



## NETWORK SECURITY LAB SERIES

### Lab 8: Implementing RIP, RIPv2 and Securing RIP

Document Version: **2015-09-28**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCT) 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 .....	3
Lab Topology .....	4
Lab Settings .....	5
1 Configuring RIP Version 1 .....	6
1.1 Setting up RIPv1 .....	6
1.2 Conclusion .....	26
1.3 Discussion Questions.....	26
2 Configuring RIP Version 2 .....	27
2.1 Setting up RIPv2 .....	27
2.2 Conclusion .....	33
2.3 Discussion Questions.....	33
3 Securing RIP .....	34
3.1 Securing RIP .....	34
3.2 Conclusion .....	40
3.3 Discussion Questions.....	40
References .....	41



## 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. Configuring RIP Version 1
2. Configuring RIP Version 2
3. Securing RIP

Key terms for this lab:

**RIPv1** – Routing Information Protocol, Version 1, uses a broadcast address to update information about routing over UDP (User Datagram Protocol) port 520.

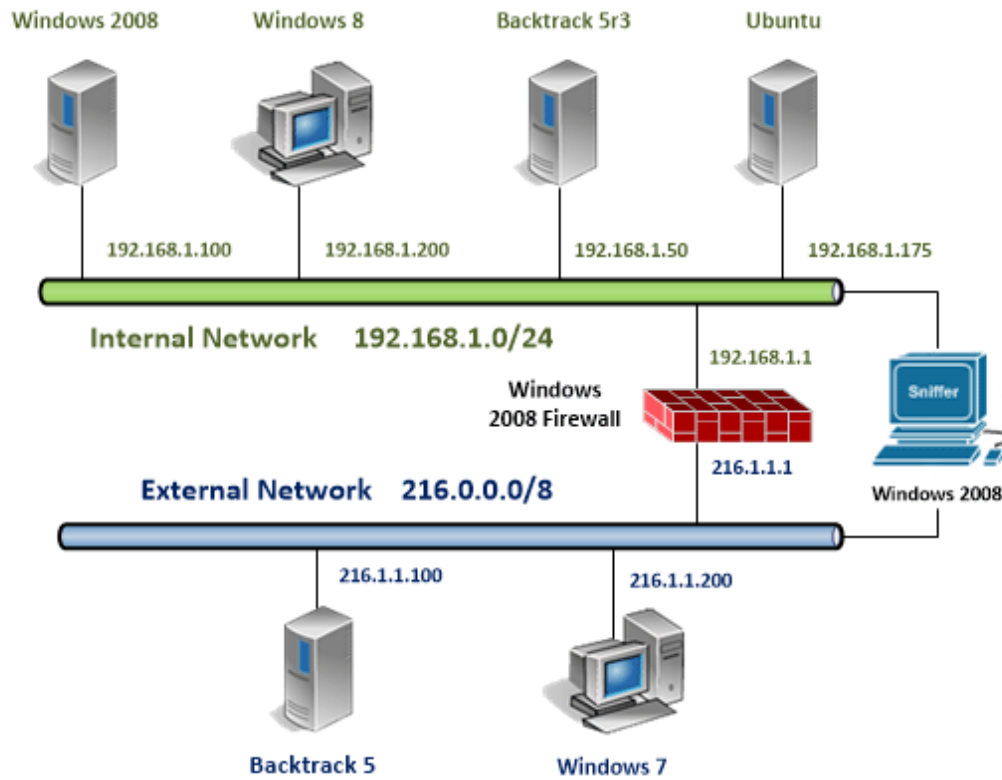
**RIPv2** – Routing Information Protocol, Version 2, uses a multicast address to update information about routing over UDP (User Datagram Protocol) port 520.

**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** – 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 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.

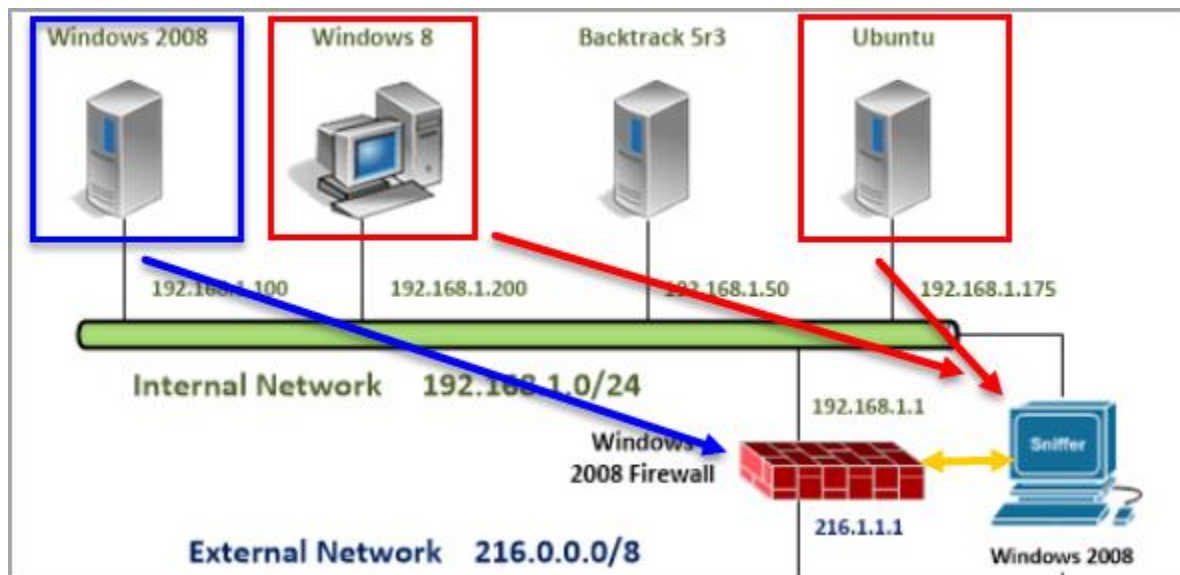


## 1 Configuring RIP Version 1

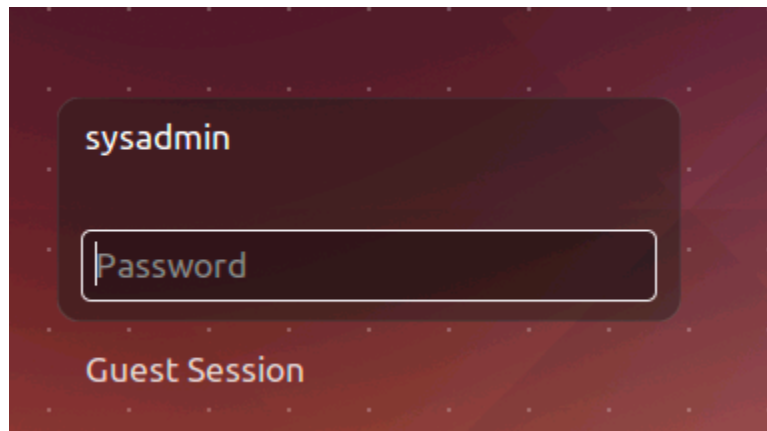
In this section, we will set up RIPv1 on the Windows 2008 Firewall and Sniffer. RIPv1 uses UDP (User Datagram Protocol) and broadcasts. After configuring RIP, all of the machines on the different subnets we set up will be able to communicate with each other.

### 1.1 Setting up RIPv1

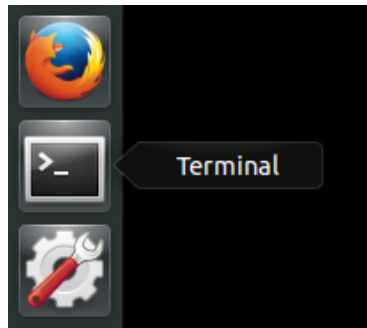
We will now change the IP addresses of some machines on the internal Network. There will be two subnets, 172.168.1.0/24, and 192.168.1.0/24. The Windows 2008 machines with two network interfaces will be configured as routers with RIP (Routing Information Protocol). A computer with two network cards can be used as a router on a network.



1. Log into the **Ubuntu Server** by clicking on the Ubuntu icon on the topology. Log in as the user **sysadmin** with the password of **P@ssw0rd**.



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



- 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** at the sudo prompt. Press **Enter**.

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

- 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
```

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

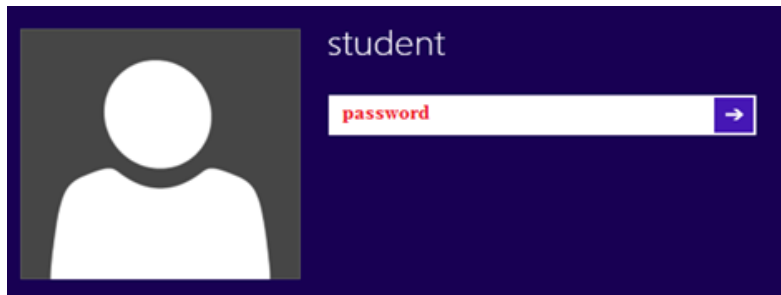
```
sysadmin@ubuntu:~$ netstat -r
Kernel IP routing table
Destination      Gateway         Genmask        Flags   MSS Window  irtt Iface
default          172.16.1.1     0.0.0.0        UG      0 0        0 eth0
172.16.1.0       *              255.255.255.0  U       0 0        0 eth0
sysadmin@ubuntu:~$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

- Type the following command to ping the gateway four times:  
 sysadmin@ubuntu:~# **ping 172.16.1.1 -c 4**

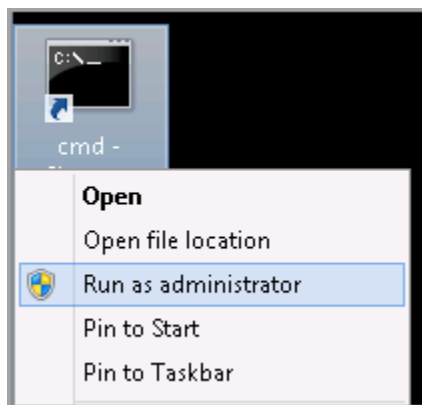
```
sysadmin@ubuntu:~$ ping 172.16.1.1 -c 4
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=128 time=0.444 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=128 time=0.279 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=128 time=0.267 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=128 time=1.26 ms

--- 172.16.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.267/0.563/1.265/0.411 ms
sysadmin@ubuntu:~$
```

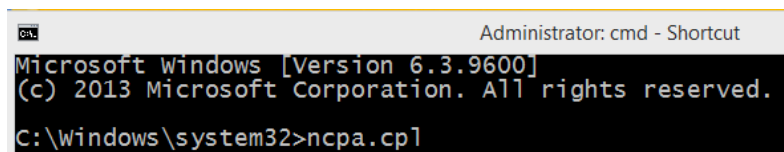
- Click on the **Windows 8** icon on the lab topology to bring up the login screen. For the student password, type **password**, and then press Enter.



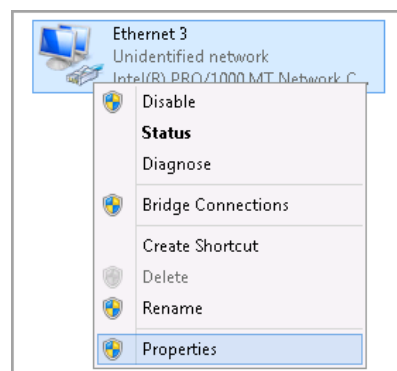
- Right-click on the cmd-Shortcut on the desktop and select **Run as administrator**.



- Type the following command to go to the adapter in the Network Connections Control Panel applet.  
`C:\Windows\system32>ncpa.cpl`

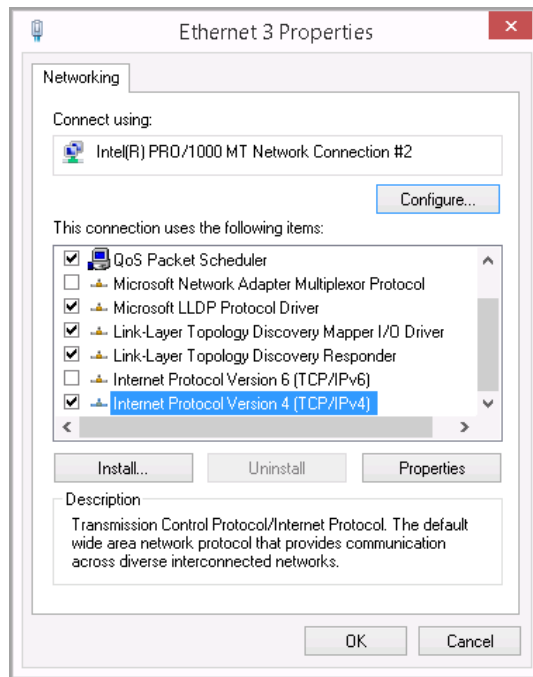


- Right-click on **Ethernet 3** and select **Properties** from the menu bar.

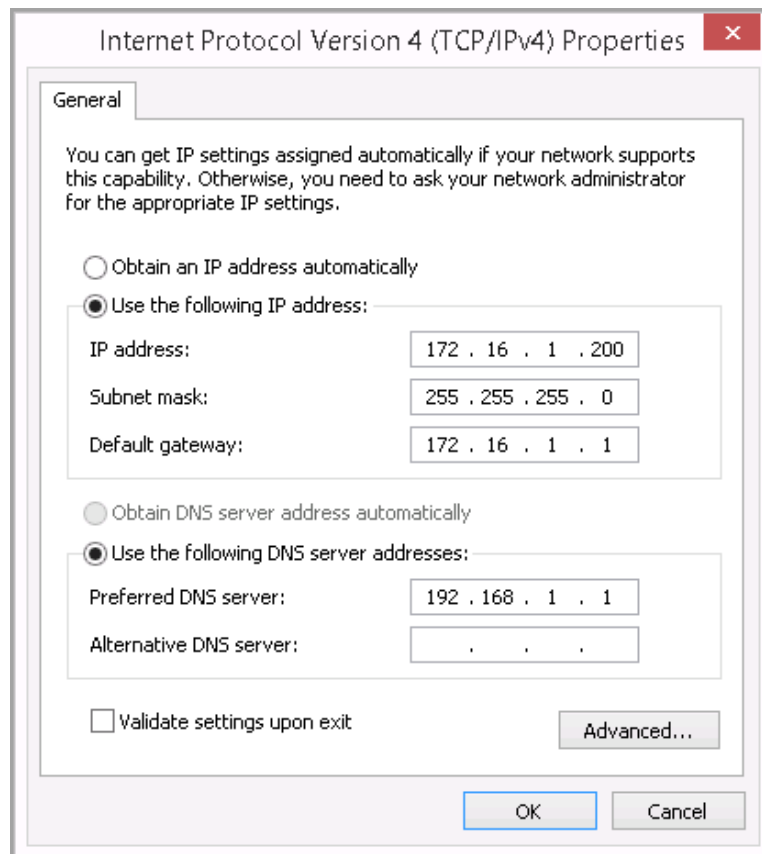




11. Scroll down to **Internet Protocol (TCP/IPv4)** and double-click on it.

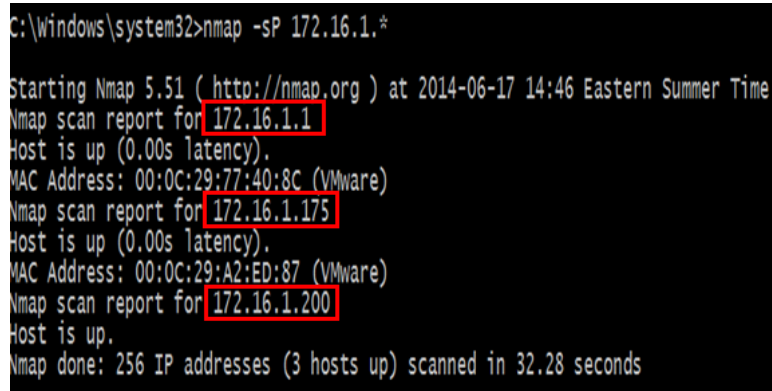


12. Change the IP address to **172.16.1.200** and the Default Gateway to **172.16.1.1**. Leave Subnet Mask and DNS (Domain Name System) fields alone. Click **OK** twice.



13. Go back to command prompt and type the following command to scan the 172.16.1.0/24 network for hosts:

C:\>nmap -sP 172.16.1.\*



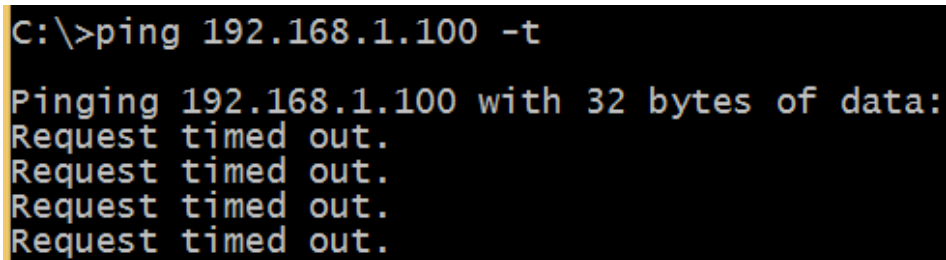
```
C:\Windows\system32>nmap -sP 172.16.1.*  
Starting Nmap 5.51 ( http://nmap.org ) at 2014-06-17 14:46 Eastern Summer Time  
Nmap scan report for 172.16.1.1  
Host is up (0.00s latency).  
MAC Address: 00:0C:29:77:40:8C (VMware)  
Nmap scan report for 172.16.1.175  
Host is up (0.00s latency).  
MAC 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
```

Three hosts: 172.16.1.1, 172.16.1.175 and 172.16.1.200 should all be recognized. This will take a few 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:

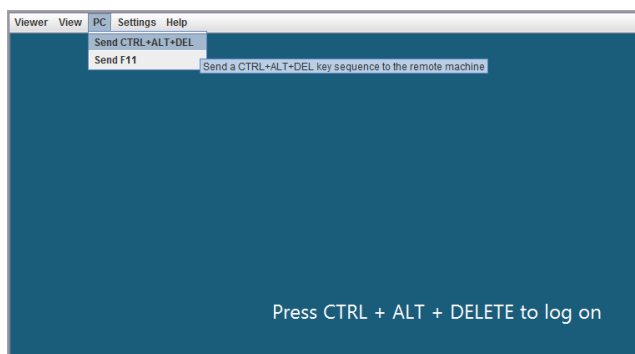
C:\>ping 192.168.1.100 -t

Allow the pings to continue; they will be used later in the lab



```
C:\>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.  
Request timed out.
```

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



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



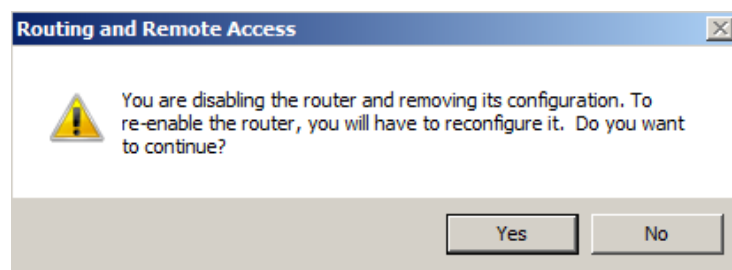
17. On the Windows 2008 Firewall, double-click the shortcut to **Routing and Remote Access** on the desktop.



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



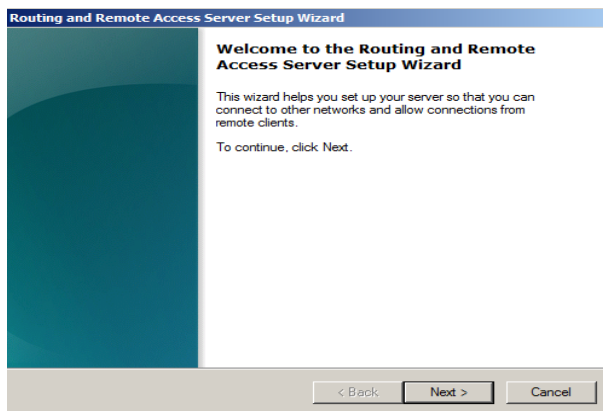
19. Select **Yes** when you are asked if you want to continue.



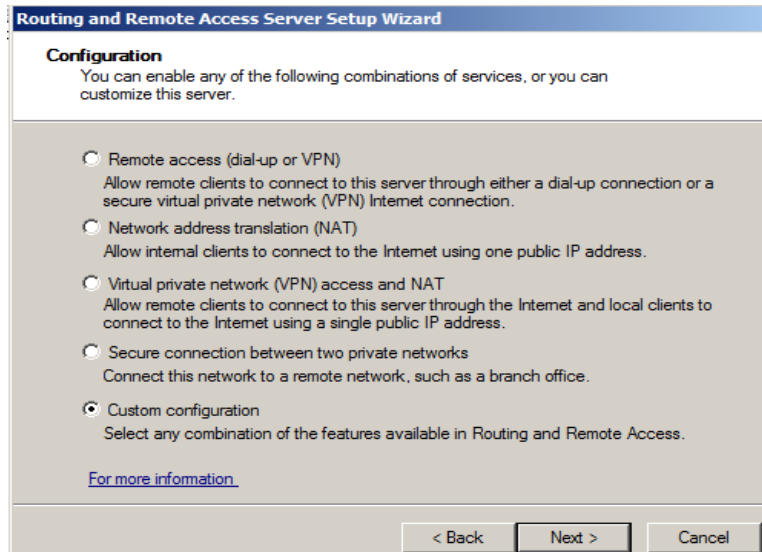
20. Right-click on FW (local) and select **Configure Routing and Remote Access**.



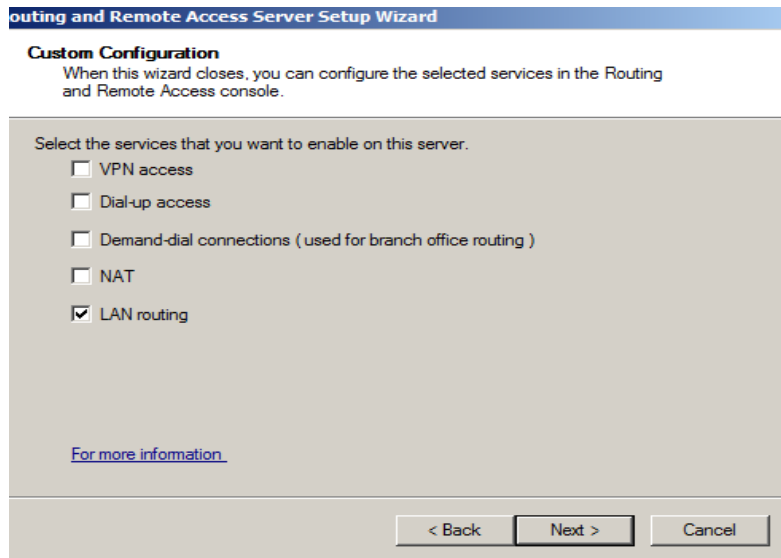
21. Click **Next** on the **Welcome to the Routing and Remote Access Setup Wizard**.



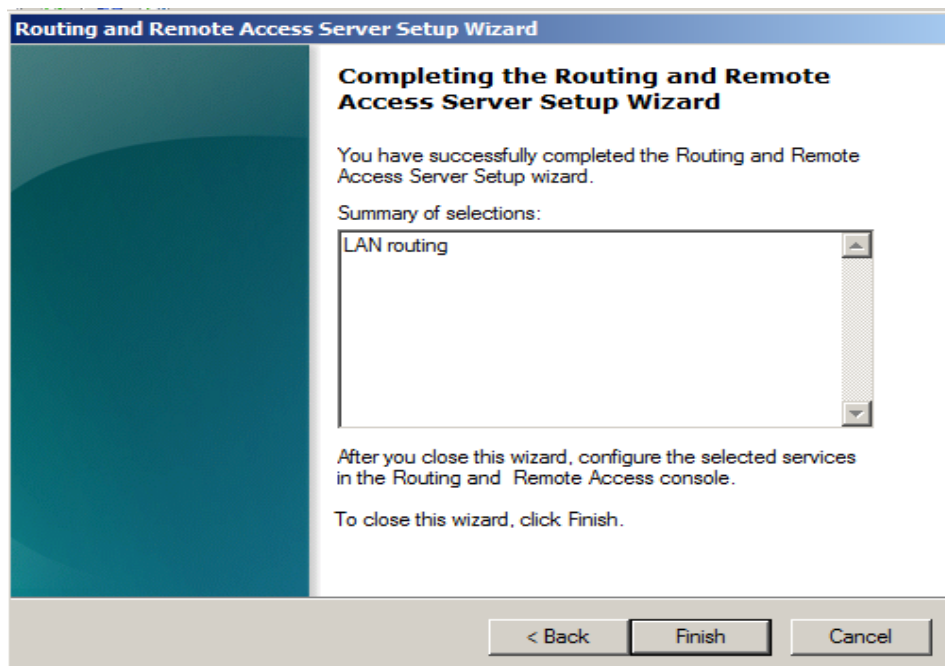
22. Choose **Custom Configuration** and click **Next**.



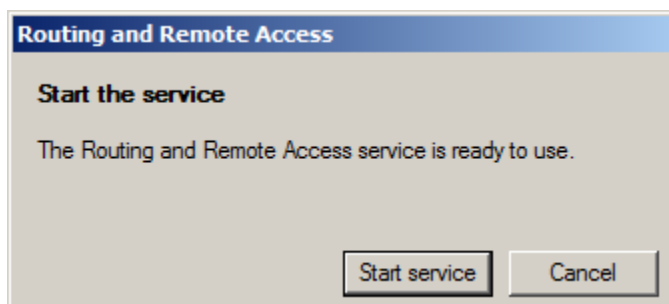
23. Select **LAN routing** and click the **Next** button.



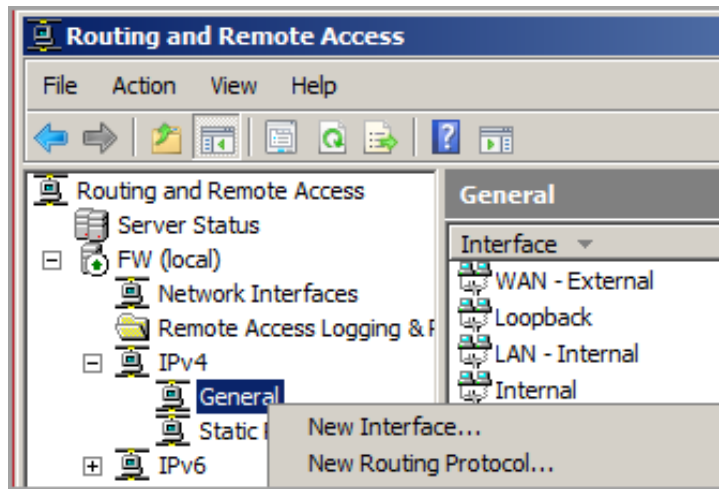
24. Click **Finish** on the Completing Routing and Remote Access Setup Wizard.



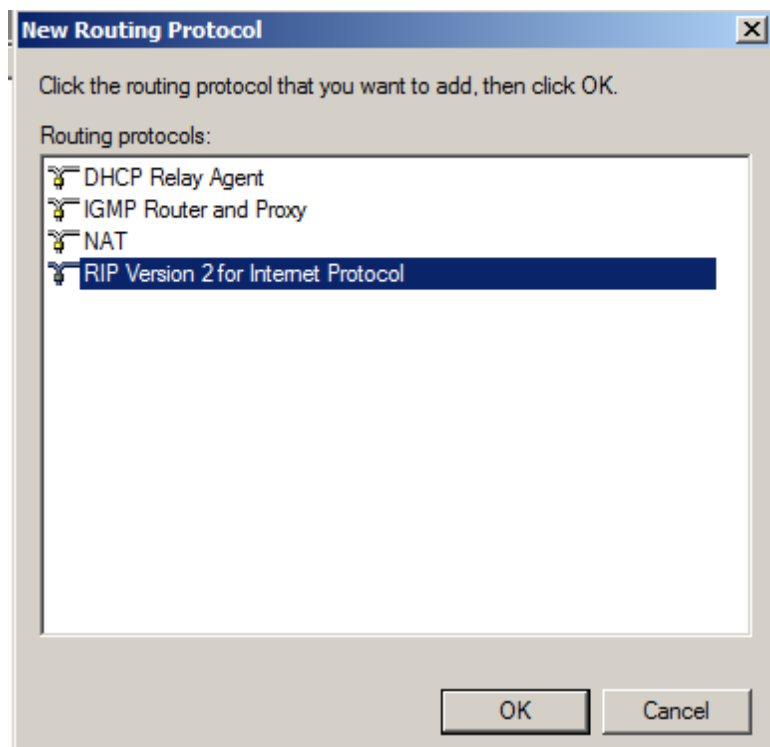
25. Click **Start service**.



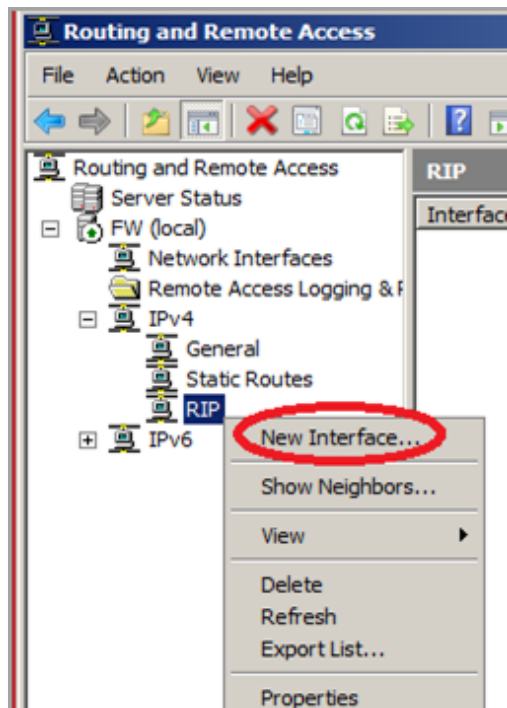
26. Expand FW (local), then expand IPv4, right-click on General and select **New Routing Protocol**.



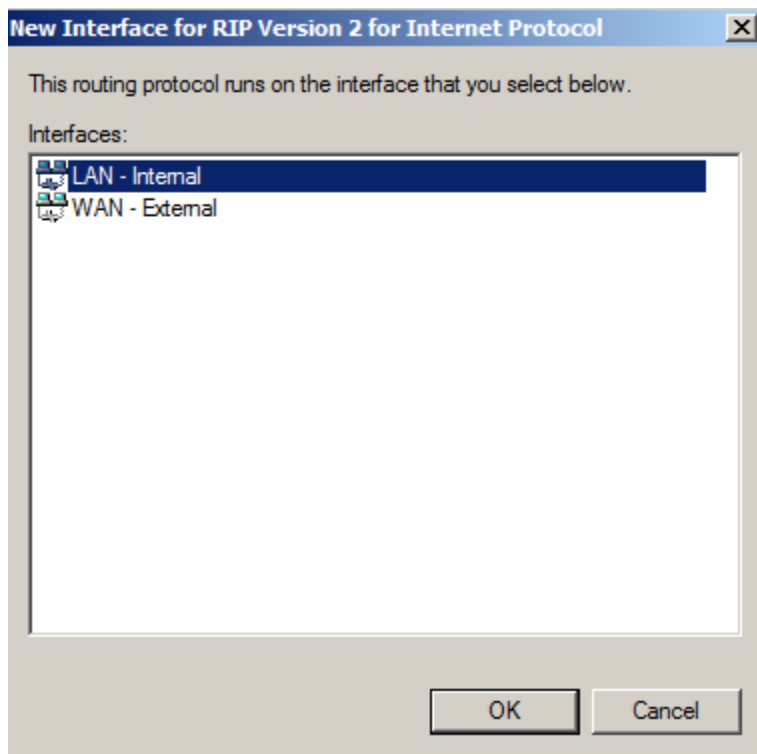
27. Select **RIP Version 2 for Internet Protocol** and click **OK**.



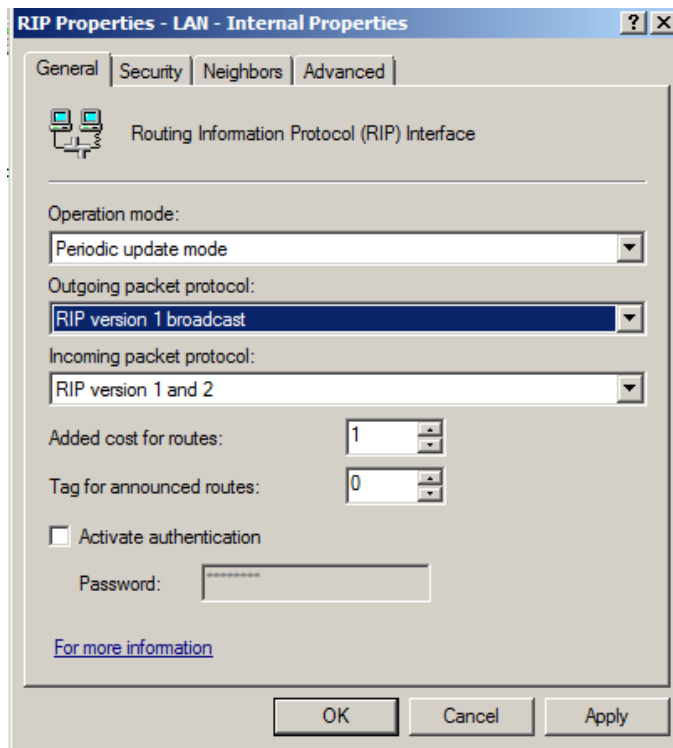
28. Under **IPv4**, right-click **RIP** and select **New Interface**.



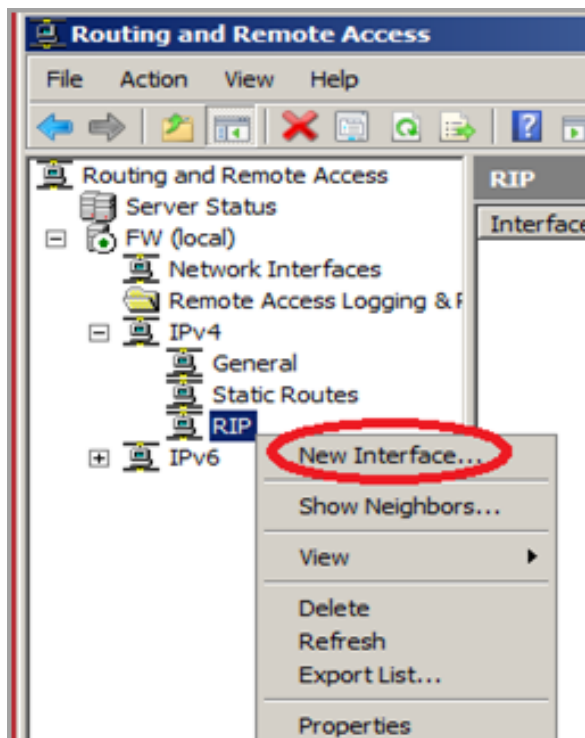
29. Select **LAN-Internal** and select the **OK** button.



30. For **Outgoing packet protocol**, select **RIP version 1 broadcast** and click **Apply** then **OK**.

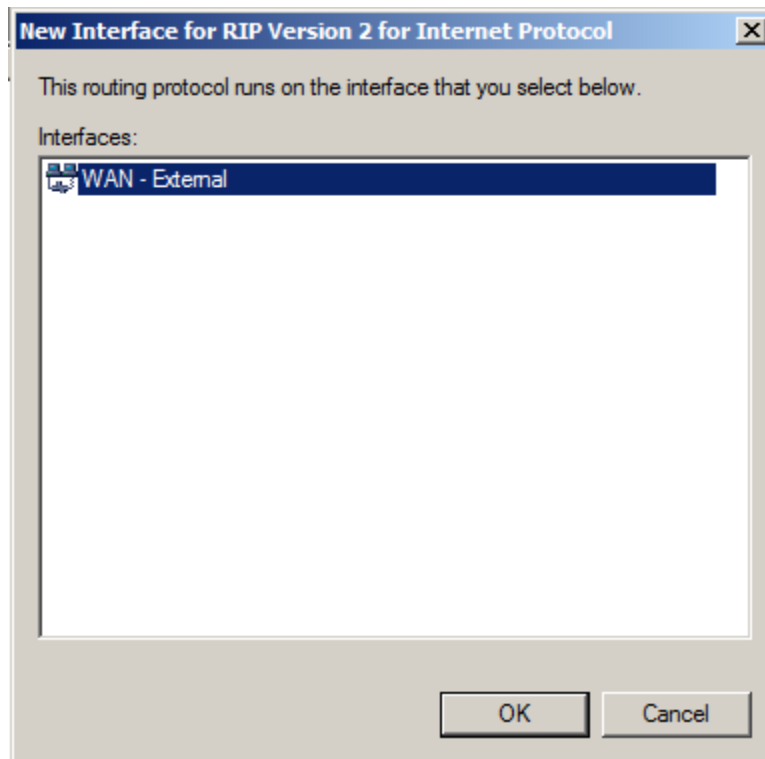


31. Under IPv4, right-click RIP and select **New Interface**.

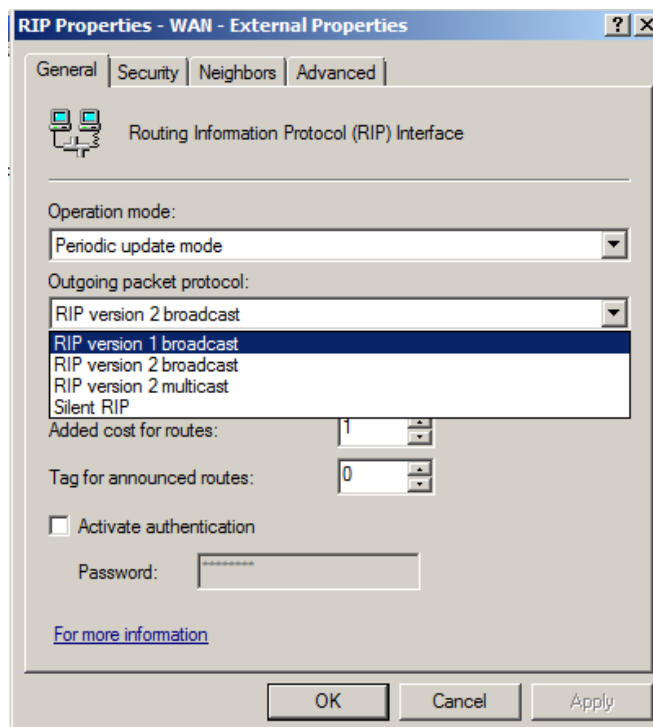




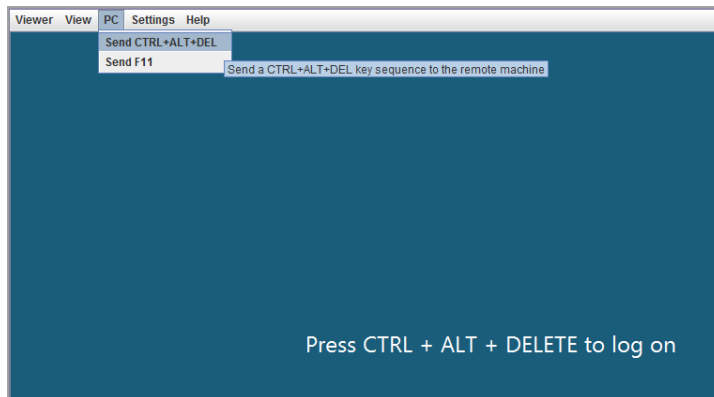
32. Select **WAN-External** and select the **OK** button.



33. For **Outgoing packet protocol**, select **RIP version 1 broadcast** and click **Apply**, then **OK**.



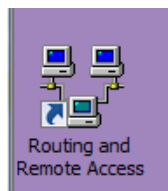
34. Click on the **Windows 2008 Sniffer** icon on the topology. Click **PC** in the upper-left and **Send Ctrl+Alt+Del** in order to log on to the Windows 2008 server.



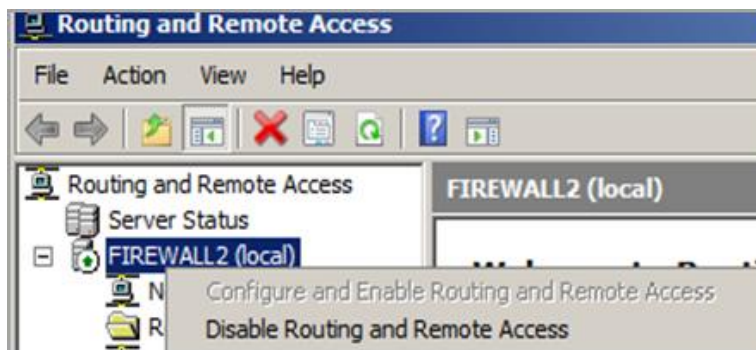
35. Enter **sniffer** for the Administrator password to the Windows 2008 Server.



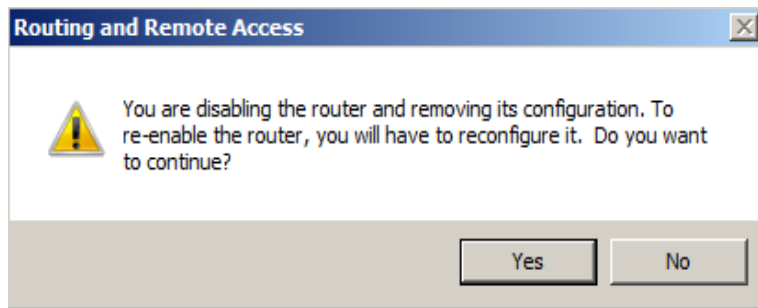
36. Click the shortcut to **Routing and Remote Access** on the desktop.



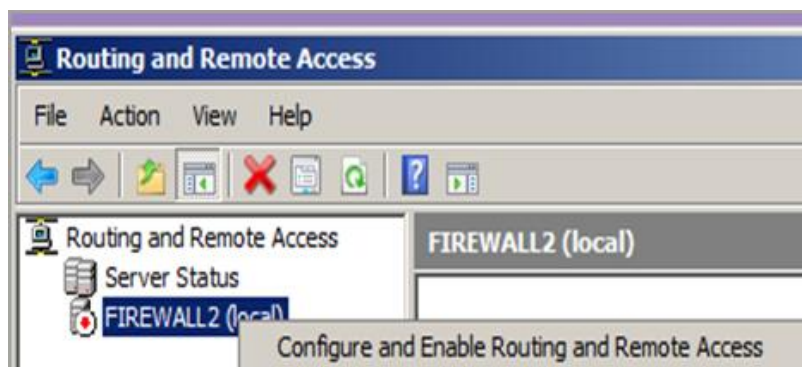
37. Right-click on **Firewall2** and select **Disable Routing and Remote Access**.



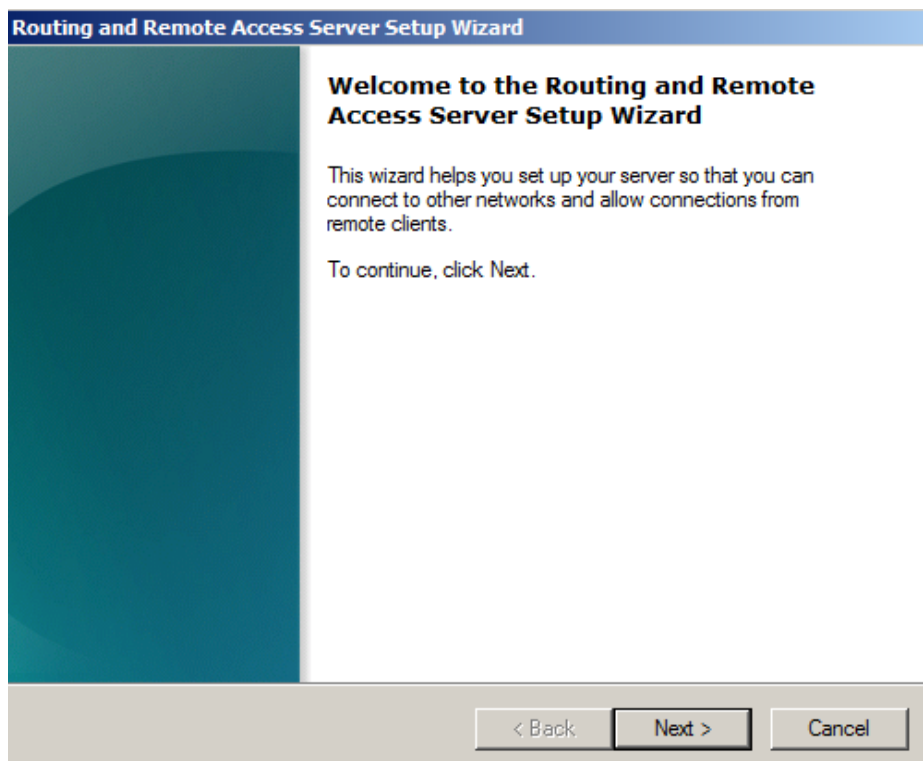
38. Select **Yes** when asked if you want to continue.



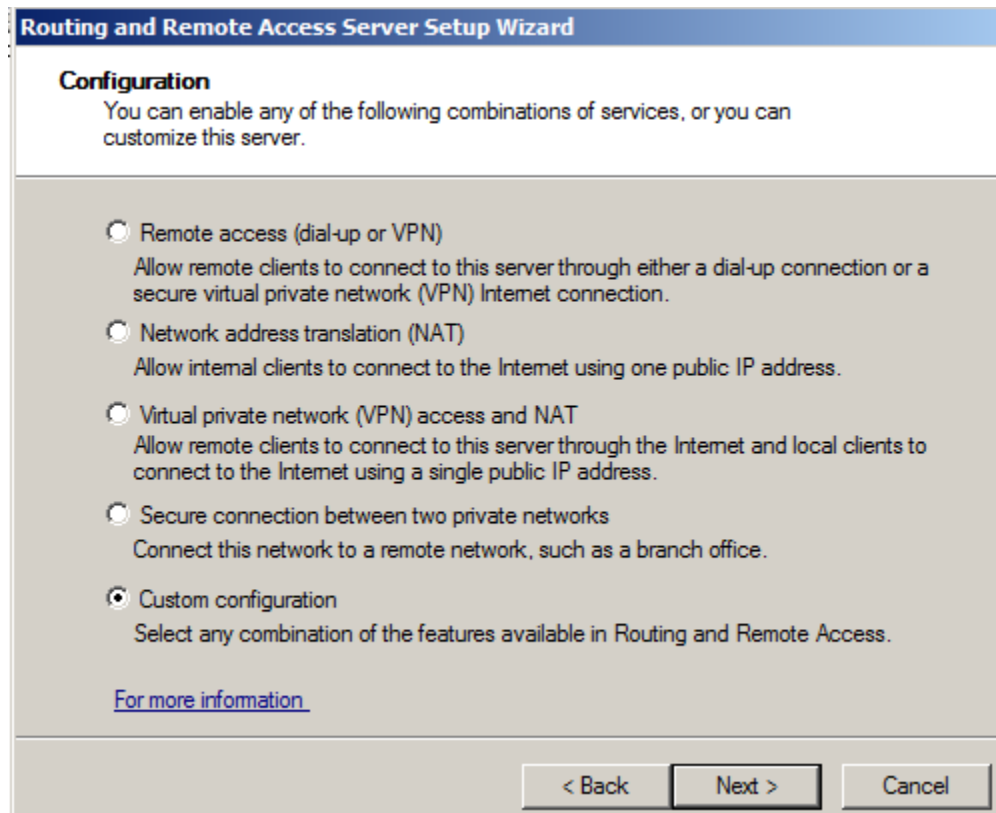
39. Right-click on **FIREWALL2 (local)** and select **Configure Routing and Remote Access**.



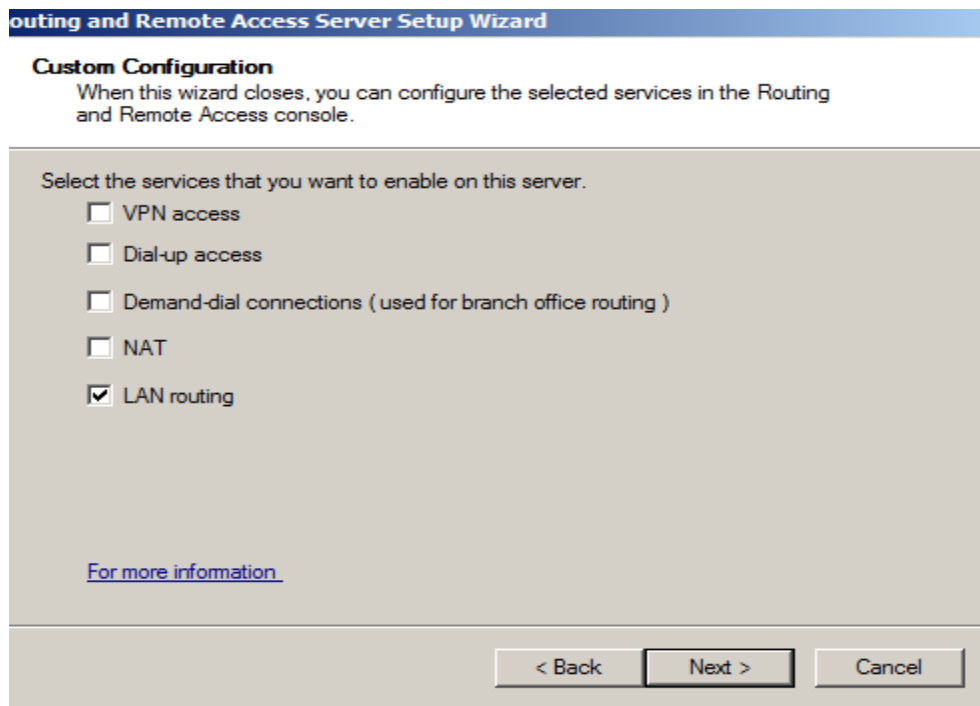
40. Click **Next** to the **Welcome to the Routing and Remote Access Setup Wizard**.



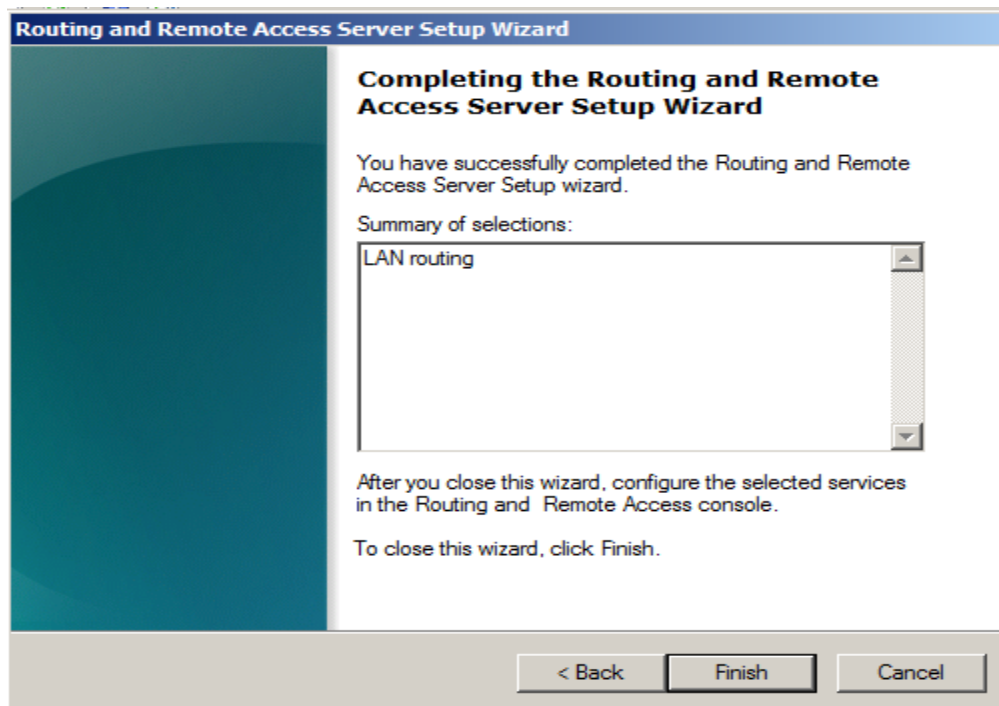
41. Chose **Custom Configuration** and click **Next**.



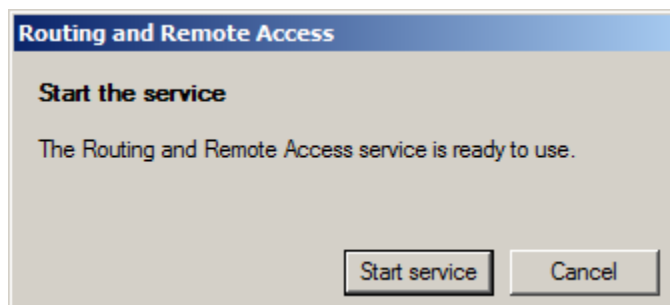
42. Select **LAN Routing** and click the **Next** button.



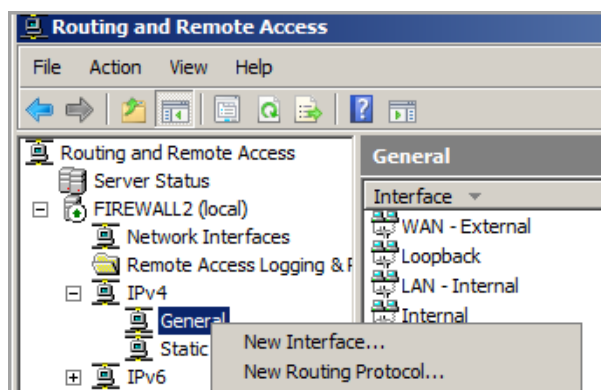
43. Click **Finish** on the **Completing Routing and Remote Access Setup Wizard**.



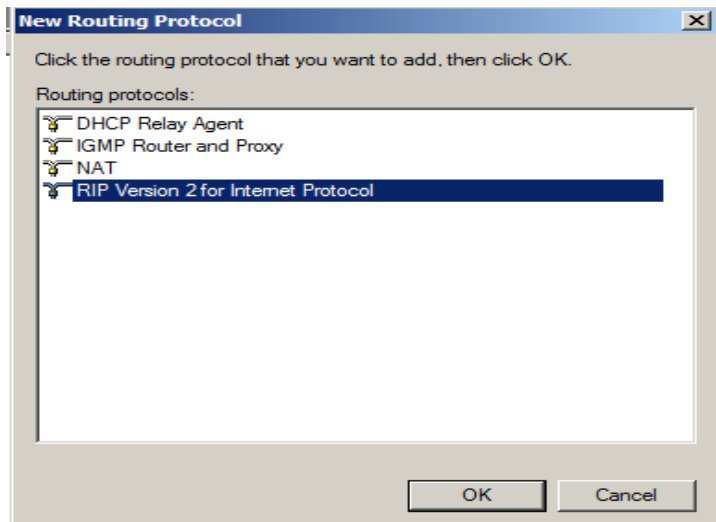
44. Click **Start Service**.



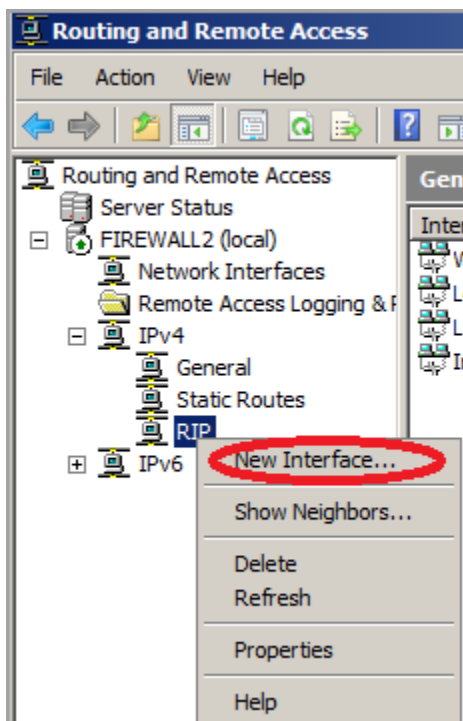
45. Expand **FIREWALL2**, then **IPv4**, Right-click on **General** and select **New Routing Protocol**.



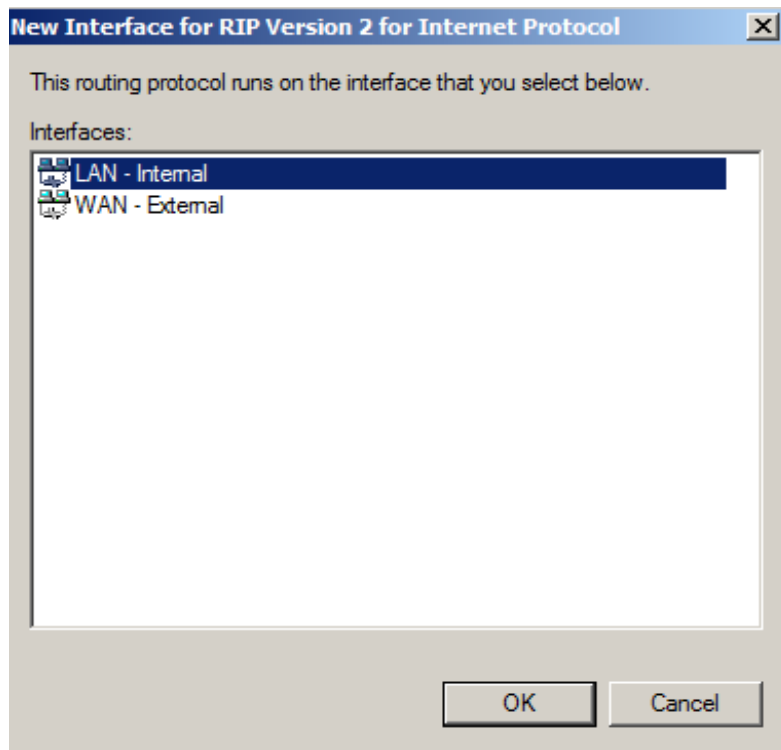
46. Select **RIP Version 2 for Internet Protocol** and click **OK**.



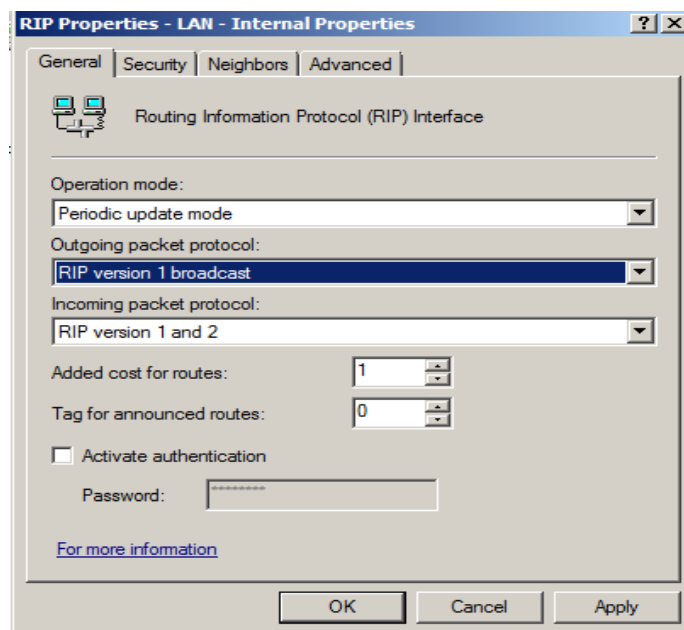
47. Under IPv4, right-click RIP and select **New Interface**.



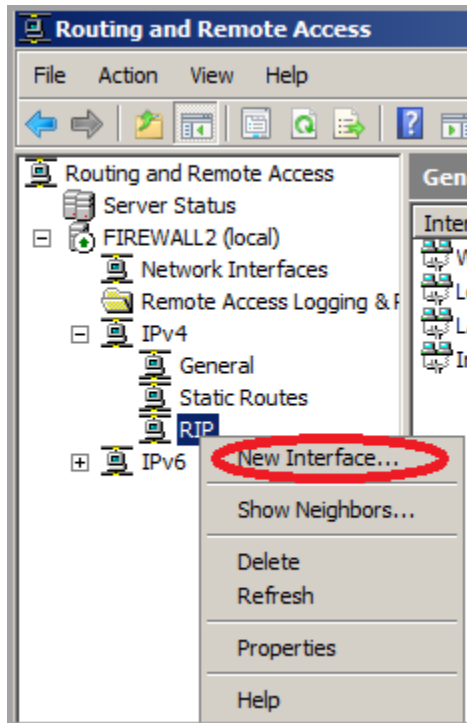
48. Select **LAN-Internal** and select the OK button.



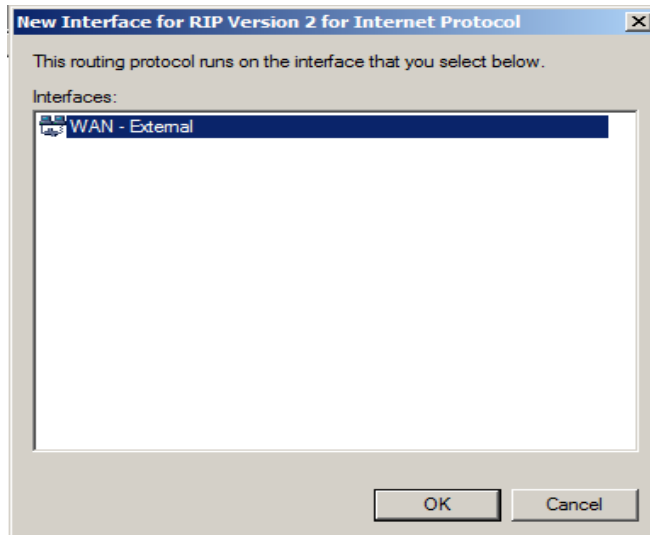
49. For Outgoing packet protocol, select **RIP version 1 broadcast** and click **Apply** then **OK**.



50. Under IPv4, right-click RIP and select **New Interface**.

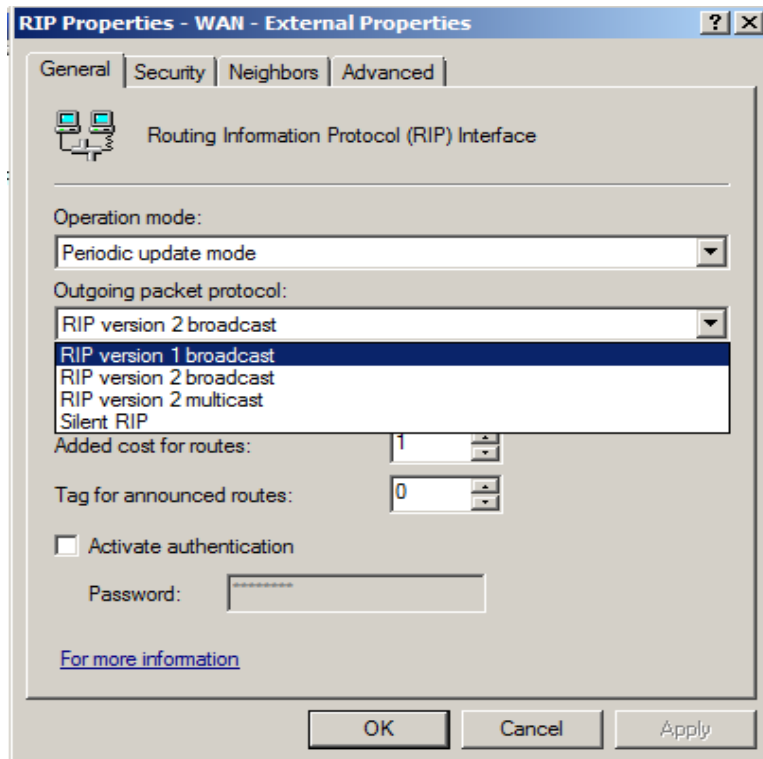


51. Select **WAN-External** and select the **OK** button.





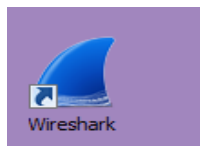
52. For Outgoing packet protocol, select **RIP version 1 broadcast** and click **Apply** then **OK**.



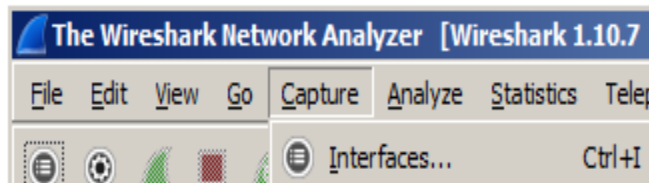
53. Navigate back to the **Windows 8 Internal Machine**. After a few minutes, the pings should respond. After you receive replies, press **Ctrl+C** to stop the continuous ping.

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
```

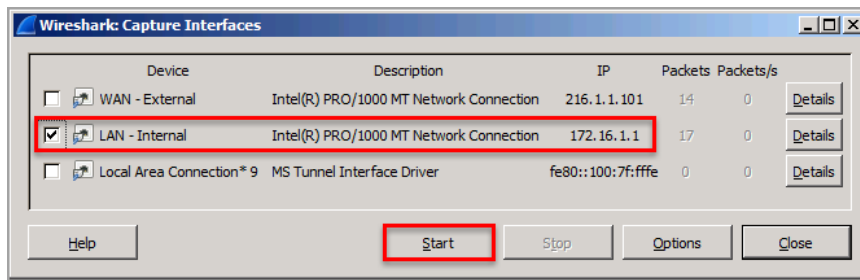
54. On the Sniffer machine, click on the shortcut to Wireshark on the desktop to launch the program.



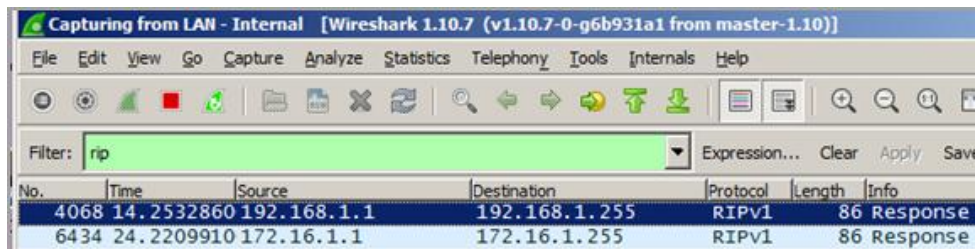
55. Click on Capture from the menu bar and select **Interfaces**.



56. Select the **LAN - Internal** check-box. Click the **Start** button.



57. Type **rip** in the Wireshark filter pane and click apply. View the broadcast address. Continue to leave Wireshark running, since it will be used again in the next task.



## 1.2 Conclusion

Routing Information Protocol (RIP), version 1 uses broadcast messages to send out information about routes. RIP is an open standard that can be used on devices other than Cisco Equipment. A computer with 2 Network Cards (NICS) can act as a router.

## 1.3 Discussion Questions

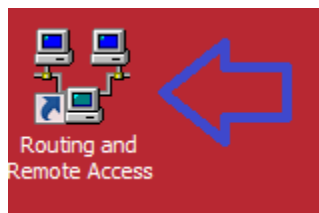
1. What does RIP stand for?
2. Does RIP use UDP or TCP?
3. What port does RIP use?
4. Why is the RIP protocol useful in networks?

## 2 Configuring RIP Version 2

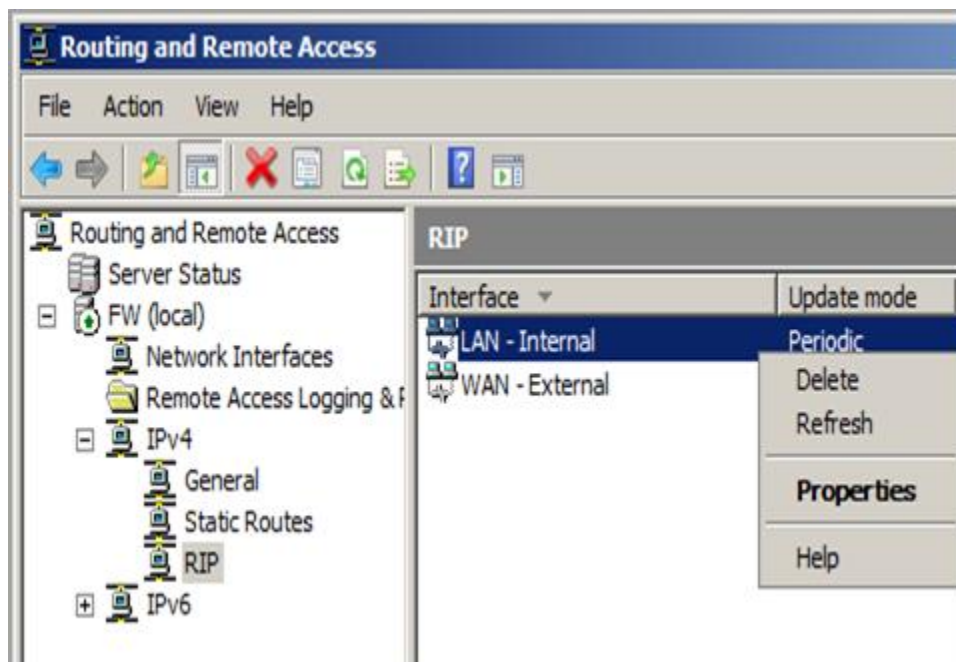
While RIP version 1 uses broadcasts to send out updates about routing information, RIP version 2 uses multicast. A multicast address is a class D address, and can range from 224-239 for the first octet. RIPv2 uses a multicast address of 224.0.0.9. RIP version 2 still uses UDP port 520. RIPv2 is an open standard, and can be used on non-Cisco devices.

### 2.1 Setting up RIPv2

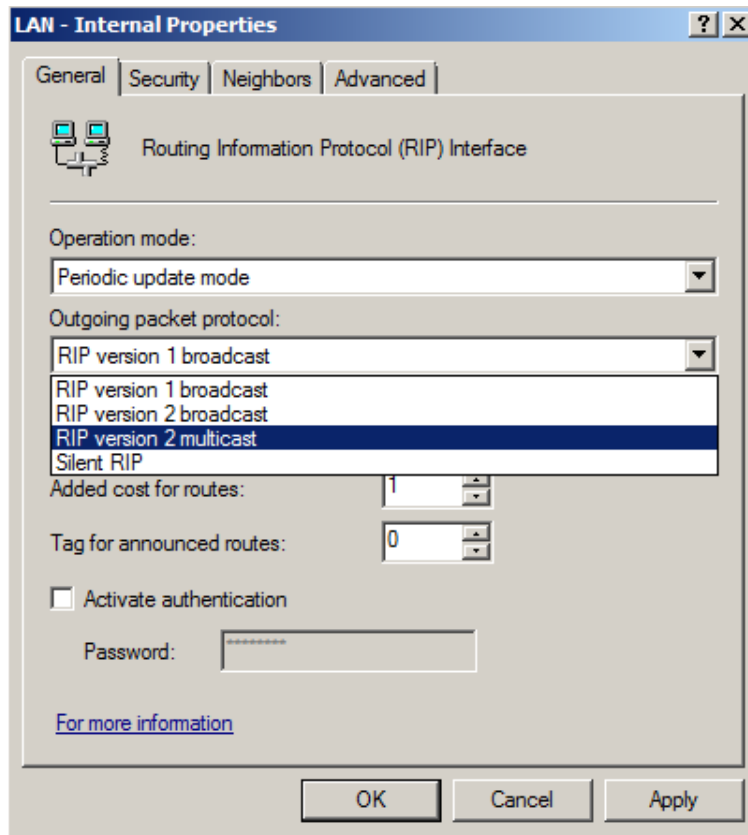
1. On the **Windows 2008 Firewall**, double-click the shortcut to **Routing and Remote Access** on the desktop.



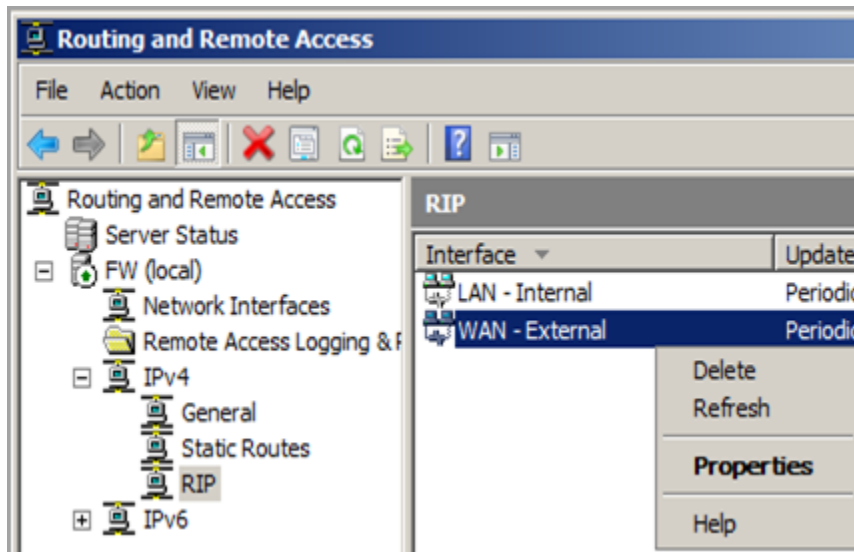
2. Expand FW, IPv4, and click on RIP. Right-click on **LAN - Internal** and go to **Properties**.



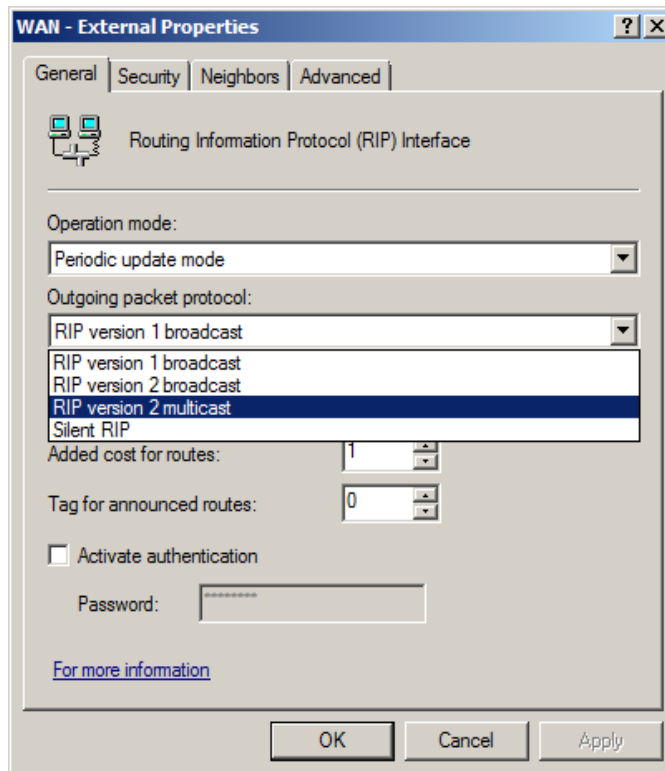
- For **Outgoing packet protocol**, select **RIP version 2 multicast** and click **Apply** then **OK**.



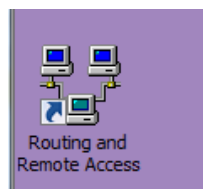
- Right-click on **WAN - External** and go to **Properties**.



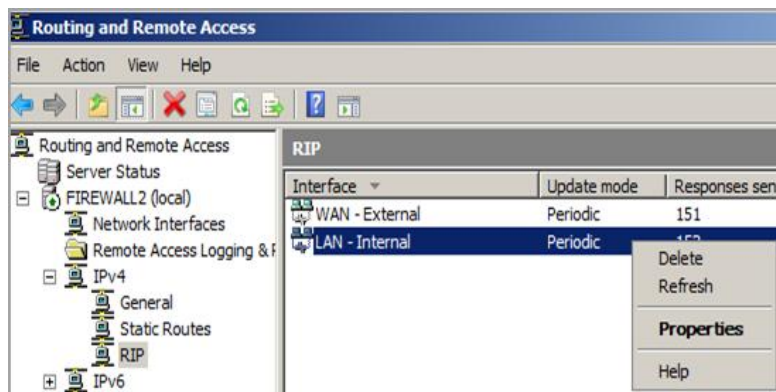
- For **Outgoing packet protocol**, select **RIP version 2 multicast** and click **Apply** then **OK**.



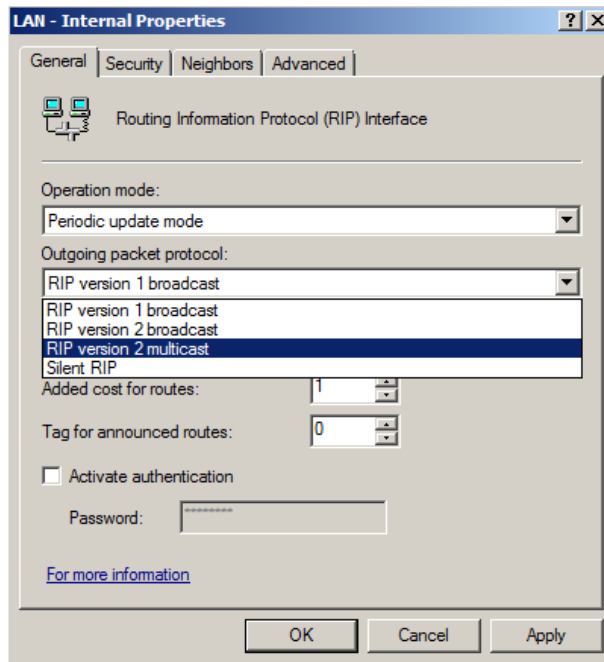
- On the **Windows 2008 Sniffer**, double-click the shortcut to **Routing and Remote Access** on the desktop.



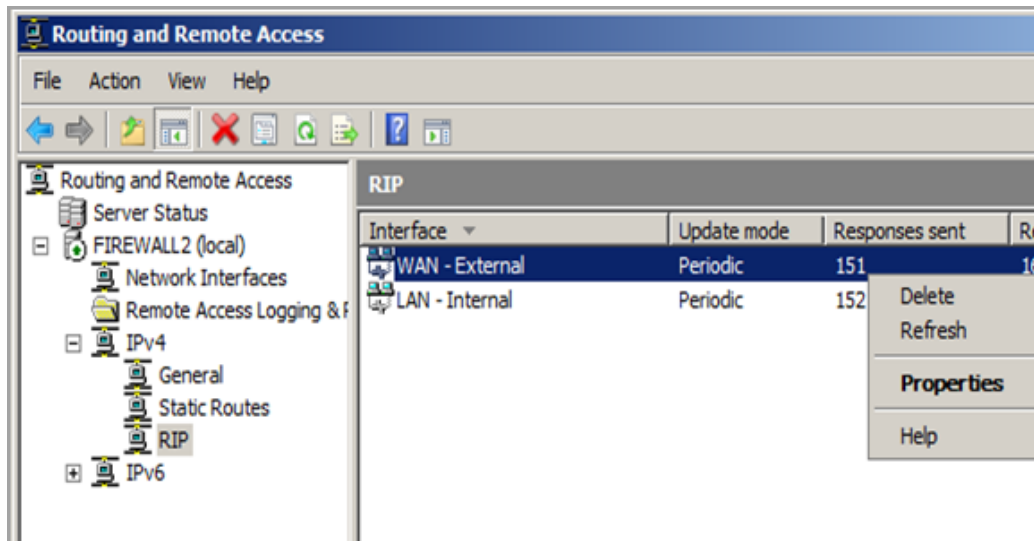
- Expand FIREWALL2, IPv4, and click on RIP. Right-click on **LAN – Internal** and go to **Properties**.



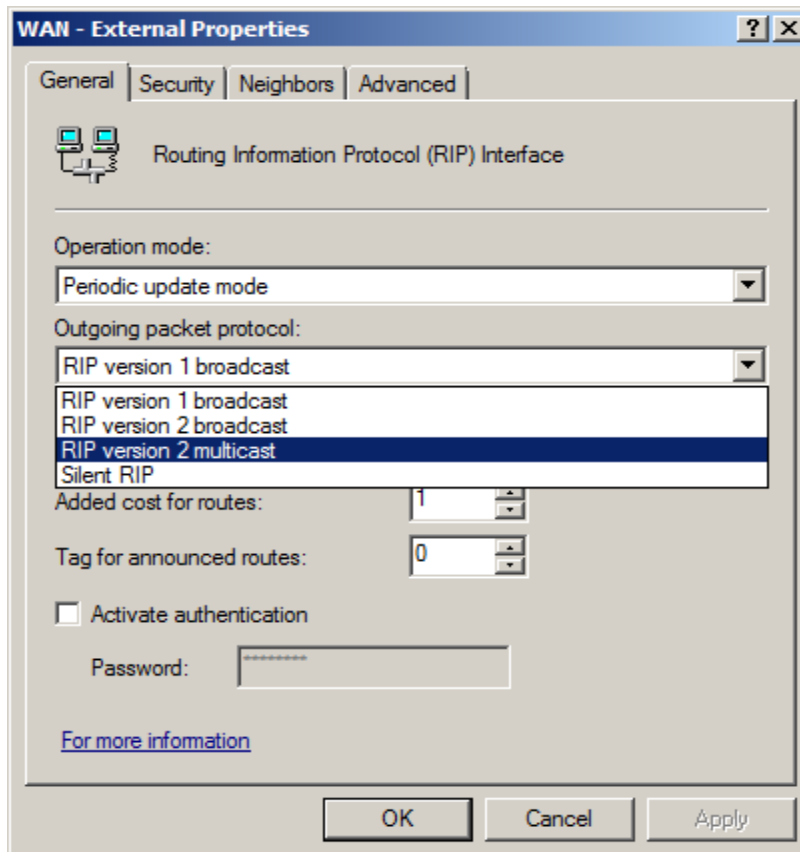
8. For **Outgoing packet protocol**, select **RIP version 2 multicast** and click **Apply** then **OK**.



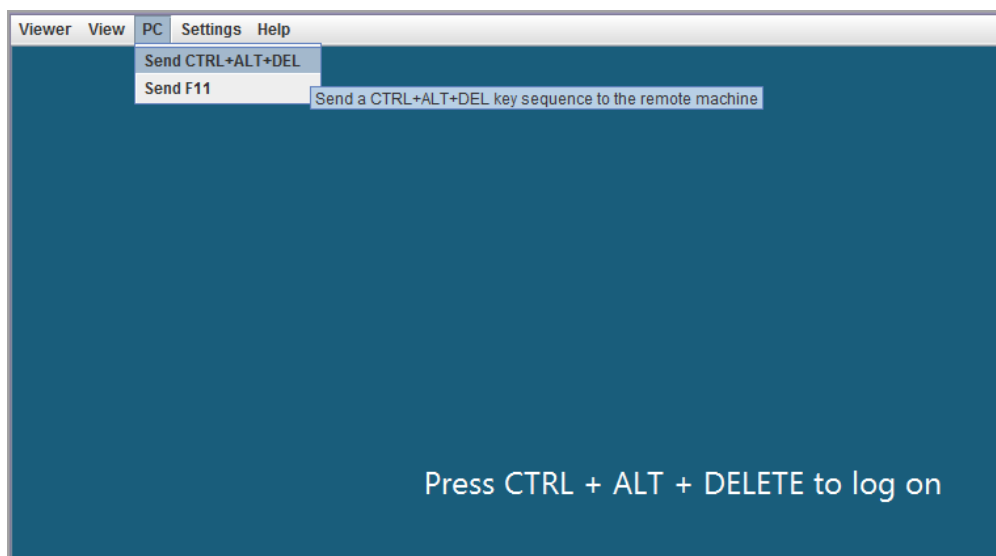
9. Right-click on **WAN – External** and go to **Properties**.



10. For **Outgoing packet protocol**, select **RIP version 2 multicast** and click **Apply** then **OK**.



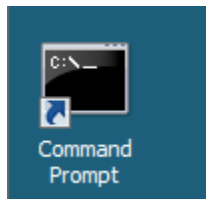
11. Click on the **Windows 2008 Internal Server** icon on the topology. Click **PC**, then **Send Ctrl+Alt+Del** in the top- left corner of the screen in order to log on to the Windows 2008 server.



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



13. Double-click on the shortcut to the **Command Prompt** on the desktop.



14. Type the following command on the Internal 2008 Server machine:  
**C:\>ping 172.16.1.175**

```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

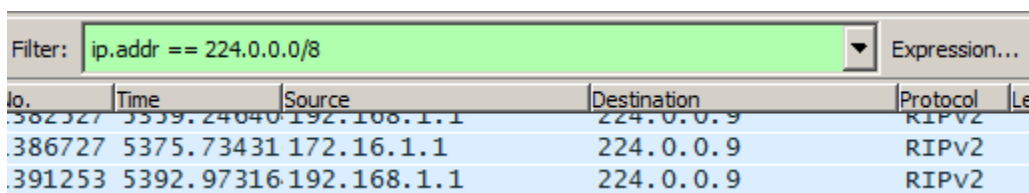
C:\>ping 172.16.1.175

Pinging 172.16.1.175 with 32 bytes of data:
Reply from 172.16.1.175: bytes=32 time=1ms TTL=62
Reply from 172.16.1.175: bytes=32 time<1ms TTL=62
Reply from 172.16.1.175: bytes=32 time=1ms TTL=62
Reply from 172.16.1.175: bytes=32 time=1ms TTL=62

Ping statistics for 172.16.1.175:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Perform the next step on the sniffer machine (where Wireshark is already running):

15. Type **ip.addr == 224.0.0.0/8** in the Wireshark filter pane and click apply. View the multicast traffic. Notice the multicast address of 224.0.0.9 for the RIPv2 packets.





**16. Open a command prompt on your local computer. On the command line, type your first and last names. Take a screenshot that contains your full name and the output window generated at above Step 15.**

## **2.2 Conclusion**

While RIP version 1 uses a broadcast address, RIPv2 uses multicast. The multicast address range (Class D) is from 224-239 for the first octet. RIPv2 uses a multicast address of 224.0.0.9. RIP version 2 still uses UDP port 520. RIPv2 is an open standard, and can be used on non-Cisco devices. A machine with 2 NICs can be a router.

## **2.3 Discussion Questions**

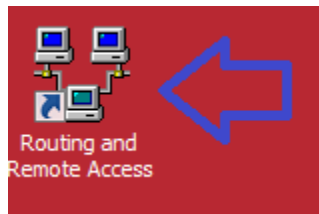
1. Does RIP version 2 use a multicast or broadcast address?
2. What is the multicast address for RIPv2?
3. What filter is used in Wireshark to locate RIP version 2 traffic?
4. What User Datagram (UDP) port does RIP use?

### 3 Securing RIP

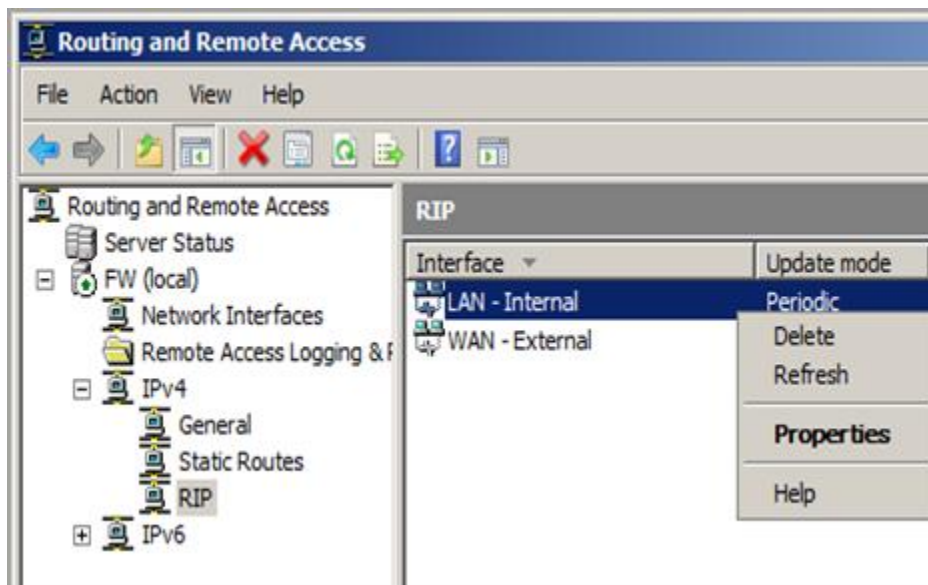
We will add a password so routing updates cannot be accessed without routers having the same password. It is important to protect the routing information on a network.

#### 3.1 Securing RIP

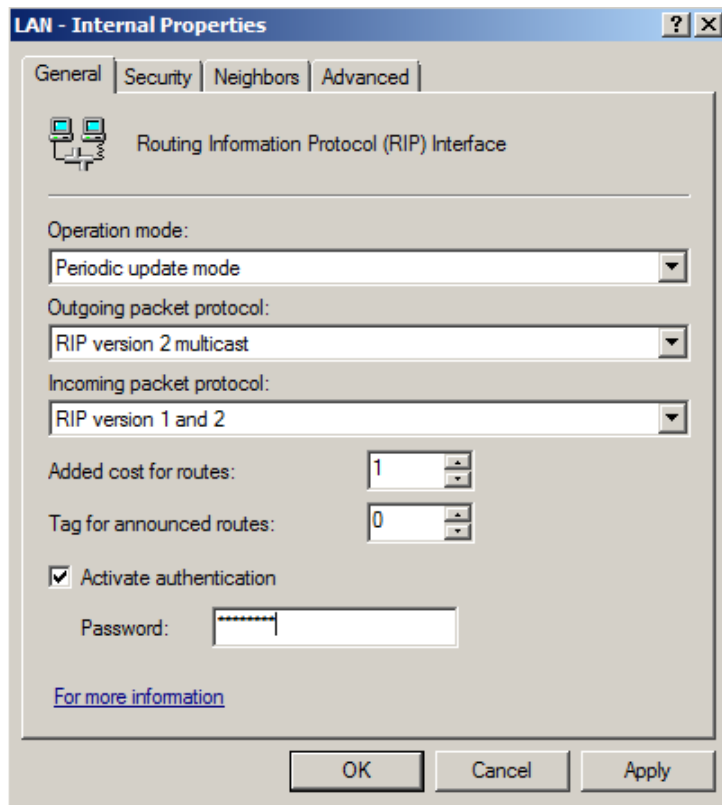
1. Return to the Windows 2008 Firewall. If not already open, double-click the Shortcut to Routing and Remote Access on the Desktop.



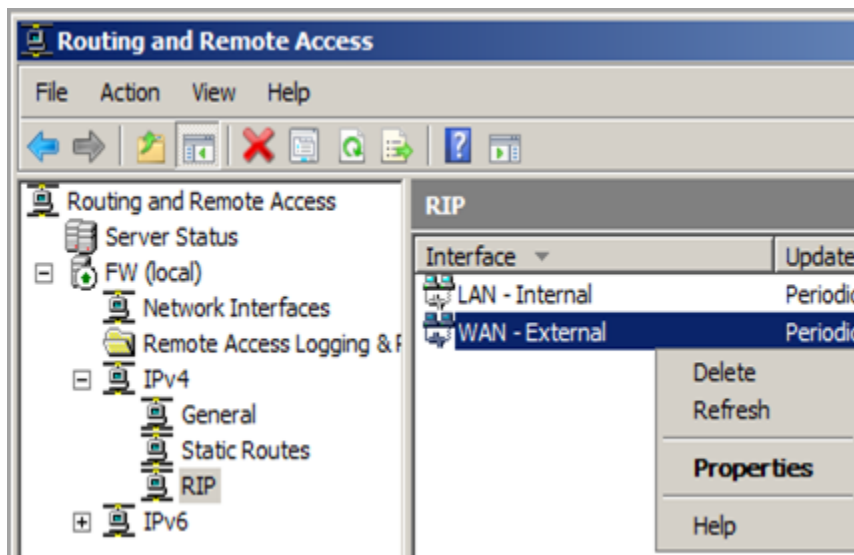
2. Expand FW, IPv4, and click on RIP. Right-click on **LAN - Internal** and go to **Properties**.



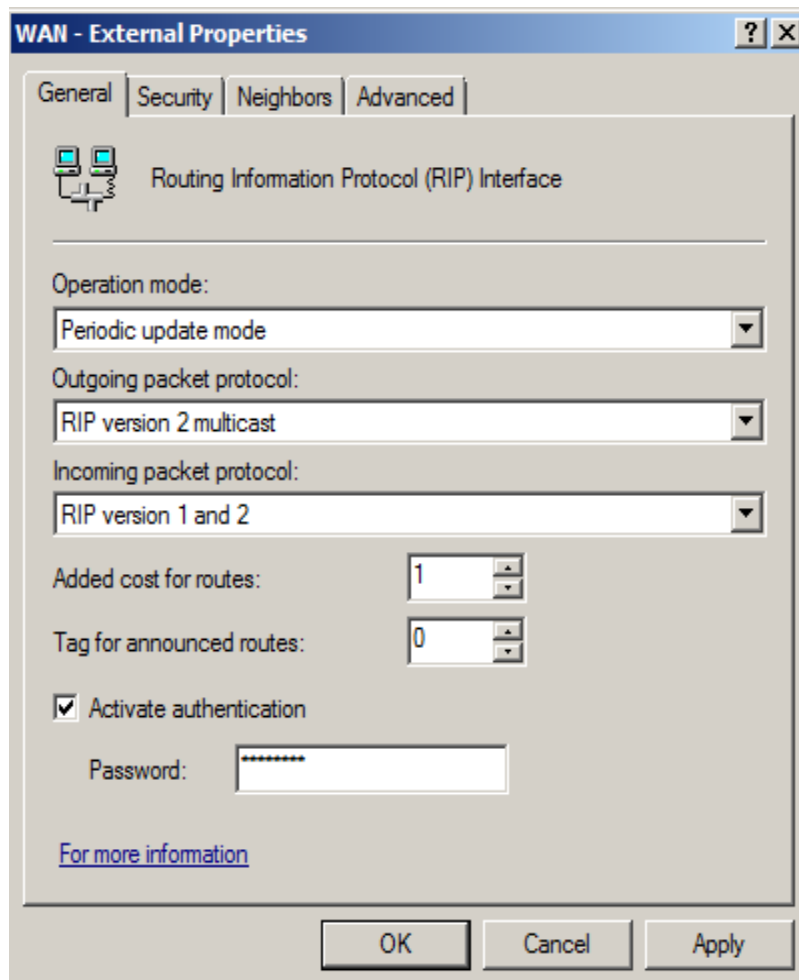
3. Check the **Activate authentication** check box, type **password** and click OK.



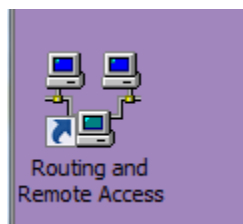
4. Right-click on **WAN – External** and go to **Properties**.



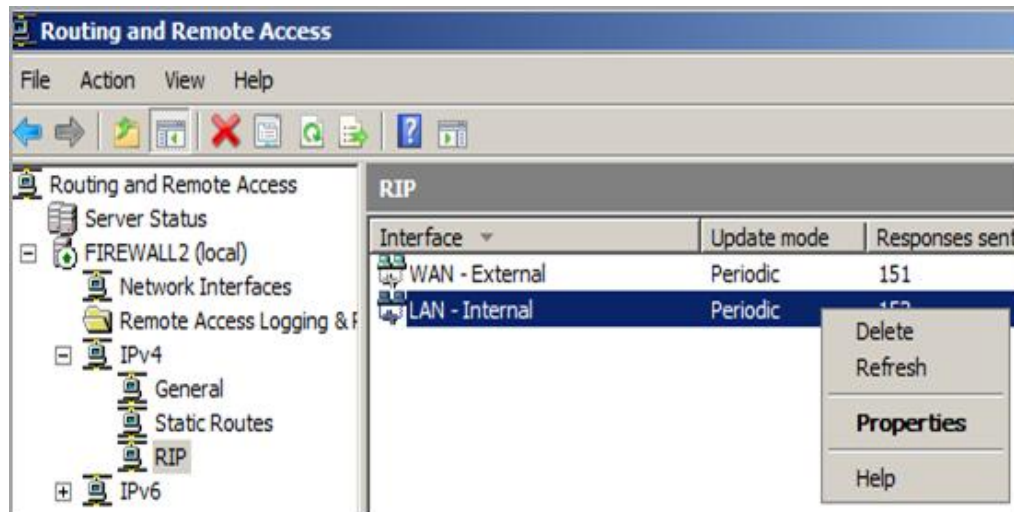
5. Check the **Activate authentication** check box, type **password** and click OK.



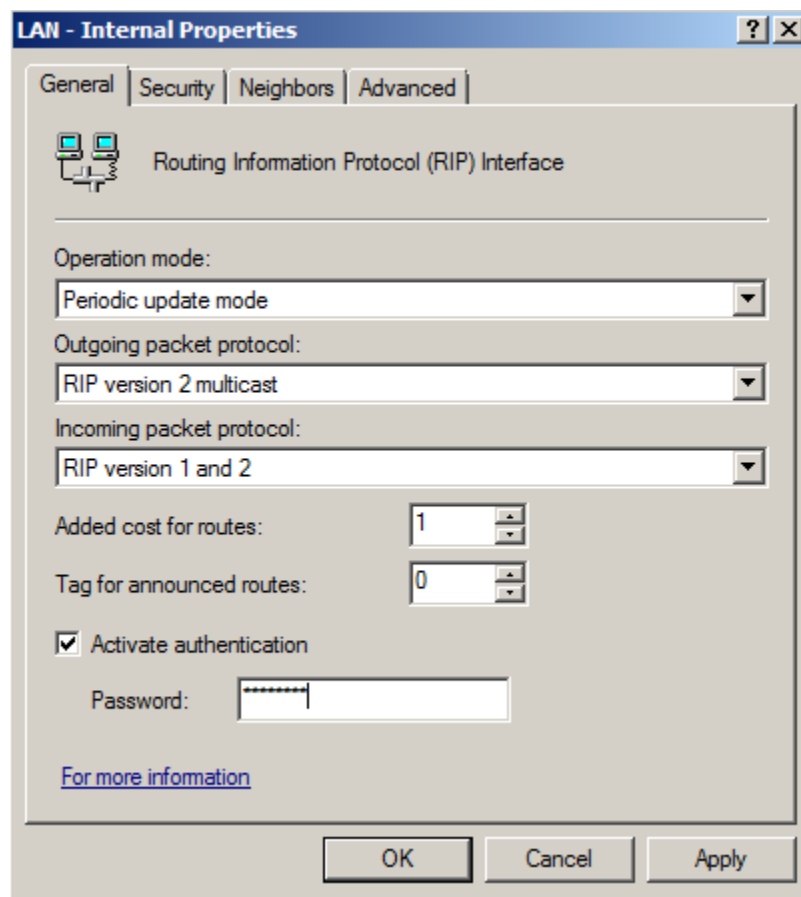
6. Return to the **Windows 2008 Sniffer**. If not already open, double-click the shortcut to **Routing and Remote Access** on the desktop.



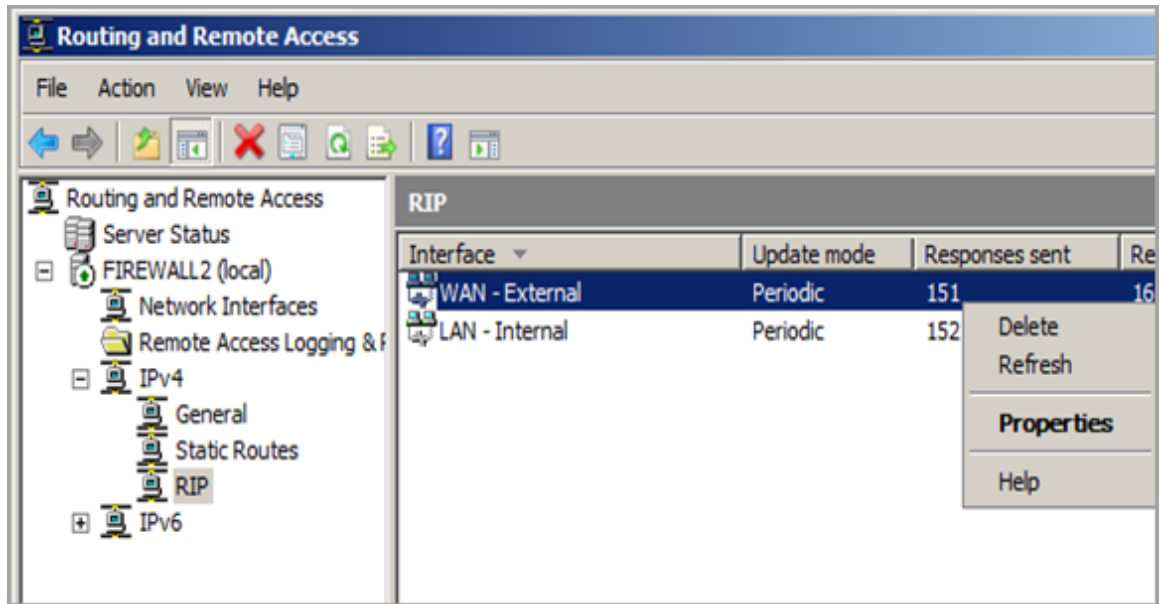
7. Expand FIREWALL2, IPv4, and click on RIP. Right-click on **LAN-Internal** and go to **Properties**.



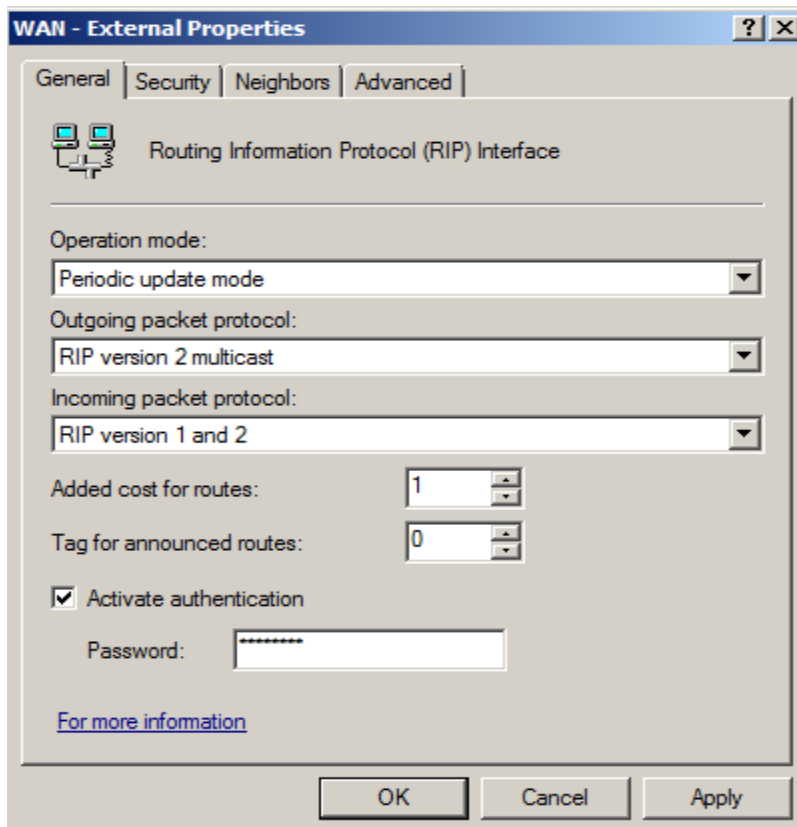
8. Check the **Activate authentication** check-box, type **password** and click OK.



9. Right-click on **WAN – External** and go to **Properties**.

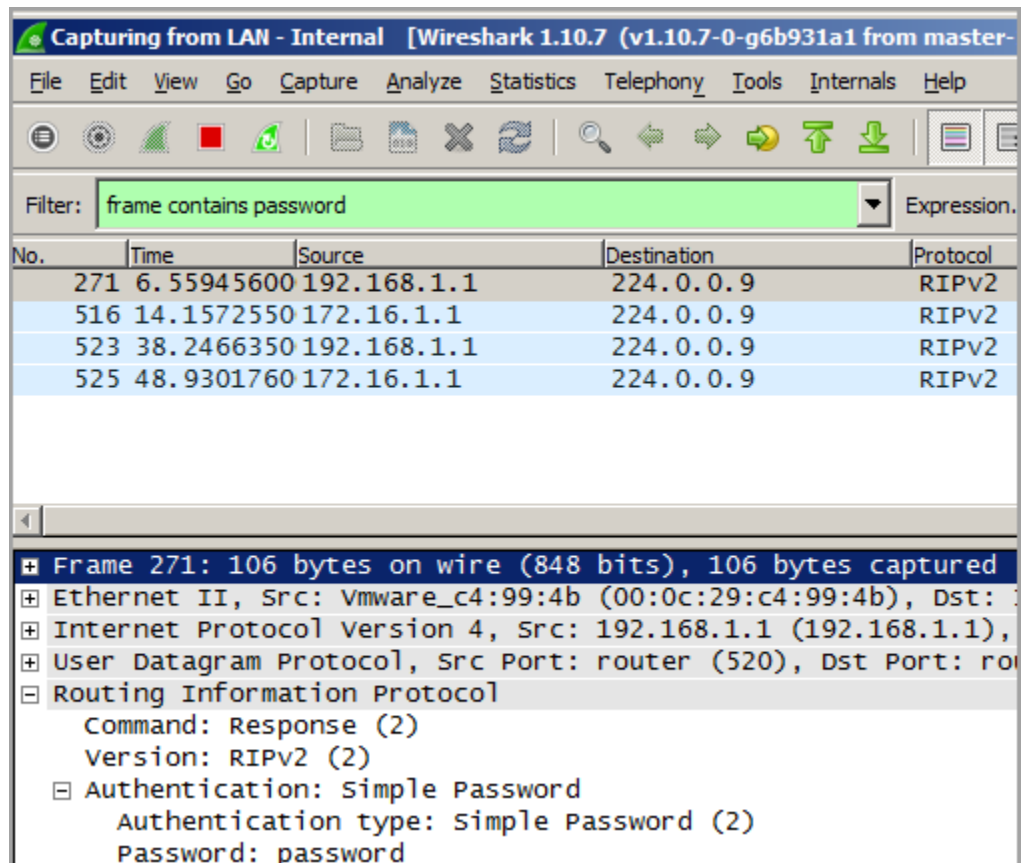


10. Check the **Activate authentication** check box, type **password** and click OK.



11. Return to the Wireshark window running on the sniffer machine. Type **frame contains password** in the filter pane and click Apply. Expand **Routing Information Protocol**, and then expand **Authentication**. You will see the password in clear text.

Microsoft's implementation of RIPv2 does not encrypt the password. However, Cisco's version does. This does illustrate the danger of sniffers on a network.



12. Open a command prompt on your local computer. On the command line, type your first and last names. Take a screenshot that contains your full name and the output window generated at above Step 11.

## 3.2 Conclusion

Routing updates sent over a network over broadcast and multicast can be seen by an attacker using a sniffer. It is a good idea to use Cisco implementation of RIP version 2, because the password sent between the routers will be encrypted. With Microsoft's implementation of RIPv2, which is more limited, the password is sent in cleartext.

## 3.3 Discussion Questions

1. What are the dangers that sniffers can pose on a network?
2. If a Microsoft implementation of RIPv2 is secured, is the password cleartext?
3. If a Cisco implementation of RIPv2 is secured, is the password cleartext?
4. What does Cisco do to the password for RIPv2 so it is not discovered in cleartext?



## References

1. RIP:  
[http://en.wikipedia.org/wiki/Routing\\_Information\\_Protocol](http://en.wikipedia.org/wiki/Routing_Information_Protocol)
2. RIPv2:  
<http://blog.pluralsight.com/cisco-how-to-configure-rip-2>
3. Configuring RIP:  
[http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/configuration/guide/config/route\\_rip.html](http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/configuration/guide/config/route_rip.html)
4. Routing and Remote Access on Windows Server 2008:  
[http://technet.microsoft.com/en-us/library/cc770798\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc770798(v=ws.10).aspx)
5. Command Line Linux:  
<http://linuxcommand.org/>

