

ỨNG DỤNG IIS ĐỂ THIẾT LẬP DỊCH VỤ FTP

Tô Vũ Song Phương
Cao Đẳng Kỹ Thuật Cao Thắng

Nội dung

1. IIS là gì?
2. FTP là gì?
3. Mô hình FTP
4. Các chế độ truyền file trong FTP
5. Cô lập người dùng (FTP User Isolation) và phân quyền tài nguyên truy cập (FTP Authorization)
6. TFTP, SFTP là gì?

1.1 IIS là gì?

- **IIS** (Internet Information Services - các dịch vụ cung cấp thông tin Internet) là các dịch vụ dành cho máy chủ chạy trên Hệ điều hành Windows nhằm cung cấp và phân tán các thông tin lên mạng
- IIS bao gồm nhiều dịch vụ: dịch vụ Web, dịch vụ FTP, ...

1.2 Chức năng của IIS

- Xuất bản Website trên Internet
- Tạo các giao dịch thương mại điện tử trên Internet (hiện catalog và nhận các đơn đặt hàng từ người tiêu dùng)
- Chia sẻ dữ liệu thông qua giao thức FTP
- Cho phép người ở xa có thể truy xuất database (Database remote access)

1.3 Các phiên bản của IIS

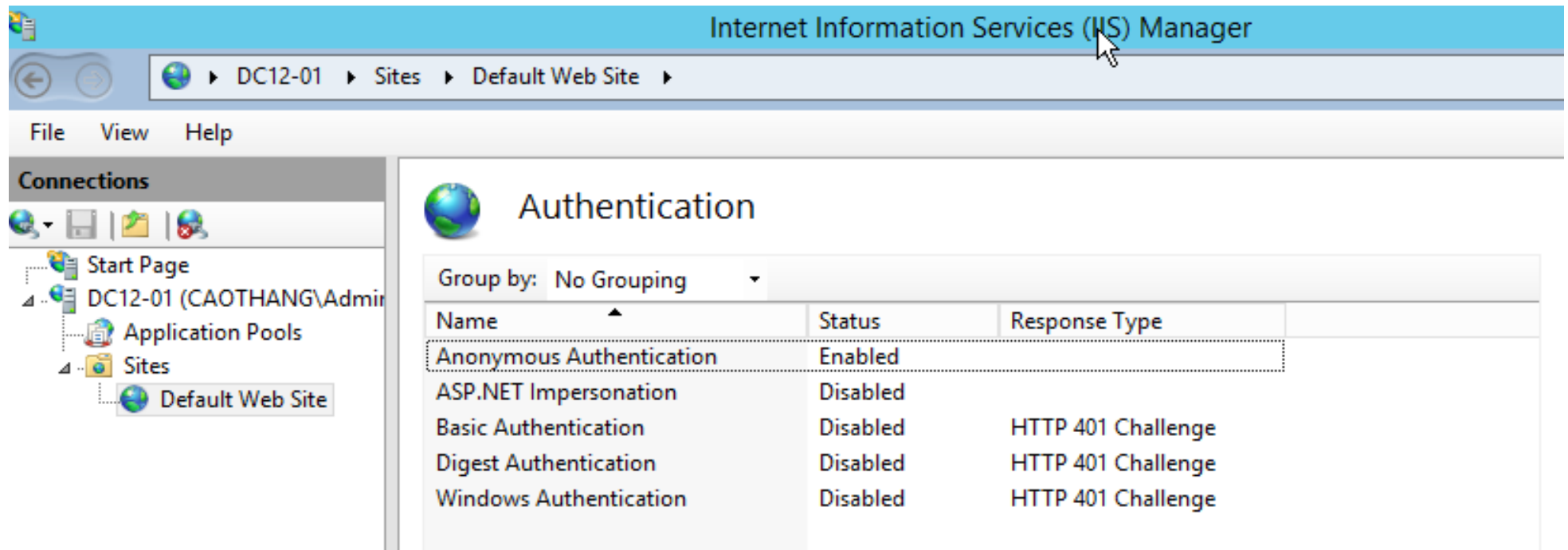
Mỗi phiên bản IIS thường đính kèm trong các phiên bản Microsoft Windows

- IIS 1.0 được phát hành đầu tiên dưới dạng add-on cho Windows NT 3.51
- IIS 6.0 có trong Windows Server 2003 và Windows XP Pro x64. Hiện nay không còn được cập nhật từ Microsoft nhưng có hỗ trợ IPv6
- IIS 7.5 có trong Windows 7 và Windows Server 2008 R2. Có thêm chức năng TLS 1.1 và 1.2 và quản trị dòng lệnh trong PowerShell. Đây là phiên bản cũ nhất còn nhận được cập nhật chính thức từ Microsoft.
- IIS 8.5 có trong Windows 8.1 và Windows Server 2012 R2. Có nhiều tính năng mới như Enhanced logging, Dynamic Site Activation, v.v
- IIS 10.0 version 1607 có trong Windows Server 2016 và Windows 10 update. Có hỗ trợ HTTP/2 và có thể chạy trên Nano Server và Wildcard Host Headers
- IIS 10.0 version 1809 có trong Windows Server 2019 và Windows 10 update. Được bổ sung những tính năng mới.
- Tham khảo:

https://en.wikipedia.org/wiki/Internet_Information_Services

1.4 Một số tính năng bảo mật trên IIS

- Để thấy các tính năng bảo mật của IIS, vào mục Authentication trong IIS Manager



1.4 Một số tính năng bảo mật trên IIS

- Anonymous Authentication
 - Cho phép mọi người có thể truy xuất tài nguyên mà không cần yêu cầu username và password
- Basic Authentication
 - Yêu cầu người dùng cung cấp username và password khi muốn truy xuất tài nguyên
 - Username và password không được mã hóa khi qua mạng

1.4 Một số tính năng bảo mật trên IIS

- Digest Authentication

- Hoạt động giống Basic authentication, nhưng username và password trước khi gửi đến Server thì phải được mã hóa và sau đó Client gửi thông tin này dưới một giá trị băm (hash value)
- Chỉ sử dụng trên máy chủ là thành viên miền Active Directory

- Windows Authentication

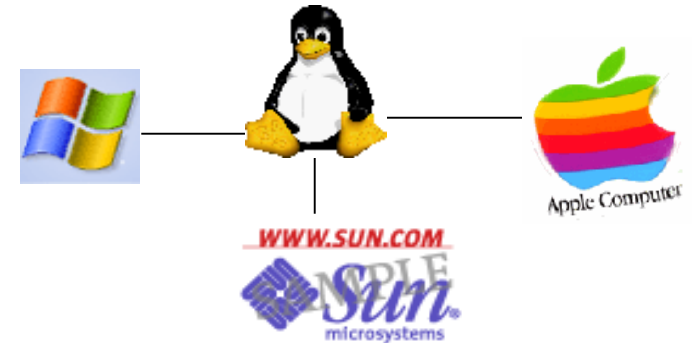
- Sử dụng kỹ thuật băm để xác nhận thông tin của users mà không cần phải yêu cầu gửi mật khẩu qua mạng

2.1 Các dịch vụ lưu trữ đám mây nào?

- Dropbox
- Google Drive
- Mega
- OneDrive
- iCloud
- Box
- NextCloud
- SpiderOak
- iDrive
- pCloud
- ...

2.2 Các vấn đề khi truyền tải file

- Ban đầu, việc truyền tải file dường như dễ dàng
- Nhưng, các hệ thống khác nhau về:
 - Hệ điều hành (Operating Systems)
 - Cấu trúc thư mục
(Directory Structures)
 - Cấu trúc và định dạng file
(File Structures and Formats)
- FTP đáp ứng và giải quyết các vấn đề trên



2.3 FTP là gì?

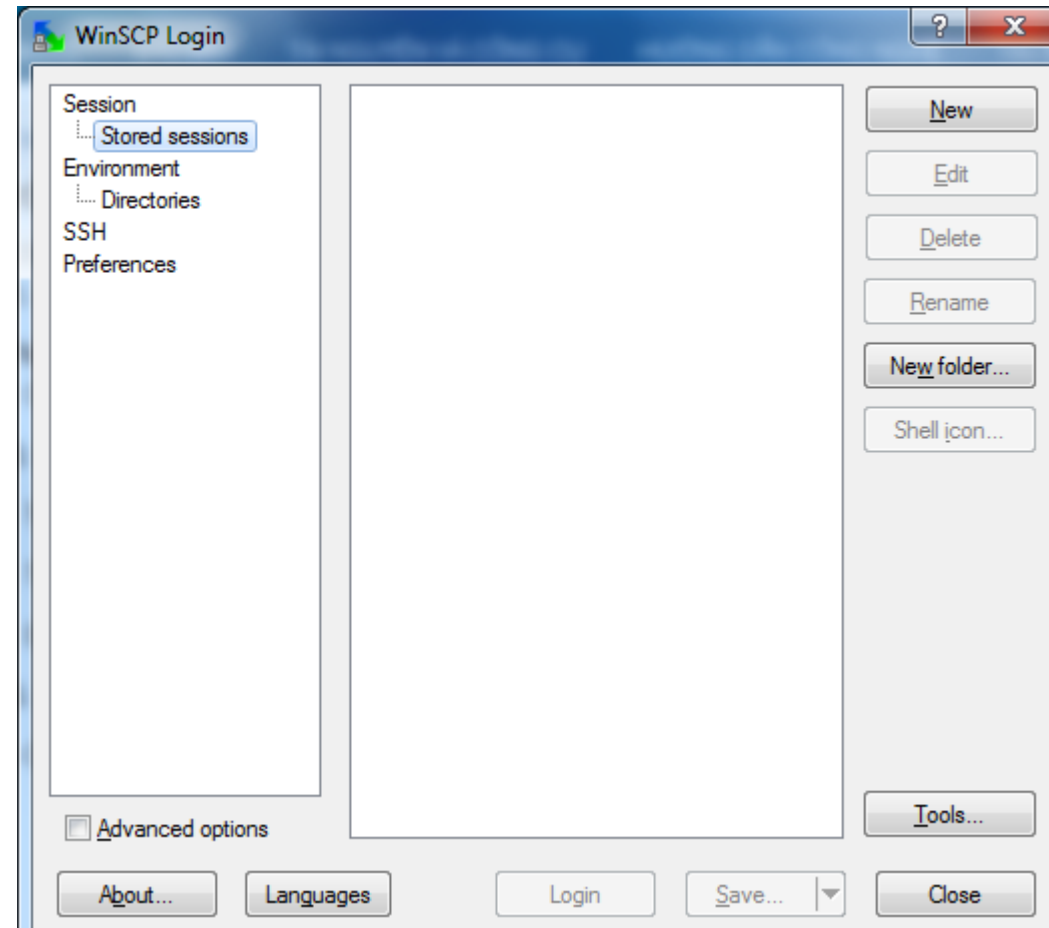
- **FTP (File Transfer Protocol)** là giao thức truyền tải tập tin từ host này đến host khác
- FTP sử dụng TCP (giao thức vận chuyển gói tin đáng tin cậy), không sử dụng UDP (không tin cậy)
- FTP sử dụng kiến trúc Client /Server
- FTP dùng đến 2 cổng (port):
 - Port 20 dùng để truyền dữ liệu (data port)
 - Port 21 dùng để truyền lệnh (command port)

2.4 Lịch sử ngắn gọn FTP

- Đặc tả đầu tiên được viết bởi Abhay Bhushan năm 1971
- Năm 1980, với sự xuất hiện của TCP/IP, FTP được đặc tả trong tài liệu RFC 765, sau đó là RFC 959 cho đến ngày nay. Sau này có thêm một số cải tiến về tính bảo mật, chế độ truyền nhị phân và hỗ trợ IPv6

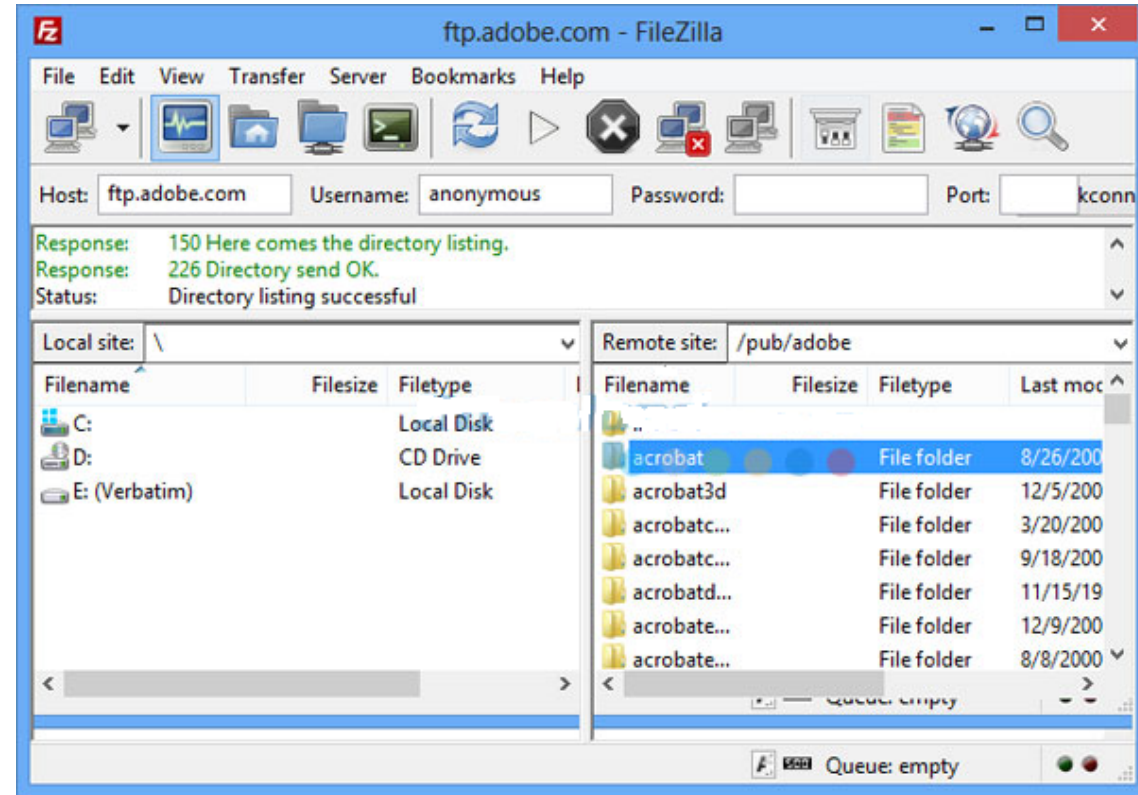
2.5 Các công cụ tải file lên FTP Server

- **WinSCP:** một tiện ích SFTP, FTP client miễn phí, mã nguồn mở dành cho hệ điều hành Windows. Giúp truyền tải file một cách an toàn giữa máy tính của ta và máy tính từ xa. Cung cấp các chức năng quản lý file. Chương trình có hỗ trợ cả SSH để bảo mật.
- Download:
<http://winscp.net/eng/download.php>



2.5 Các công cụ tải file lên FTP Server

- **FileZilla Client:** Giao diện đơn giản, có sẵn nhiều ngôn ngữ, hỗ trợ các giao thức chuyển đổi file FTP, SSH. Thư mục bộ nhớ đệm sẽ tăng tốc độ duyệt các trang web FTP. Ngoài ra, có nhiều tùy chọn kết nối an toàn sẽ đảm bảo rằng ta có thể tải file mà không cần phải lo lắng
- Download: <https://filezilla-project.org/>



2.6 Một số lệnh của FTP trong cmd

- Để kết nối tới FTP server ta dùng cú pháp:

`ftp <ftp_address>`

Ví dụ: `ftp ftp.caothang.edu.vn`

- Để thiết lập 1 phiên giao dịch ta cần phải có địa chỉ IP (tên PC), 1 tài khoản (username, password)

2.6 Một số lệnh của FTP trong cmd

Tên lệnh	Cú pháp	Ý nghĩa
? hoặc help	? [command]	Hiển thị giúp đỡ
append	append local-file [remote-file]	Ghép 1 file cục bộ với 1 file trên server
binary	binary	Chỉ định kiểu truyền file là binary (default)
Bye	bye	Kết thúc ftp session
cd	cd remote-directory	Thay đổi đường dẫn thư mục trên FTP server

2.6 Một số lệnh của FTP trong cmd

delete	delete remote-file	Xóa file trên ftp server
dir	dir remote-directory	Liệt kê danh sách file
get	get remote-file [local-file]	Download file từ FTP server về máy cục bộ
lcd	lcd [directory]	Thay đổi thư mục trên máy cục bộ
ls	ls [remote-directory] [local-file]	Liệt kê các tập tin và thư mục
mdelete	mdelete remote-file [...]	Xóa nhiều file cùng lúc

2.6 Một số lệnh của FTP trong cmd

mget	mget remote-file [...]	Download nhiều file
mkdir	mkdir directory	Tạo thư mục
put	put local-file [remote-file]	Upload tập tin
mput	mput local-file [...]	Upload nhiều tập tin
open	open computer [port]	Kết nối tới FTP server
prompt	prompt	Tắt cơ chế confirm sau mỗi lần download file

2.6 Một số lệnh của FTP trong cmd

disconnect	disconnect	Hủy kết nối FTP
pwd	pwd	Xem thư mục hiện hành
quit	quit	Thoát khỏi FTP session
recv	recv remote-file [local-file]	Copy file từ remote về local
rename	rename filename newfilename	Thay đổi tên file
rmdir	rmdir directory	Xóa thư mục
send	send local-file [remote-file]	Copy file từ local đến server
user	user user-name [password] [account]	Chuyển đổi user khác

2.7 Các mã phản hồi từ FTP Server trong cmd

- Tất cả phản hồi đều được gửi qua kênh điều khiển (control connection)
- Phản hồi chứa gồm
 - Mã gồm 3 chữ số
 - Đoạn văn bản.

2.7 Các mã phản hồi từ FTP Server trong cmd

Chữ số đầu trong mã xác định kiểu phản hồi: tốt, xấu, chưa hoàn thành

- '1xx': Positive Preliminary Reply (got it, but wait).
- '2xx': Positive Completion Reply (success).
- '3xx': Positive Intermediate Reply (waiting for more information).
- '4xx': Transient Negative Completion (error – try again).
- '5xx': Permanent Negative Reply (error - can't do).

2.7 Các mã phản hồi từ FTP Server trong cmd

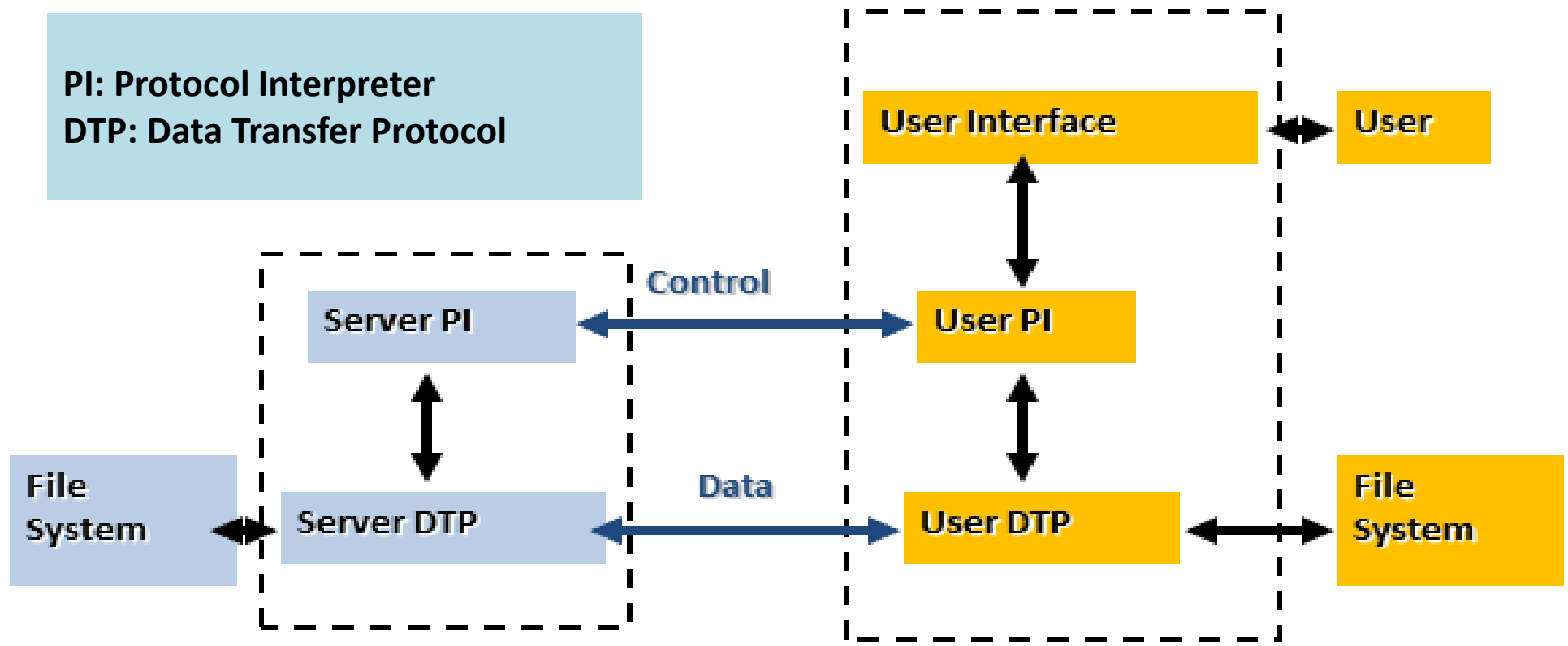
Chữ số thứ 2 trong mã xác định vấn đề gặp phải

- 'x0x': Syntax (problem with command syntax).
- 'x1x': Information (reply to help or status cmds).
- 'x2x': Connections (problem with a connection).
- 'x3x': Authentication (problem with login).
- 'x4x': Unspecified.
- 'x5x': File system (related to file system).

2.7 Các mã phản hồi từ FTP Server trong cmd

- **120** Service ready in ... minutes
- **200** Command OK
- **230** User login OK
- **331** User name OK; password is needed
- **421** Service not available, closing control connection
- **430** Invalid username or password
- **530** User not logged in

3.1 Mô hình FTP



- **Protocol Interpreter (PI)**: thành phần quản lý kênh điều khiển, với chức năng phát và nhận lệnh
- **Data Transfer Protocol (DTP)**: có chức năng gửi và nhận dữ liệu giữa phía client với server

3.1 Mô hình FTP

Kênh điều khiển (Control Connection)

- Là kênh logic được dùng để khởi tạo một phiên kết nối FTP
- Được duy trì xuyên suốt phiên kết nối FTP và được sử dụng chỉ để truyền các thông tin điều khiển, các lệnh và các hồi đáp
- Không được dùng để truyền file

Kênh dữ liệu (Data Connection)

- Khi dữ liệu được truyền từ server tới client, một kênh kết nối dữ liệu được khởi tạo giữa chúng
- Khi file được truyền xong, kênh này được ngắt. Việc sử dụng các kênh riêng lẻ tạo sự linh hoạt trong việc truyền dữ liệu
- Lưu ý: trong quá trình truyền dữ liệu thì kênh điều khiển phải được mở

3.2 Cách hoạt động của FTP

Xem clip

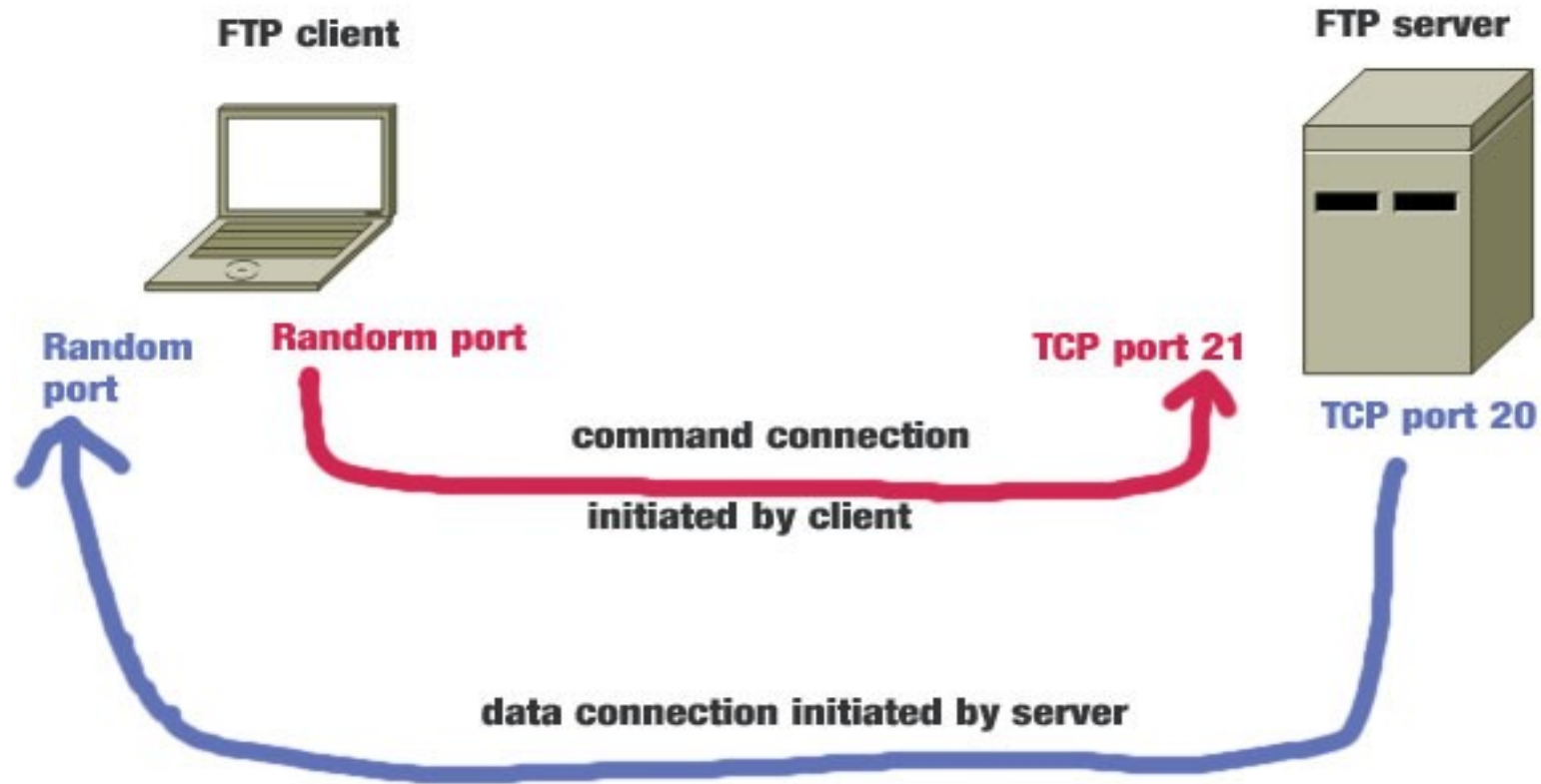


Link: https://www.youtube.com/watch?v=U0LzX_tTiNw

4. Các chế độ truyền file trong FTP

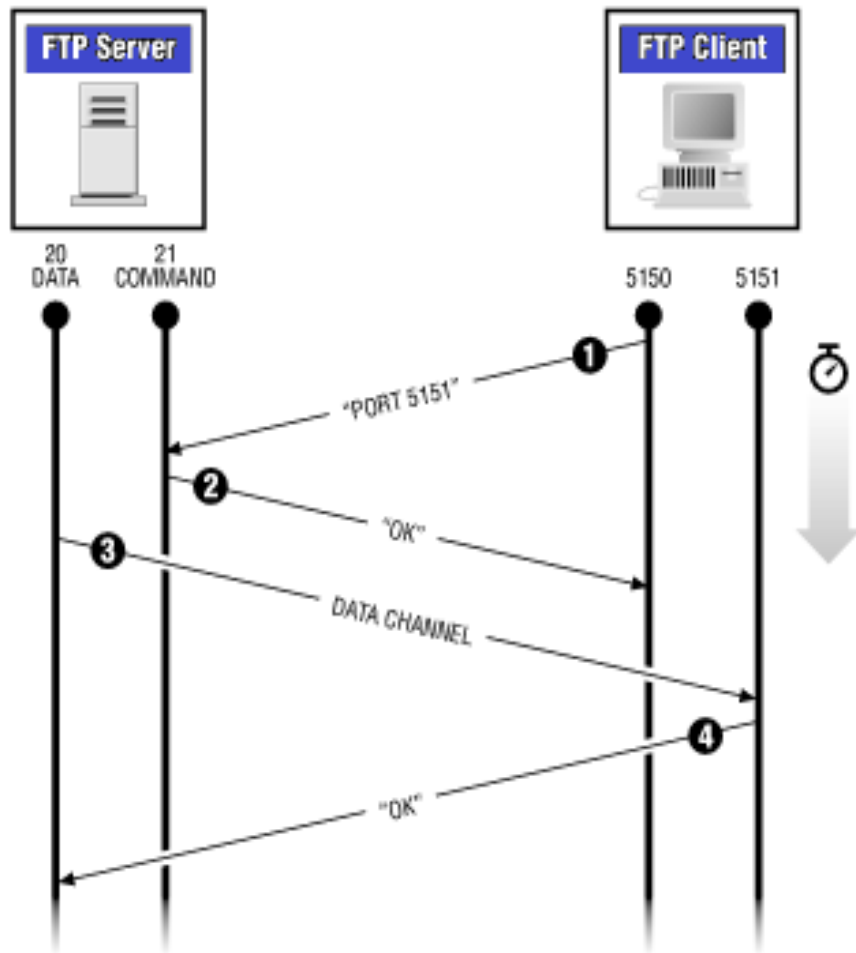
- Truyền file dạng chủ động (Active FTP)
- Truyền file dạng bị động (Passive FTP)

4.1 Active FTP



FTP mode: Active

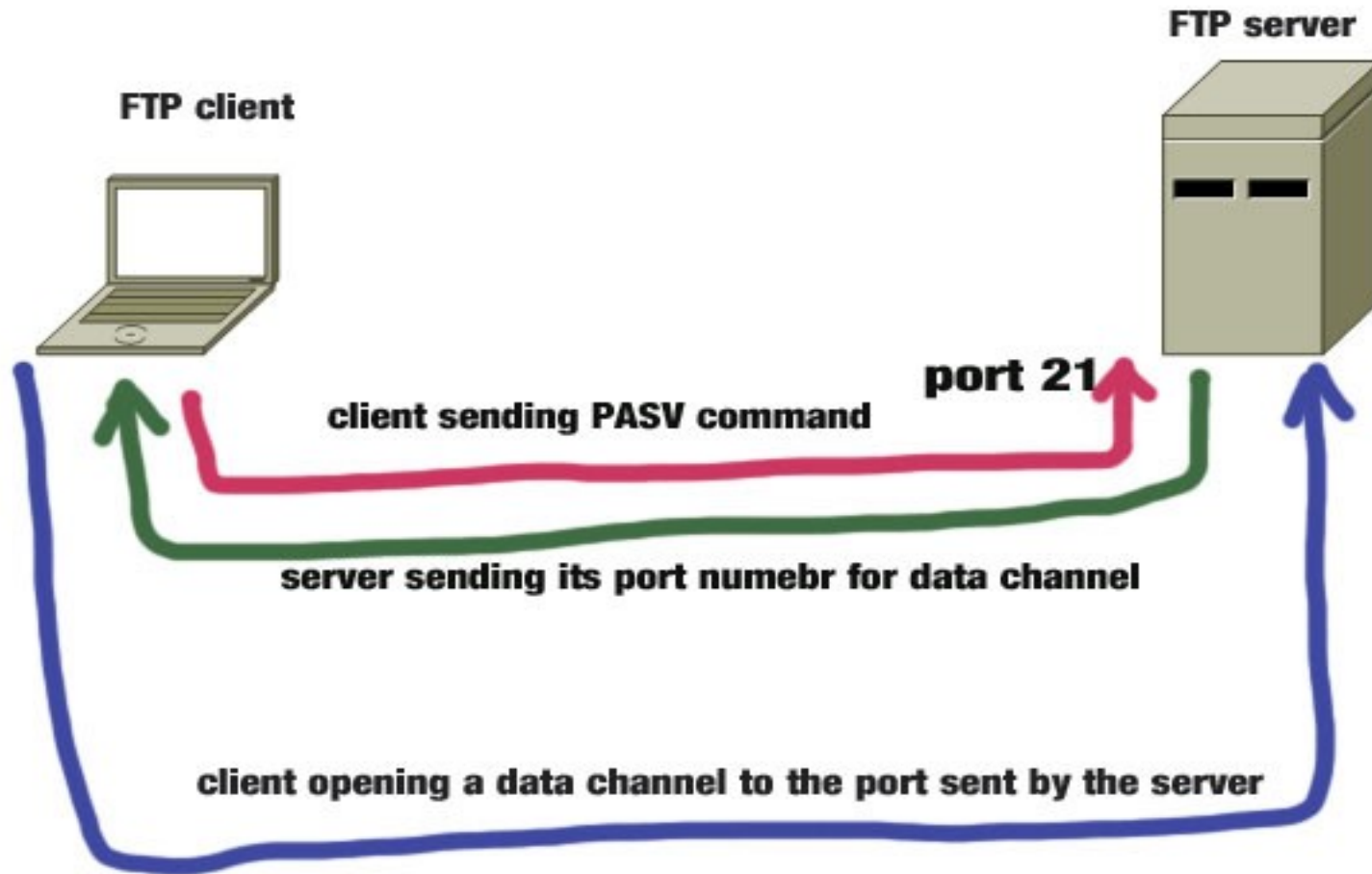
4.1 Active FTP



Minh họa truyền file dạng chủ động khi $n = 5150$, $m = 5151$

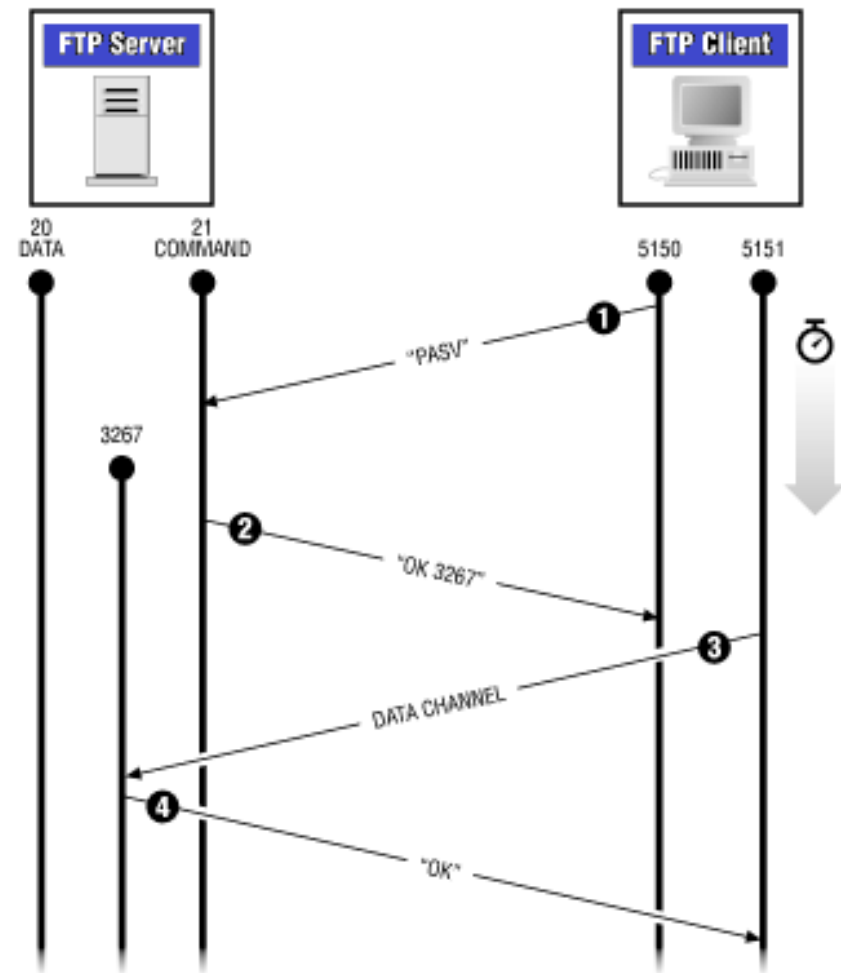
- ❖ Client mở port ngẫu nhiên n ($n > 1023$) khởi tạo kết nối tới port 21 của FTP Server và gửi lệnh PORT m để cho FTP Server biết sẽ trao đổi file qua data port này (m ngẫu nhiên, $m > 1023$)
- ❖ FTP Server gửi xác nhận ACK về port n của Client.
- ❖ Server khởi tạo kết nối từ cổng 20 đến data port m mà Client đã khai báo trước đó.
- ❖ Client gửi ACK phản hồi tới data port 20 của Server cho biết đã sẵn sàng tiếp nhận dữ liệu.

4.2 Passive FTP



FTP mode: Passive

4.2 Passive FTP

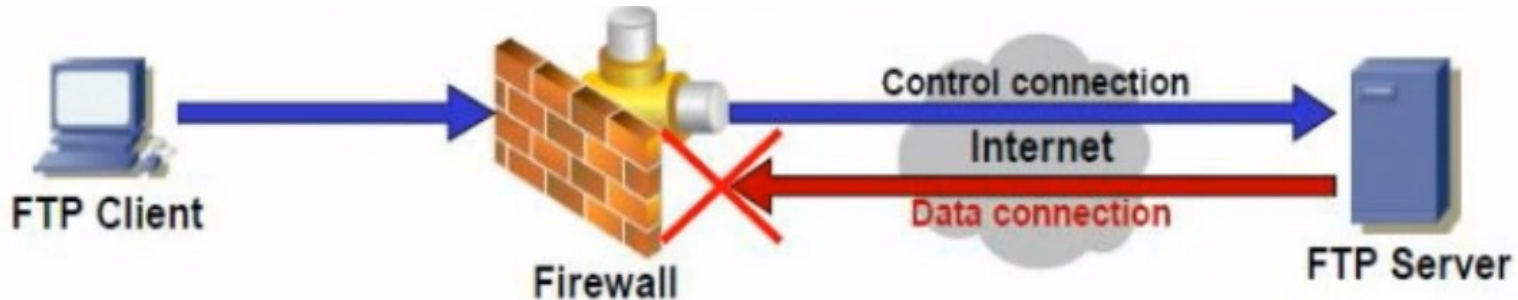


- ❖ Client mở port n ($n > 1023$) kết nối vào cổng 21 của Server và phát lệnh PASV.
- ❖ Server trả lời bằng lệnh PORT x (x ngẫu nhiên) cho Client biết nó mở port x để nhận kết nối dữ liệu.
- ❖ Client tạo kết nối truyền dữ liệu từ cổng m (m ngẫu nhiên) đến data port x của Server.
- ❖ Server gửi ACK phản hồi tới cho data port m của client cho biết nó đã sẵn sàng tiếp nhận.

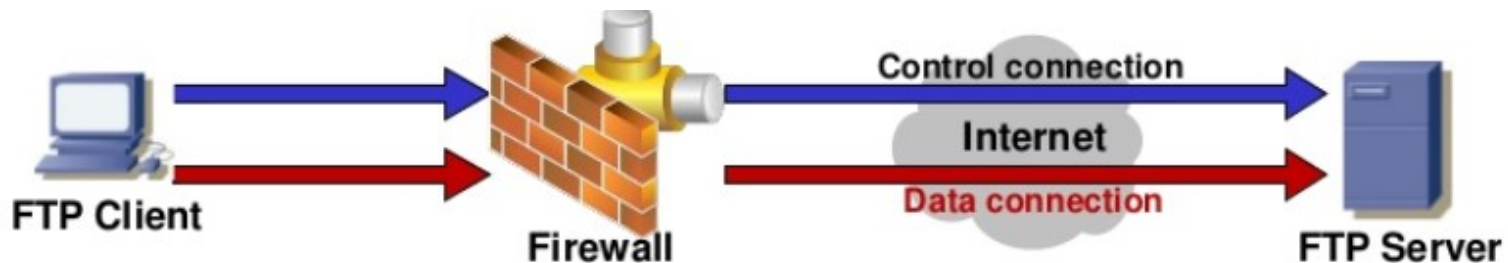
Minh họa truyền file dạng bị
động khi $n = 5150$, $m = 5151$, $x = 3267$

4.3 Active FTP vs Passive FTP

- **Active FTP:** client chờ server kết nối tới. Nếu có firewall đứng trước client thì data connection sẽ bị blocked



- **Passive FTP:** giải quyết vấn đề ở client, nhưng server phải chấp nhận hầu hết các kết nối có port > 1023, dẫn đến lỗ hổng nguy hiểm trên server



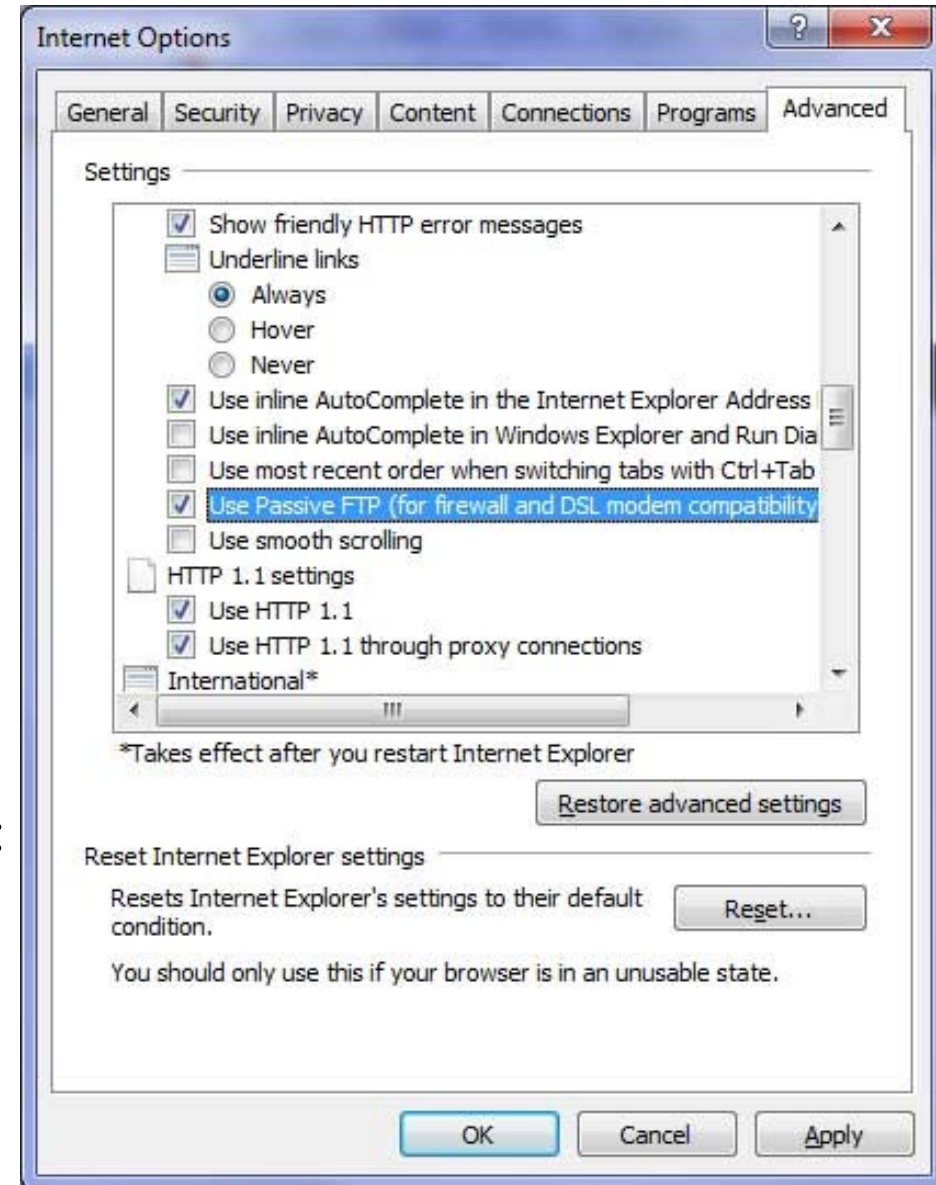
4.3 Active FTP vs Passive FTP

- **Active FTP**: tăng tính bảo mật trên Server
- **Passive FTP**: không đòi hỏi cấu hình nhiều từ Client.
- **Vậy chế độ truyền nào an toàn hơn?**

Cả 2 đều không an toàn. Vì cả 2 đều không sử dụng giao thức SSL (Secured Socket Layer) nên dữ liệu và password truyền đi không được mã hóa.

4.3 Active FTP vs Passive FTP

- Làm thế nào để enable/disable Passive FTP trong IE ?
 - Vào IE
 - Mở menu Tool, chọn Internet Options
 - Chọn tab Advanced
 - Tìm đến setting tên là Use Passive FTP (for firewall and DSL modem compatability)
 - Muốn enable: check. Muốn disable: uncheck
 - OK



5.1 FTP User Isolation

- Là tính năng có từ Windows Server 2003 hỗ trợ tải file và cập nhật nội dung Web cho từng User
- FTP user isolation cấp mỗi user một thư mục riêng lẻ, người dùng chỉ có khả năng xem, thay đổi, xóa nội dung trong thư mục của mình
- Phân biệt giữa **virtual directory** và **physical directory**:
 - **Physical directory**: thư mục vật lý. Là thư mục có trên đĩa cứng của máy chủ
 - **Virtual directory**: thư mục ảo. Là tên thân thiện hoặc bí danh cho thư mục vật lý trên ổ cứng máy chủ. Thường ngắn hơn đường dẫn của thư mục vật lý nên thuận tiện cho người dùng

5.1 FTP User Isolation

Isolation Mode	Chức năng
Do not isolate users	Không sử dụng FTP User Isolation. Ở mode này không giới hạn truy xuất của người dùng. Thông thường ta sử dụng mode này để tạo một public FTP Site
Isolate users	Mode này chứng thực người dùng cục bộ (Local User) và người dùng miền (Domain User) truy xuất vào FTP Site. Người quản trị phải tạo cho mỗi người dùng một thư mục con của thư mục FTP Root, với tên thư mục này là username của người dùng
Isolate users using Active Directory	Sử dụng Active Directory để tách lập từng user truy xuất vào FTP Server

Các chế độ FTP user isolation trong Windows Server 2003

5.1 FTP User Isolation

- Trong Windows Server 2012, FTP user isolation chia làm 2 phần
 - Do not isolate users: không dùng chức năng cô lập người dùng
 - Isolate users: sử dụng chức năng cô lập người dùng



FTP User Isolation

FTP user isolation prevents users from accessing the FTP home directory of another user on this FTP site.

Do not isolate users. Start users in:

- ☒ FTP root directory
- ☐ User name directory

Isolate users. Restrict users to the following directory:

- ☐ User name directory (disable global virtual directories)
- ☐ User name physical directory (enable global virtual directories)
- ☐ FTP home directory configured in Active Directory

Set...

- ☐ Custom

5.1 FTP User Isolation

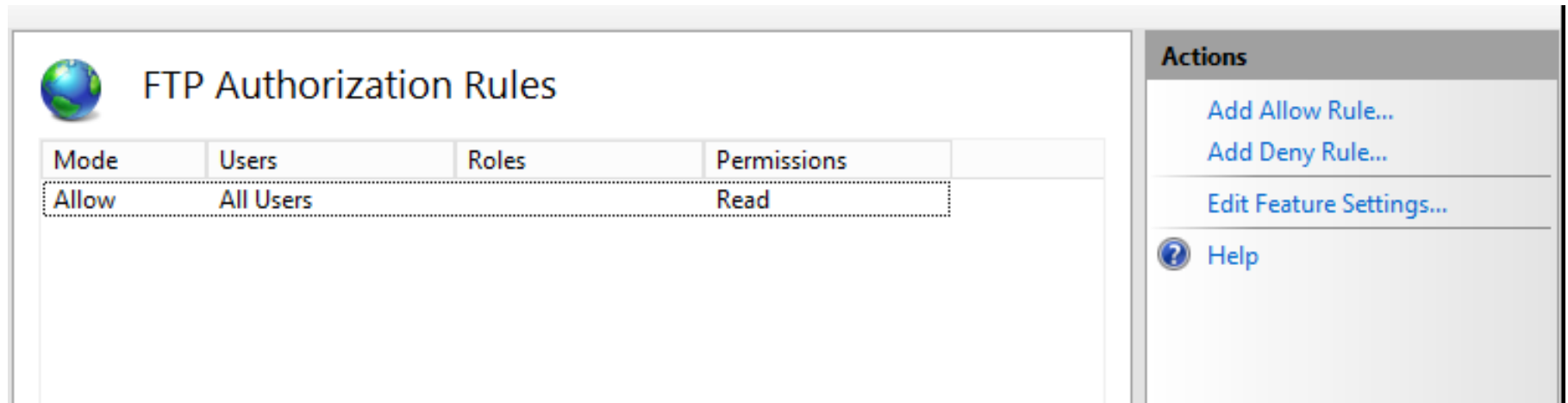
- Trong phần Do not isolate users
 - **FTP root directory**: mọi user kết nối tới FTP Server đều bắt đầu ở FTP Root
 - **User name directory**: mọi user kết nối tới FTP Server sẽ bắt đầu ở thư mục vật lý/ảo cùng tên. Nếu FTP Root không có tên thư mục username đó thì sẽ bắt đầu ở FTP Root. Lưu ý: các user có thể truy cập thư mục lẫn nhau

5.1 FTP User Isolation

- Trong phần Isolate users
 - User name directory (disable global virtual directories): khi user kết nối tới FTP Server chỉ nhìn thấy thư mục riêng (đó là thư mục gốc của user đó). Các user đều không thấy thư mục ảo nào.
 - User name physical directory (enable global virtual directories): khi user kết nối tới FTP Server chỉ nhìn thấy thư mục riêng. Tuy nhiên, các user có thể thấy thư mục ảo toàn cục.
 - FTP home directory configured in Active Directory: khi user kết nối tới FTP Server chỉ nhìn thấy thư mục riêng chỉ trên Active Directory.

5.2 FTP Authorization

- Đây là tính năng có từ Windows Server 2008 (từ IIS 7.0) hỗ trợ việc xác định tài nguyên nào mà user được phép/không được phép truy cập



5.2 FTP Authorization

- Có 2 loại luật trong FTP

Authorization

- **Allow Rule**: định nghĩa user, group có thể truy cập một site, một ứng dụng hoặc tất cả site trên server
- **Deny Rule**: định nghĩa user, group không thể truy cập một site, một ứng dụng hoặc tất cả site trên server



The screenshot shows a dialog box titled "Add Allow Authorization Rule" with a blue header bar containing a question mark icon and a red close button. The main content area is light gray and contains the following elements:

- A label "Allow access to this content to:" followed by three radio button options:
 - ☒ All Users
 - ☐ All Anonymous Users
 - ☐ Specified roles or user groups:
 - A text input field with the placeholder text "Example: Admins, Guests".
- ☐ Specified users:
 - A text input field with the placeholder text "Example: User1, User2".
- A section titled "Permissions" with two checkboxes:
 - ☐ Read
 - ☐ Write
- At the bottom right, there are two buttons: "OK" and "Cancel".

6.1 TFTP

- Mặc dù FTP là giao thức truyền tập tin tổng quát nhất trong bộ giao thức TCP/IP, nhưng nó rất phức tạp. Nhiều ứng dụng không cần đến tất cả các tính năng mà FTP cung cấp. Do đó người ta đưa ra một giao thức thứ hai cung cấp dịch vụ ít tốn kém và không phức tạp. Đó chính là TFTP
- **TFTP (Trivial File Transfer Protocol):** “giao thức truyền tập tin tầm thường”
- TFTP không cần chứng thực người dùng

6.1 TFTP

Công dụng của TFTP

- Lúc trước, TFTP được dùng để download boot code (ảnh đĩa) cho các máy trạm không ổ đĩa (diskless workstation) (vài KB code)



- Ngày nay, TFTP hầu như được dùng để download và boot cho các thiết bị mạng (thiết bị truy cập Internet, router, switch, VOIP gateway, ...)

6.2 Các loại thông điệp trong TFTP

Chỉ có 5 loại thông điệp trong TFTP

- RRQ: yêu cầu đọc 1 file (Request To Read a File)
- WRQ: yêu cầu viết 1 file (Request To Write a File)
- DATA: chứa một block dữ liệu file
- ACK: báo nhận được mỗi block DATA
- ERROR: xác định lỗi tác vụ

6.3 Sự khác biệt giữa FTP và TFTP

	FTP	TFTP
Chức năng	Truyền file	Truyền file
Xác thực	Yes	No
Kênh điều khiển & Kênh dữ liệu	Tách rời 2 kênh	Không tách
Giao thức	TCP	UDP
Port	20, 21	69
Truyền dữ liệu	Tin cậy	Không tin cậy

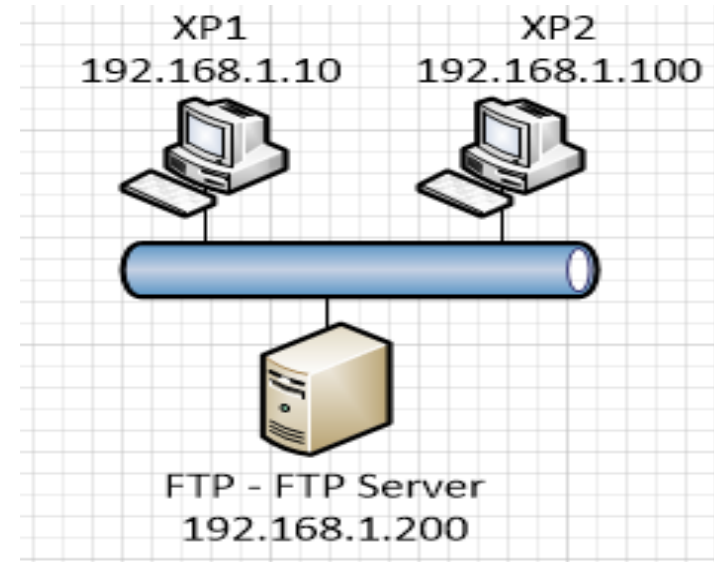
6.4 SFTP

- SFTP (SSH File Transfer Protocol hay Secure File Transfer Protocol) là giao thức trao đổi dữ liệu giữa Server và Client, nhưng dữ liệu được mã hóa.
- SFTP hoạt động dựa trên FTP nhưng có sử dụng SSH để thay thế cho FTP vốn không an toàn.
- Port: 22
- Chạy nhanh hơn FTP do SFTP gộp 2 kênh data và control connection thành 1
- Có thể resume các file download bị ngắt do SFTP truyền, quản lý file dựa trên data stream

Thực hành 1

Hãy xây dựng một FTP Site theo yêu cầu sau:

- Cho phép tài khoản anonymous truy cập vào Server thông qua địa chỉ <ftp://192.168.1.200:21>, người dùng sẽ thấy các tập tin chia sẻ đang để trong thư mục C:\FTPRoot
- Trong cùng một thời điểm chỉ cho phép tối đa 1000 người truy cập.
- Tạo các thông điệp khi đăng nhập “Chuc mot ngay lam viec vui ve” và thông điệp khi thoát ra “Hen gap lai lan sau”.
- Nếu sau khoảng thời gian 150 giây, người dùng đã kết nối với Server mà không tương tác thì hủy kết nối.
- Cắm máy có địa chỉ 192.168.1.100 truy cập vào FTP Site



Thực hành 1

	FTP	XP1	XP2
VMNET	Vmnet2	Vmnet2	Vmnet2
IP	192.168.1.200	192.168.1.10	192.168.1.100
SM	255.255.255.0	255.255.255.0	255.255.255.0

Bảng địa chỉ IP các máy

Thực hành 1

Các bước thực hiện

- Cài đặt bổ sung dịch vụ FTP
- Hiệu chỉnh FTP Site Default
 - ✓ Cho phép tài khoản anonymous được phép truy cập
 - ✓ Chỉ định thư mục gốc của FTP Site
 - ✓ Cấp quyền Read và Write cho FTP Site này
 - ✓ Cho phép tối đa 1000 người truy cập
 - ✓ Tạo thông điệp khi đăng nhập và khi thoát
 - ✓ Sau 150 giây người dùng không tương tác thì hủy kết nối
 - ✓ Cắm máy có IP là 192.168.1.100 truy cập vào FTP Site
- Kiểm tra trên máy Win XP

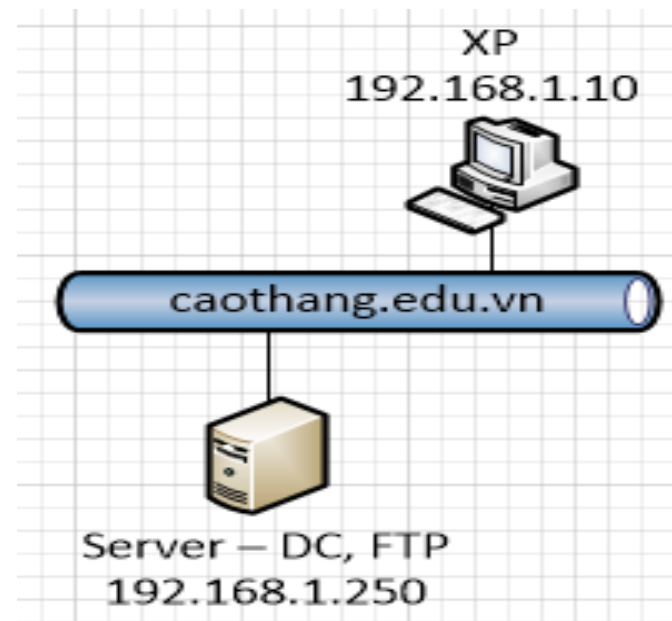
Thực hành 1bis

Chuẩn bị:

- Máy Server làm DC quản lý miền caothang.edu.vn và cài đặt dịch vụ FTP
- Một máy XP

Yêu cầu:

- Cho phép các tài khoản anonymous, sv1, sv2 truy cập vào Server thông qua địa chỉ <ftp://192.168.1.250:21> sẽ thấy các tập tin chia sẻ đang để trong thư mục C:\FTPRoot

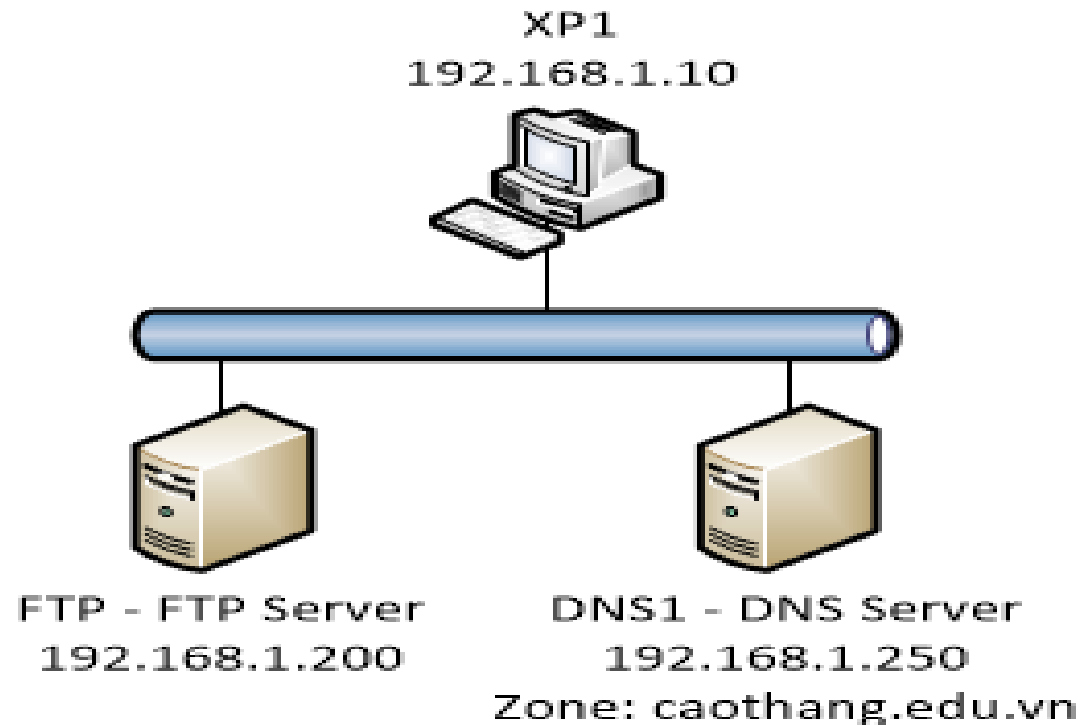


Thực hành 1bis

	Server	XP1
VMNET	Vmnet2	Vmnet2
IP	192.168.1.250	192.168.1.10
SM	255.255.255.0	255.255.255.0
P.DNS	192.168.1.250	192.168.1.250

Bảng địa chỉ IP các máy

Thực hành 2



Hãy cấu hình để khi người dùng đăng nhập vào địa chỉ

<ftp://ftp.caothang.edu.vn> thì thấy các thư mục sau:

Thư mục **Software** ứng với thư mục **C:\Software** trên máy FTP Server

Thư mục **Baocao** ứng với thư mục **C:\Baocao** trên máy FTP Server. Thư mục này không cho phép tài khoản anonymous được truy cập.

Thực hành 2

	FTP	DNS1	XP1
VMNET	Vmnet2	Vmnet2	Vmnet2
IP	192.168.1.200	192.168.1.250	192.168.1.10
SM	255.255.255.0	255.255.255.0	255.255.255.0
P.DNS	192.168.1.250	192.168.1.250	192.168.1.250

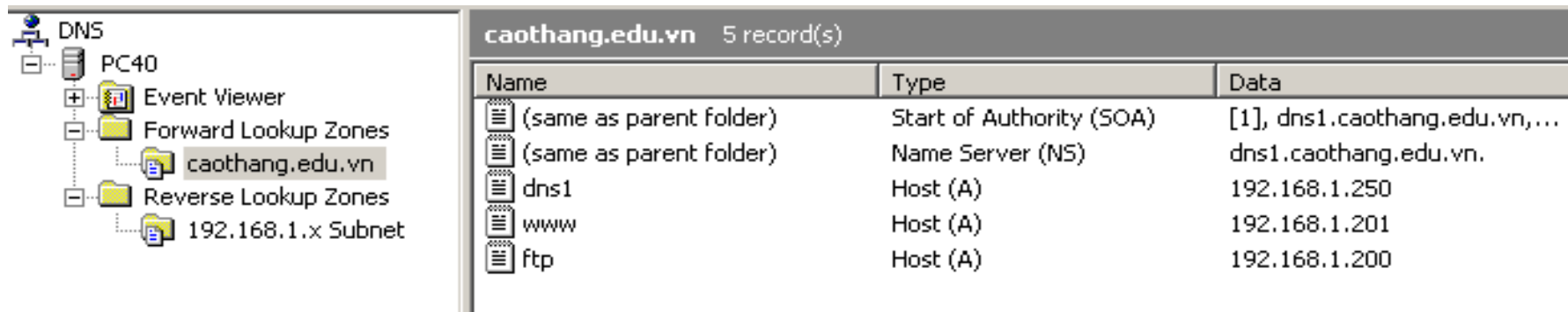
Bảng địa chỉ IP các máy

Hướng dẫn thực hành 2

Gợi ý:

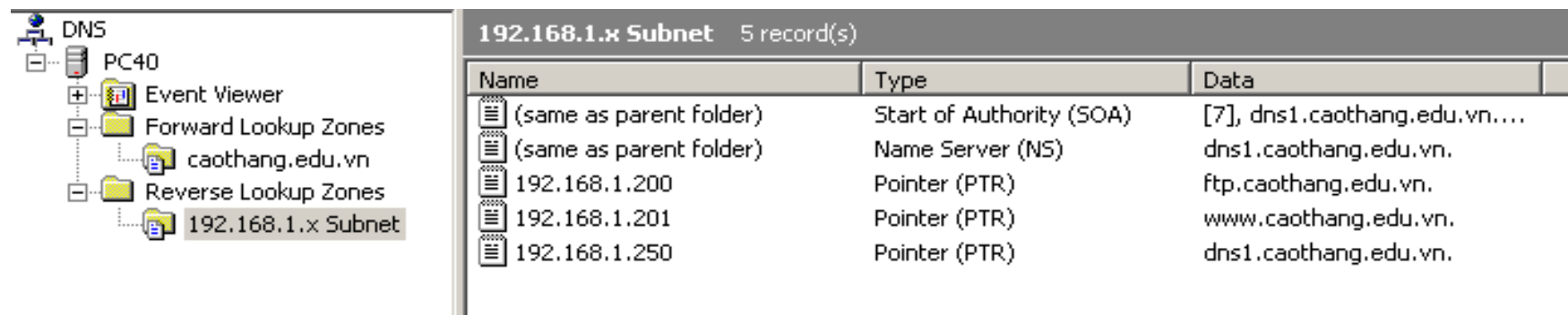
- Cấu hình trên DNS Server để có thể phân giải tên <ftp.caothang.edu.vn> thành địa chỉ IP của FTP Server.
- Tạo Virtual Directory với tên ánh xạ là Software và thư mục gốc là C:\Software.
- Tạo Virtual Directory với tên ánh xạ là Baocao và thư mục gốc là C:\Baocao. Tài khoản anonymous không được đăng nhập Virtual Directory này.

Hướng dẫn thực hành 2



The screenshot shows the DNS console on a PC40. The left pane displays the hierarchy: DNS > Forward Lookup Zones > caothang.edu.vn. The right pane shows the records for the caothang.edu.vn zone, which contains 5 records. The records are listed in a table with columns Name, Type, and Data.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], dns1.caothang.edu.vn,...
(same as parent folder)	Name Server (NS)	dns1.caothang.edu.vn.
dns1	Host (A)	192.168.1.250
www	Host (A)	192.168.1.201
ftp	Host (A)	192.168.1.200

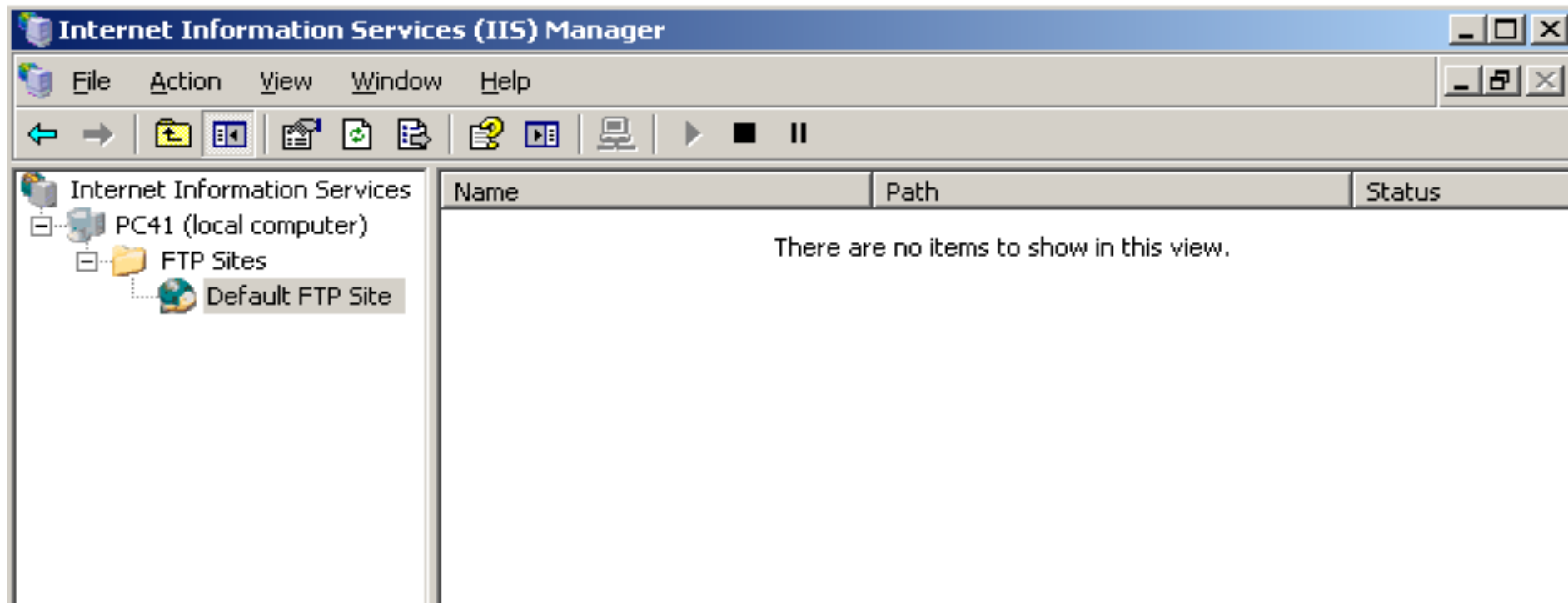


The screenshot shows the DNS console on a PC40. The left pane displays the hierarchy: DNS > Forward Lookup Zones > 192.168.1.x Subnet. The right pane shows the records for the 192.168.1.x Subnet zone, which contains 5 records. The records are listed in a table with columns Name, Type, and Data.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[7], dns1.caothang.edu.vn....
(same as parent folder)	Name Server (NS)	dns1.caothang.edu.vn.
192.168.1.200	Pointer (PTR)	ftp.caothang.edu.vn.
192.168.1.201	Pointer (PTR)	www.caothang.edu.vn.
192.168.1.250	Pointer (PTR)	dns1.caothang.edu.vn.

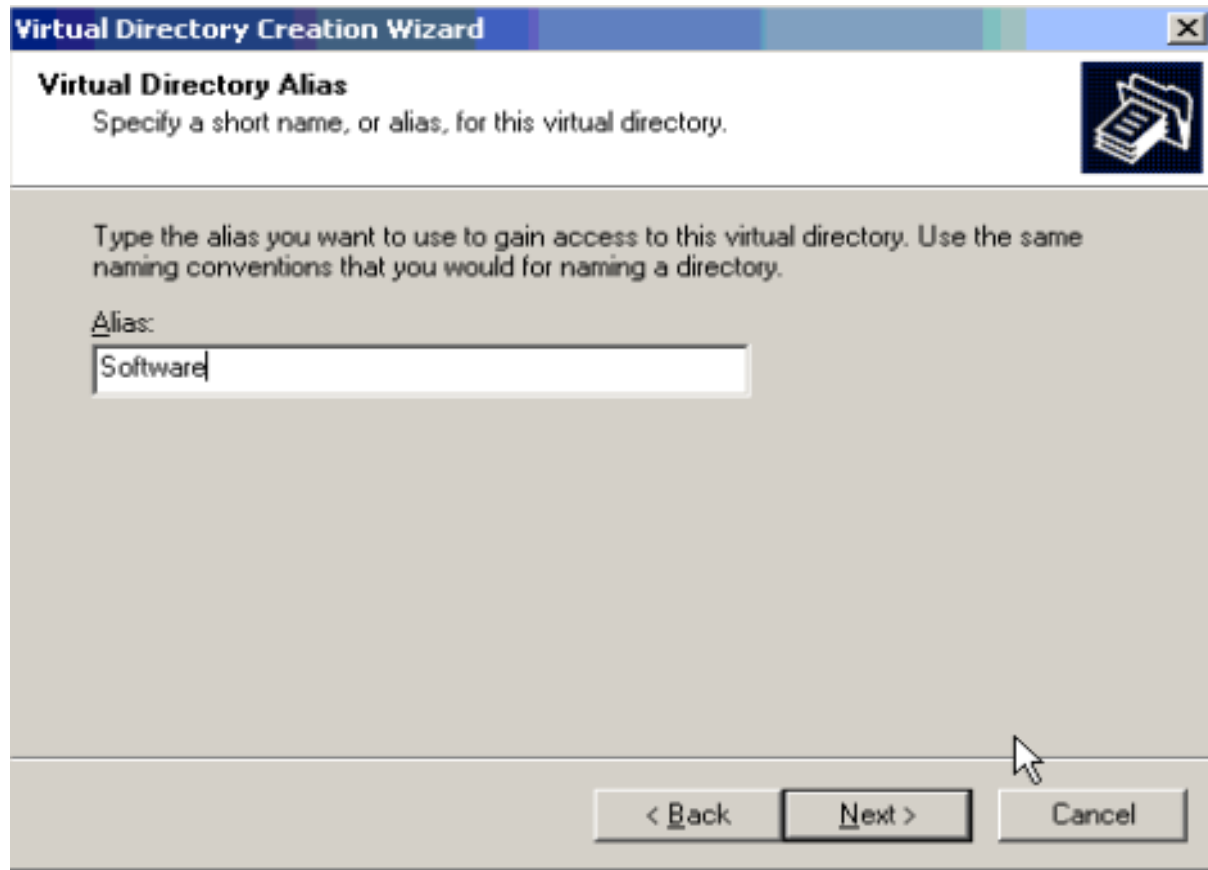
Trên DNS1, cài đặt và cấu hình dịch vụ DNS.

Hướng dẫn thực hành 2



Trên FTP, cài đặt và cấu hình dịch vụ FTP như trong bài thực hành 1.

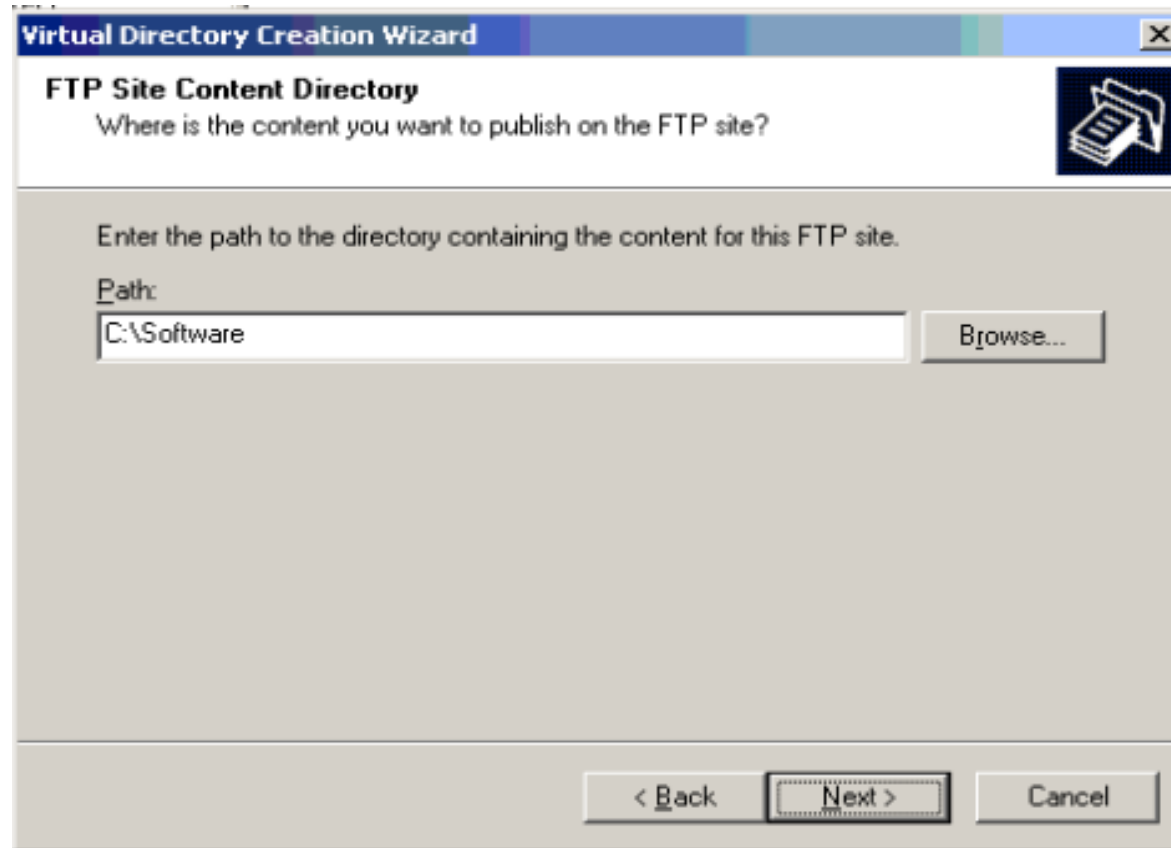
Hướng dẫn thực hành 2



Trên FTP, tạo Virtual Directory với tên ánh xạ Software.

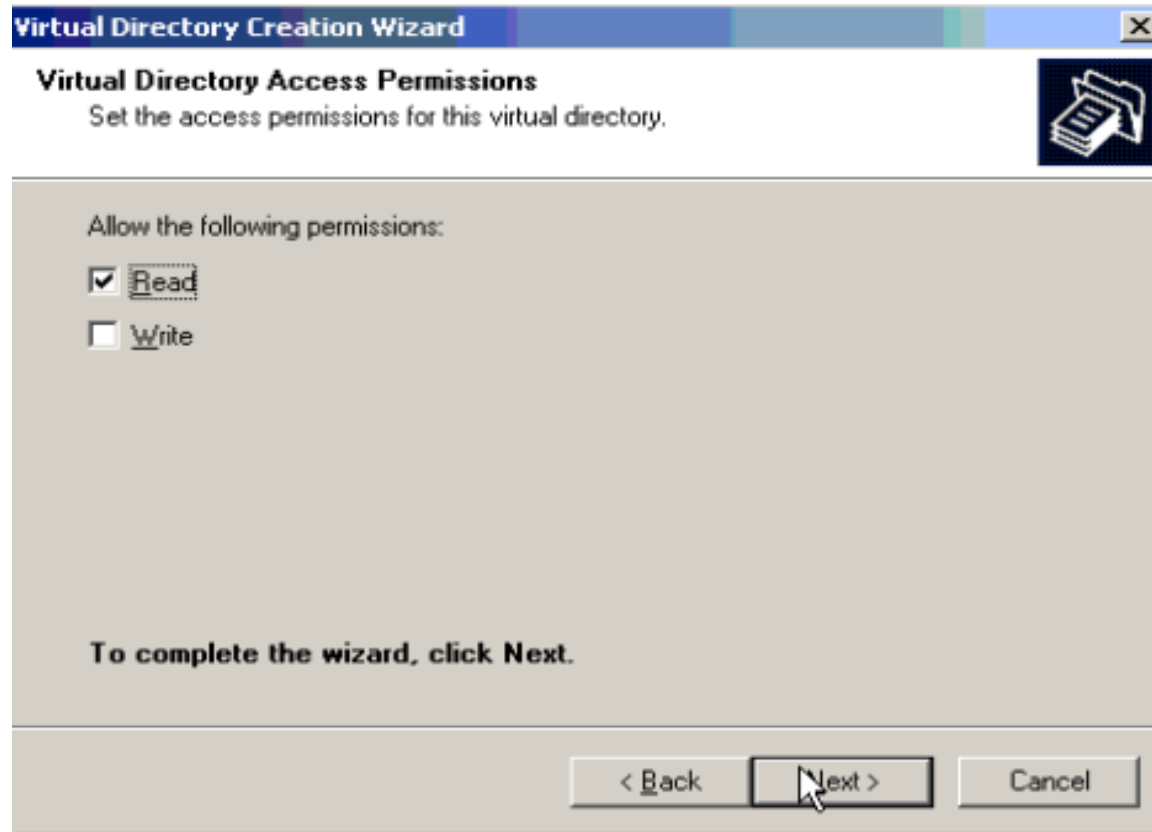
Click chuột phải Default FTP Site, chọn New, Virtual Directory. Nhập tên Alias là Software

Hướng dẫn thực hành 2



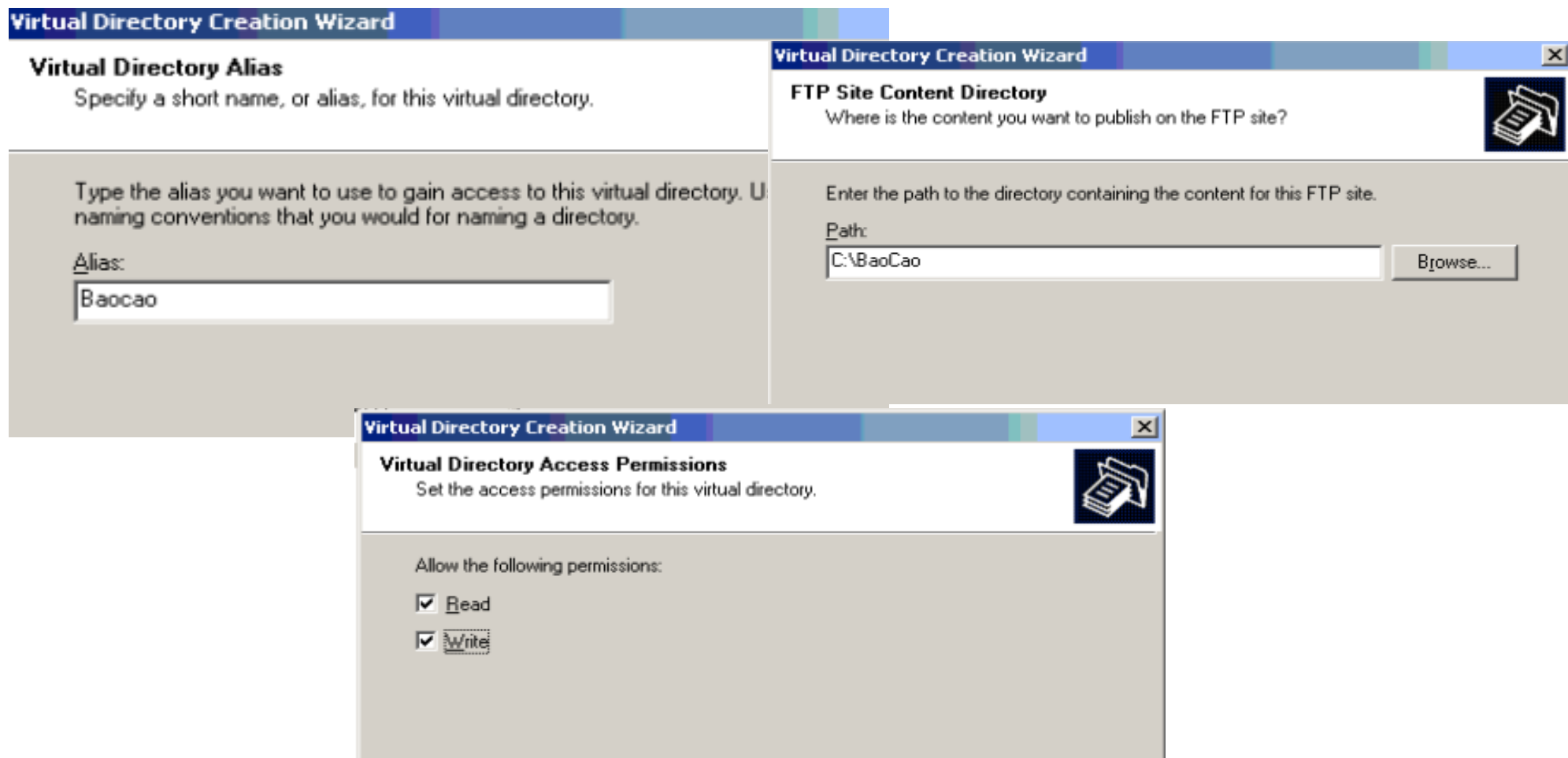
Trên FTP, chỉ đường dẫn đến thư mục C:\Software

Hướng dẫn thực hành 2



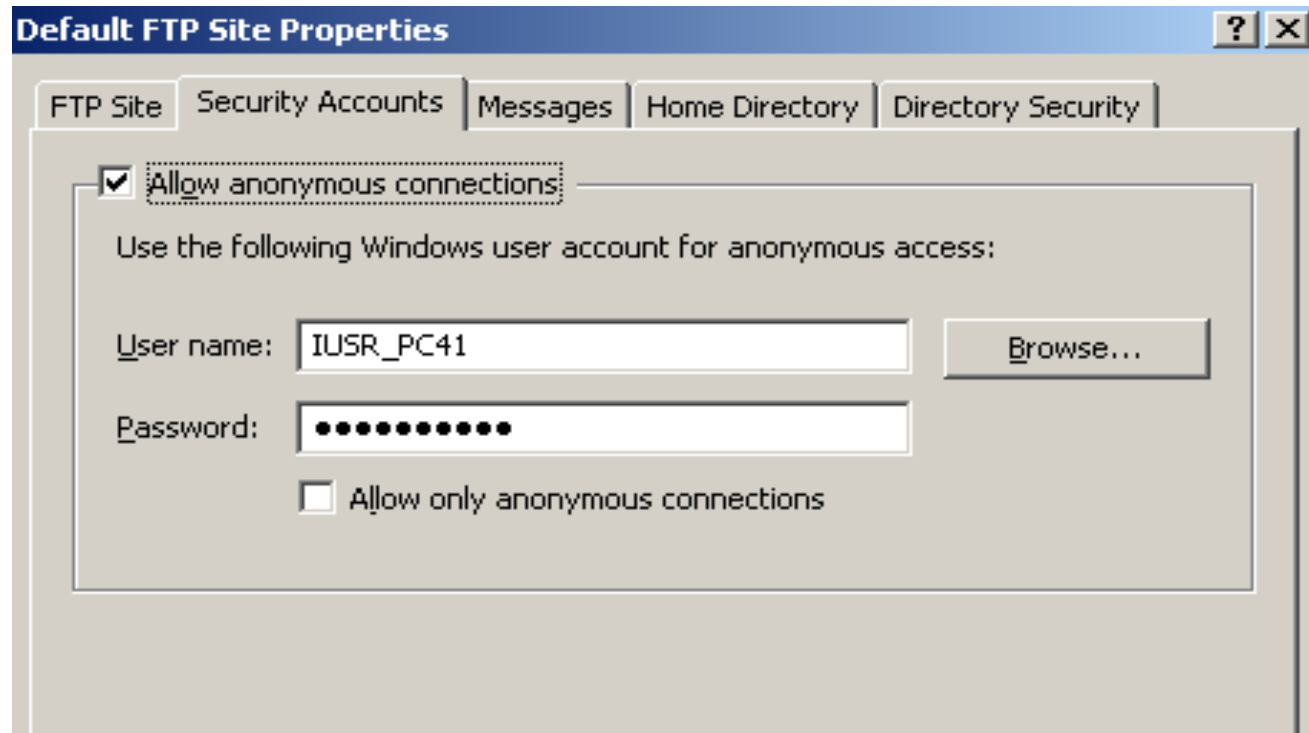
Trên FTP, chỉ cấp quyền Read

Hướng dẫn thực hành 2



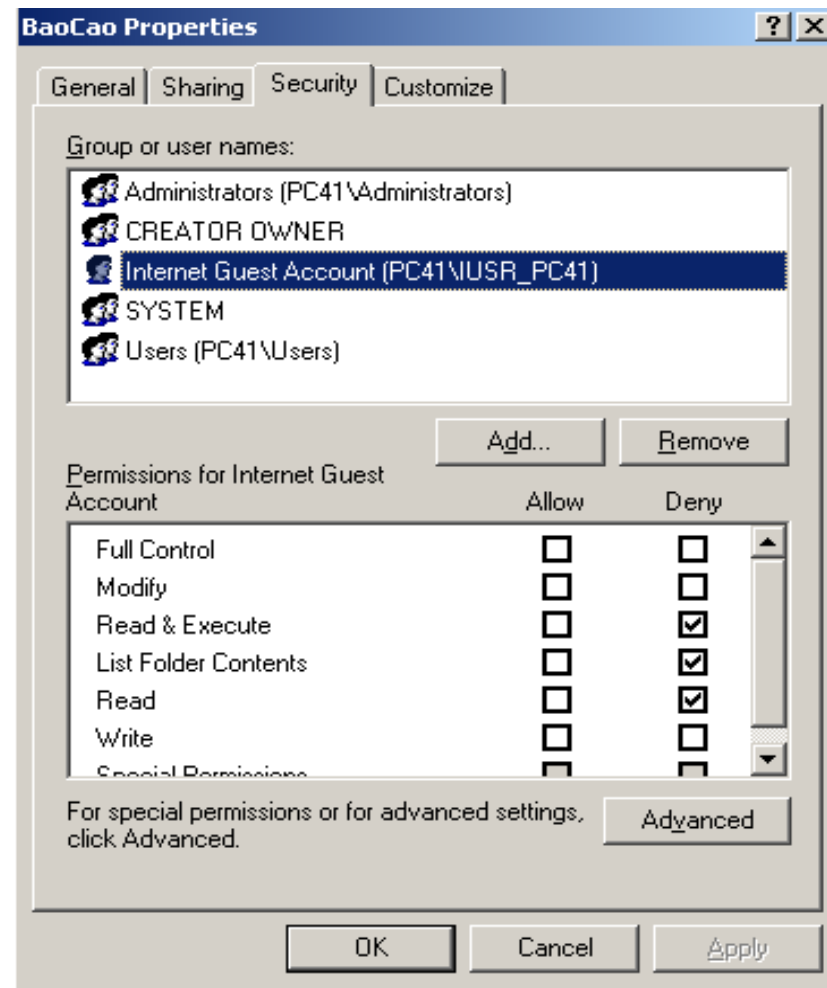
Trên FTP, làm tương tự với Virtual Directory với tên ánh xạ Baocao. Cấp quyền Read và Write cho Virtual Directory này.

Hướng dẫn thực hành 2



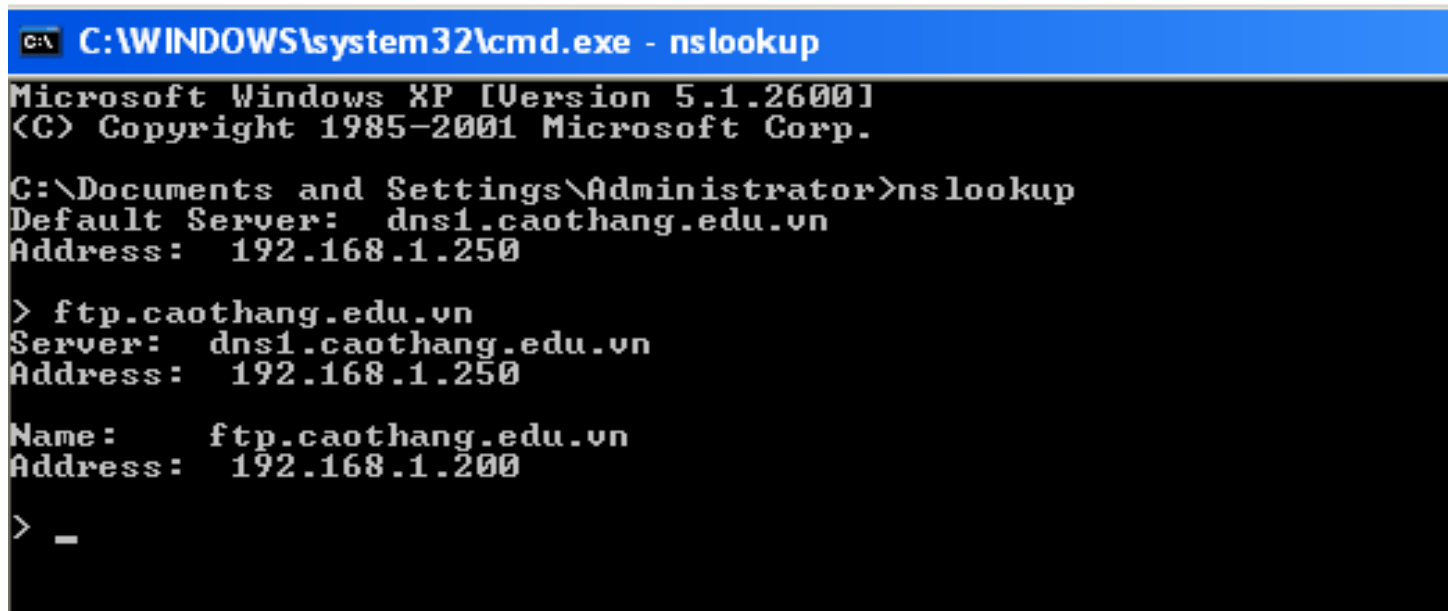
Trên FTP, xác định tên user đăng nhập bằng anonymous. Click chuột phải vào Default FTP Site, chọn Properties, vào tab Security Accounts

Hướng dẫn thực hành 2



Trên FTP, không cho anonymous truy cập vào Virtual Directory Baocao.

Hướng dẫn thực hành 2



```
C:\ C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>nslookup
Default Server:  dns1.caothang.edu.vn
Address:  192.168.1.250

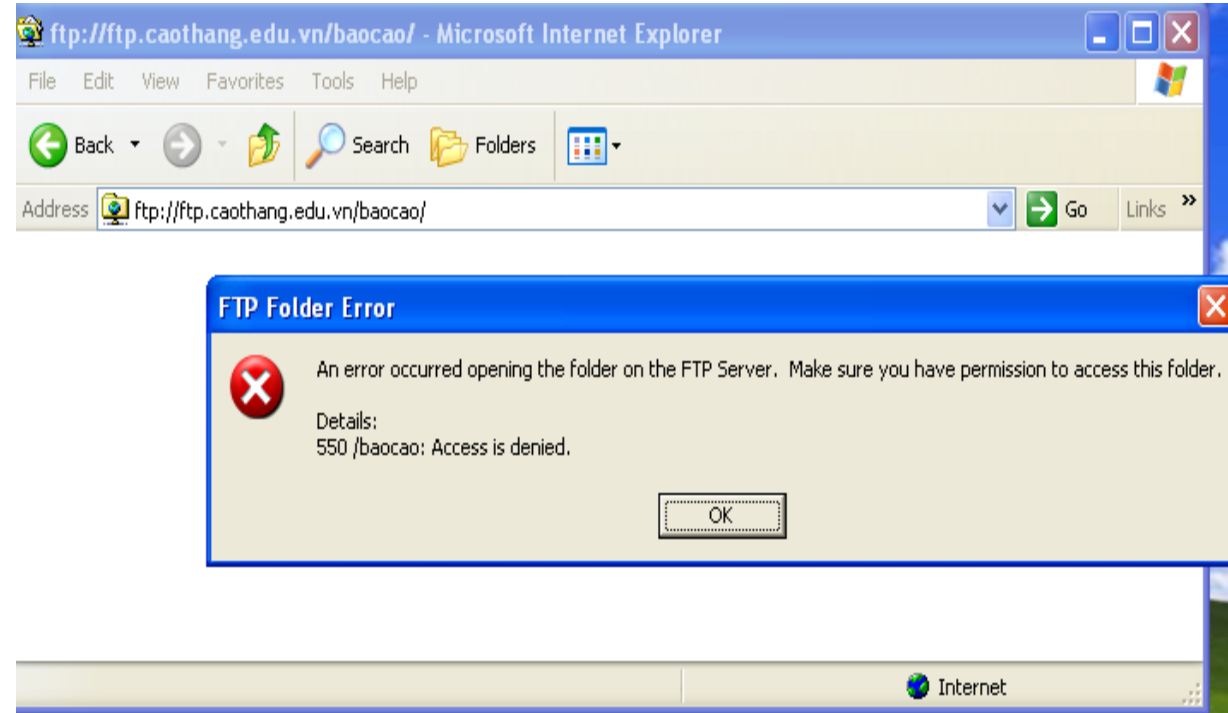
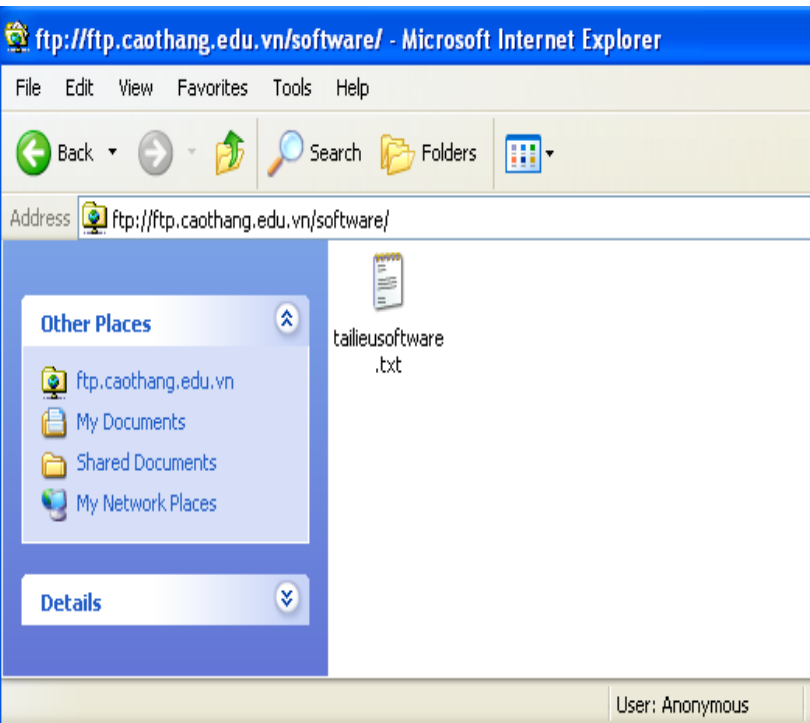
> ftp.caothang.edu.vn
Server:  dns1.caothang.edu.vn
Address:  192.168.1.250

Name:    ftp.caothang.edu.vn
Address:  192.168.1.200

> _
```

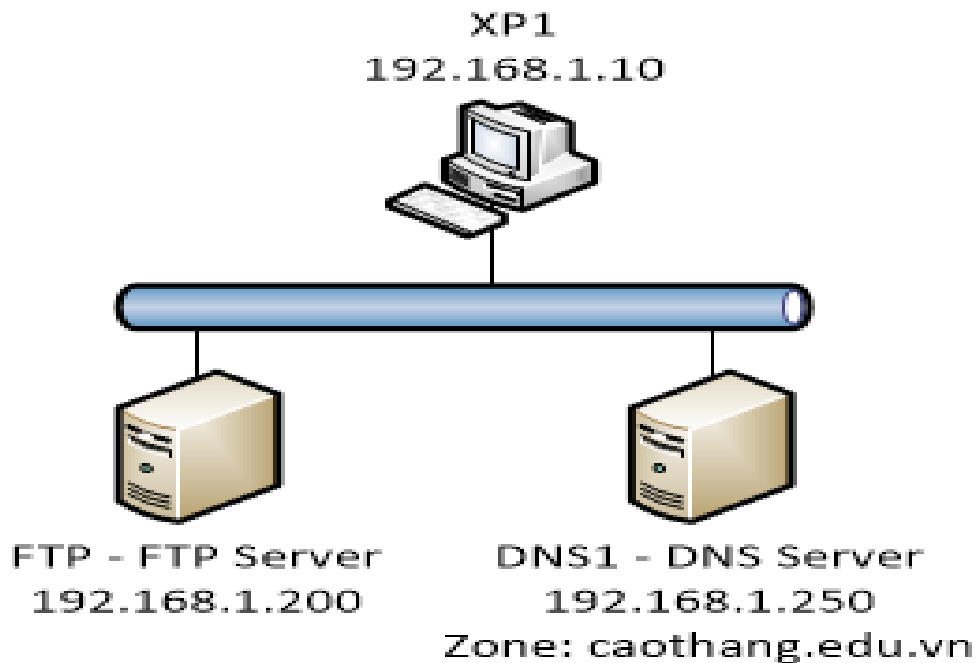
Trên XP, kiểm tra phân giải tên miền ftp. caothang.edu.vn.

Hướng dẫn thực hành 2



Trên XP, đăng nhập bằng anonymous vào software thành công. Nhưng đăng nhập vào baocao báo lỗi không có quyền.

Thực hành 3



Cho mô hình mạng như hình. Hãy thêm một FTP Site theo yêu cầu sau:

- Thư mục gốc là C:\FTPRoot
- Chỉ cho phép các user anonymous, administrator, sv1, sv2, gv được phép truy cập.
- Mỗi người vào một thư mục khác nhau, đồng thời được phép thay đổi nội dung trong thư mục đó.
- Mọi người sẽ truy cập vào FTP Server theo địa chỉ

`ftp://ftp.caothang.edu.vn`

Thực hành 3

	FTP	DNS1	XP1
VMNET	Vmnet2	Vmnet2	Vmnet2
IP	192.168.1.200	192.168.1.250	192.168.1.10
SM	255.255.255.0	255.255.255.0	255.255.255.0
P.DNS	192.168.1.250	192.168.1.250	192.168.1.250

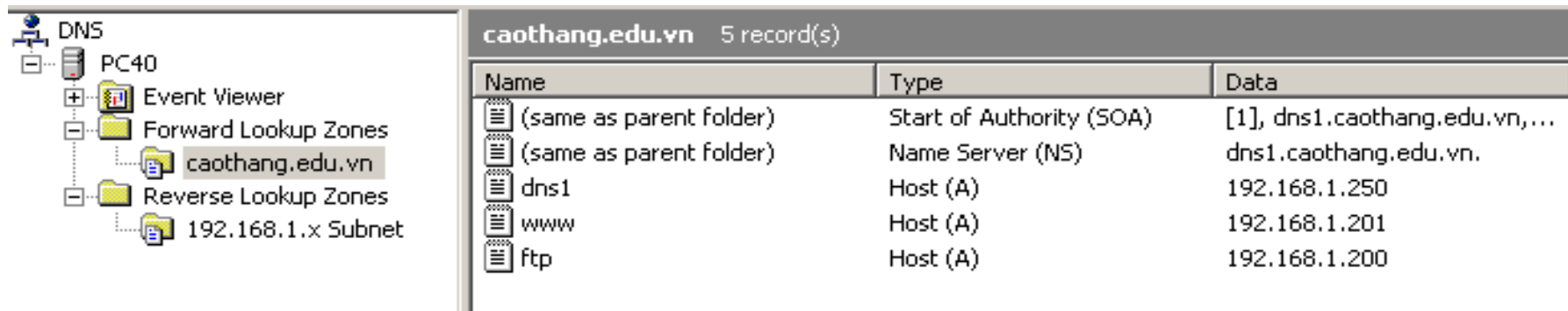
Bảng địa chỉ IP các máy

Hướng dẫn thực hành 3

Bước thực hiện

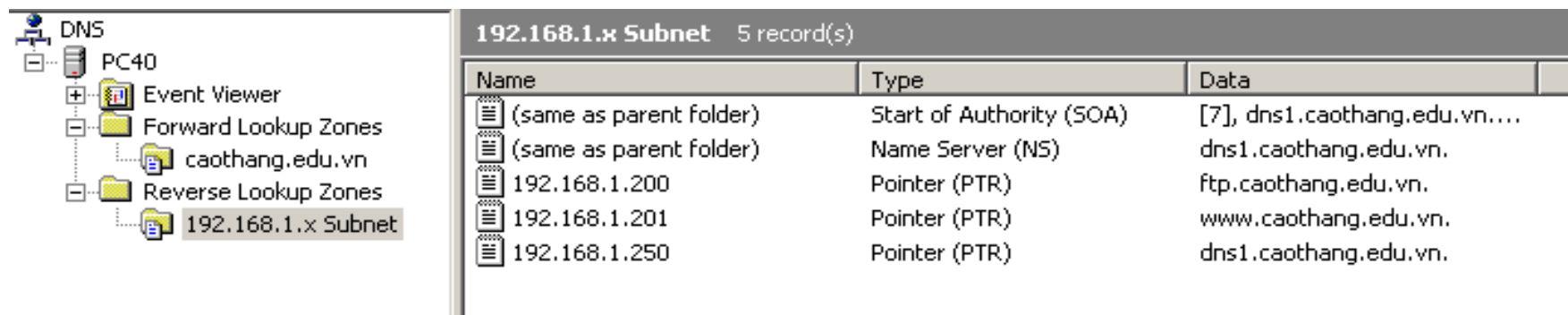
1. Cấu hình DNS để phân giải tên miền <ftp.caothang.edu.vn> thành địa chỉ IP 192.168.1.200 của máy FTP Server.
2. Tạo FTP Site theo kiểu **isolate users**, cho quyền read và write trong quá trình tạo FTP Site.
3. Tạo home directory cho các tài khoản anonymous, sv1, sv2, gv.

Hướng dẫn thực hành 3



The screenshot shows the DNS console on a PC40. The left pane displays the hierarchy: DNS > Forward Lookup Zones > caothang.edu.vn. The right pane shows the records for the caothang.edu.vn zone, which contains 5 records.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], dns1.caothang.edu.vn,...
(same as parent folder)	Name Server (NS)	dns1.caothang.edu.vn.
dns1	Host (A)	192.168.1.250
www	Host (A)	192.168.1.201
ftp	Host (A)	192.168.1.200

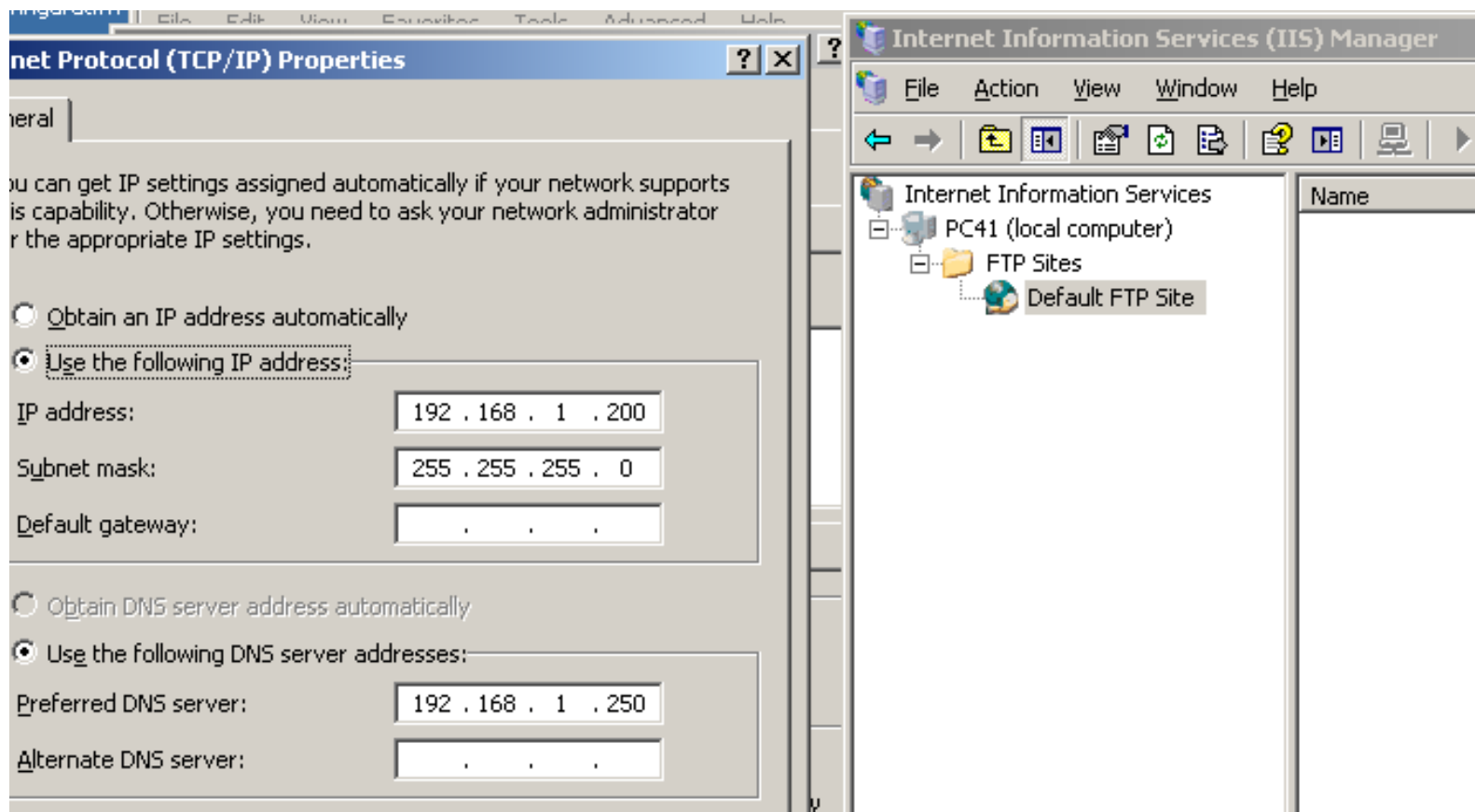


The screenshot shows the DNS console on a PC40. The left pane displays the hierarchy: DNS > Forward Lookup Zones > 192.168.1.x Subnet. The right pane shows the records for the 192.168.1.x Subnet zone, which contains 5 records.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[7], dns1.caothang.edu.vn....
(same as parent folder)	Name Server (NS)	dns1.caothang.edu.vn.
192.168.1.200	Pointer (PTR)	ftp.caothang.edu.vn.
192.168.1.201	Pointer (PTR)	www.caothang.edu.vn.
192.168.1.250	Pointer (PTR)	dns1.caothang.edu.vn.

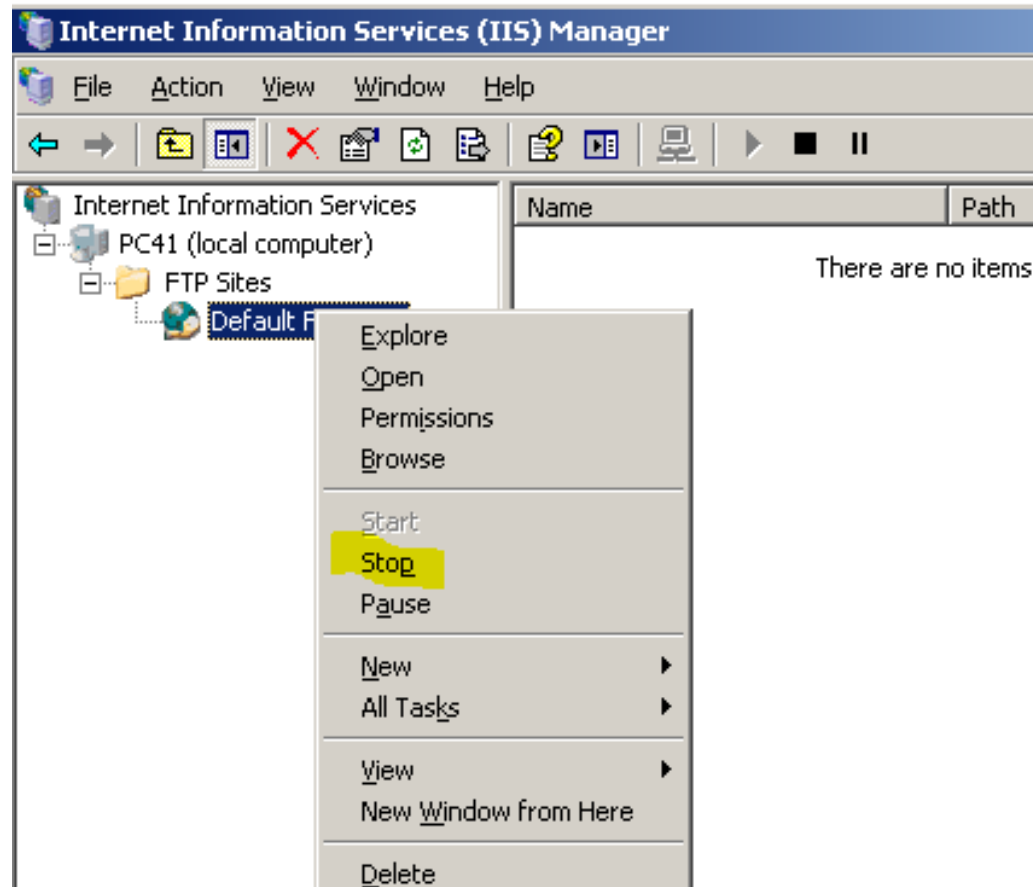
Trên DNS1, cài đặt và cấu hình dịch vụ DNS

Hướng dẫn thực hành 3



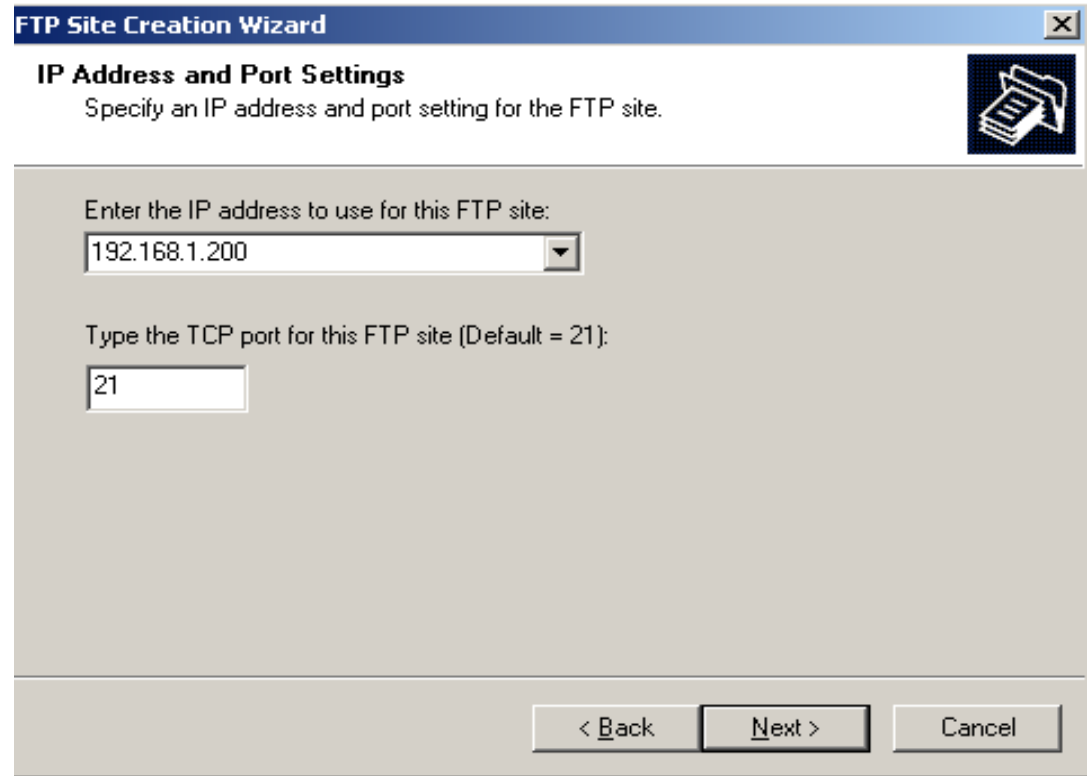
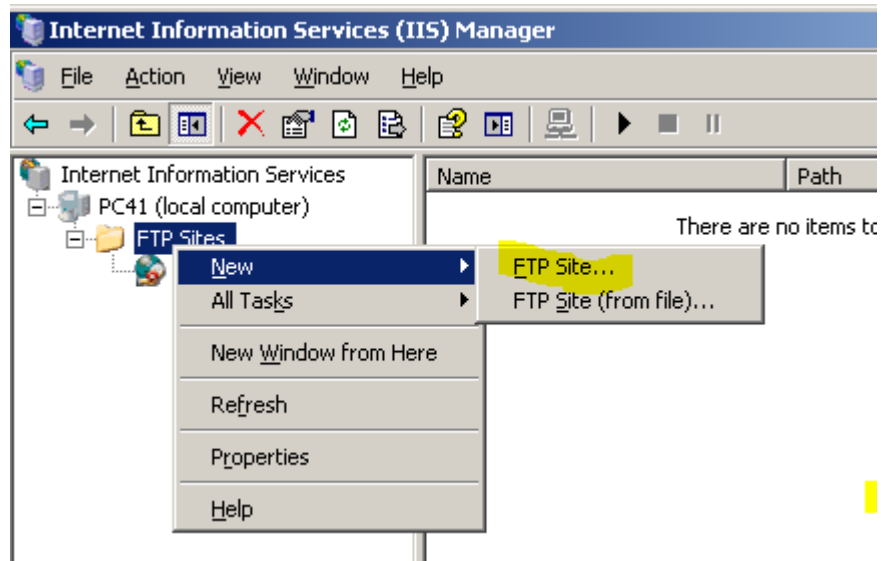
Trên FTP, đặt IP và cài đặt dịch vụ FTP

Hướng dẫn thực hành 3



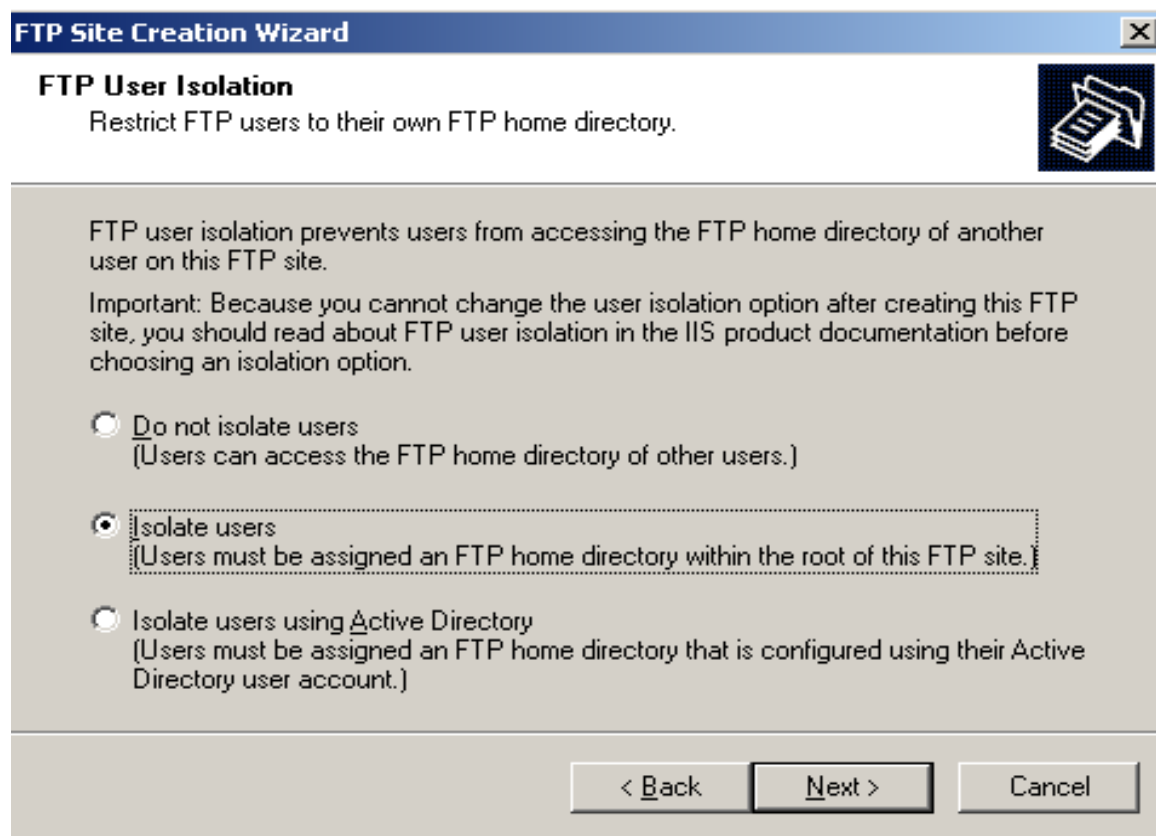
Trên FTP, stop Default FTP Site. Click phải vào Default FTP Site, chọn Stop

Hướng dẫn thực hành 3



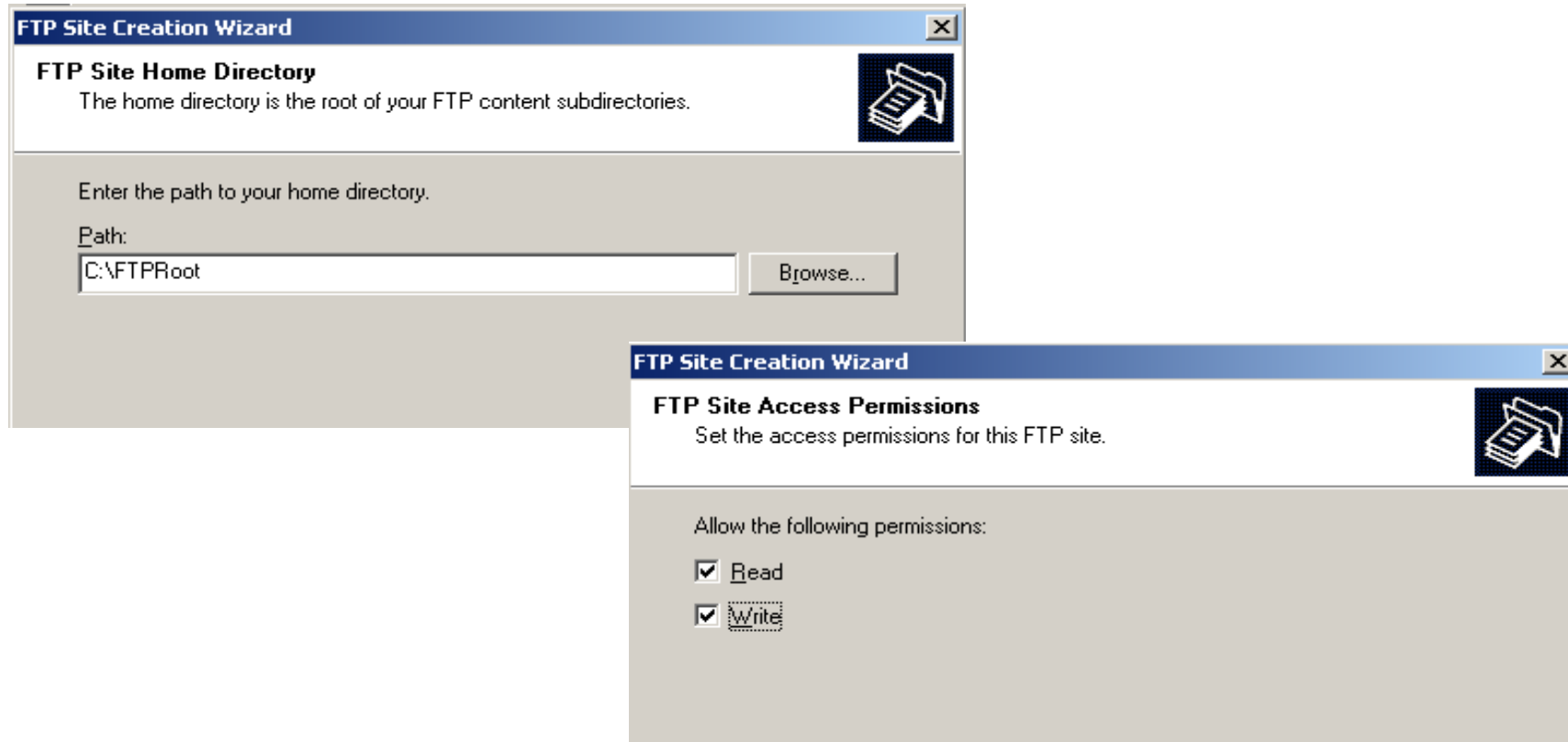
Trên FTP, tạo mới FTP Site: click chuột phải FTP Sites, chọn New \ FTP Site... Nhập Description là FTPSite2 và nhập địa chỉ IP để sử dụng cho FTPSite2 này.

Hướng dẫn thực hành 3



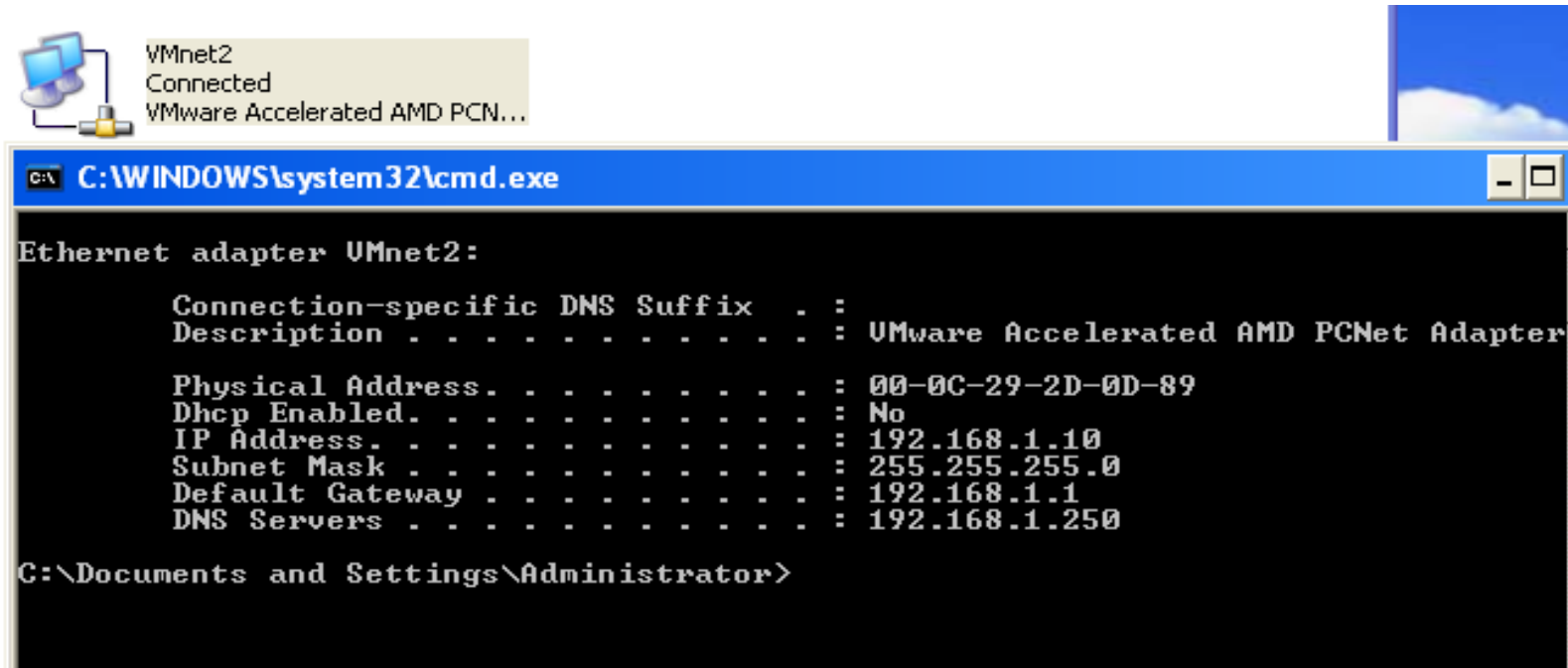
Trên FTP, chọn Isolate users.

Hướng dẫn thực hành 3



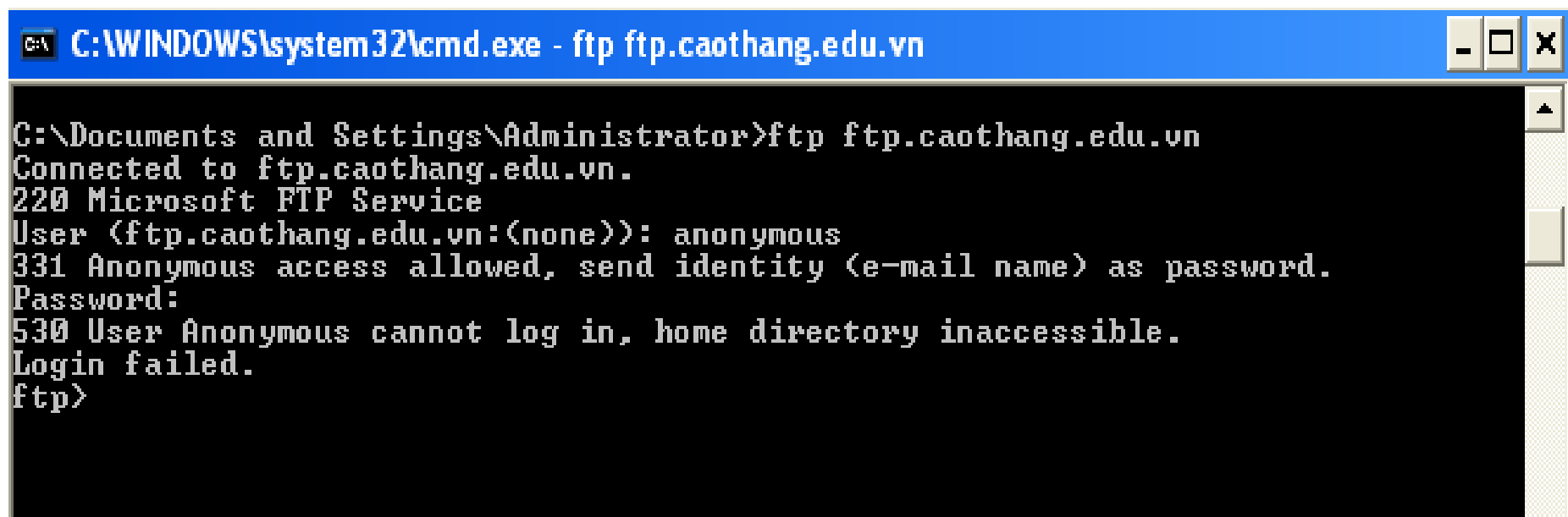
Trên FTP, chọn đường dẫn đến thư mục C:\FTPRoot và cấp quyền Read và Write.

Hướng dẫn thực hành 3



Trên XP, đặt IP.

Hướng dẫn thực hành 3

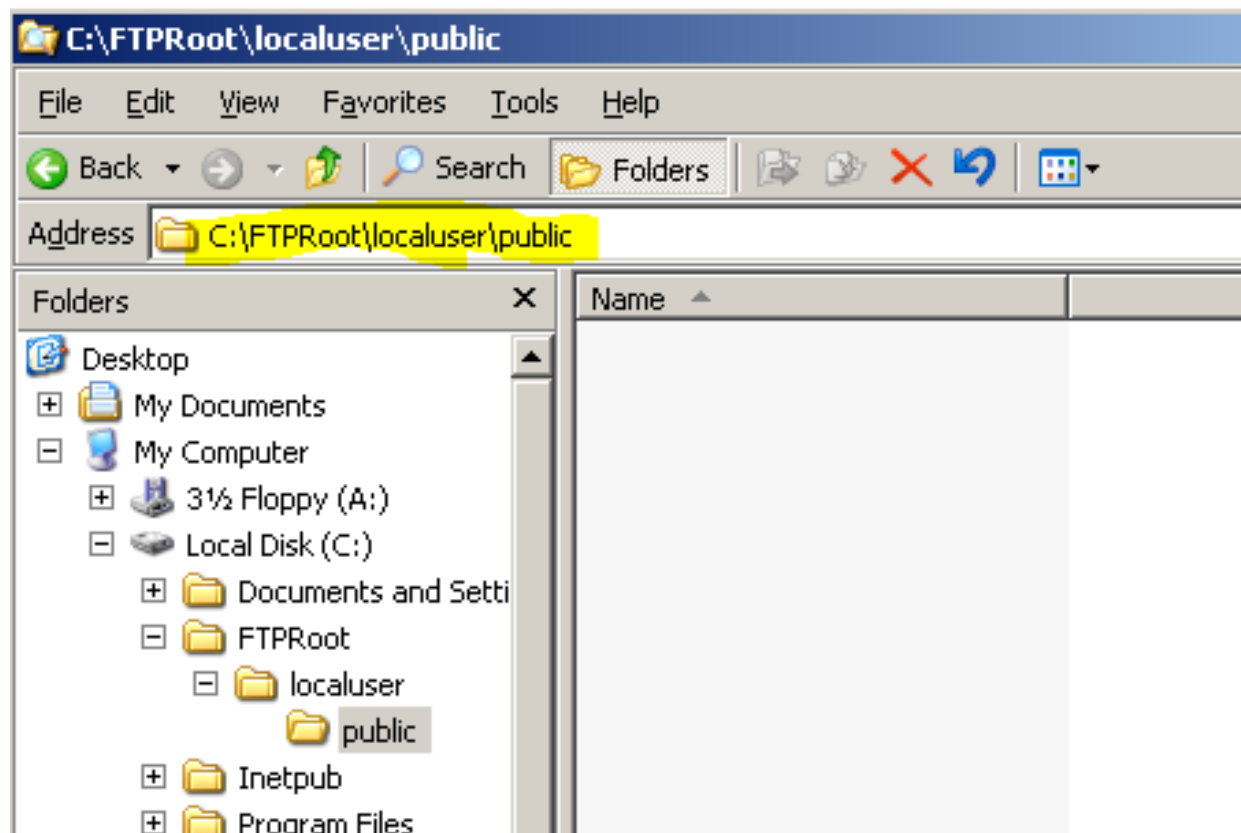


```
C:\WINDOWS\system32\cmd.exe - ftp ftp.caothang.edu.vn

C:\Documents and Settings\Administrator>ftp ftp.caothang.edu.vn
Connected to ftp.caothang.edu.vn.
220 Microsoft FTP Service
User (ftp.caothang.edu.vn:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
530 User Anonymous cannot log in, home directory inaccessible.
Login failed.
ftp>
```

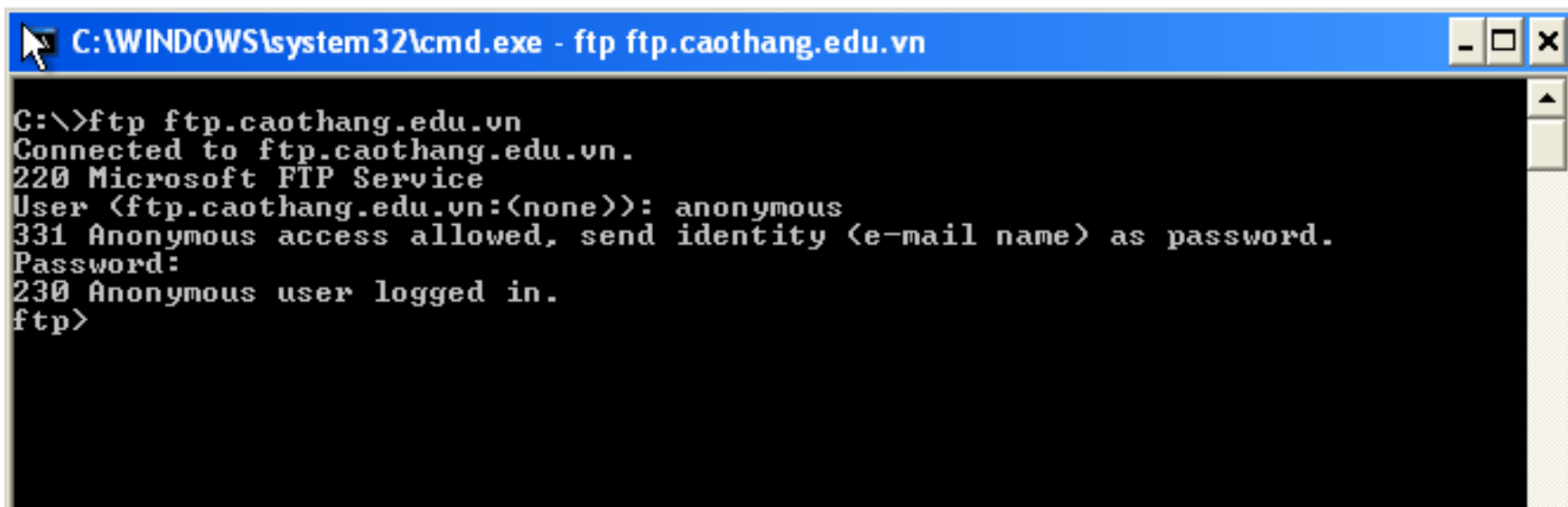
Trên XP, truy cập vào [ftp.caothang.edu.vn](ftp://ftp.caothang.edu.vn) bằng anonymous. Đăng nhập thất bại.

Hướng dẫn thực hành 3



Trên FTP, tạo thư mục và tập tin ở đường dẫn là
C:\FTPRoot\localuser\public

Hướng dẫn thực hành 3

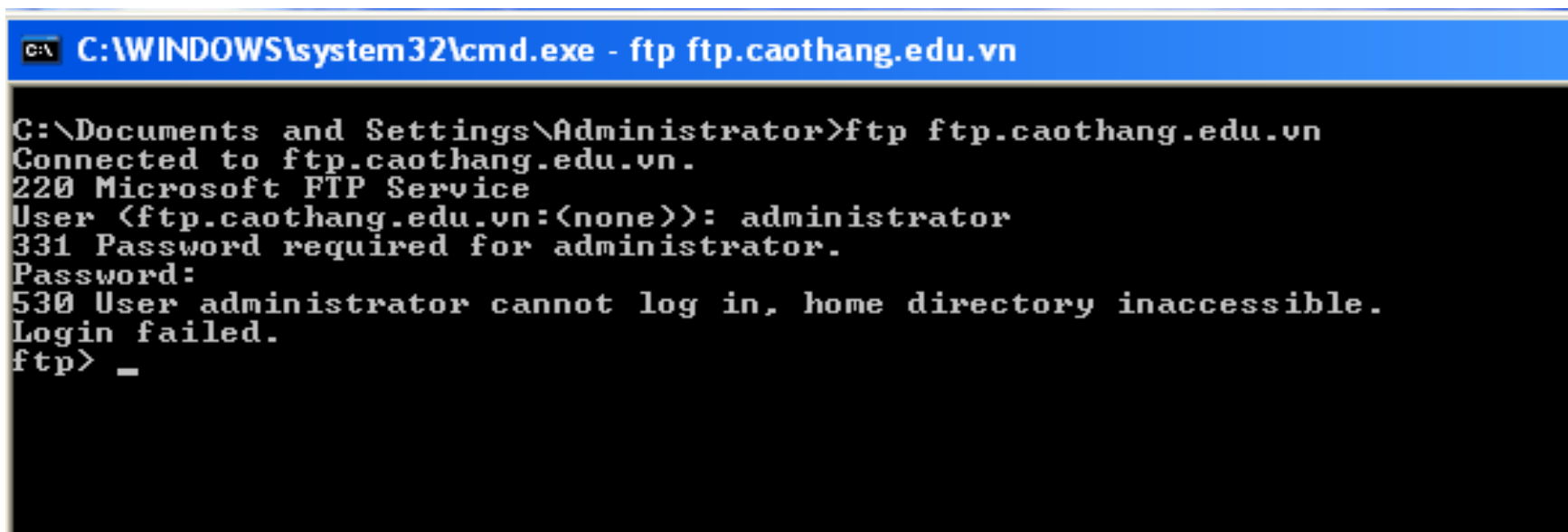


```
C:\WINDOWS\system32\cmd.exe - ftp ftp.caothang.edu.vn

C:\>ftp ftp.caothang.edu.vn
Connected to ftp.caothang.edu.vn.
220 Microsoft FTP Service
User (ftp.caothang.edu.vn:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

Trên XP, đăng nhập lại anonymous. Đăng nhập thành công.

Hướng dẫn thực hành 3

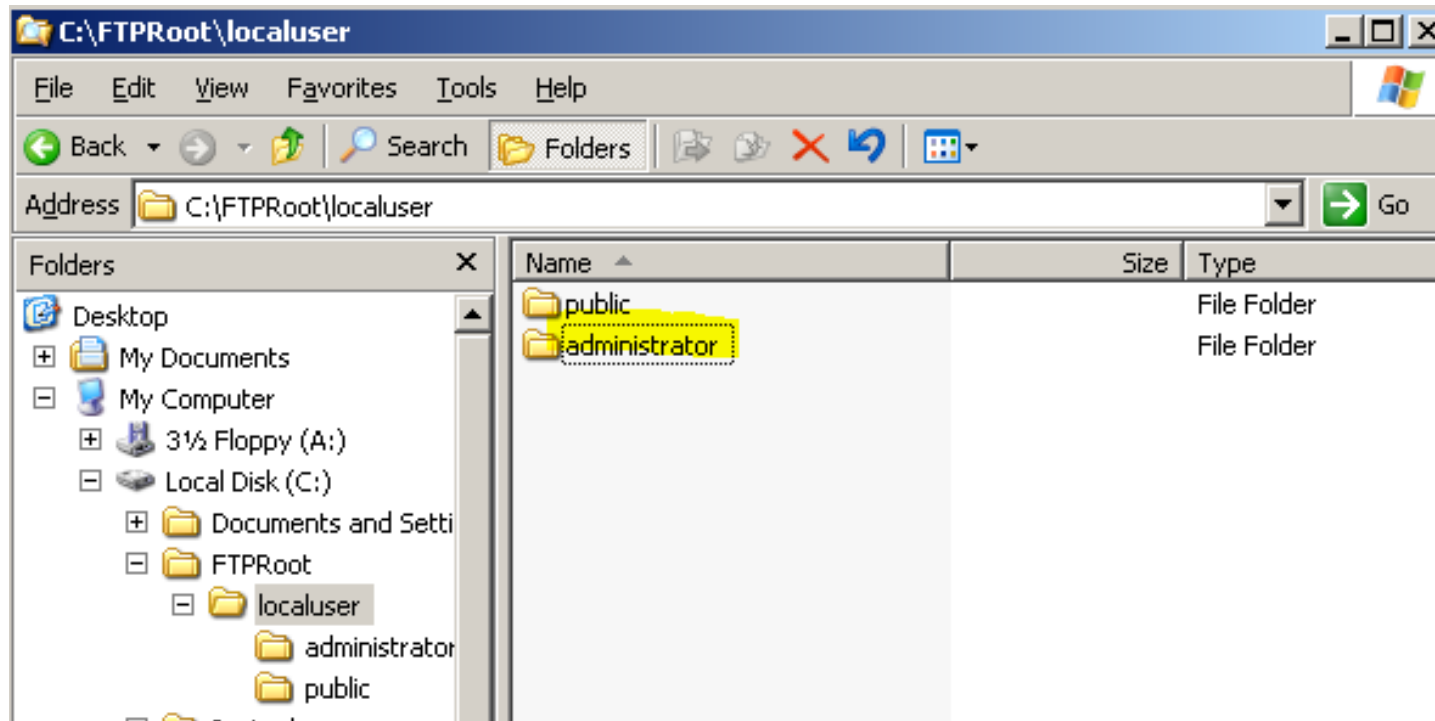


```
C:\WINDOWS\system32\cmd.exe - ftp ftp.caothang.edu.vn

C:\Documents and Settings\Administrator>ftp ftp.caothang.edu.vn
Connected to ftp.caothang.edu.vn.
220 Microsoft FTP Service
User (ftp.caothang.edu.vn:(none)): administrator
331 Password required for administrator.
Password:
530 User administrator cannot log in, home directory inaccessible.
Login failed.
ftp> _
```

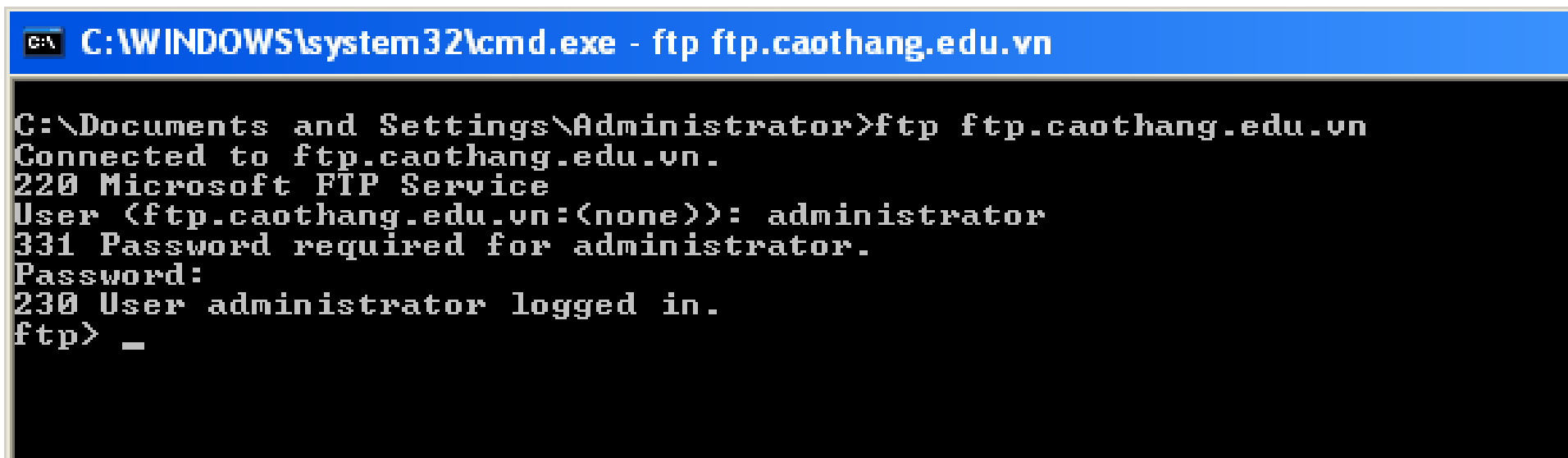
Trên XP, đăng nhập bằng tài khoản administrator. Đăng nhập thất bại.
(set password cho administrator trên máy FTP là 123)

Hướng dẫn thực hành 3



Trên XP, tạo thư mục C:\FTPRoot\Localuser\administrator

Hướng dẫn thực hành 3

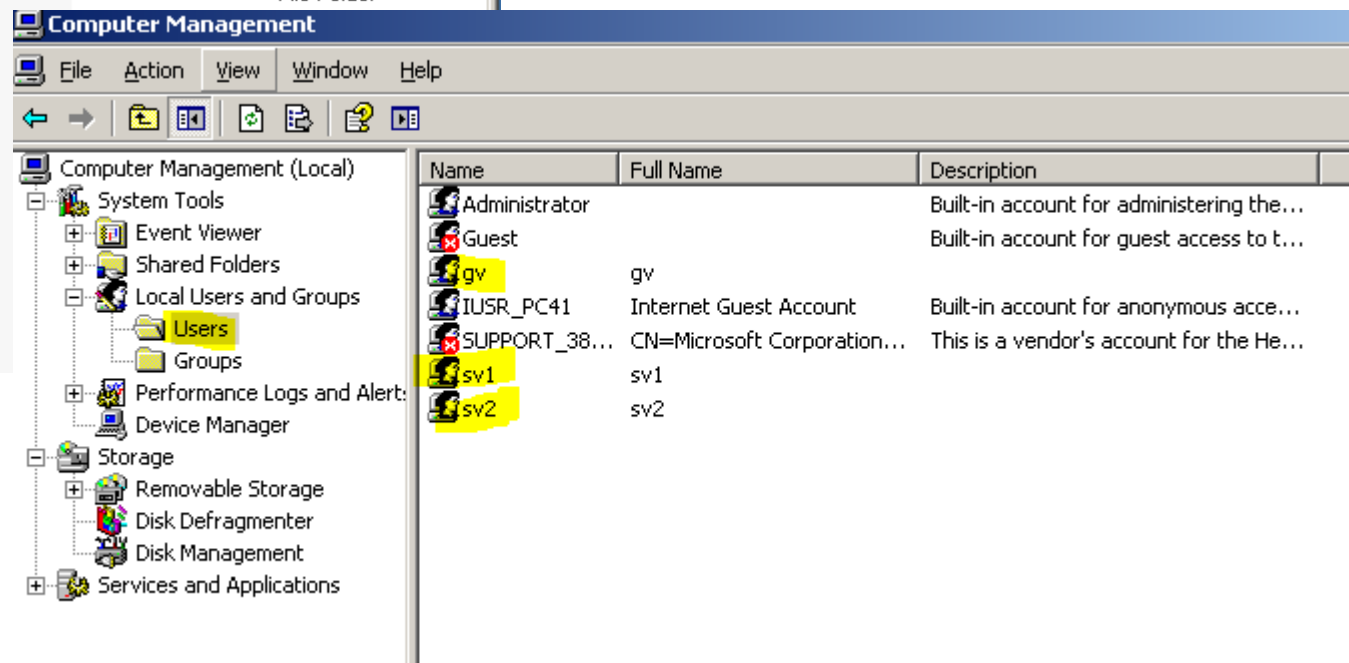
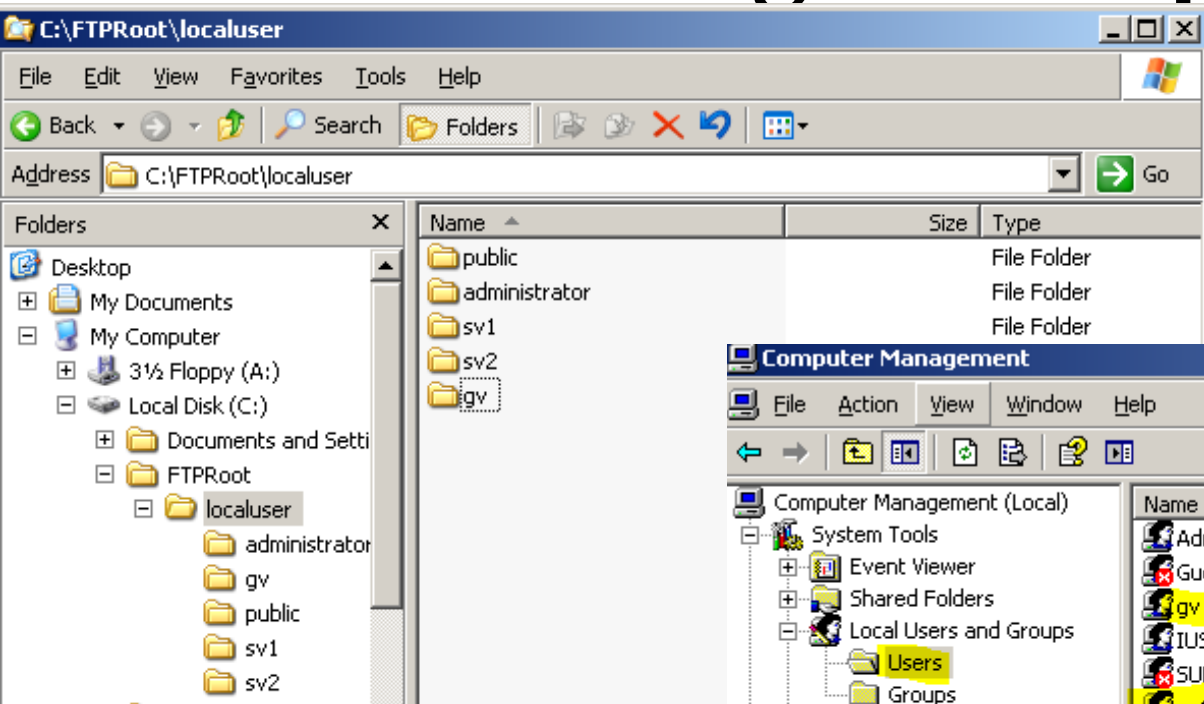


```
C:\WINDOWS\system32\cmd.exe - ftp ftp.caothang.edu.vn

C:\Documents and Settings\Administrator>ftp ftp.caothang.edu.vn
Connected to ftp.caothang.edu.vn.
220 Microsoft FTP Service
User (ftp.caothang.edu.vn:(none)): administrator
331 Password required for administrator.
Password:
230 User administrator logged in.
ftp> _
```

Trên XP, đăng nhập lại tài khoản administrator. Đăng nhập thành công.

Hướng dẫn thực hành 3



Trên FTP, tạo các thư mục để đăng nhập trên XP. Tạo các user trùng tên với tên các thư mục vừa tạo

Hướng dẫn thực hành 3

```
C:\WINDOWS\system32\cmd.exe - ftp ftp.caothang.edu.vn

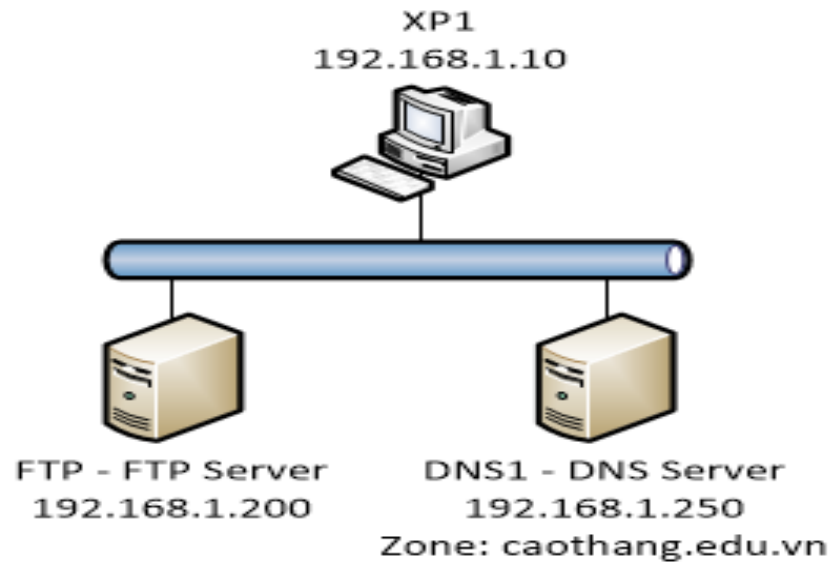
C:\>ftp ftp.caothang.edu.vn
Connected to ftp.caothang.edu.vn.
220 Microsoft FTP Service
User (ftp.caothang.edu.vn:(none)): sv1
331 Password required for sv1.
Password:
230 User sv1 logged in.
ftp> bye
221

C:\>ftp ftp.caothang.edu.vn
Connected to ftp.caothang.edu.vn.
220 Microsoft FTP Service
User (ftp.caothang.edu.vn:(none)): sv2
331 Password required for sv2.
Password:
230 User sv2 logged in.
ftp> bye
221

C:\>ftp ftp.caothang.edu.vn
Connected to ftp.caothang.edu.vn.
220 Microsoft FTP Service
User (ftp.caothang.edu.vn:(none)): gv
331 Password required for gv.
Password:
230 User gv logged in.
ftp> _
```

Trên XP, đăng nhập vào các tài khoản sv1, sv2, gv đều thành công.

Thực hành 4



Cho mô hình mạng như hình. Hãy thêm một FTP Site theo yêu cầu sau:

- Thư mục gốc là C:\FTPRoot
- Chỉ cho phép các user sv1, sv2, gv được phép truy cập.
- Mỗi user sv1, sv2 có quyền Read, Write trong một thư mục của mình. Còn user gv được phép vào bất kỳ thư mục trong FTP Root và có quyền Read, Write
- Mọi người sẽ truy cập vào FTP Server 2012 theo địa chỉ ftp://ftp.caothang.edu.vn

Thực hành 4

	FTP	DNS1	XP1
VMNET	Vmnet2	Vmnet2	Vmnet2
IP	192.168.1.200	192.168.1.250	192.168.1.10
SM	255.255.255.0	255.255.255.0	255.255.255.0
P.DNS	192.168.1.250	192.168.1.250	192.168.1.250

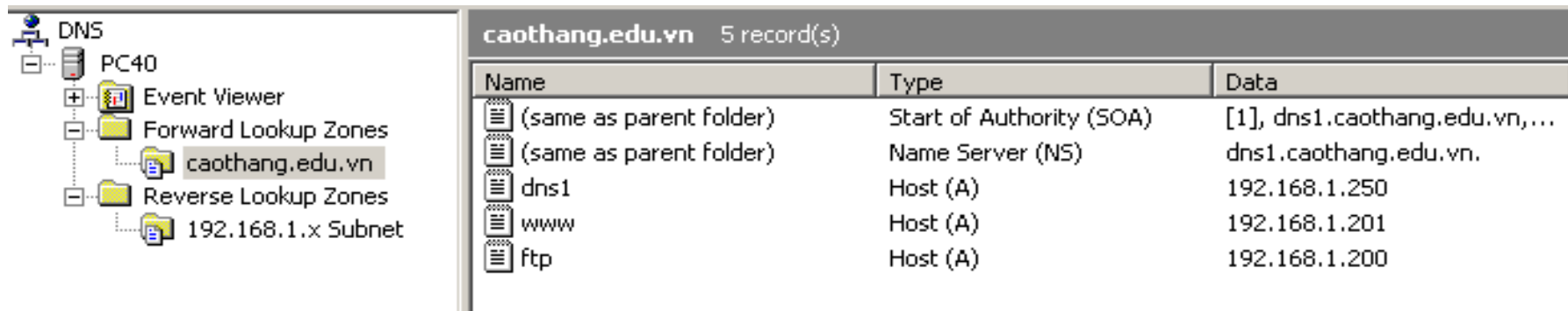
Bảng địa chỉ IP các máy

Hướng dẫn thực hành 4

Bước thực hiện

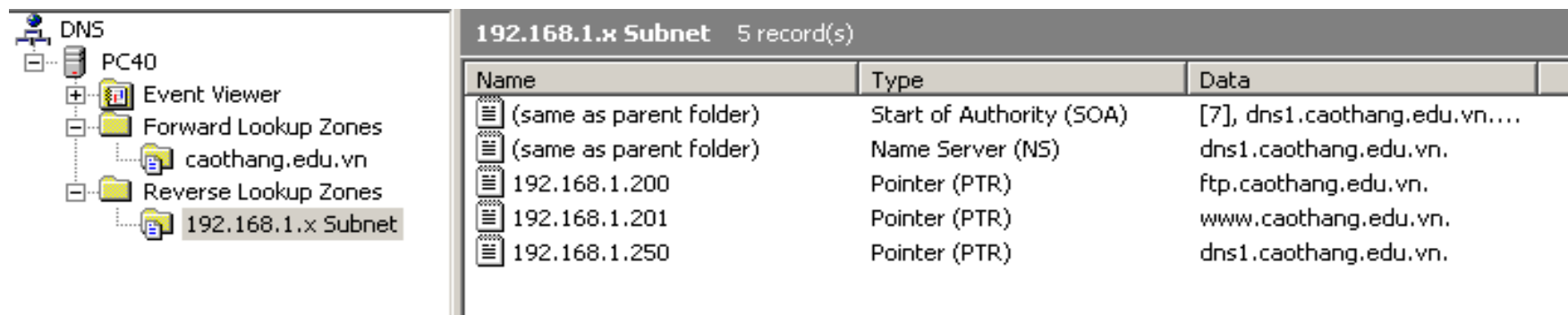
1. Cấu hình DNS để phân giải tên miền <ftp.caothang.edu.vn> thành địa chỉ IP 192.168.1.200 của máy FTP Server.
2. Tạo FTP Site theo kiểu **isolate users**, cho quyền read và write trong quá trình tạo FTP Site cho các user sv1, sv2 trong mỗi thư mục của mình, còn user gv được quyền read, write cho FTP Root.

Hướng dẫn thực hành 4



The screenshot shows the DNS console on a PC. The left pane displays the hierarchy: DNS > PC40 > Forward Lookup Zones > caothang.edu.vn. The right pane shows the records for caothang.edu.vn, which has 5 records.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], dns1.caothang.edu.vn,...
(same as parent folder)	Name Server (NS)	dns1.caothang.edu.vn.
dns1	Host (A)	192.168.1.250
www	Host (A)	192.168.1.201
ftp	Host (A)	192.168.1.200

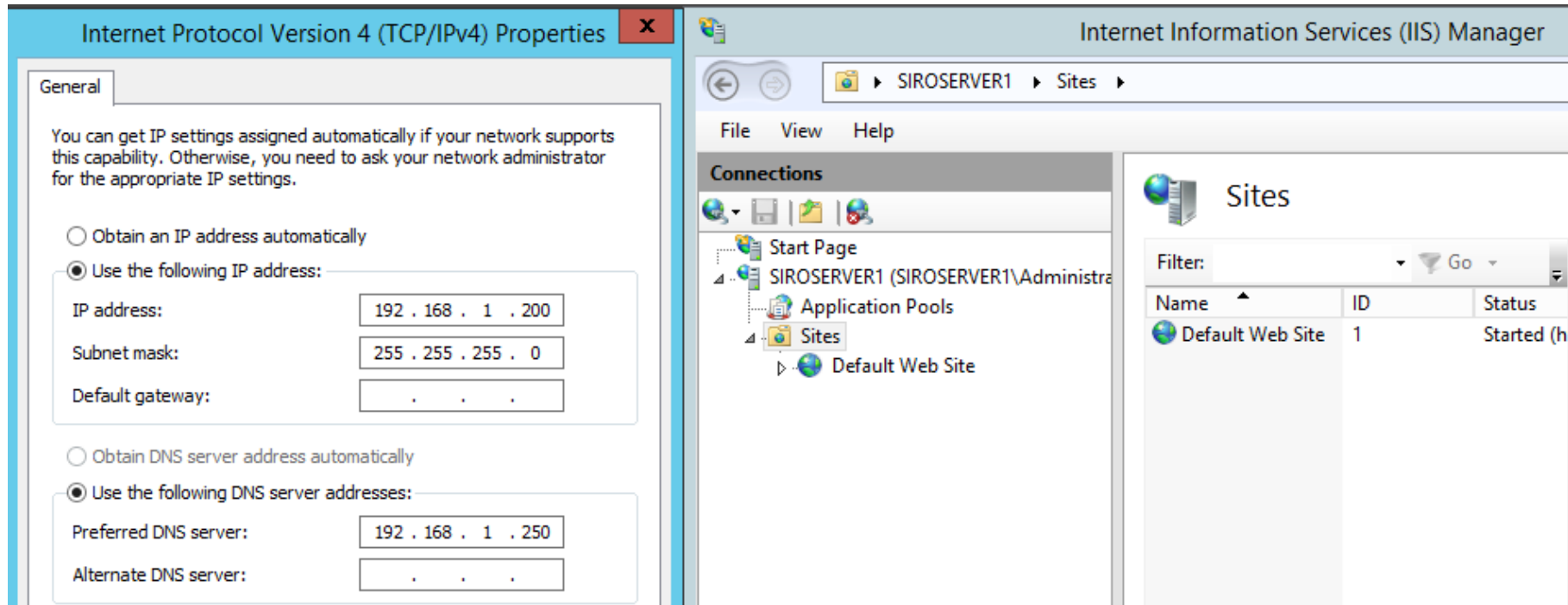


The screenshot shows the DNS console on a PC. The left pane displays the hierarchy: DNS > PC40 > Reverse Lookup Zones > 192.168.1.x Subnet. The right pane shows the records for 192.168.1.x Subnet, which has 5 records.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[7], dns1.caothang.edu.vn,...
(same as parent folder)	Name Server (NS)	dns1.caothang.edu.vn.
192.168.1.200	Pointer (PTR)	ftp.caothang.edu.vn.
192.168.1.201	Pointer (PTR)	www.caothang.edu.vn.
192.168.1.250	Pointer (PTR)	dns1.caothang.edu.vn.

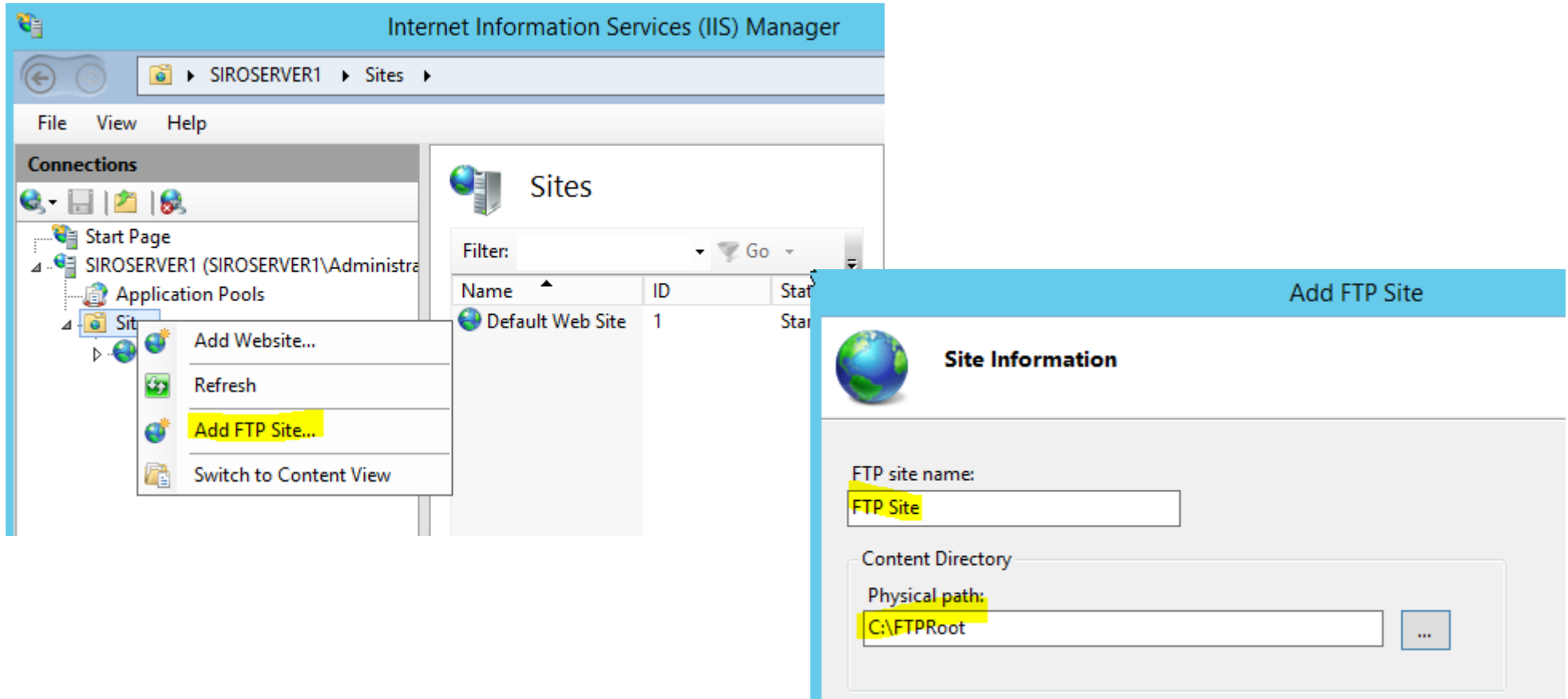
Trên DNS1, cài đặt và cấu hình dịch vụ DNS

Hướng dẫn thực hành 4



Trên FTP, đặt IP và cài đặt dịch vụ FTP

Hướng dẫn thực hành 4



Trên FTP, thêm mới một FTP Site. Click phải vào Sites chọn Add FTP Site. Nhập tên FTP site và đường dẫn C:\FTPRoot đã tạo trên ổ cứng

Hướng dẫn thực hành 4

The image displays two screenshots of the 'Add FTP Site' wizard in Windows Server.

Left Screenshot: Binding and SSL Settings

- Binding:**
 - IP Address: All Unassigned (dropdown)
 - Port: 21
 - ☐ Enable Virtual Host Names:
 - Virtual Host (example: ftp.contoso.com):
- ☒ Start FTP site automatically
- SSL:**
 - ☒ No SSL (highlighted)
 - ☐ Allow SSL
 - ☐ Require SSL
 - SSL Certificate: Not Selected (dropdown) [Select...]

Buttons: Previous, Next

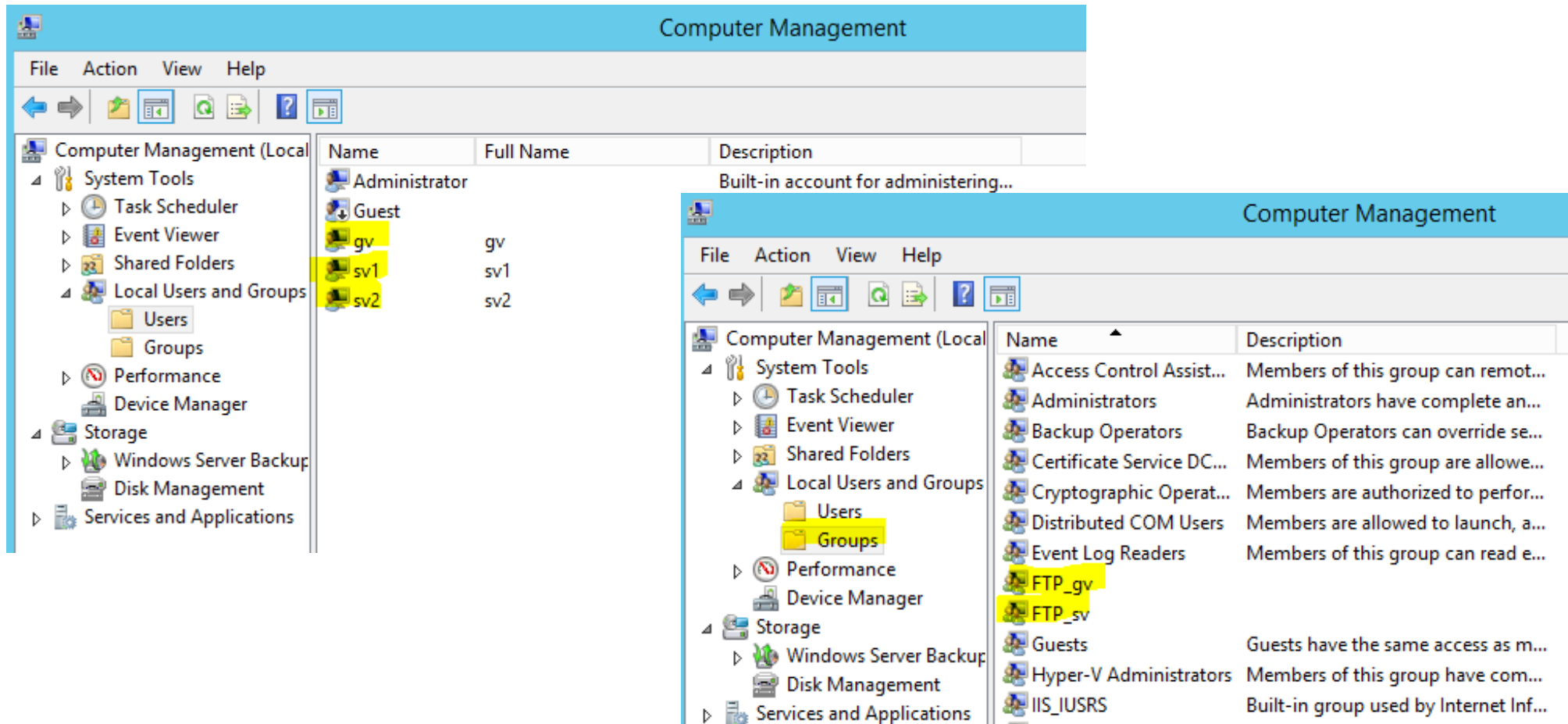
Right Screenshot: Authentication and Authorization Information

- Authentication:**
 - ☐ Anonymous
 - ☒ Basic (highlighted, with mouse cursor)
- Authorization:**
 - Allow access to: Not Selected (dropdown)
 - [Empty text box]
- Permissions:**
 - ☐ Read
 - ☐ Write

Buttons: Previous, Next, Finish, Cancel

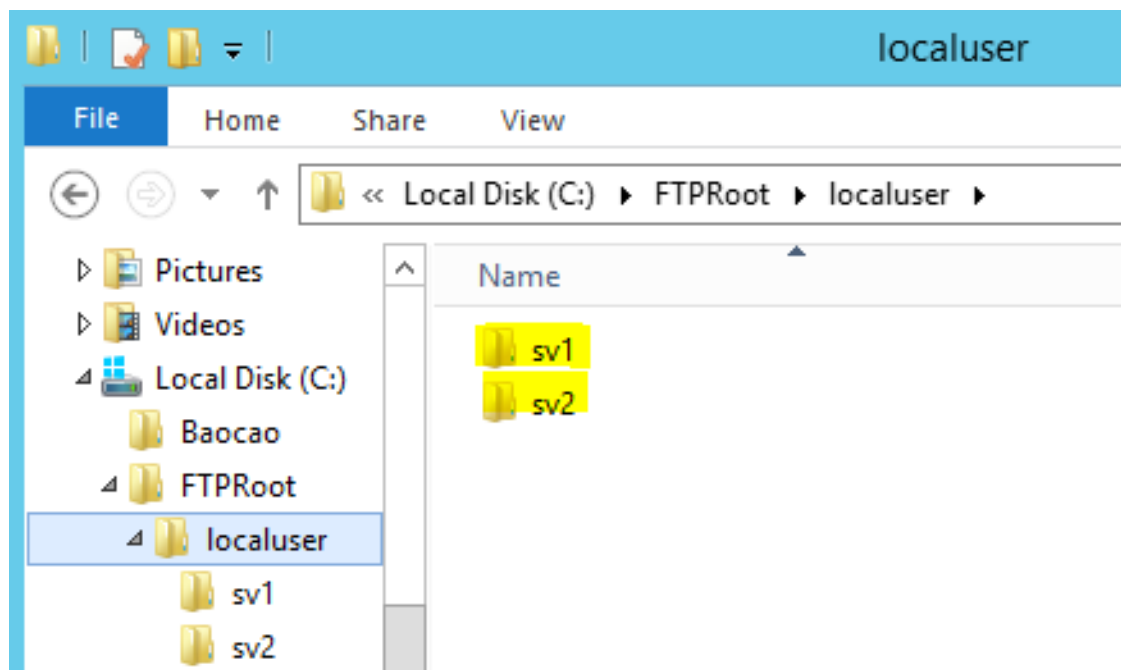
Trên FTP, chọn No SSL không cần tính năng mã hóa dữ liệu. Sau đó chọn kiểu xác thực là Basic

Hướng dẫn thực hành 4



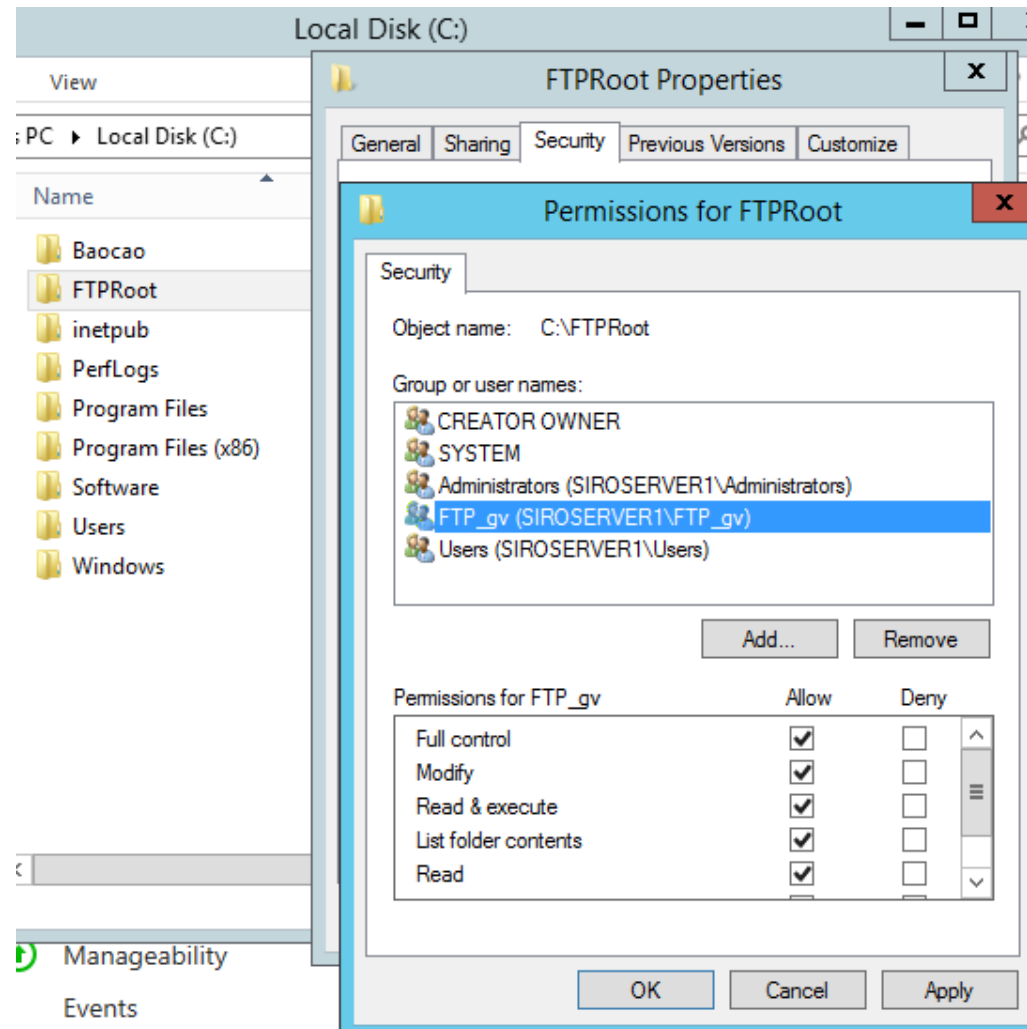
Trên FTP, tạo các user gv, sv1, sv2 và tạo các group FTP_gv, FTP_sv. Thêm các user sv1, sv2 vào group FTP_sv. Thêm user gv vào group FTP_gv

Hướng dẫn thực hành 4



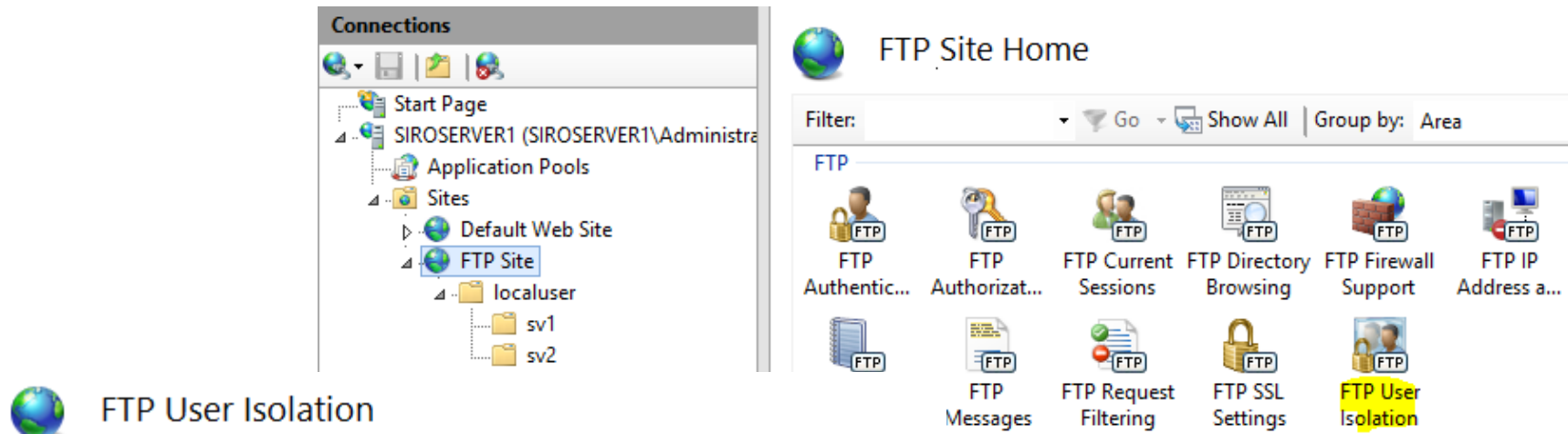
Trên FTP, tạo các thư mục sv1, sv2 tại đường dẫn C:\FTPRoot\localuser

Hướng dẫn thực hành 4



Trên FTP, phân quyền Security cho thư mục FTPRoot thêm group FTP_gv có quyền Full control

Hướng dẫn thực hành 4



FTP User Isolation

FTP user isolation prevents users from accessing the FTP home directory of another user on this FTP site.

Do not isolate users. Start users in:

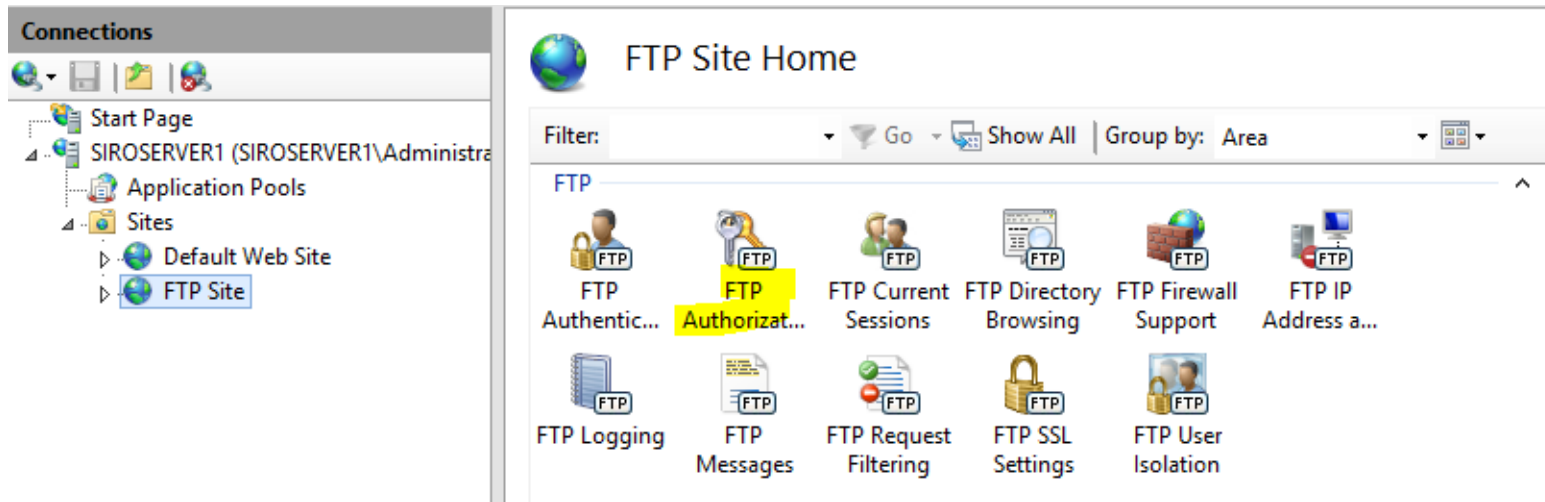
- ☐ FTP root directory
- ☐ User name directory

Isolate users. Restrict users to the following directory:

- ☒ User name directory (disable global virtual directories)
- ☐ User name physical directory (enable global virtual directories)
- ☐ FTP home directory configured in Active Directory

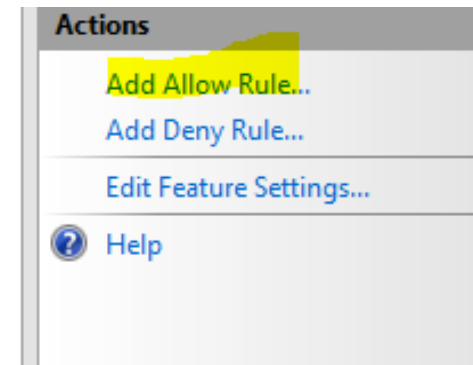
Trên FTP, chọn FTP Site đã tạo, double click vào FTP User Isolation, chọn User name directory. Sau đó Apply

Hướng dẫn thực hành 4



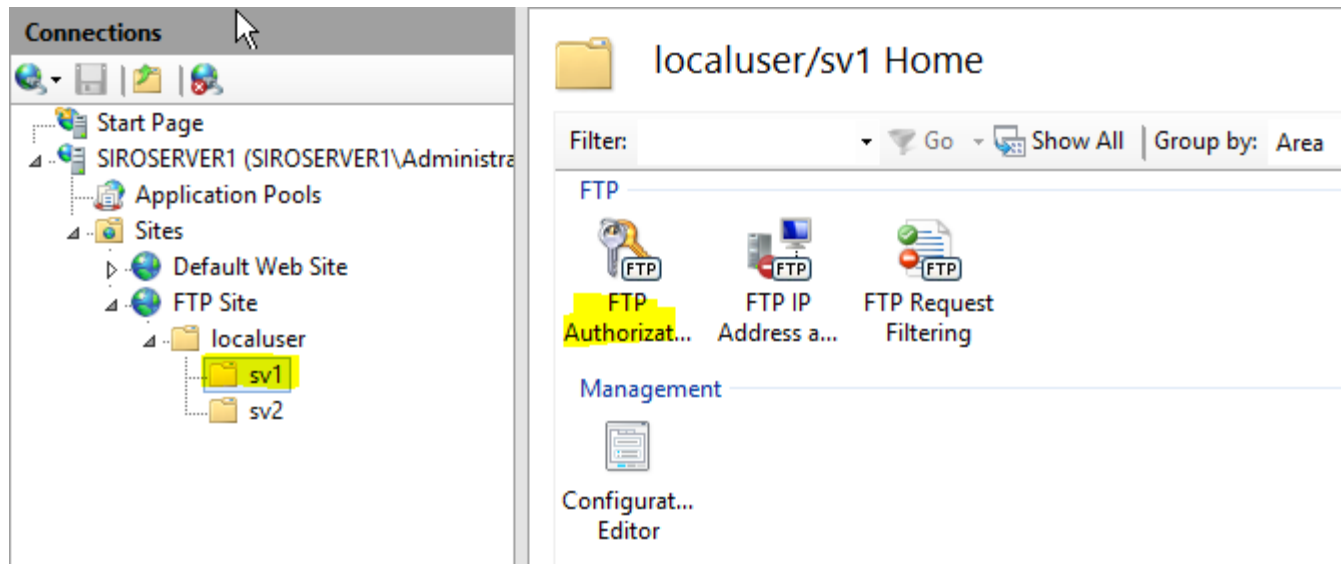
FTP Authorization Rules

Mode	Users	Roles	Permissions
Allow		FTP_sv	Read
Allow		FTP_gv	Read, Write



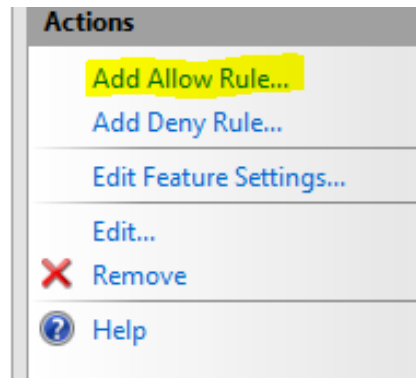
Trên FTP, chọn FTP Site đã tạo, double click vào FTP Authorization. Thêm 2 rule cho phép FTP_gv có quyền Read, Write và FTP_sv có quyền Read

Hướng dẫn thực hành 4



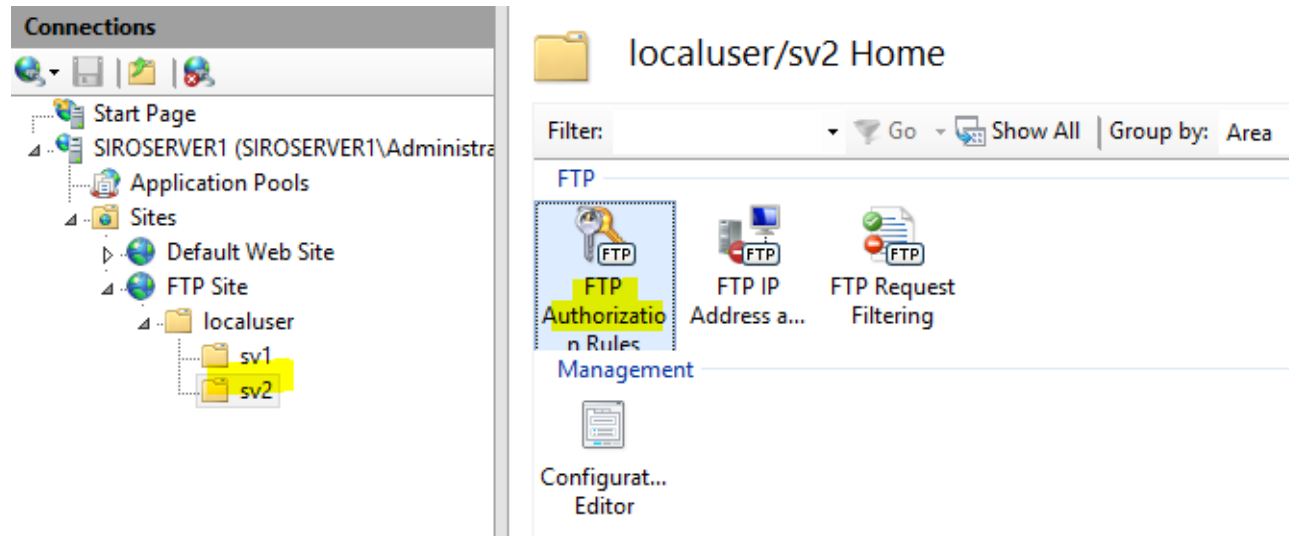
FTP Authorization Rules

Mode	Users	Roles	Permissions
Allow		FTP_sv	Read
Allow		FTP_gv	Read, Write
Allow	sv1		Read, Write



Trên FTP, chọn thư mục sv1, double click vào FTP Authorization. Thêm rule cho phép user sv1 có quyền Read, Write

Hướng dẫn thực hành 4



FTP Authorization Rules

Mode	Users	Roles	Permissions
Allow		FTP_sv	Read
Allow		FTP_gv	Read, Write
Allow	sv2		Read, Write

Actions

[Add Allow Rule...](#)

[Add Deny Rule...](#)

[Edit Feature Settings...](#)

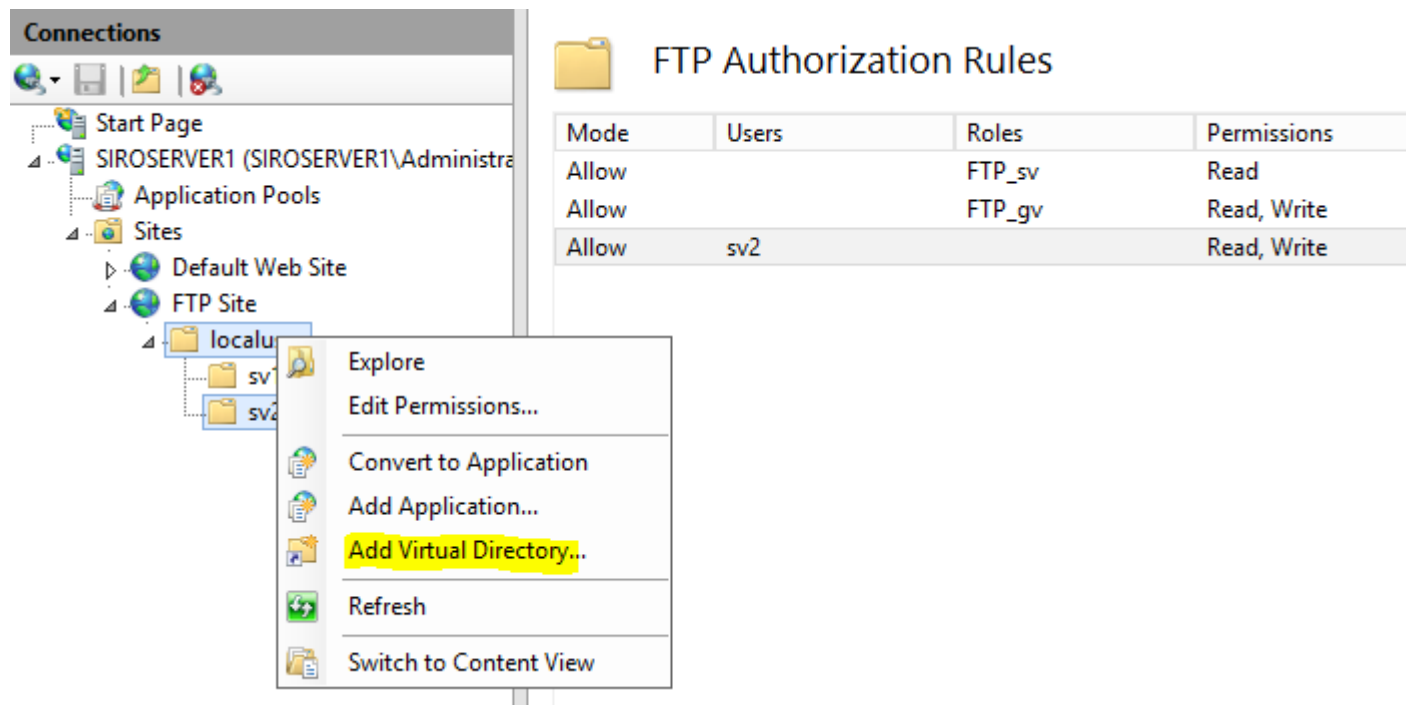
[Edit...](#)

[Remove](#)

[Help](#)

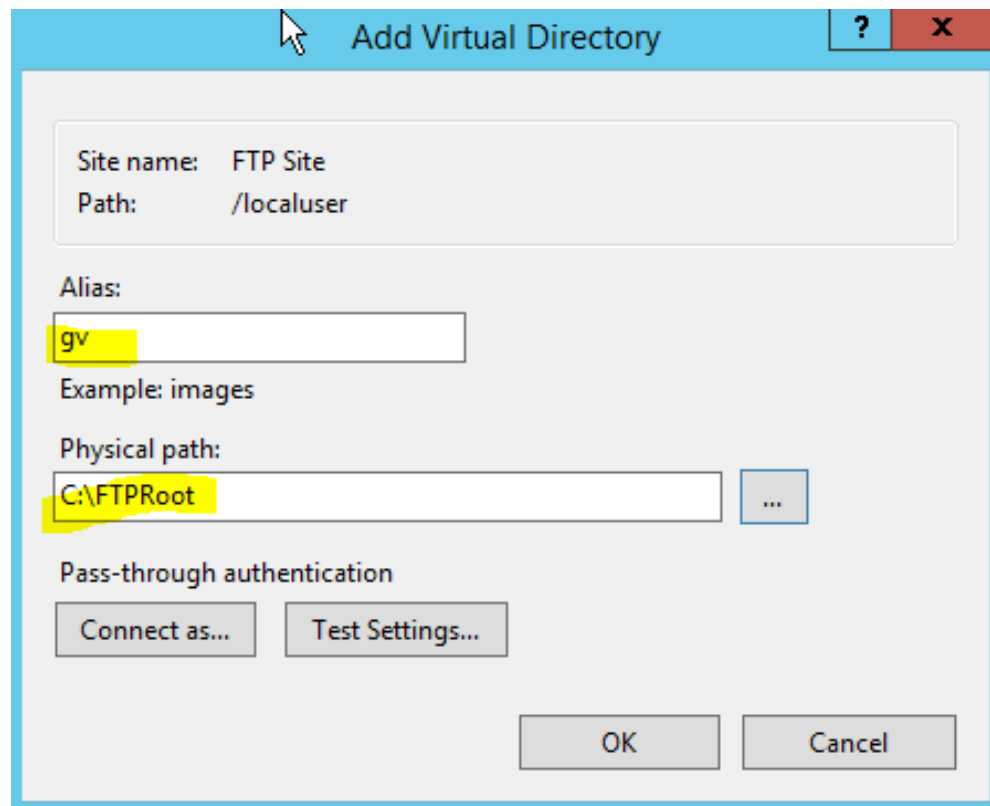
Trên FTP, chọn thư mục sv2, double click vào FTP Authorization. Thêm rule cho phép user sv2 có quyền Read, Write

Hướng dẫn thực hành 4



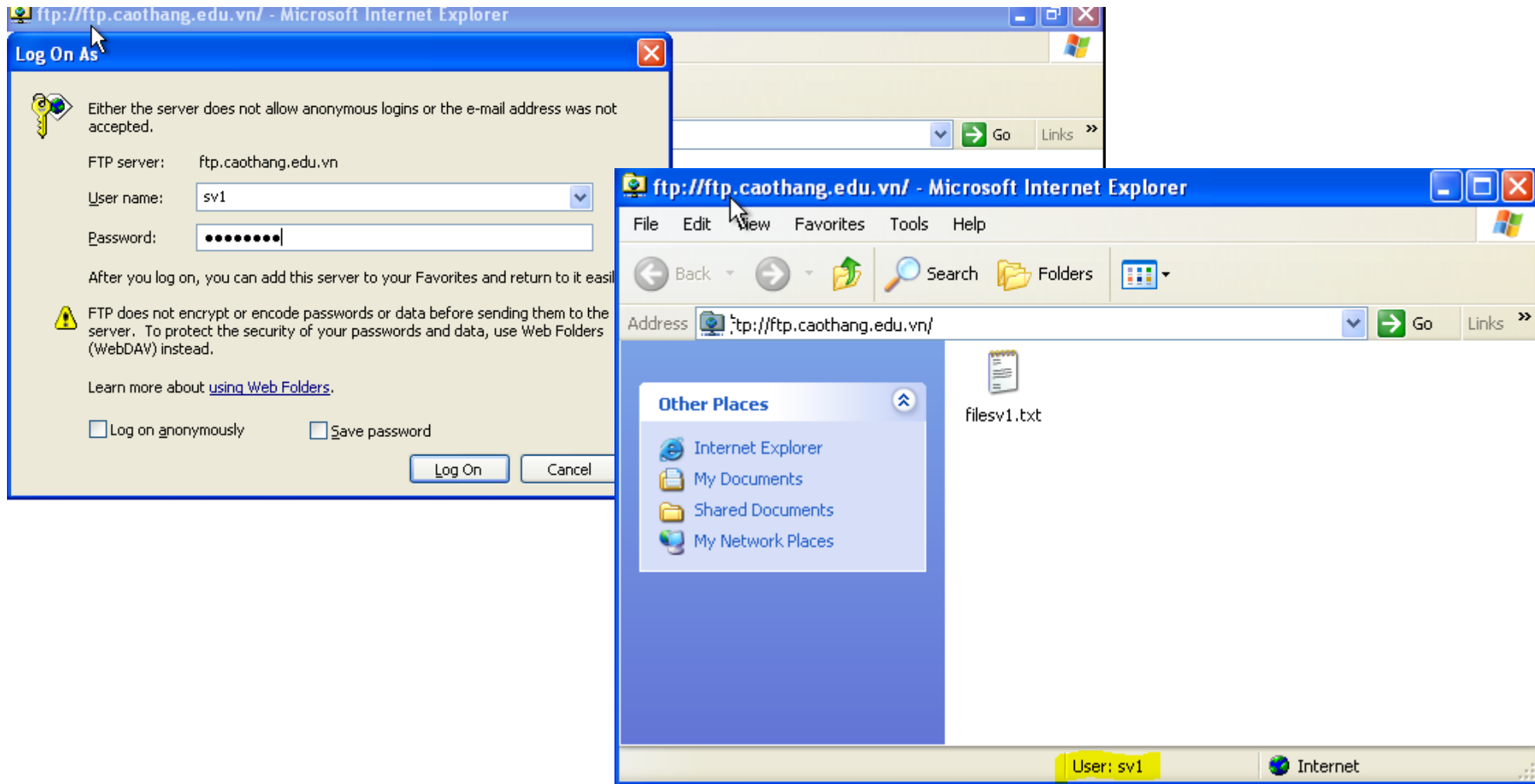
Trên FTP, thêm virtual directory trong thư mục localuser. Click phải localuser chọn Add Virtual Directory

Hướng dẫn thực hành 4



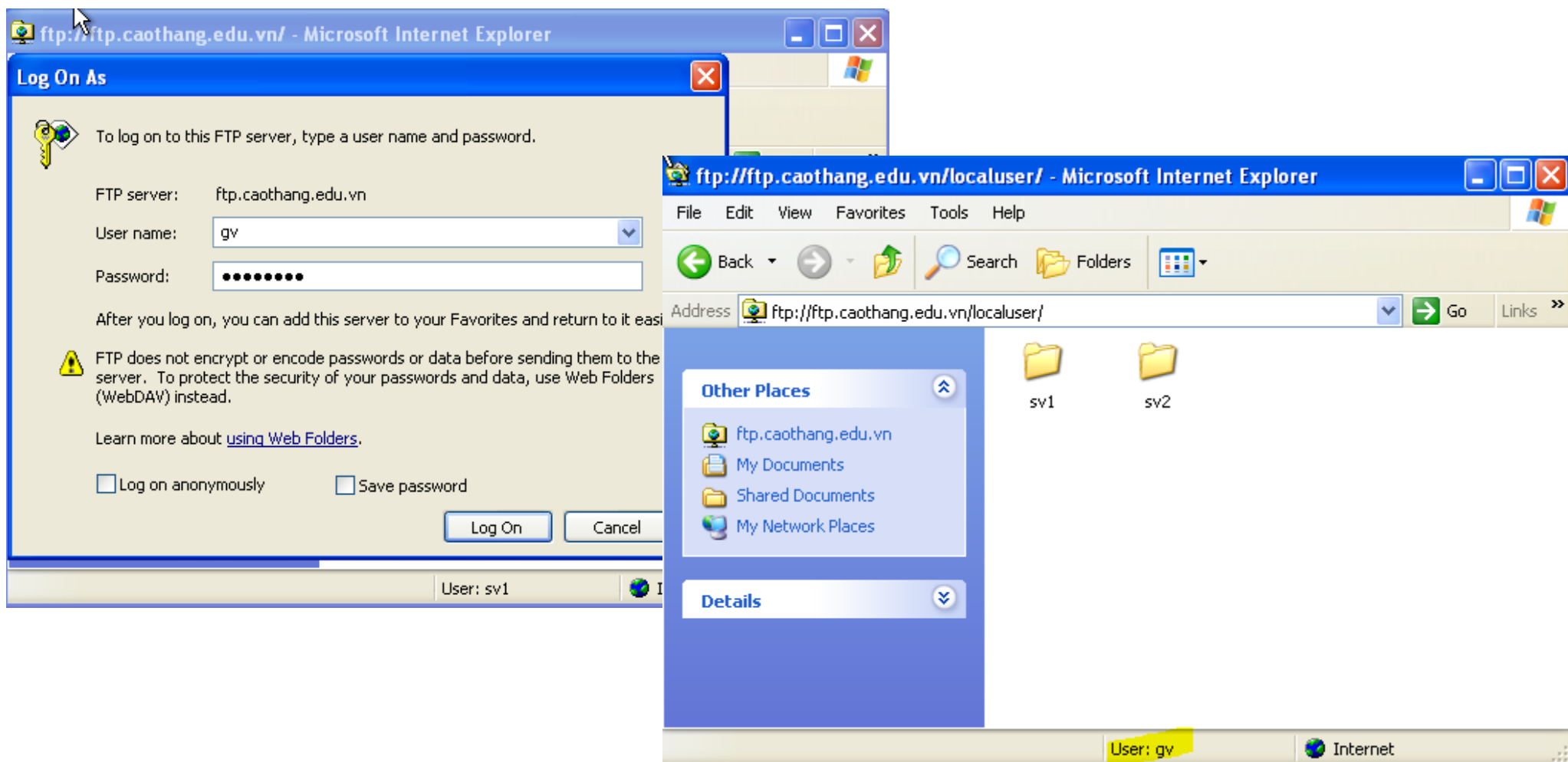
Trên FTP, nhập tên alias là gv và đường dẫn C:\FTPRoot

Hướng dẫn thực hành 4



Trên XP, đăng nhập vào user sv1 thành công

Hướng dẫn thực hành 4



Trên XP, đăng nhập vào user gv thành công và thấy các tập tin và thư mục sv1, sv2