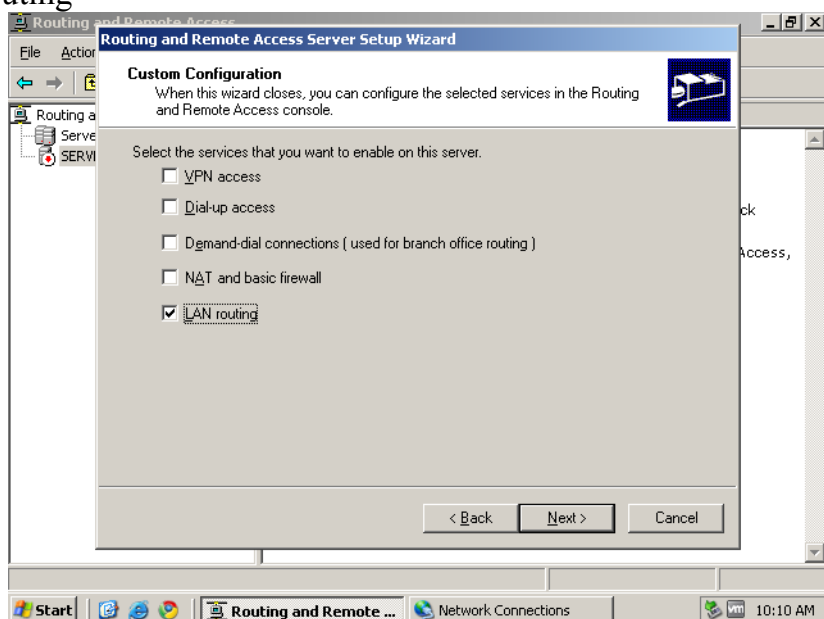
B2: Click chuột phải lên biểu tượng Server, chọn Configure And Enable Routing And Remote Access từ menu ngữ cảnh



B3: Chọn Next, chọn Custom Configuration



B4: Chọn LAN Routing



B5: Chọn Finish hoàn tất

**Kiểm tra lại:**

Từ máy tính có địa chỉ IP 192.168.3.2, ping địa chỉ 172.16.3.2.

**Kết quả:**

Tìm thấy địa chỉ 172.16.3.2

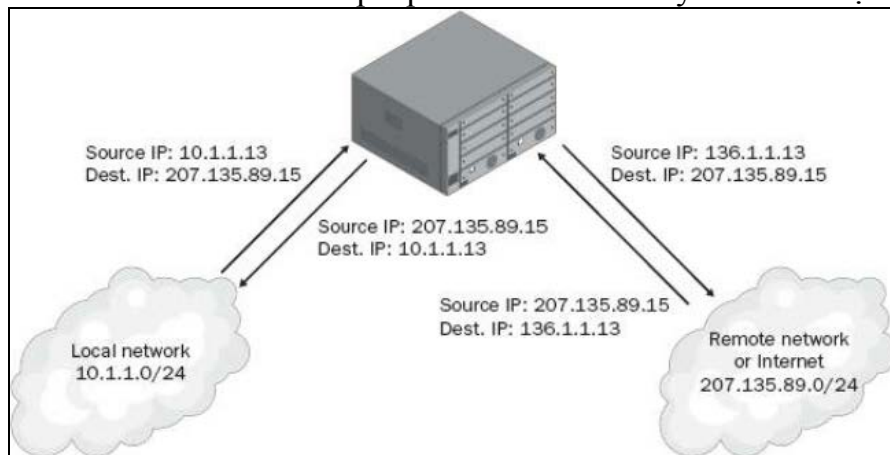
## II. NAT

### II.1. Giới thiệu

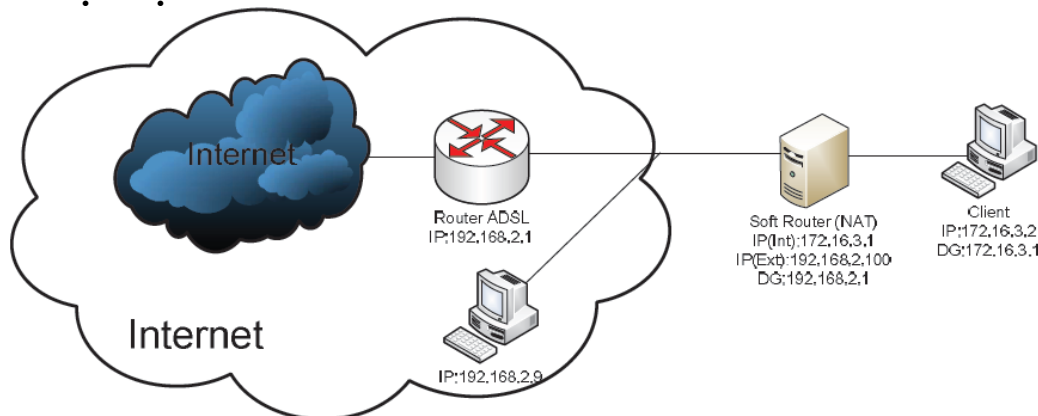
NAT là dịch vụ được tích hợp trên router với mục đích thay đổi thông tin trong gói tin IP trước khi chuyển gói tin đến máy tính/thiết bị đích.

NAT cho phép nhiều máy tính/thiết bị có private IP chia cùng chia sẻ một public IP.

Một ưu điểm khác của NAT là: NAT cho phép “che dấu” các máy tính/thiết bị bên trong.



### II.2. Cấu hình dịch vụ NAT



**Kiểm tra:**

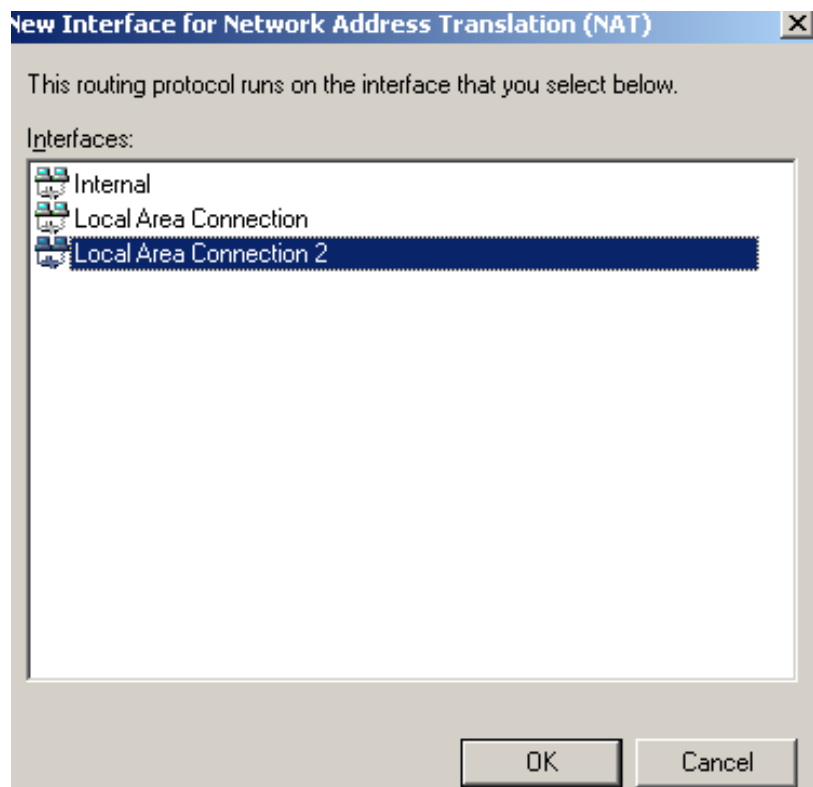
Cấu hình địa chỉ IP của các máy tính theo mô hình trên

Kiểm tra máy tính Client không thể ping được Router ADSL 192.168.2.1

**Cấu hình NAT:**

B1: Trong Routing And Remote Access, click chuột phải lên NAT/Basic Firewall, chọn New Interface từ menu ngữ cảnh

B2: Chọn card mạng mà NAT sử dụng. Tại đây, chọn card mạng nối vào mạng nội bộ



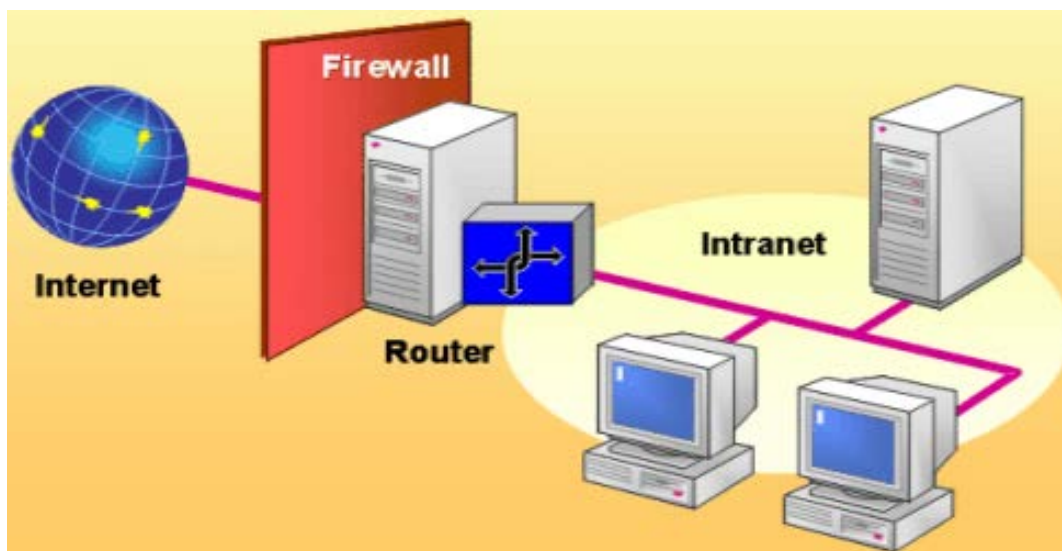
- B3. Chỉ rõ card mạng vừa chọn được nối vào mạng nội bộ.
- B4. Chọn card mạng nối ra mạng ngoài.
- B5. Xác nhận card mạng nối ra mạng ngoài.
- B6. Kiểm tra máy client đã ping được router ADSL 192.168.2.1

# BÀI 8: DỊCH VỤ PROXY

## I. GIỚI THIỆU VỀ FIREWALL

Trong công nghệ thông tin, firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại việc truy cập trái phép, bảo vệ các nguồn tài nguyên cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn. Cụ thể hơn, có thể hiểu firewall là một cơ chế bảo vệ giữa mạng tin tưởng (trusted network), ví dụ mạng intranet nội bộ, với các mạng không tin tưởng mà thông thường là Internet.

Về mặt vật lý, firewall bao gồm một hoặc nhiều hệ thống máy chủ kết nối với bộ định tuyến (Router) hoặc có chức năng Router.



Về mặt chức năng, firewall có nhiệm vụ:

- Tất cả các trao đổi dữ liệu từ trong ra ngoài và ngược lại đều phải thực hiện thông qua firewall.
- Chỉ có những trao đổi được cho phép bởi hệ thống mạng nội bộ (trusted network) mới được quyền lưu thông qua firewall.
- Các phần mềm quản lý an ninh chạy trên hệ thống máy chủ bao gồm :

Quản lý xác thực (Authentication): ngăn cản truy cập trái phép vào hệ thống mạng nội bộ

Quản lý cấp quyền (Authorization): xác định quyền sử dụng tài nguyên cũng như các nguồn thông tin trên mạng theo từng người, từng nhóm người sử dụng.

Quản lý kiểm toán (Accounting Management): Ghi nhận tất cả các sự kiện xảy ra liên quan đến việc truy cập và sử dụng nguồn tài nguyên trên mạng theo từng thời điểm (ngày/giờ) và thời gian truy cập đối với vùng tài nguyên nào đã được sử dụng hoặc thay đổi bổ sung ...

## II. GIỚI THIỆU DỊCH VỤ WEB PROXY

Dịch vụ Proxy thường được áp dụng trong hệ thống mạng vì các lý do sau:

- An toàn mạng: Thông thường các máy tính trong mạng LAN sẽ không được phép kết nối trực tiếp với mạng Internet mà phải thông qua các máy trung gian, gọi là máy proxy. Khi có nhu cầu ra mạng bên ngoài (ví dụ như duyệt web), các máy workstation trong mạng LAN sẽ gửi yêu cầu cho proxy. Proxy sẽ thay mặt cho các máy tính này liên lạc với web server, sau đó gửi lại kết quả cho máy trạm đã yêu cầu thông tin
- Tiết kiệm băng thông: Khi có nhiều máy trong mạng LAN cần lấy cùng nội dung 1 trang web, nếu không sử dụng proxy thì mỗi máy trạm đều tự liên hệ web server và lấy dữ liệu khiến hao tốn băng thông cho cùng 1 nội dung giống nhau. Nếu thông qua proxy, khi lấy thông tin từ mạng

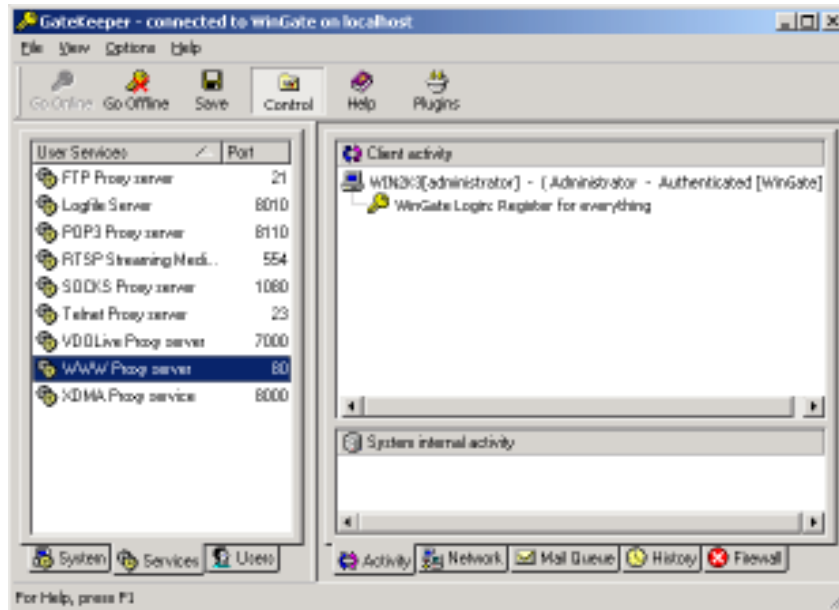


internet, proxy sẽ lưu caching nội dung đó vào vùng nhớ tạm. Nếu có máy tính khác yêu cầu nội dung tương tự, dữ liệu sẽ lấy trực tiếp từ bộ nhớ caching đã lưu mà không cần phải liên hệ với web server nhằm tiết kiệm băng thông.

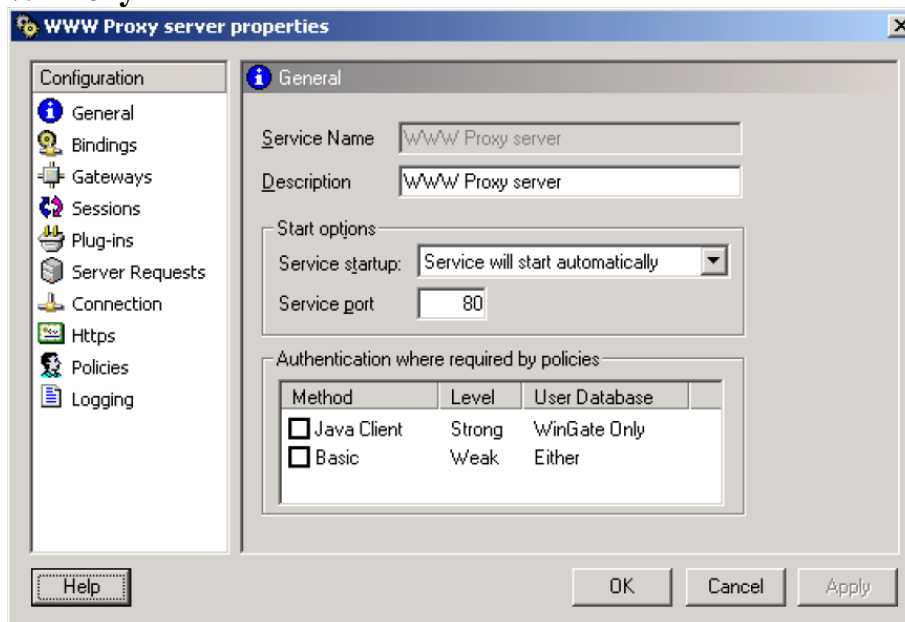
- Ngăn chặn các truy cập web “xấu”: dùng proxy ta có thể cấm các máy trạm truy cập một số trang web nào đó tùy theo chính sách tổ chức.

### III. CẤU HÌNH WEB PROXY SỬ DỤNG WINGATE

#### Giao diện chính



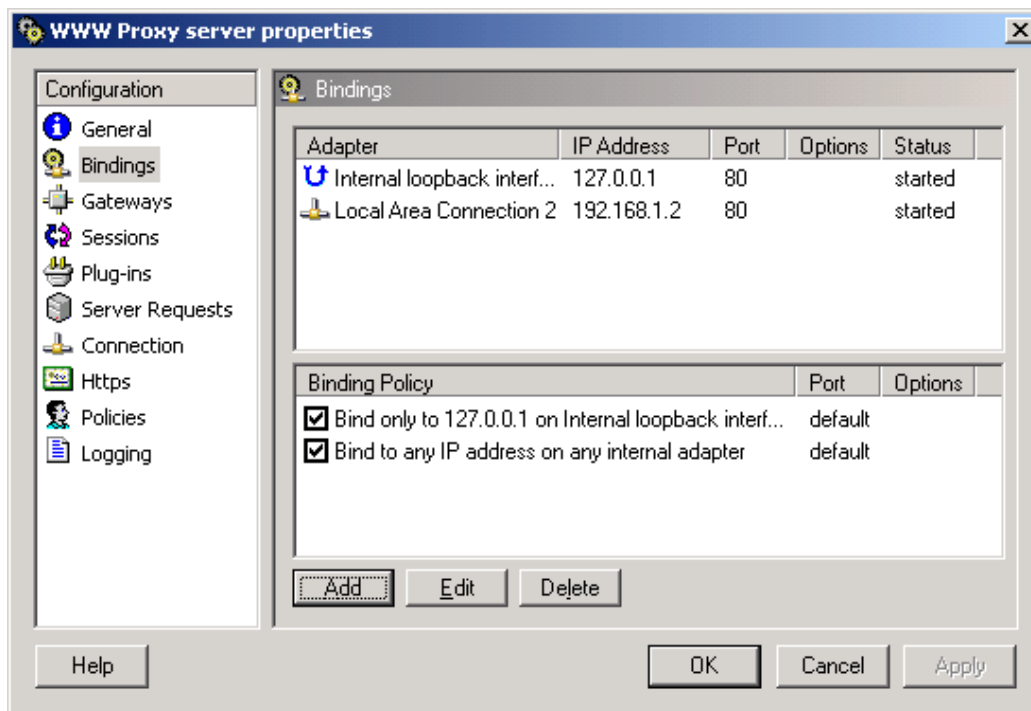
#### Giao diện WWW Proxy



Service port qui định cổng mà proxy server sẽ lắng nghe.

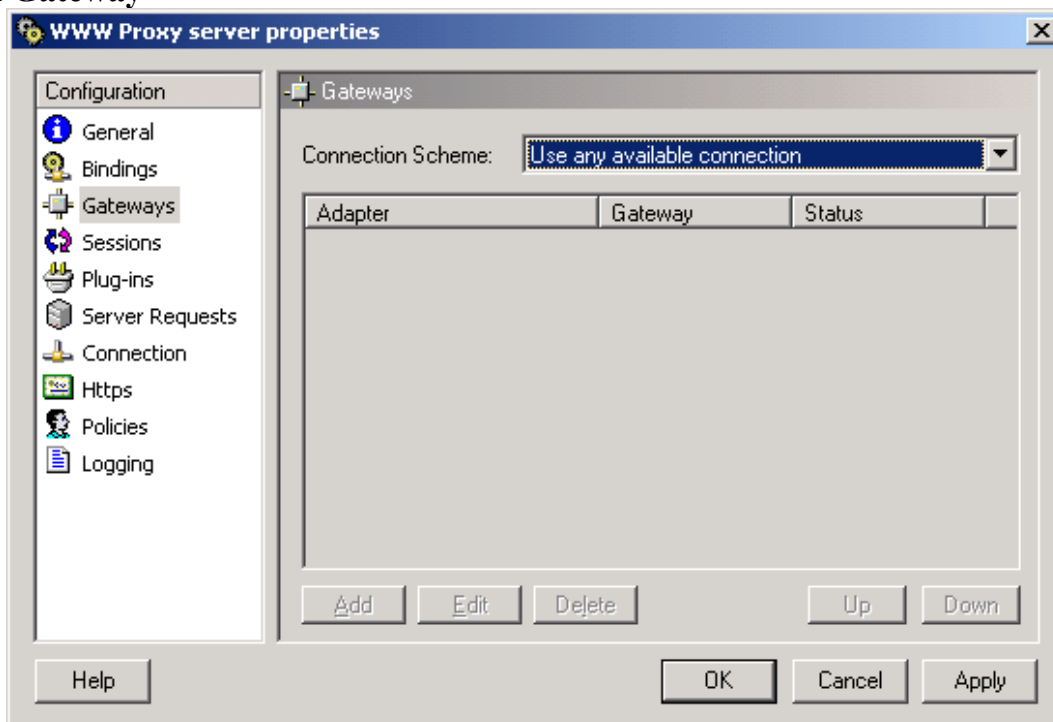
Authentication: cấu hình phương thức chứng thực trước khi user muốn sử dụng proxy server.

#### Giao diện Bindings:



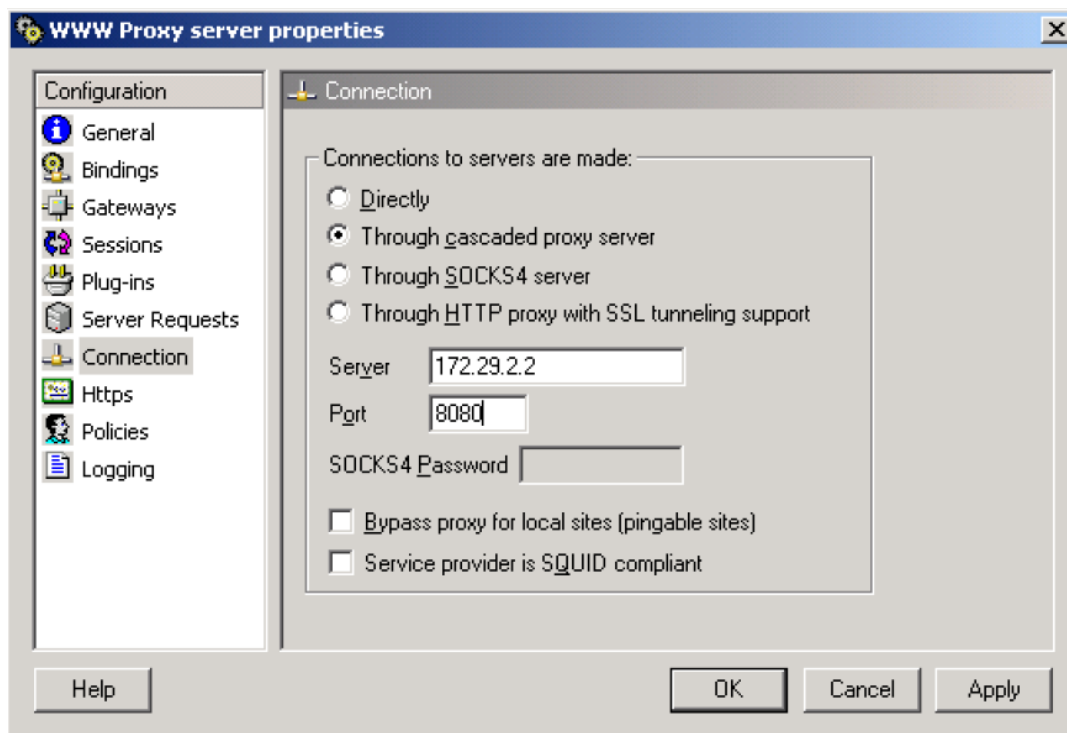
Qui định WWW Proxy sẽ lắng nghe trên các địa chỉ nào. Mặc định proxy server sẽ lắng nghe trên mọi địa chỉ của các card mạng.

### Giao diện Gateway



Qui định Proxy server sẽ sử dụng các gateway nào để truy cập internet. Mặc định proxy server sẽ sử dụng Default Gateway được cấu hình sẵn trong máy.

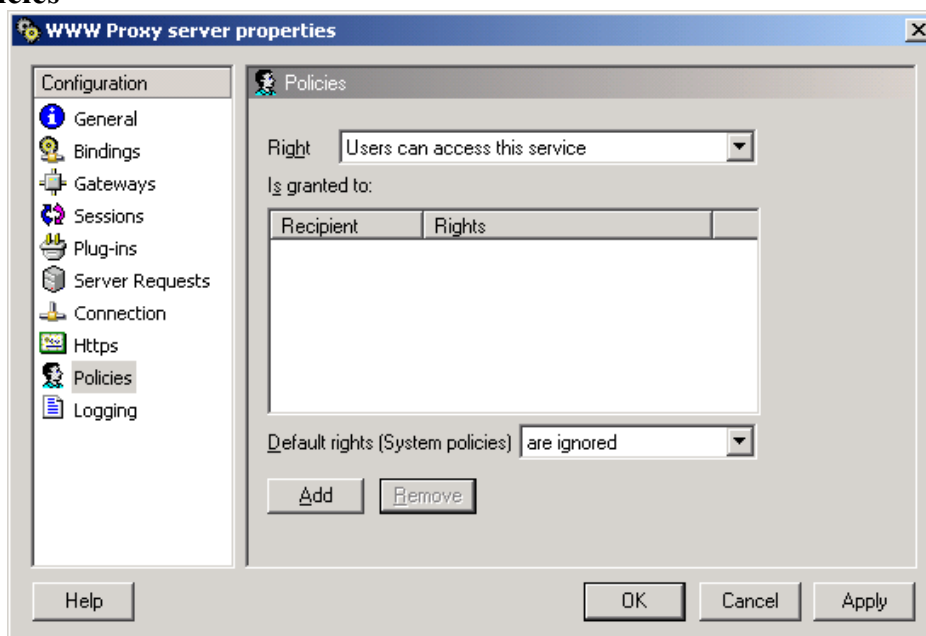
### Giao diện Connection



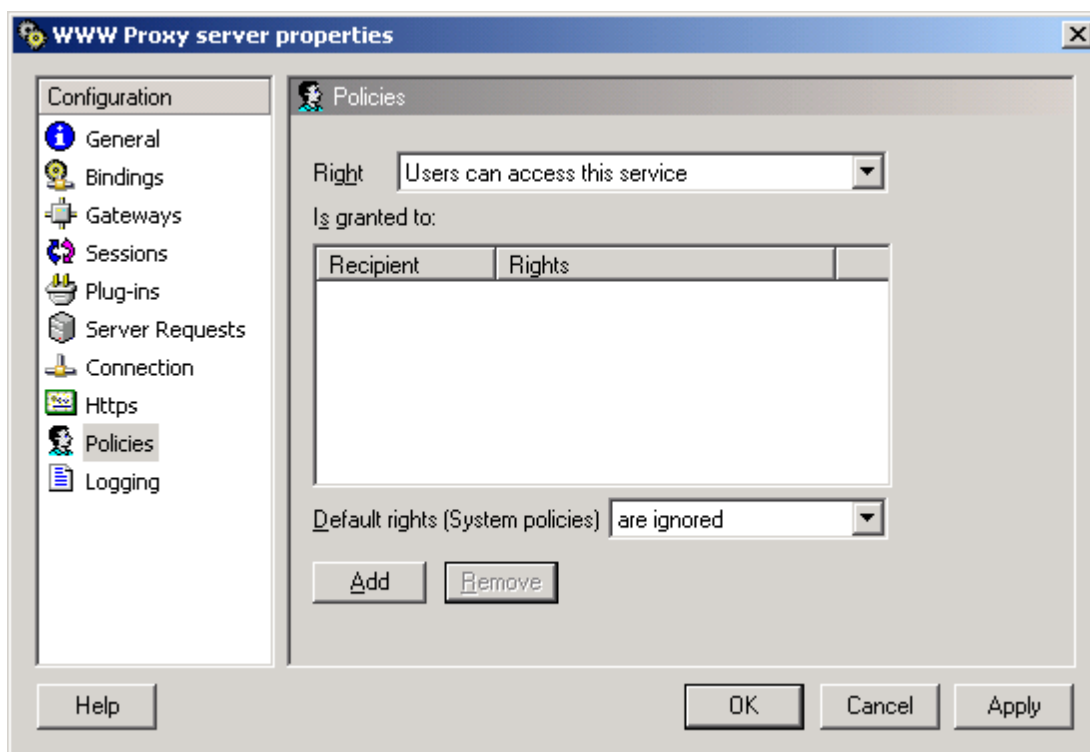
Qui định cách thức proxy server sẽ liên hệ đến các web server bên ngoài:

- Direct: liên hệ trực tiếp (Với điều kiện proxy server được các firewall cho phép ra internet trực tiếp).
- Through cascaded proxy server: Thông qua một proxy server khác để hình thành 1 chuỗi các proxy server.
- Through SOCKS 4 Server: Sử dụng thông qua một proxy khác, sử dụng giao thức SOCKS
- Through HTTP proxy with SSL: Thông qua một proxy khác, hỗ trợ giao thức bảo mật SSL.

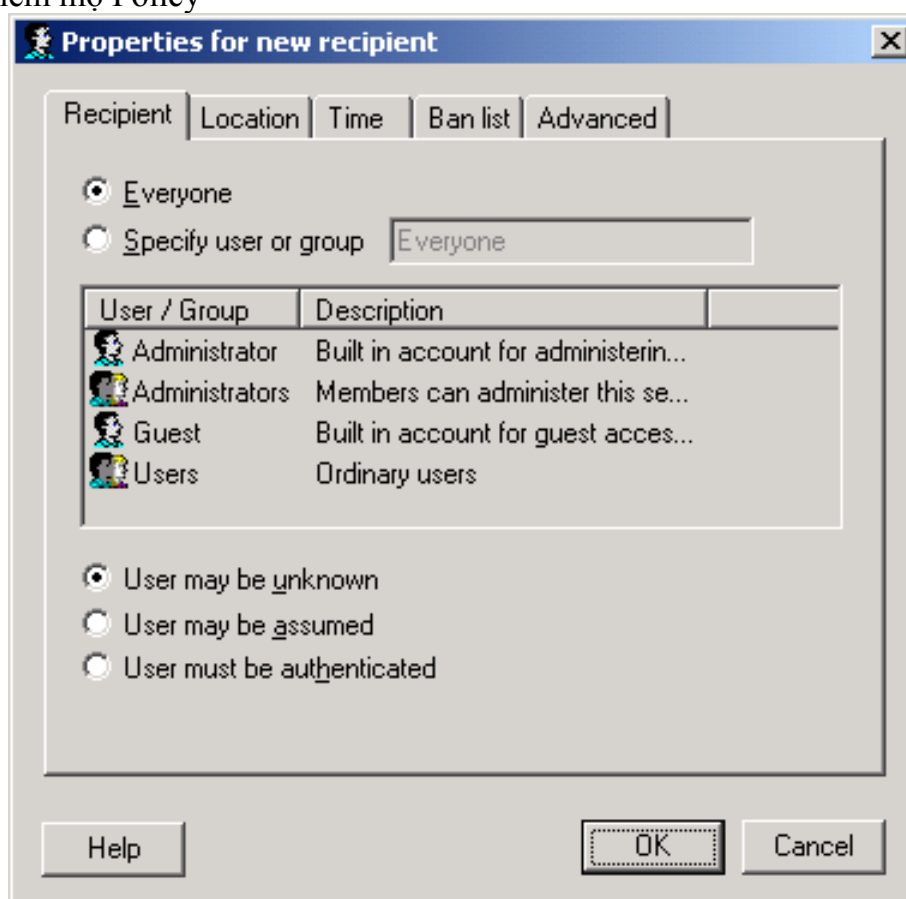
### Giao diện Policies



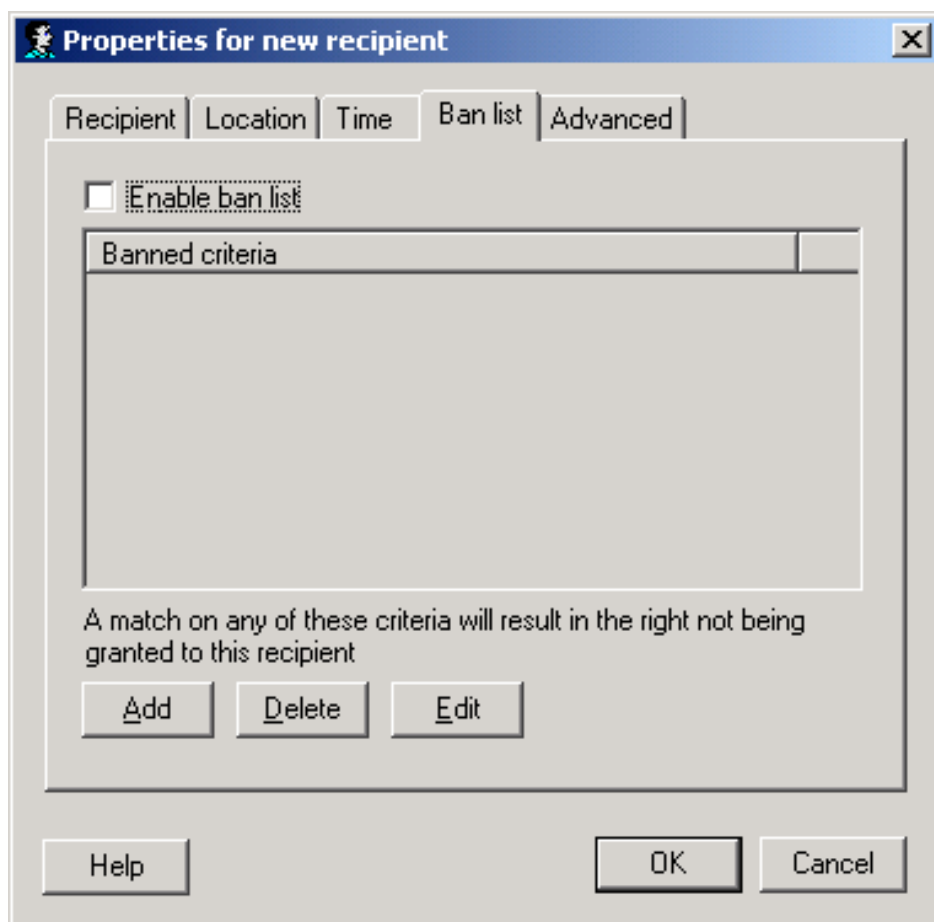
Qui định chính sách đối với người dùng. Ta sẽ cấu hình một chính sách mang tính ví dụ: Cấm người dùng truy cập trang [www.vnexpress.net](http://www.vnexpress.net)



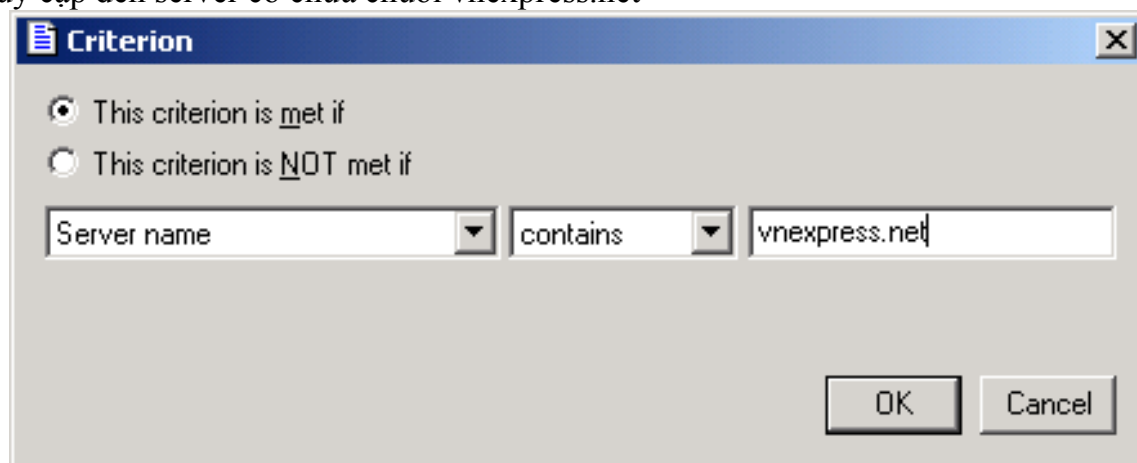
Chọn Add để thêm một Policy



Chọn Tab Ban list để cập nhật danh sách các địa chỉ cấm

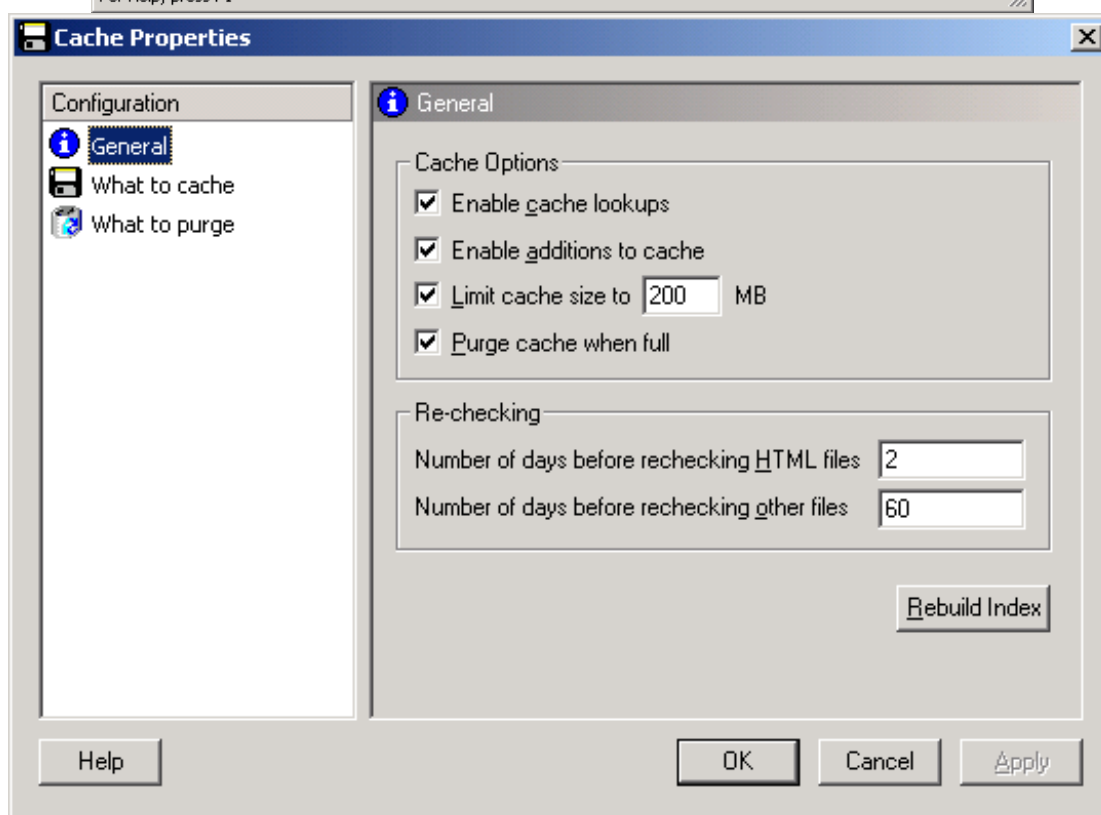
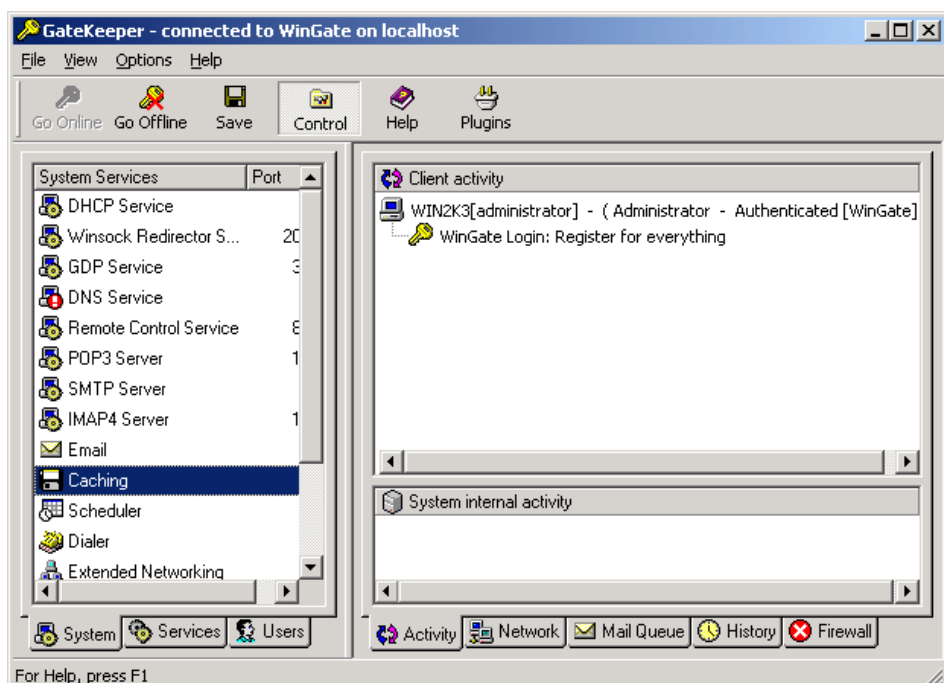


Cấm truy cập đến server có chứa chuỗi vnexpress.net



### Các thông số về Caching trên WinGate

Tính năng caching giúp WinGate lưu tạm các thông tin tại proxy server, khi có yêu cầu thông tin sẽ cung cấp ngay cho client mà không cần kết nối đến web server thật sự trên hệ thống internet. Chức năng này giúp tiết kiệm băng thông cho hệ thống mạng.

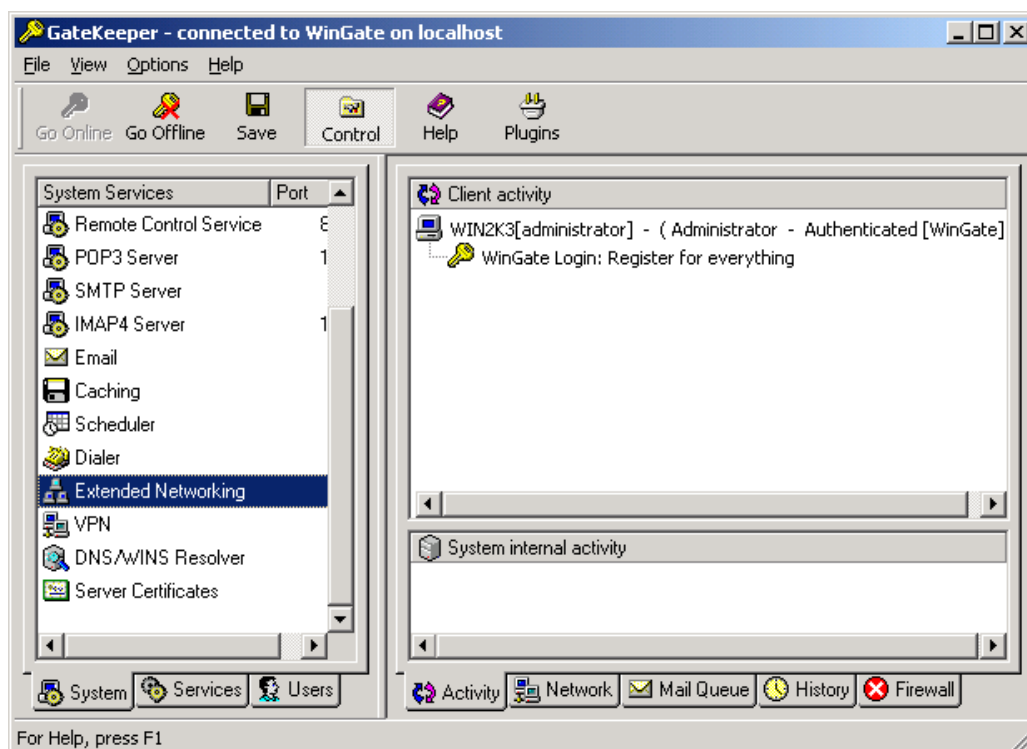


Tại cửa sổ này, chúng ta có thể quy định WinGate sẽ dùng bao nhiêu dung lượng để lưu trữ cache, thời gian caching và nội dung được lưu trữ trong cache...

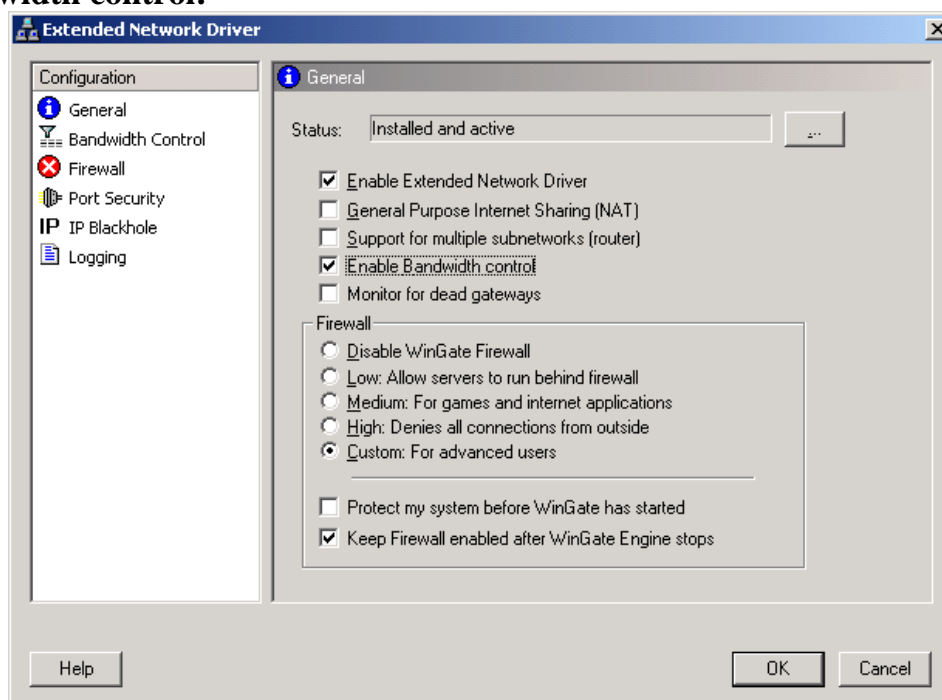
### **Tính năng phân phối Bandwidth (băng thông)**

Đây là tính năng nâng cao, dùng để phân phối băng thông cho những luồng dữ liệu trên đường truyền chung

Chức năng Bandwidth nằm trong phần Extended networking



## Enable Bandwidth control:



# BÀI 9: QUẢN TRỊ MÁY IN

## I. CÀI ĐẶT MÁY IN

Nếu máy in 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 từng bước để cài đặt máy in.
- Nếu hệ điều hành nhận diện không chính xác thì dùng đĩa CD được hãng sản xuất cung cấp kèm theo máy để cài đặt.

Có thể tự cài đặt máy in bằng cách sử dụng tiện ích Add Printer Wizard.

\*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) mới có thể cài đặt máy in (tạo ra một máy in logic) trong Windows Server 2003.

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).

Các bước thực hiện để cài đặt một máy in cục bộ hay một máy in mạng:

Chọn Start -> Printers And Faxes.

Chọn Add Printer, tiện ích Add Printer Wizard sẽ được khởi động.

Chọn Next để tiếp tục.

Hộp thoại Local Or Network Printer xuất hiện.

- Chọn 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, có thể chọn thêm tính năng Automatically Detect And Install My Plug And Play Printer.
- Chọn A Printer Attached To Another Computer nếu đang tạo ra một máy in logic ứng với một máy in mạng.

Khi đã hoàn tất việc chọn lựa, chọn Next để tiếp tục.

Nếu máy in vật lý đã được tự động nhận diện bằng tiện ích Found New Hardware Wizard. Tiện ích này sẽ hướng dẫn từng bước cài đặt driver máy in.

Hộp thoại Print Test Page xuất hiện. Nếu thiết bị máy in được gắn trực tiếp vào máy tính thì nên in thử một trang kiểm tra để xác nhận rằng mọi thứ đều được cấu hình chính xác. Ngược lại, thì bỏ qua bước này. Chọn Next để tiếp tục.

Hộp thoại Completing The Add Printer Wizard hiện ra. Hộp thoại này xác nhận rằng tất cả các thuộc tính máy in đã được xác lập chính xác. Chọn Finish hoàn tất.

Một biểu tượng máy in mới sẽ hiện ra trong cửa sổ Printer And Faxes. Theo mặc định, máy in sẽ được chia sẻ.

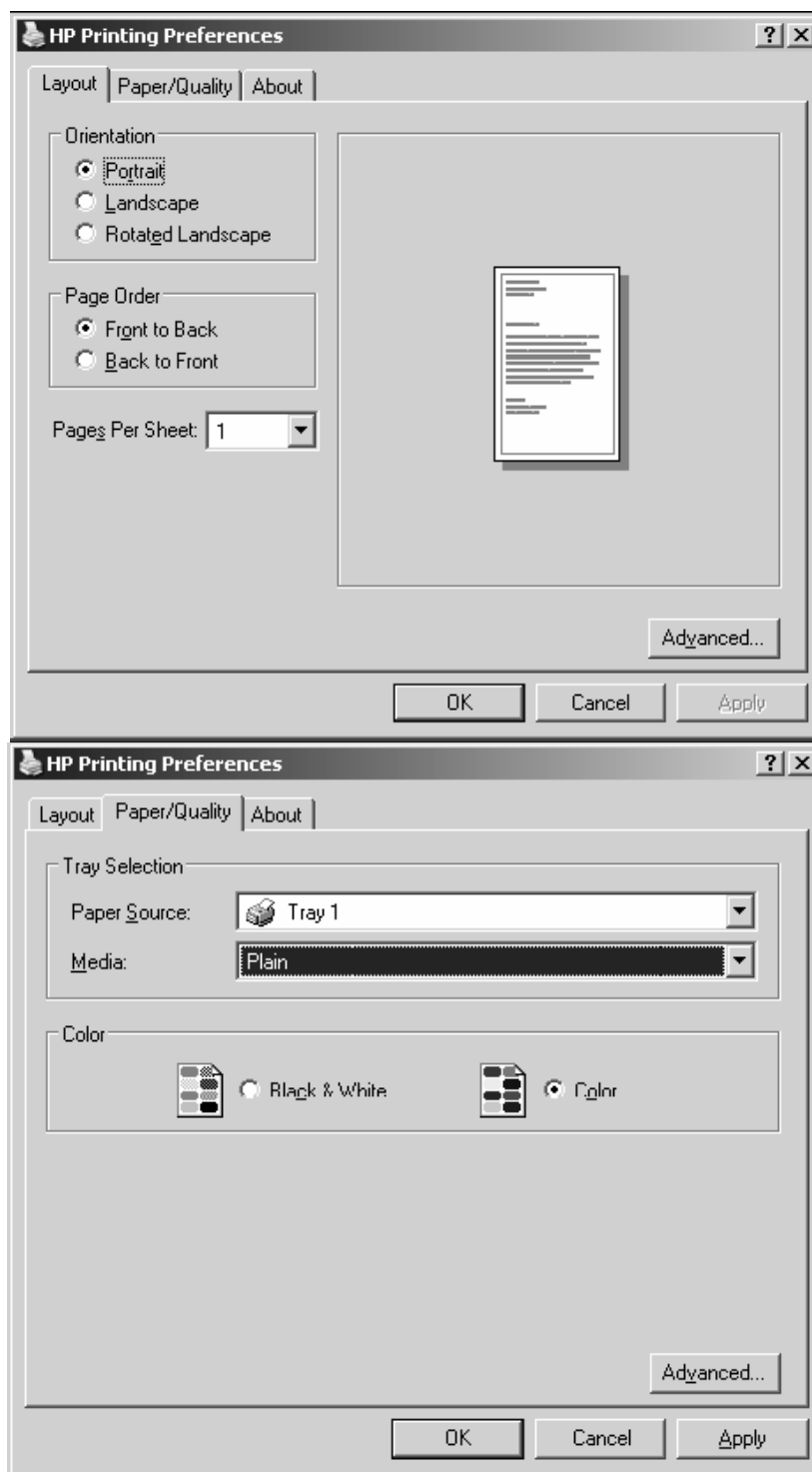
## II. QUẢN LÝ THUỘC TÍNH MÁY IN

### Cấu hình Layout

Trong hộp thoại Printing Preferences, chọn Tab Layout.

Trong mục Orientation, chọn cách thức in trang theo chiều ngang hay chiều dọc.





Trong mục Page Order, 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.

### **Giấy và chất lượng in**

Trong hộp thoại Printing Preferences, 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.

### **Các thông số mở rộng**

Chọn Advanced ở góc dưới bên phải của hộp thoại Printing Preferences. Hộp thoại Advanced Options xuất hiện cho phép điều chỉnh các thông số mở rộng: 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 đang sử dụng.

### III. CẤU HÌNH CHIA SẺ MÁY IN

Click phải chuột lên máy in, chọn Properties. Hộp thoại Properties xuất hiện, chọn Tab Sharing.



Để chia sẻ máy in này cho nhiều người dùng, chọn Share this printer. Trong mục Share name, nhập vào tên chia sẻ của máy in (giống như khi chia sẻ thư mục), tên này sẽ được nhìn thấy trên mạng.

Có thể 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.

### IV. CẤU HÌNH THÔNG SỐ PORT

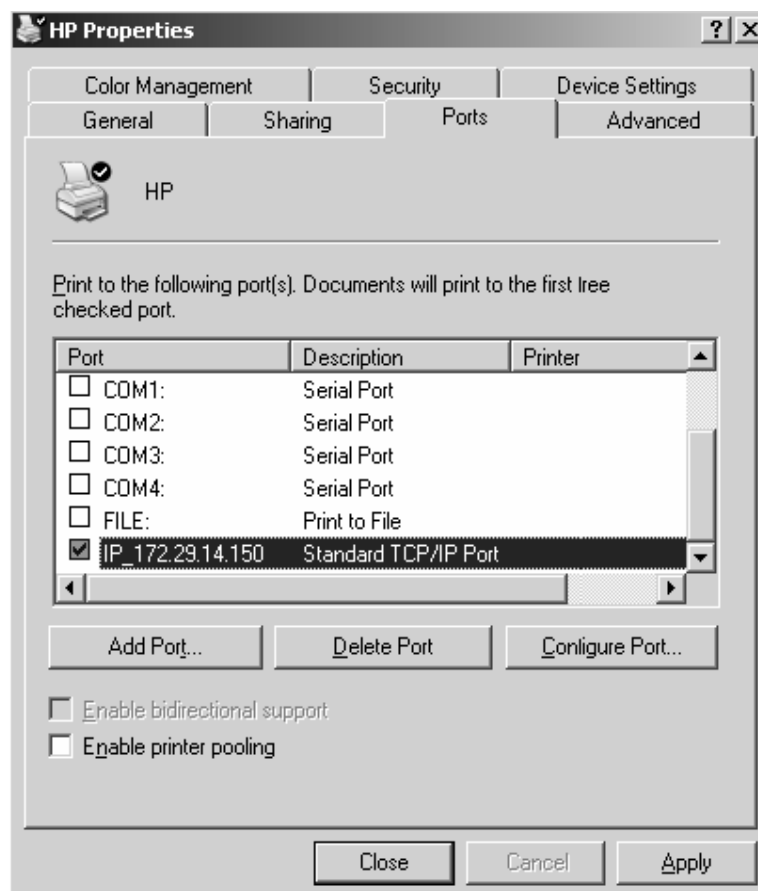
#### Cấu hình các thông số trong Tab Port

Trong hộp thoại Properties, chọn Tab Port để cấu hình tất cả các port đã được định nghĩa cho máy in sử dụng.

Một port được xem như một interface để máy tính giao tiếp với máy in. Windows Server 2003 hỗ trợ các port vật lý (local port) và các port TCP/IP chuẩn (port logic).

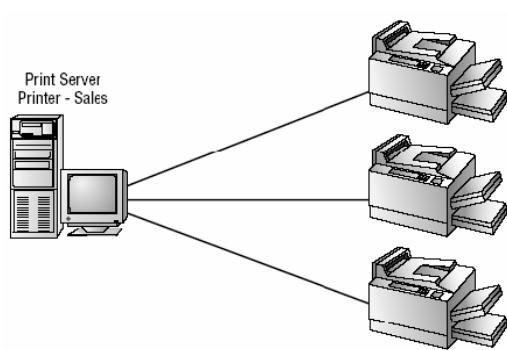
Port vật lý chỉ được sử dụng khi ta gắn trực tiếp máy in vào máy tính.

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.

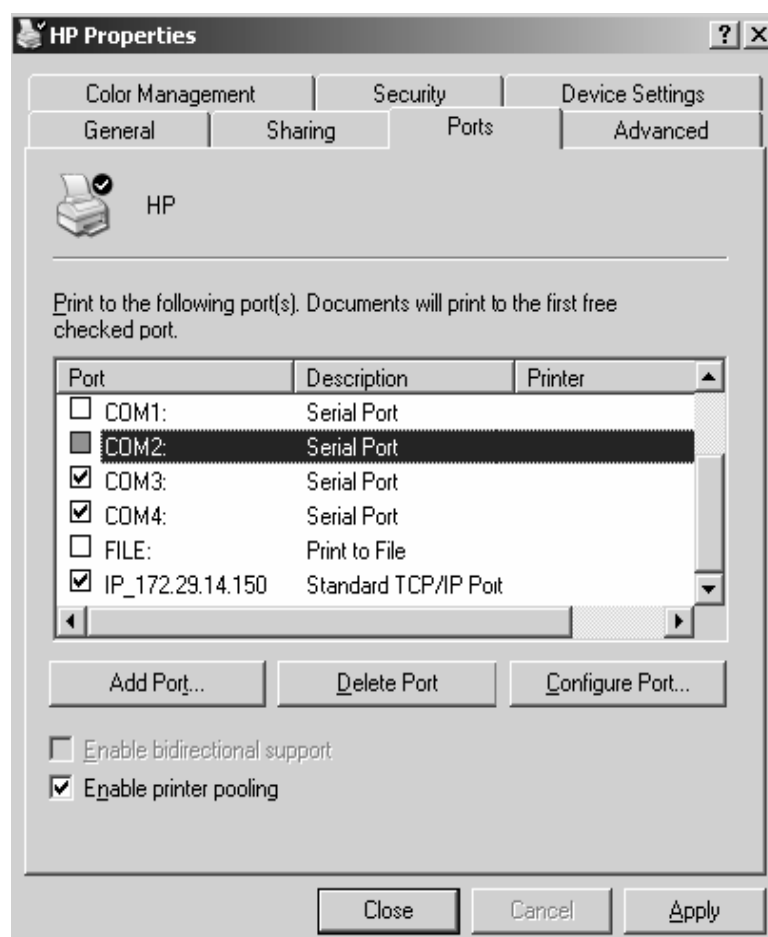


## Printer Pooling

Printer pool được sử dụng nhằm phối hợp nhiều máy in vật lý với nhau thành 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. 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.



### Các bước cấu hình một printer pool:

Chọn tùy chọn Enable Printer Pooling nằm ở phía dưới Tab Port trong hộp thoại Properties.

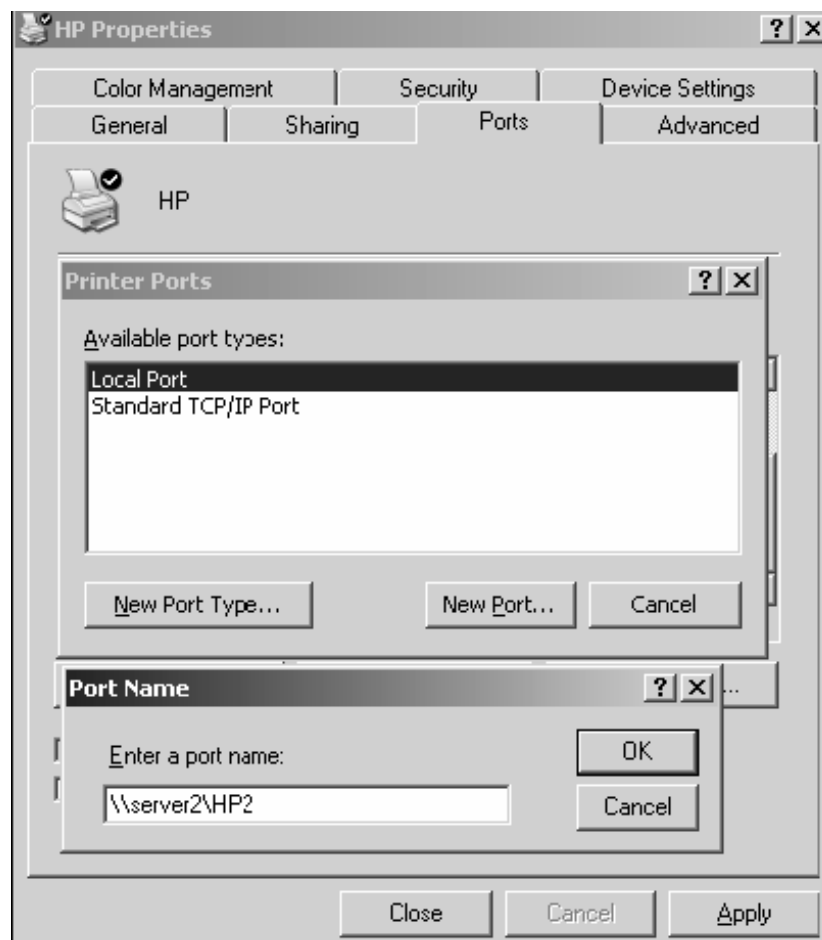
Kiểm tra lại tất cả các port mà ta dự định gắn các máy in vật lý trong printer pool vào.

Nếu không chọn tùy chọn Enable Printer Pooling thì 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.

### Điều hướng tác vụ in đến một máy in khác

Nếu một máy in vật lý bị hư, có thể chuyển tất cả các tác vụ in ẩn của máy in bị hư sang một máy in khác. Để làm được điều này, máy in mới phải có driver giống với máy in cũ.



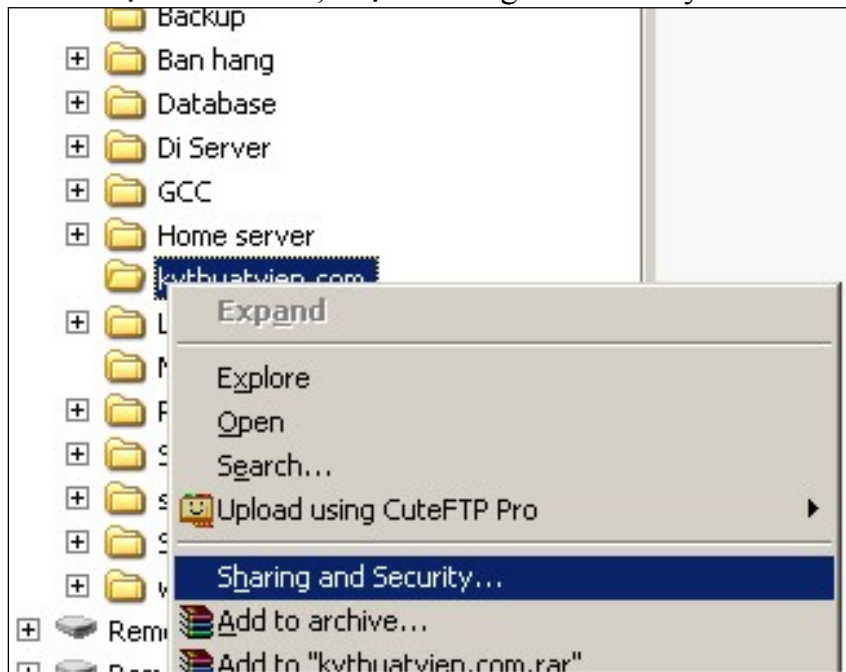
Trong Tab Port, chọn Add Port, chọn Local port rồi chọn tiếp New Port. Hộp thoại Port Name xuất hiện, gõ vào tên UNC của máy in mới theo định dạng: \\computername\printer\_sharename.

# BÀI 10: BẢO MẬT HỆ THỐNG

## I. SHARE PERMISSION

### Chia sẻ tài nguyên

Click chuột phải lên thư mục cần chia sẻ, chọn Sharing and Security



Chọn Share this folder



### Phân quyền cho User

Chọn Permissions

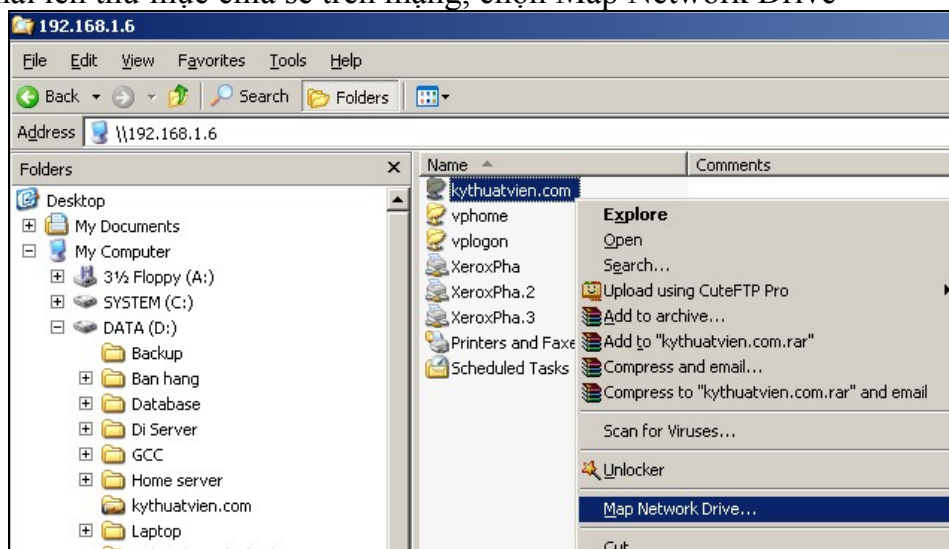
Có thể giới hạn quyền cho từng group hoặc user

Allow: có quyền

Denny: không có quyền

## Tạo ổ đĩa ánh xạ (Map Network Drive)

Click chuột phải lên thư mục chia sẻ trên mạng, chọn Map Network Drive



Chọn tên ổ đĩa dùng để ánh xạ rồi chọn Finish



## II. ROAMING USER - HOMEDIR & PROFILE

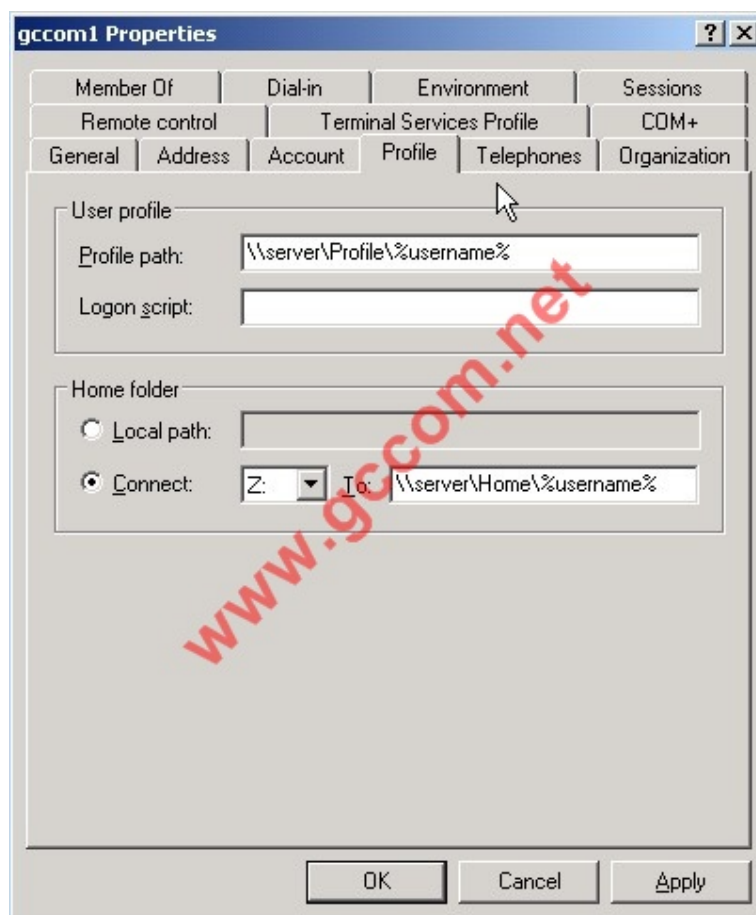
### Giới thiệu

Khi user ngồi vào máy nào login vẫn ok nhưng những tài liệu mà user đó đang làm chứa trên máy Client 01 thì khi login vào máy Client 02 chẳng thấy đâu những thay đổi màn hình desktop, tính chỉnh start menu cũng không được lưu lại. Bởi vì khi đăng nhập vào bất cứ máy Client nào, các Profile của User này sẽ chỉ lưu trên máy Client đó mà thôi.

Vì vậy để cho tiện dụng với các user thường xuyên thay đổi chỗ làm việc ta sử dụng Roaming User.

### Khởi tạo

- Tạo 2 folder tên là Home và Profile
- Chia sẻ 2 folder trên với Full cho Everyone
- Tạo 2 user gcom1 & gcom2
- Double click vào từng user chọn Tab Profile:
  - \\[Tên Server][Thư mục Profile]\%username%
  - \\[Tên Server][Thư mục Home]\%username%



### Kiểm tra

- Logon bằng user gcom1 từ máy client 1
- Chỉnh sửa màn hình Desktop sau đó Logoff
- Logon bằng user gcom1 từ máy client 2

## III. ORGANIZATION UNIT

### Giới thiệu

Khi triển khai hệ thống mạng cho hàng trăm (thậm chí hàng ngàn) người sử dụng thì việc tạo tài khoản sẽ mất rất nhiều thời gian.

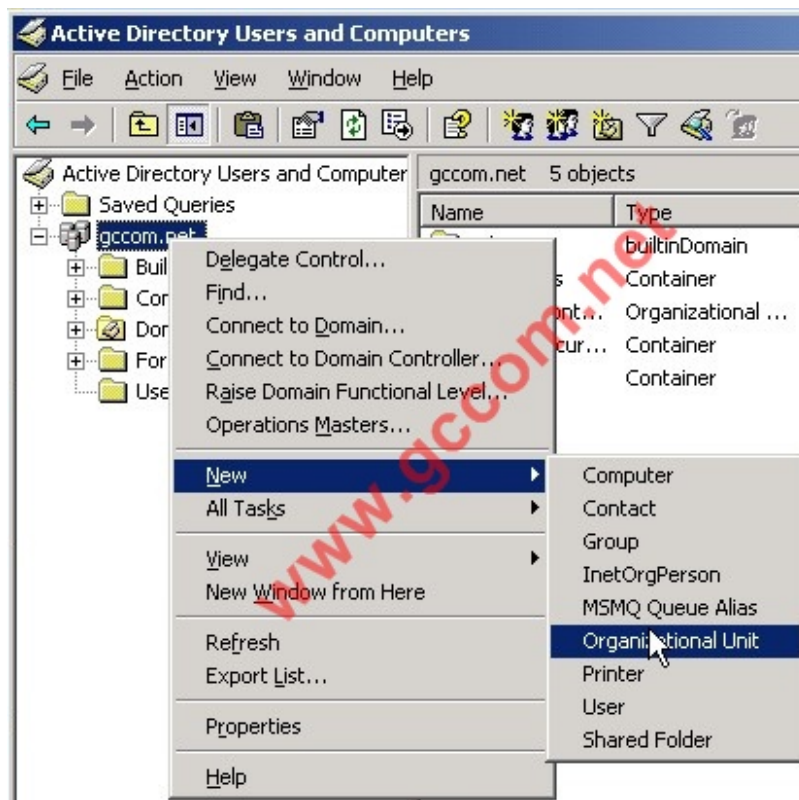
Organizational Unit (OU) giúp giảm tải công việc cho người quản trị mạng bằng cách uỷ quyền cho một User nào đó có quyền thay thế anh ta trong việc quản lý các User Account nhưng với quyền hạn chế hơn. Ví dụ anh quản trị mạng sẽ uỷ quyền cho User gcom1 có quyền tạo, xoá, disable các Account chung Group với anh ta nhưng không có quyền với các Group khác.

### Tạo OU

Click chuột phải vào domain chọn New -> Organizational Unit

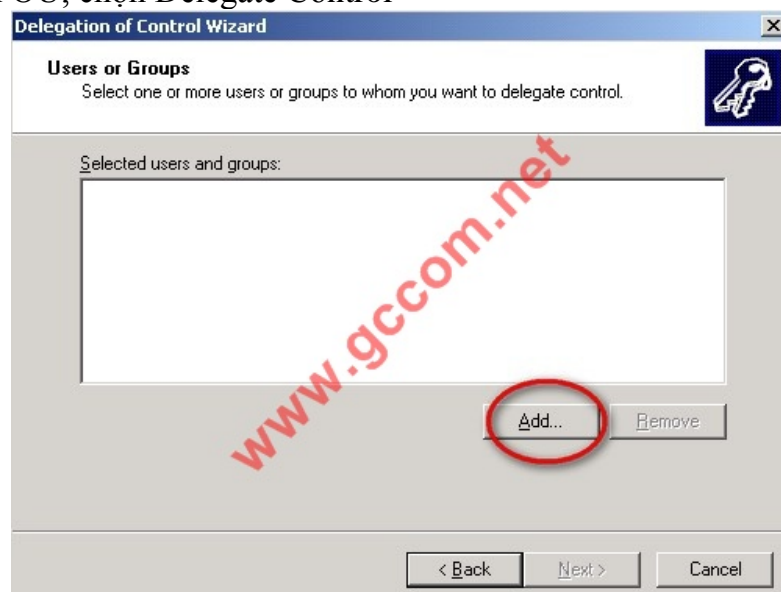
Di chuyển user vào OU: Click chuột phải lên user, chọn Move rồi chọn OU



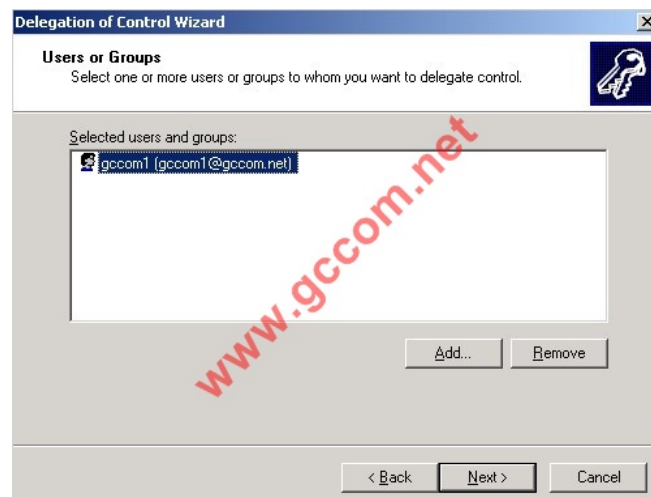


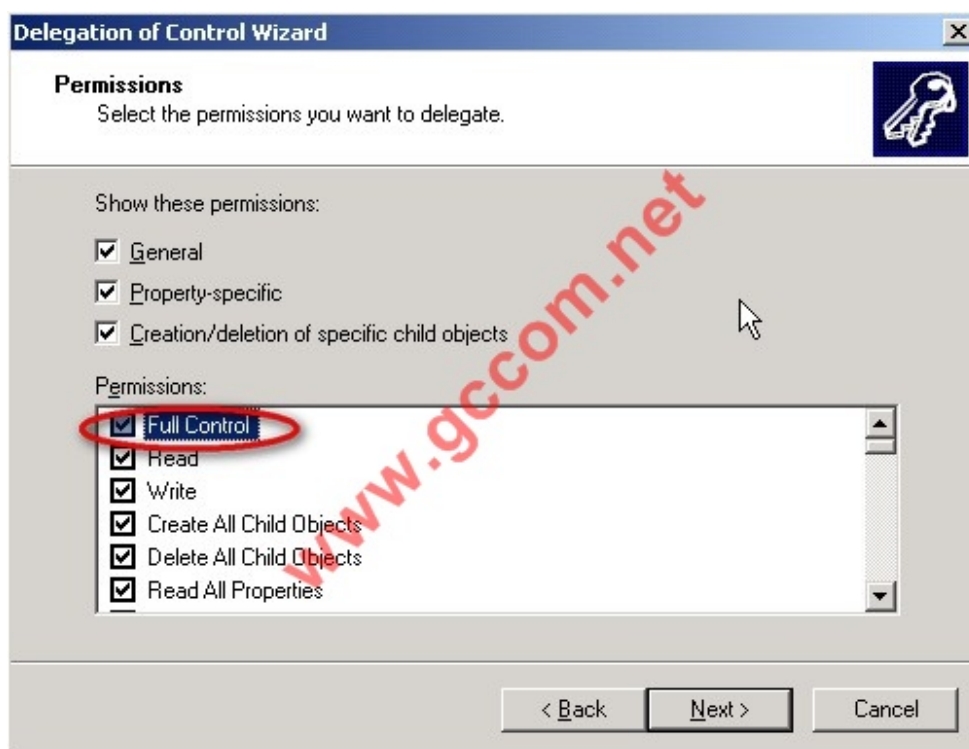
## Gán quyền

Click chuột phải lên OU, chọn Delegate Control



Chọn Add.





Chọn User, Next

Chọn Create a custom task to delegate

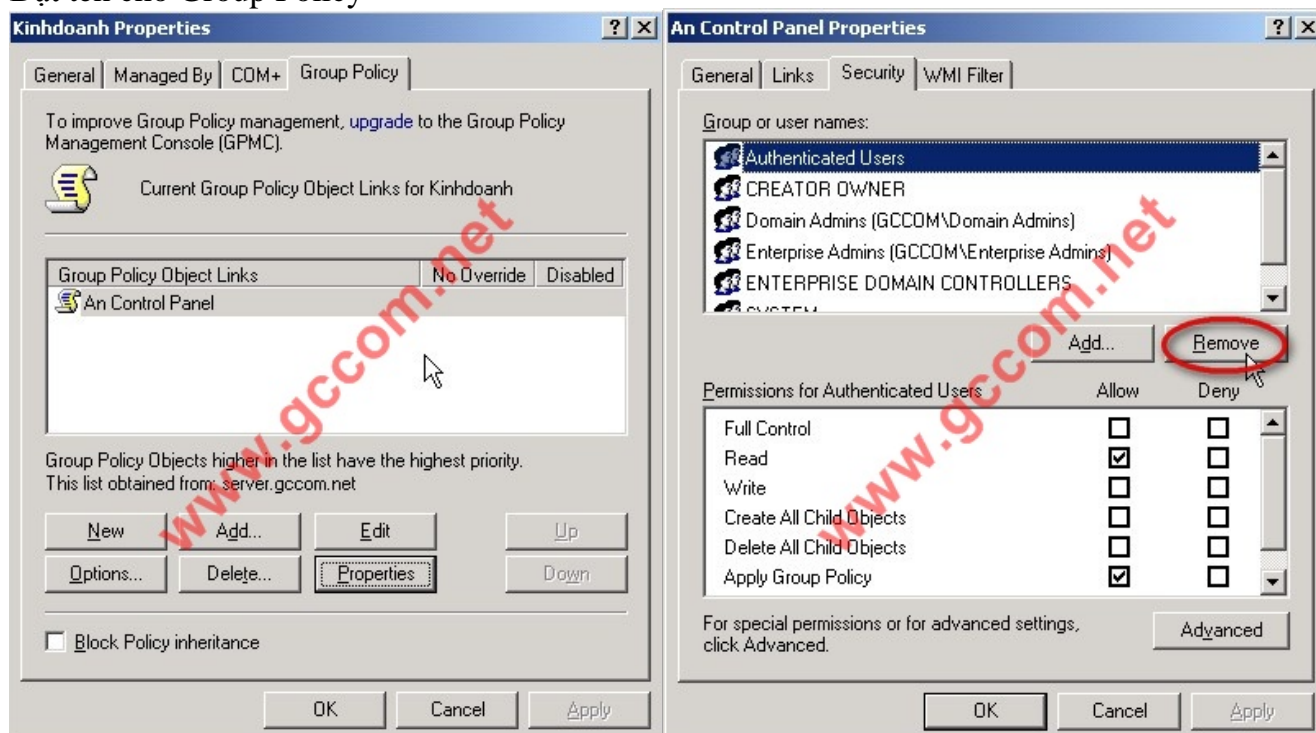
Chọn Next, chọn Full control

## OU Group Policy

Click chuột phải lên tên của OU, chọn Properties

Chọn tab Group Policy, chọn New

Đặt tên cho Group Policy



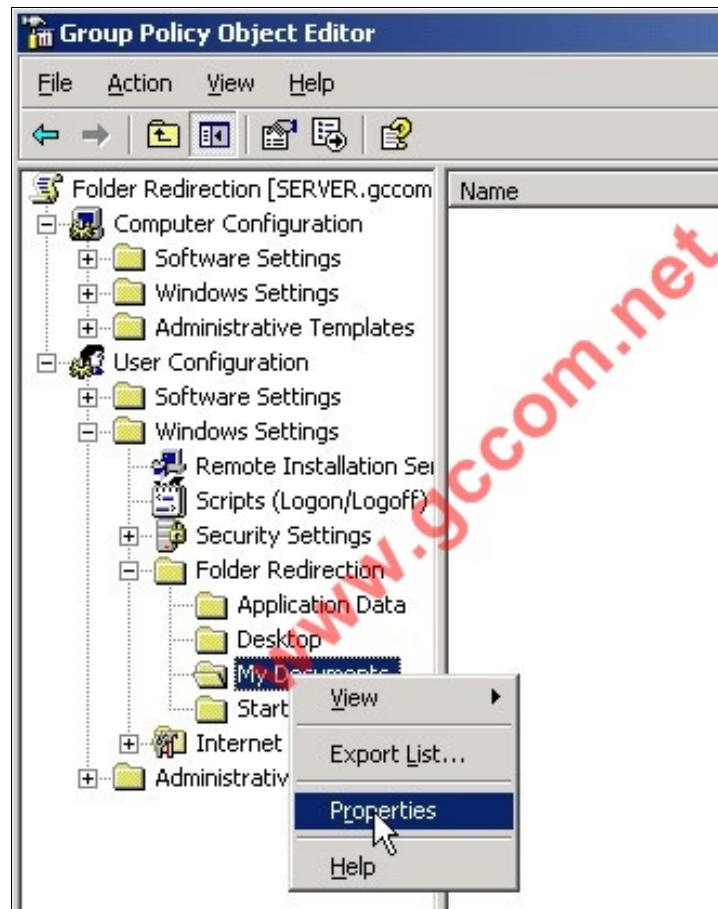
Chọn Edit để cấu hình các thông số

Chọn Properties để cấu hình áp đặt người dùng chịu tác động

## IV. FOLDER REDIRECTED

### Giới thiệu

Roaming User dành cho các User thường xuyên thay đổi nơi làm việc, với dữ liệu luôn luôn được lưu tại 2 nơi là Server và máy Client mà User đó ngồi. Nhưng trong một số trường hợp ta không muốn lưu trữ lung tung như thế mà chỉ muốn dữ liệu của User tạo ra chỉ lưu trên Server mà thôi, chính vì thế Windows Server 2003 có công cụ gọi là Folder Redirection giúp ta giải quyết vấn đề này.



### Thiết lập

Trên Server, tạo một thư mục mang tên FolderRD và Share nó với Everyone là Full Control  
Trong Active Directory Users and Computers, click chuột phải lên tên OU, chọn Properties  
Chọn tab Group Policy, chọn New, đặt tên là Folder Redirection, chọn Edit  
Folder Redirection hỗ trợ 4 folder

- Application Data
- Desktop
- My Documents
- Start Menu

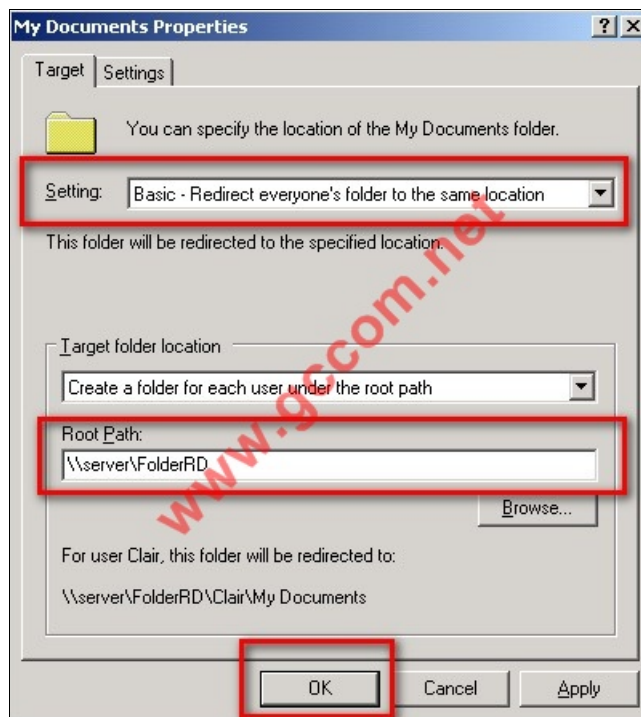
Các thay đổi của user khi ngồi trên máy Client sẽ được lưu lên 4 thư mục này

Click phải vào My Documents -> Properties

Trong ô Setting, chọn Basic - Redirect everyone's folder to the same location

Trong dòng Root path, nhập \\SERVER\FolderRD Trong đó SERVER là tên máy DC Folder  
FolderRD là thư mục ta vừa Share

Sau đó chọn OK



Từ máy Client ta đăng nhập với Account gccom1 sẽ thấy thư mục mặc định của My Documents là \\server\FolderRD\gccom1\My Documents  
Logoff máy Client ra và trở lại thư mục FolderRD trên server sẽ thấy máy tự lưu dữ liệu từ Client lên Server