



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

KHOA AN TOÀN THÔNG TIN
TS. ĐINH TRƯỜNG DUY



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

Microsoft Windows

KHOA AN TOÀN THÔNG TIN

TS. ĐINH TRƯỜNG DUY

Biên soạn từ giáo trình: Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.



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

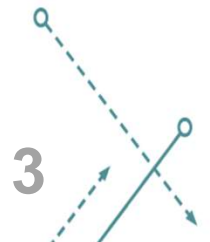
3.1 Quản trị Active Directory

3.2 Quản trị máy chủ dịch vụ web

3.3 Quản trị máy chủ dịch vụ DNS và DHCP

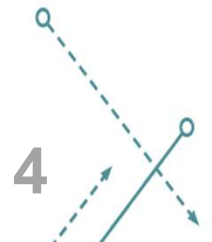
3.4 Quản trị máy chủ dịch vụ file và in ấn

3.5 Quản trị máy chủ dịch vụ truy nhập từ xa



Active Directory (1)

- 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: các dịch vụ (2)

- Thư mục động là công nghệ do Microsoft đưa ra cung cấp một số dịch vụ:
 - LDAP (Lightweight Directory Access Protocol),
 - Xác thực một lần dựa trên Kerberos,
 - Đặt tên dựa trên DNS,
 - Quản trị mạng tập trung.

Active Directory: các dịch vụ (3)

- **Giao thức truy nhập thư mục đơn giản - 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.
 - Thư mục LDAP được tổ chức theo một kiến trúc cây đơn giản gồm:
 - Thư mục gốc,
 - Country,
 - Organizations,
 - Organizational units,
 - Individuals.

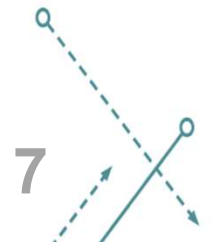
Active Directory: các dịch vụ (3)

- **Kerberos**

- Giao thức xác thực mạng máy tính cho phép các máy xác định danh của mình qua mạng không an toàn một cách đảm bảo.
- Các thành phần trung tâm phân phối khóa (Key Distribution Centre – KDC):
 - Máy chủ xác thực (Authentication Server – AS);
 - Máy chủ cấp vé ((Ticket Granting Server – TGS);
 - Cơ sở dữ liệu (Database)

- **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: về tổ chức (4)

- **Đơn vị tổ chức – Organisation Units:**

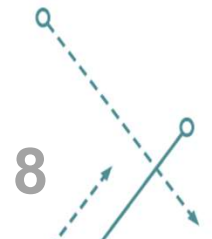
- Là các đối tượng bên trong một miền cho phép bố trí và nhóm các tài nguyên lại để làm thuận tiện cho công việc quản trị và cho phép ủy thác các quyền quản trị.

- **Miền – Domain:**

- là đơn vị logic các máy tính và tài nguyên mạng xác định ranh giới an ninh.
- Sử dụng một cơ sở dữ 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.

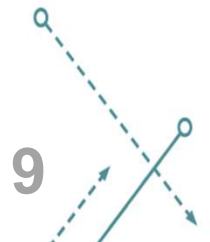
- **Cây – Tree:**

- Chứa một hay nhiều miền dùng chung không gian định danh.
- Ví dụ: fit.ptit.edu.vn



Active Directory: về tổ chức (5)

- **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.
- **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.



Global Catalog (1)

- 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.

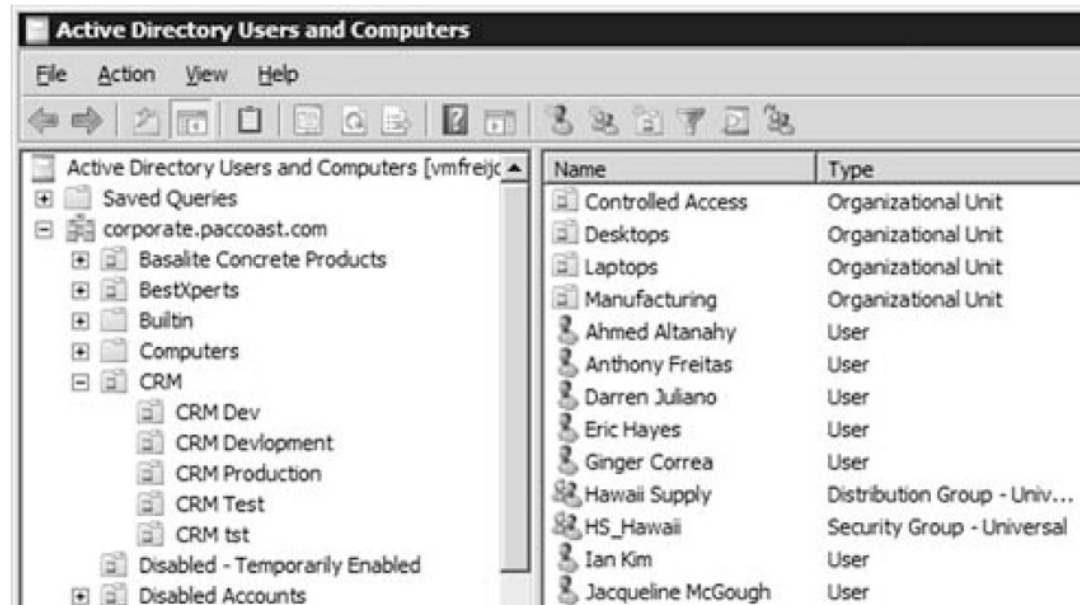


Global catalog

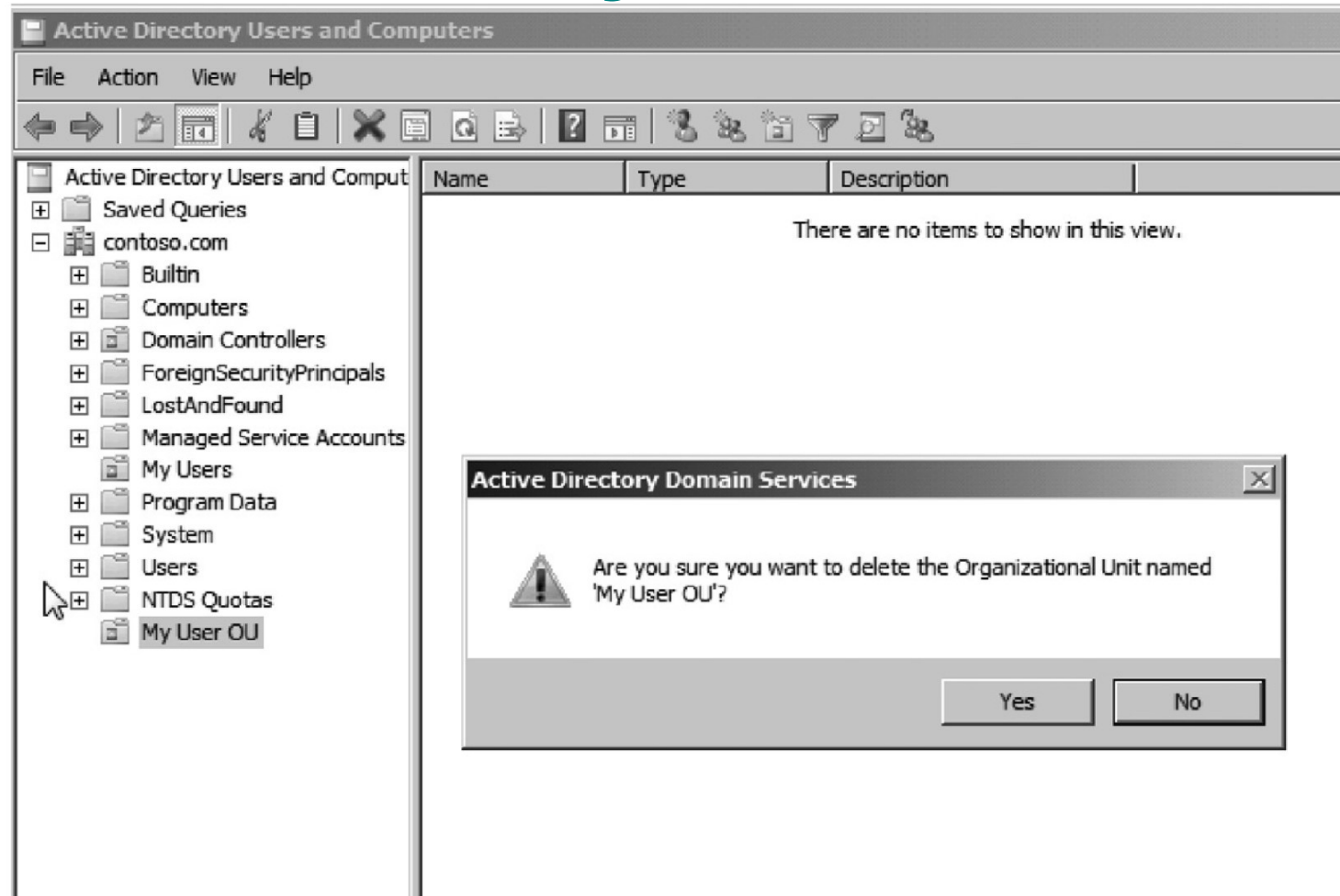


Organizational Units

- 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.



Active Directory



Đối tượng

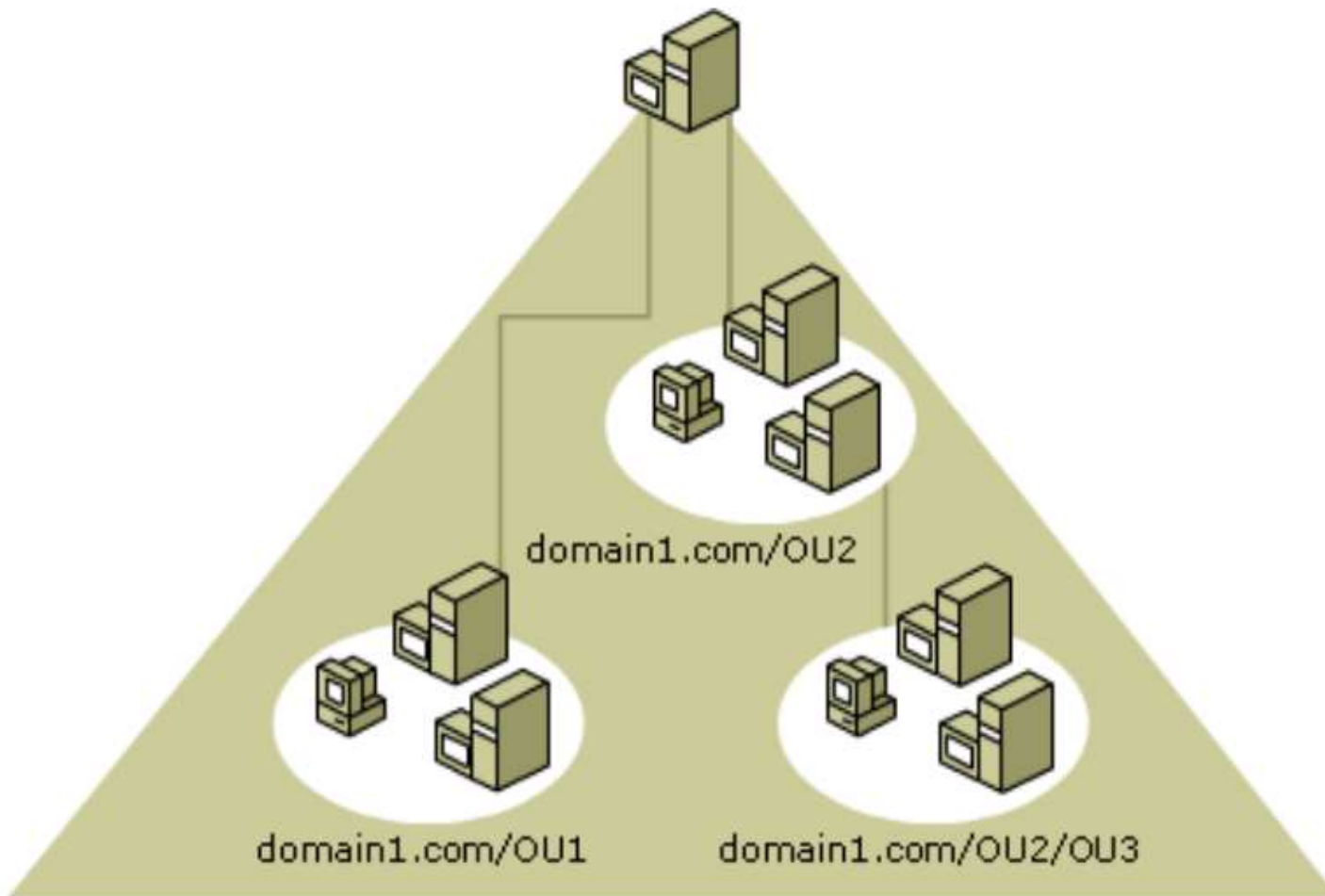
- **Đối tượng – Object**

- 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 GUID (*Globally unique identifier*) hay định danh an ninh (*Security identifier*).

- **Lược đồ – 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.

Đơn vị tổ chức của thư mục động

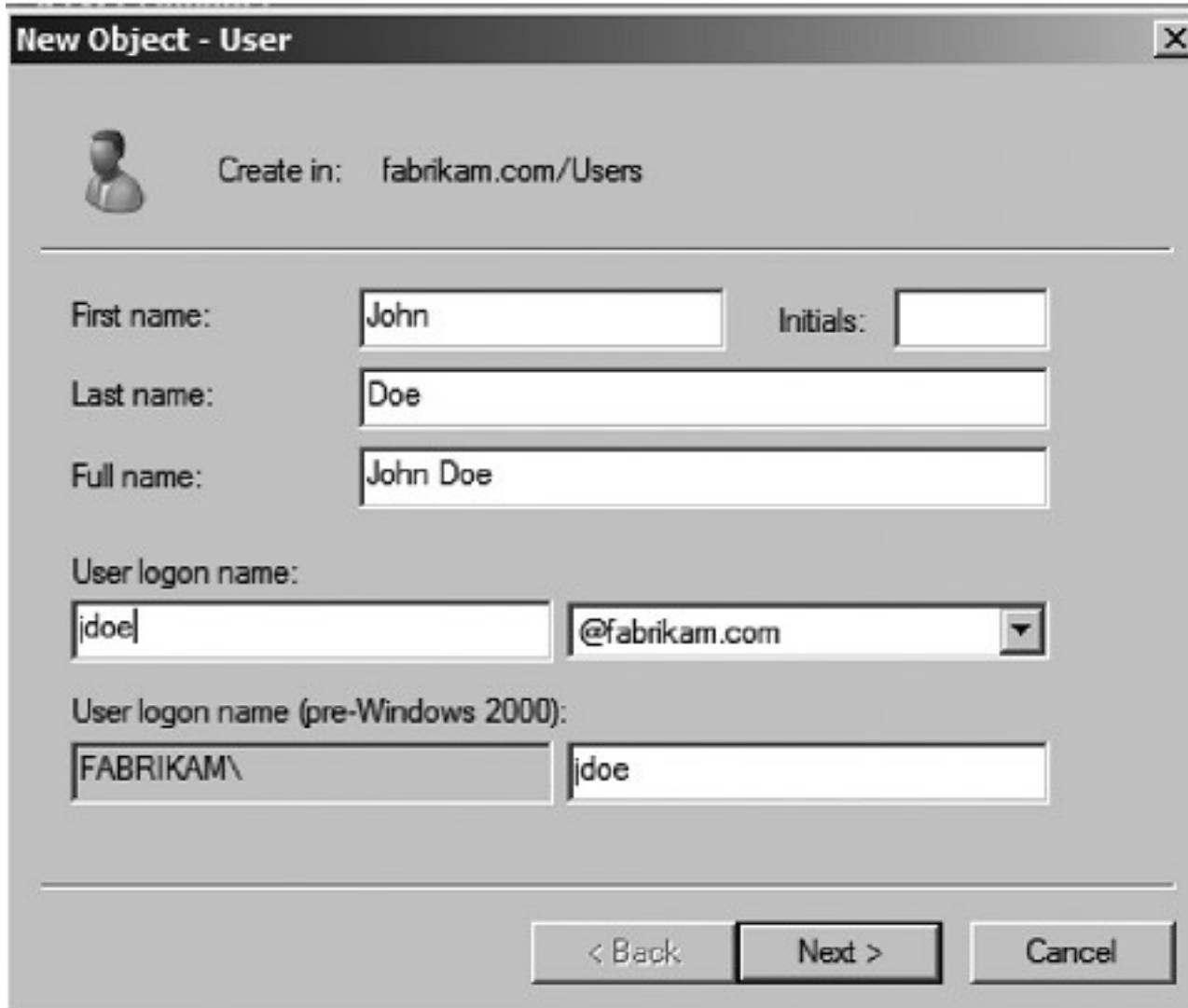


Người dùng (1)

- 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.



Người dùng (2)



New Object - User

Create in: fabrikam.com/Users

First name: John Initials:

Last name: Doe

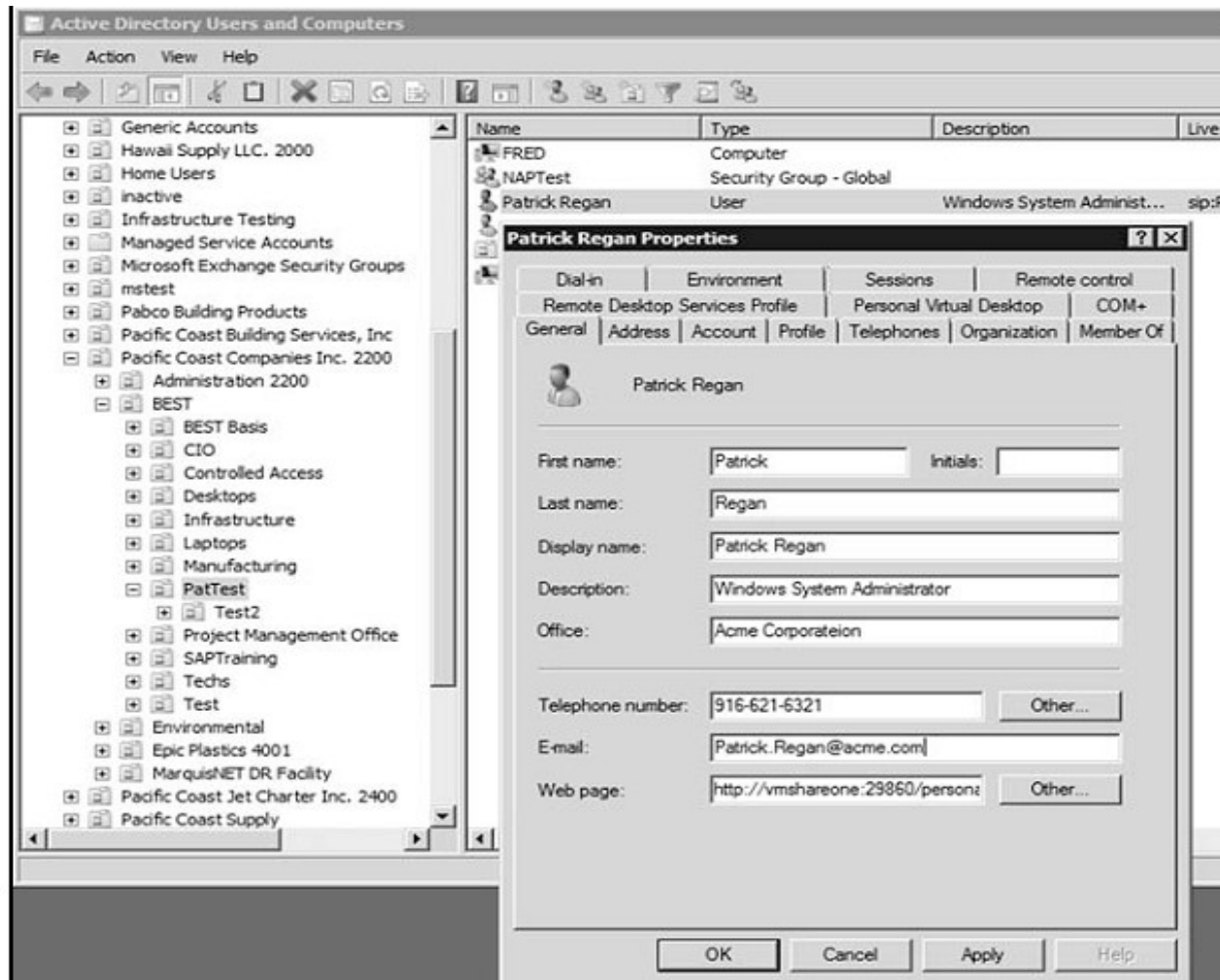
Full name: John Doe

User login name: jdoe @fabrikam.com

User login name (pre-Windows 2000): FABRIKAM\ jdoe

< Back Next > Cancel

Người dùng (3)

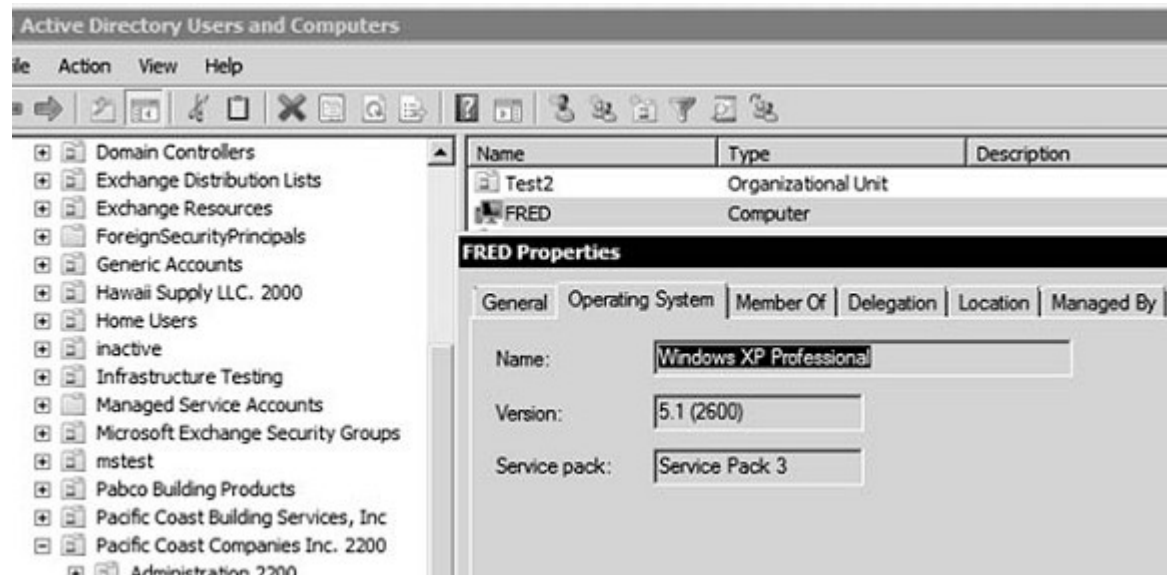


User profile

- 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:
 - **Hồ sơ người dùng cục bộ – Local user profile:**
 - Lưu trong ổ cứng cục bộ mà người dùng đăng nhập.
 - **Hồ sơ người dùng di chuyển – 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.
 - **Hồ sơ người dùng bắt buộc – Mandatory user profile:**
 - Được dùng như profile người dùng chuyển vùng như các thay đổi của người dùng không được lưu lại.

Máy tính

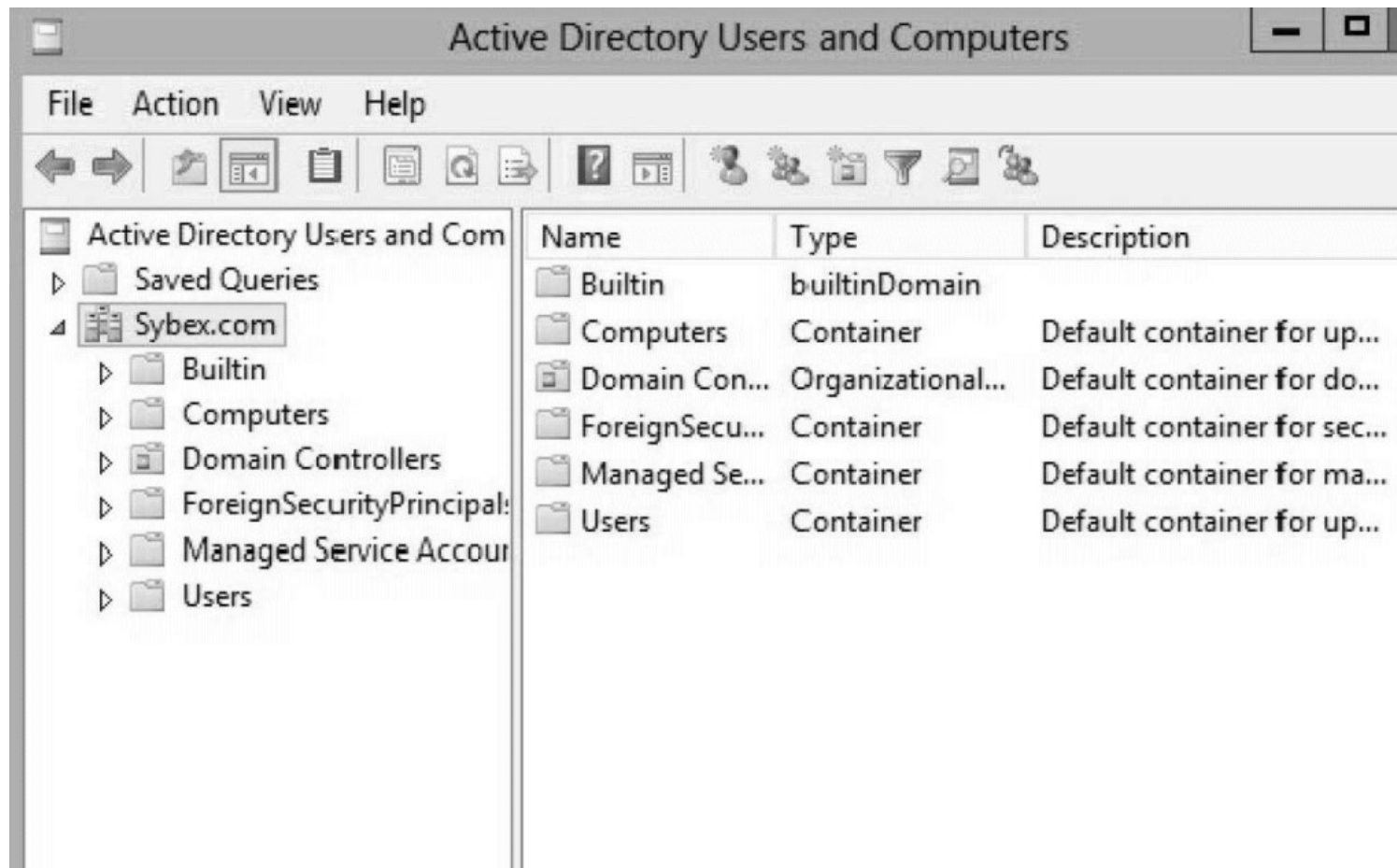
- Tài khoản ứng với máy tính:
 - Cung cấp công cụ để theo dõi và giám sát việc truy nhập của máy tính vào mạng và tài nguyên của miền.
 - Mỗi máy tính có 1 tài khoản duy nhất.



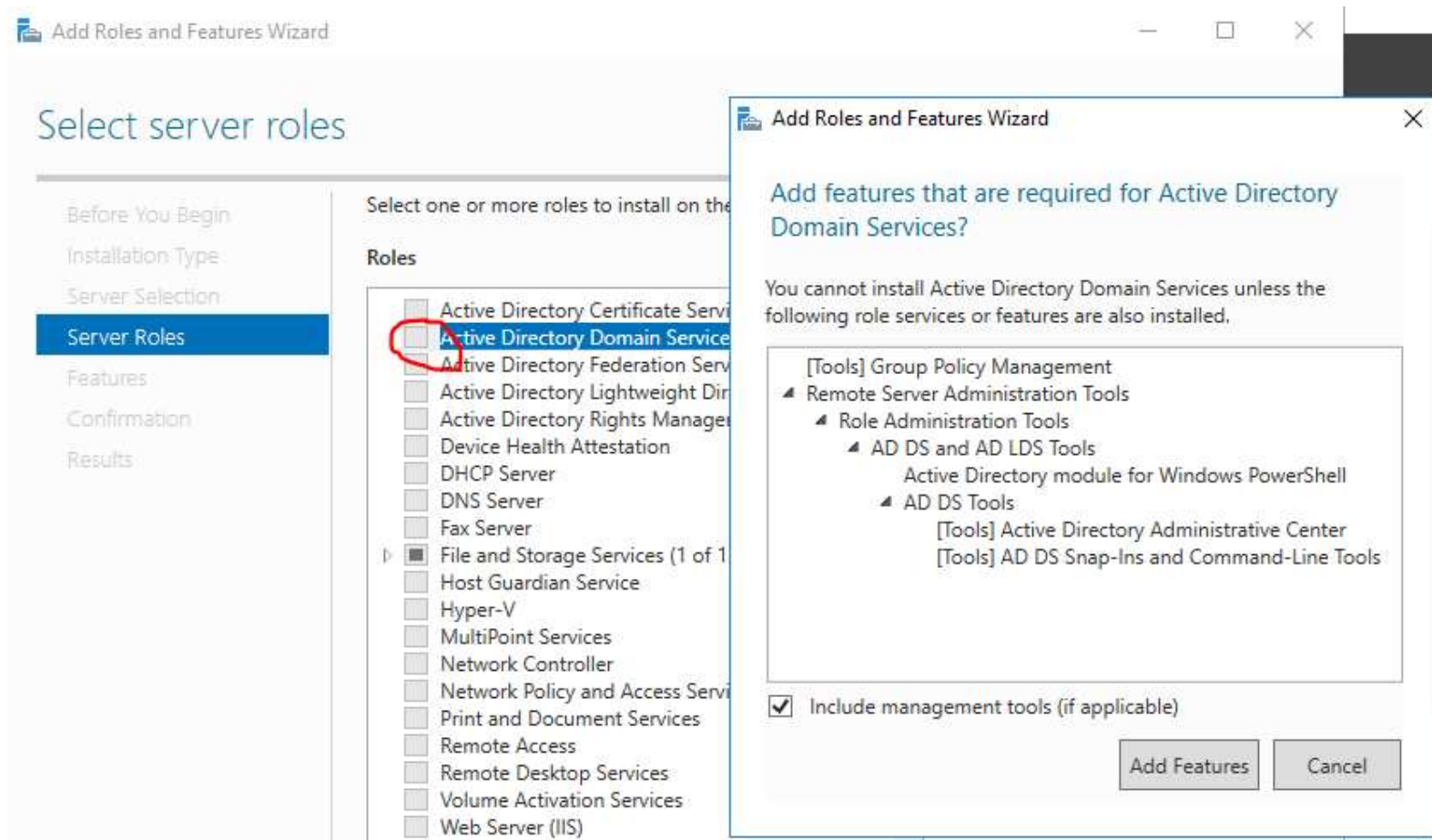
Công cụ quản lý Active Directory

- **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.

Giao diện quản trị người dùng thư mục động



Cài đặt dịch vụ thư mục động



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



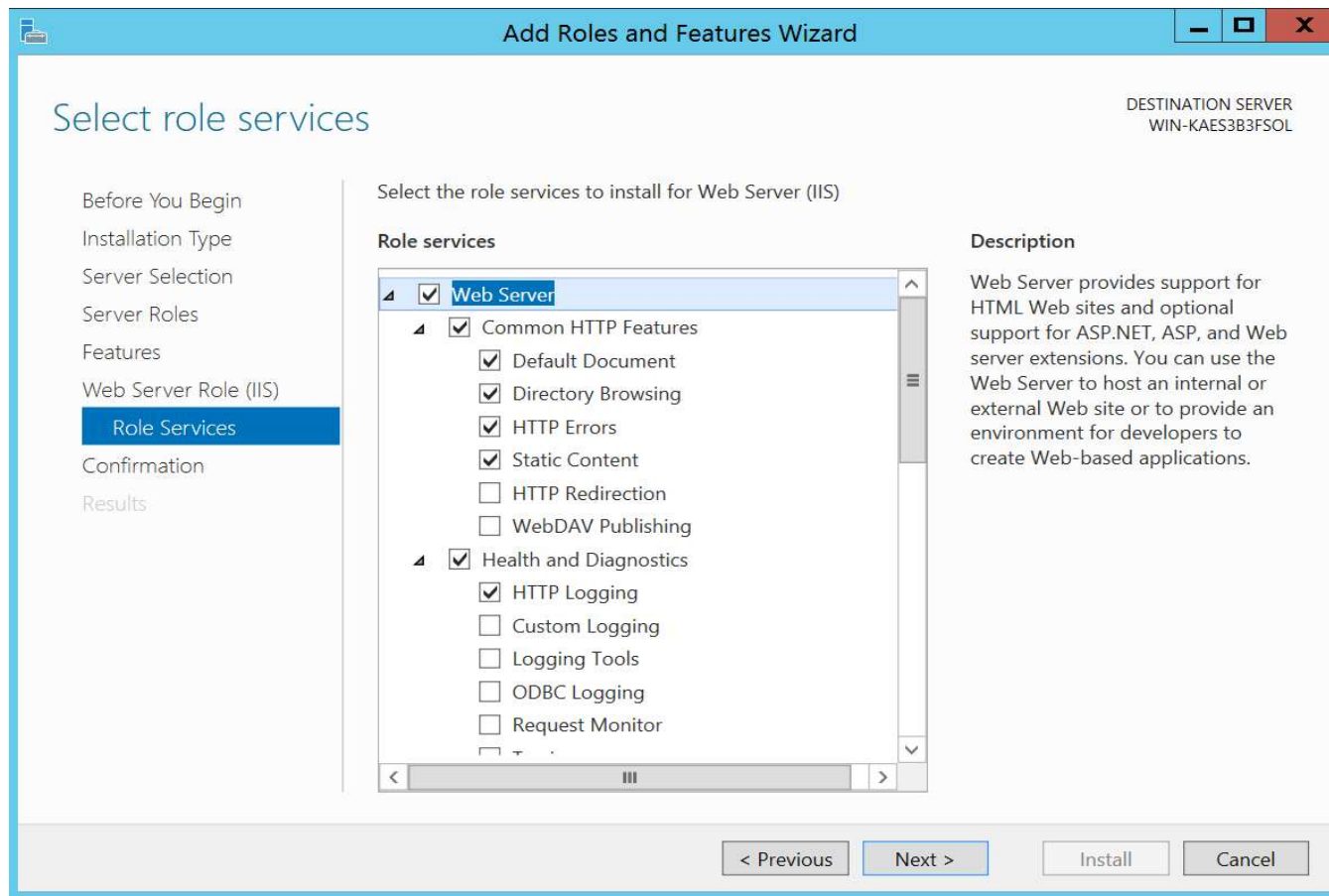
WEB-IIS (1)

- 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.

WEB-IIS (2)

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

Cài đặt dịch vụ Web

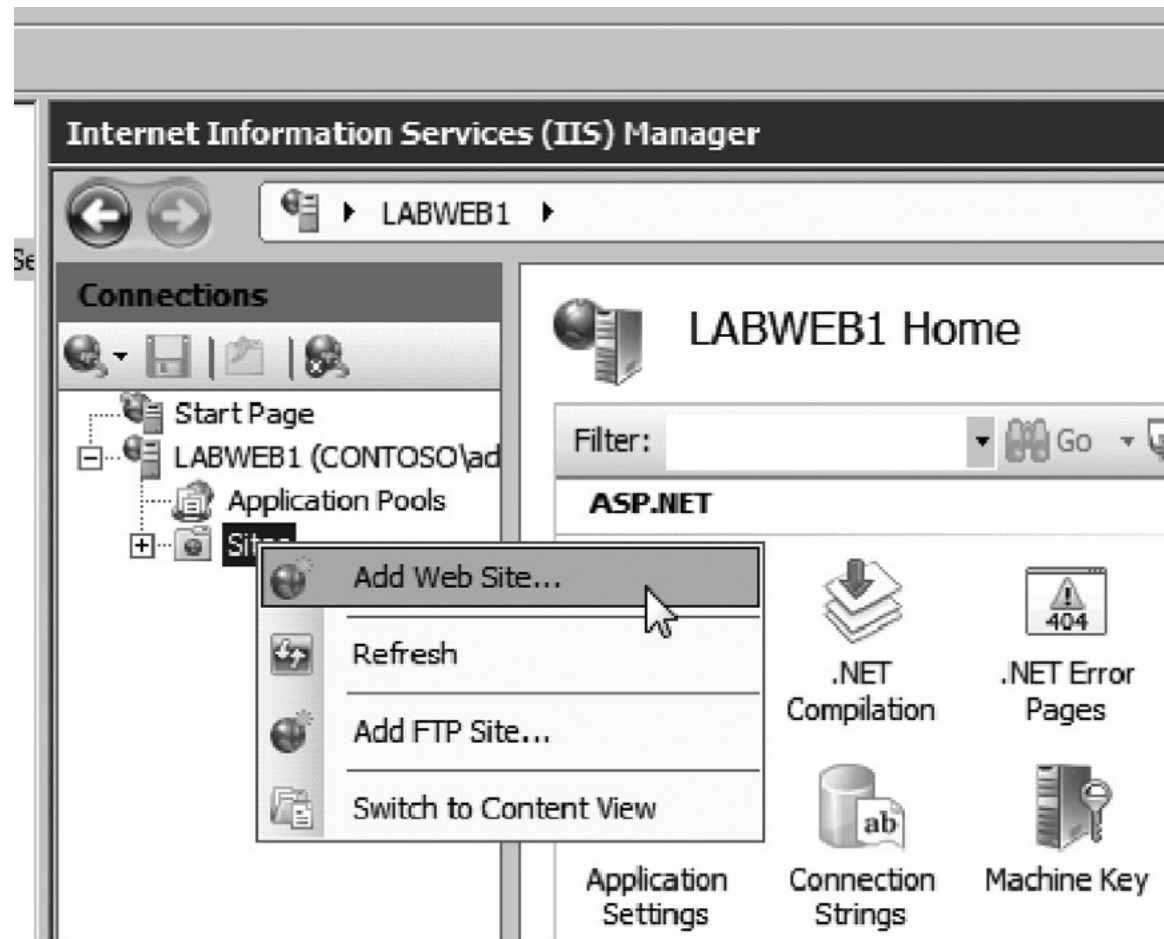


Tạo web site (1)

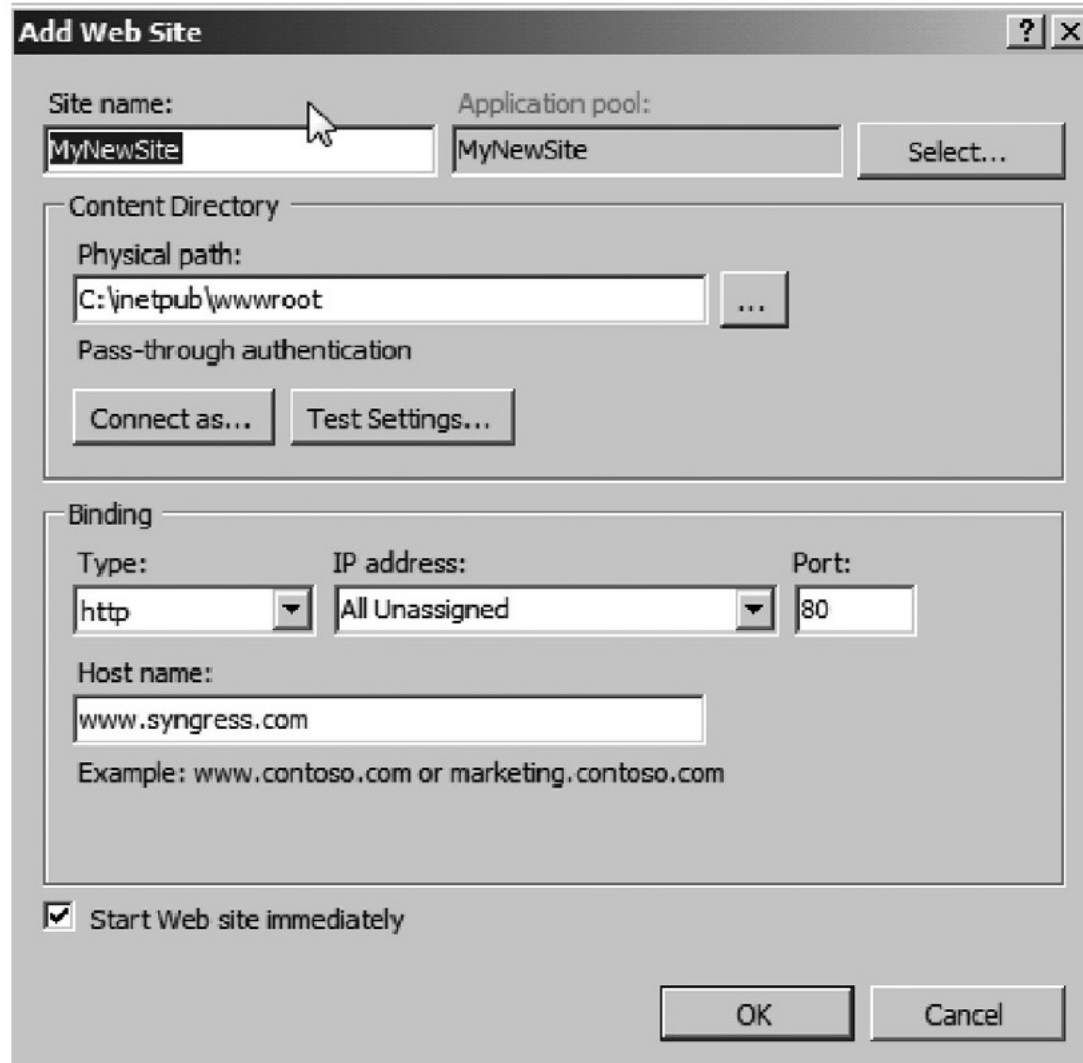
- Sử dụng công cụ IIS (Internet Information Services).
- Trong cửa sổ Connections:
 - Chọn vị trí trong cây site.
 - Đặt đường dẫn vật lý lưu trữ các file.
 - Đặt mật khẩu (nếu cần thiết) xác định người dùng.
 - Xác định địa chỉ IP trang web.



Tạo web site (2)



Tạo Web site (3)



Add Web Site

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

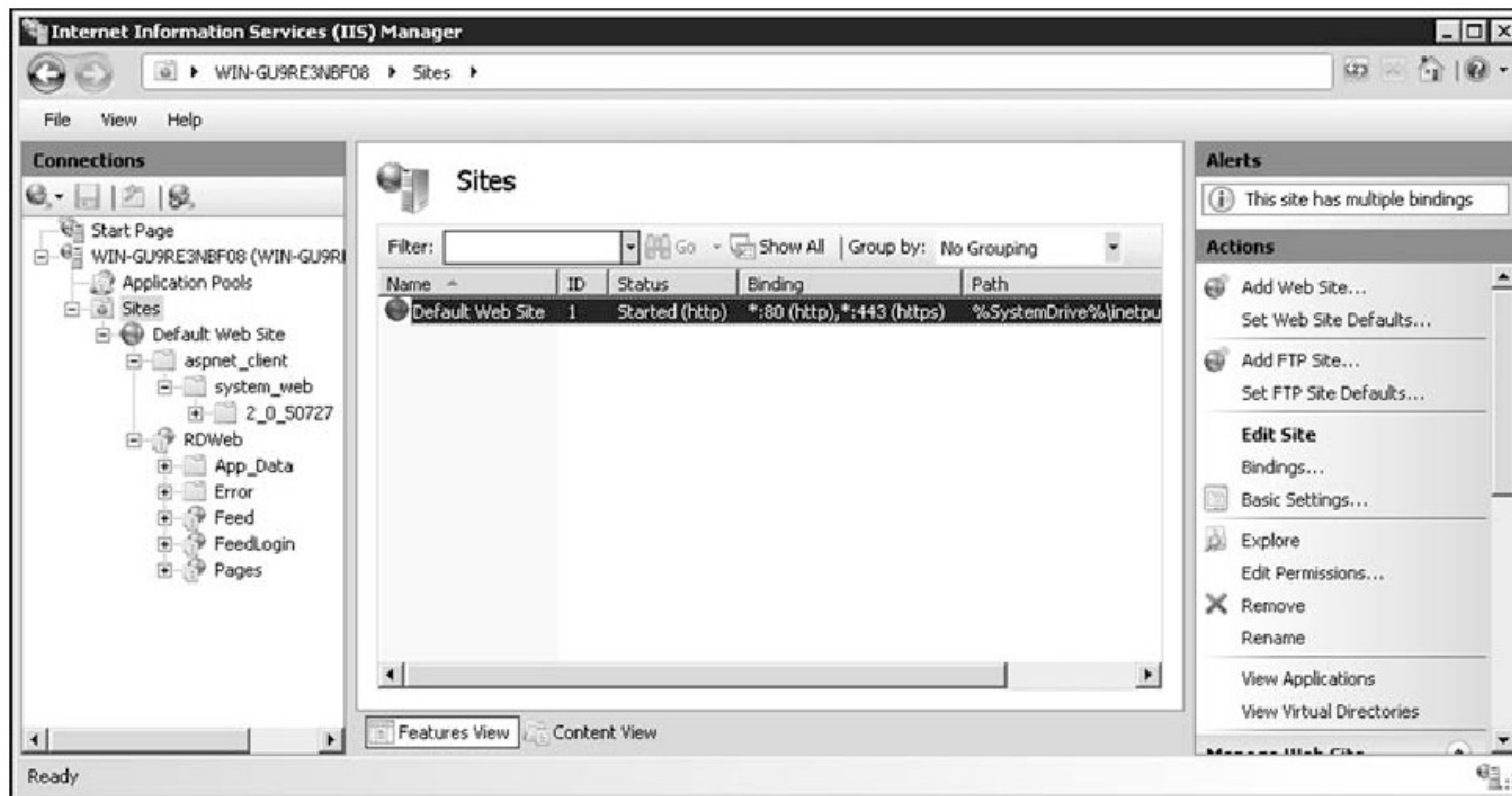
Host name:

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

☒ Start Web site immediately

WEB-IIS (3)

- Thêm chức năng Web server



Cách thức xác thực vào trang Web

- Nặc danh (Anonymous): cho phép bất cứ người dùng nào cũng được truy nhập mà không cần xác thực.
- Xác thực cơ bản (Basic Authentication): yêu cầu người dùng cung cấp tên và mật khẩu hợp lệ. Tuy nhiên cách này không mã hóa thông tin nên chứa đựng rủi ro an toàn.
- Xác thực số (Digest Authentication): dùng máy chủ miền xác thực.
- Xác thực Windows (Windows Authentication): sử dụng giao thức NTLM hay Kerberos để xác thực.

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



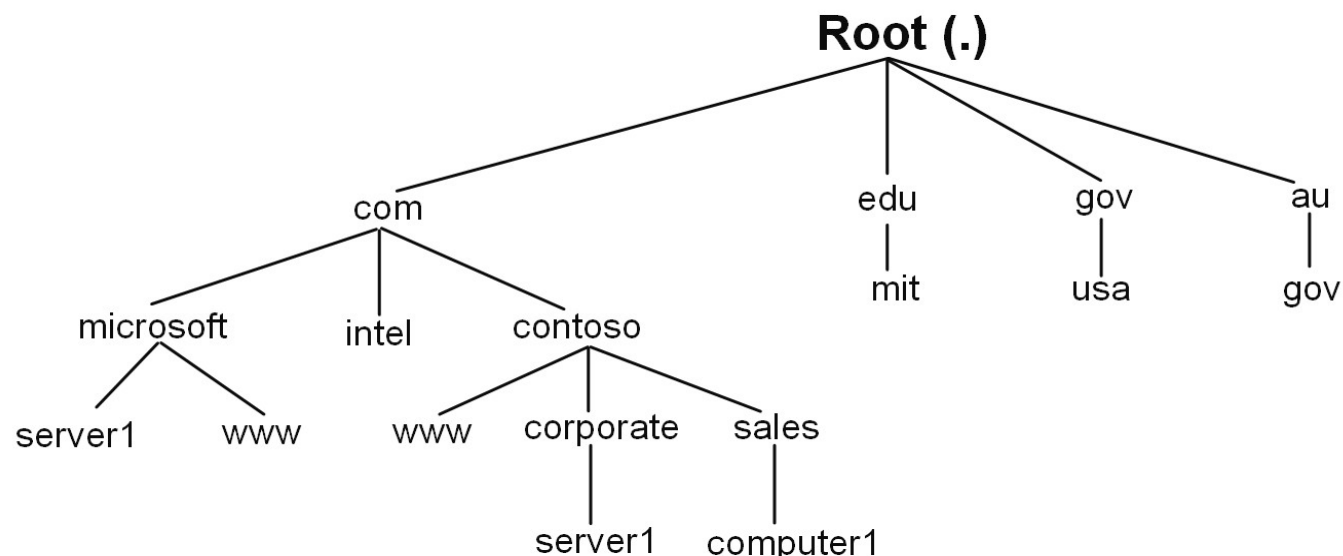
DNS (1)

- **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 mạng Internet.
- **Ưu điểm của DNS**
 - ✓ Dễ sử dụng và đơn giản.
 - ✓ Có khả năng mở rộng.
 - ✓ Có tính nhất quán.

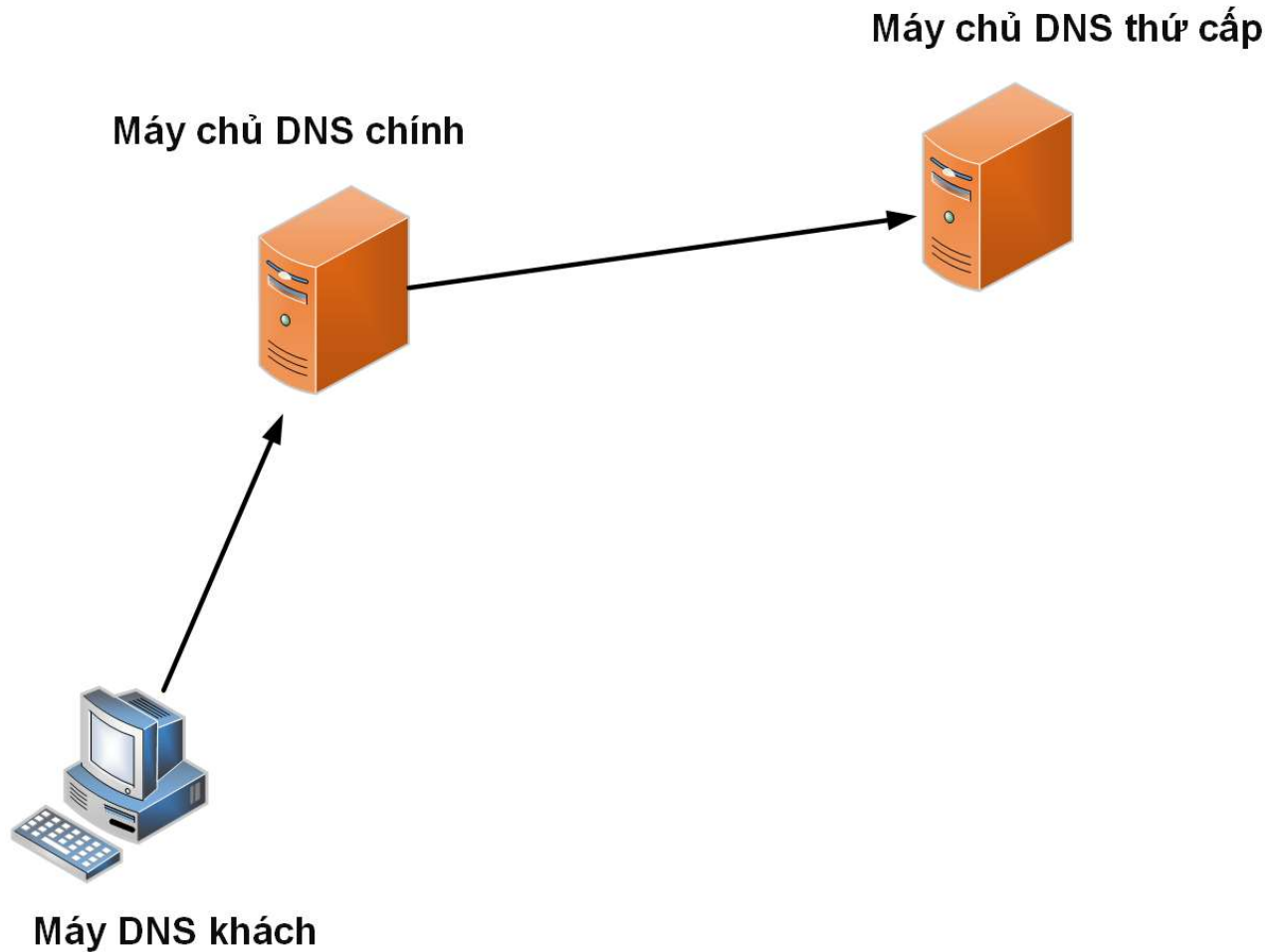


DNS (2)

- Miền gốc nằm trên đỉnh của cây tên miền
 - Top-level domain: .com, .edu, .vn
 - Second-level domain: contoso.com
 - Subdomain: sales.contoso.com
- Tên máy chủ (hostname) được gán cho một máy tính cụ thể trong miền để xác định trạm TCP/IP



Cách phân rã địa chỉ DNS



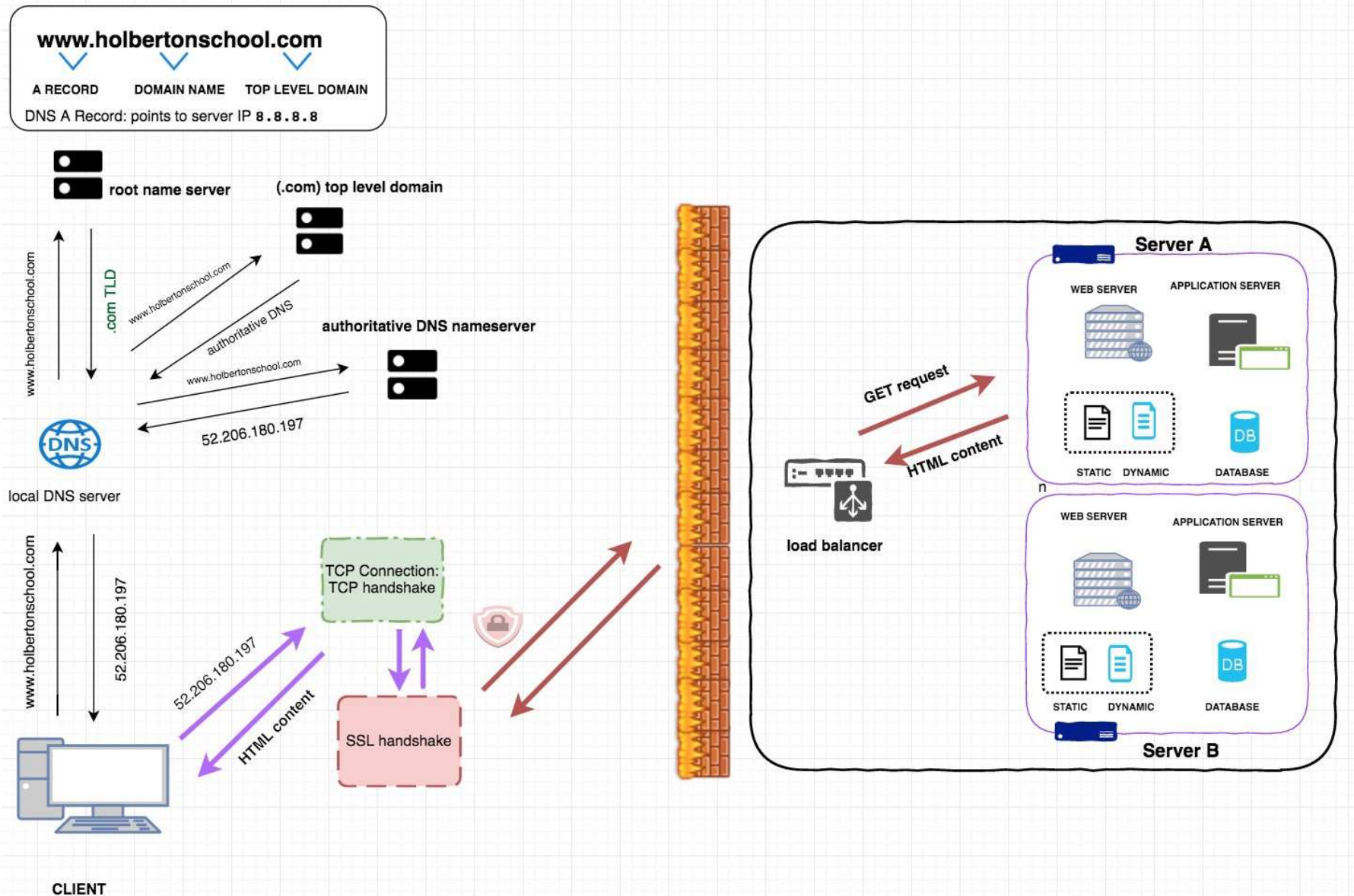


Protocol Domain(name)

https://www.holbertonschool.com

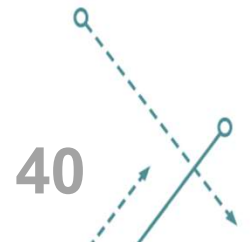
Subdomain Top Level Domain





DNS Zone (vùng DNS)

- 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.
- Máy chủ DNS có thể quản lý:
 - Miền chính (primary zone): cho phép cập nhật các bản ghi về tên miền.
 - Miền phụ (secondary zone): chỉ lưu bản sao của miền chính, không cho phép sửa đổi các bản ghi.
- 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 (1)

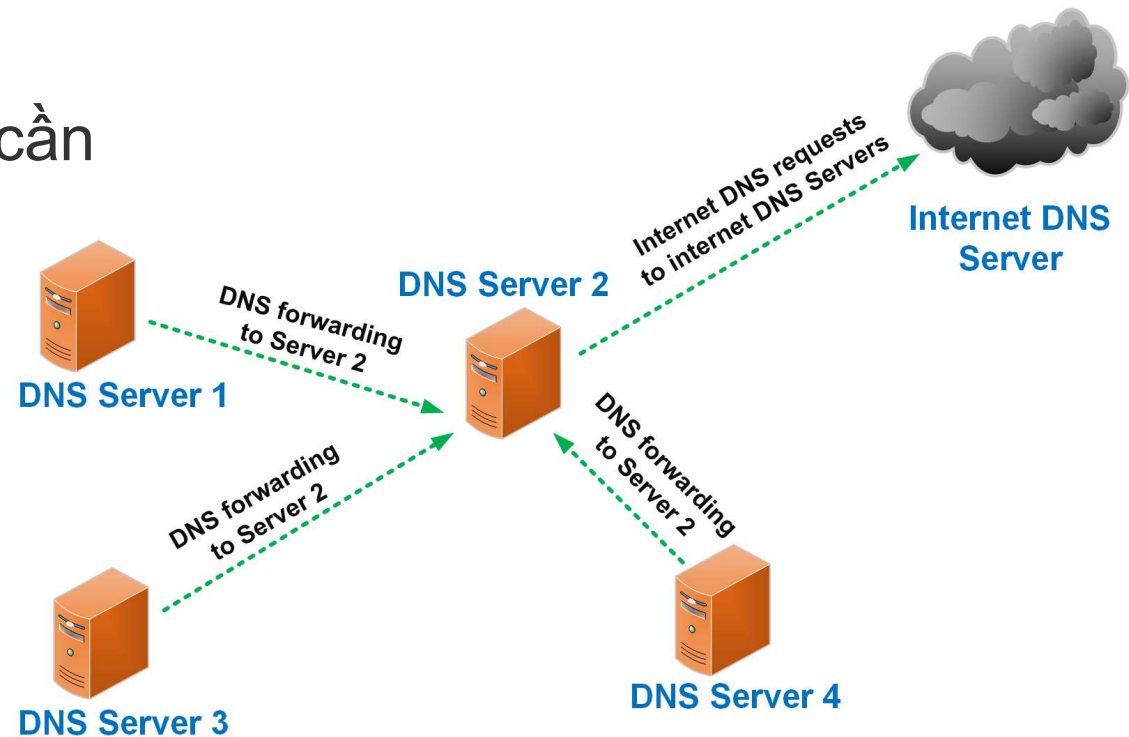
- **Bản ghi khởi đầu SOA** (Start of Authority): xác định tham số chung cho vùng DNS
 - Vd: *@IN SOA win2k3r3.example.com.
Hostmaster.example.com.(....)*
- **Bản ghi máy chủ**: Thông tin căn bản ánh xạ tên của một máy chủ ra địa chỉ IP.
 - Vd: *SMTP IN A 192.168.3.144*
- **Bản ghi CNAME**: Ánh xạ máy chủ tới một tên có sẵn
 - Vd: *www IN CNAME chaos.example.com*
- **Bản ghi NS**: Lưu định danh các máy chủ DNS trong miền
 - Vd: *example.com. IN NS Hostname.example.com*

Bản ghi DNS (1)

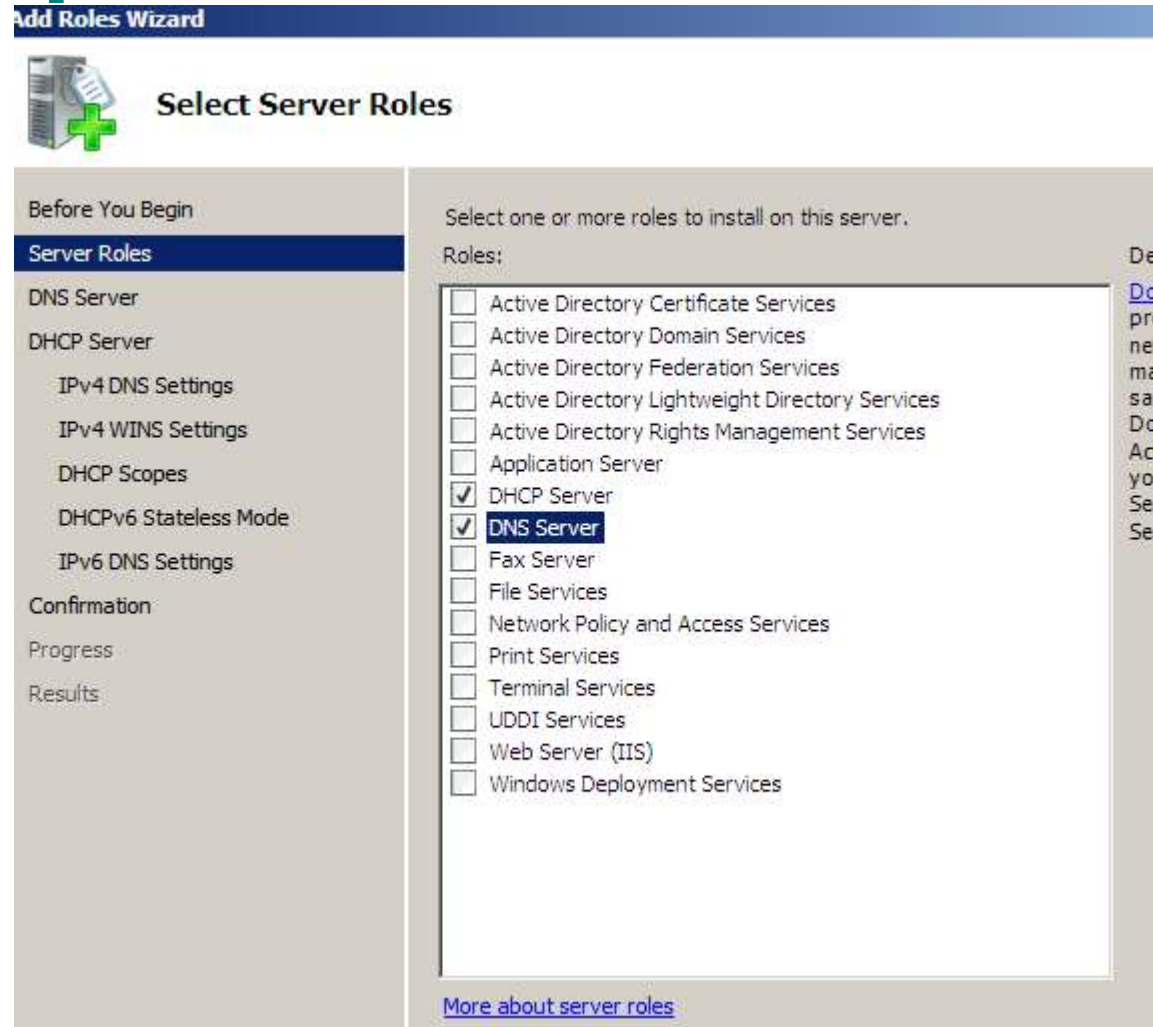
- **Bản ghi dịch vụ SRV:** Hỗ trợ việc tự động phát hiện các tài nguyên TCP/IP có trên mạng
 - Vd:
ldap.tcp.example.com. 86400 In SRV 10 100 389 hsv.example.com
- **Bản ghi con trỏ PTR:** Là các bản ghi tìm kiếm ngược
 - Vd: *10.1.168.192.in-addr.arpa. IN PTR www.example.com*
- **Bản ghi máy chủ thư:** chỉ định máy chủ nhận thư của miền
 - Vd: *example.com IN MX 10 mail.example.com*

Xác định hạ tầng DNS

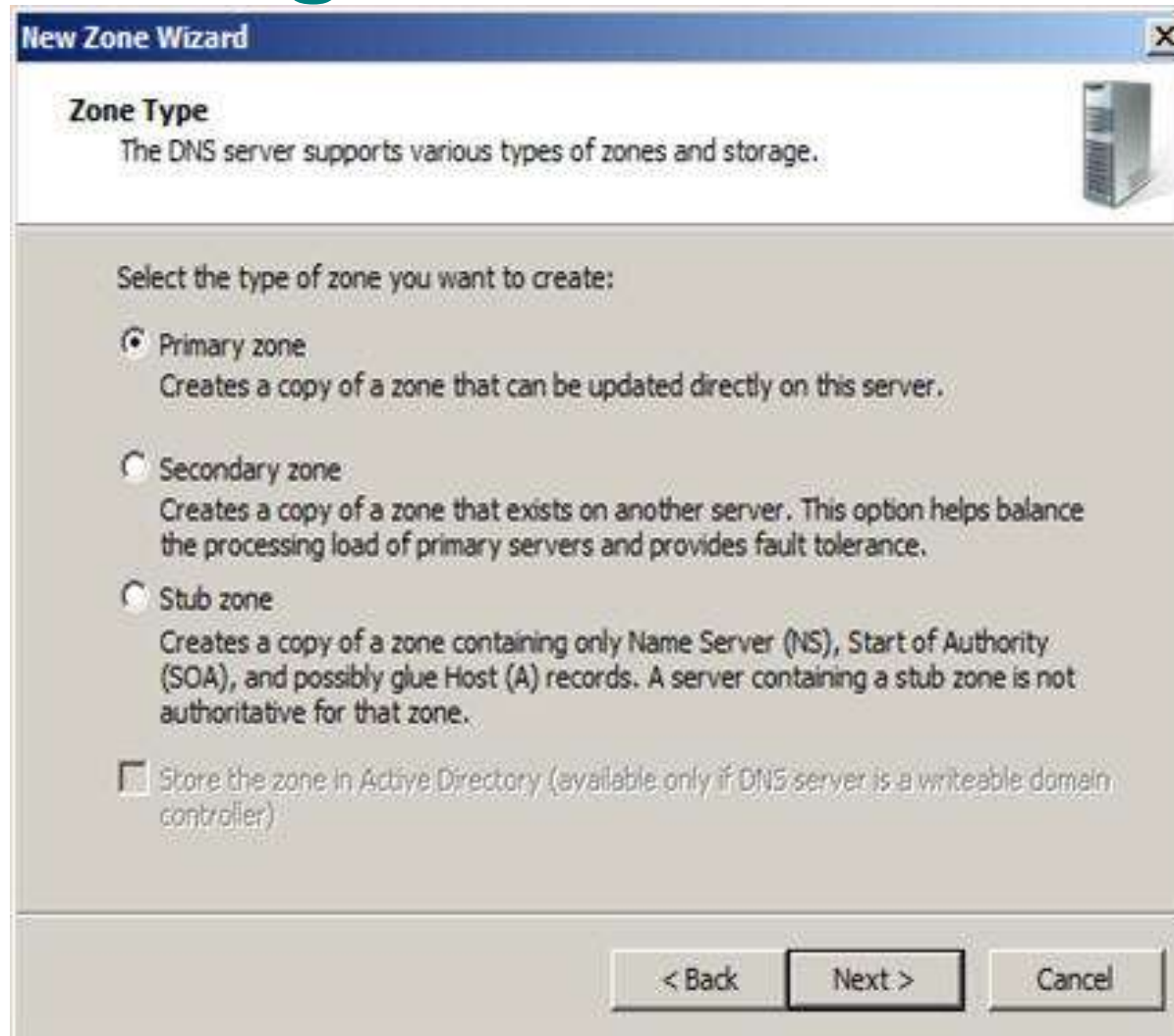
- Cần xem xét một số vấn đề sau:
 - Số các mạng vật lý cần dịch vụ DNS.
 - Bảng thông WAN.
 - Số miền hay vùng.
 - Các dạng bản ghi.
 - Số lượng bản ghi.



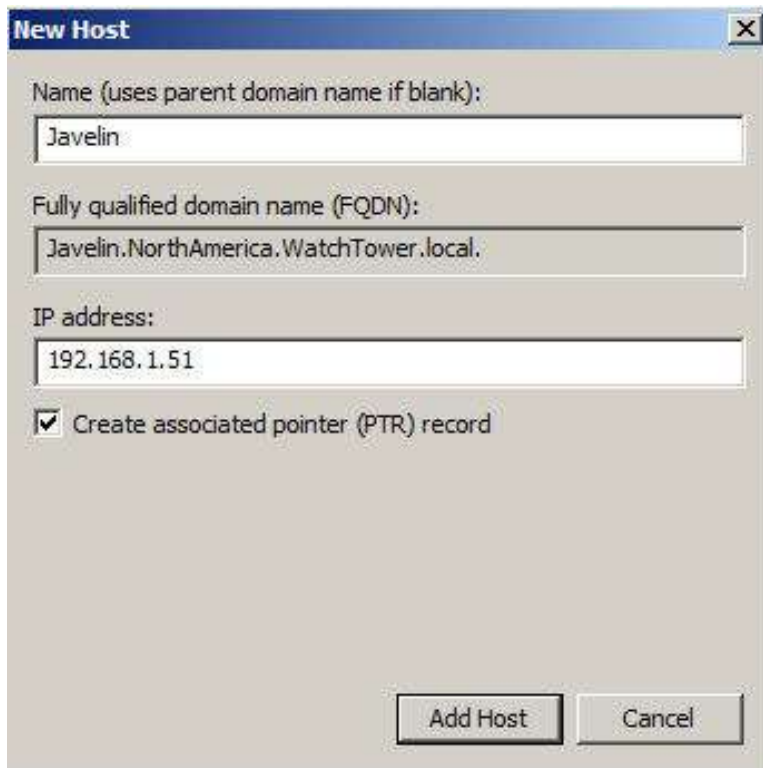
Cài đặt DNS



Tạo vùng DNS



Bản ghi DNS



New Host

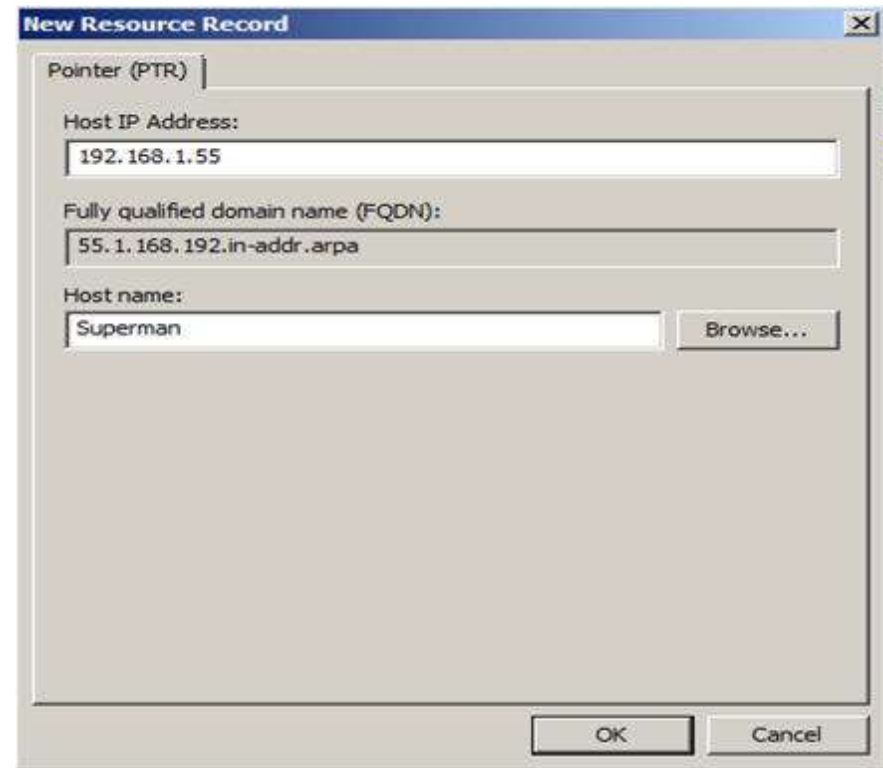
Name (uses parent domain name if blank):
Javelin

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

Cài đặt DNS

- Khi cài đặt và cấu hình máy chủ DNS, cần xem xét một số vấn đề sau:
 - Số các mạng vật lý cần dịch vụ DNS
 - Số lượng máy chủ DNS
 - Bảng thông WAN
 - Số miền hay vùng
 - Các dạng và số lượng bản ghi



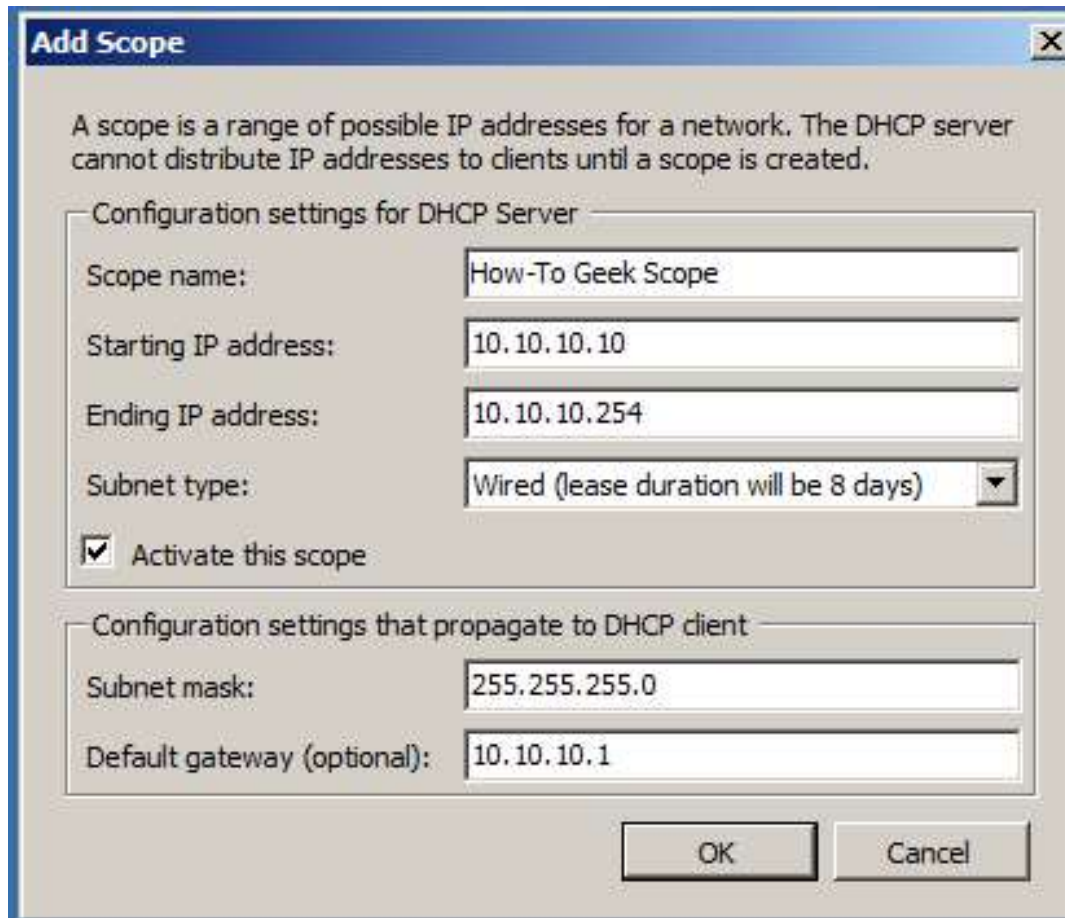
DHCP (1)

- Quản lý và cấp phát tập trung và tự động địa chỉ mạng Internet cho các máy tính trong mạng. Cài đặt tự động các tham số khác trong mạng như máy chủ DNS, cổng kết nối ra ngoài.
- 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 logic cần tự động cấu hình IP.
 - Vị trí bộ định tuyến.
 - Số mạng LAN ảo.



DHCP (2)

- Định nghĩa một vùng địa chỉ



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

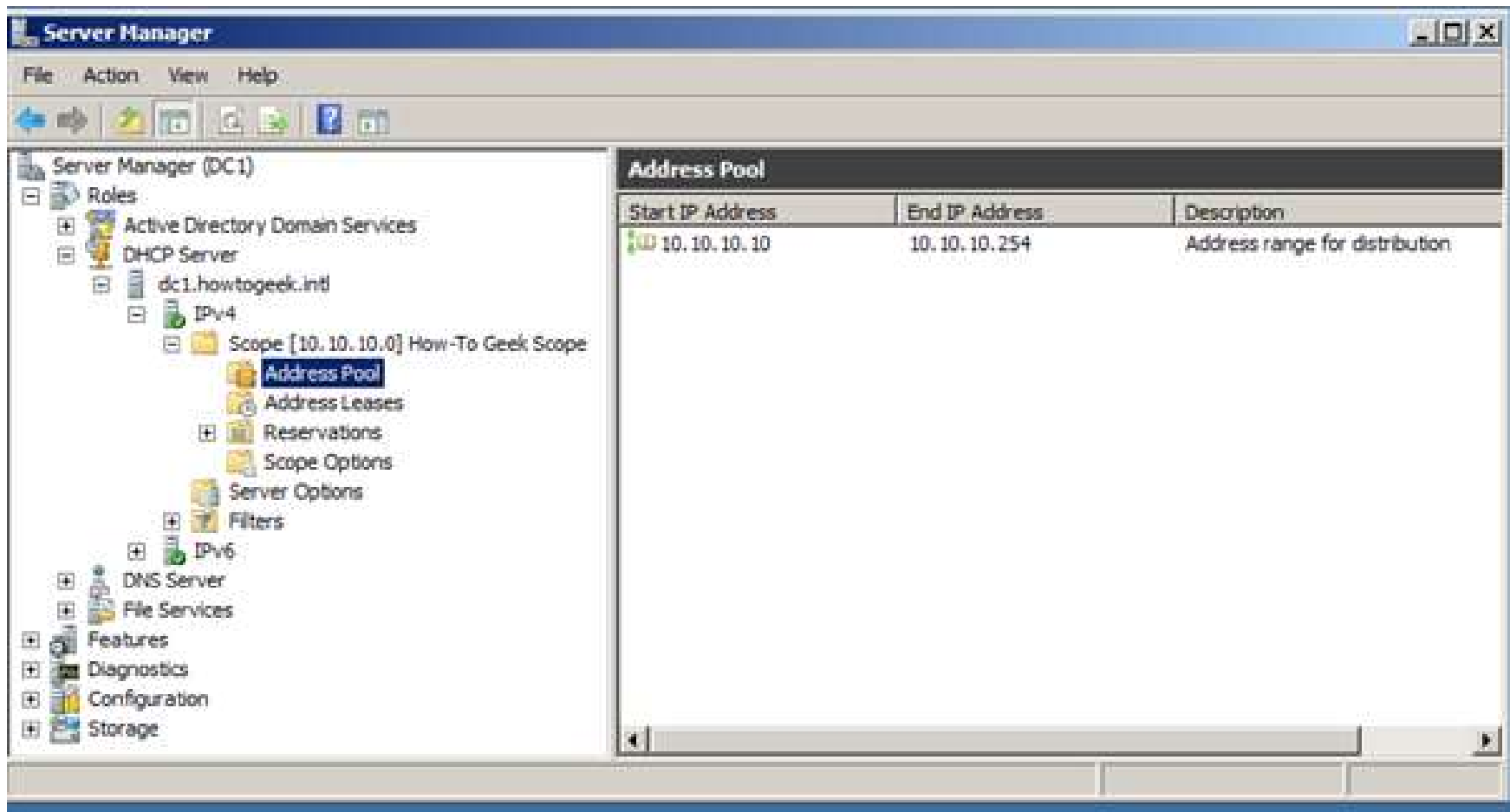
Configuration settings that propagate to DHCP client

Subnet mask: 255.255.255.0

Default gateway (optional): 10.10.10.1

OK Cancel

DHCP(3)



Kiểm tra

- **Ping:** PING (Packet Internet Grouper), được sử dụng để kiểm tra lỗi mạng, kiểm tra 2 thiết bị trong mạng nào đó có kết nối, hay đơn giản là có thông với nhau hay không.
- **Pathping:** là công cụ dòng lệnh dựa trên nền tảng hệ điều hành Windows được dùng để cung cấp thông tin về dữ liệu đường dẫn tới địa chỉ đích, độ trễ mạng và tổn thất mạng tại các bước truyền trung gian giữa nguồn và đích.
- **Nslookup:** Hiển thị các thông tin có thể được sử dụng để khai thác thông tin về cơ sở hạ tầng của Hệ thống tên miền.
- **Ipconfig:** sử dụng để xem hoặc thay đổi địa chỉ IP của máy tính.



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



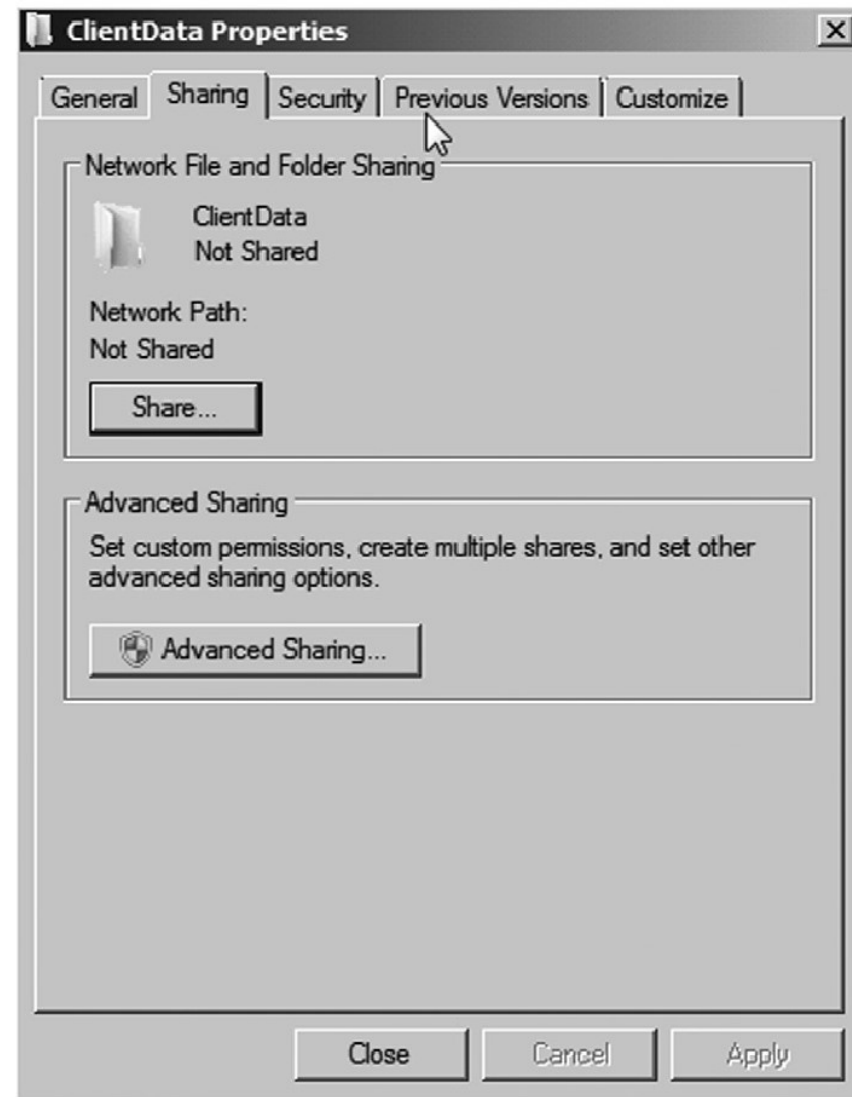
Dịch vụ file và in ấn

- 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.



Chia sẻ file (1)

- Tạo thư mục chia sẻ

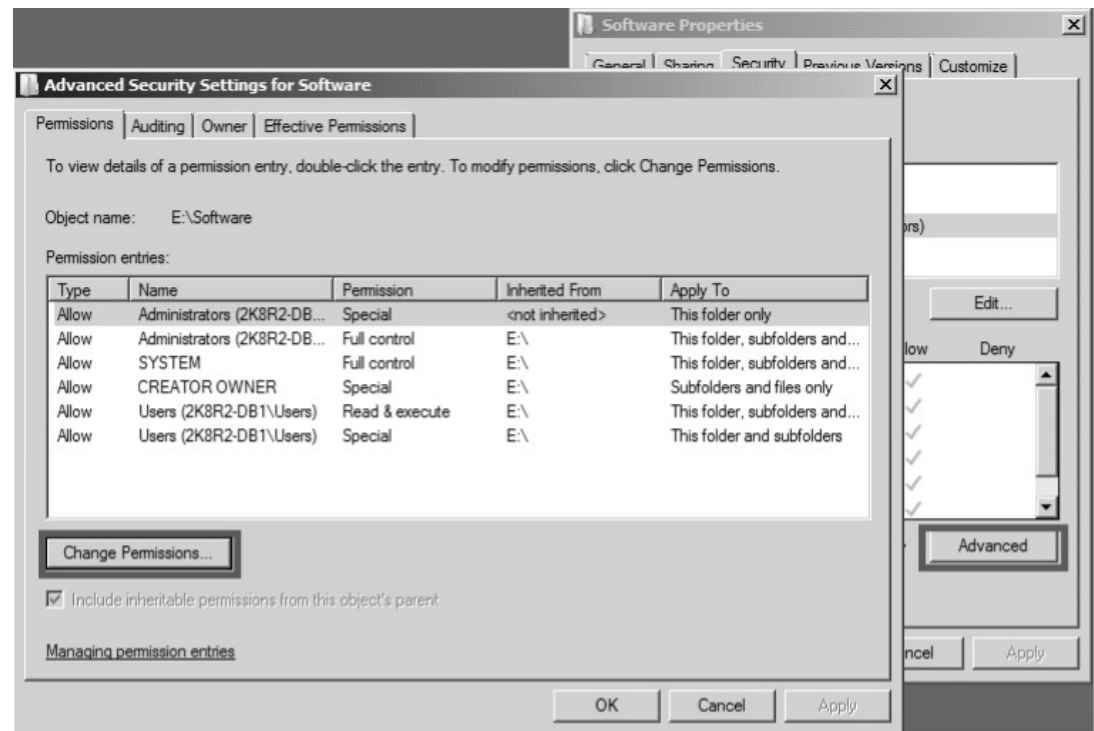
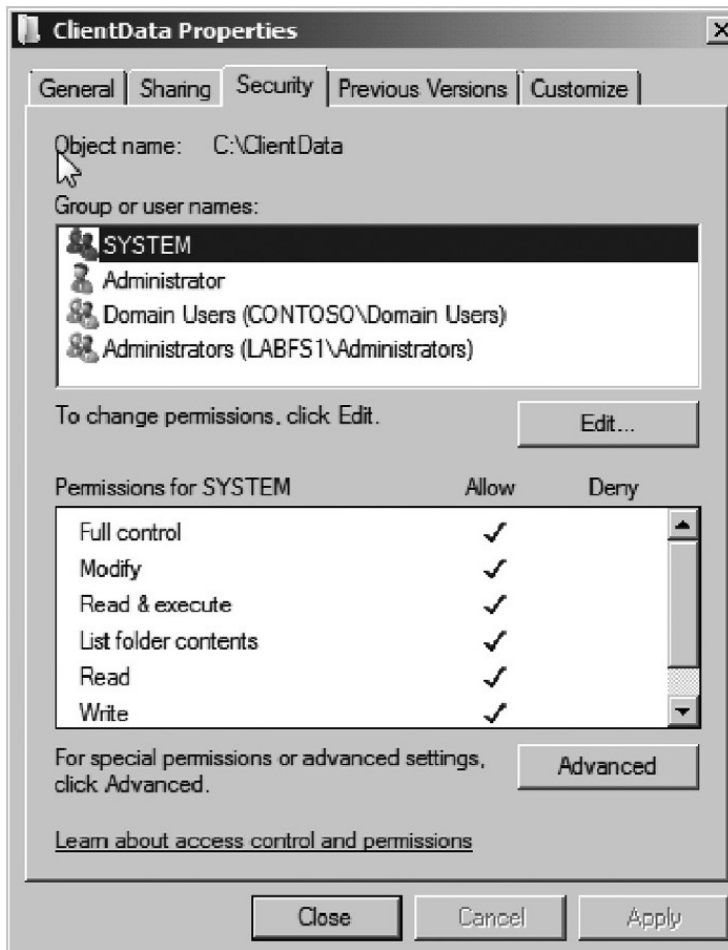


Chia sẻ file (2)

- 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/Sở hữu
 - Đặt quyền file/thư mục
 - Sử dụng NTFS để hạn chế việc truy nhập.
 - Cho phép giám sát tốt hơn và các quyền chi tiết hơn.



Quyền với thư mục chia sẻ (bên trái) và NTFS (bên phải)

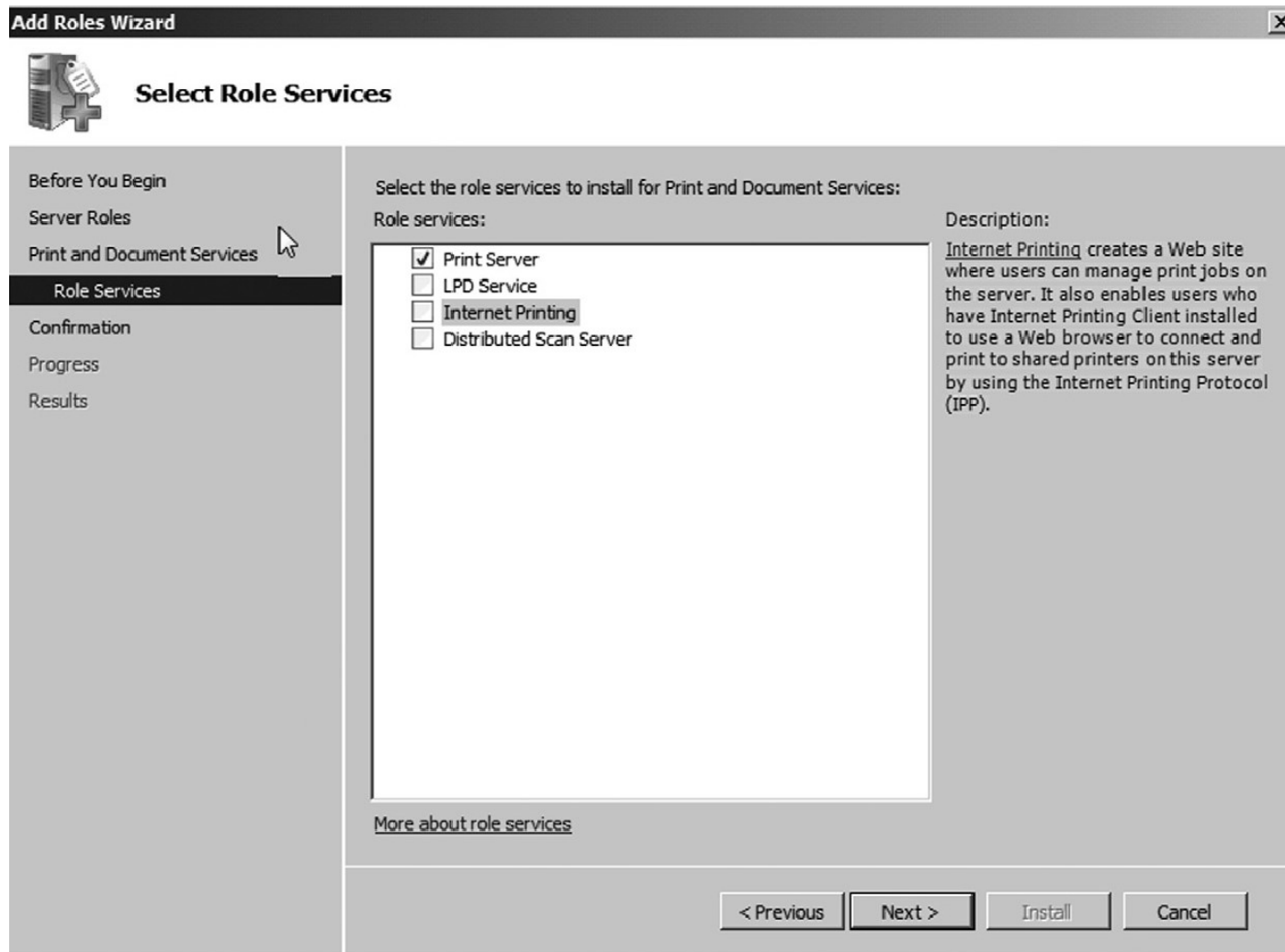


Dịch vụ in (1)

- Cho phép nhiều người dùng chia sẻ cùng 1 máy in.
- Các máy chủ in ấn là máy tính kết nối với máy in và làm nhiệm vụ xử lý các yêu cầu in ấn từ các người dùng trong mạng.
- 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.

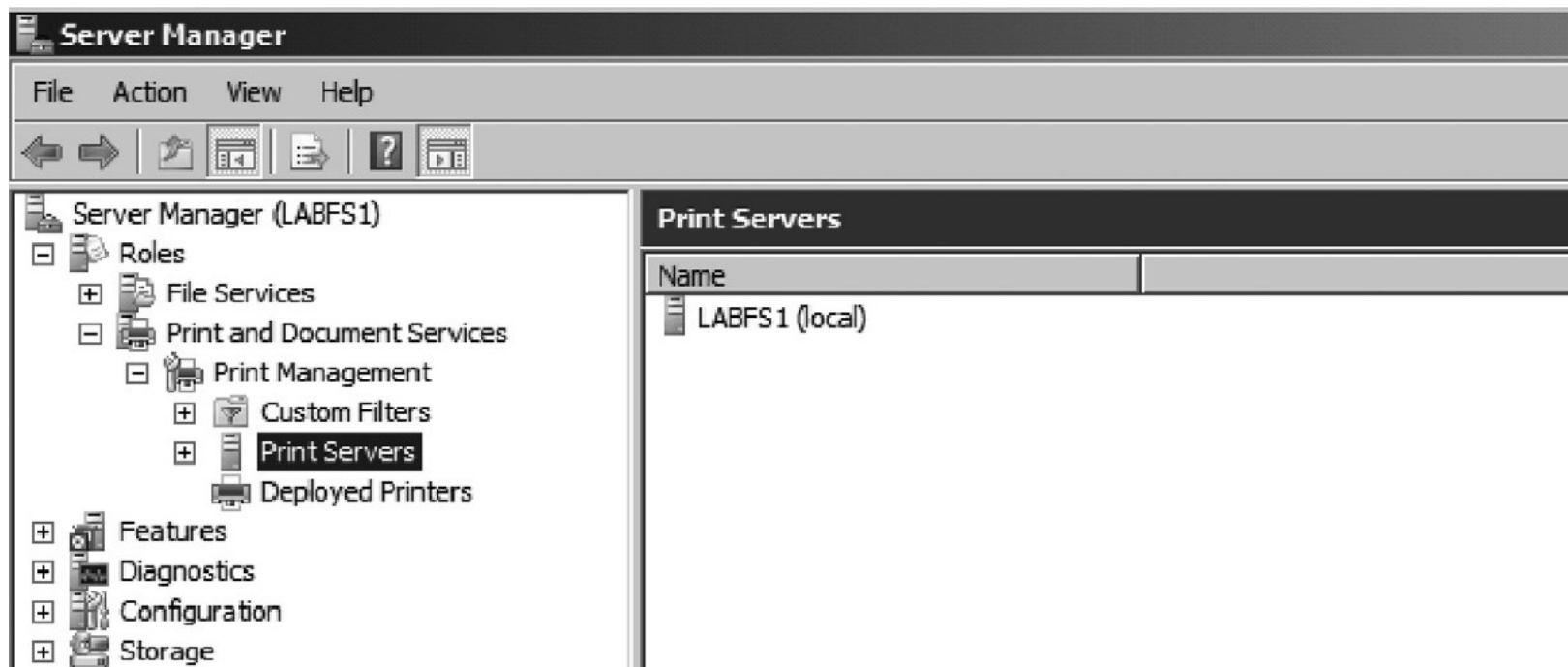


Dịch vụ in (2)



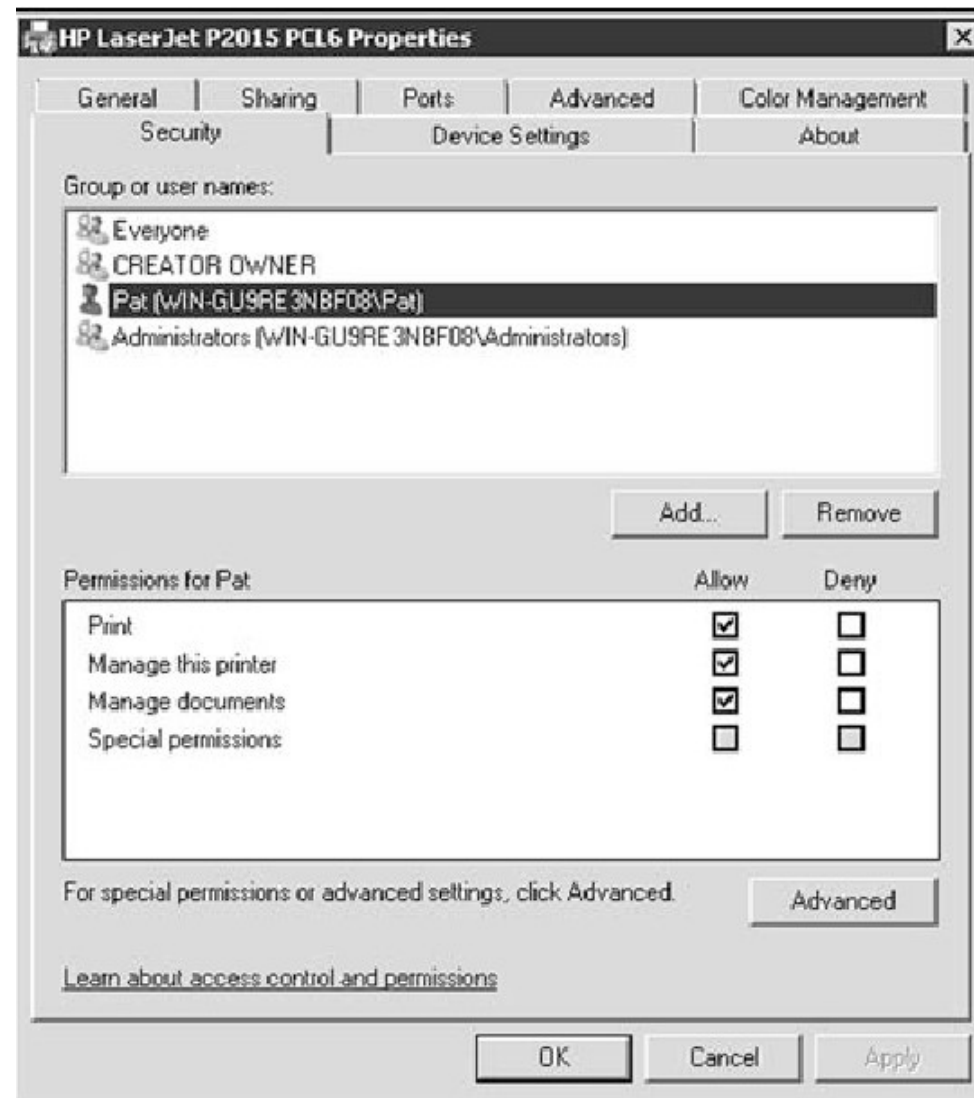
Dịch vụ in (1)

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

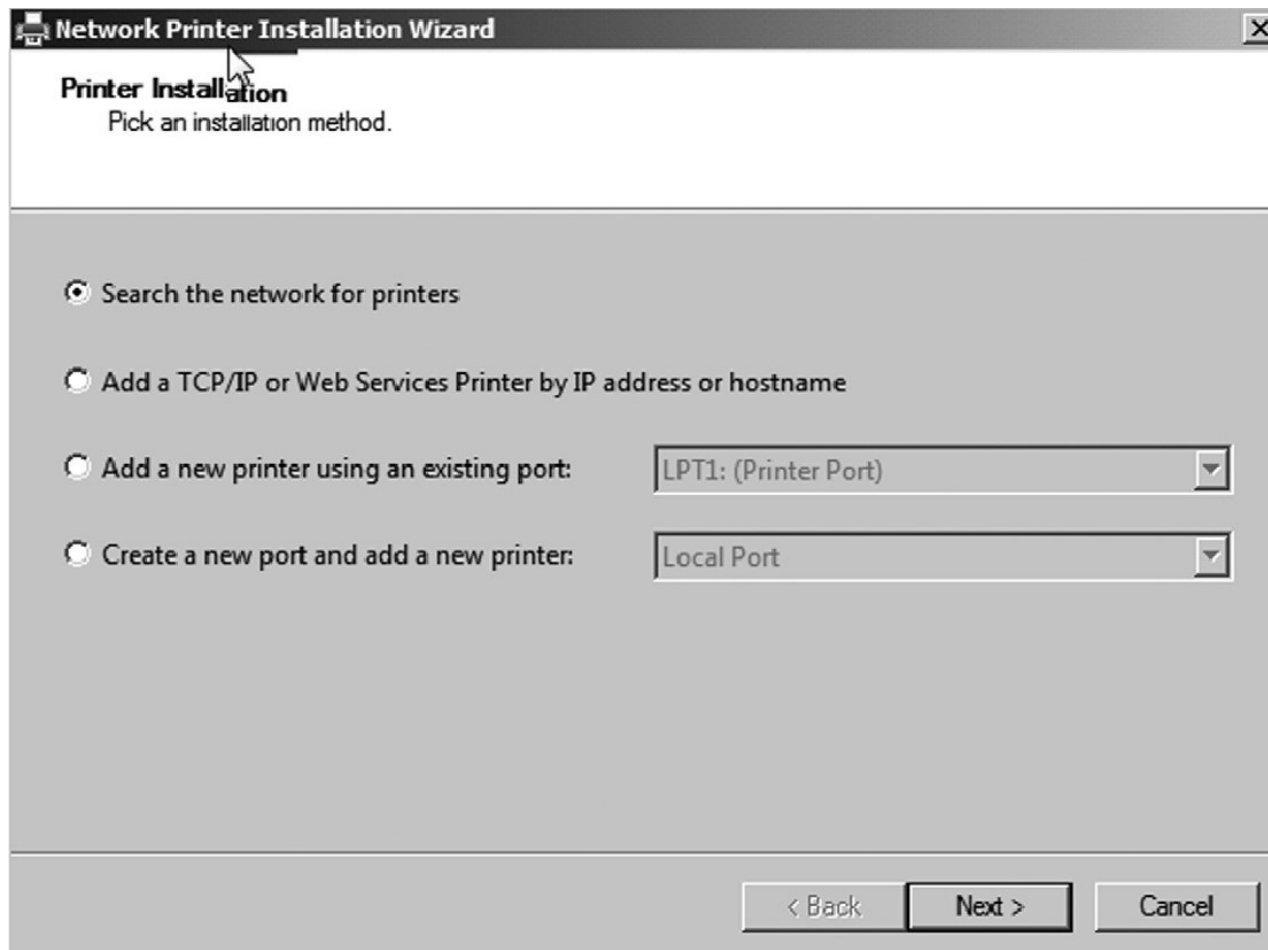


Dịch vụ in (4)

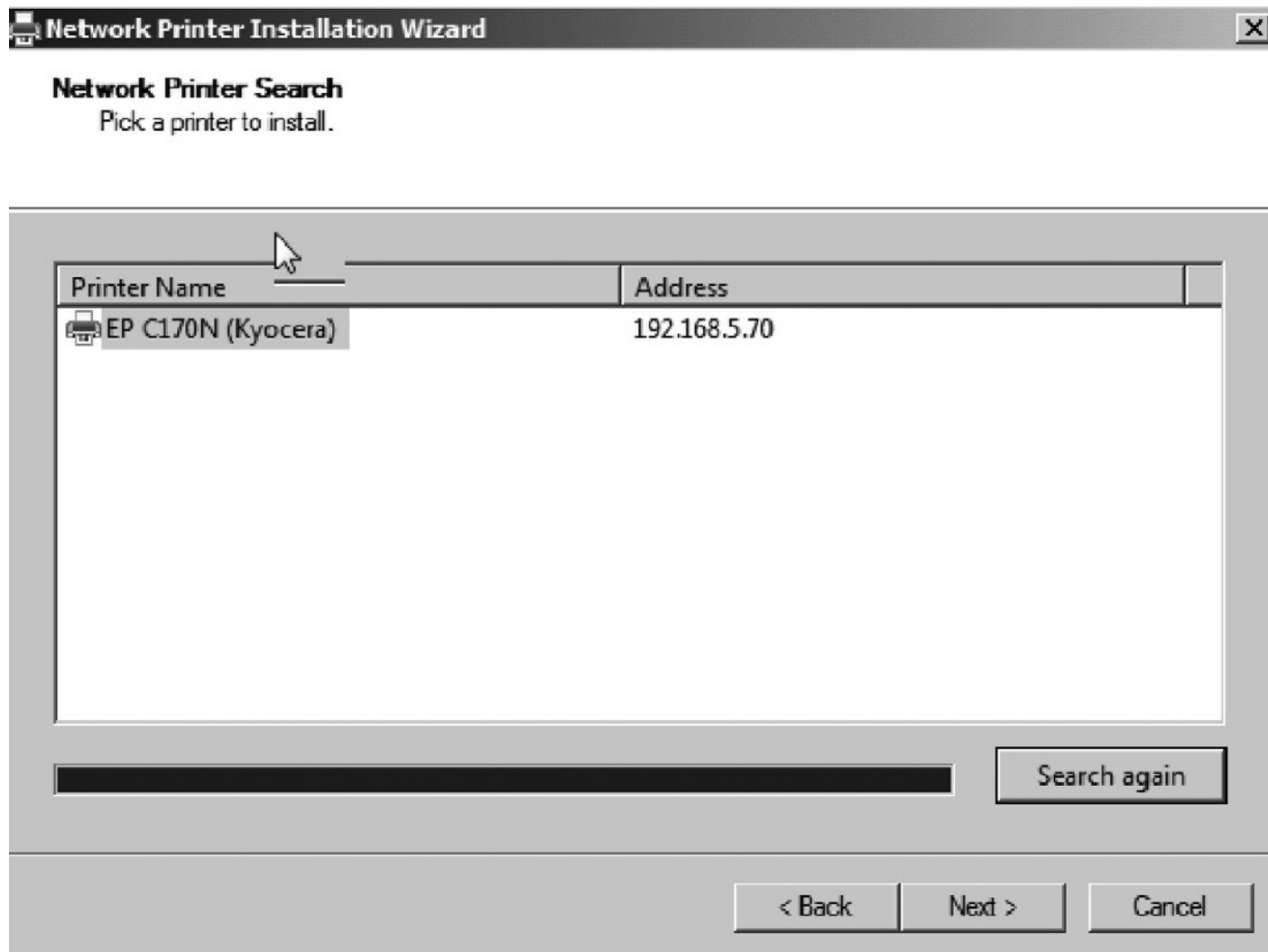
- Quyền in:
- Quyền quản lý máy in: Cho phép người dùng thay đổi cài đặt và cấu hình
- Quyền quản lý tài liệu in: Hủy, dừng, in lại hay khởi động lại máy in



Cài đặt máy in mạng (1)



Cài đặt máy in mạng (2)



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

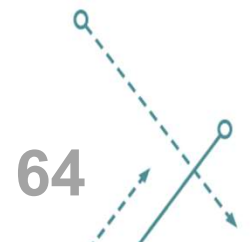
3.4 Quản trị máy chủ dịch vụ file và in ấn

3.5 Quản trị máy chủ dịch vụ truy nhập từ xa

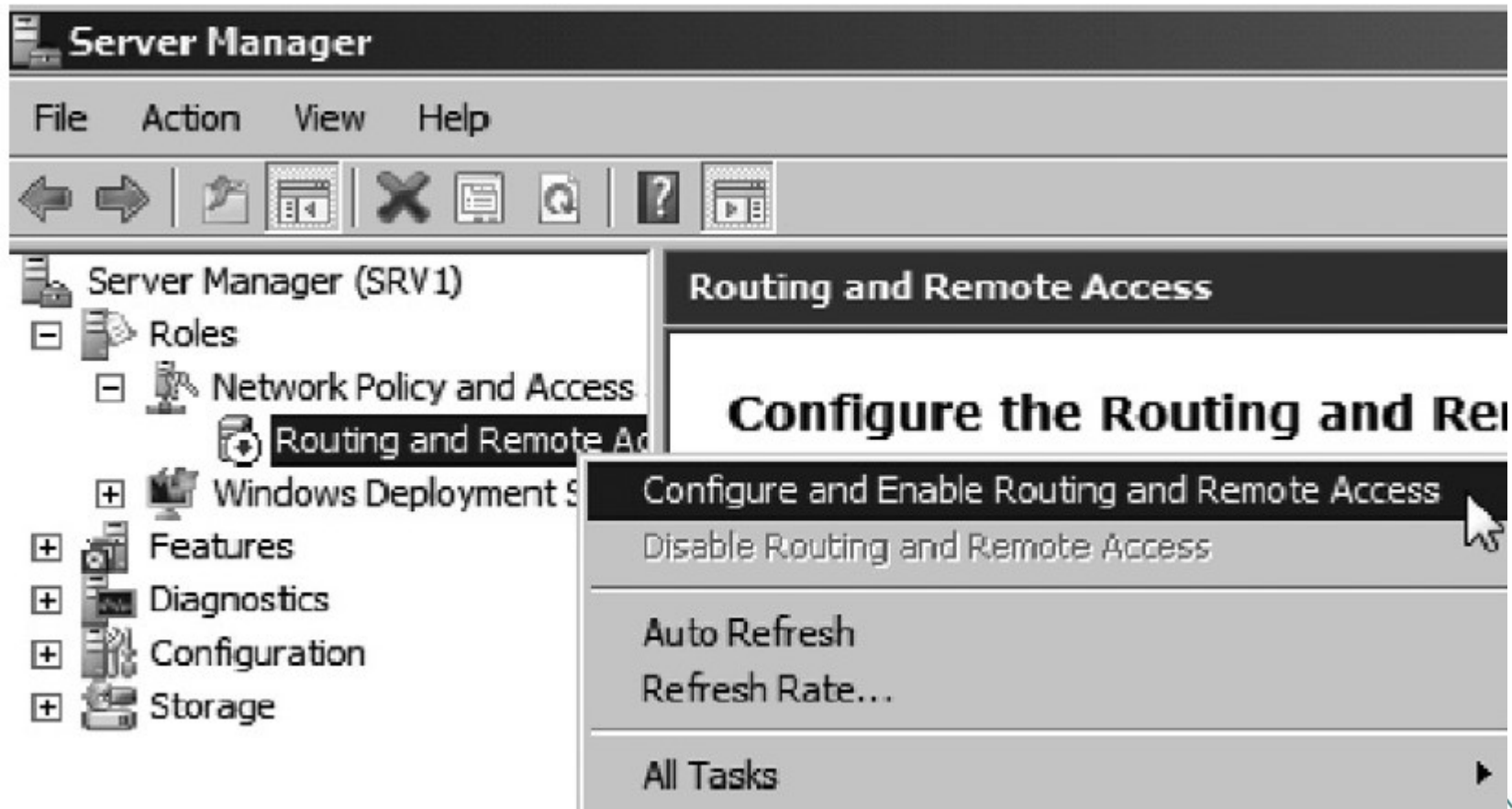


Dịch vụ truy nhập từ xa (1)

- 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.
- Sử dụng mạng riêng ảo VPN (Virtual Private Networks). 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 bảo mật.



Dịch vụ truy nhập từ xa (2)



Dịch vụ truy nhập từ xa (3)

Routing and Remote Access Server Setup Wizard

Remote Access
You can set up this server to receive both dial-up and VPN connections.

☒ **VPN**
A VPN server (also called a VPN gateway) can receive connections from remote clients through the Internet.

☐ **Dial-up**
A dial-up remote access server can receive connections directly from remote clients through dial-up media, such as a modem.

[For more information](#)

< Back Next > Cancel

