NETWORK SECURITY LAB SERIES

Lab 6: Configuring a Virtual Private Network with PPTP

Document Version: 2015-09-28

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction

This lab is a part of a series of lab exercises intended to support courseware for Network Security training. This lab includes the following tasks:

1. Testing the Firewall and Configuring the VPN Server
2. Configuring the VPN client
3. Using Internal Services from an External Machine

Key Terms for this lab:

PPTP – Point to Point tunneling protocol is an older VPN technology that allows remote users to connect to a company's VPN server and access internal resources.

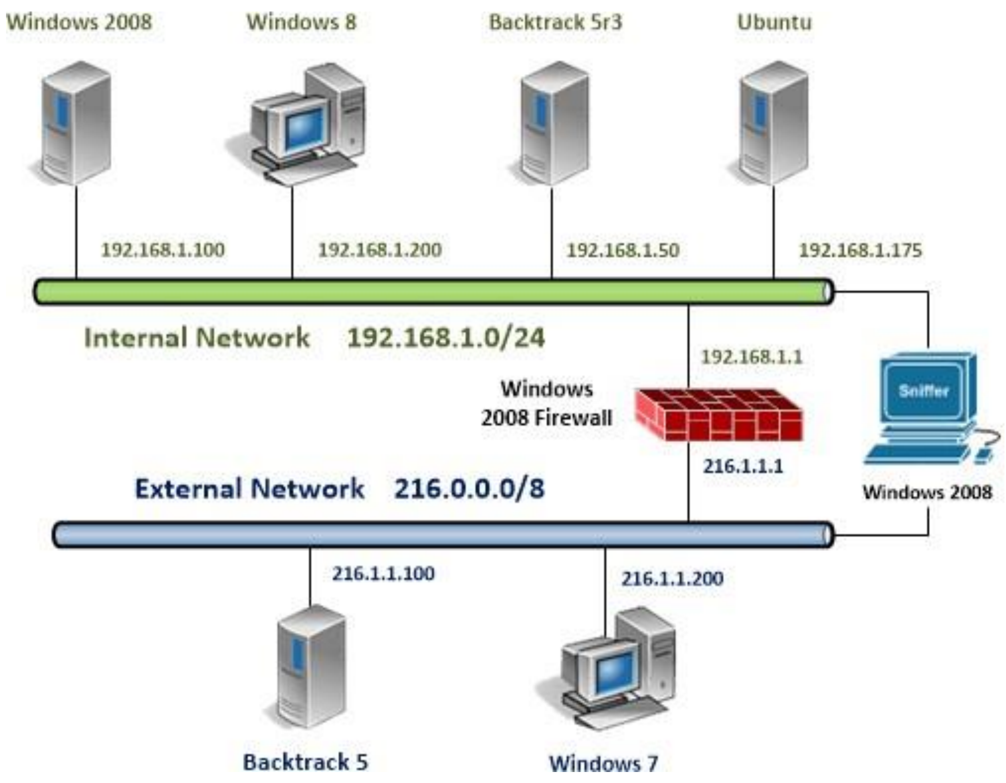
L2TP – Layer 2 tunneling protocol is a VPN technology that uses IPsec and allows remote users to connect to a company's VPN server and access internal resources.

VPN – Most firewalls can be configured to allow incoming traffic on their external interfaces to be redirected to internal hosts.

NAT – Network Address Translation will allow internal hosts to reach the external network through a single IP address. Most firewalls can be configured to perform NAT.

IPsec – IPsec is a technology that encrypts IP packets so they are not sent in the clear. Layer 2 tunneling protocol is a VPN technology that uses IPsec.

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Windows 8 Internal Machine	192.168.1.200	Student	password
Windows 7 External Machine	216.1.1.200	student	password
Windows 2008 Firewall	216.1.1.1 192.168.1.1	administrator	firewall
Windows 2008 Sniffer	n/a	administrator	sniffer

For all the tasks in this lab, you will be asked to open and return to various machines and applications within each machine. For some steps, this can get confusing.

To minimize confusion and the need to reopen machines and applications, it is suggested that you minimize, rather than close a machine before opening another.

At the end of the lab, remember to close all open windows and close the PC viewers.

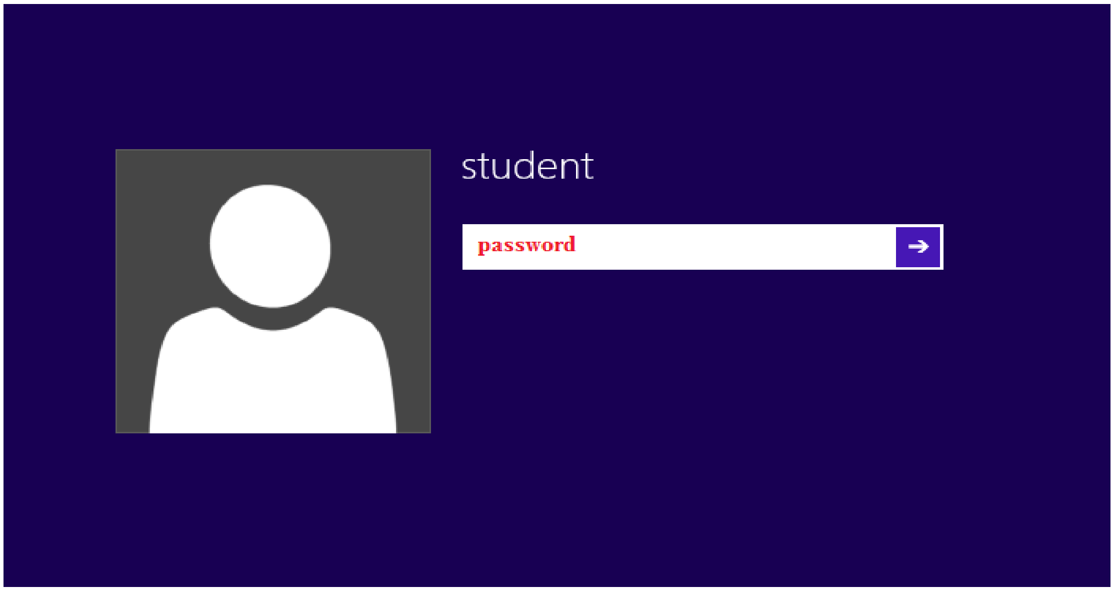
1 Installing the Windows Firewall

In this section, we will examine the current Firewall configuration. Then, we will reconfigure the Windows Firewall and change it into a VPN server. After the VPN server is configured, authorized external users will be able to access internal resources.

1.1 Testing the Current Firewall and Setting up the VPN Server

We will now install and configure a VPN Server. We will configure it to allow all traffic outbound. We will also allow incoming connections for users on the External Network. This will allow them to access resources on the Internal Network, like email and web resources.

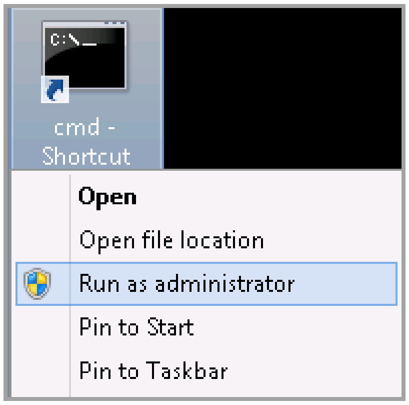
1. Log onto the **Windows 8 Machine** by clicking on the **Windows 8** icon on the lab topology to bring up the login screen. For the student password, type **password**, and then press **Enter**.



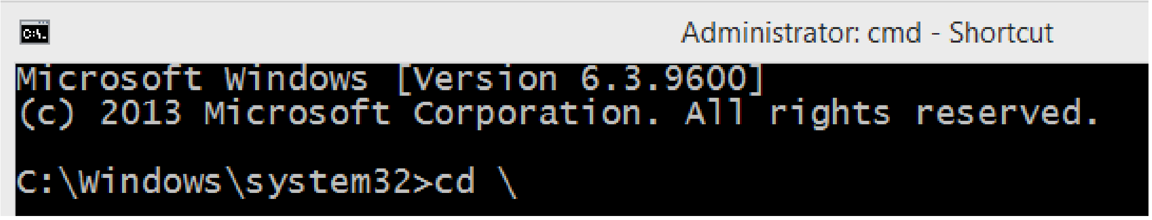
student

password

2. Right-click the **cmd-Shortcut** on the desktop and select **Run as administrator**.

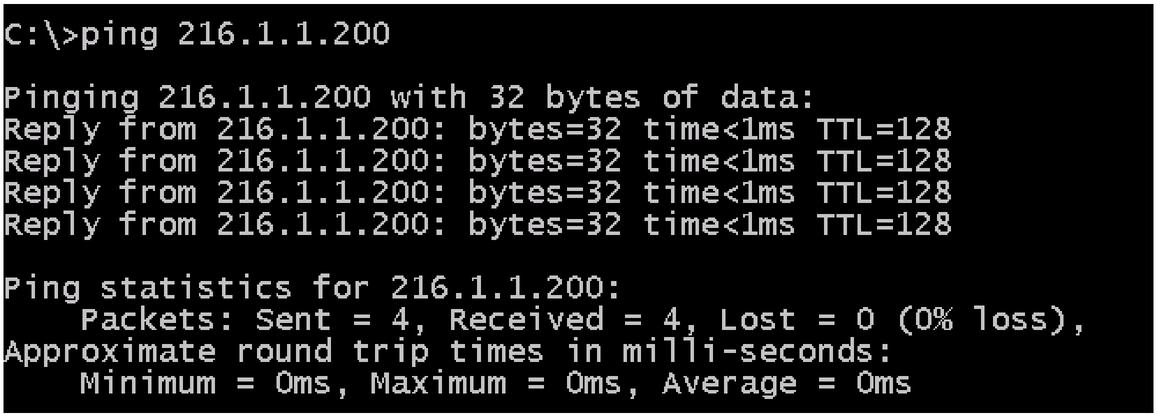


3. Type the command **cd \** to go to the root of the C: Drive
   C:\Windows\system32>**cd \**



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \
```

4. Type the following command to ping the external Windows 7 External Machine.
   C:\>**ping 216.1.1.200**

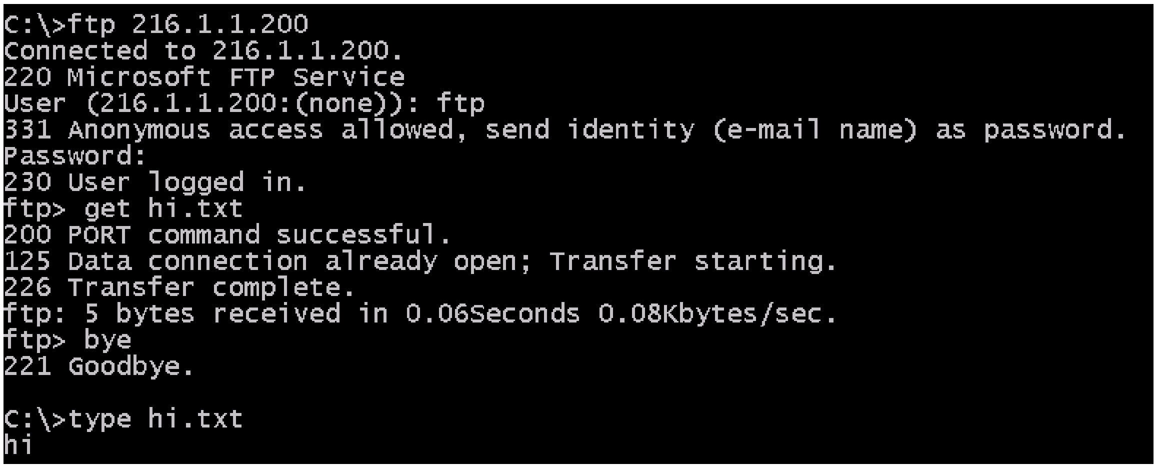


```
C:\>ping 216.1.1.200

Pinging 216.1.1.200 with 32 bytes of data:
Reply from 216.1.1.200: bytes=32 time<1ms TTL=128
Reply from 216.1.1.200: bytes=32 time<1ms TTL=128
Reply from 216.1.1.200: bytes=32 time<1ms TTL=128
Reply from 216.1.1.200: bytes=32 time<1ms TTL=128

Ping statistics for 216.1.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

5. Type the following command to clear the command prompt screen.
   C:\>**cls**

```
C:\>cls
```

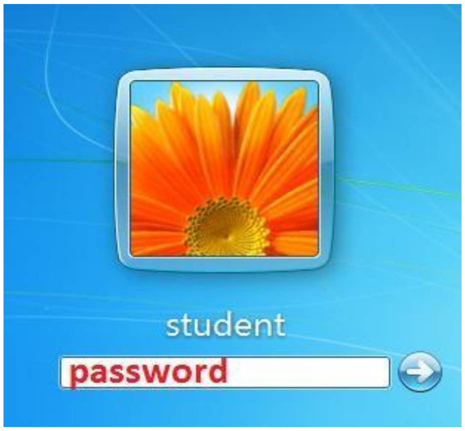
6. Type the following commands to connect to the FTP site and download a file.
   C:\>ftp 216.1.1.200
   user: **ftp**
   Password: **password**
   ftp> **get hi.txt**
   ftp> **bye**
   C:\>**type hi.txt**



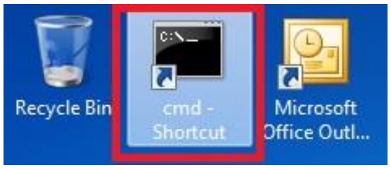
```
C:\>ftp 216.1.1.200
Connected to 216.1.1.200.
220 Microsoft FTP Service
User (216.1.1.200:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp> get hi.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 5 bytes received in 0.06Seconds 0.08Kbytes/sec.
ftp> bye
221 Goodbye.

C:\>type hi.txt
hi
```

The Windows based firewall is allowing all outbound traffic. Network Address Translation (NAT), is set up allowing this Windows 8 Internal Machine with the IP address of 192.168.1.200 to communicate with the Windows 7 External Machine on the public network.

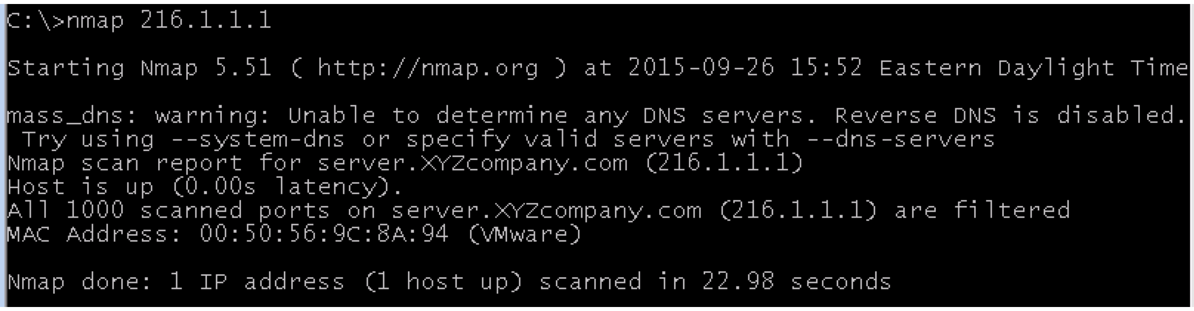
7. Log into the **Windows 7 External Machine** by clicking on the **Windows 7** icon on the topology. If required, enter the username, **student**. Type in the password, **password,** and press **Enter** to log in.



8. Open a command prompt by double-clicking on the shortcut on the desktop

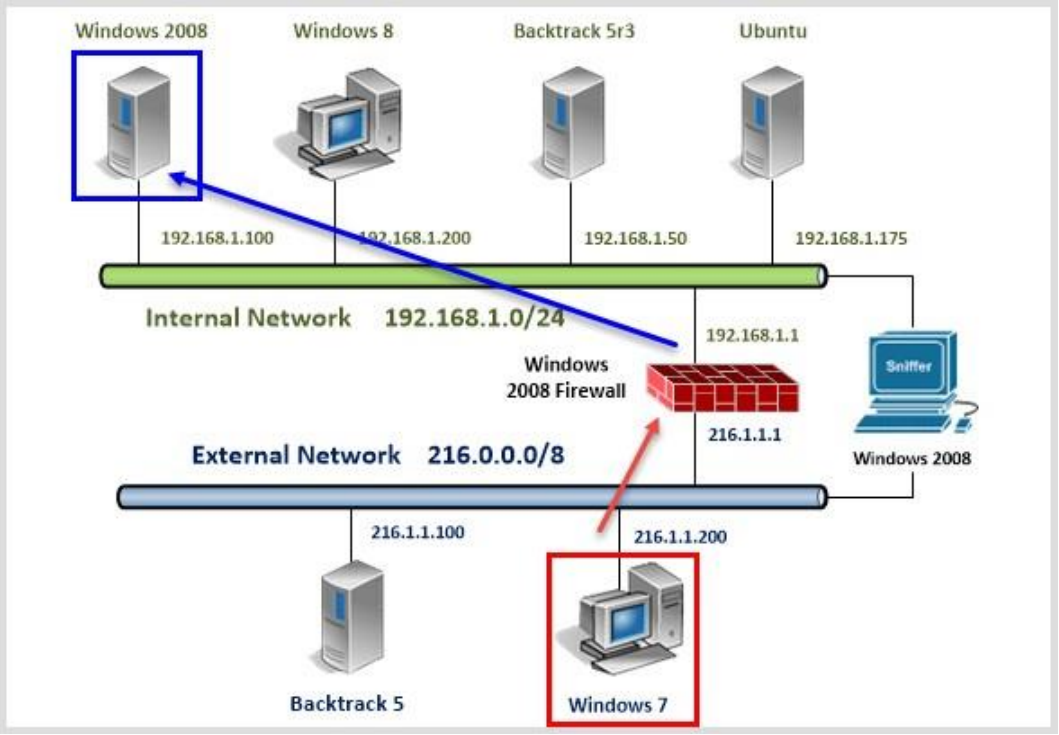


9. Type the following command to scan the firewall for open ports:
   C:\>**nmap 216.1.1.1**



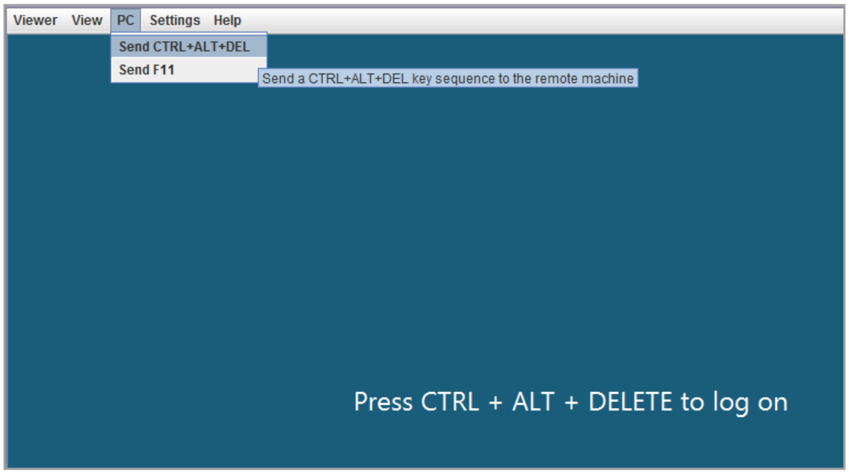
```
C:\>nmap 216.1.1.1

Starting Nmap 5.51 ( http://nmap.org ) at 2015-09-26 15:52 Eastern Daylight Time

mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for server.XYZcompany.com (216.1.1.1)
Host is up (0.00s latency).
All 1000 scanned ports on server.XYZcompany.com (216.1.1.1) are filtered
MAC Address: 00:50:56:9C:8A:94 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.98 seconds
```

Currently, the firewall is not configured to redirect incoming requests for any applications to the Windows 2008 machine on the Internal Network.

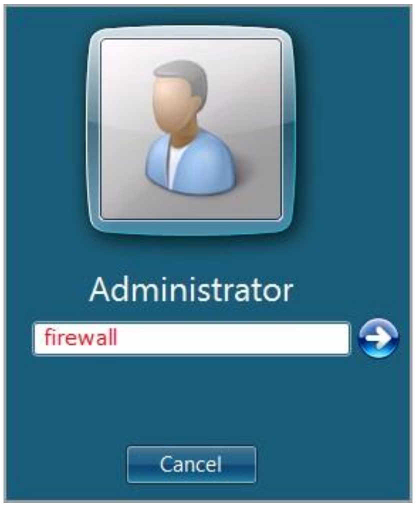


We will now configure a VPN server. After this is done and we re-scan the public IP address of the firewall from the external network, only a single port will be open.

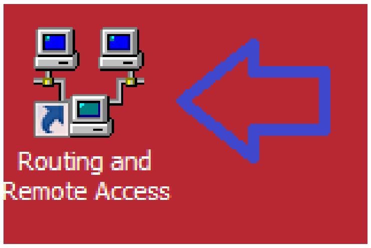
10. Log into the **Windows 2008 Server Firewall** by clicking on the **Windows 2008 Firewall** icon o the topology. Click **PC,** and then **Send Ctrl+Alt+Del** in the top-left corner of the screen in order to log on to the Windows 2008 server.


Viewer
View
PC
Settings
Help
Send CTRL+ALT+DEL
Send F11
Send a CTRL+ALT+DEL key sequence to the remote machine
Press CTRL + ALT + DELETE to log on

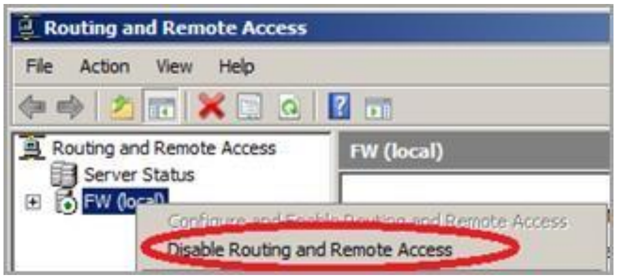
11. Enter **firewall** for the Administrator password to the Windows 2008 Server.



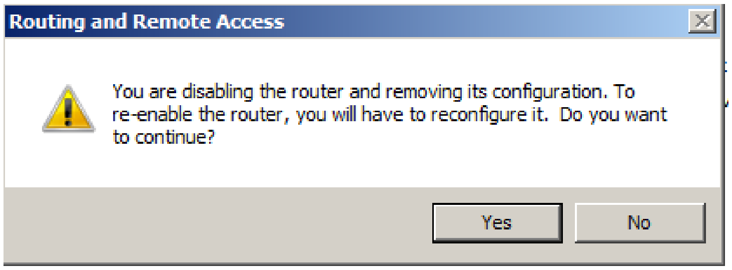
12. Double-click the shortcut to **Routing and Remote Access** on the desktop.



13. Right-click on **FW (local)** and select **Disable Routing and Remote Access**.

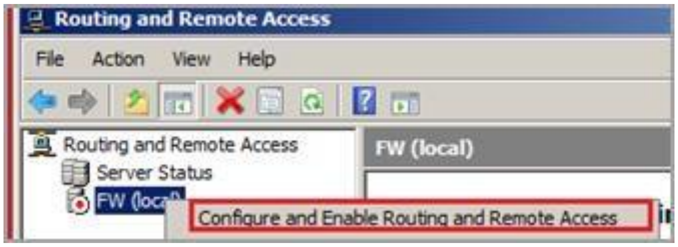

Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
FW (local)
FW (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access

14. Select **Yes** when you are asked if you want to continue.

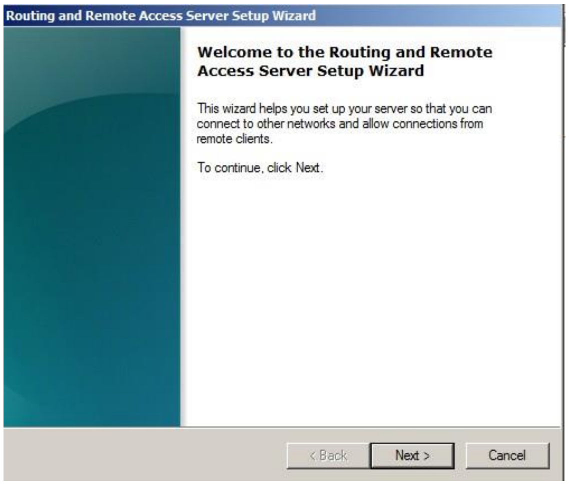


You are disabling the router and removing its configuration. To re-enable the router, you will have to reconfigure it. Do you want to continue?

15. Right-click on **FW (local)** and select **Configure Routing and Remote Access**.


Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
FW (local)
FW (local)
Configure and Enable Routing and Remote Access

16. Click **Next** to the welcome to the Routing and Remote Access Setup Wizard.

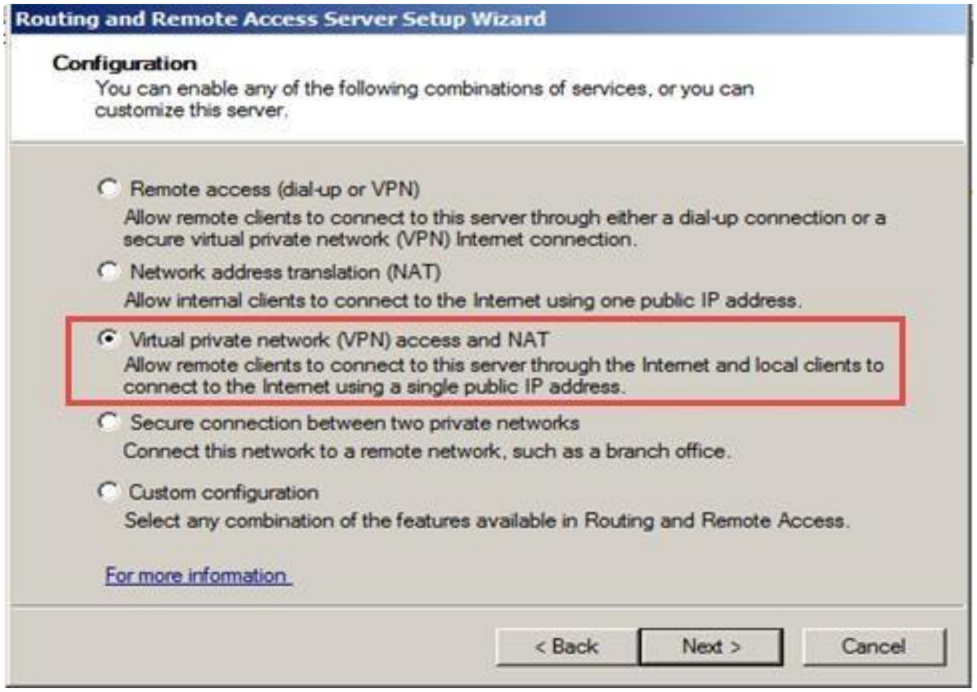


Welcome to the Routing and Remote Access Server Setup Wizard

This wizard helps you set up your server so that you can connect to other networks and allow connections from remote clients.

To continue, click Next.

17. Choose **Virtual private network (VPN) access and NAT**. Click **Next**.



Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

○ Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

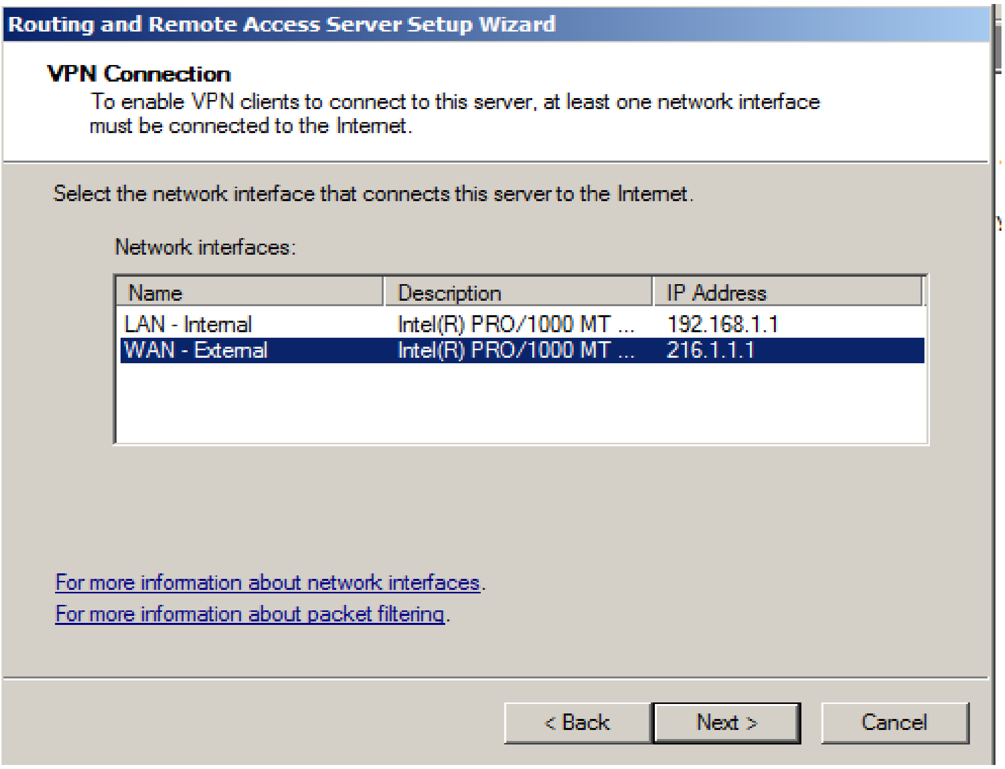
○ Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

● Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

○ Secure connection between two private networks
Connect this network to a remote network, such as a branch office.

○ Custom configuration
Select any combination of the features available in Routing and Remote Access.

18. Select the **WAN-External** interface and then click the **Next** button.



Routing and Remote Access Server Setup Wizard

VPN Connection

To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.

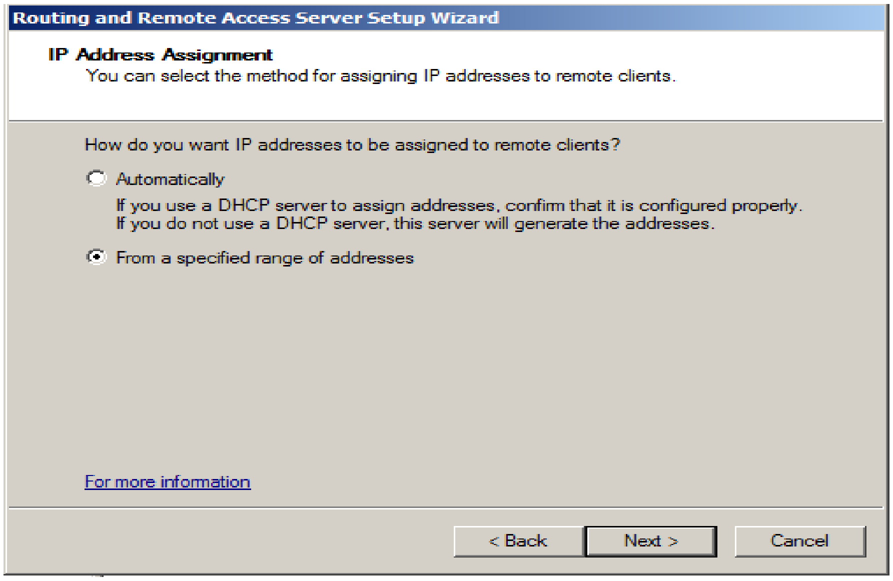
Select the network interface that connects this server to the Internet.

Network interfaces:

Name	Description	IP Address
LAN - Internal	Intel(R) PRO/1000 MT ...	192.168.1.1
WAN - External	Intel(R) PRO/1000 MT ...	216.1.1.1

For more information about network interfaces.
For more information about packet filtering.
< Back
Next >
Cancel

19. Select **From a specified range of addresses** and click the **Next** button.



Routing and Remote Access Server Setup Wizard

IP Address Assignment

You can select the method for assigning IP addresses to remote clients.

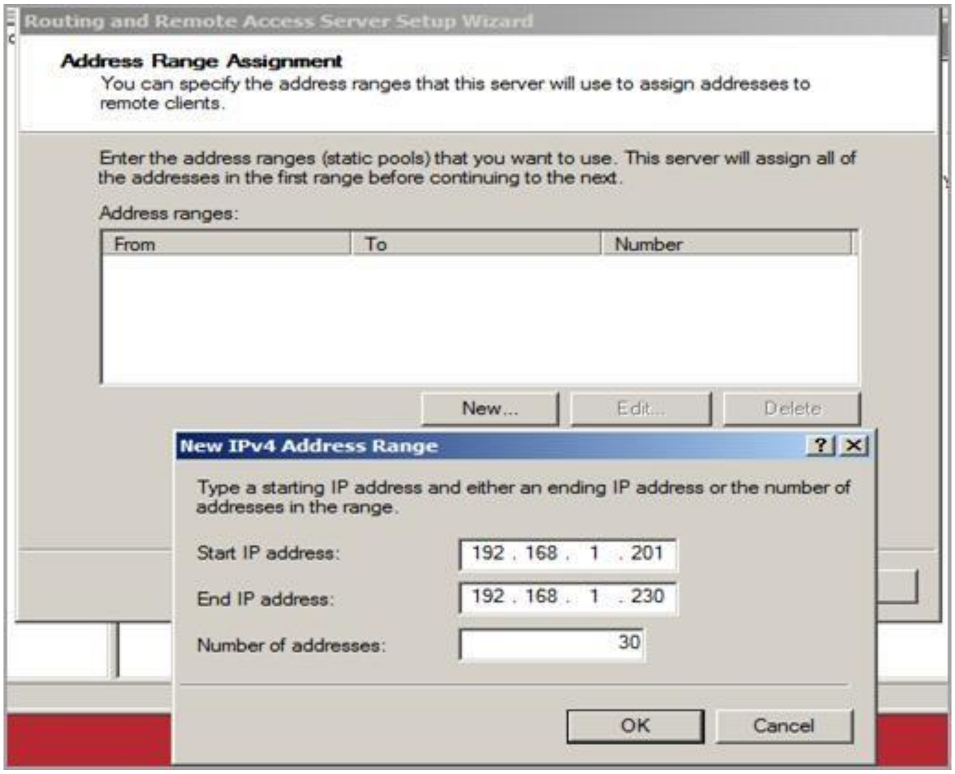
How do you want IP addresses to be assigned to remote clients?

○ Automatically

If you use a DHCP server to assign addresses, confirm that it is configured properly. If you do not use a DHCP server, this server will generate the addresses.

● From a specified range of addresses

20. Click **New**, type Start IP Address: **192.168.1.201,** End IP Address: **192.168.1.230**. Click **OK** and click **Next.**



Routing and Remote Access Server Setup Wizard

Address Range Assignment

You can specify the address ranges that this server will use to assign addresses to remote clients.

Enter the address ranges (static pools) that you want to use. This server will assign all of the addresses in the first range before continuing to the next.

Address ranges:

From	To	Number

New IPv4 Address Range

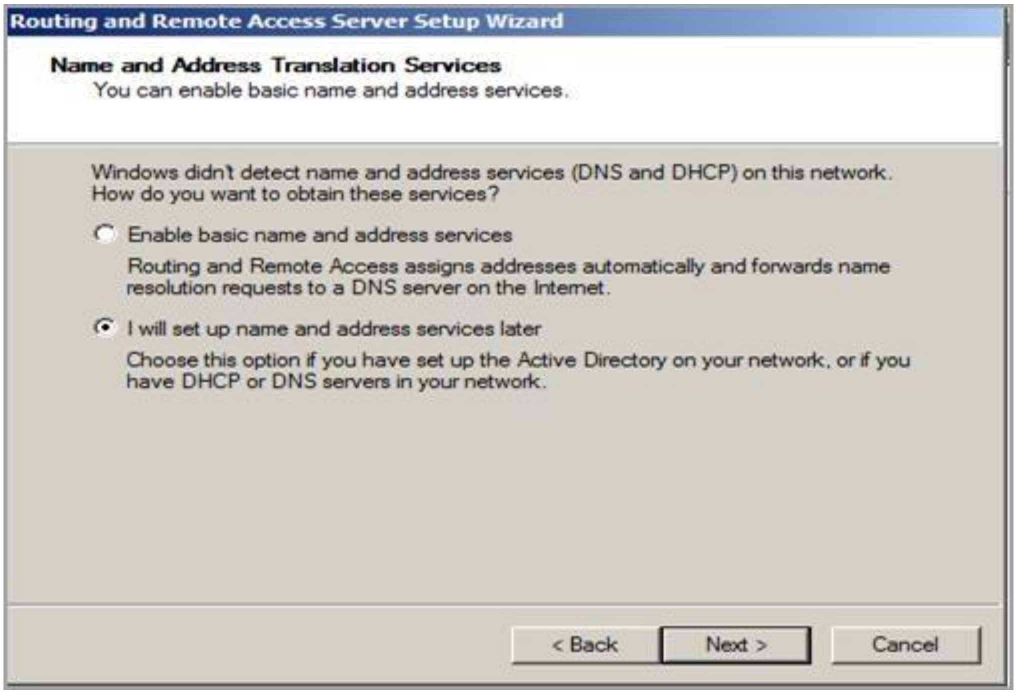
Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 192 . 168 . 1 . 201

End IP address: 192 . 168 . 1 . 230

Number of addresses: 30

21. Select **I will set up name and address services later** and click the **next** button.



Routing and Remote Access Server Setup Wizard

Name and Address Translation Services

You can enable basic name and address services.

Windows didn't detect name and address services (DNS and DHCP) on this network. How do you want to obtain these services?

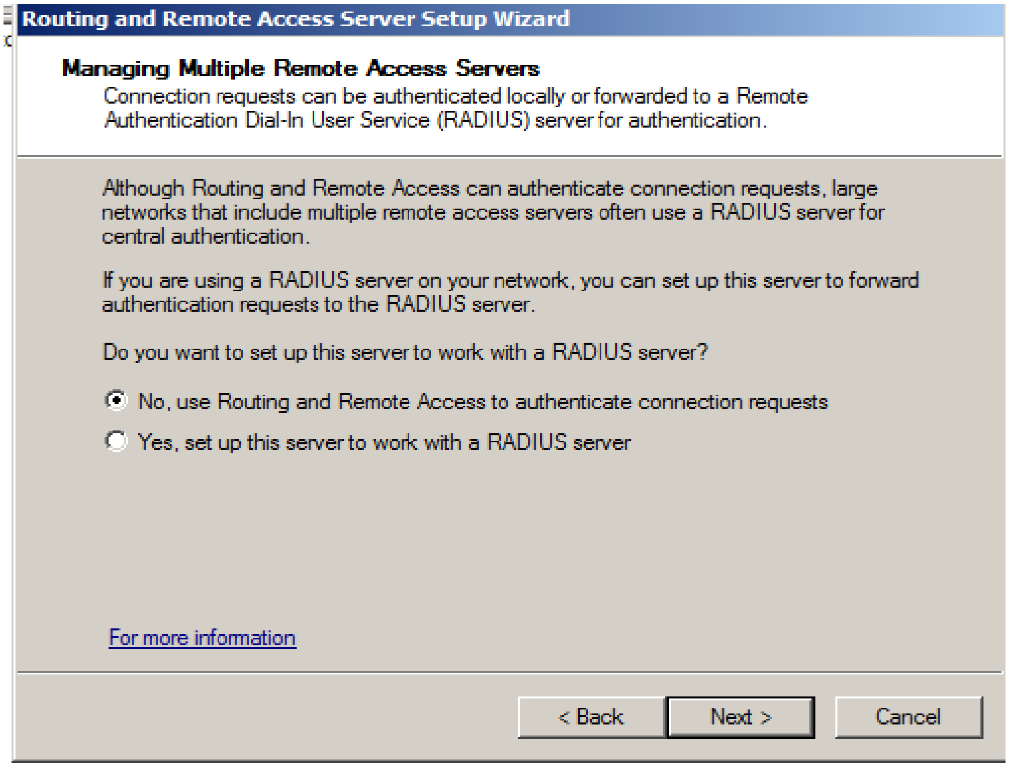
○ Enable basic name and address services

Routing and Remote Access assigns addresses automatically and forwards name resolution requests to a DNS server on the Internet.

● I will set up name and address services later

Choose this option if you have set up the Active Directory on your network, or if you have DHCP or DNS servers in your network.

22. Select **No** at the RADIUS screen and click the **Next** button.



Routing and Remote Access Server Setup Wizard

Managing Multiple Remote Access Servers

Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.

Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.

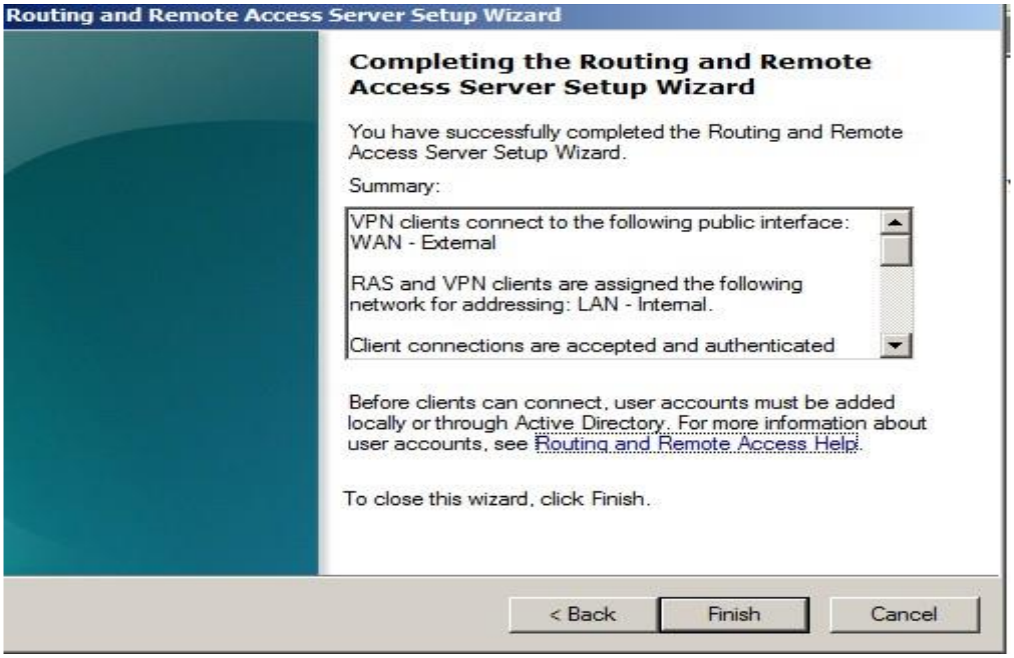
If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

Do you want to set up this server to work with a RADIUS server?

● No, use Routing and Remote Access to authenticate connection requests

○ Yes, set up this server to work with a RADIUS server

23. Click **Finish** to complete the setup of Routing and Remote Access.



Routing and Remote Access Server Setup Wizard

Completing the Routing and Remote Access Server Setup Wizard

You have successfully completed the Routing and Remote Access Server Setup Wizard.

Summary:

VPN clients connect to the following public interface: WAN - External

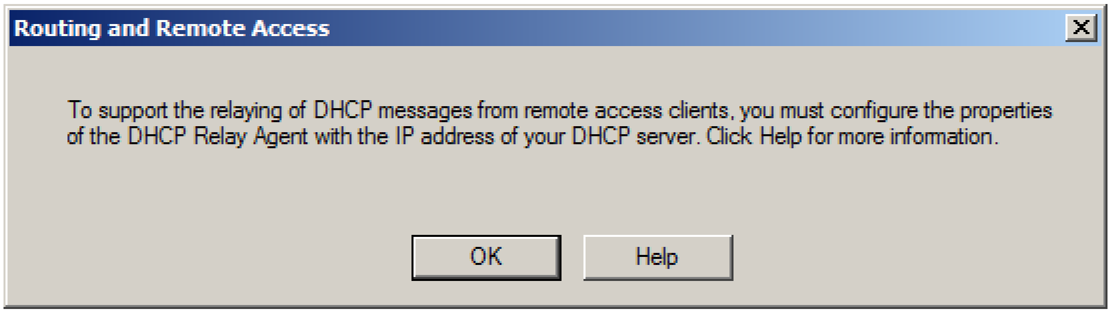
RAS and VPN clients are assigned the following network for addressing: LAN - Internal.

Client connections are accepted and authenticated

Before clients can connect, user accounts must be added locally or through Active Directory. For more information about user accounts, see Routing and Remote Access Help.

To close this wizard, click Finish.

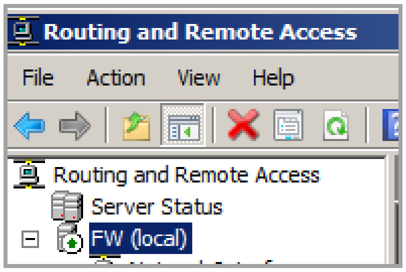
24. Click **OK** to the warning message about the DCHP relay agent.



Routing and Remote Access

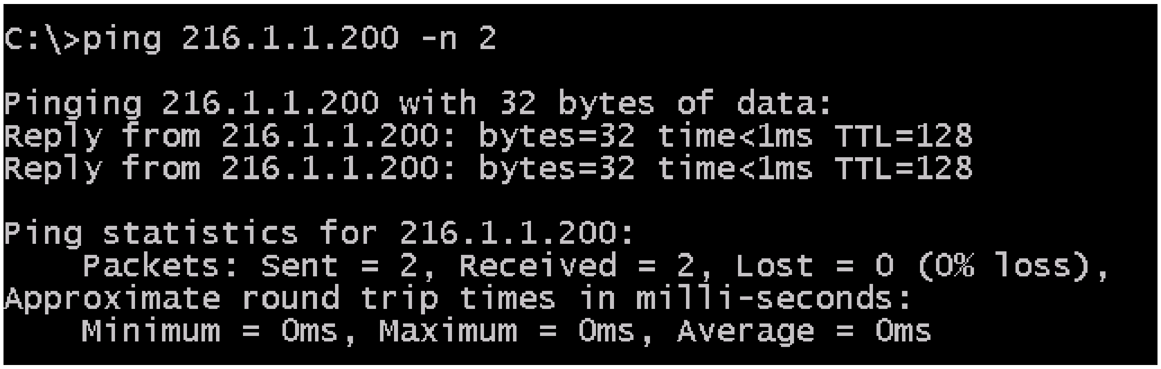
To support the relaying of DHCP messages from remote access clients, you must configure the properties of the DHCP Relay Agent with the IP address of your DHCP server. Click Help for more information.

25. The Routing and Remote Access **FW (local)** machine icon will now turn green again.



26. Go back to the **Windows 8 Internal Machine** again. We will now verify that the machine can once again contact machines on the external network. Type the following command on your Windows 8 Internal Machine to ping the Windows 7 External Machine.

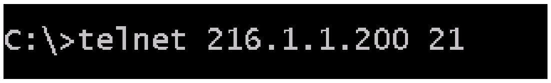
    C:\>**ping 216.1.1.200 -n 2**



```
C:\>ping 216.1.1.200 -n 2

Pinging 216.1.1.200 with 32 bytes of data:
Reply from 216.1.1.200: bytes=32 time<1ms TTL=128
Reply from 216.1.1.200: bytes=32 time<1ms TTL=128

Ping statistics for 216.1.1.200:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

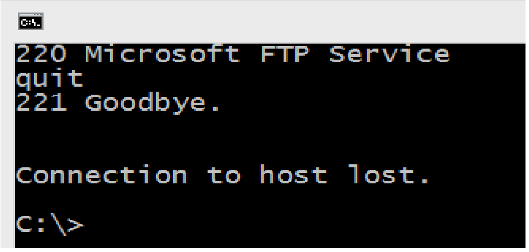
27. Next, we will test if traffic is allowed outbound by performing a banner grab. From the Windows 8 Internal Machine, type the following to perform a banner grab of the Windows 7 External Machine:

    C:\>**telnet 216.1.1.200 21**



```
C:\>telnet 216.1.1.200 21
```

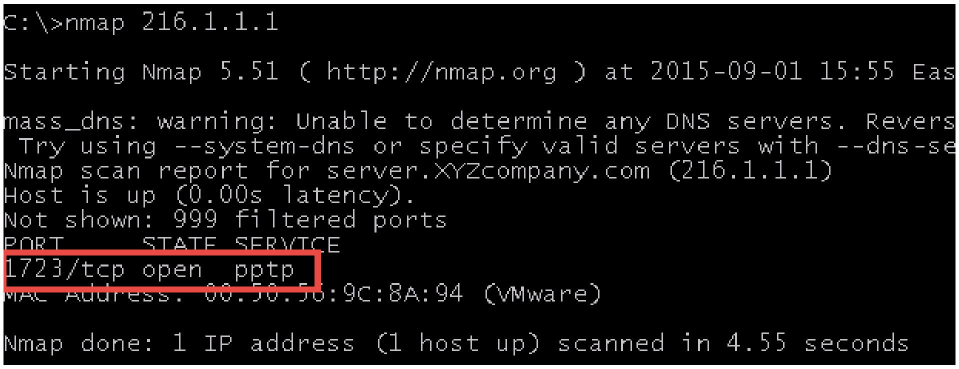
28. You will receive the message 220 Microsoft FTP Service. Type the following: **quit**



```
220 Microsoft FTP Service
quit
221 Goodbye.


Connection to host lost.

C:\>
```

You should receive the message, *Connection to host lost.*
Next, we will test things from the external network. Use the Windows 7 External machine to perform an nmap scan of the public firewall IP address of the firewall.

29. Go back to the **Windows 7 External Machine**.
30. Login as the user **student** with the password as **password**.
31. Open a new command prompt by double-clicking on **cmd – Shortcut**.
32. While in the command prompt, type the following to scan the firewall for open ports:
    C:\>**nmap 216.1.1.1**



```
C:\>nmap 216.1.1.1

Starting Nmap 5.51 ( http://nmap.org ) at 2015-09-01 15:55 Eas

mass_dns: warning: Unable to determine any DNS servers. Revers
 Try using --system-dns or specify valid servers with --dns-se
Nmap scan report for server.XYZcompany.com (216.1.1.1)
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
1723/tcp open  pptp
MAC Address: 00:50:56:9C:8A:94 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.55 seconds
```

You may ignore the DNS warning message.

One port, 1723, is reported as open. PPTP or point-to-point tunneling protocol uses port 1723. Point to Point tunneling protocol is an older VPN technology that allows remote users to connect to a company's VPN server and access internal resources.

1.2 Conclusion

Some firewalls include VPN capabilities. A Virtual Private Network can be set up so that external users from the Internet can connect in and access internal network resources. VPNs encrypt traffic so that the communication between the VPN server and client is safe.

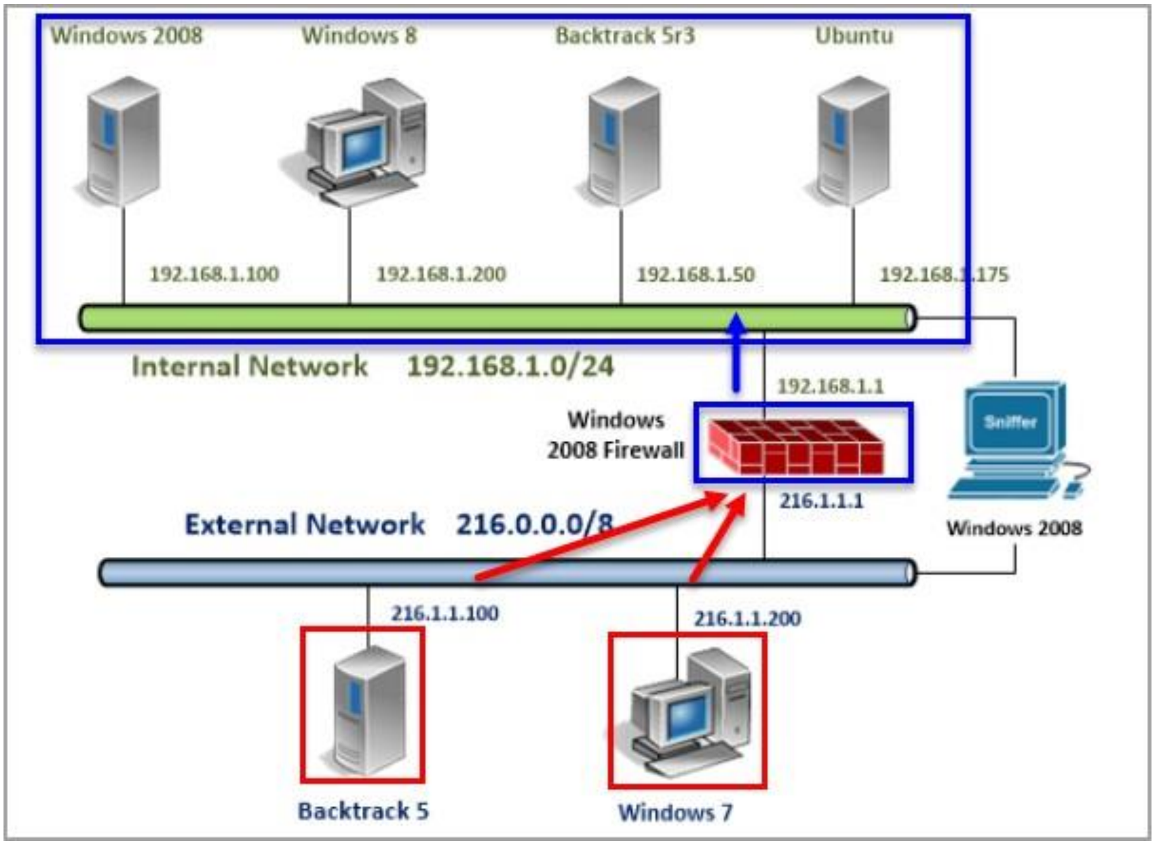
1.3 Discussion Questions

1. What does PPTP stand for?
   Ans: PPTP stands for Point-to-point Tunneling Protocol.
2. What is a banner grab?
   Ans: Grab is a technique used to gather information about a remote server by capturing the banner message that is sent by the server when a connection is established. It is prominent tool in VPN.
3. What are ways that you can verify outbound TCP/IP traffic is allowed?
   Ans: To verify outbound TCP/IP traffic is allowed by performing a banned grap that is c:1>telnet 216.1.1200.21.
4. What tool can be used to scan an IP address for any open ports?
   Ans: The tools used to scan open port in VPN is NMAP and it is also used to identify hosts on a network in Open source program.

2 Configuring the VPN

A Virtual Private Network (VPN) allows clients from an external network to connect to and utilize the resources of an internal network. Virtual Private Networks, which are encrypted, allow individuals to work from remote locations. The encryption of a Virtual Private Network allows external users to access internal resources in a secure manner.

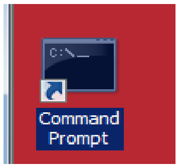
The VPN that we configured on the Windows 2008 server will allow external users to access internal resources on the network. After connecting to the firewall, the external user will be assigned an internal IP address on the internal 192.168.100.0/24 network.



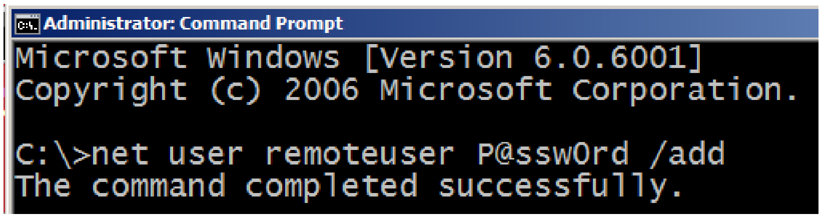
2.1 Configuring the VPN Client

We will now add a user to the firewall and configure the Windows 7 External Machine so it can connect to the public IP address of the Firewall and establish a VPN (Virtual Private Network) connection.

1. On the **Windows 2008 Firewall**, double-click the **Command Prompt** shortcut.



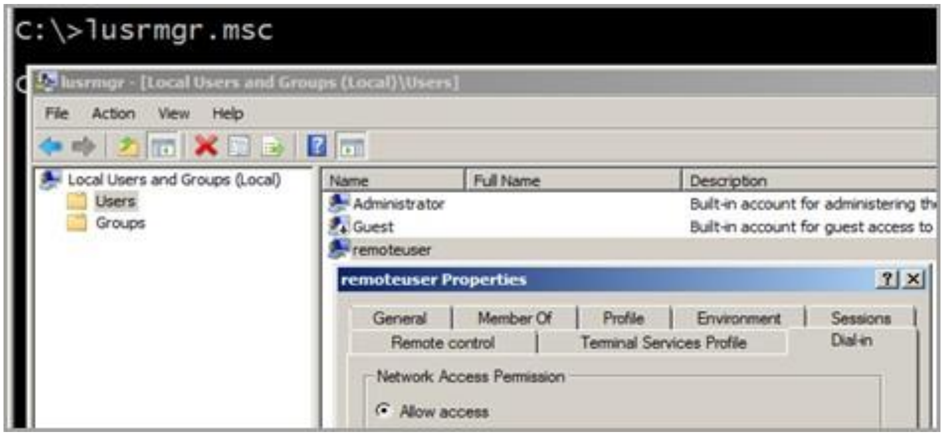
2. Type the following to add a remote user account:
   C:\>**net user remoteuser P@ssw0rd /add**



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.

C:\>net user remoteuser P@ssw0rd /add
The command completed successfully.
```

3. Type the following to manage the remote user:
   C:\>**lusrmgr.msc**

Double-click the **Users** folder. Double-click on **remoteuser**. Click the **Dial-in** Tab. Click the button that says **Allow access**. Click **Apply** and then **OK**. Close the Local User Manager.

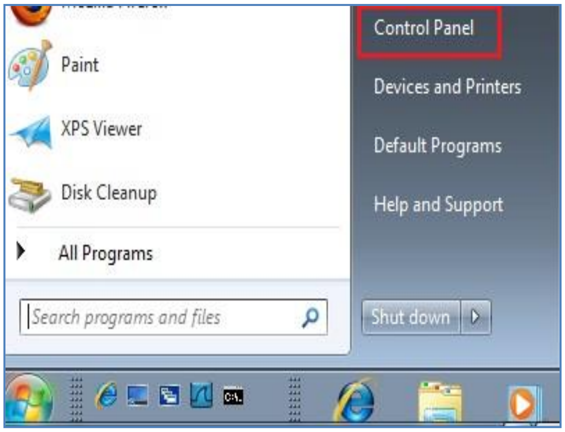

lusrmgr - [Local Users and Groups (Local)\Users]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
remoteuser Properties
General
Member Of
Profile
Environment
Sessions
Remote control
Terminal Services Profile
Dial-in
Network Access Permission

```
C:\>lusrmgr.msc
```

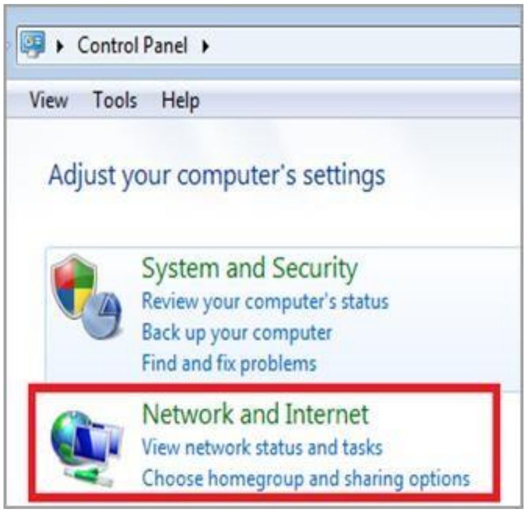
Name	Full Name	Description
Administrator		Built-in account for administering th
Guest		Built-in account for guest access to
remoteuser		

● Allow access

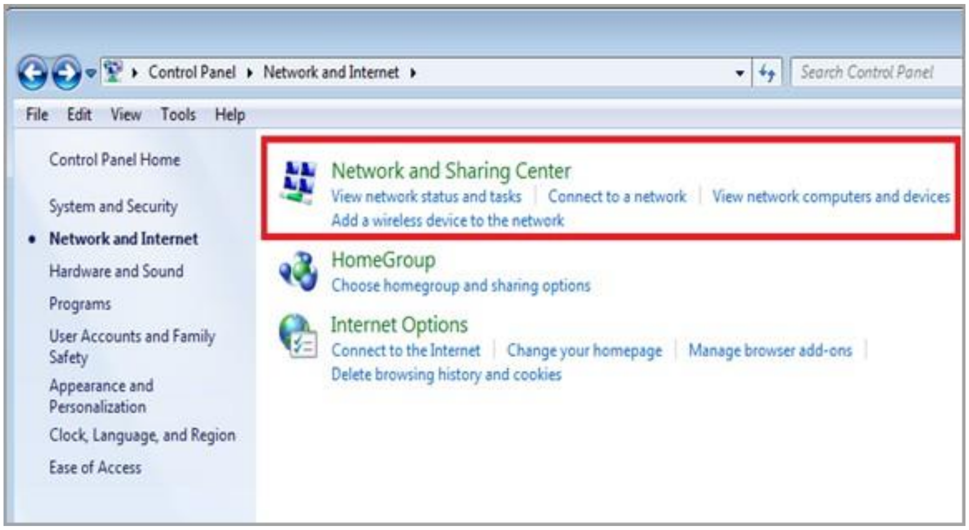
4. On the **Windows 7 External Machine**, click **Start > Control Panel**.



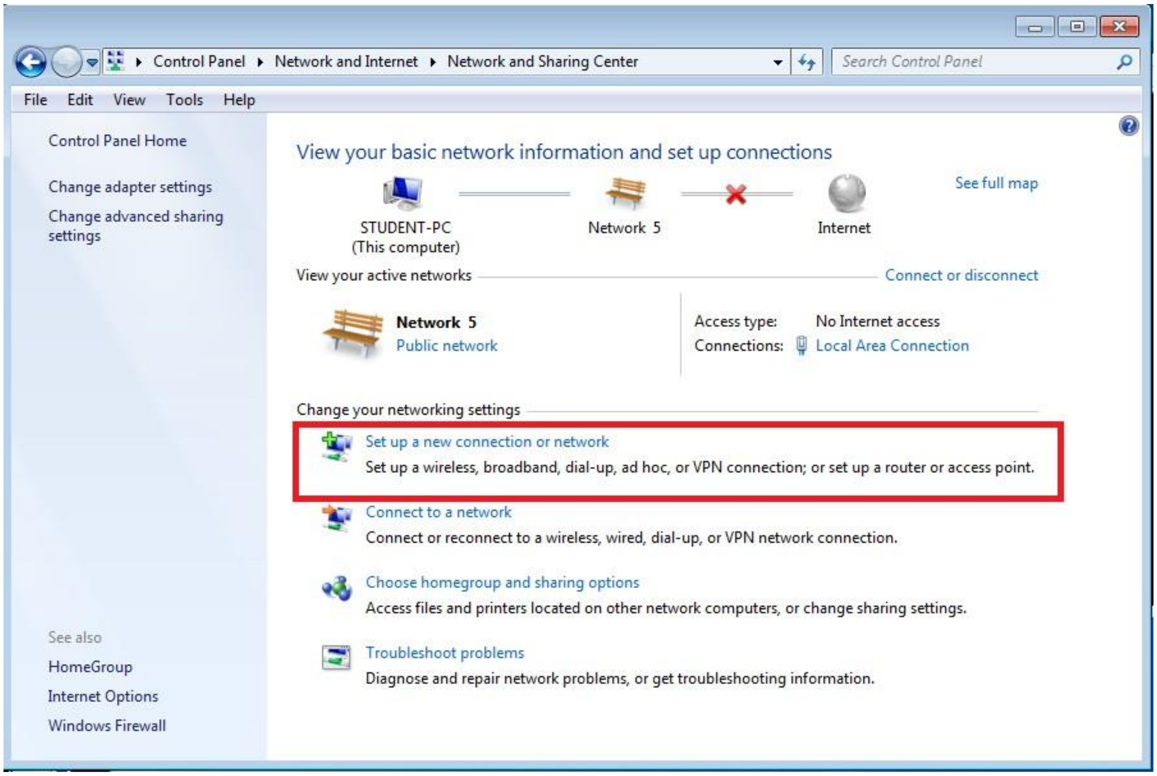
5. In the Control Panel, click on **Network and Internet.**


Control Panel
View
Tools
Help
Adjust your computer's settings
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options

6. Click the **Network and Sharing Center** link under Network and Internet.


Control Panel ▸ Network and Internet ▸
Search Control Panel
File
Edit
View
Tools
Help
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Add a wireless device to the network
HomeGroup
Choose homegroup and sharing options
Internet Options
Connect to the Internet
Change your homepage
Manage browser add-ons
Delete browsing history and cookies

7. Click the link to **Set up a new connection or network**.



View your basic network information and set up connections

View your active networks

Network 5
Public network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

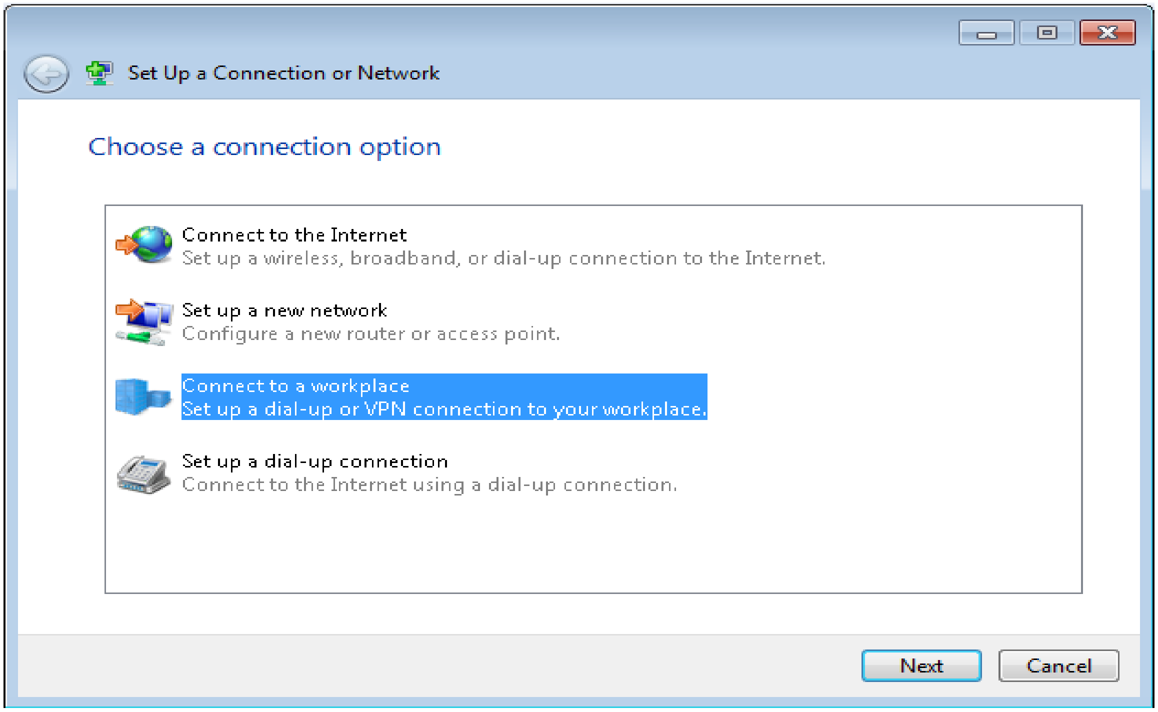
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

8. Select **Connect to a workplace** and click the **Next** button.



Choose a connection option

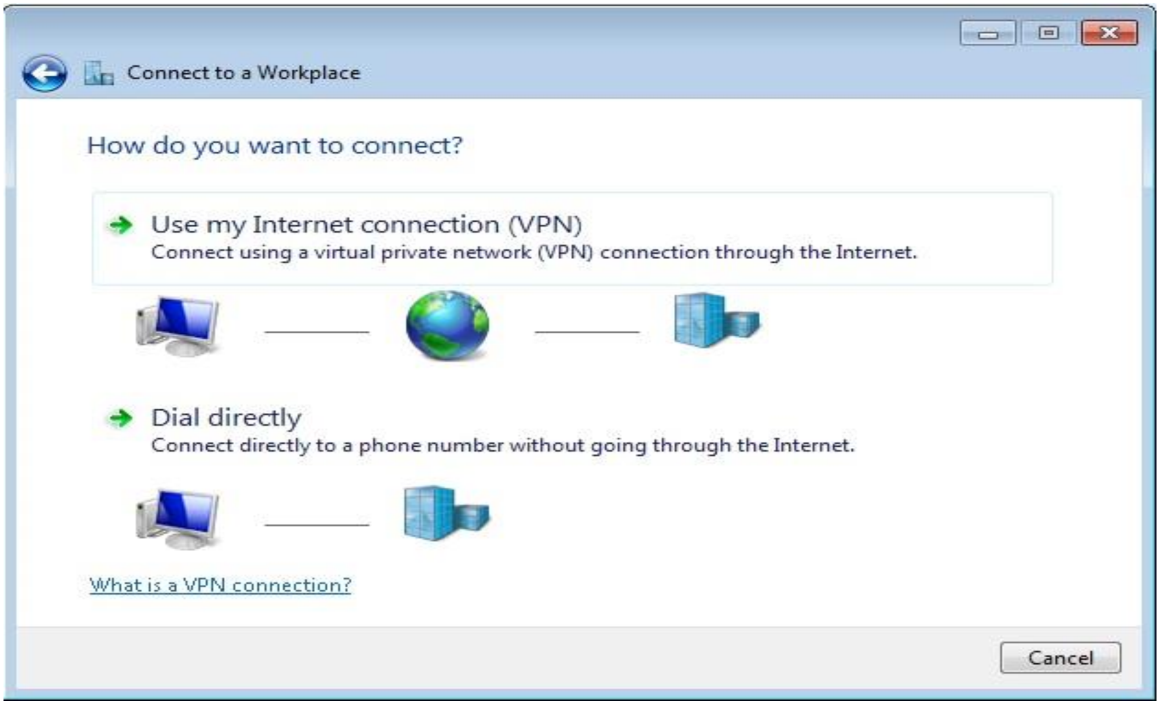
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

9. Select the top choice of **Use my Internet connection (VPN).**



Connect to a Workplace

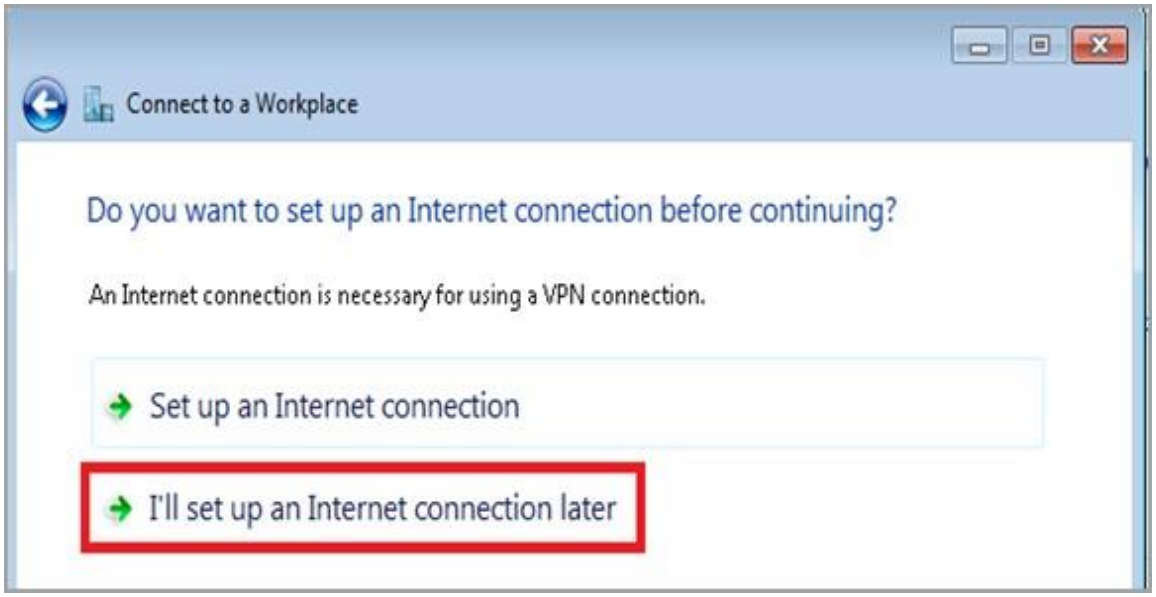
How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

10. Select **I'll set up an Internet connection later**.



Connect to a Workplace

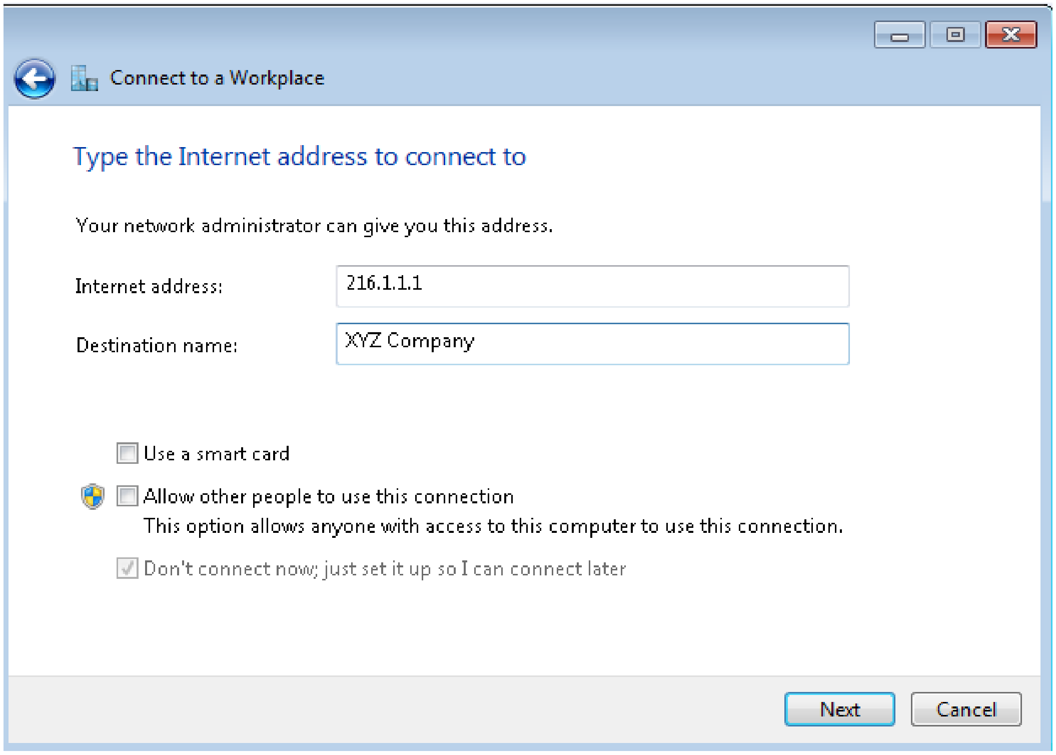
Do you want to set up an Internet connection before continuing?

An Internet connection is necessary for using a VPN connection.

→ Set up an Internet connection

→ I'll set up an Internet connection later

11. Type **216.1.1.1** for the Internet Address and **XYZ Company** for Destination name. Click the **Next** button to continue the VPN client setup process on Windows 7.



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 216.1.1.1

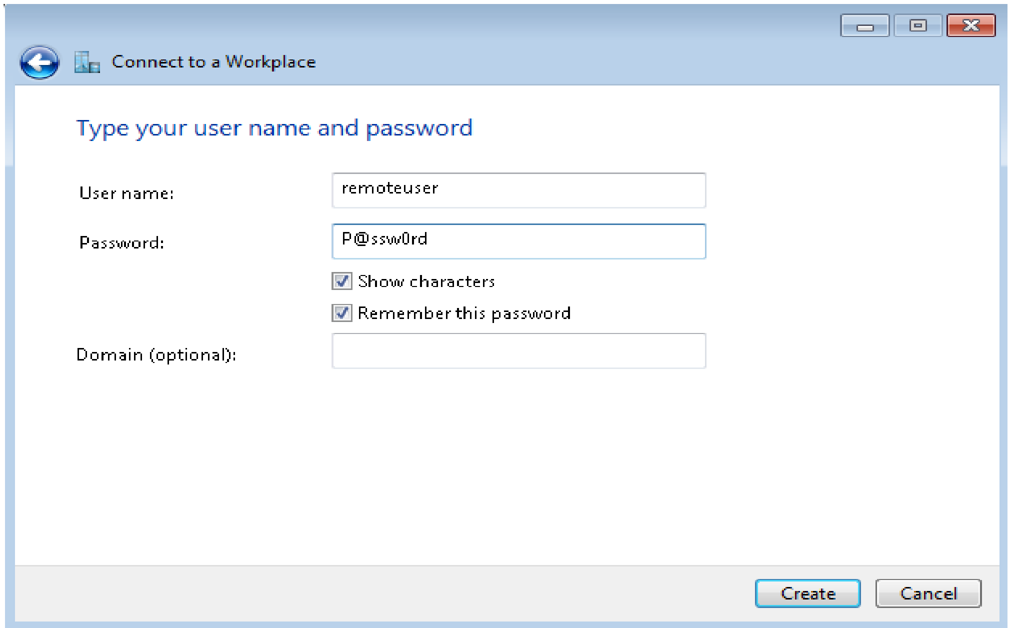
Destination name: XYZ Company

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

12. Type **remoteuser** for the username and **P@ssw0rd** for the password. If you prefer, you can click the show characters box to verify you typed the correct password (if you do this, watch out for shoulder surfing). Also, check the box to **Remember this password** so it does not have to be retyped again. Click **Create**.



Type your user name and password

User name: remoteuser

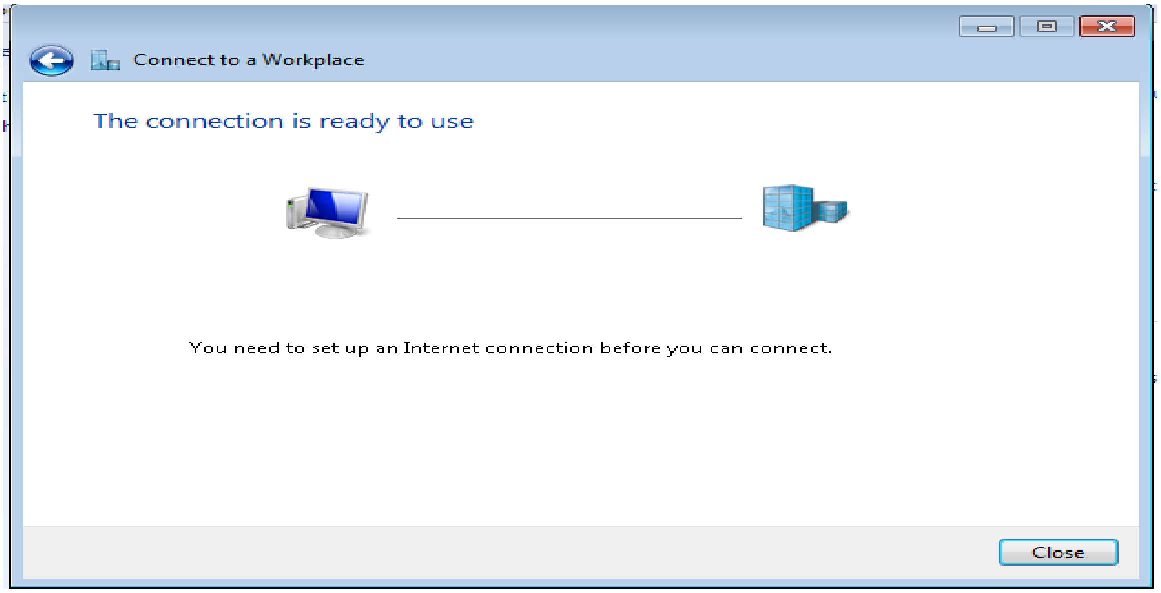
Password: P@ssw0rd

☑ Show characters

☑ Remember this password

Domain (optional):

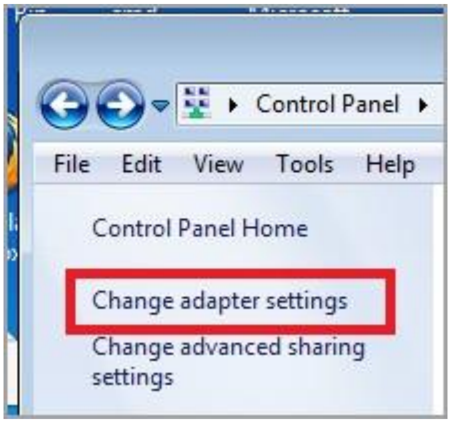
13. You will receive the message that the connection is ready to use. Click **Close**.



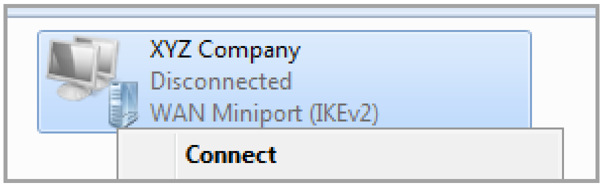
The connection is ready to use

You need to set up an Internet connection before you can connect.

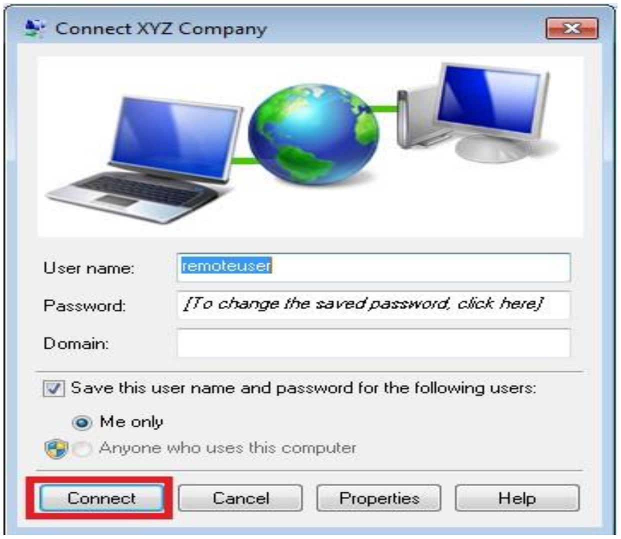
14. Click the link in the top-left pane to **Change adapter settings**.



15. Right-click on the **XYZ Company** Network Card and click **Connect**.



16. Click the **Connect** button to connect to the Windows 2008 VPN Server.



User name: remoteuser

Password: [To change the saved password, click here]

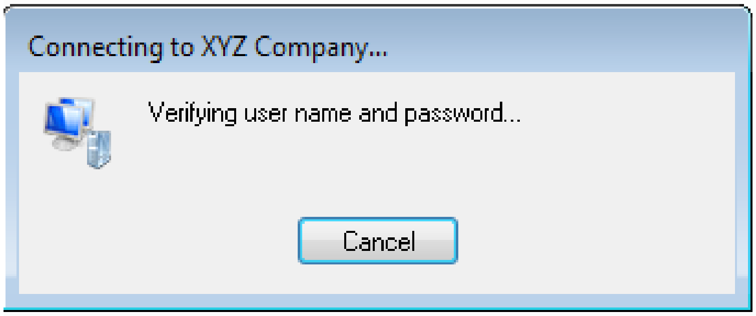
Domain:

☑ Save this user name and password for the following users:

● Me only

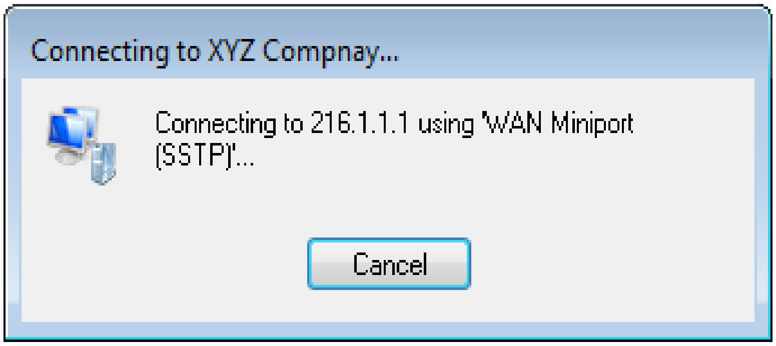
○ Anyone who uses this computer

A box will be temporarily displayed saying, *"verifying username and password".*


Connecting to XYZ Company...

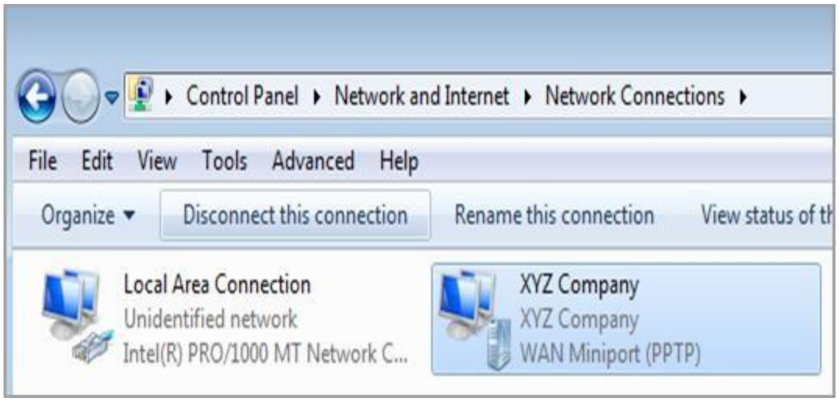
Verifying user name and password...

A box will be displayed that states, *"Connecting to 216.1.1.1 using WAN Miniport (SSTP)"*

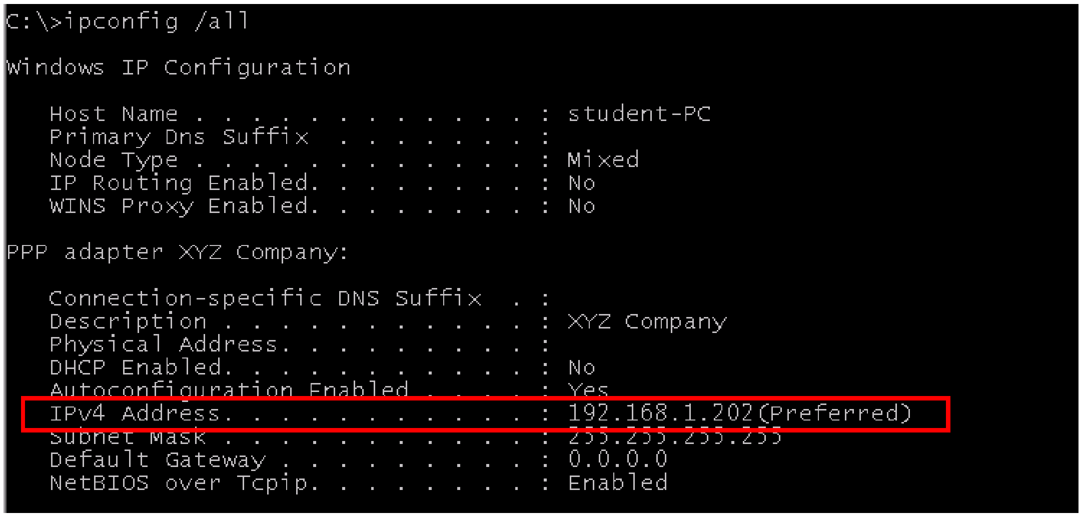

Connecting to XYZ Compnay...

Connecting to 216.1.1.1 using 'WAN Miniport (SSTP)'...

17. After the connection is successful, you will receive an IP address from the VPN.


Control Panel ▸ Network and Internet ▸ Network Connections ▸
File Edit View Tools Advanced Help
Organize ▾
Disconnect this connection
Rename this connection
View status of th
Local Area Connection
Unidentified network
Intel(R) PRO/1000 MT Network C...
XYZ Company
XYZ Company
WAN Miniport (PPTP)

18. Go back to the command prompt and type the following command:
C:\>**ipconfig /all**



```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : student-PC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

PPP adapter XYZ Company:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : XYZ Company
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.202(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

You may have to scroll up to find the PPP adapter XYZ Company

2.2 Conclusion

When you use a Virtual Private Network (VPN), users can connect to internal systems and access resources. Users must have accounts with proper credentials in order to successfully authenticate to the server. After establishing a VPN connection with a remote server, the client will be issued a new IP address allowing internal access.

2.3 Discussion Questions

1. Where do you go to connect to a VPN server in Windows 7?
   Ans: Select Control Panel > Network and Internet > Network Sharing Centre > Connect to a workplace > use my Internet Connection (VPN).
2. What is the command to manage accounts on Server 2008?
   Ans: To manage accounts on server lusrmgr.msc.
3. What tab must be configured so a user can obtain remote access?
   Ans: User to obtain remote access, the "Remote Access" or "VPN" tab must be configured.
4. After connecting to a VPN server, will you have an additional address?
   Ans: Yes, after connecting to a VPN server an IP address will change to additional address.

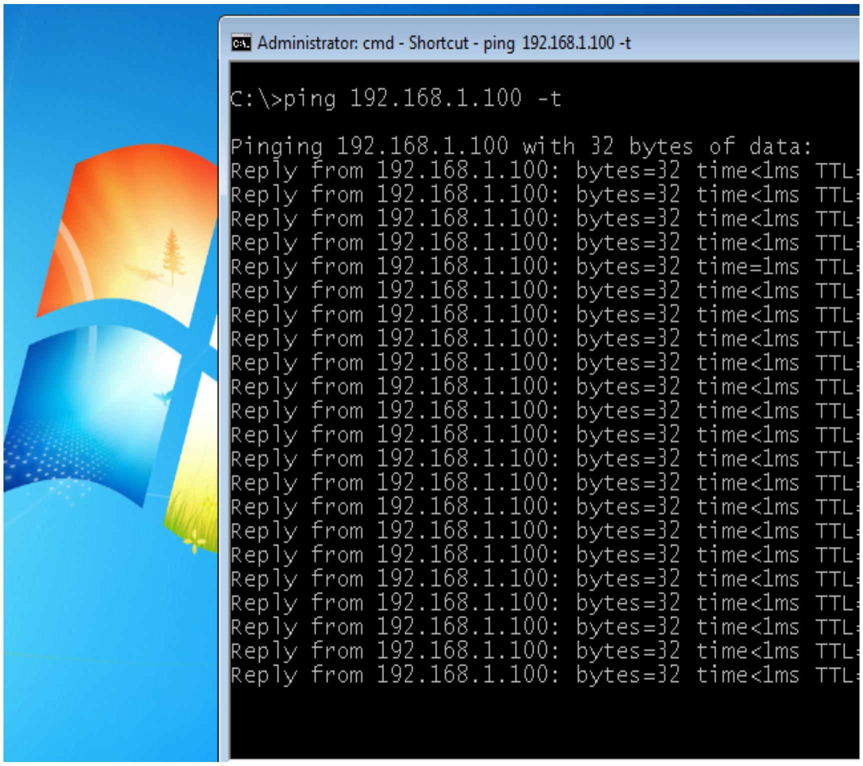
3 Using Internal Services from an External Machine

Now that we have successfully connected to the VPN server and received an IP address on the 192.168.1.0/24 network, we can access some of the company's internal resources, all over a secure connection.

3.1 Testing the Firewall

1. From the command prompt on the **Windows 7 External Machine**, type the following to continuously ping the Windows 2008 Internal Server Machine that is a Domain Controller and running IIS.

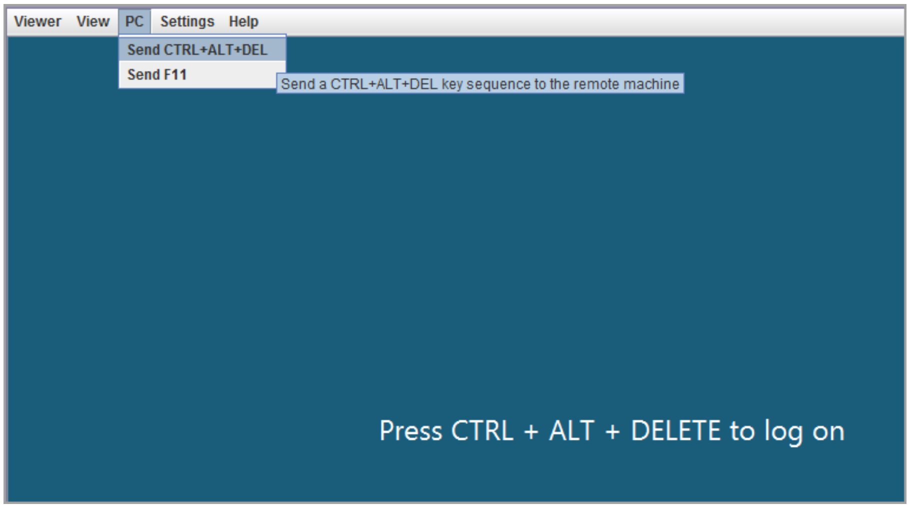
   C:\>**ping 192.168.1.100 -t**



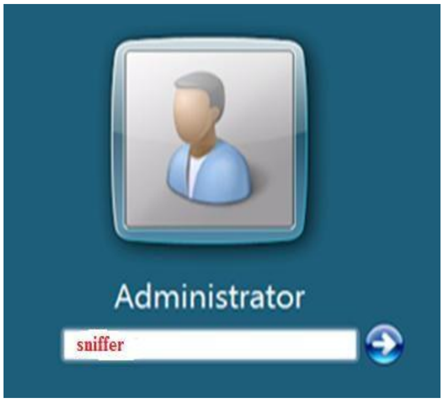
```
C:\>ping 192.168.1.100 -t

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time=1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
Reply from 192.168.1.100: bytes=32 time<1ms TTL
```

Do not stop the ping. At a later time, you can press Ctrl+C to stop the ping.

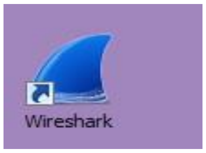
2. Log into the **Windows 2008 Sniffer Server** by clicking the Windows 2008 Sniffer icon on the topology. Click **PC** in the upper-left and **Send Ctrl+Alt+Del** in order to log on to the Windows 2008 server.


Viewer
View
PC
Settings
Help
Send CTRL+ALT+DEL
Send F11
Send a CTRL+ALT+DEL key sequence to the remote machine
Press CTRL + ALT + DELETE to log on

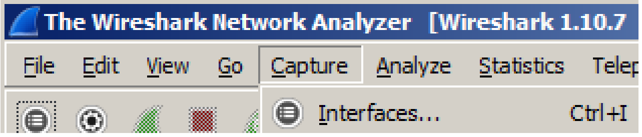
3. Enter **sniffer** for the Administrator password to the Windows 2008 Server.



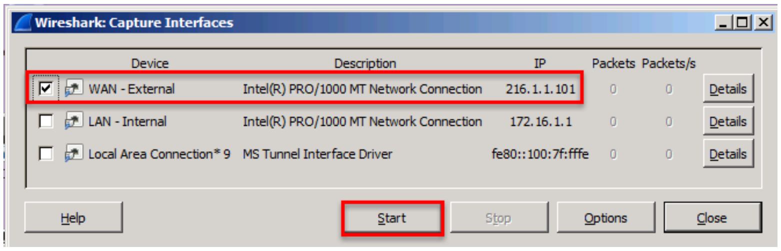
4. Double-click on the shortcut to **Wireshark** on the desktop to launch the program.



5. Click on **Capture** from the menu bar and select **Interfaces**.



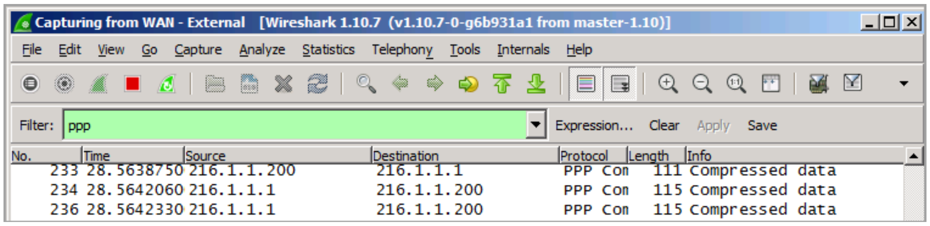
6. Select the **WAN – External** interface check-box. Click **Start**.



Wireshark: Capture Interfaces

	Device	Description	IP	Packets	Packets/s	
☑	WAN - External	Intel(R) PRO/1000 MT Network Connection	216.1.1.101	0	0	Details
☐	LAN - Internal	Intel(R) PRO/1000 MT Network Connection	172.16.1.1	0	0	Details
☐	Local Area Connection* 9	MS Tunnel Interface Driver	fe80::100:7f:fffe	0	0	Details

7. Type **ppp** in the Wireshark filter pane and click Apply.



Capturing from WAN - External [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

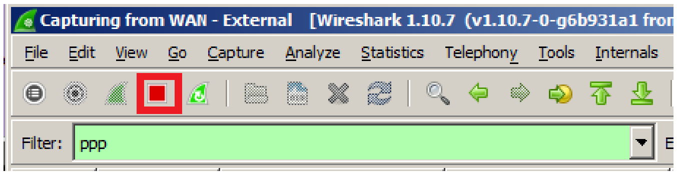
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ppp

```
No.    Time        Source       Destination   Protocol Length Info
 233 28.5638750 216.1.1.200   216.1.1.1      PPP Con  111 Compressed data
 234 28.5642060 216.1.1.1     216.1.1.200    PPP Con  115 Compressed data
 236 28.5642330 216.1.1.1     216.1.1.200    PPP Con  115 Compressed data
```

On the WAN side, you will not see the ICMP traffic between the Windows 7 VPN Client machine and the Windows server 2008 machine on the company's internal network.

8. Click on **red square** to stop the capture on the WAN – External interface.

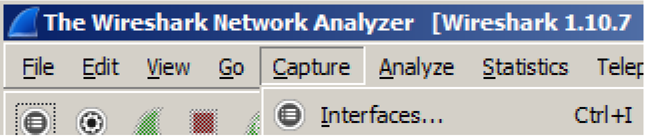


Capturing from WAN - External [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 fro

File Edit View Go Capture Analyze Statistics Telephony Tools Internals

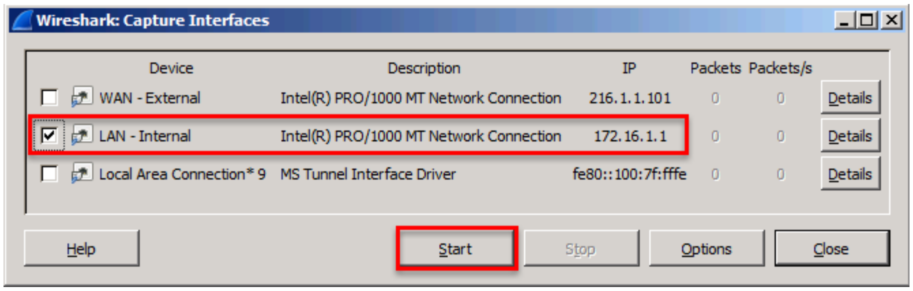
Filter: ppp

9. Click on **Capture** from the menu bar and select **Interfaces.**



The Wireshark Network Analyzer [Wireshark 1.10.7
File Edit View Go Capture Analyze Statistics Telep
Interfaces... Ctrl+I

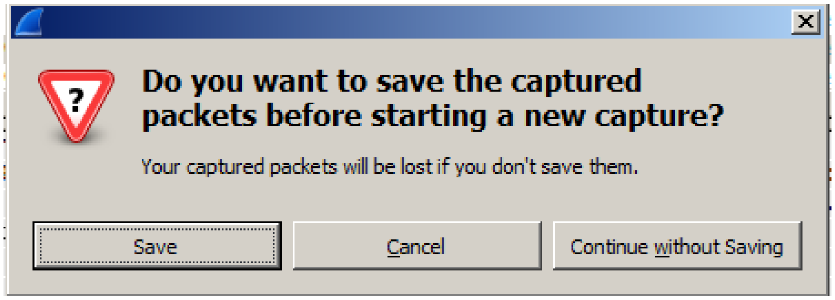
10. Deselect WAN – External and select the **LAN – Internal** check box. Click the **Start** button.



Wireshark: Capture Interfaces

	Device	Description	IP	Packets	Packets/s	
☐	WAN - External	Intel(R) PRO/1000 MT Network Connection	216.1.1.101	0	0	Details
☑	LAN - Internal	Intel(R) PRO/1000 MT Network Connection	172.16.1.1	0	0	Details
☐	Local Area Connection* 9	MS Tunnel Interface Driver	fe80::100:7f:fffe	0	0	Details

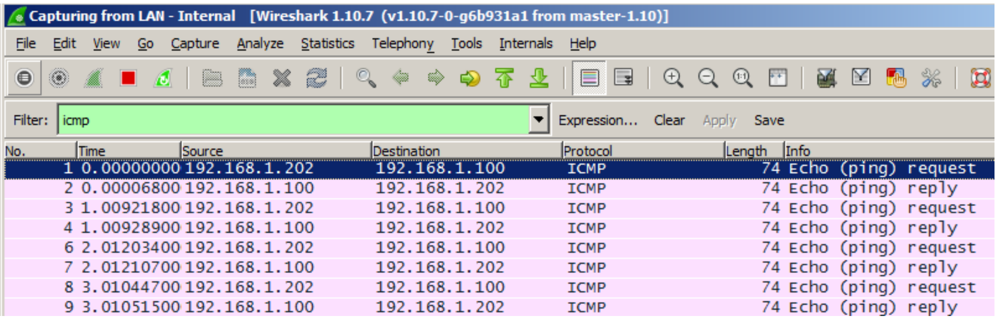
11. Click on **Continue without saving** to start a new packet capture.



Do you want to save the captured packets before starting a new capture?

Your captured packets will be lost if you don't save them.

12. Type **icmp** in the Wireshark filter pane and click **Apply**. Although traffic is encrypted to the VPN server, it is decrypted on the LAN, unless a protocol that supports encryption, such as HTTPS or SSH is being utilized.



Capturing from LAN - Internal [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

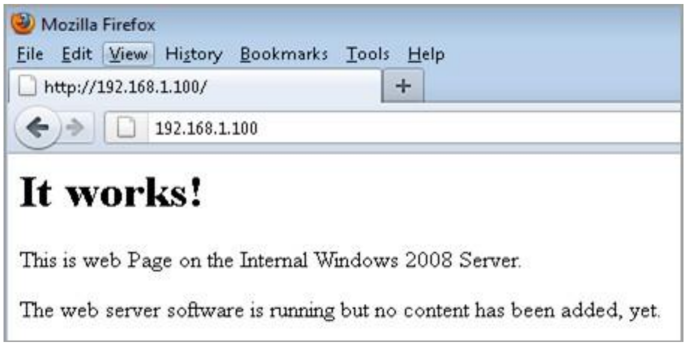
Filter: icmp

```
No.  Time        Source         Destination    Protocol  Length Info
  1 0.00000000 192.168.1.202  192.168.1.100  ICMP        74 Echo (ping) request
  2 0.00006800 192.168.1.100  192.168.1.202  ICMP        74 Echo (ping) reply
  3 1.00921800 192.168.1.202  192.168.1.100  ICMP        74 Echo (ping) request
  4 1.00928900 192.168.1.100  192.168.1.202  ICMP        74 Echo (ping) reply
  6 2.01203400 192.168.1.202  192.168.1.100  ICMP        74 Echo (ping) request
  7 2.01210700 192.168.1.100  192.168.1.202  ICMP        74 Echo (ping) reply
  8 3.01044700 192.168.1.202  192.168.1.100  ICMP        74 Echo (ping) request
  9 3.01051500 192.168.1.100  192.168.1.202  ICMP        74 Echo (ping) reply
```

Go back to the **Windows 7 External machine**. Press **CTRL+C** to stop the continuous ping.

13. Double-click on the shortcut to **Firefox** on the desktop.

14. Type **http://192.168.1.100** in the URL bar to connect to the internal web site.

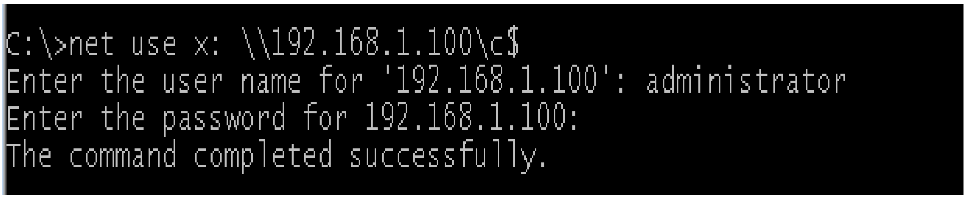


It works!

This is web Page on the Internal Windows 2008 Server.

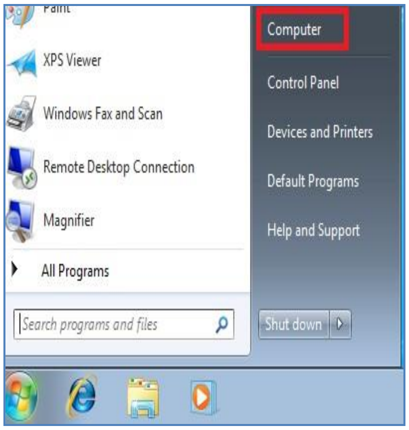
The web server software is running but no content has been added, yet.

15. From the command prompt, type the following command:
C:\>**net use x: \\192.168.1.100\c$**
When you are asked to enter the user name, type **administrator**
When you are asked for the password, type **P@ssw0rd**

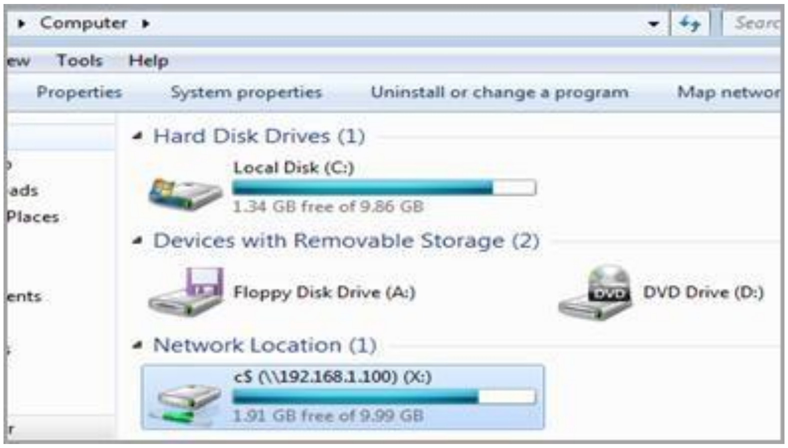


```
C:\>net use x: \\192.168.1.100\c$
Enter the user name for '192.168.1.100': administrator
Enter the password for 192.168.1.100:
The command completed successfully.
```

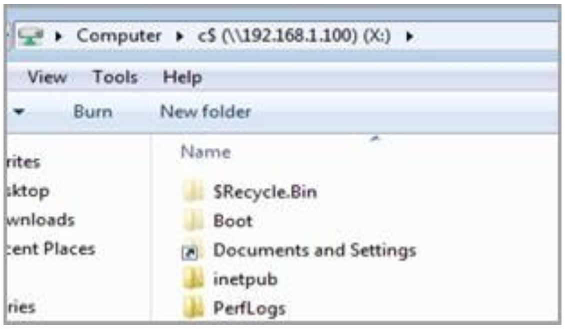
16. Click on the **Start** button and go to the **Computer** link.



17. Double-click the Network Location Link for - **c$ (\\192.168.1.100) (X:).**

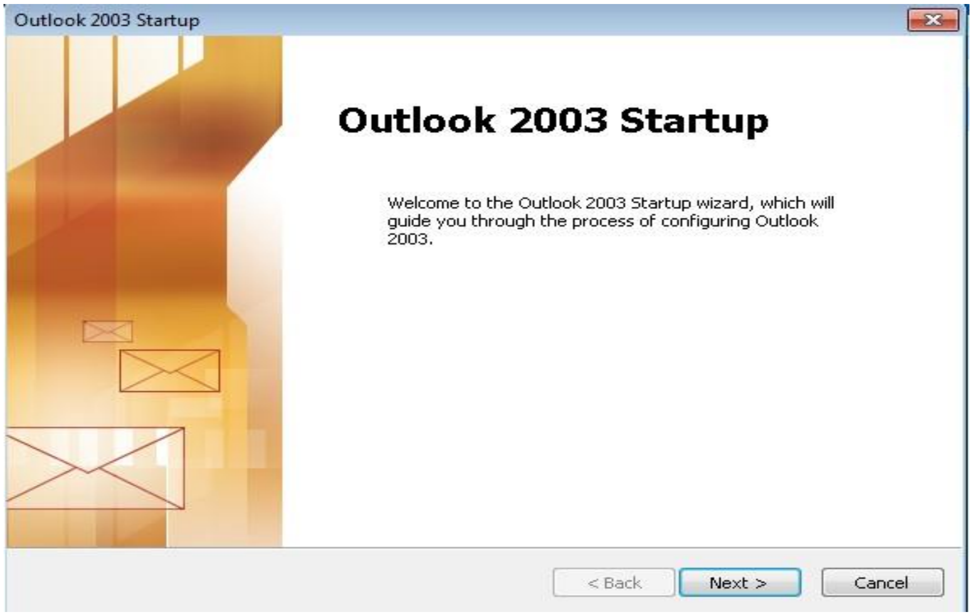


18. View the C: Drive of the Remote Computer.



19. Navigate to the desktop and double-click on the shortcut to **Outlook**.

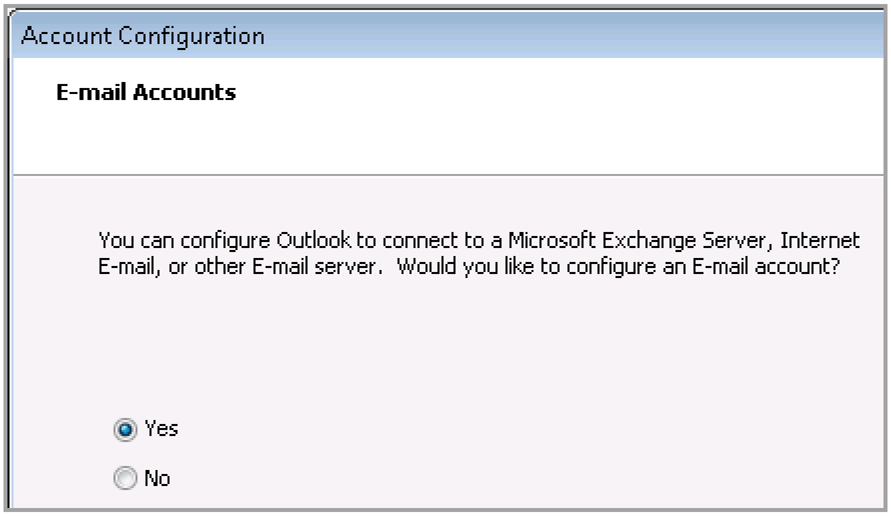
20. Click **Next** on the Outlook 2003 Startup screen.



Outlook 2003 Startup

Welcome to the Outlook 2003 Startup wizard, which will guide you through the process of configuring Outlook 2003.

21. On the Account Configuration window, click **Next**.



Account Configuration

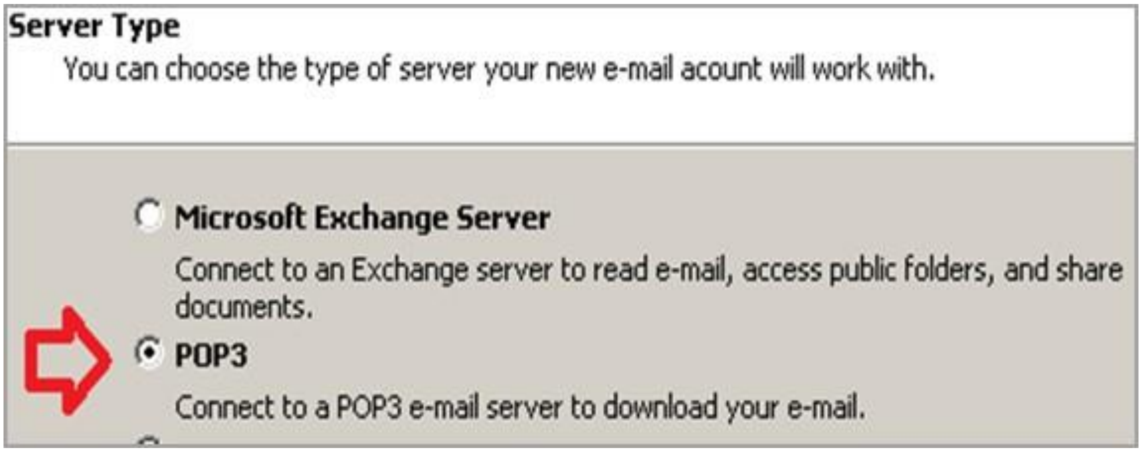
E-mail Accounts

You can configure Outlook to connect to a Microsoft Exchange Server, Internet E-mail, or other E-mail server. Would you like to configure an E-mail account?

● Yes

○ No

22. Select **POP3** (Post Office Protocol) as the server type. Click the **Next** button.



Server Type

You can choose the type of server your new e-mail acount will work with.

○ **Microsoft Exchange Server**

Connect to an Exchange server to read e-mail, access public folders, and share documents.

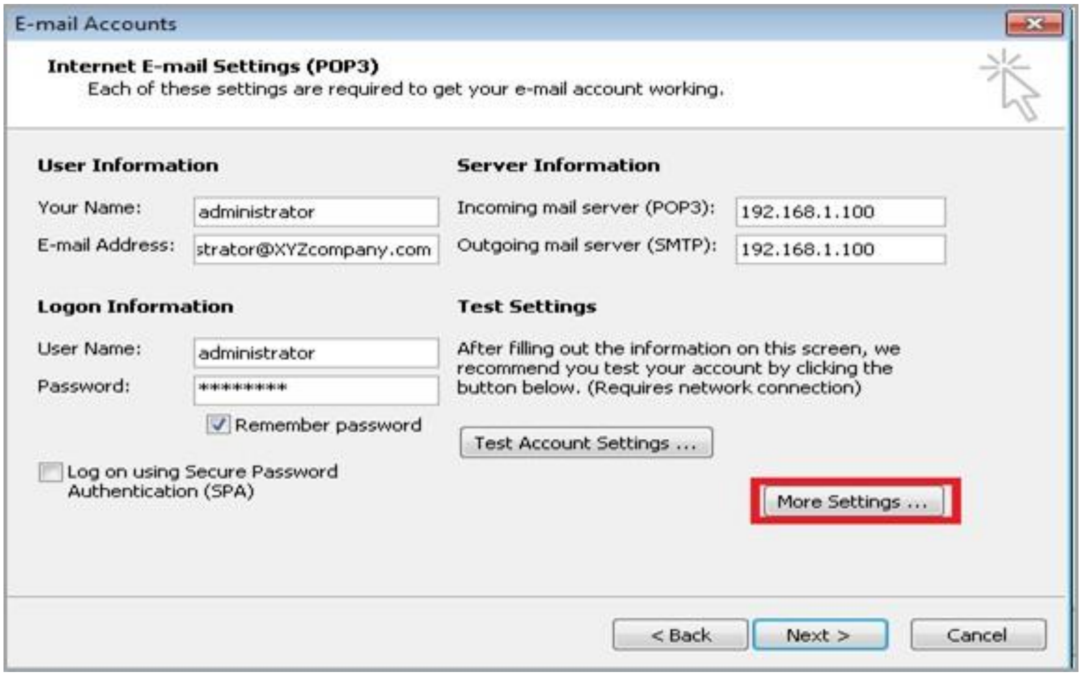
● **POP3**

Connect to a POP3 e-mail server to download your e-mail.

23. Fill out the following fields:

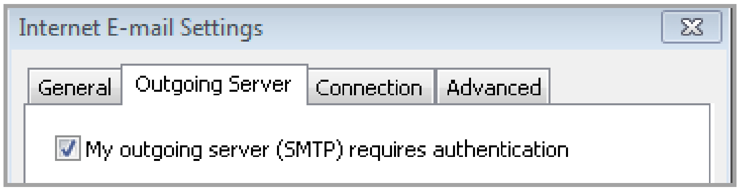
Name	administrator
Email Address	administrator@XYZcompany.com
User Name	administrator
Password	P@ssw0rd
Incoming mail server (POP3)	192.168.1.100
Outgoing mail server (SMTP)	192.168.1.100

24. Click the **More Settings** button.


E-mail Accounts
Internet E-mail Settings (POP3)
Each of these settings are required to get your e-mail account working.
User Information
Server Information
Logon Information
Test Settings
After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)
Test Account Settings ...
More Settings ...
< Back
Next >
Cancel

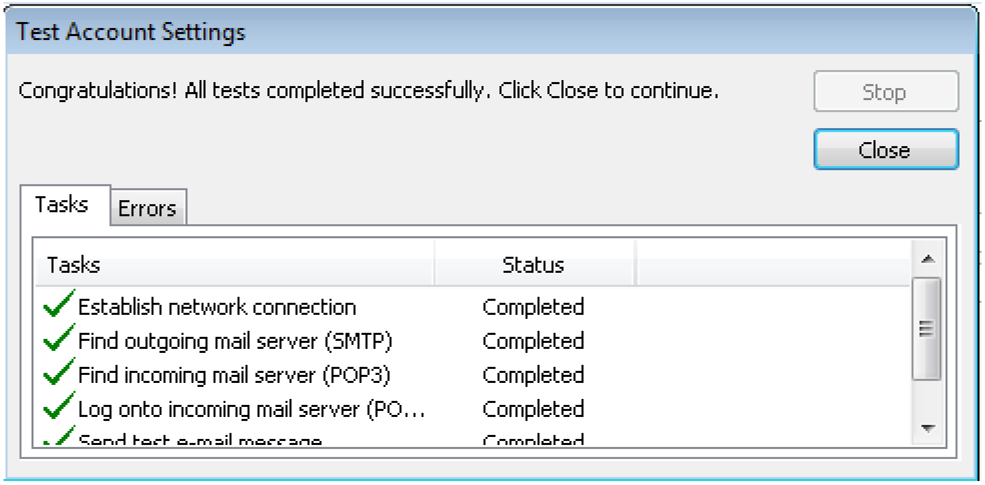
Your Name: administrator
E-mail Address: strator@XYZcompany.com
Incoming mail server (POP3): 192.168.1.100
Outgoing mail server (SMTP): 192.168.1.100
User Name: administrator
Password: *********
☑ Remember password
□ Log on using Secure Password Authentication (SPA)

25. Click on the **Outgoing Server** tab and check the box that states**, My outgoing server (SMTP) requires authentication.** Click **OK**.



☑ My outgoing server (SMTP) requires authentication

26. Click the **Test Account Settings** button. You should receive 5 green checks.


Test Account Settings

Congratulations! All tests completed successfully. Click Close to continue.

Tasks	Status
✓ Establish network connection	Completed
✓ Find outgoing mail server (SMTP)	Completed
✓ Find incoming mail server (POP3)	Completed
✓ Log onto incoming mail server (PO...	Completed
✓ Send test e-mail message	Completed

27. Close all open windows and PC viewers. End the reservation.

3.2 Conclusion

In this section of the lab, we connected to the resources on the internal network, including an internal website, a share on the domain controller, and we used internal Email. VPN connections allow users to work from home as if they were on the physical computer network, all over an encrypted connection over the Internet.

3.3 Discussion Questions

1. What is the command to map a drive?
   Ans: Net use is the command for replacing the drive letter type.
2. How can you view a mapped drive?
   Ans: It can be viewed by Double-clicking the mapped drive under Network. Locations.
3. What filter in Wireshark will allow you to see VPN traffic over the WAN?
   Ans: Wireshark will allow you to see VPN traffic over the WAN.
   by using the GCV adaptor
4. What filter in Wireshark will allow you to view the results of a ping command?
   Ans: To view the results of a ping command in Wireshark ICMP filter is used.

References

1. nmap:
   http://www.nmap.org

2. PPTP:
   http://searchnetworking.techtarget.com/definition/Point-to-Point-Tunneling-Protocol

3. VPN:
   http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs

4. Routing and Remote Access on Windows Server 2008:
   http://technet.microsoft.com/en-us/library/cc770798(v=ws.10).aspx

5. More PPTP Information:
   http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol