



**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**



**BÀI GIẢNG MÔN**

# **Hệ Điều Hành Windows và LINUX/UNIX**

**Giảng viên:**

**TS. Phạm Hoàng Duy**

**Điện thoại/E-mail:**

**phamhduy@gmail.com**

**Bộ môn:**

**An Toàn Thông Tin- Khoa CNTT1**

**Học kỳ/Năm biên soạn:2015**

## Microsoft Windows

### ❖ Chương 3: Quản trị các máy chủ dịch vụ của Windows Server

- 3.1 Quản trị Active Directory
- 3.2 Quản trị máy chủ dịch vụ web
- 3.3 Quản trị máy chủ dịch vụ DNS và DHCP
- 3.4 Quản trị máy chủ dịch vụ file và in ấn
- 3.5 Quản trị máy chủ dịch vụ truy nhập từ xa

## DNS

- ❖ Dịch vụ tên miền - Domain Name Service
  - Là hệ thống quản lý cơ sở dữ liệu phân tán dựa trên mô hình phân cấp chủ khách để chuyển đổi tên máy chủ/miền thành địa chỉ IP
- ❖ Miền gốc nằm trên đỉnh của cây tên miền
  - Tên miền gốc .com, .edu, .vn
  - Tên miền mức 2: microsoft.com
- ❖ Tên máy chủ (hostname) được gán cho một máy tính cụ thể trong miền để xác định trạm TCP/IP

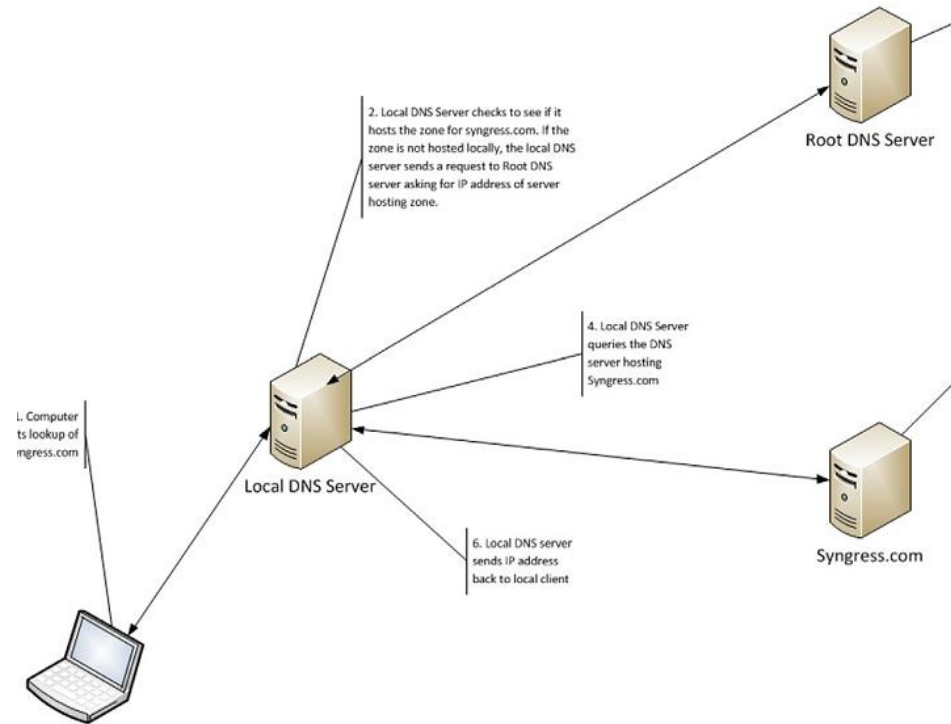


FIGURE 2.20 DNS Lookup Process

## DNS Zone

- ❖ Vùng DNS về căn bản tương ứng với một miền chứa máy chủ DNS
  - Ví dụ: máy chủ DNS ứng với vùng ptit.edu.vn thì tên này phải tạo trên máy chủ DNS.
- ❖ Forward Lookup Zone: cho phép máy tính truy vấn địa chỉ IP ứng với một tên
- ❖ Reverse Lookup Zone: là việc ngược lại trả lại tên miền ứng với địa chỉ IP

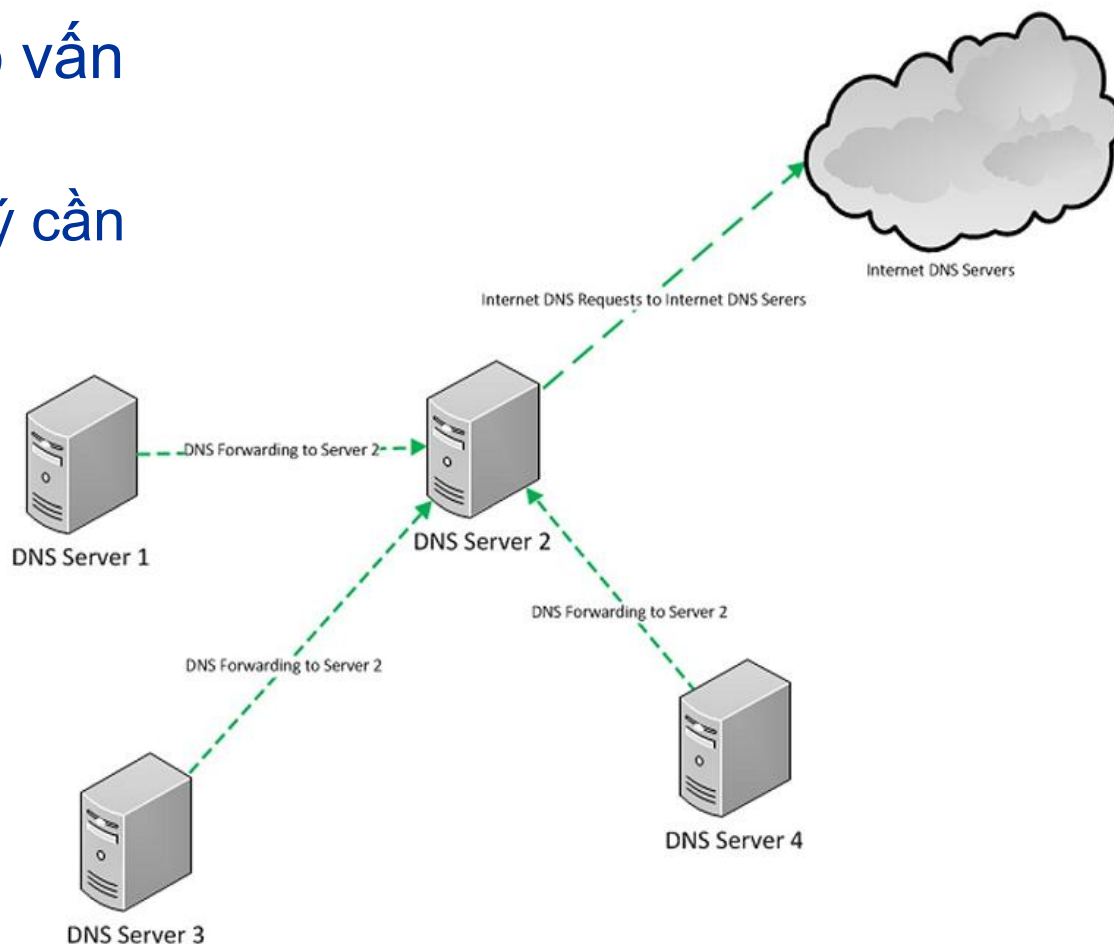
## Bản ghi DNS

- ❖ Bản ghi máy chủ
  - Thông tin căn bản ánh xạ tên của một máy chủ ra địa chỉ IP
- ❖ Bản ghi CNAME
  - Ánh xạ máy chủ tới một tên có sẵn
  - Ví dụ: ptit.edu.vn ptit1.edu.vn
- ❖ Bản ghi NS
  - Lưu định danh các máy chủ DNS trong miền
- ❖ Bản ghi dịch vụ SRV
  - Hỗ trợ việc tự động phát hiện các tài nguyên TCP/IP có trên mạng
- ❖ Bản ghi con trỏ PTR
  - Là các bản ghi tìm kiếm ngược

## Xác định hạng tầng DNS


### ❖ Cần xem xét một số vấn đề sau

- Số các mạng vật lý cần dịch vụ DNS
- Bảng thông WAN
- Số miền hay vùng
- Các dạng bản ghi
- Số lượng bản ghi



## Cài đặt DNS

**Add Roles Wizard**

 **Select Server Roles**

**Before You Begin**

**Server Roles**

- DNS Server
- DHCP Server
  - IPv4 DNS Settings
  - IPv4 WINS Settings
  - DHCP Scopes
  - DHCPv6 Stateless Mode
  - IPv6 DNS Settings
- Confirmation
- Progress
- Results

Select one or more roles to install on this server.

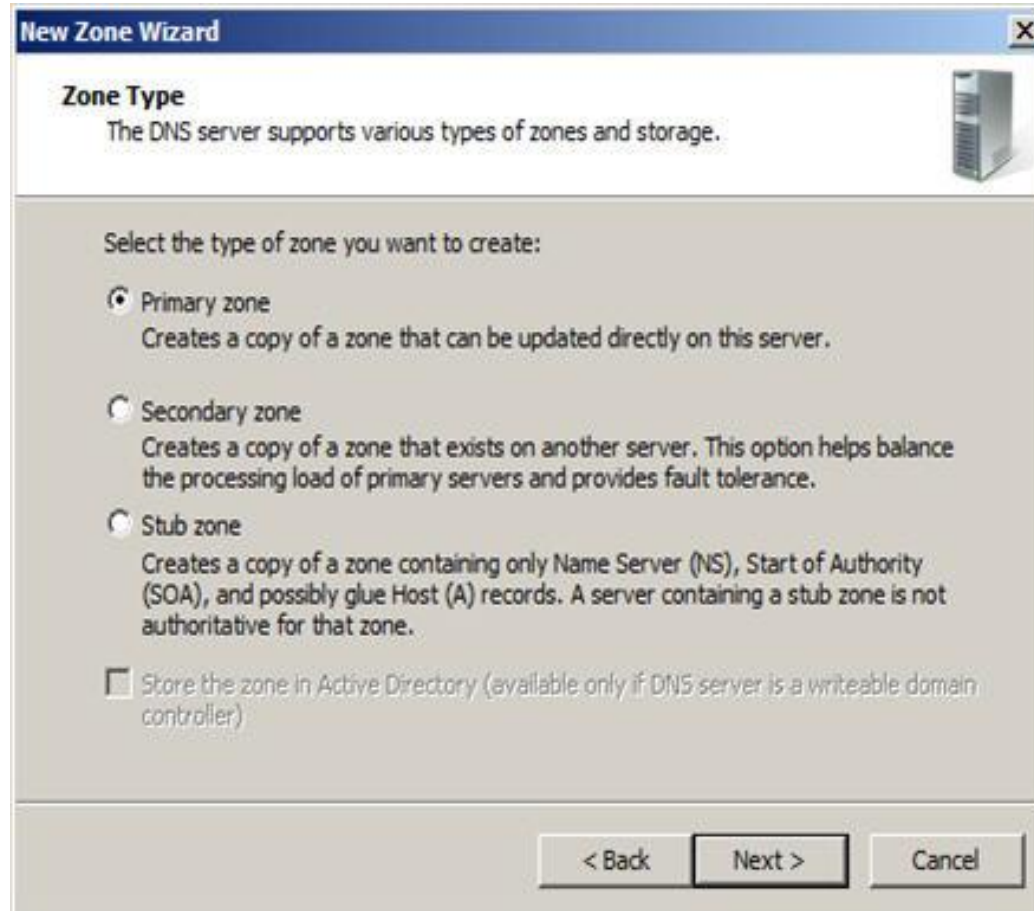
Roles:

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☒ DHCP Server
- ☒ **DNS Server**
- ☐ Fax Server
- ☐ File Services
- ☐ Network Policy and Access Services
- ☐ Print Services
- ☐ Terminal Services
- ☐ UDDI Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

[More about server roles](#)



## Tạo vùng DNS



## Bản ghi DNS

**New Host**

Name (uses parent domain name if blank):  
Javelin

Fully qualified domain name (FQDN):  
Javelin.NorthAmerica.WatchTower.local.

IP address:  
192.168.1.51

☒ Create associated pointer (PTR) record

Add Host Cancel

**New Resource Record**

Pointer (PTR)

Host IP Address:  
192.168.1.55

Fully qualified domain name (FQDN):  
55.1.168.192.in-addr.arpa

Host name:  
Superman Browse...

OK Cancel

## DHCP

- ❖ Duy trì danh sách các địa chỉ IP và cấp cho các máy tính trong mạng sử dụng theo khoảng thời gian xác định
- ❖ Khi xây dựng hạ tầng cho DHCP cần xem xét
  - Số lượng mạng vật lý hay lô-gisc cần tự động cấu hình IP
  - Vị trí bộ định tuyến
  - Số mạng LAN ảo

## DHCP

### ❖ Định nghĩa một vùng địa chỉ

The screenshot shows the 'Add Scope' dialog box in the Windows DHCP console. The dialog box has a title bar with 'Add Scope' and a close button. Below the title bar, there is a descriptive text: 'A scope is a range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.' The dialog is divided into two main sections: 'Configuration settings for DHCP Server' and 'Configuration settings that propagate to DHCP client'. In the first section, the 'Scope name' is 'How-To Geek Scope', 'Starting IP address' is '10.10.10.10', 'Ending IP address' is '10.10.10.254', 'Subnet type' is 'Wired (lease duration will be 8 days)', and the 'Activate this scope' checkbox is checked. In the second section, the 'Subnet mask' is '255.255.255.0' and the 'Default gateway (optional)' is '10.10.10.1'. At the bottom right, there are 'OK' and 'Cancel' buttons.

**Add Scope**

A scope is a range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Configuration settings for DHCP Server

Scope name: How-To Geek Scope

Starting IP address: 10.10.10.10

Ending IP address: 10.10.10.254

Subnet type: Wired (lease duration will be 8 days)

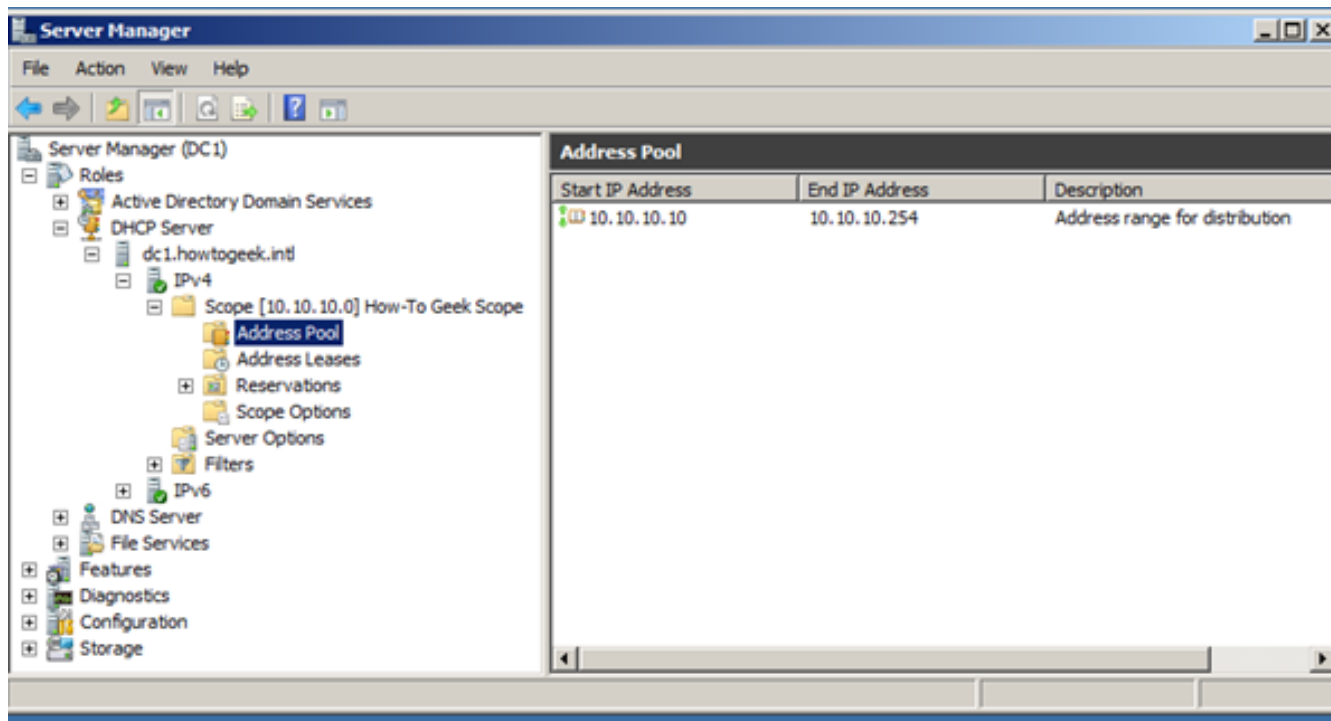
☒ Activate this scope

Configuration settings that propagate to DHCP client

Subnet mask: 255.255.255.0

Default gateway (optional): 10.10.10.1

OK Cancel



## Kiểm tra

- ❖ Ping
- ❖ Pathping
- ❖ Nslookup
- ❖ ipconfig

## Microsoft Windows

### ❖ Chương 3: Quản trị các máy chủ dịch vụ của Windows Server

- 3.1 Quản trị Active Directory
- 3.2 Quản trị máy chủ dịch vụ web
- 3.3 Quản trị máy chủ dịch vụ DNS và DHCP
- 3.4 Quản trị máy chủ dịch vụ file và in ấn
- 3.5 Quản trị máy chủ dịch vụ truy nhập từ xa

## Active Directory

- ❖ Dịch vụ thư mục nhằm lưu trữ, tổ chức và đảm bảo truy nhập các thông tin trong thư mục
- ❖ Dịch vụ thư mục mạng được dùng để xác định, quản lý và quản trị và tổ chức các mục, tài nguyên mạng dùng chung như ổ đĩa, thư mục, máy in người dùng ...



## Active Directory

- ❖ Thư mục động là công nghệ do Microsoft đưa ra cung cấp một số dịch vụ
  - LDAP
  - Xác thực một lần dựa trên Kerberos
  - Đặt tên dựa trên DNS
  - Quản trị mạng tập trung

## Active Directory

### ❖ LDAP

- Giao thức mức ứng dụng dùng cổng 389 cho truy vấn và thay đổi dữ liệu sử dụng dịch vụ thư mục mạng trên TCP/IP.
- Các đối tượng trong thư mục được tổ chức theo giới hạn của cơ quan hay địa lý.

### ❖ Kerberos

- Giao thức xác thực mạng máy tính cho phép các máy xác định định danh cửa mình qua mạng không an toàn một cách đảm bảo.

### ❖ Quản trị mạng tập trung

- Cho phép tổ chức các tài nguyên mạng bao gồm người dùng, nhóm, máy in, máy tính và các đối tượng khác sao cho các người dùng mạng được gán mật khẩu, quyền sử dụng các đối tượng này

## Active Directory

- ❖ Miền – Domain
  - Đơn vị lô gíc các máy tính và tài nguyên mạng xác định ranh giới an ninh.
  - Sử dụng một cơ sở liệu miền động đơn lẻ chia sẻ thông tin chung về an ninh và người dùng cho phép quản lý tập trung toàn bộ người dùng, nhóm và tài nguyên mạng
  - Một cơ quan có thể có nhiều miền
- ❖ Cây – Tree
  - Chứa một hay nhiều miền dùng chung không gian định danh
    - Ví dụ: fit.ptit.edu.vn
- ❖ Rừng – Forest
  - Chứa một hay nhiều cây
  - Không gian định danh có thể tách biệt
- ❖ Quan hệ tin cậy – Trust relationship
  - Cho phép người dùng từ các miền khác nhau sử dụng tài nguyên mạng của các miền.

## Active Directory

### ❖ Điểm – Site

- Nhóm các máy tính cùng mạng con IP kết nối tốc độ cao với nhau

### ❖ Máy chủ miền – Domain controller

- Lưu bản sao thông tin tài khoản và an ninh của miền
- Để chống lỗi một điểm có thể có nhiều hơn 1 máy chủ miền.

## Công cụ quản lý Active Directory

### ❖ Active Directory Users and Computers:

- Quản lý người dùng, nhóm, các máy tính và đơn vị tổ chức

### ❖ Active Directory Domains and Trusts:

- Quản trị các độ tin cậy miền, các mức phục vụ miền và rừng và hậu tiếp tổ tên người dùng

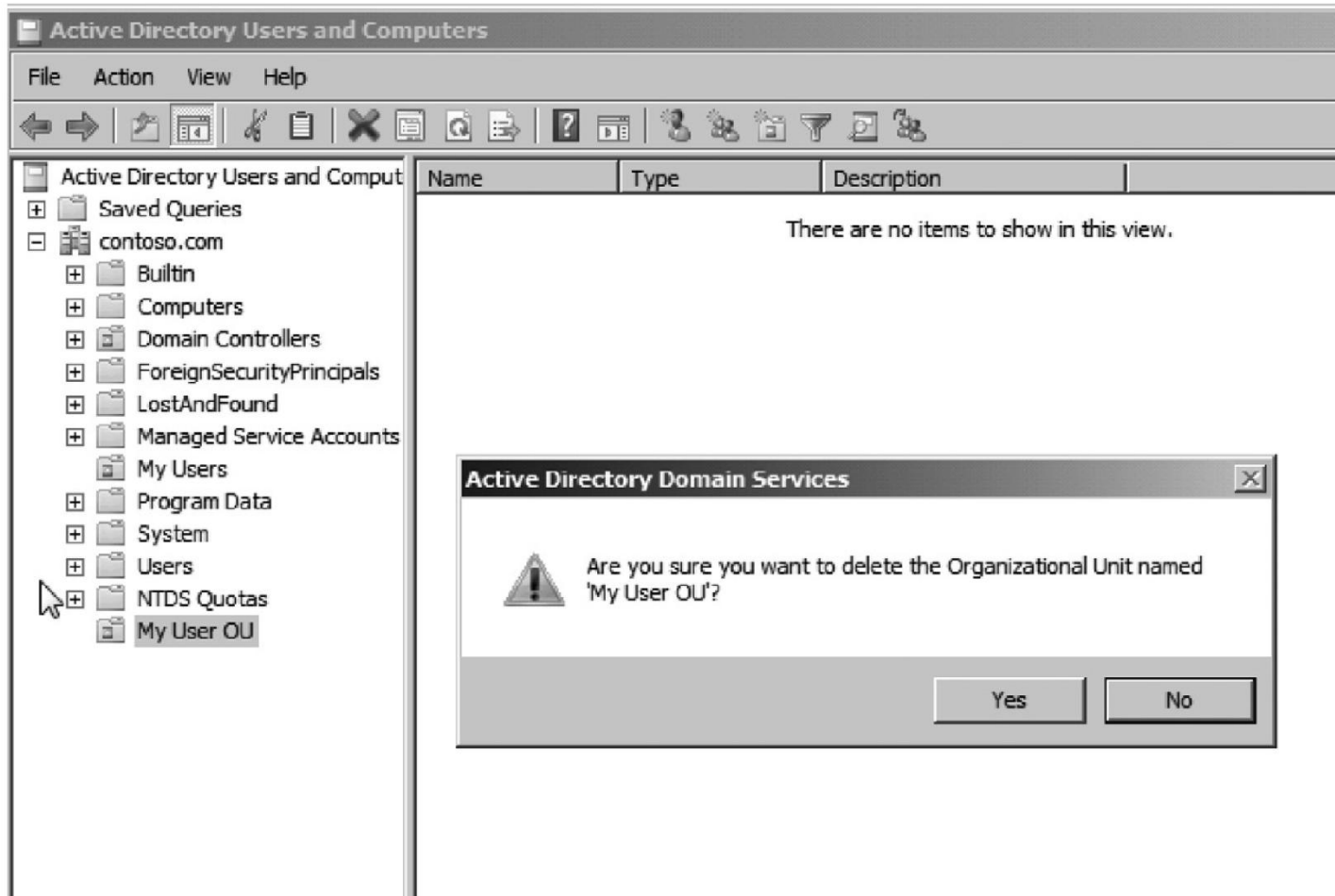
### ❖ Active Directory Sites and Services:

- Quản trị bản sao thư mục giữa các điểm.

### ❖ Active Directory Administrative Center:

- Quản trị và cung cấp thông tin trong thư mục bao gồm quản lý người dùng, nhóm, máy tính, miền, máy chủ miền và các đơn vị tổ chức.

## Active Directory



## Global Catalog

### ❖ Danh mục toàn cục - Global catalog

- Sao chép thông tin cửa từng đối tượng trong cây và rừng
- Giúp truy nhập các đối tượng giữa các miền khác nhau
- Thường lưu các thuộc tính được tìm kiếm thường xuyên như tên người dùng, tên máy tính
- Được tự động tạo ra khi triển khai máy chủ miền đầu tiên của rừng (forest)

### ❖ Danh mục toàn cục được dùng khi người dùng đăng nhập

- Liệt kê thành viên nhóm
- Xác định định danh người dùng khi có nhiều miền

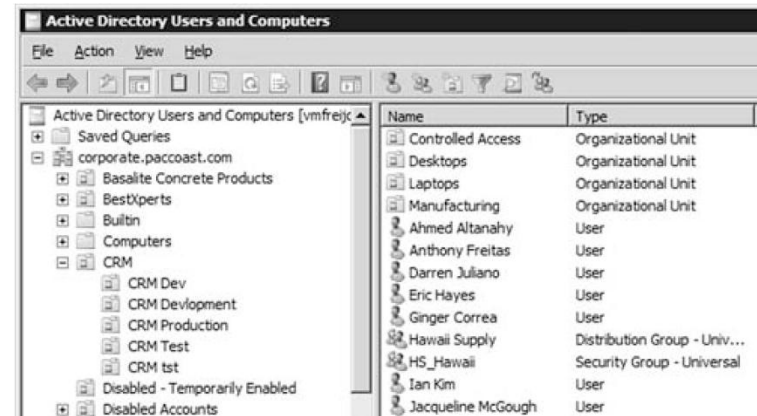
## Global catalog





## Organizational Units

- ❖ Đơn vị tổ chức trợ giúp việc sắp xếp các đối tượng trong miền và giảm thiểu số miền cần thiết
- ❖ Đơn vị tổ chức có thể lưu trữ người dùng, nhóm, máy tính và các đơn vị tổ chức khác
- ❖ Các đơn vị tổ chức tạo trước (như máy tính, người dùng) thì không thể gán quyền hay chính sách nhóm



## Đối tượng

### ❖ Đối tượng – Object

- Tập đặt tên phân biệt các thuộc tính hay đặc tính biểu diễn tài nguyên mạng
- Các đối tượng phổ biến trong thư mục động là máy tính, người dùng, nhóm
- Mỗi đối tượng được gán số duy nhất gọi là Globally unique identifier (GUID) hay định danh an ninh (Security identifier)


### ❖ Schema

- Xác định định dạng các đối tượng và các thuộc tính hay trường trong mỗi đối tượng
- Ví dụ: người dùng có tên, họ số điện thoại, email

## Người dùng

- ❖ Tài khoản người dùng – user account
  - Cho phép người dùng đăng nhập vào máy tính hay miền
- ❖ Trong mạng Windows có hai dạng tài khoản
  - Tài khoản người dùng cục bộ:
    - Thông tin lưu trong phần quản lý tài khoản Security Account Manager trên máy cục bộ
  - Tài khoản người dùng miền
    - Thông tin lưu trong máy chủ miền

**New Object - User** [X]

 Create in: fabrikam.com/Users

---

First name:  Initials:

Last name:

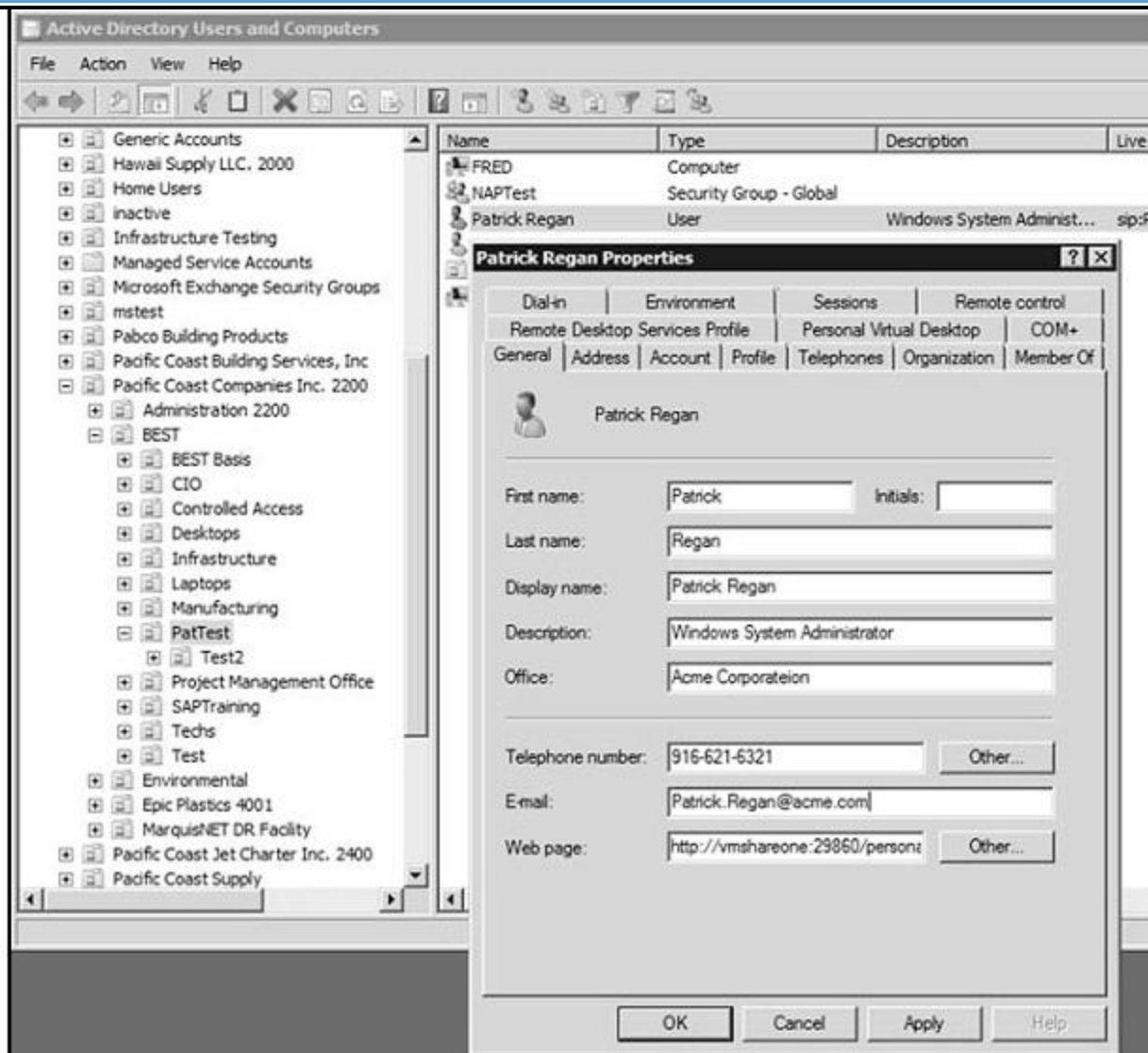
Full name:

User logon name:

User logon name (pre-Windows 2000):

---

< Back   Next >   Cancel



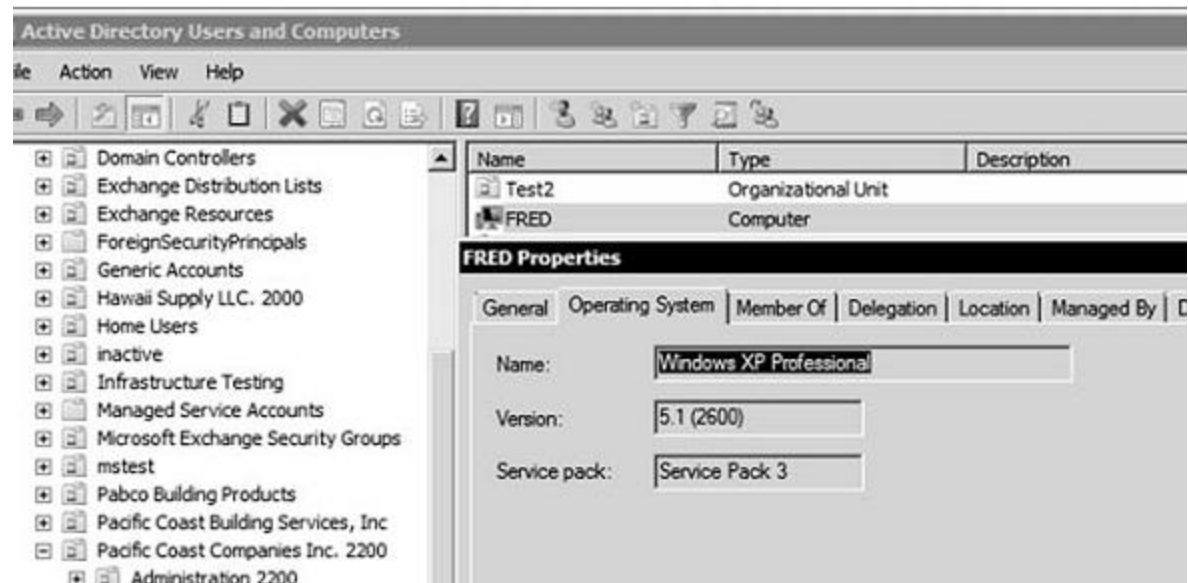
## User profile

- ❖ Liên kết với tài khoản người dùng là danh sách thư mục và dữ liệu về môi trường làm việc của người dùng và cài đặt ứng dụng
  - **Local user profile:**
    - Lưu trong ổ cứng cục bộ mà người dùng đăng nhập
  - **Roaming user profile:**
    - Được tạo và lưu trong thư mục chia sẻ trên máy chủ mạng. Với bất cứ máy tính nào trong miền người dùng có cùng một cài đặt
  - **Mandatory user profile:**
    - Được dùng như profile người dùng chuyển vùng như các thay đổi của người dùng không được lưu lại.

## Máy tính

### ❖ Tài khoản máy tính

- Cung cấp công cụ để theo dõi và giám sát việc truy nhập của máy tính vào mạng và tài nguyên của miền
- Mỗi máy tính có 1 tài khoản duy nhất



## Quản trị người dùng

❖ Sử dụng Active Directory Users and Computers



## WEB-IIS

- ❖ Web là hệ thống các tài liệu dạng siêu văn bản liên kết với nhau (trang web) mà có thể xem được nhờ trình duyệt
- ❖ HTML là ngôn ngữ đánh dấu được trình duyệt thông dịch
- ❖ Các trang web truyền thống là trang web tĩnh. Nội dung không thay đổi nếu không có sự can thiệp của con người.
- ❖ Các trang web được lưu trong máy chủ web dùng cổng TCP 80.

**Add Web Site** [?] [X]

Site name:  Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type:  IP address:  Port:

Host name:

Example: www.contoso.com or marketing.contoso.com

☒ Start Web site immediately

## Tạo Web site

### ❖ Xác thực

- Cài đặt phương thức xác thực dùng cho trang web
- Nặc danh: không hạn chế
- Cơ bản
- Sử dụng Windows

### ❖ Dạng tài liệu ngầm định

- Tự động chuyển đến file ngầm định che dấu cấu trúc thư mục
- Ví dụ: index.htm

## Microsoft Windows

### ❖ Chương 3: Quản trị các máy chủ dịch vụ của Windows Server

- 3.1 Quản trị Active Directory
- 3.2 Quản trị máy chủ dịch vụ web
- 3.3 Quản trị máy chủ dịch vụ DNS và DHCP
- 3.4 Quản trị máy chủ dịch vụ file và in ấn
- 3.5 Quản trị máy chủ dịch vụ truy nhập từ xa

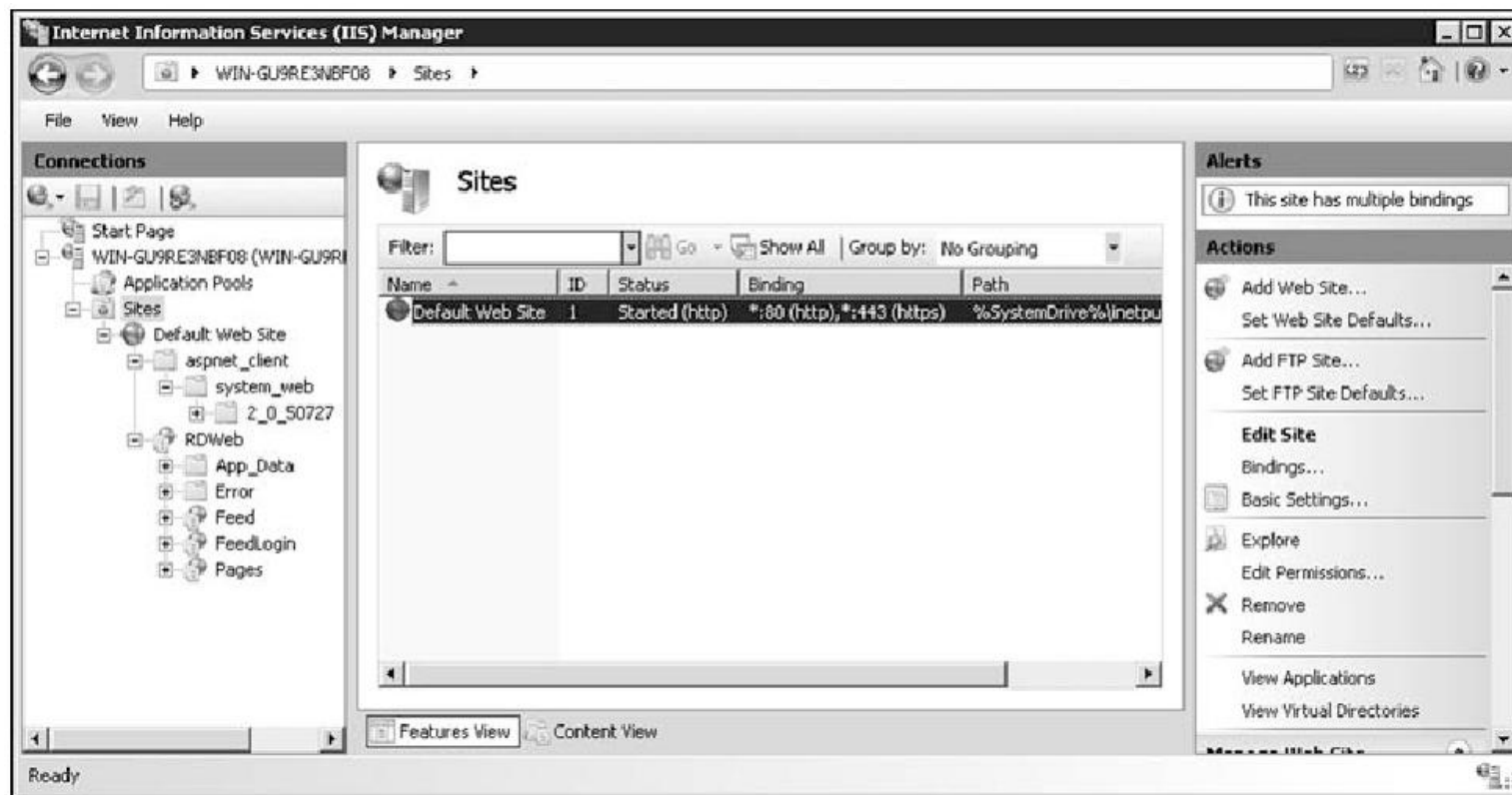
## WEB-IIS

- ❖ Dịch vụ truyền file – FTP Cho phép gửi nhập file giữa hai máy tính qua mạng TCP/IP. Sử dụng 2 cổng 20, 21
- ❖ Dịch vụ gửi thư điện tử SMTP dùng cổng TCP 25

# Hệ Điều Hành Windows và LINUX/UNIX

## WEB-IIS

### ❖ Thêm chức năng Web server

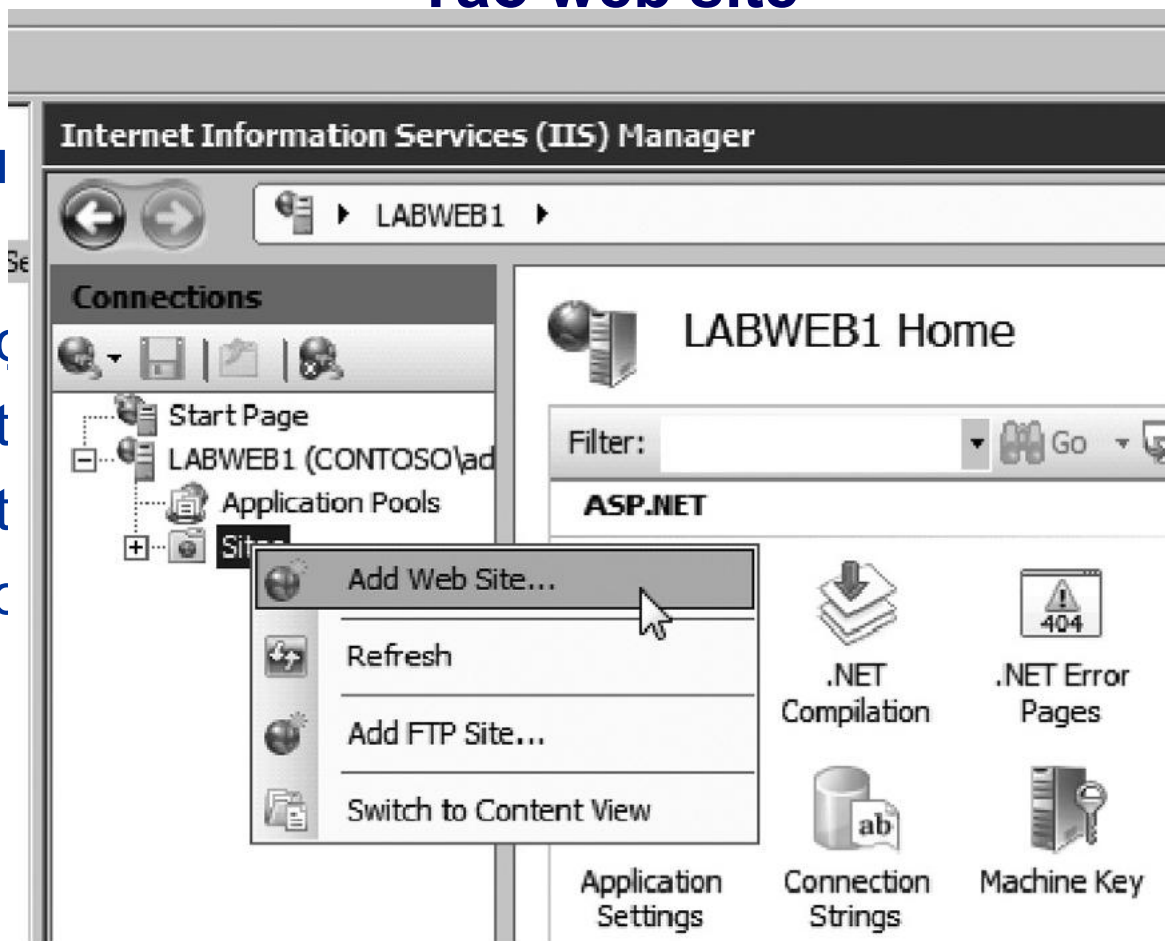


## Tạo web site

❖ Sử dụng

❖ Trong

- Chọn
- Đặt
- Đặt
- Xác



## Microsoft Windows

### ❖ Chương 3: Quản trị các máy chủ dịch vụ của Windows Server

- 3.1 Quản trị Active Directory
- 3.2 Quản trị máy chủ dịch vụ web
- 3.3 Quản trị máy chủ dịch vụ DNS và DHCP
- 3.4 Quản trị máy chủ dịch vụ file và in ấn
- 3.5 Quản trị máy chủ dịch vụ truy nhập từ xa

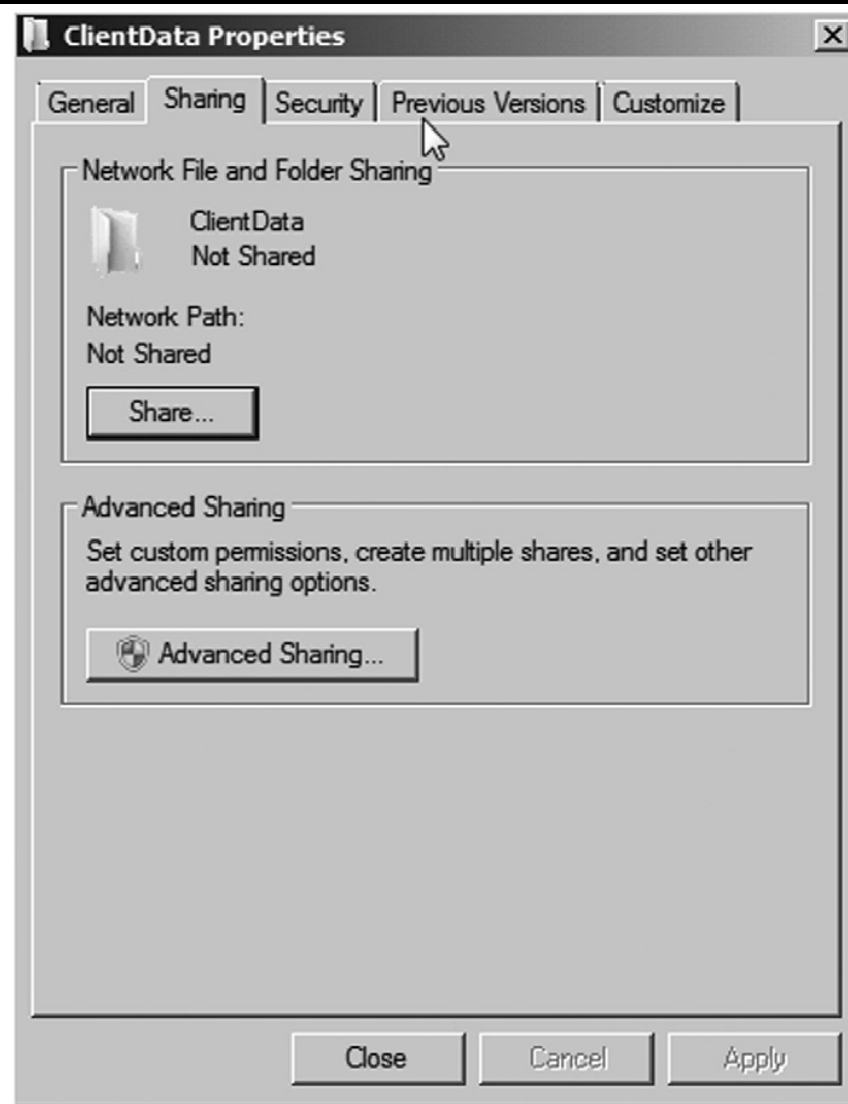


## Dịch vụ file và in ấn

- ❖ Là các dịch vụ căn bản trong môi trường mạng Windows
- ❖ Cung cấp công cụ làm đơn giản hóa việc chia sẻ và quản lý

## Chi

❖ Tạo thư mục chia sẻ

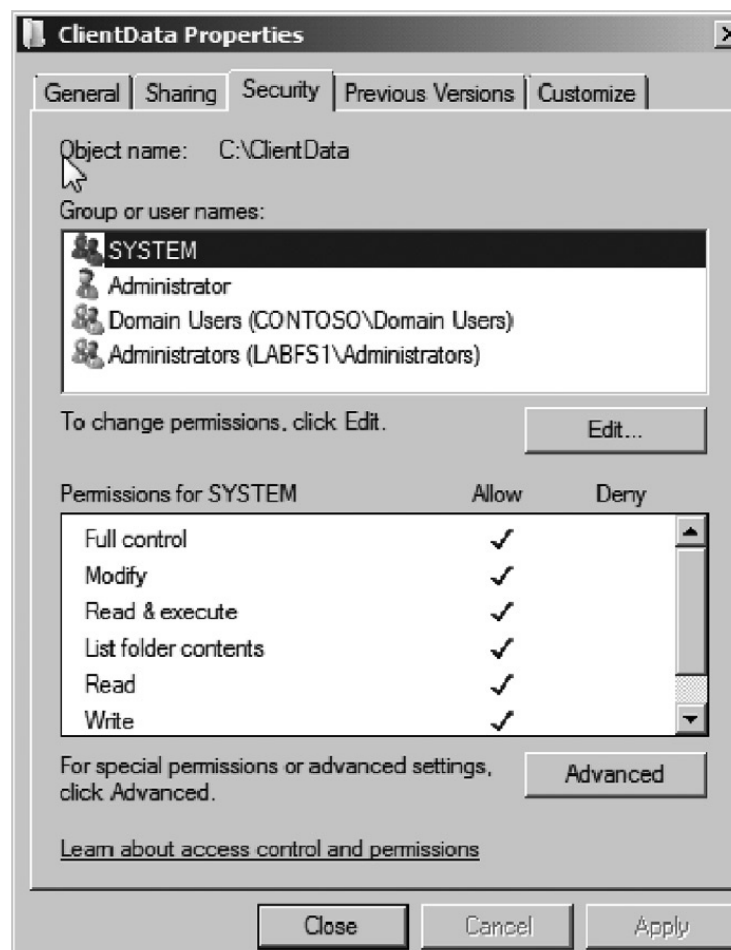
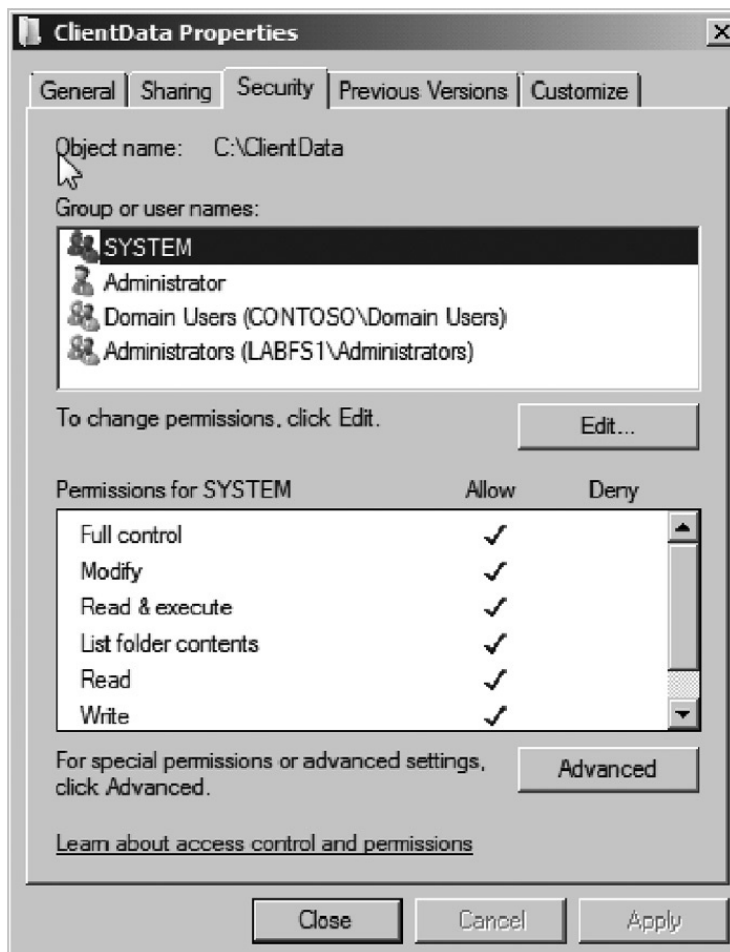


## Chia sẻ file

### ❖ Hỗ trợ hai hình thức đảm bảo an ninh

- Quyền với thư mục chia sẻ
  - Chỉ áp dụng với thư mục.
  - Quyền giới hạn: Đọc Ghi Sơ hữu
- Đặt quyền file/thư ục
  - Sr dụng NTFS để hạn chế việc truy nhập
  - Cho phép giám sát tốt hơn và các quyền chi tiết hơn

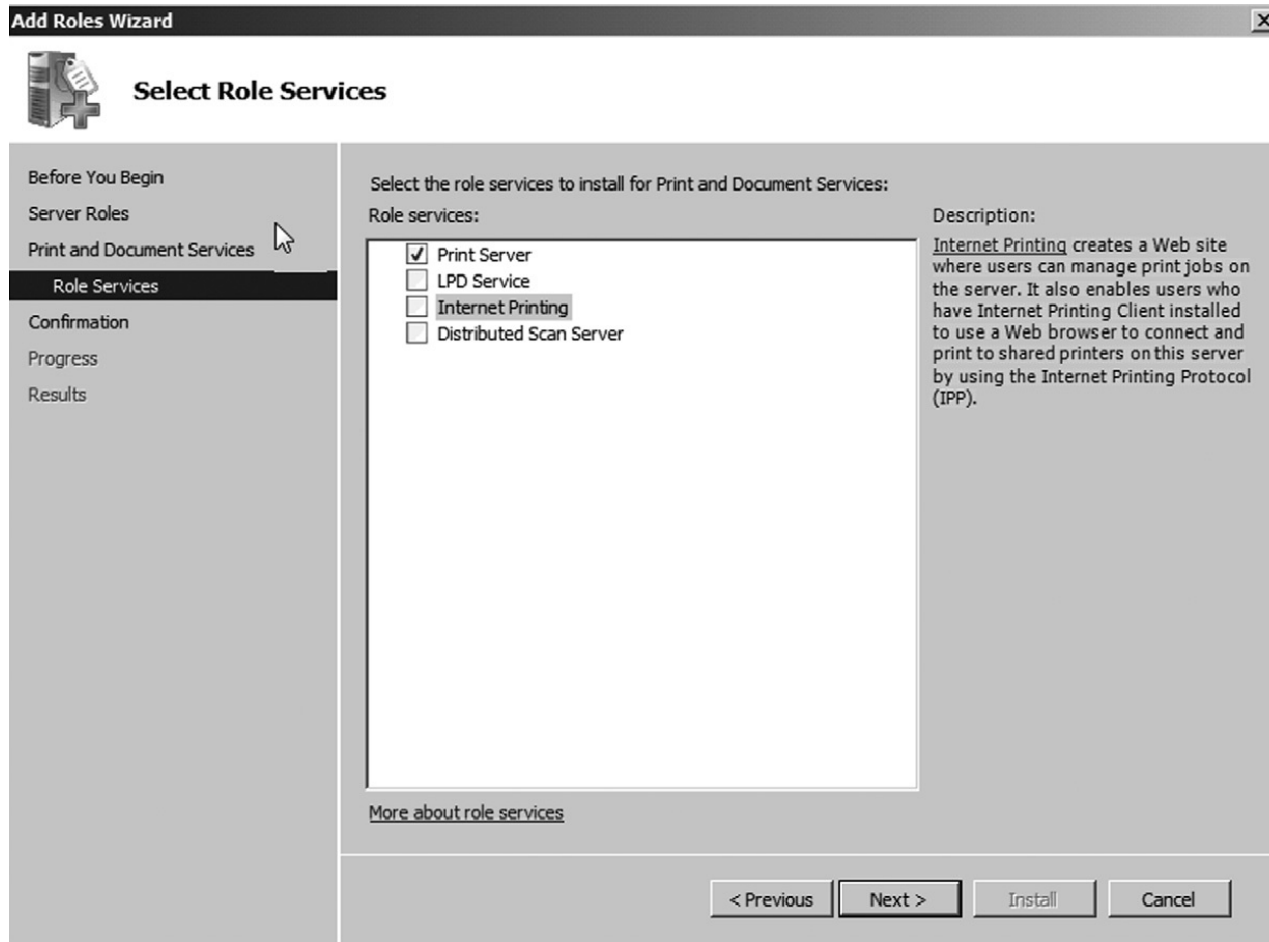
## Chia sẻ file



## Máy in

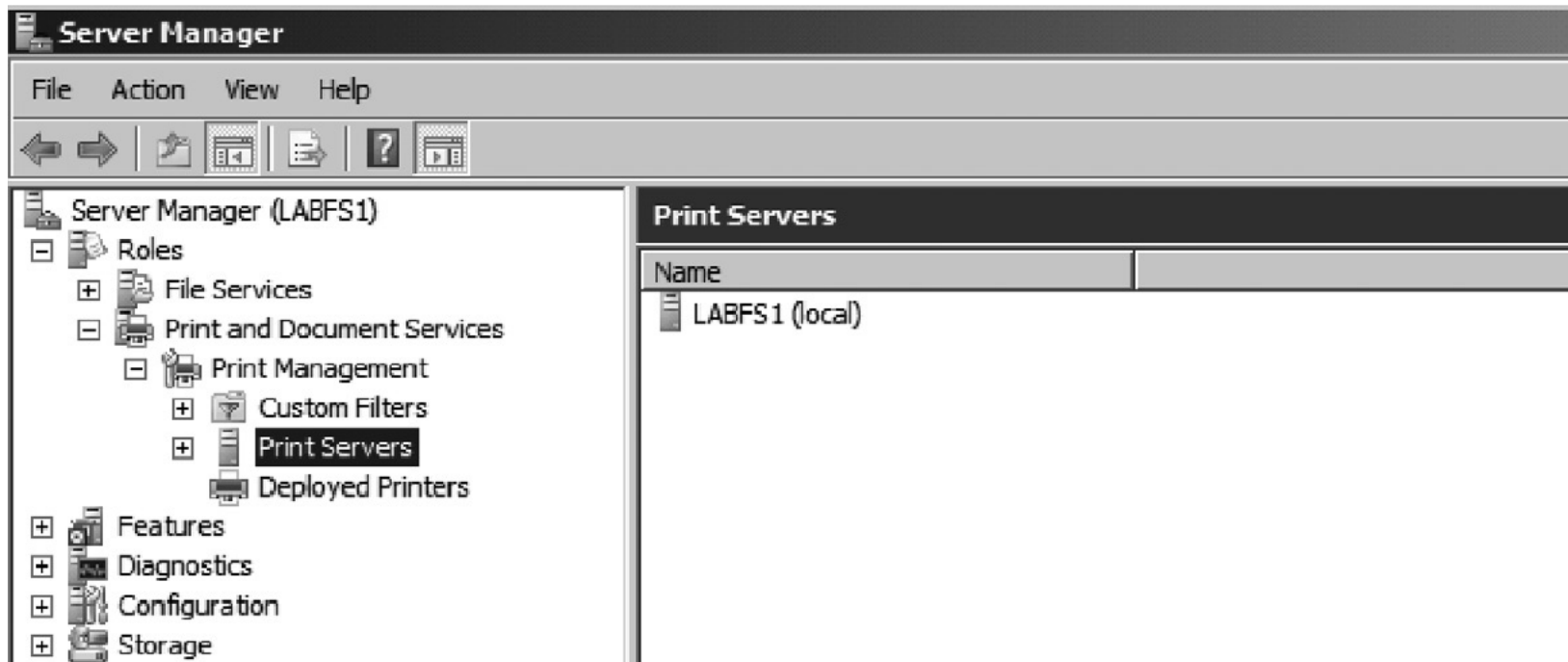
- ❖ Cho phép nhiều người dùng chia sẻ cùng 1 máy in
- ❖ Windows phân biệt
  - Thiết bị in (máy in vật lý): kết nối trực tiếp với máy chủ
  - Máy in (máy in lô-gíc): giao tiếp với máy in vật lý
  - Trình điều khiển máy in: giúp giao tiếp với máy in và che dấu thông tin chi tiết về máy in

## Dịch vụ In

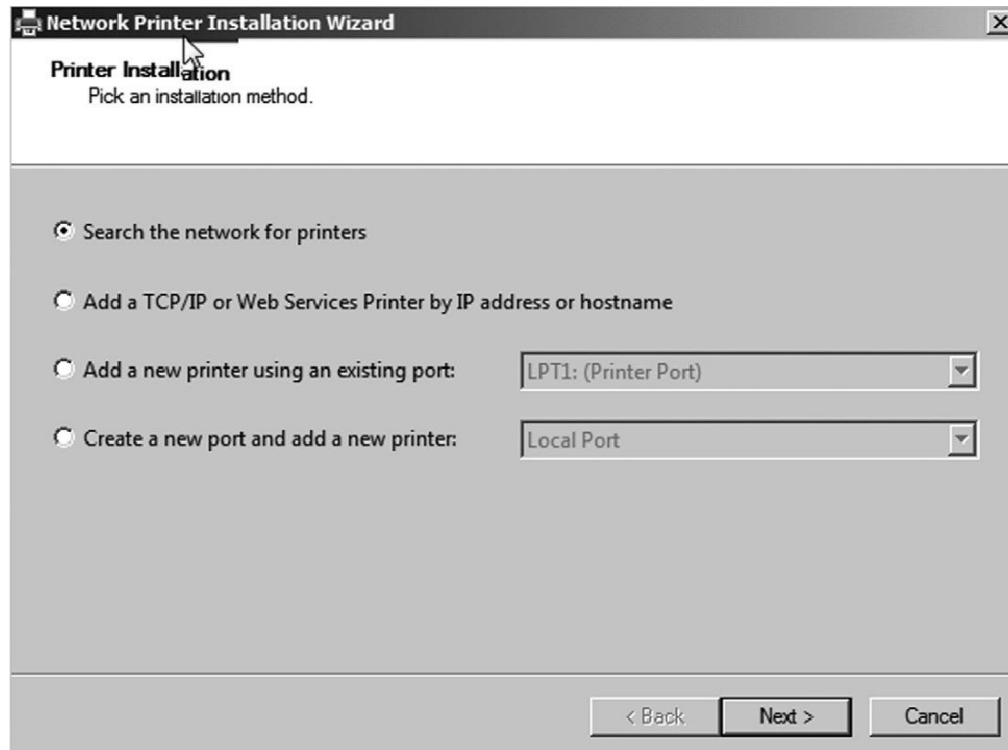


## Dịch vụ In

- ❖ Việc cài đặt thực hiện thông qua thêm chức năng máy chủ

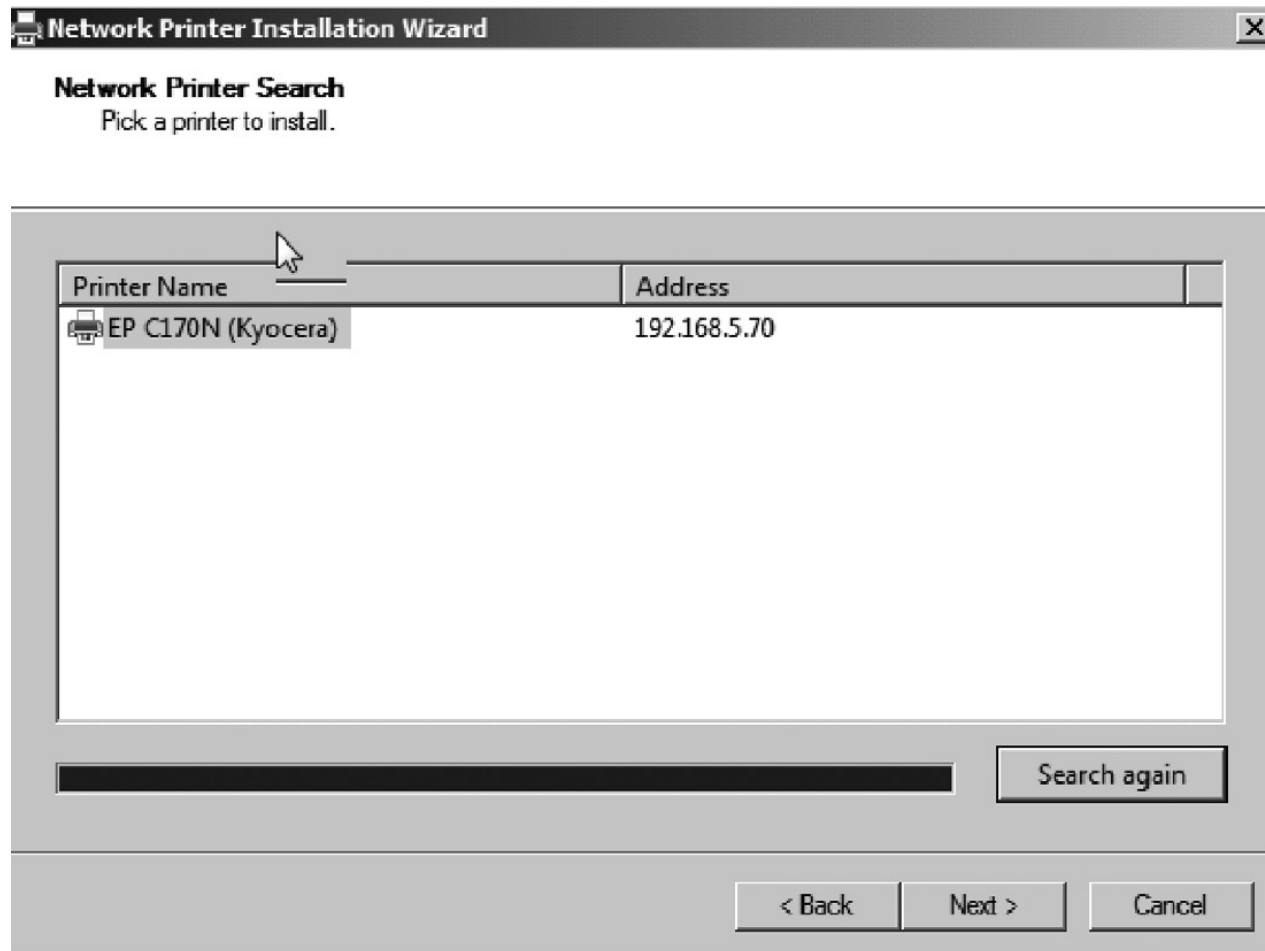


## Cài đặt máy in mạng



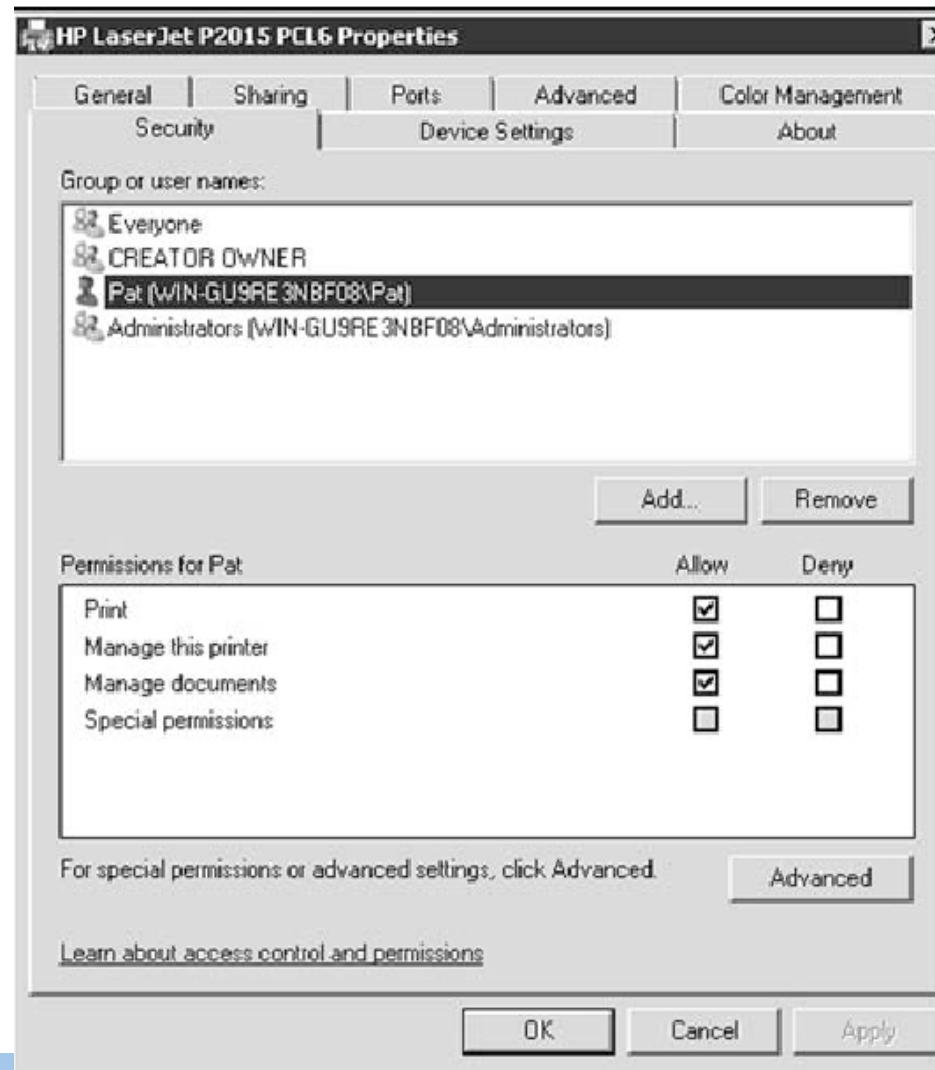


## Cài đặt máy in mạng



## Dịch vụ In

- ❖ Quyền in:
- ❖ Quyền quản lý máy in: Cho phép người dùng thay đổi cài đặt và cấu hình
- ❖ Quyền quản lý tài liệu in: Hủy, dừng, in lại hay khởi động lại máy in



## Microsoft Windows

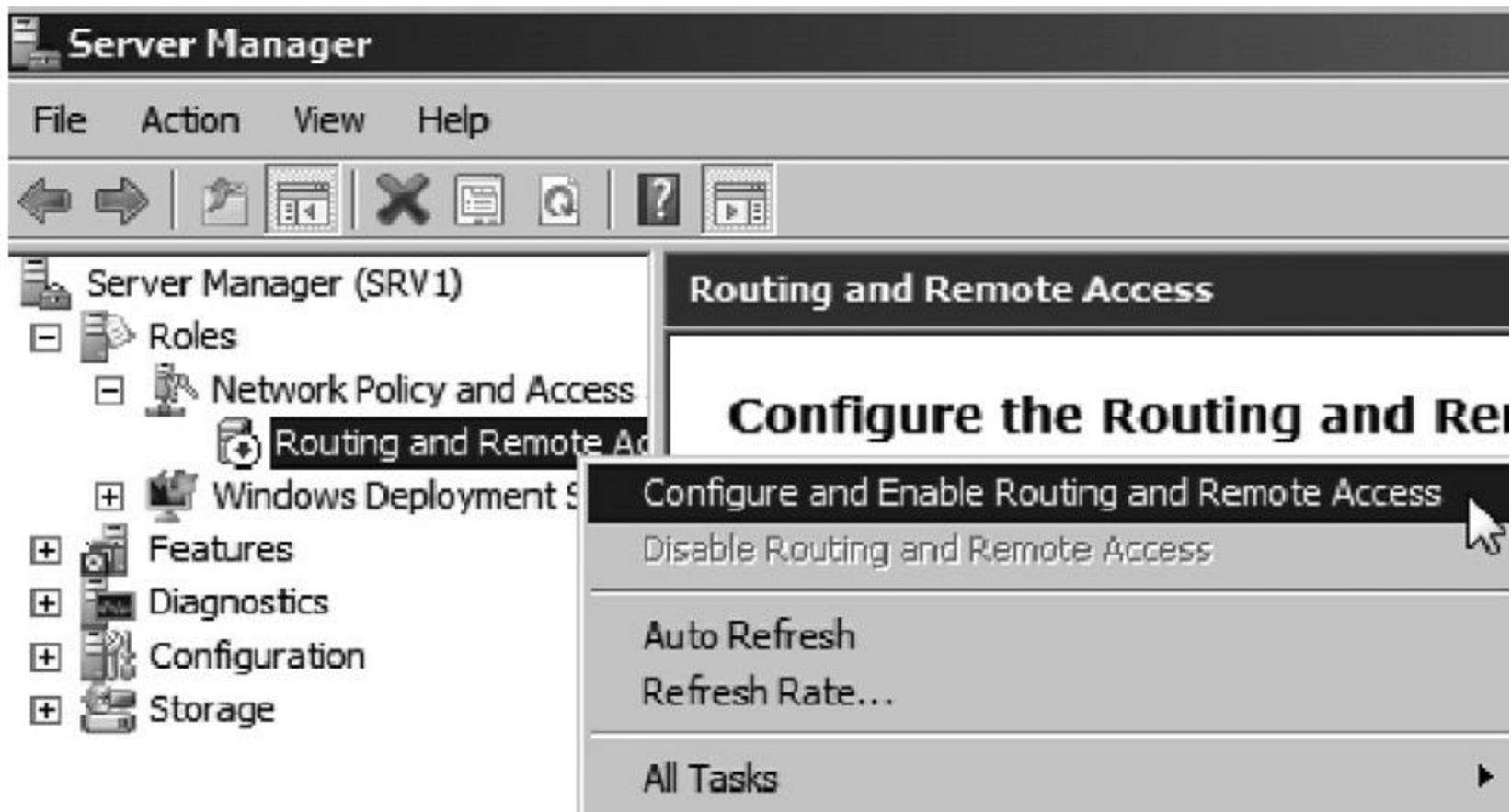
### ❖ Chương 3: Quản trị các máy chủ dịch vụ của Windows Server

- 3.1 Quản trị Active Directory
- 3.2 Quản trị máy chủ dịch vụ web
- 3.3 Quản trị máy chủ dịch vụ DNS và DHCP
- 3.4 Quản trị máy chủ dịch vụ file và in ấn
- 3.5 Quản trị máy chủ dịch vụ truy nhập từ xa

## Dịch vụ truy nhập từ xa

- ❖ Cho phép người dùng kết nối từ bên ngoài vào mạng để truy nhập dữ liệu và các ứng dụng như trong môi trường làm việc cục bộ thông thường.
- ❖ Các giao thức hỗ trợ:
  - **Point-to-Point Tunneling Protocol (PPTP):** Đơn giản khi triển khai song tính bảo mật yếu
  - **Layer 2 Tunneling Protocol (L2TP):** Dùng chuẩn IPSec.
  - **Secure Socket Tunneling Protocol (SSTP):** dùng https

## Dịch vụ truy nhập từ xa



## Dịch vụ truy nhập từ xa

