NETWORK SECURITY LAB SERIES

Lab 14: Configuring a Site to Branch Virtual Private Network

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. Setting up the Branch Office Machines
2. Configuring the Main Office VPN Server and the Branch Server
3. Accessing Resources on the Remote Network

Key terms for this lab:

Branch Office – Part of a company's network may be located in a different physical location. This other part of the network is often referred to as a branch office.

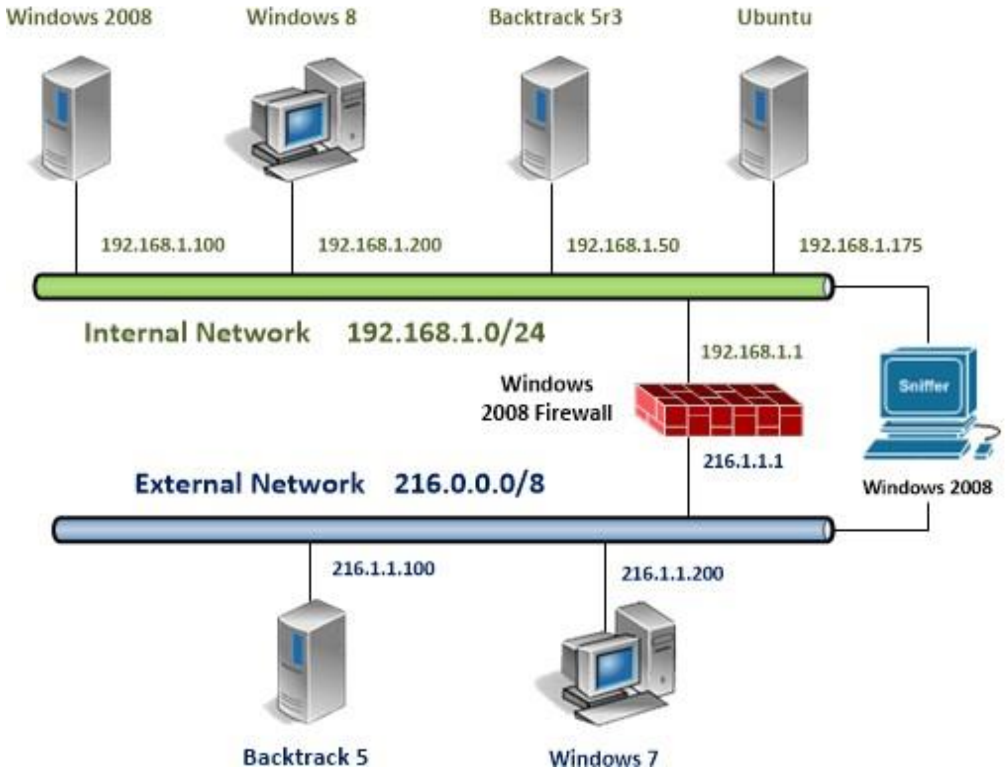
RIPv2 – Routing Information Protocol, Version 2, uses a multicast address to update information about routing over UDP (User Datagram Protocol) port 520.

UDP – User Datagram Protocol is a connection-less oriented protocol in contrast to TCP (Transmission Control Protocol) which is a connection-oriented protocol.

Wireshark – A Protocol Analyzer that will allow you to capture traffic.

Routing and Remote Access – A Microsoft Application Program Interface (API) and server software that makes it possible to create applications to administer the routing and remote access service capabilities of the operating system, to function as a network router.

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 2008 Internal Machine	192.168.1.100	Administrator	P@ssw0rd
Windows 8 Internal Machine	192.168.1.200	Student	password
Ubuntu Internal Machine	192.168.1.175	Sysadmin	P@ssw0rd
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.

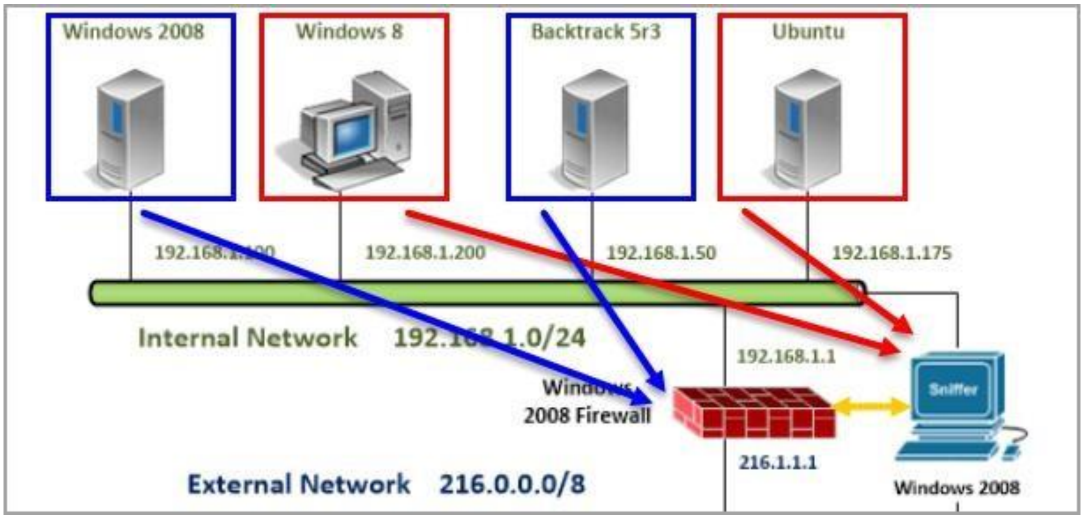
At the end of the lab, remember to close all open windows and close the PC viewers.

1 Configuring the Branch Office Machines

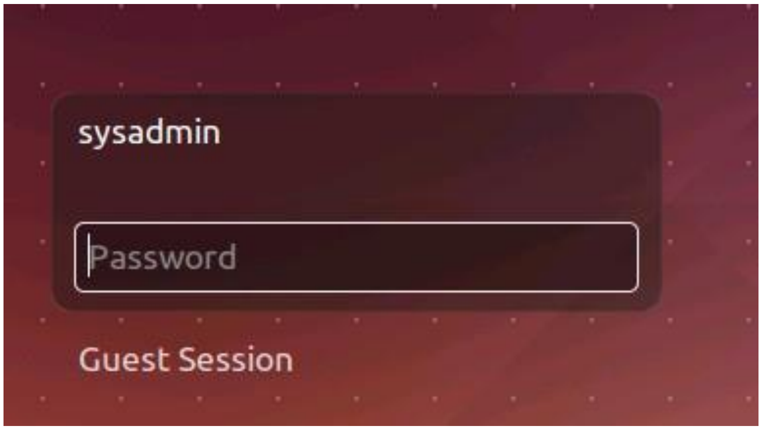
In this section, we will change the IP address of the Windows 8 Internal Machine and the Ubuntu Internal Machine so that they will be on a different network. These machines will be part of a branch office.

1.1 Changing Networks for Ubuntu and Windows 8

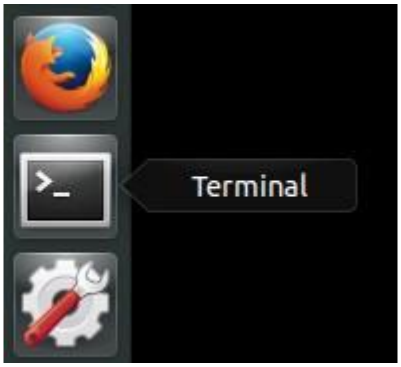
We will now change the IP addresses of some machines on the internal Network. There will be two subnets, 172.16.1.0/24 and 192.168.1.0/24. The Windows 8 Internal Machine and Ubuntu Internal Machines will be part of a branch office. The Windows 2008 Internal Machine and BackTrack 5 R3 Internal Machine are going to stay part of the main site, so those machines will not need to be reconfigured.



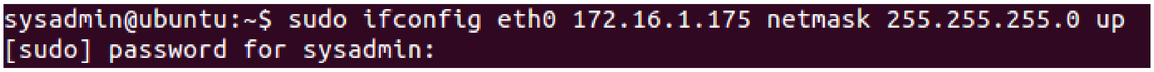
1. Click on the **Ubuntu Server** icon on the topology. Log on as the user **sysadmin** with the password of **P@ssw0rd**.



2. Open the terminal by clicking on the **Terminal** icon on the left side of the screen.

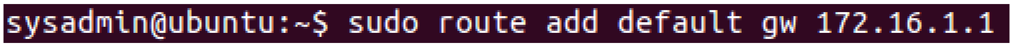


3. Type the following command to set the IP address of the Ubuntu Server: sysadmin@ubuntu:~# **sudo ifconfig eth0 172.16.1.175 netmask 255.255.255.0 up.** Type **P@ssw0rd** as the sudo password.



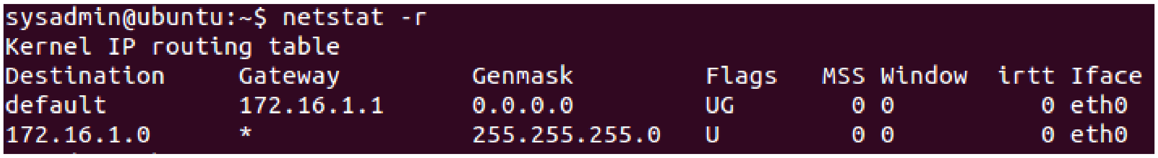
```
sysadmin@ubuntu:~$ sudo ifconfig eth0 172.16.1.175 netmask 255.255.255.0 up
[sudo] password for sysadmin:
```

4. Type the following command to set the Gateway of the Ubuntu Server: sysadmin@ubuntu:~# **sudo route add default gw 172.16.1.1**



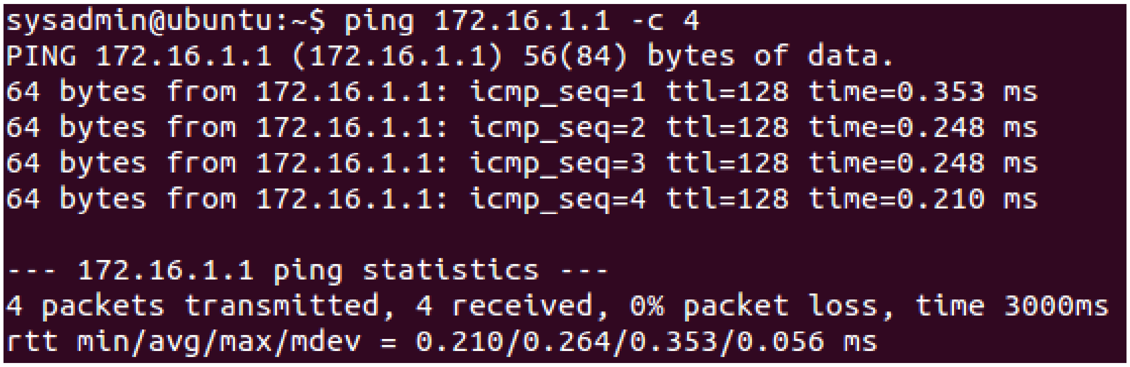
```
sysadmin@ubuntu:~$ sudo route add default gw 172.16.1.1
```

5. Type the following command to view the gateway of the Ubuntu Server: sysadmin@ubuntu:~# **netstat -r**



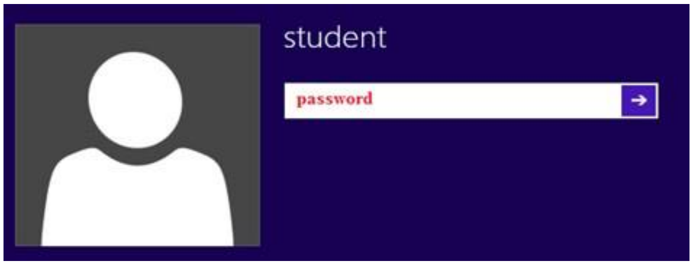
```
sysadmin@ubuntu:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         172.16.1.1      0.0.0.0         UG        0 0          0 eth0
172.16.1.0      *               255.255.255.0   U         0 0          0 eth0
```

6. Type the following command to ping the gateway four times: root@ubuntu:~# **ping 172.16.1.1 –c 4**

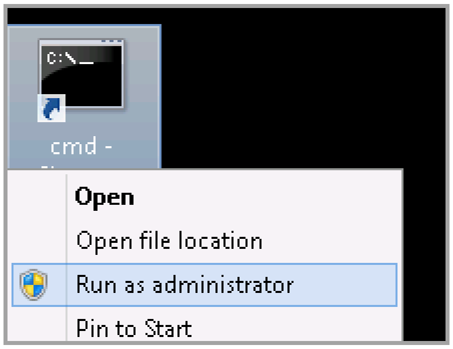


```
sysadmin@ubuntu:~$ ping 172.16.1.1 -c 4
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=128 time=0.353 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=128 time=0.248 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=128 time=0.248 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=128 time=0.210 ms

--- 172.16.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.210/0.264/0.353/0.056 ms
```

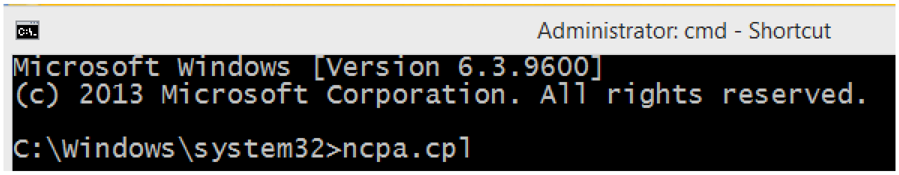
7. Click on the **Windows 8** icon on the lab topology to bring up the login screen. For the student password, type **password**, and then press **Enter**.



8. Right-click on the cmd-Shortcut on the desktop and select **Run as Administrator**.

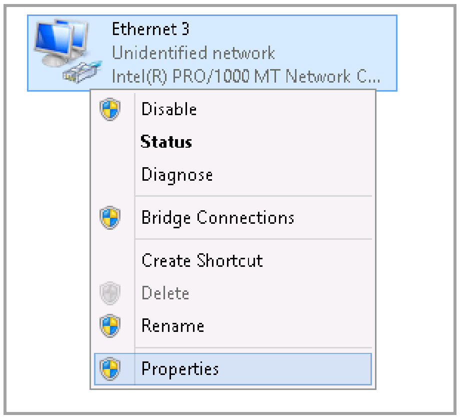


9. Type the following command to go to the root of the C: Drive C:\Windows\system32>**ncpa.cpl**

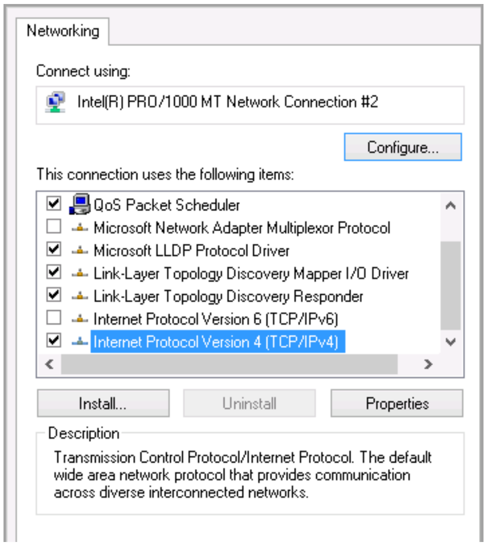


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ncpa.cpl
```

10. Right-click on **Ethernet 3** and select **Properties** from the menu-bar.



11. Scroll down to **Internet Protocol (TCP/IPv4)** and double-click on it.



Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection #2

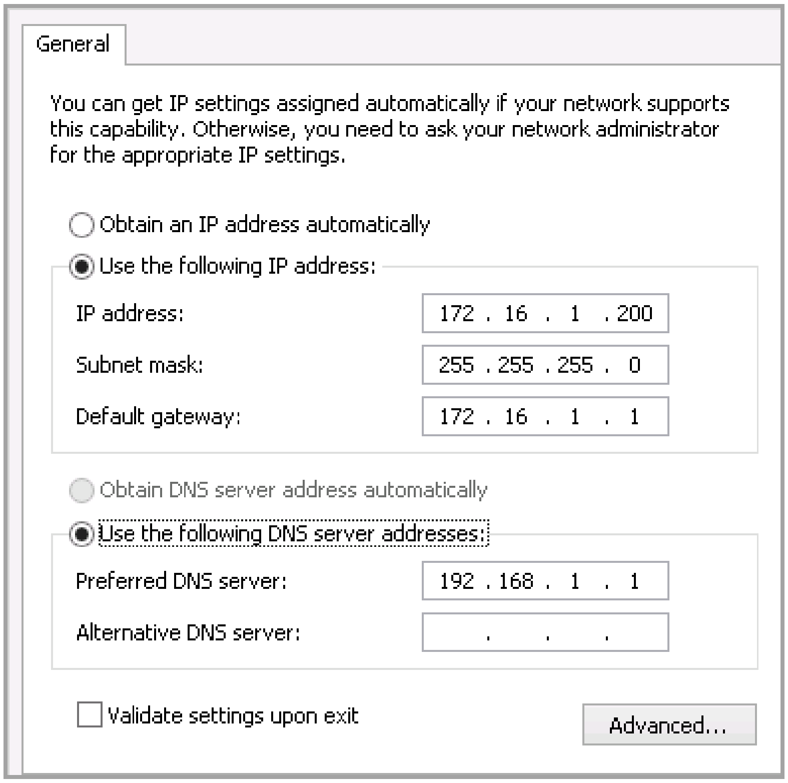
This connection uses the following items:

- ☑ QoS Packet Scheduler
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- □ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

12. Change the IP address to **172.16.1.200** and the Default Gateway to **172.16.1.1.** Leave the Subnet Mask and DNS (Domain Name System) fields alone. Click **OK** twice.



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 172 . 16 . 1 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 172 . 16 . 1 . 1

○ Obtain DNS server address automatically

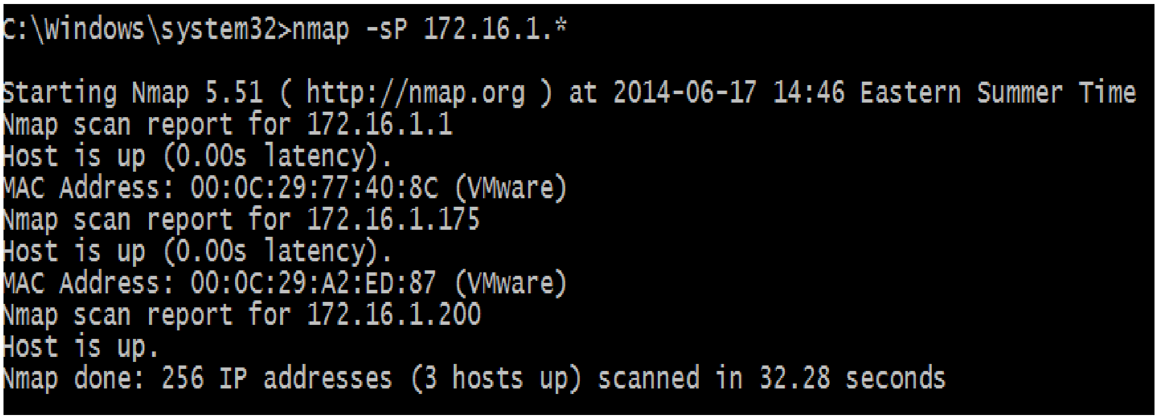
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

Alternative DNS server: . . .

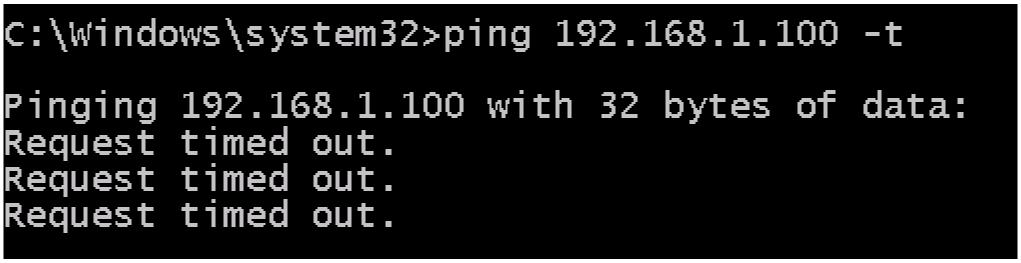
□ Validate settings upon exit

13. Go back to the command prompt and type the following command to scan the 172.16.1.0/24 network for the 3 hosts. This may take a few seconds.
C:\>**nmap –sP 172.16.1.***



```
C:\Windows\system32>nmap -sP 172.16.1.*

Starting Nmap 5.51 ( http://nmap.org ) at 2014-06-17 14:46 Eastern Summer Time
Nmap scan report for 172.16.1.1
Host is up (0.00s latency).
MAC Address: 00:0C:29:77:40:8C (VMware)
Nmap scan report for 172.16.1.175
Host is up (0.00s latency).
MAC Address: 00:0C:29:A2:ED:87 (VMware)
Nmap scan report for 172.16.1.200
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 32.28 seconds
```

14. To prove that computers on the 172.16.1.0/24 subnet cannot reach the computers on the 192.168.1.0/24 subnet, type the following command:
C:\>**ping 192.168.1.100 -t**



```
C:\Windows\system32>ping 192.168.1.100 -t

Pinging 192.168.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

Do not stop the ping. We will return to this later in the lab.

1.2 Conclusion

A branch network will likely be on a different IP subnet than the main site or location, and likely have a different gateway. A branch site is a part of a company's network that may be located in a different physical location. Branches can be connected by using a VPN.

1.3 Discussion Questions

1. What is a Branch Office?
Ans: When two internal machines work together it comes under Branch Office.

2. What is the command to set your IP address in Linux?
Ans: The Command to set your IP address in Linux is sudo ifconfig eth0 172.16.1.175 netmask 255.255.255.0.

3. What is the command to set your Gateway Address in Linux?
   Ans: The command to set your Gateway Address in Linux is sudo route add default gw 172.16.1.1.

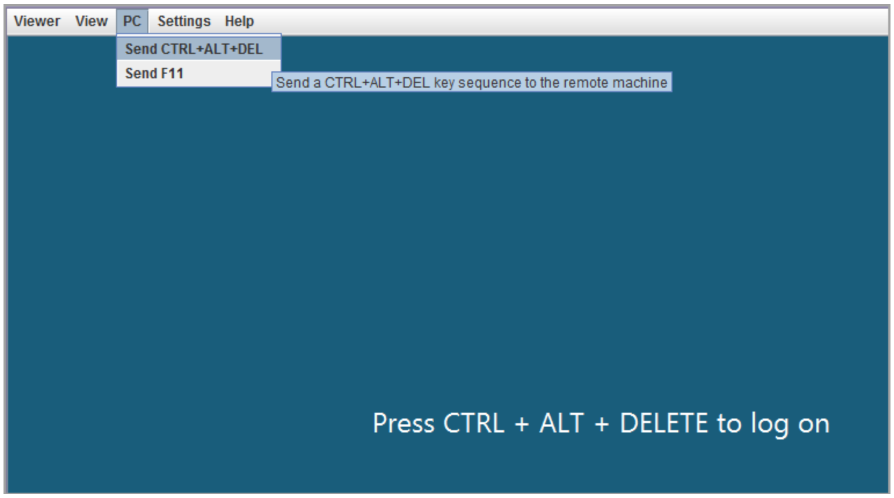
4. What is the command to view your Gateway address in Linux?
   Ans: netstat -r.

2 Configuring the Main Office VPN Server and the Branch Server

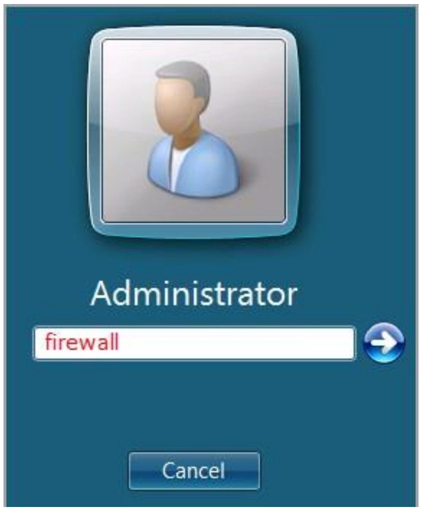
In previous labs, we configured Virtual Private Networks so external clients could access the company's internal resources. In this lab, we will configure a VPN between the Main Office and a Branch location. This will allow users on a different physical network (at a branch location) to access resources on the internal network of the main office.

2.1 Setting up a VPN between the Main and Branch Offices

1. Click the **Windows 2008 Firewall** icon on the topology. Click **PC**, then **Send Ctrl+Alt+Del** in the top left corner of the screen in order to log on to the Windows 2008 Firewall server.

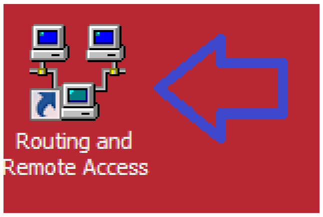

Viewer
View
PC
Settings
Help
Send CTRL+ALT+DEL
Send F11
Send a CTRL+ALT+DEL key sequence to the remote machine
Press CTRL + ALT + DELETE to log on

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

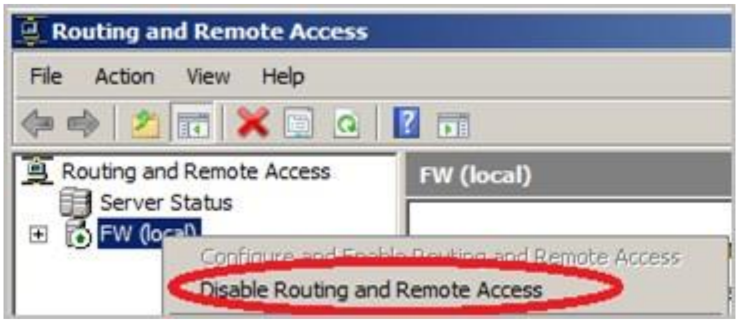


firewall

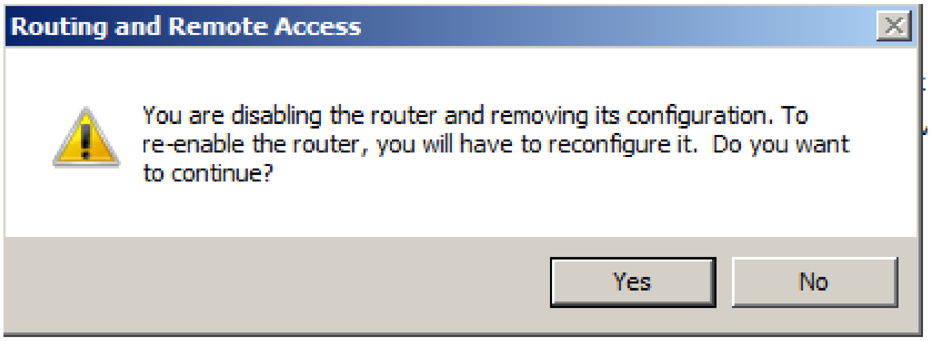
3. Double-click the shortcut to **Routing and Remote Access** on the desktop.



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

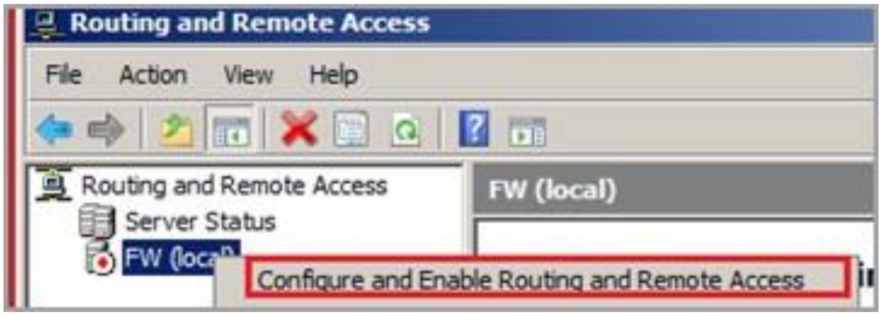

Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
FW (local)
FW (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access

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

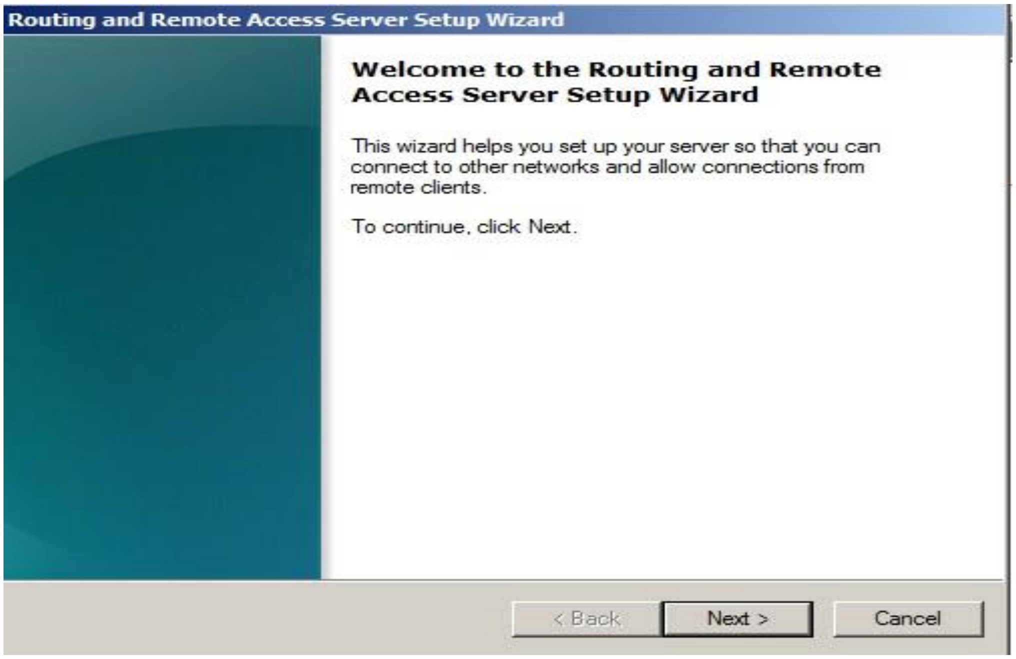

Routing and Remote Access

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?

6. Right-click on FW (local) and select **Configure and Enable 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

7. Click **Next** to the Welcome to the Routing and Remote Access Setup Wizard.



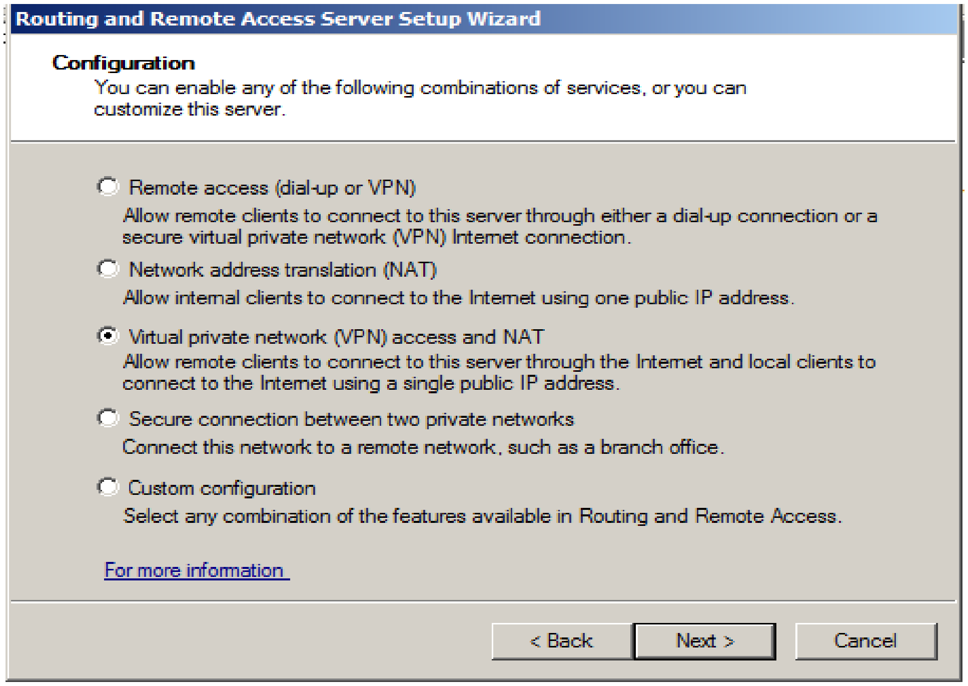
Routing and Remote Access Server Setup Wizard

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.

8. 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.

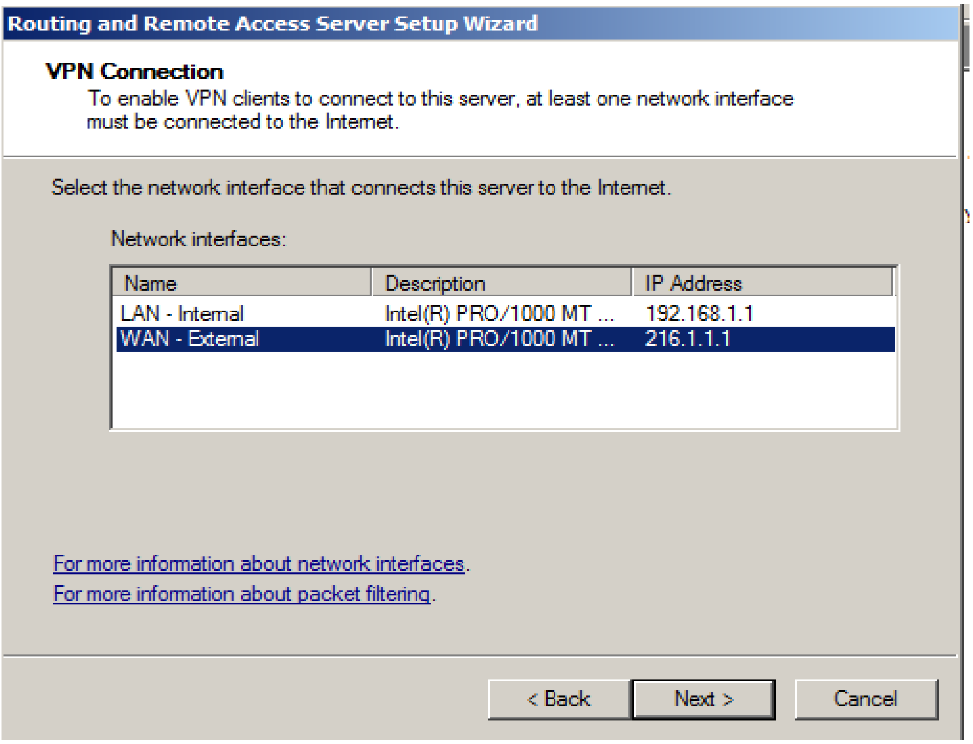
○ Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

● 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.

9. 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.

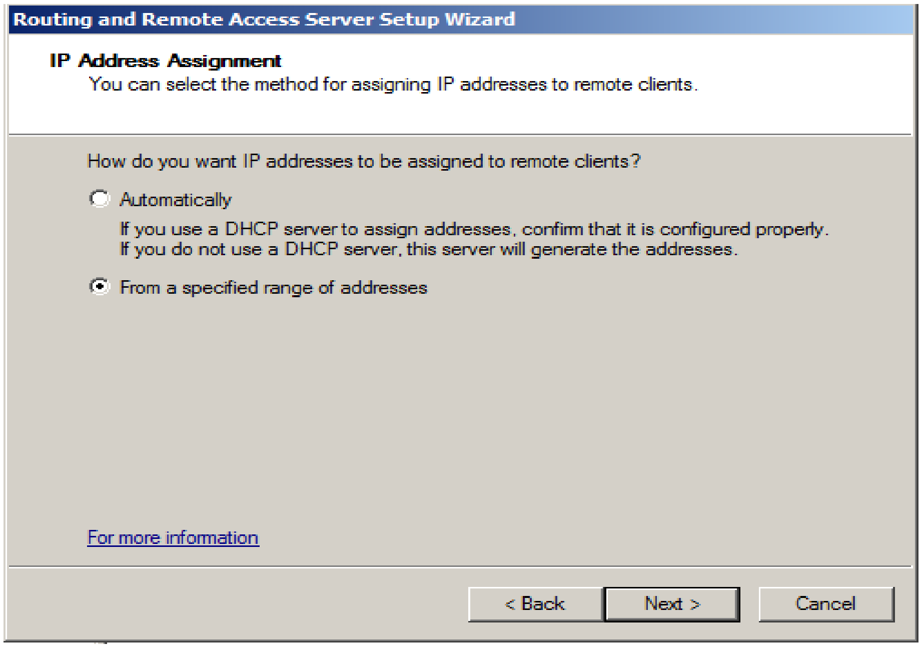
Select the network interface that connects this server to the Internet.

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

10. 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.

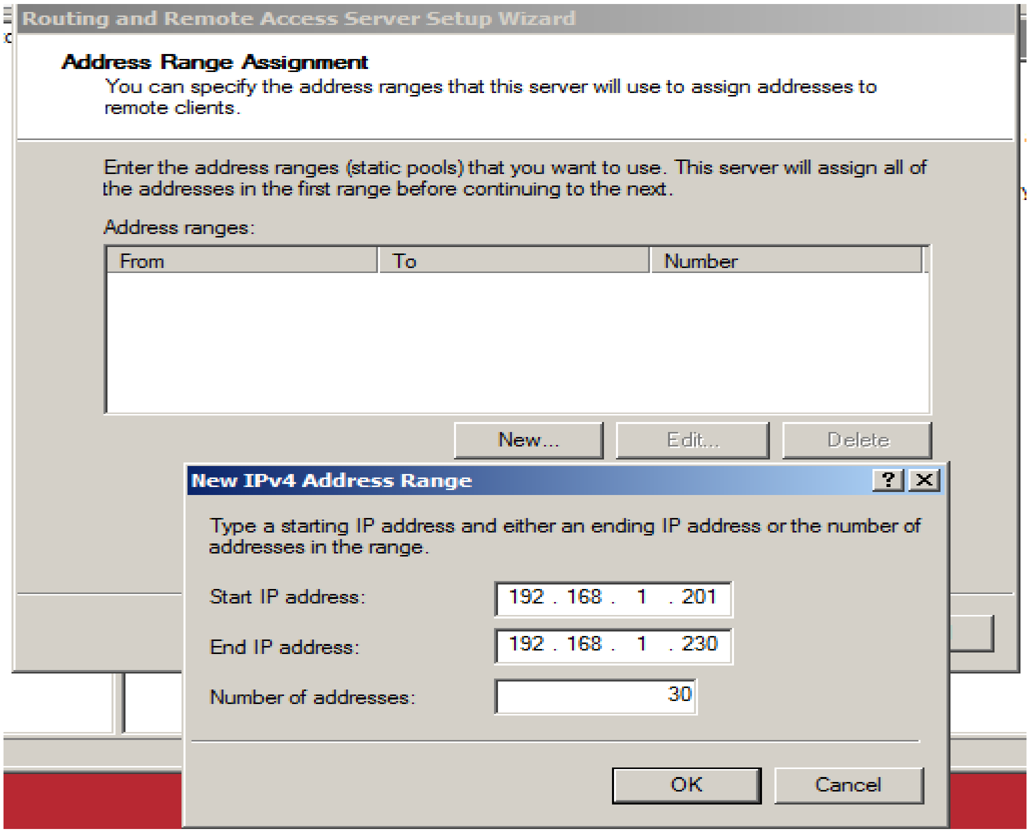
How do you want IP addresses to be assigned to remote clients?

○ 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

11. Click New. Enter the Start IP address: **192.168.1.201** and the 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

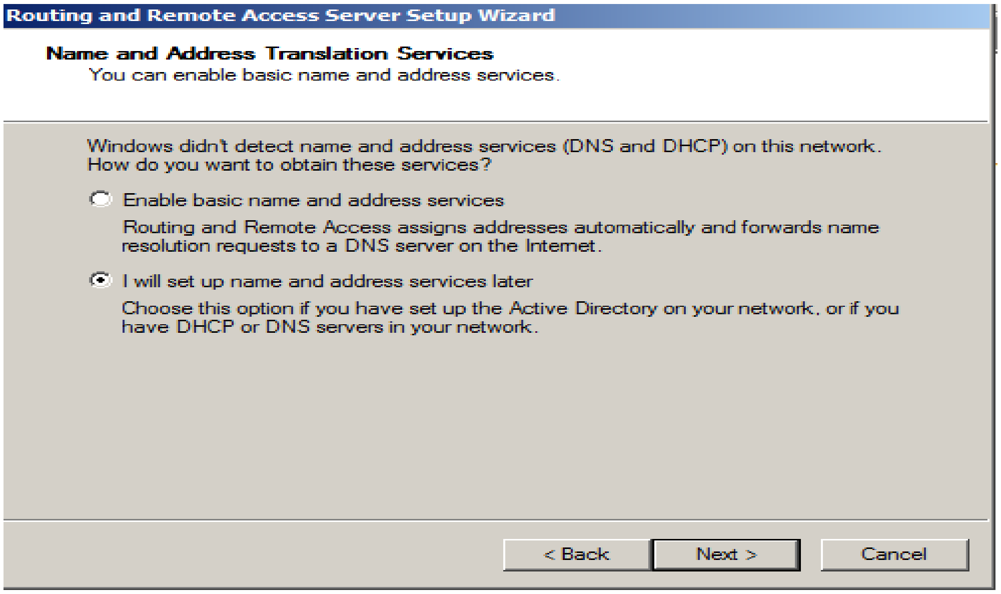
Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 192 . 168 . 1 . 201

End IP address: 192 . 168 . 1 . 230

Number of addresses: 30

12. 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?

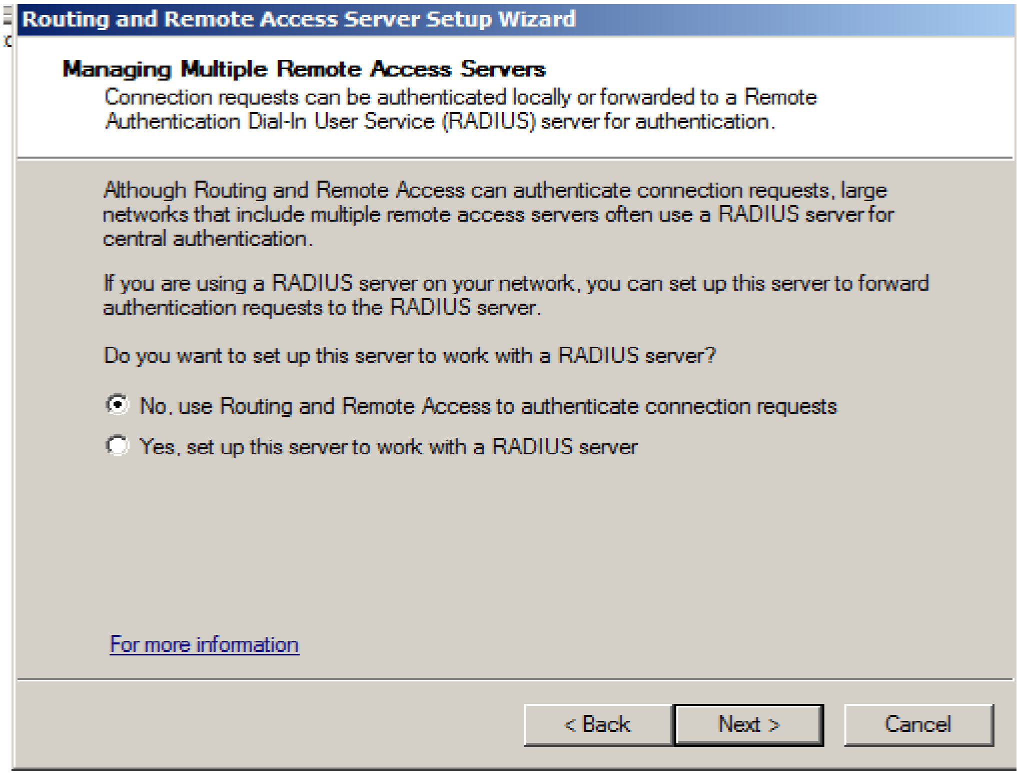
○ Enable basic name and address services

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.

13. Select **No, use Routing and Remote Access to authenticate connection requests** 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.

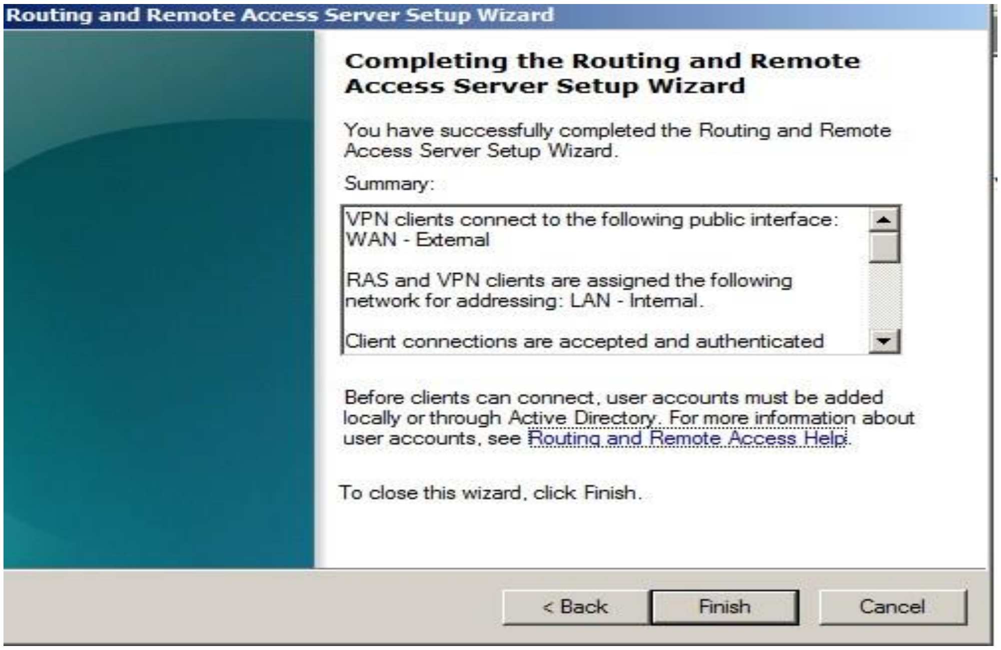
If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

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

14. 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

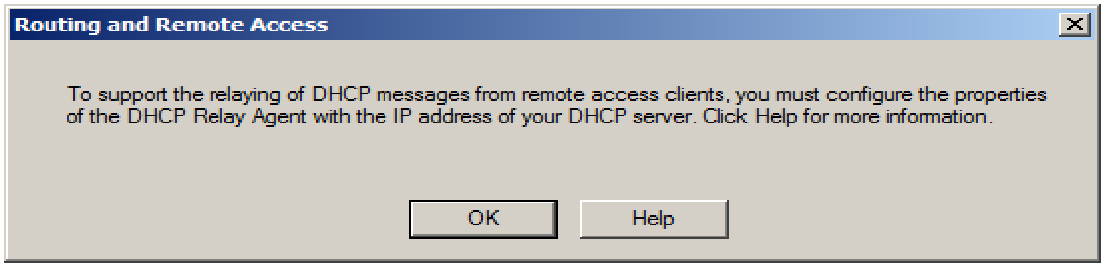
RAS and VPN clients are assigned the following network for addressing: LAN - Internal.

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.

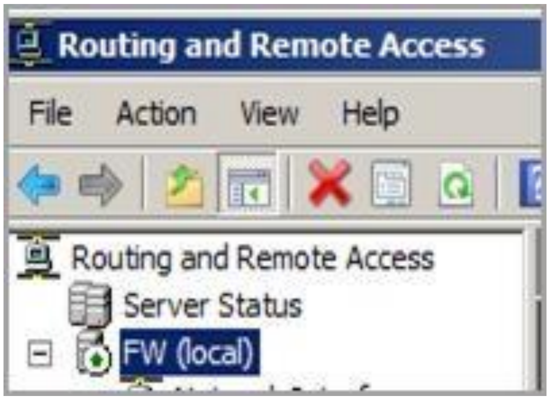
To close this wizard, click Finish.

15. Click **OK** to the warning message about the DHCP relay agent.

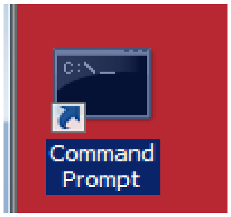


To support the relaying of DHCP messages from remote access clients, you must configure the properties of the DHCP Relay Agent with the IP address of your DHCP server. Click Help for more information.

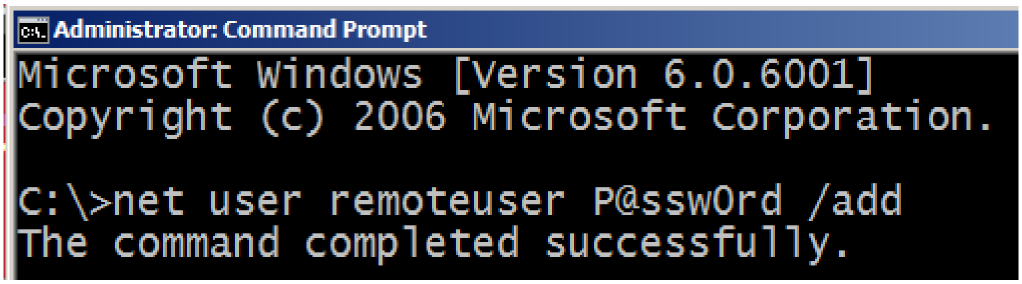
16. The Routing and Remote Access FW (local) machine will now turn green again.



17. On the desktop, double-click the Command Prompt shortcut.



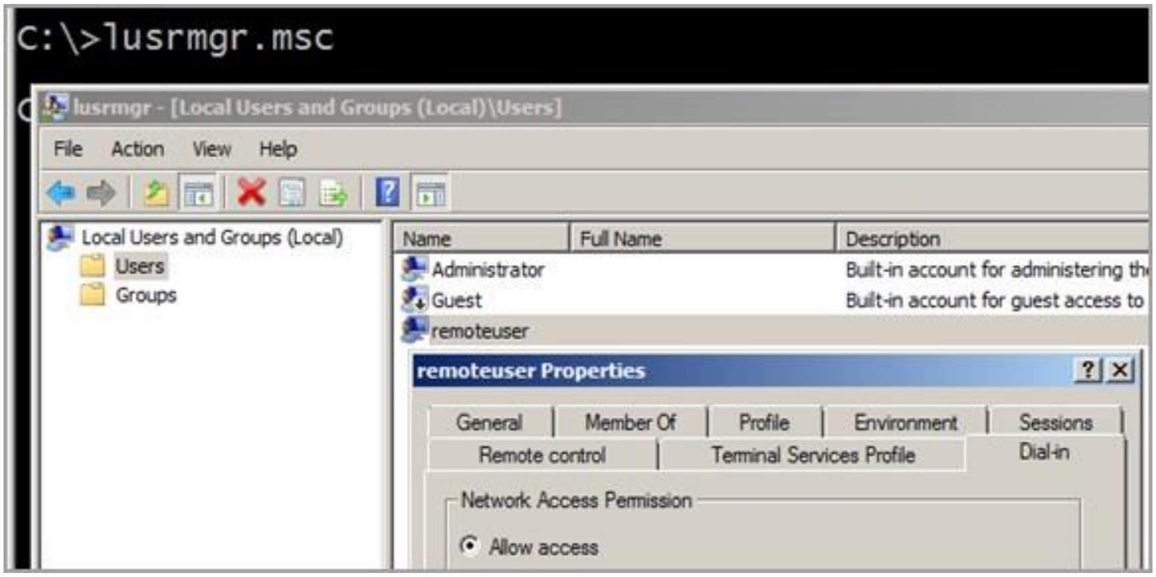
18. On the Windows 2008 Firewall, type the following to add a remote user account: C:\>**net user remoteuser P@ssw0rd /add**



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

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

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

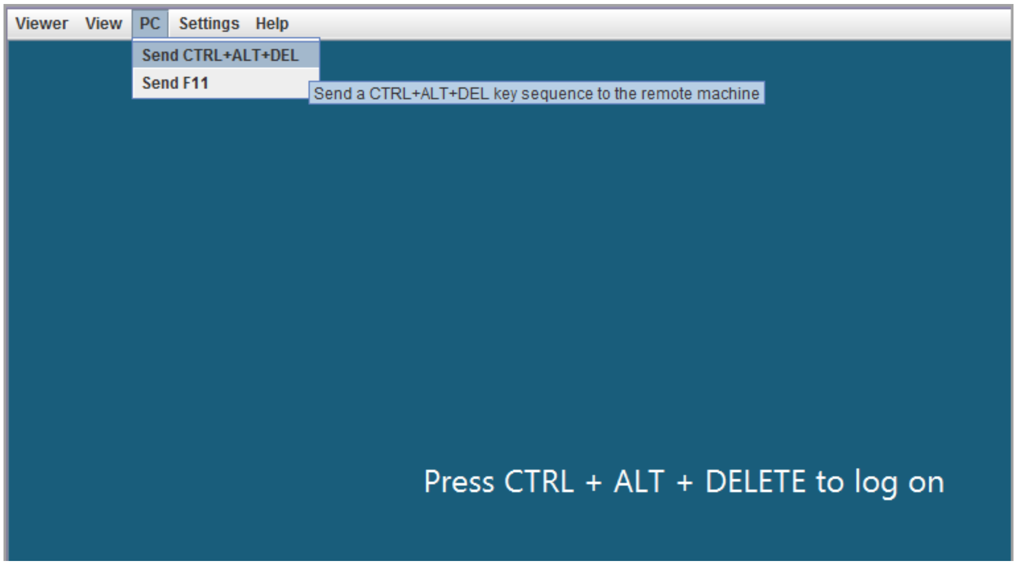
20. Double-click the **Users** folder. Double-click on **remoteuser**. Click the **Dial-in** tab. Click the button marked **Allow access**. Click **Apply** and then **OK**. Close the Local User Manager.



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

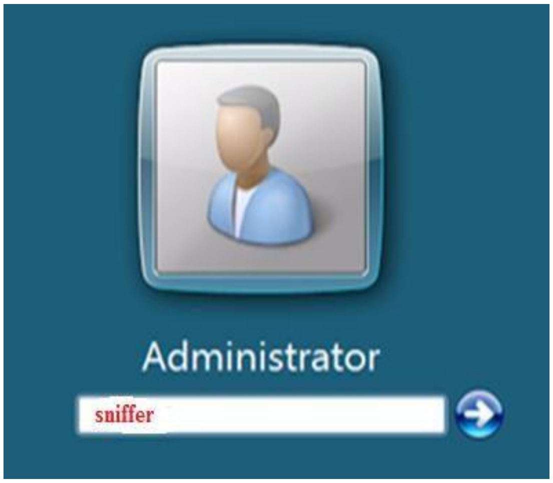
lusrmgr - [Local Users and Groups (Local)\Users]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
Name
Full Name
Description
Administrator
Built-in account for administering th
Guest
Built-in account for guest access to
remoteuser
remoteuser Properties
General
Member Of
Profile
Environment
Sessions
Remote control
Terminal Services Profile
Dial-in
Network Access Permission
● Allow access

21. Click on the **Windows 2008 Sniffer** icon on 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.

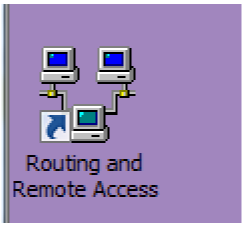


Press CTRL + ALT + DELETE to log on

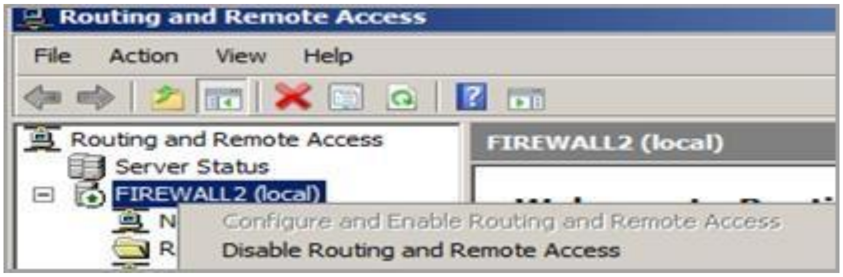
22. Enter **sniffer** for the Administrator password to the Windows 2008 Server.



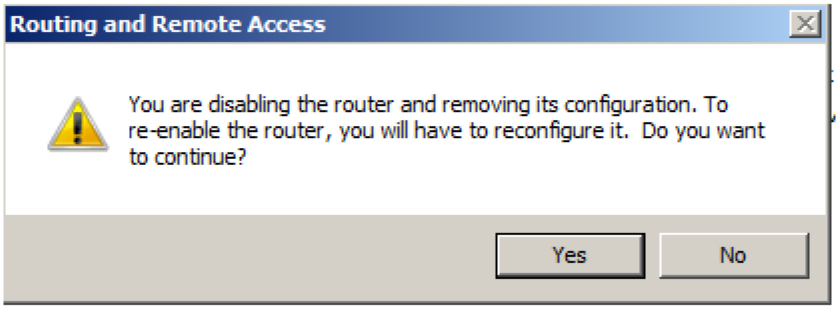
23. On the Sniffer, double-click the shortcut to **Routing and Remote Access** on the desktop.



24. Right-click on **FIREWALL2** and select **Disable Routing and Remote Access**.

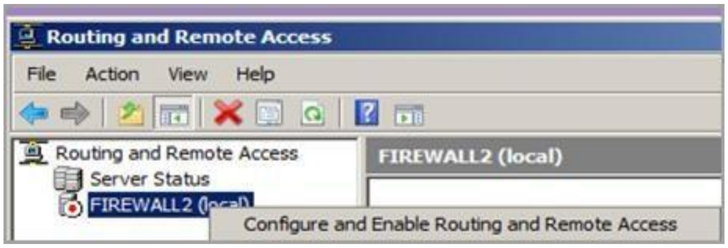

Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
FIREWALL2 (local)
N
R
FIREWALL2 (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access

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

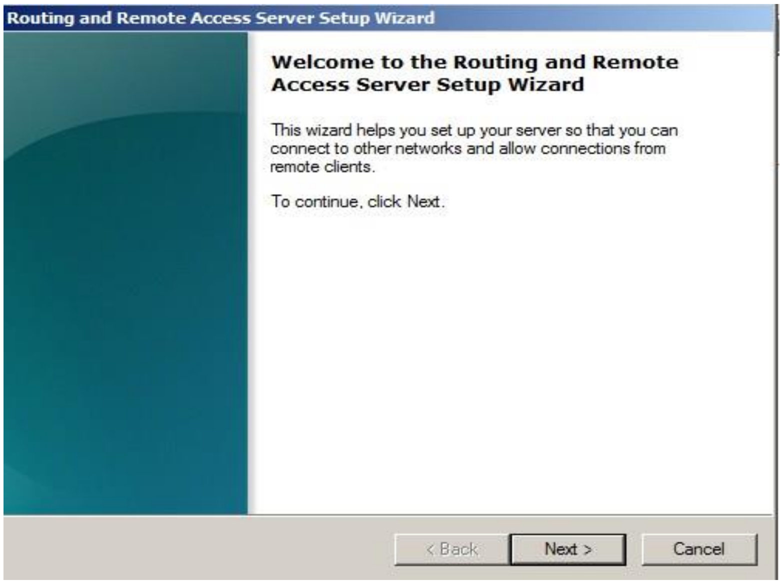

Routing and Remote Access

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?

26. Right-click on FIREWALL2 and select **Configure and Enable Routing and Remote Access.**


Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
FIREWALL2 (local)
FIREWALL2 (local)
Configure and Enable Routing and Remote Access

27. Click **Next** to the Welcome to the Routing and Remote Access Setup Wizard.

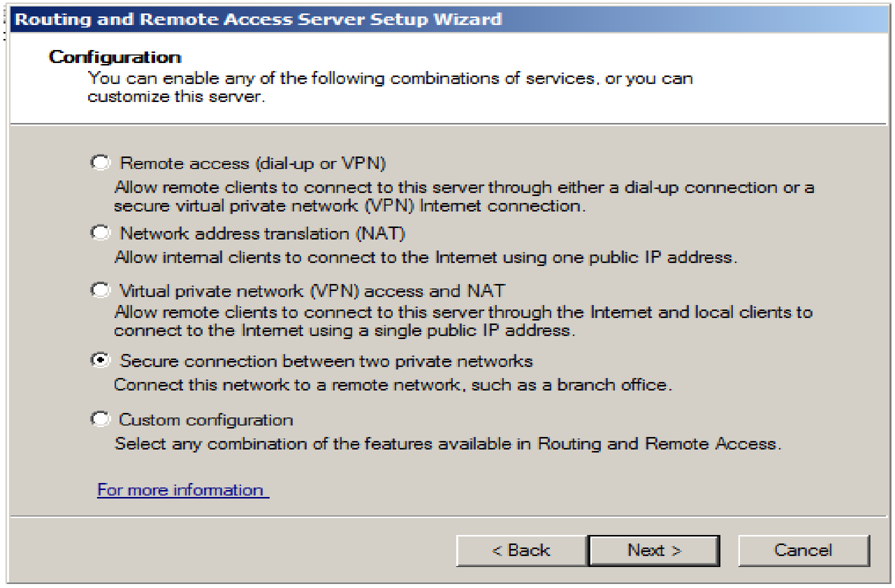


Welcome to the Routing and Remote Access Server Setup Wizard

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.

28. Choose **Secure Connection between two private networks**. Click **Next**.



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.

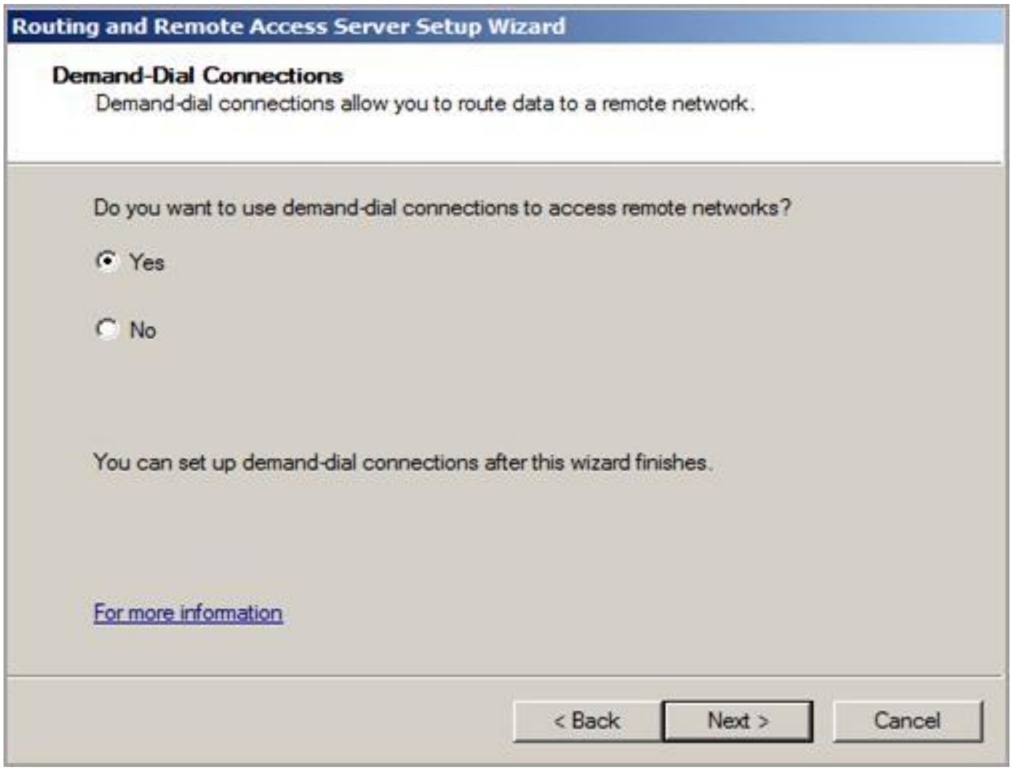
○ Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

○ 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.

29. Leave the Demand Dial Connections selection as **Yes** and click **Next**.



Routing and Remote Access Server Setup Wizard

Demand-Dial Connections

Demand-dial connections allow you to route data to a remote network.

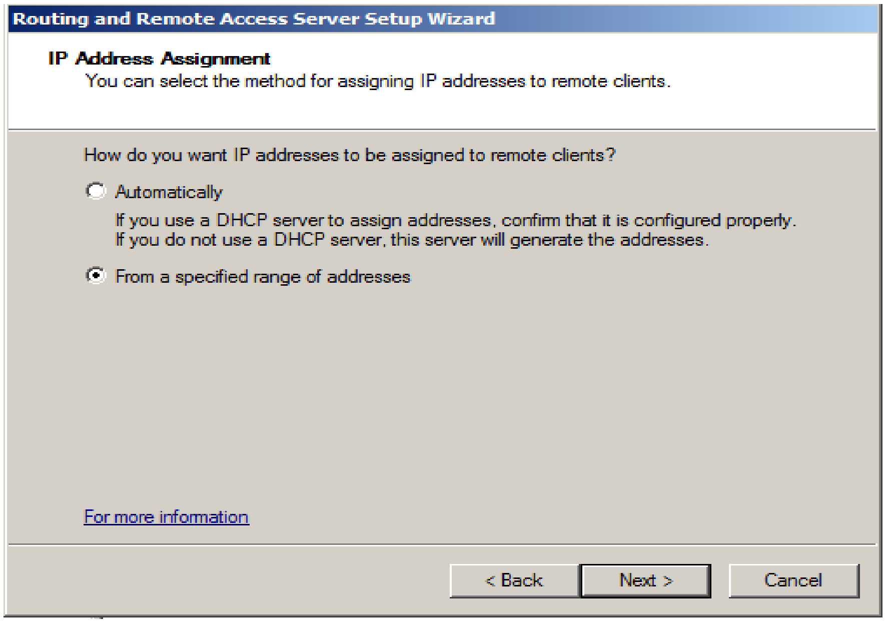
Do you want to use demand-dial connections to access remote networks?

● Yes

○ No

You can set up demand-dial connections after this wizard finishes.

30. 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.

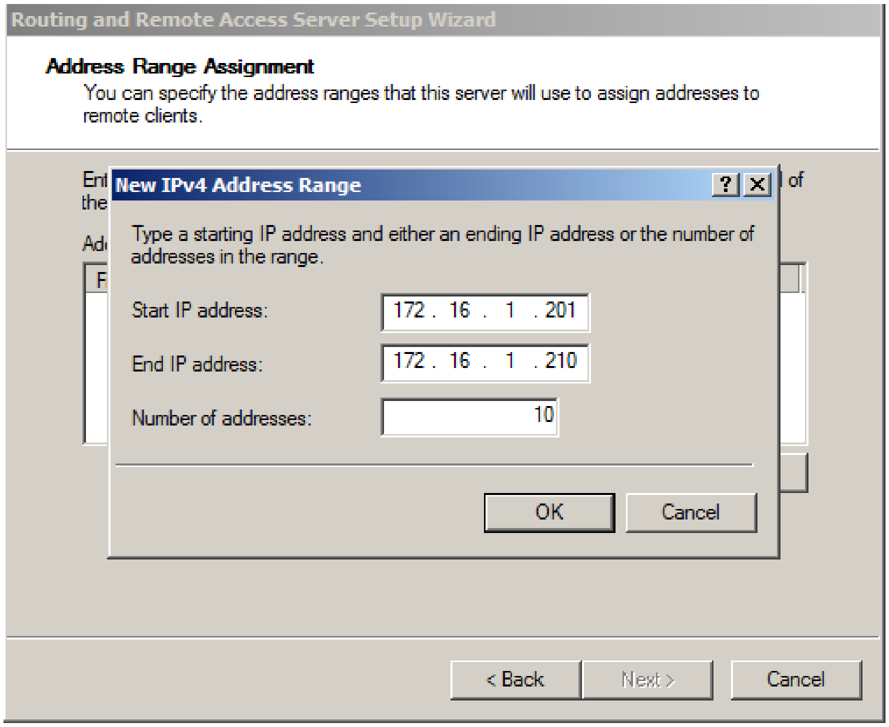
How do you want IP addresses to be assigned to remote clients?

○ 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

31. Click New. Type the Start IP address: **172.16.1.201** and the End IP address: **172.16.1.210.** 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.

New IPv4 Address Range

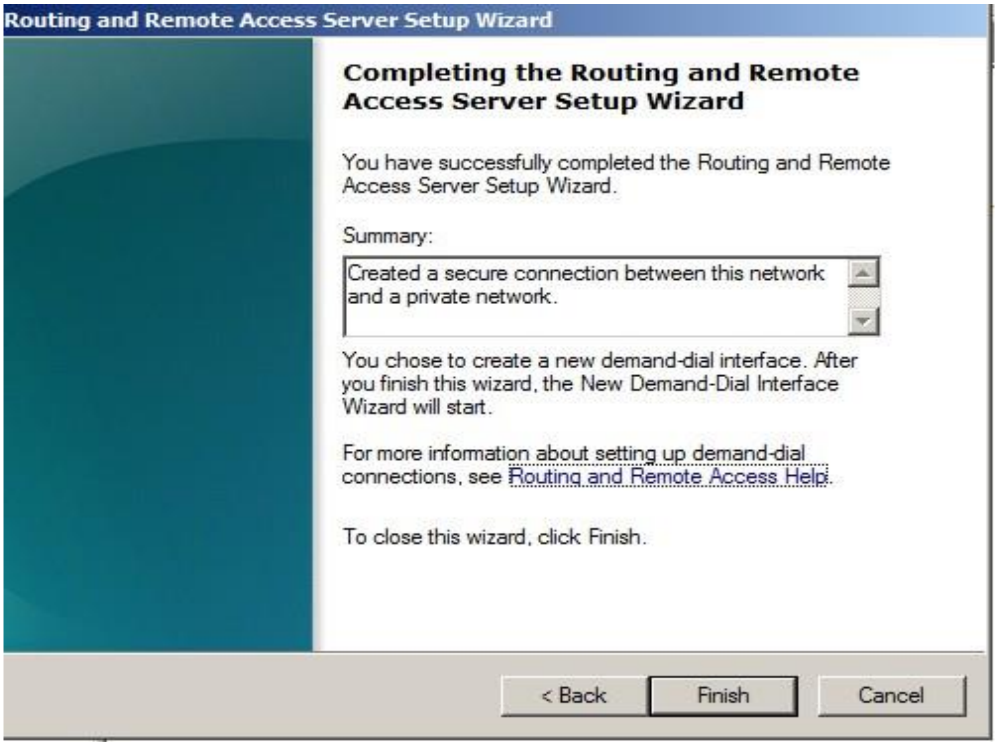
Type a starting IP address and either an ending IP address or the number of addresses in the range.

Start IP address: 172 . 16 . 1 . 201

End IP address: 172 . 16 . 1 . 210

Number of addresses: 10

32. Click **Finish** on the Access Server Setup Wizard.



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:

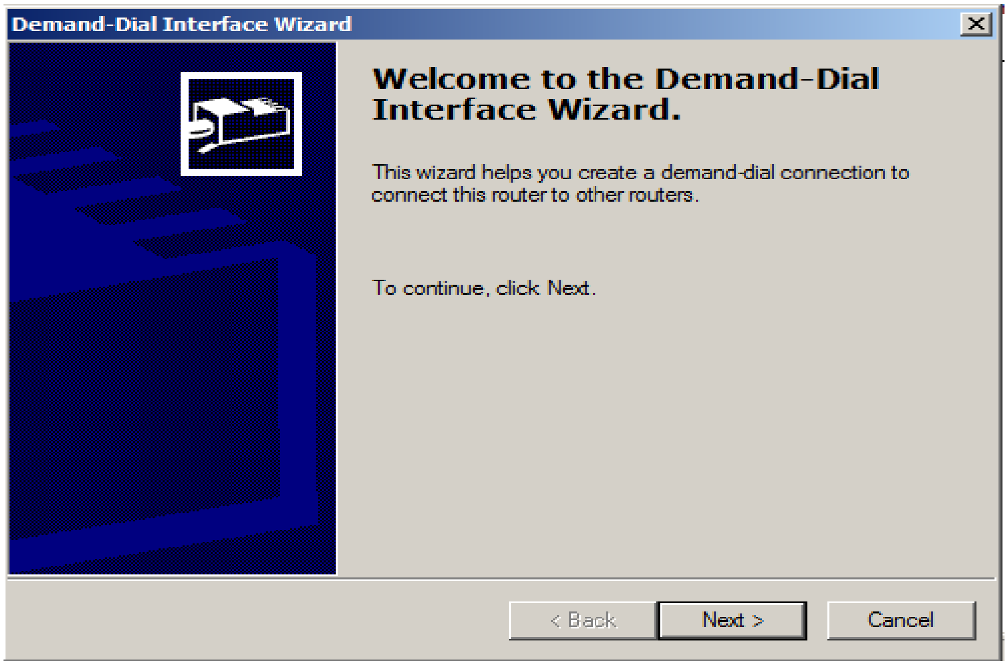
Created a secure connection between this network and a private network.

You chose to create a new demand-dial interface. After you finish this wizard, the New Demand-Dial Interface Wizard will start.

For more information about setting up demand-dial connections, see Routing and Remote Access Help.

To close this wizard, click Finish.

33. Click **Next** at the **Welcome to the Demand Dial Interface Wizard** screen.



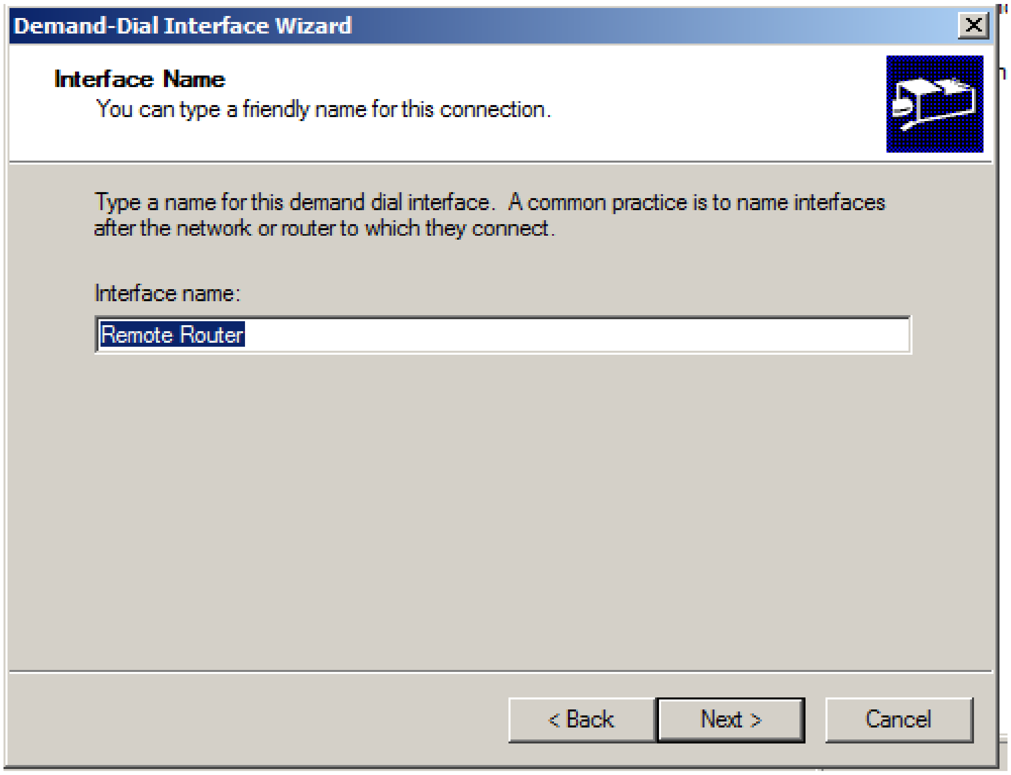
Demand-Dial Interface Wizard

Welcome to the Demand-Dial Interface Wizard.

This wizard helps you create a demand-dial connection to connect this router to other routers.

To continue, click Next.

34. Click **Next** at the **Interface Name** Screen.



Demand-Dial Interface Wizard

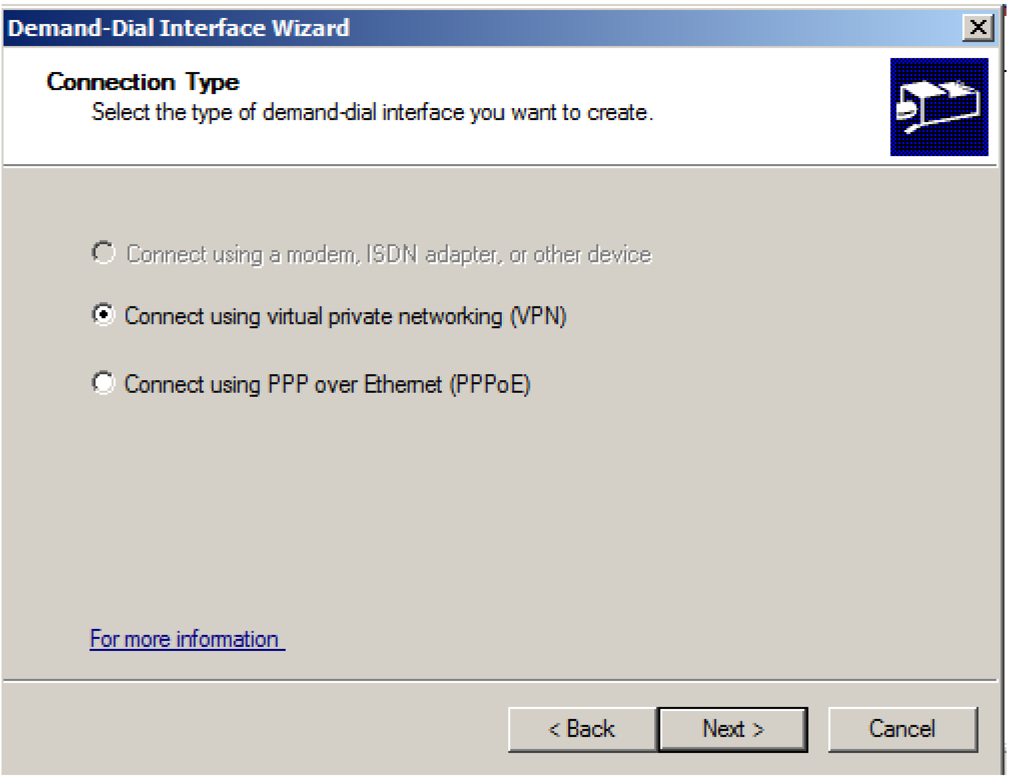
Interface Name

You can type a friendly name for this connection.

Type a name for this demand dial interface. A common practice is to name interfaces after the network or router to which they connect.

Interface name: Remote Router

35. Select **Connect using virtual private networking (VPN)** and click **Next**.



Demand-Dial Interface Wizard

Connection Type

Select the type of demand-dial interface you want to create.

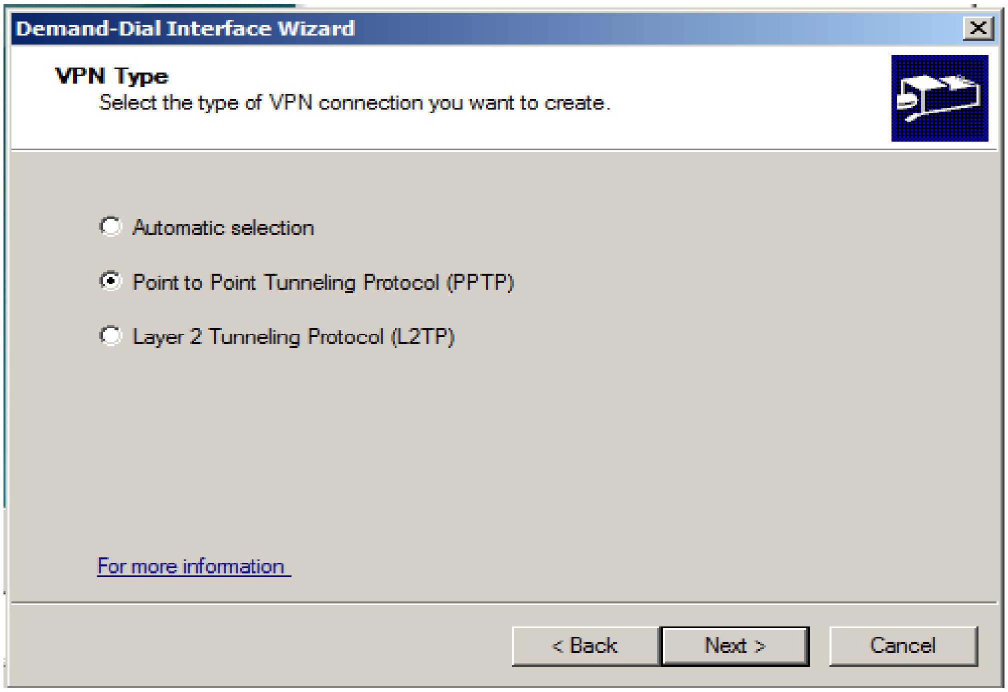
○ Connect using a modem, ISDN adapter, or other device

● Connect using virtual private networking (VPN)

○ Connect using PPP over Ethernet (PPPoE)

For more information

36. Select **Point to Point Tunneling Protocol** (**PPTP)** and click **Next**.



Demand-Dial Interface Wizard

VPN Type

Select the type of VPN connection you want to create.

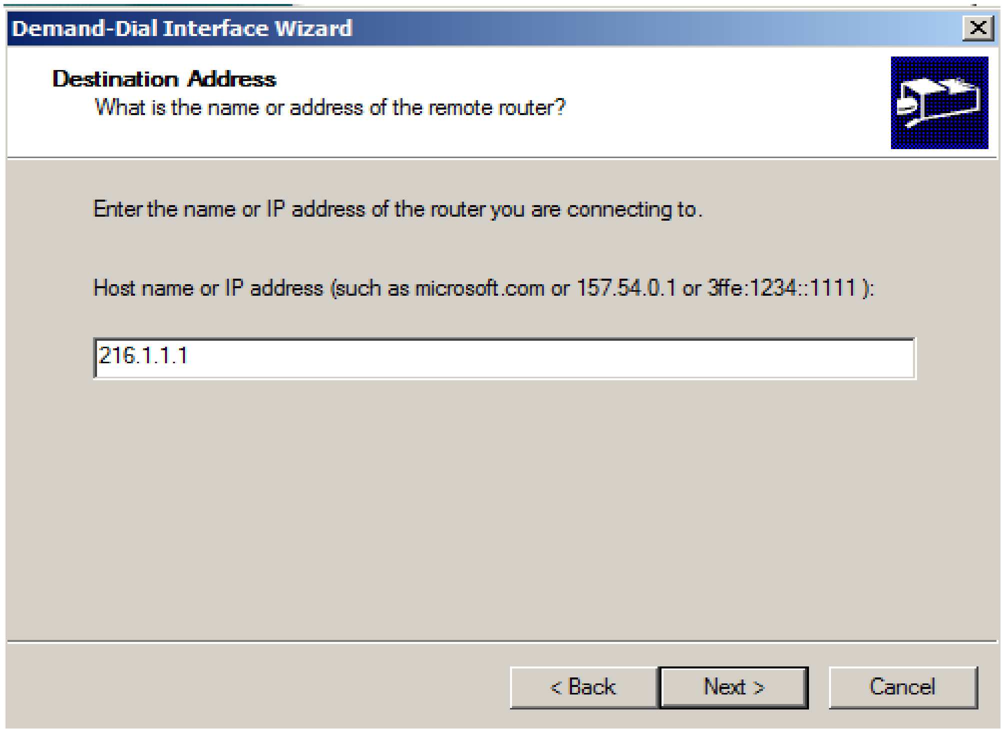
○ Automatic selection

● Point to Point Tunneling Protocol (PPTP)

○ Layer 2 Tunneling Protocol (L2TP)

For more information

37. In the **Destination Address**, type **216.1.1.1,** and click Next.



Demand-Dial Interface Wizard

Destination Address

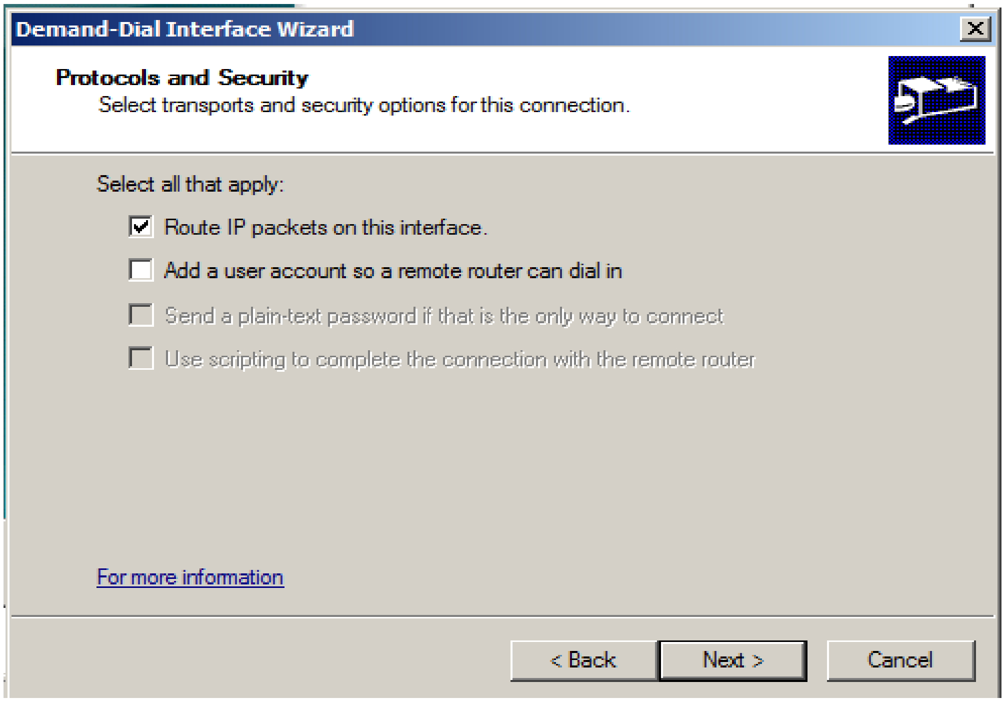
What is the name or address of the remote router?

Enter the name or IP address of the router you are connecting to.

Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

216.1.1.1

38. Click **Next** to **Route IP Packets on this Interface**.



Demand-Dial Interface Wizard

Protocols and Security

Select transports and security options for this connection.

Select all that apply:

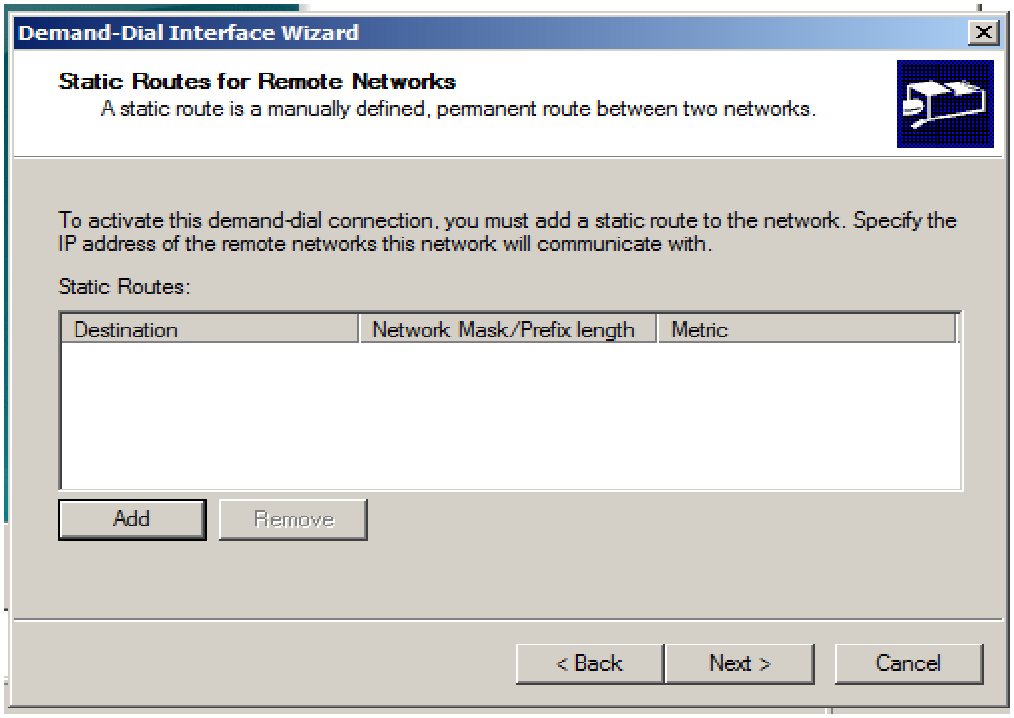
☑ Route IP packets on this interface.

□ Add a user account so a remote router can dial in

□ Send a plain-text password if that is the only way to connect

□ Use scripting to complete the connection with the remote router

39. Click **Next** at the **Static route for Remote Networks** screen. We will add the static route later.



Demand-Dial Interface Wizard

Static Routes for Remote Networks

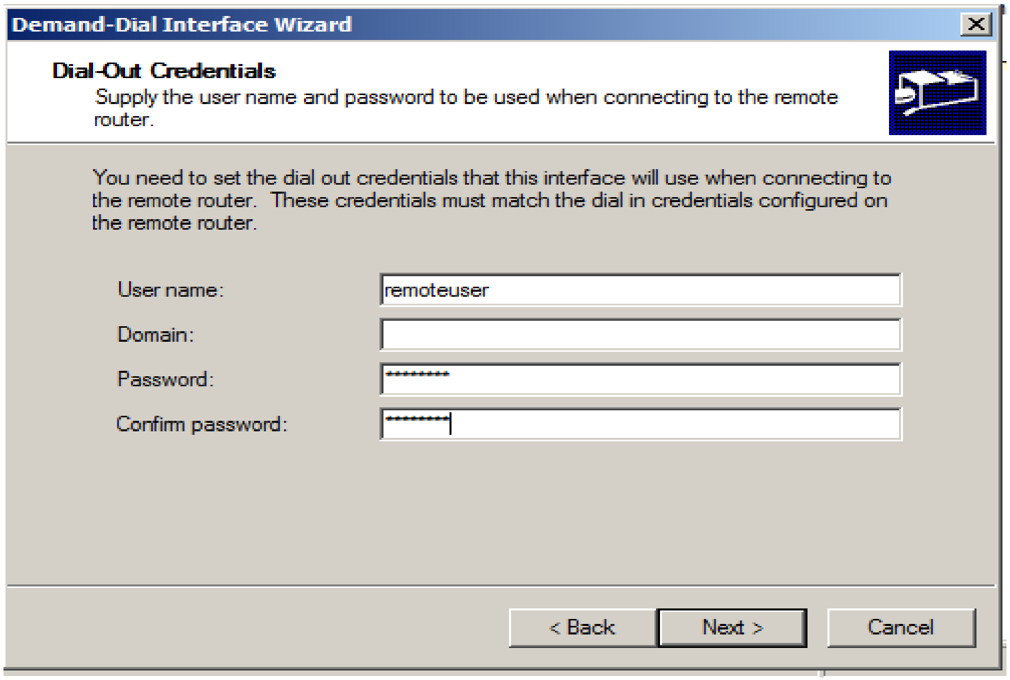
A static route is a manually defined, permanent route between two networks.

To activate this demand-dial connection, you must add a static route to the network. Specify the IP address of the remote networks this network will communicate with.

Static Routes:

Destination	Network Mask/Prefix length	Metric

40. For the username, type **remoteuser**. Leave the domain field blank. For the password and the confirmation password, type **P@ssw0rd** and click **Next**.



Demand-Dial Interface Wizard

Dial-Out Credentials

Supply the user name and password to be used when connecting to the remote router.

You need to set the dial out credentials that this interface will use when connecting to the remote router. These credentials must match the dial in credentials configured on the remote router.

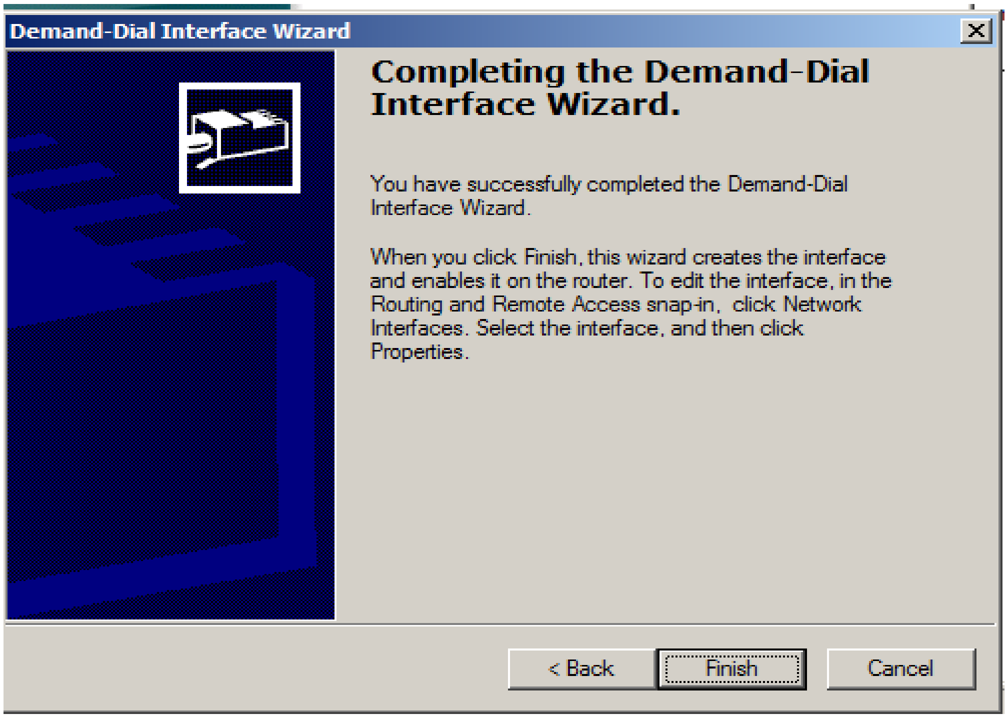
User name: remoteuser

Domain:

Password: *********

Confirm password: *********

41. Click **Finish** to complete the **Demand Dial Interface Wizard**.

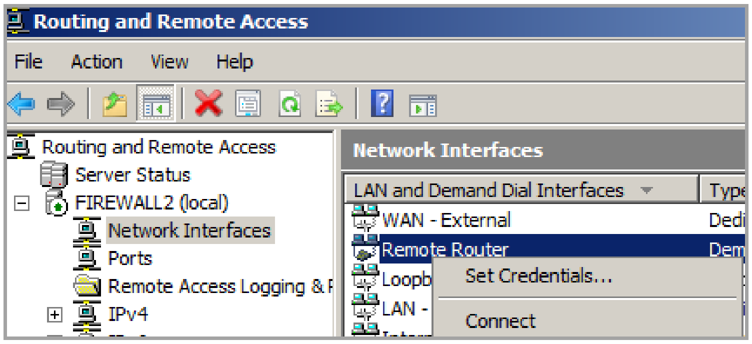


Completing the Demand-Dial Interface Wizard.

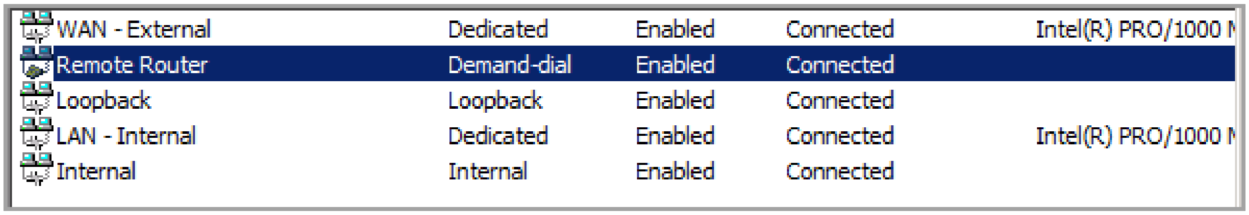
You have successfully completed the Demand-Dial Interface Wizard.

When you click Finish, this wizard creates the interface and enables it on the router. To edit the interface, in the Routing and Remote Access snap-in, click Network Interfaces. Select the interface, and then click Properties.

42. Expand **FIREWALL2 (local)**, click on **Network Interfaces**, Right-click on **Remote Router** and click **Connect**.

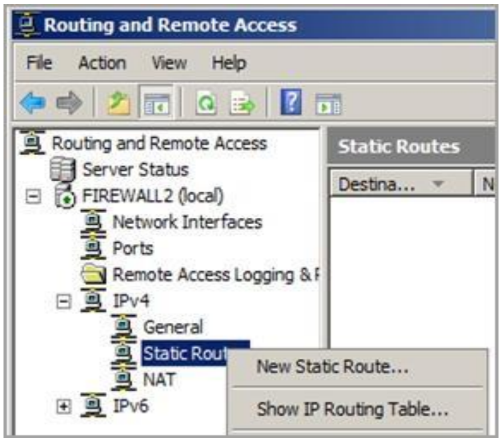


43. After a few seconds, the status of the router should change to Connected.

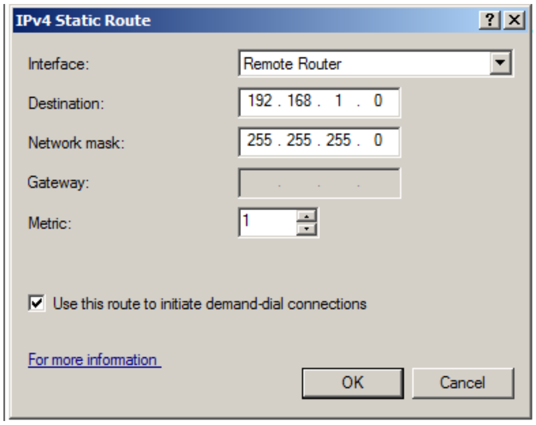


WAN - External	Dedicated	Enabled	Connected	Intel(R) PRO/1000 M
Remote Router	Demand-dial	Enabled	Connected	
Loopback	Loopback	Enabled	Connected	
LAN - Internal	Dedicated	Enabled	Connected	Intel(R) PRO/1000 M
Internal	Internal	Enabled	Connected	

44. Expand IPv4, right-click **Static Routes** and select **New Static Route**.



45. For Interface, select **Remote Router**, for the Destination type **192.168.1.0** and for the Network Mask, type **255.255.255.0**. Type **1** for the metric. Click OK.


IPv4 Static Route

Interface: Remote Router

Destination: 192 . 168 . 1 . 0

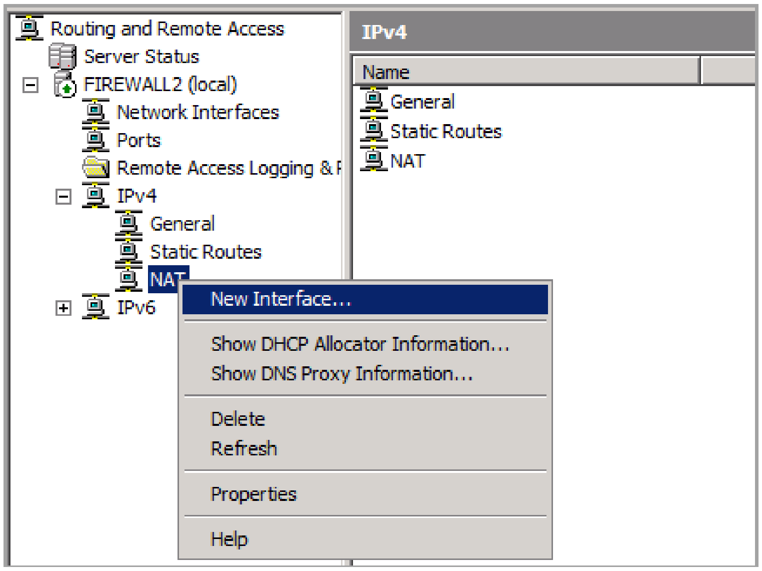
Network mask: 255 . 255 . 255 . 0

Gateway:

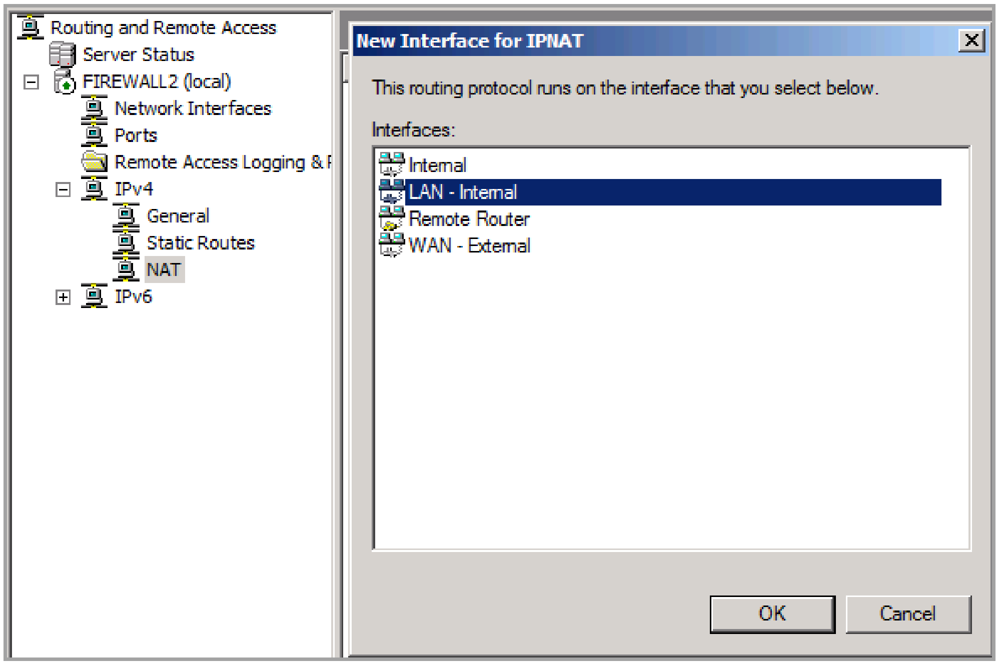
Metric: 1

☑ Use this route to initiate demand-dial connections

46. Under IPv4, right-click on **NAT** and select **New Interface**.



47. Select **LAN – Internal** and click **OK**.



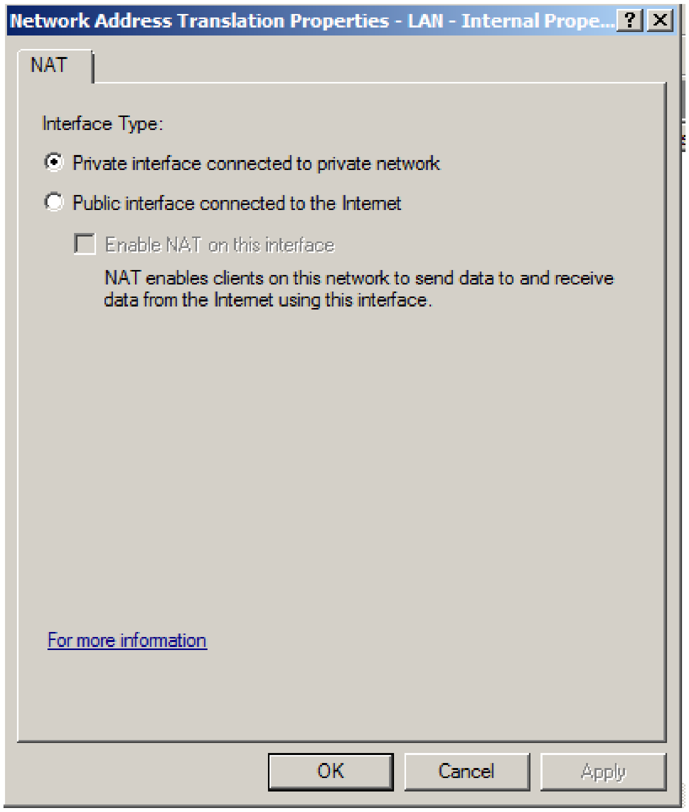
New Interface for IPNAT

This routing protocol runs on the interface that you select below.

Interfaces:

- Internal
- LAN - Internal
- Remote Router
- WAN - External

48. Click **Private interface connected to the private network** and click **OK**.



Network Address Translation Properties - LAN - Internal Prope...

Interface Type:

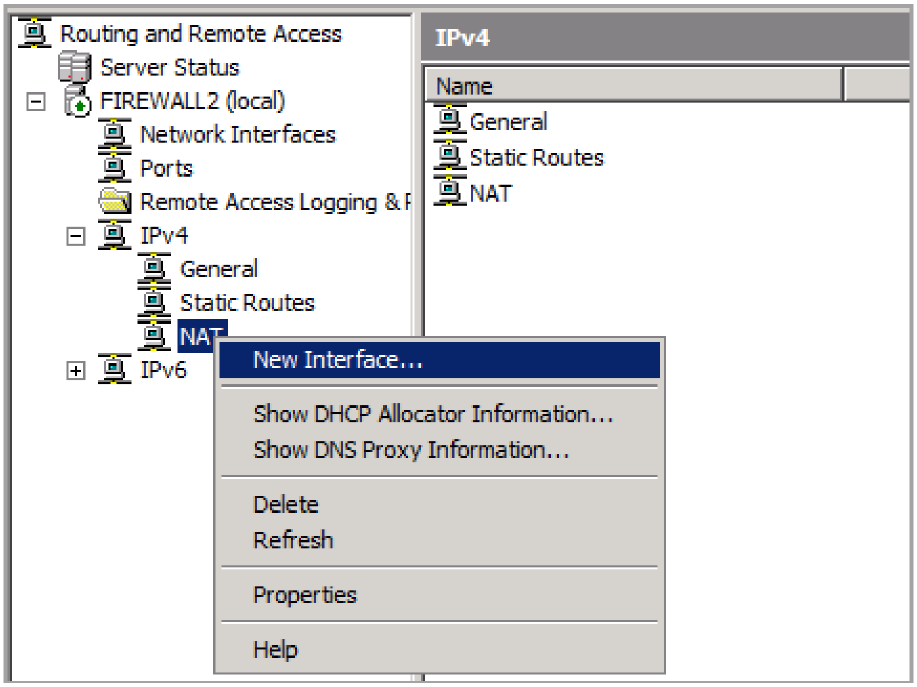
● Private interface connected to private network

○ Public interface connected to the Internet

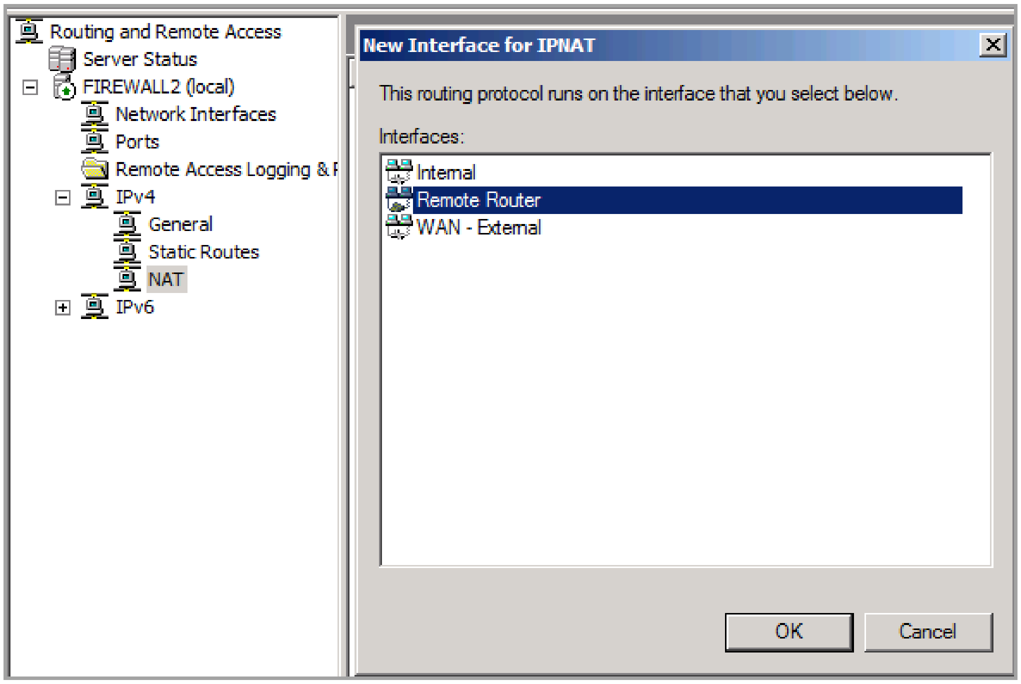
□ Enable NAT on this interface

NAT enables clients on this network to send data to and receive data from the Internet using this interface.

49. Under IPv4, right-click on **NAT** and select **New Interface.**



50. Select **Remote Router** and click **OK**.

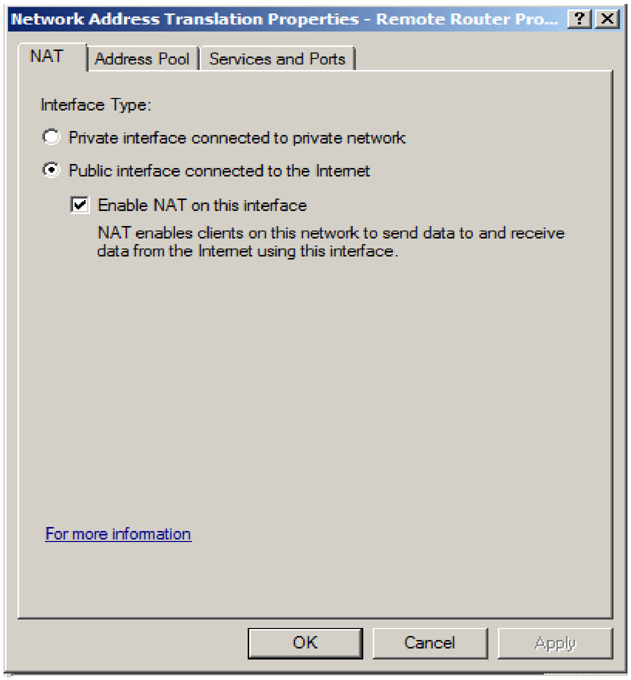


This routing protocol runs on the interface that you select below.

Interfaces:

- Internal
- Remote Router
- WAN - External

51. Click **Public interface connected to the Internet**. Leave the box checked that states **Enable NAT on this interface** and click **OK**.



Interface Type:

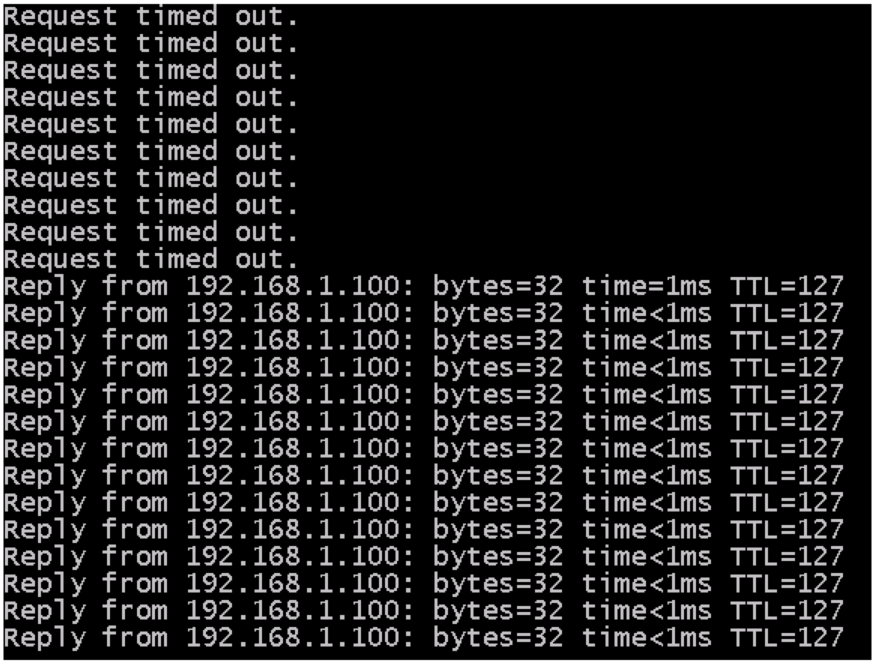
○ Private interface connected to private network

● Public interface connected to the Internet

☑ Enable NAT on this interface

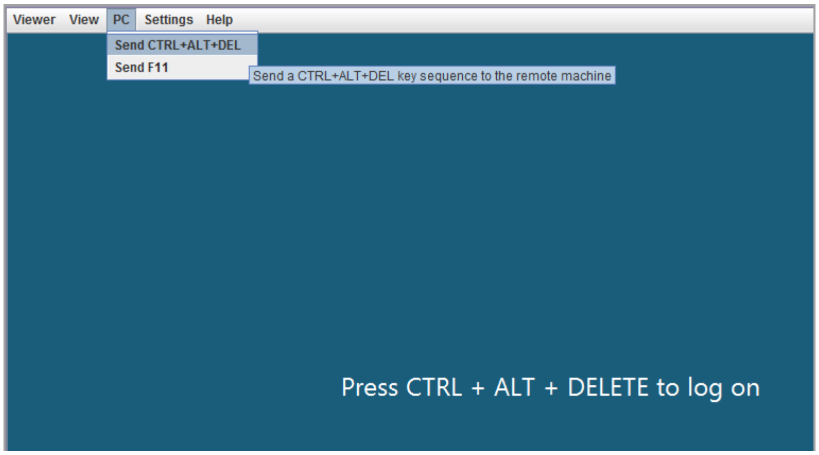
NAT enables clients on this network to send data to and receive data from the Internet using this interface.

52. Return to the **Windows 8 Internal Machine**. After a few minutes, the pings should respond. After you receive replies, press **Ctrl+ C** to stop the continuous ping.



```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.100: bytes=32 time=1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
Reply from 192.168.1.100: bytes=32 time<1ms TTL=127
```

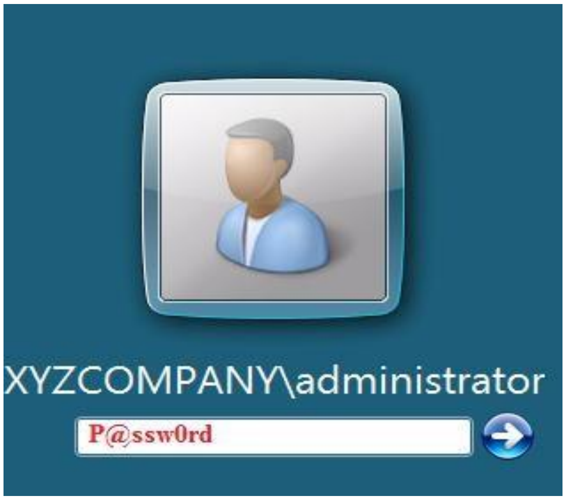
53. Click on the **Internal Windows 2008 Server** icon in the topology. Click **PC**, and then **Send Ctrl+Alt+Del** in the top-left corner of the screen in order to log on to the Windows 2008 server.



Send a CTRL+ALT+DEL key sequence to the remote machine

Press CTRL + ALT + DELETE to log on

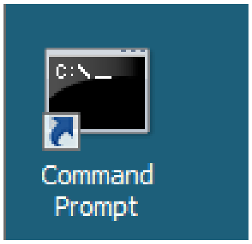
54. Enter **P@ssw0rd** for the Administrator password on the Windows 2008 Server Internal Machine.



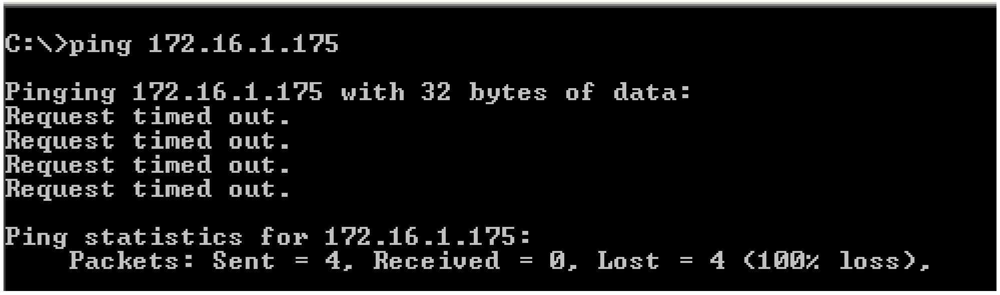
XYZCOMPANY\administrator

P@ssw0rd

55. Double-click on the shortcut to the Command Prompt on the desktop.



56. Type the following command:
C:\>**ping 172.16.1.175**



```
C:\>ping 172.16.1.175

Pinging 172.16.1.175 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.175:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

We have configured the VPN, so the branch users can access the resources on the main office's internal network. We are not allowing internal machines on the main office site to connect back to the workstations (Windows 8 and Ubuntu) on the branch site. That can be accomplished via static routes or by creating another VPN connection.

2.2 Conclusion

Setting up a VPN between a main office and a branch office can be beneficial because users can share resources and companies can avoid the cost of duplicate infrastructure. The encrypted connection will help prevent attackers on the Internet from examining traffic between the main and the branch offices. In some cases, depending on the configuration, static routes may need to be configured to allow clients on different internal networks to access machines on other internal subnets, if necessary.

2.3 Discussion Questions

1. What benefits does a VPN provide?
   Ans: VPN is a Virtual Private Network it has several benefits To make it more difficult for hackers to intercept on your communications, VPNs encrypt all traffic between your device and the VPN server.

2. Do you use a Public or Private IP address when connecting to a VPN server?
   Ans: Normally, you will use a private IP address that the VPN server has given you when connecting to it. Usually hidden from the public eye, this private IP address is used to create a secure connection between your device and the VPN server.

3. What does a successful ping indicate?
   Ans: A successful ping indicates that there's a network connection between the source and destination devices, and that the destination device is responding to ICMP requests. This can be useful for testing network connectivity and troubleshooting network issues.

4. What does a request time out indicate?
   Ans: request time out indicates that the destination device didn't respond to the ICMP request within a certain period.

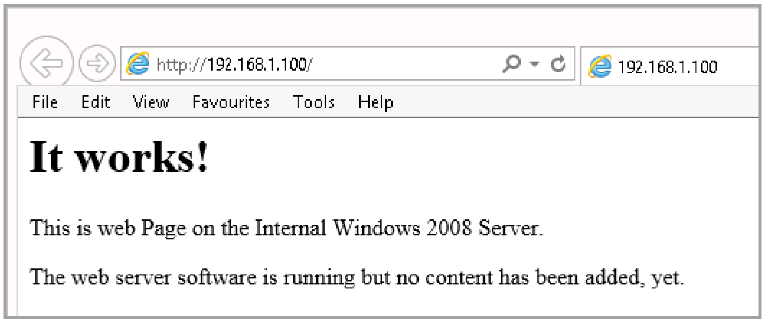
3 Using Main Office Services from the Branch Location

Now that we have successfully connected the branch office to the VPN server at the main office, branch users can access some of the company's internal resources, all over a secure connection. In this scenario, the workstations will still only have a single IP address. The VPN connection between the servers provides the connectivity.

3.1 Using Services

1. On the **Windows 8 Internal Machine**, double-click on the **Internet Explorer** shortcut on the desktop.

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

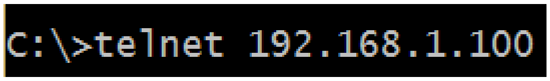


It works!

This is web Page on the Internal Windows 2008 Server.

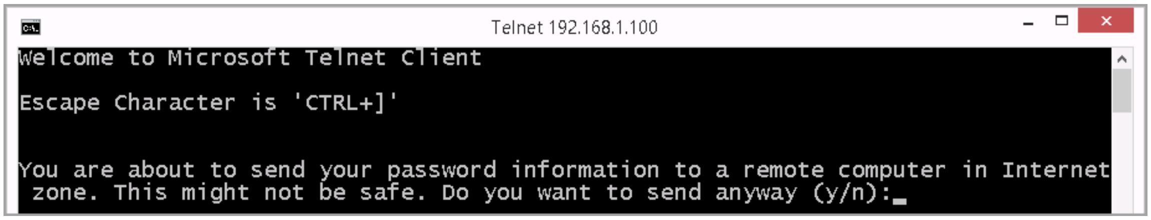
The web server software is running but no content has been added, yet.

3. Open a command prompt and type the following command to telnet to Windows 2008 Internal Machine:
C:\>**telnet 192.168.1.100**



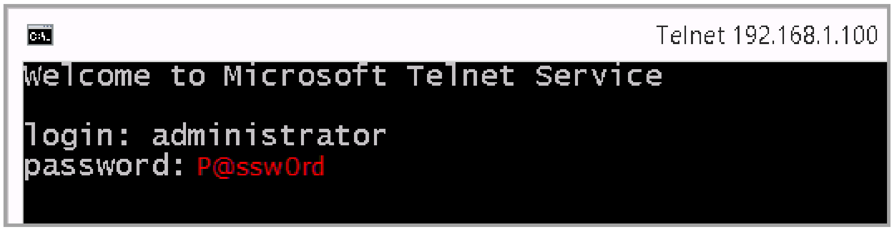
```
C:\>telnet 192.168.1.100
```

4. Type **n** to the message, "*Do you want to send anyway?*"



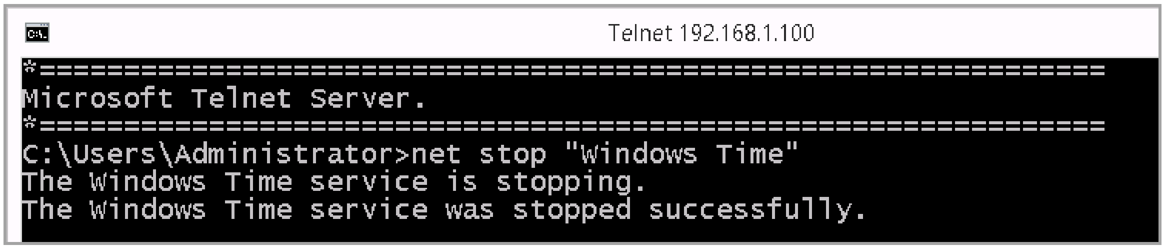
```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'


You are about to send your password information to a remote computer in Internet
 zone. This might not be safe. Do you want to send anyway (y/n):_
```

5. Type **administrator** for the username and **P@ssw0rd** for the password.



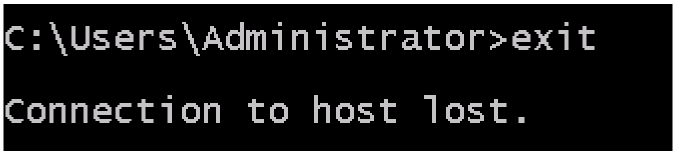
```
Welcome to Microsoft Telnet Service

login: administrator
password: P@ssw0rd
```

6. Type the following command to stop the Windows Time service:
C:\Users\Administrator>**net stop "Windows Time"**



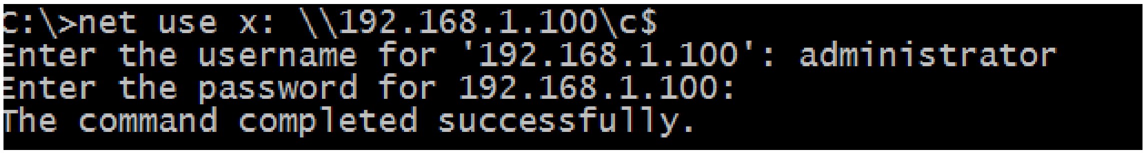
```
*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\Administrator>net stop "Windows Time"
The Windows Time service is stopping.
The Windows Time service was stopped successfully.
```

7. Type **exit** to leave the telnet session.
C:\Users\Administrator>**exit**
Close the Administrator Command prompt.



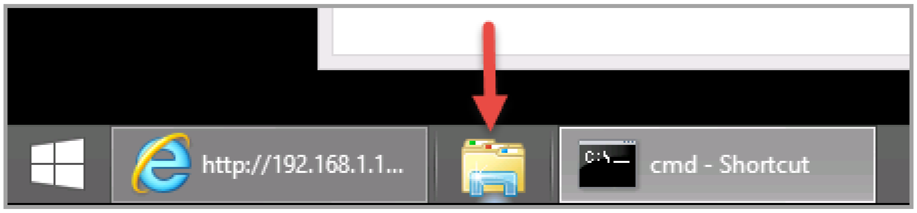
```
C:\Users\Administrator>exit

Connection to host lost.
```

8. Open another command prompt and 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**

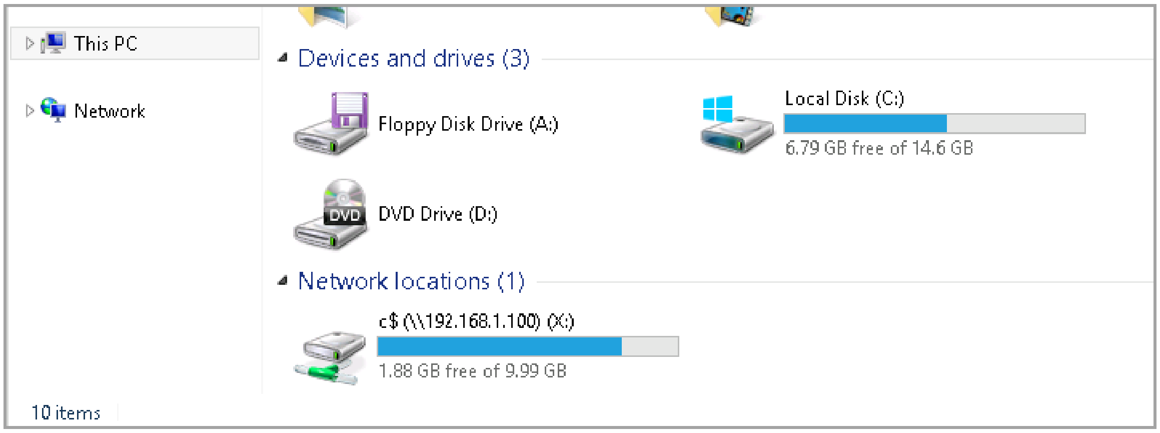


```
C:\>net use x: \\192.168.1.100\c$
Enter the username for '192.168.1.100': administrator
Enter the password for 192.168.1.100:
The command completed successfully.
```

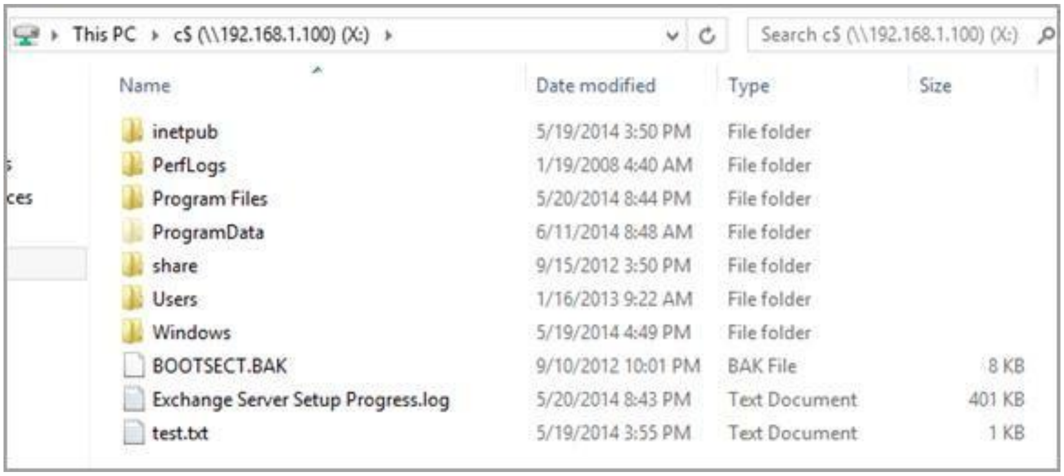
9. Click on the File Explorer Folder.



10. Scroll down and double-click the Network Locations link, **c$(\\192.168.1.100)(X:).**



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


This PC › c$ (\\192.168.1.100) (X:) ›
Search c$ (\\192.168.1.100) (X:)
ces

Name	Date modified	Type	Size
inetpub	5/19/2014 3:50 PM	File folder	
PerfLogs	1/19/2008 4:40 AM	File folder	
Program Files	5/20/2014 8:44 PM	File folder	
ProgramData	6/11/2014 8:48 AM	File folder	
share	9/15/2012 3:50 PM	File folder	
Users	1/16/2013 9:22 AM	File folder	
Windows	5/19/2014 4:49 PM	File folder	
BOOTSECT.BAK	9/10/2012 10:01 PM	BAK File	8 KB
Exchange Server Setup Progress.log	5/20/2014 8:43 PM	Text Document	401 KB
test.txt	5/19/2014 3:55 PM	Text Document	1 KB

12. Close all open windows and PC Viewers. End the reservation.

3.1 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 used telnet internally. VPN connections allow users from a branch office to use resources as if they were on the physical network, all over an encrypted connection on the Internet.

3.1 Discussion Questions

1. What is the command to map a drive?
   Ans: The command used to map a drive is z:\\computer\folder.

2. How can you view a mapped drive?
   Ans: To view a map drive command is -net use.

3. What is the command to stop the Windows Time Service?
   Ans: Enter Windows + R and type services.msc

4. What command will allow you to leave a telnet session?
   Ans: The commad used to leave a telnet session is telnet> close.

References

1. TELNET:
   http://en.wikipedia.org/wiki/Telnet

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