Lab Objective

Configuring a VPN Server

Lab Procedures

1. On Server01, on the Task bar, right-click the Network and Sharing Center icon and click Open Network and Sharing Center.

2. Click Change adapter settings.

3. Right-click Ethernet and click Rename. Change the name to Internal and press the Enter key.

4. Right-click Ethernet 2 and click Rename. Change the name to External and press the Enter key. When done, the Network Connections should look similar to Figure 10-1.

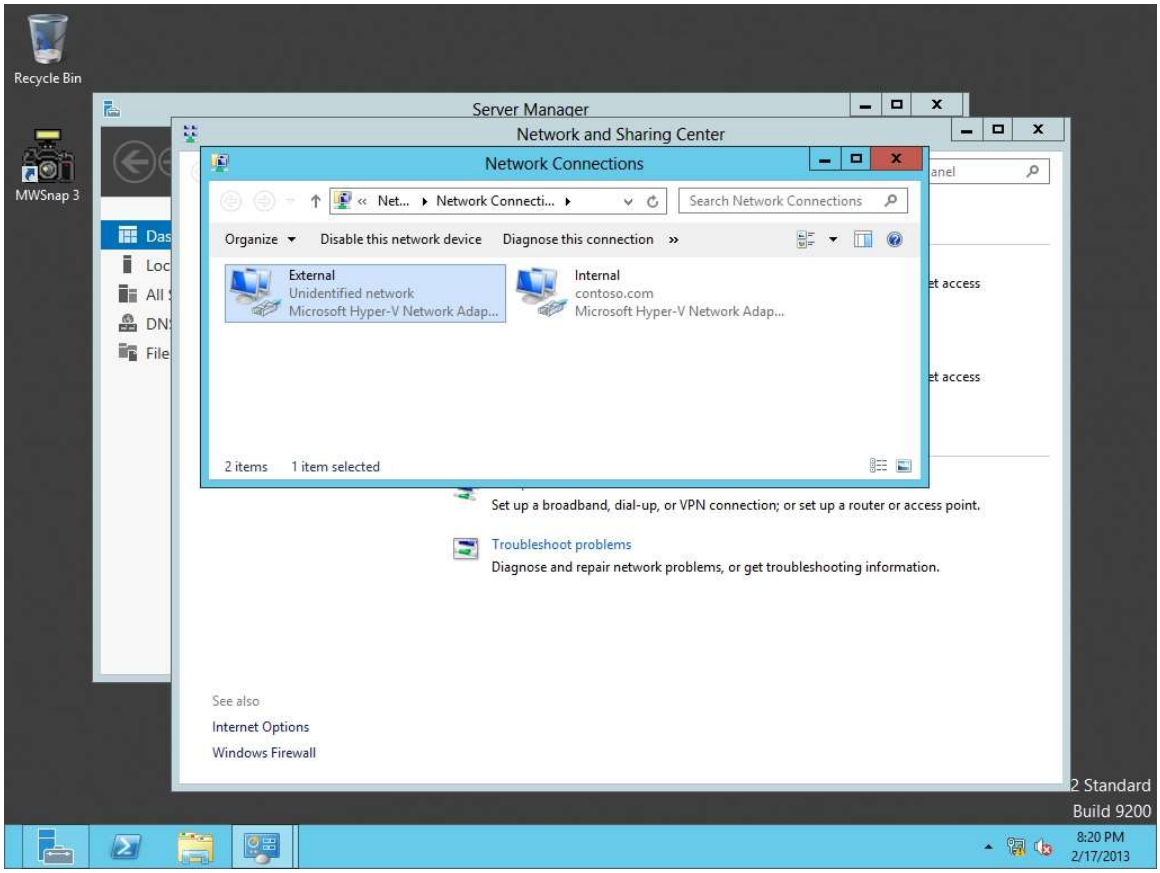

Figure 10-1
Viewing network connections

5. Right-click External and click Properties.

6. When the External Properties dialog box opens, double-click *Internet Protocol Version 4 (TCP/IPv4)*.

7. Click Use the following options and specify the following:

   IP address: **192.168.2.1**

   Subnet mask: **255.255.255.0**

   Click OK. If it says the DNS server list is empty, click OK.

8. Click OK to close the External Properties dialog box.

9. Close Network Connections.

10. On Server01, Server Manager, click Tools > Routing and Remote Access. The Routing and Remote Access console opens as shown in Figure 10-2.

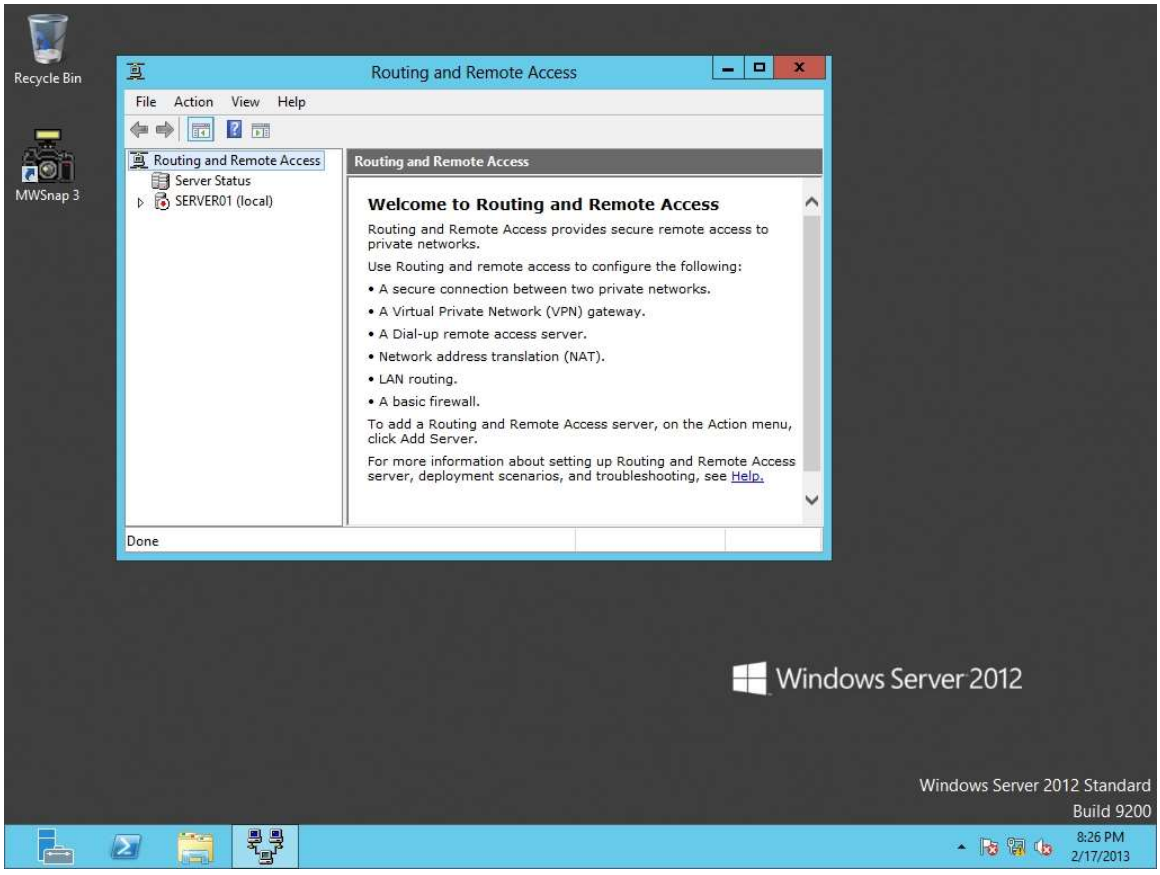

Figure 10-2
Opening the Routing and Remote Access console

11. Right-click Server01 and select *Configure and Enable Routing and Remote Access*. The Routing and Remote Access Server Setup Wizard opens.

12. On the Welcome page, click Next.

13. On the Configuration page, select *Virtual private network (VPN) access and NAT* (as shown in Figure 10-3) and click Next.

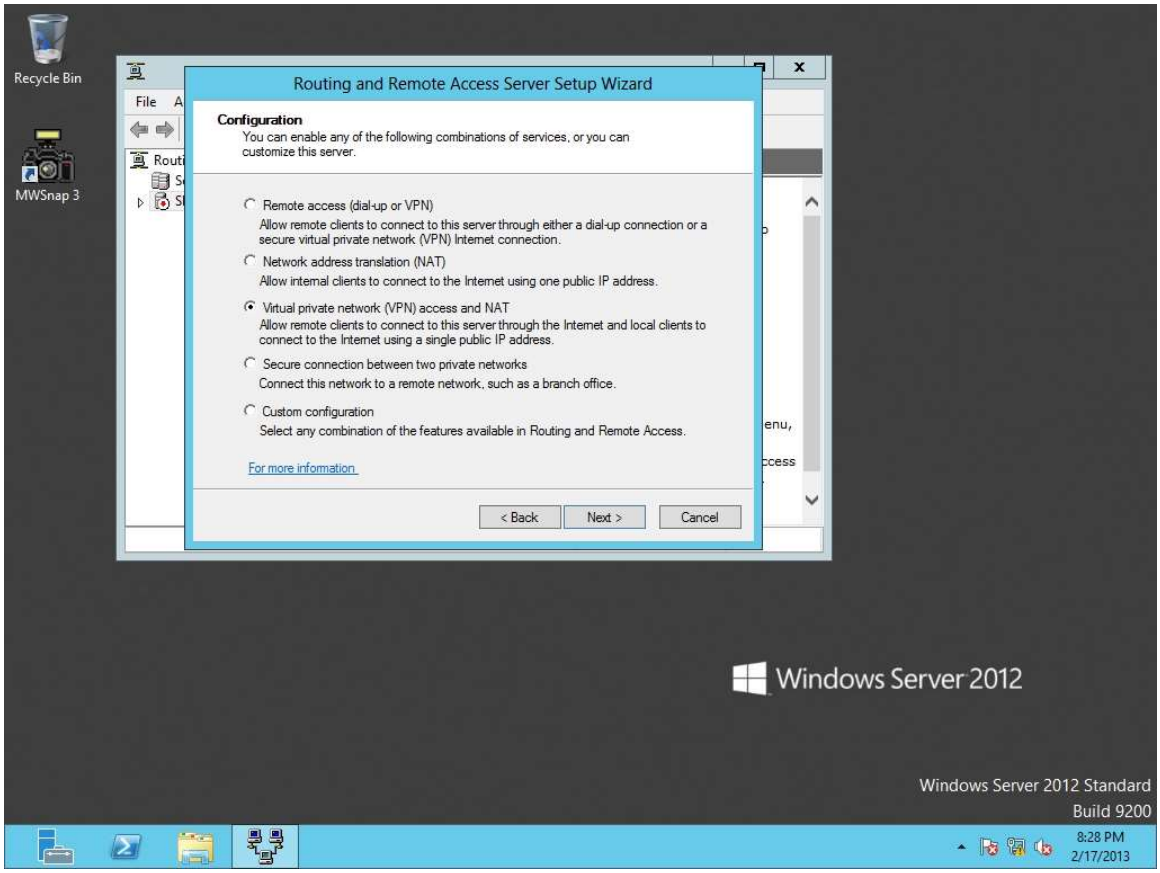

Figure 10-3
Specifying the Routing and Remote Access configuration

14. On the VPN Connection page, select External and click Next.

15. On the IP Address Assignment page, click *From a specified range of addresses* and click Next.

16. On the Address Range Assignment page, click New.

17. When the New IPv4 Address Range dialog box opens, specify the Start IP address as **192.168.1.40** and the End IP address as **192.168.1.45**. Click OK.

18. Back on the Address Range Assignment page, click Next.

19. On the *Managing Multiple Remote Access Servers* page, click Next.

20. On the Completing the Routing and Remote Access Server Setup Wizard page, click Finish.

21. When prompted to open a port of Routing and Remote access in the Windows Firewall, click OK.

22. When it asks to support the relaying of DHCP messages from remote access clients message, click OK.

23. Take a screen shot of the Routing and Remote Access window by pressing Alt+Prt Scr and then paste it into your Lab10_worksheet file in the page provided by pressing Ctrl+V.

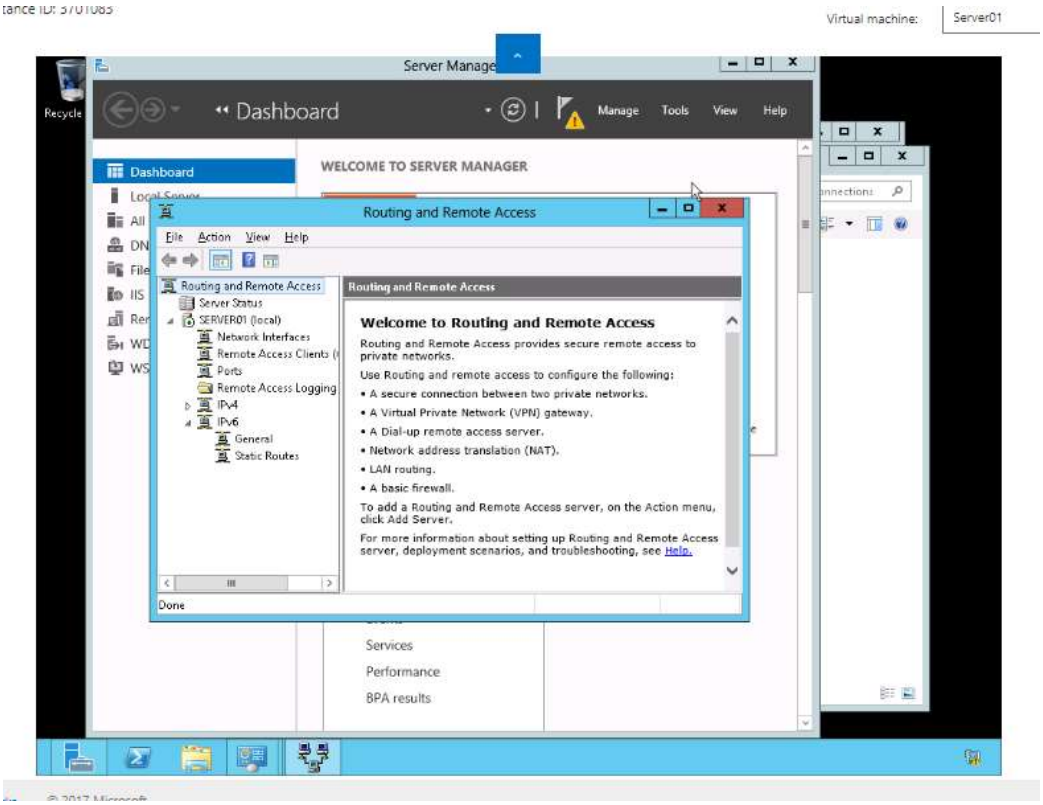

Figure 1 A screen shot of the Routing and Remote Access window

24. After RRAS starts, click the Start button, and click Administrative Tools. When theAdministrative Tools opens, double-click *Windows Firewall with Advanced Security*.

25. When Windows Firewall with Advanced Security opens, under Actions, click Properties.

26. When the *Windows Firewall with Advanced Security on Local Computer* dialog box opens, change the Firewall state to Off.

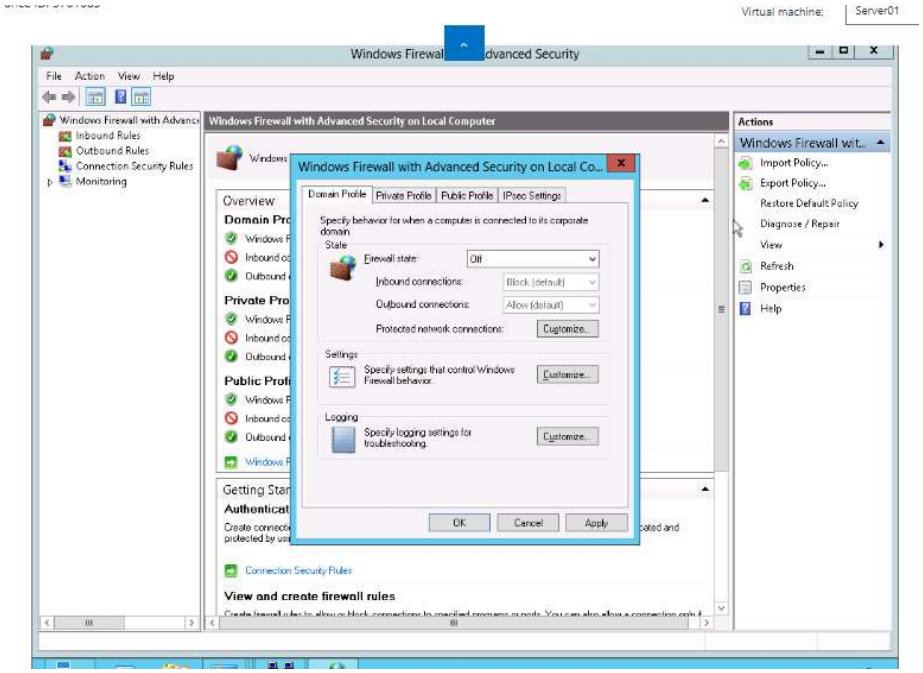

Figure 2 When the Windows Firewall with Advanced Security on Local Computer dialog box opens, change the Firewall state to Off.

27. Change the Firewall state to Off in the Private profile and Public Profile tabs.

28. Click OK to close the *Windows Firewall with Advanced Security on Local Computer* dialog box.

29. Close *Windows Firewall with Advanced Security* and *Administrative Tools*.

30. Right-click Server01 in Routing and Remote Access, and click Properties.

Question 1	*Which tab would you use to specify a preshared key for RRAS?* *Security*

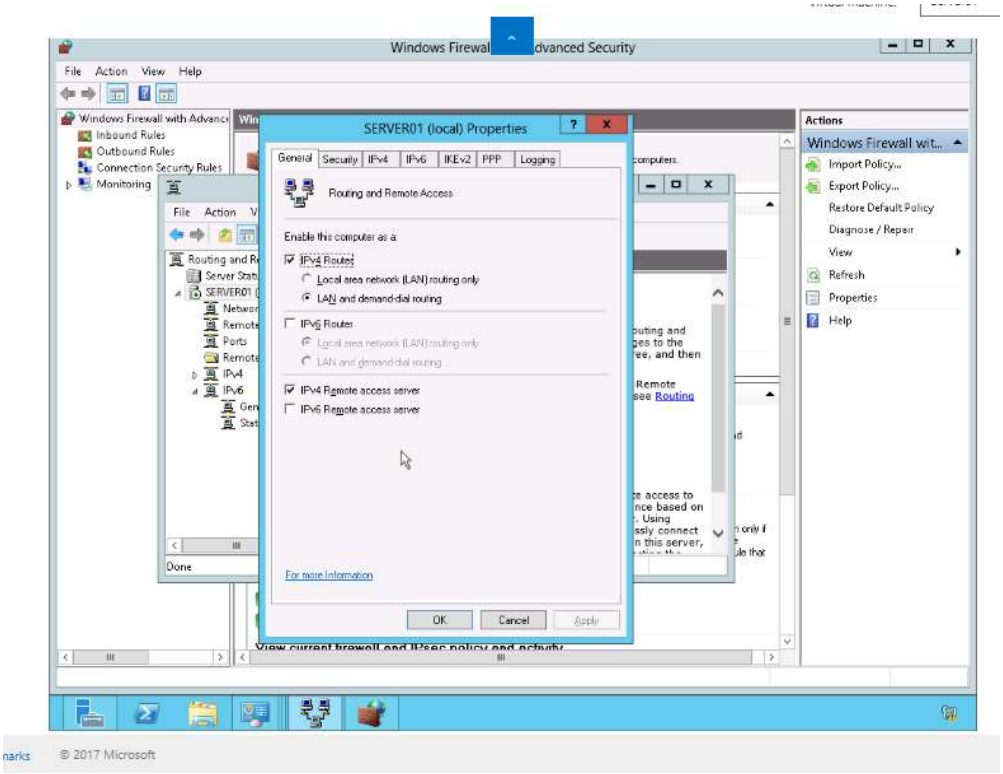

Figure 3 Right-click Server01 in Routing and Remote Access, and click Properties

Question 2	*Which VPN method requires a digital ceritificate to provide a SSL connection?* *Use HTTP (See figure below)*

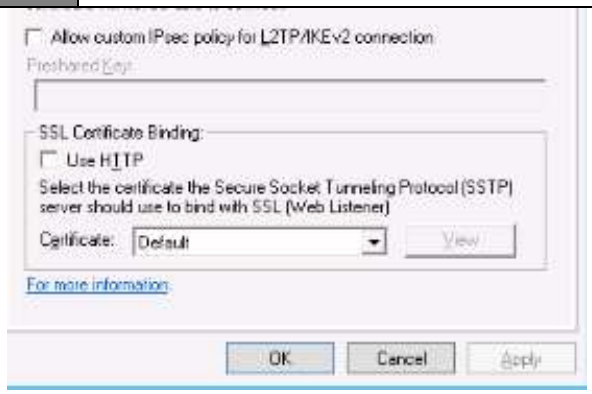

Figure 4 VPN method requires a digital certificate

31. Click OK to close the Server01 (local) Properties dialog box.

32. Right-click Ports and click Properties. The Ports Properties dialog box opens.

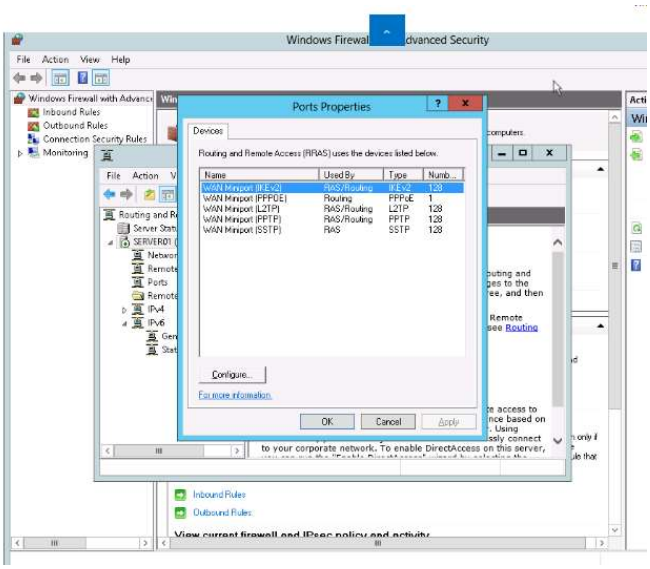

Figure 5 By default, one IKEv2 connection is available

33. Click OK to close the Ports Properties dialog box.

34. Log on to RWDC01 as Contoso**administrator**.

35. On Server Manager, from Tools, click *Active Directory Users and Computers*.

36. Expand contoso.com, if needed, and then click Users.

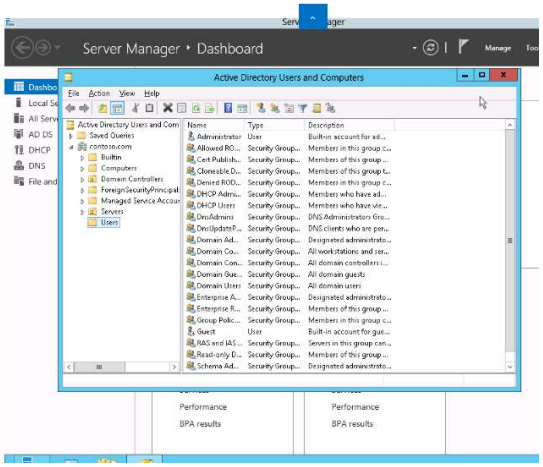

Figure 6 Expand contoso.com, if needed, and then click Users.

37. Double-click the Administrator account. The Administrator Properties dialog box opens.

38. Click the Dial-in tab.

Question 4	*What is the default setting for Network Access Permission?*

	Control access through NPS network policy

39. In the Network Access Permission section, click to select Allow access, as shown in Figure 10-4.

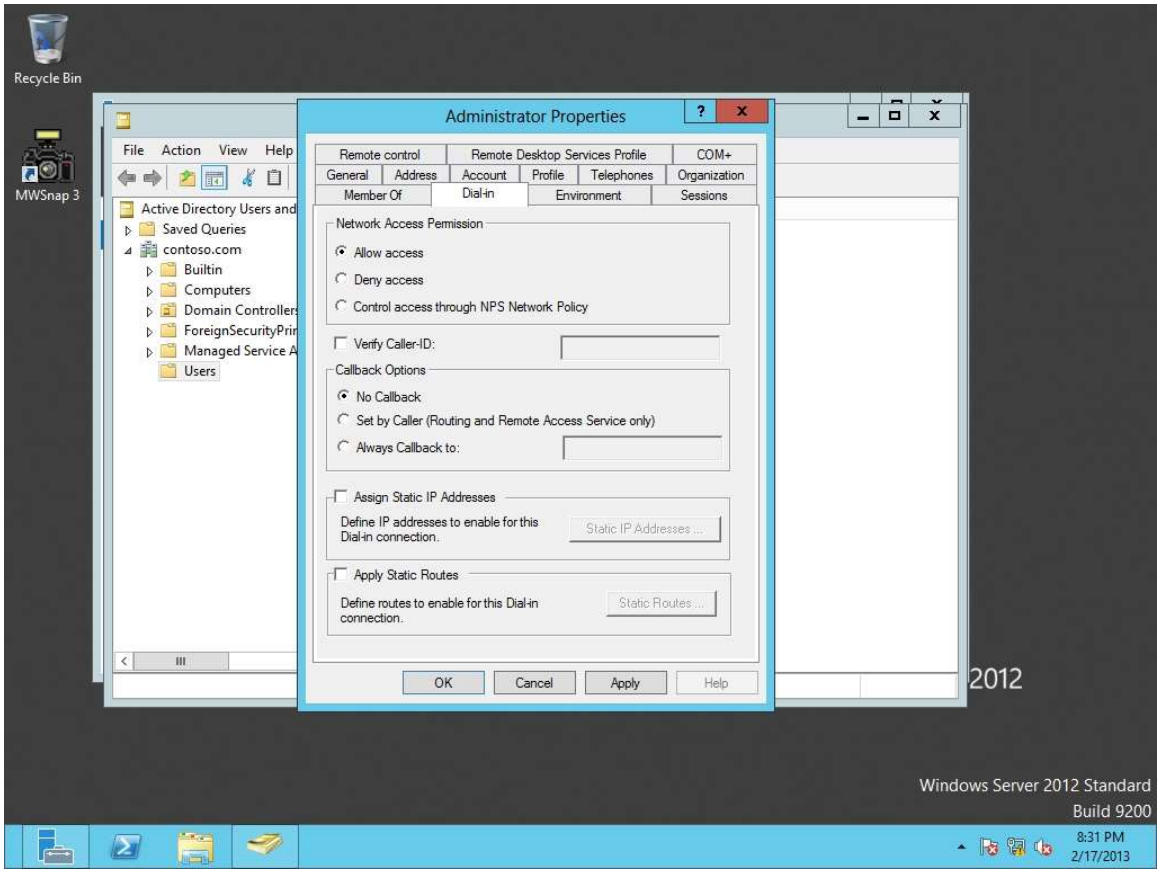

Figure 10-4
Allowing access to Dial-in for Administrator

40. Click OK to close the Administrator Properties dialog box.

41. Close Active Directory Users and Computers.

Lab Summary

Server01 will be the primary application server, which will be used for most applications. Routing and Remote Access Server supports VPN connections. Routing and Remote Access Server is able to serve as a VPN server and NAT router. It also supports two remote access: VPN and dial up.