10
WIRELESS, REMOTE, AND WIDE AREA NETWORKING

PROJECTS

Project 10.1	Understanding Key Concepts
Overview	Remote access and wide area networks (WANs) have been part of PC networking since its first days, based initially on technologies used to support remote mainframe technology. Wireless networking is a more recent, but not less important, addition to the networking mix.
	Part of preparing to support different networking options is understanding related terms. Each different networking configuration has its own related terms, many of which depend on the context in which they are used.
	During this project, you match various networking terms to the definitions and descriptions of how they are used.
Outcomes	After completing this project, you will know how to:
	▲ identify key terms and concepts related to TCP/IP
What you'll need	To complete this project, you will need:
	▲ the following worksheet
Completion time	20 minutes
Precautions	None

The worksheet includes a list of networking terms on the left and descriptions on the right. Match each term with the description that it most closely matches. You will *not* use all descriptions. Each description can be used only once.

___ PPP

A. Access method used on Wi-Fi networks. It is similar to the CSMA/CD used on Ethernet networks, except that it makes more of an effort to avoid collisions between transmitting devices

___ L2TP

B. Telephone network and infrastructure that includes the standard dial-up phone network

___ BRI

C. Circuit-switched network communication method that combines voice, video, and data communication

___ CSMA/CA

D. Protocol used for remote client connections over a variety of connection methods and supporting multiple network protocols

___ ISDN

E. Microsoft service that supports routing, remote access, and virtual private network (VPN) access

___	X.25	F. Packet-switched network standard communication method that provides improved performance compared to X.25, scalable up to 39 Gbps
___	T-carrier circuit	G. ANSI standard high-speed United States fiber-based communication network
___	SONET	H. Media access method in which a device must physically listen before transmitting
___	RRAS	I. Industry-standard VPN connection protocol
___	PSTN	J. ISDN connection device that acts like a hub for ISDN connections
___	Packet-switched network	K. Oldest packet-switched service in current use
___	NT1/NT2	L. Most common type of dedicated circuit service
___	DCF	M. Packet-switched network connection device
___	PAD	N. Cloud architecture carrier network using fixed-rate connection plus per packet charges to determine charges
		O. Transmission method that transmits data faster than X.25, but slower than ATM, but does not include any error control
		P. ISDN configuration that has two B channels and one D channel

Project 10.2	Understanding Wireless Technologies
Overview	Wireless networking is now the preferred network topology in several networking scenarios. Development of wireless networking technologies is moving more quickly than other technologies that relate to PC networking. As a result, if you aren't dealing with wireless networking now, you probably will be soon.
	One of the problems with a technology that is changing and expanding this quickly is simply keeping up with the current state of the technology. Another is understanding how to properly deploy wireless networking and how it impacts existing wired networks.
	During this project, you will review various wireless technologies and some important considerations related to wireless access point (WAP) configuration.

Outcomes	After completing this project, you will know how to: ▲ identify wireless standards and their use ▲ configure wireless support
What you'll need	To complete this project, you will need: ▲ the following worksheet
Completion time	30 minutes
Precautions	None

■ Part A: Wireless Transmission Standards

This worksheet lists commonly used 802.x wireless standards. Match each standard to its best description. You will use all of the descriptions.

___ 802.11a

A. Fixed WiMAX, sometimes used for MAN connections or to connect public Wi-Fi WAPs to a central point

___ 802.11b

B. Emerging standard that uses both 2.4- and 5-GHz ranges and is expected to support speeds up to 240 Mbps

___ 802.11g

C. Standard that operates in the 5-GHz range, but not commonly used in PC networking

___ 802.11n

D. Mobile WiMAX, designed as an alternative networking standard for cell phones and computer hardware

___ 802.16d

E. Current and most commonly used Wi-Fi networking standard

___ 802.16e

F. Original Wi-Fi networking standard

■ Part B: Wireless network configuration

You are configuring a network that will include wireless device support. The network design calls for 150 devices, 100 of which will be wireless devices. You need to allow for a potential 10% growth. The majority of the devices receive their TCP/IP configuration information automatically. The wired and wireless devices should all be part of the same network segment.

You decide to bring in three high-speed Internet lines to provide connectivity for both wired and wireless devices. You plan to install three WAPs that also act as routers and include NAT functionality to support both wireless clients and wired Internet access. DHCP service support is built into the WAPs and enabled by default. DHCP provides all general IP configuration parameters for clients leasing addresses. The WAPs support configurable private Class C addresses for intranet addresses. You can change the address range, but not the Class C address network address.

Answer the following questions related to wireless network configuration and interaction between wired and wireless networking.

1. What will act as the TCP/IP default gateway for wireless clients in this configuration?

   _____

2. What will act as the TCP/IP default gateway for wired clients in this configuration?

   _____

3. WAPs receive Internet IP addressing parameters from the Internet Service Provider (ISP) through DHCP. What are the concerns when configuring local IP address information for the WAPs?

   _____

4. The network will have ten wired servers that require static IP addresses. What guidelines should you consider when assigning IP address and subnet information?

   _____

   _____

5. For servers that need Internet access, what should you use as the default gateway?

   _____

6. How can you find values to use for Internet DNS servers?

   _____

   _____

7. Each WAP has four RJ-45 connectors for wired clients. How can you configure the network to support the necessary number of wired clients?

   _____

   _____

8. How can you prevent DHCP on the three WAPs from trying to assign duplicate addresses?

   _____

■ Part C: Wireless Access Point Configuration

This part uses the same network scenario as Part B. You are answering specific questions about DCHP and network configuration, but in the context of WAP configuration. Many of the issues discussed here would also apply to the DCHP service running on a wired server. Using the configuration screen shown in Figure 10-1, answer the following questions about WAP configuration:

Figure 10-1: WAP configuration settings

1. The Router IP settings let you set the last two dotted decimal values and select the subnet mask from the standard subnet masks supported for Class C networks. Will it be necessary to change these configuration settings, and if so, how?

_____

_____

_____

2. Configuring the Router IP and DHCP settings, what is the potential problem if you change both of the last two dotted decimal values in the Router IP address?

_____

_____

_____

_____

3. What wireless standard or standards will this WAP support?

_____

_____

4. How would you need to change the starting IP address and maximum DHCP users, if at all?

_____

_____

_____

Project 10.3	Setting up Remote Access
Overview	Windows Server 2008 Routing and Remote Access (RRAS) allows you to configure a server to support dial-up and VPN remote access connections. RRAS supports both PPTP and L2TP VPN connections. The same server can support multiple clients; however, a separate dial-up modem is needed for each dial-up client.
	Although RRAS (Routing and Remote Access Service) is installed by default when you install Windows Server 2008, you still need to enable the service in order to configure and use it. To do so, click the **Start** button from the Taskbar, then **Control Panel**, then **Administrative Tools**, and then click on **Routing and Remote Access** to open the RRAS console. Right-click the server in the left pane and choose **Configure and Enable Routing and Remote Access** to start the RRAS Setup Wizard. You can use the wizard to automatically configure RRAS for specific applications or configure the service manually.
	Under normal circumstances, you would normally not enable RRAS on a domain controller. Doing so would be a potential security hole. For the purposes of this lab and because of your limited number of computers, we will make an exception.
	In this project, you will enable RRAS on a computer running Windows Server 2008 and view its configuration.
Outcomes	After completing this project, you will know how to:
	▲ enable RRAS
	▲ configure dial-up and VPN client support

What you'll need	To complete this project, you will need: ▲ a computer running Windows Server 2008
Completion time	20 minutes
Precautions	The instructions in this project assume you are working on a two-node network with one computer running Windows 7 Professional or Windows 7 Enterprise and one computer running Windows Server 2008. If working on an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the instructions.

■ Part A: Enable Routing and Remote Access

In this part of the project, you will enable RRAS for both dial-up and VPN connections. You will assign IP addresses from a static pool. You will need to be logged on to the computer running Windows Server 2008 as Administrator at the beginning of this part of the project.

Steps 1 through 4 are specific to a wired connection, but may be adapted for wireless connections.

1. Open the **Start** menu, select **Control Panel** as in Figure 10-2, select **Network And Sharing Center** as in Figure 10-3, Manage Network Connections, and then select **Local Area Connection** as in Figure 10-4.

Figure 10-2: Control Panel

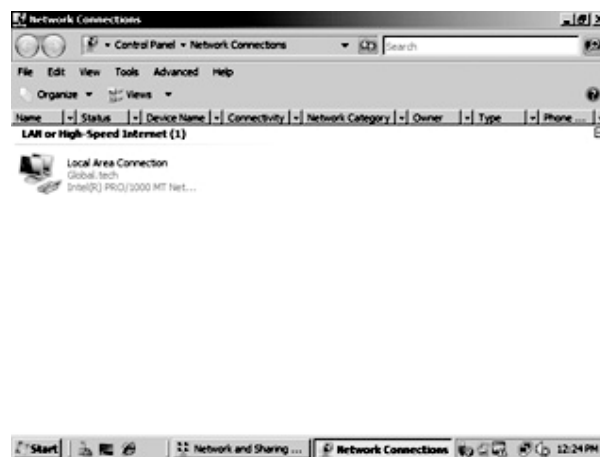**Figure 10-3: Network and Sharing Center**

Figure 10-4: Network Connections

2. Right-click *Properties* (see Figure 10-5) to display the **Local Area Connection Properties** dialog box (refer to Figure 10-6).
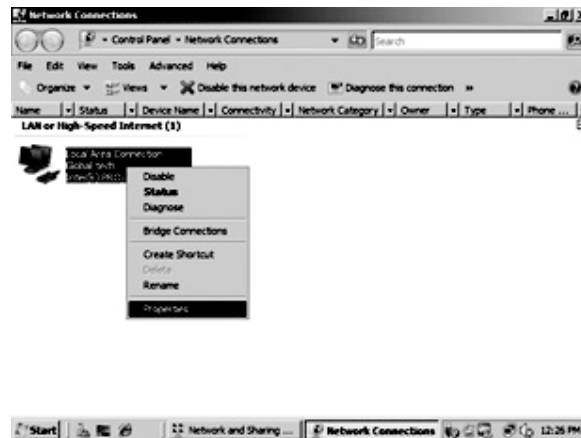

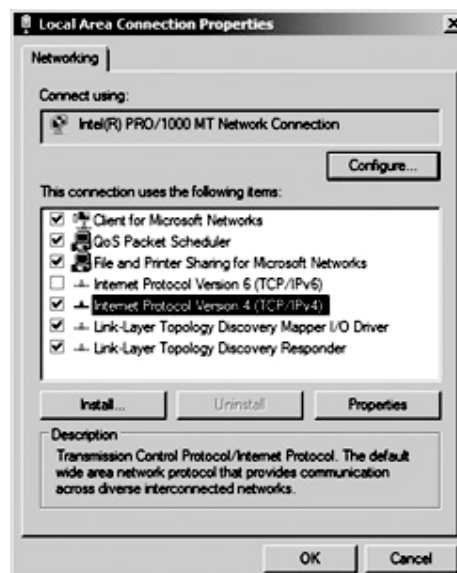**Figure 10-5: Local Area Connection Properties**

Figure 10-6: Local Area Connection Properties

You will get a warning window as Server 2008 has much higher security than earlier versions. Click *Continue.*

3. Choose **Internet Protocol Version 4** and **Properties**, to confirm that you have the correct static IP address assigned to the Server as in Figure 10-7.

Figure 10-7: Internet Protocol Version 4 Properties

Click *Close* to close the **Local Area Connection Properties** dialog box and then click *Close* to close the **Network Connections** window.

4. Open the **Start** menu, point to **All Programs** and then to **Administrative Tools**, **Server Manager**. Choose *Roles* in the left-hand window as in Figure 10-8.

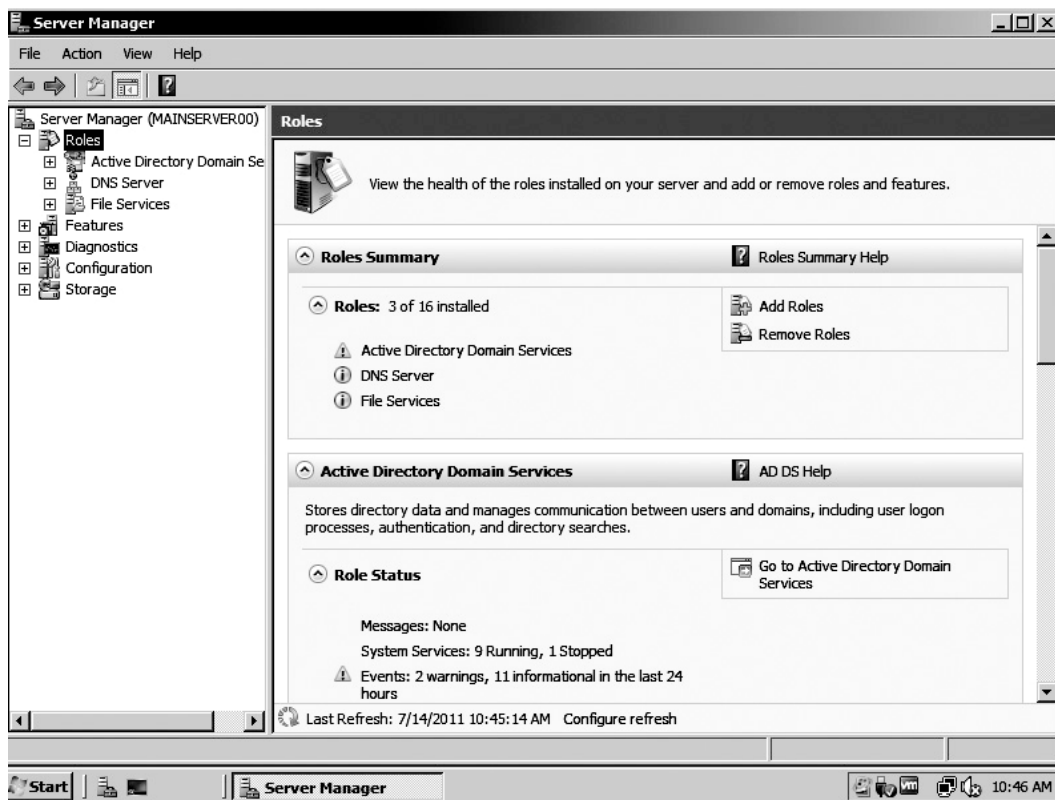**Figure 10-8: Administration tools/Server Manager**

5. Add Roles as in Figure 10-9.

Figure 10-9: Add Roles

6. Choose **Network Policies and Access Services**, then choose *Next* as in Figure 10-10. Note the information provided about security and secure networks like Figure 10-11 shows.

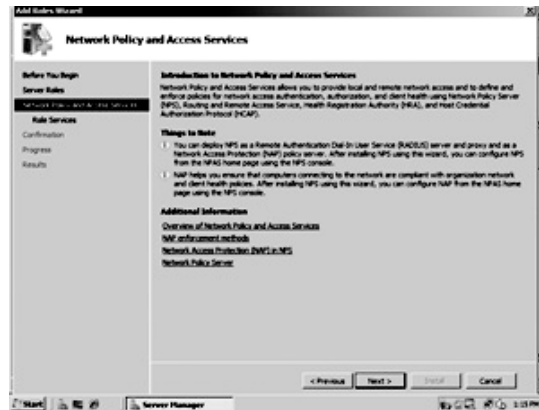**Figure 10-10: Network Policy and Access Services**

Figure 10-11: Security warning

7. Choose **Routing and Remote** access and *Next* as in Figure 10-12.

Figure 10-12: Routing and Remote Access

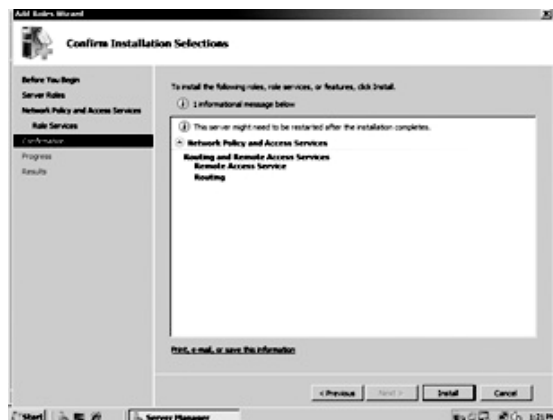8. Take note of the warning and Install like Figure 10-13 shows.

Figure 10-13: Routing and Remote Access Install

9. Close when complete. Figure 10-14 shows what the successful installation looks like.
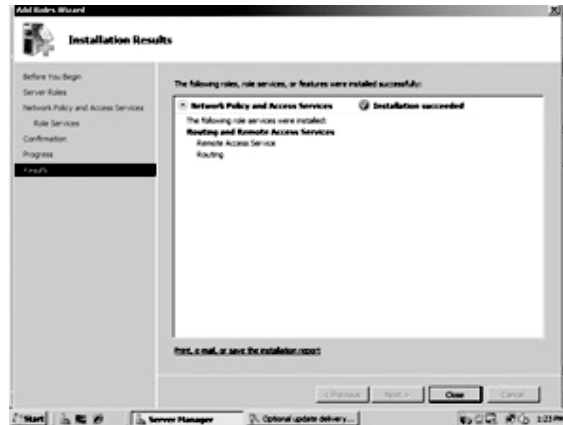

Figure 10-14: RRAS Installation Successful

Part B: Configuring Routing and Remote Access

1. Closing the RRAS installation window returns you to the Server Manager window.
2. Note the little Red down arrow indicating that the service is not currently running. Right-click on **Routing and Remote Access** and choose **Configure and Enable routing and Remote Access** from the drop down menu as in Figure 10-15.

Figure 10-15: Configure and Enable routing and Remote Access

3. Follow the wizard as in Figure 10-16 and select **Remote Access** (dial-up or VPN), and click *Next* as in Figure 10-17. ***Note:*** If you do not have two network interface devices available, you will have to choose **Custom Configuration**.
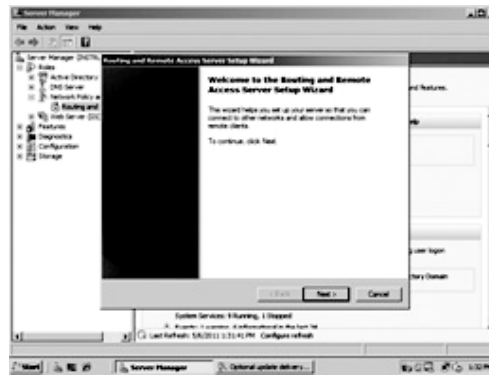

Figure 10-16: RRAS Setup Wizard

Figure 10-17: Select Remote Access(dial-up or VPN)

4. Select both the **VPN** and **Dial-up** radials, and click *Next* as in Figure 10-18.
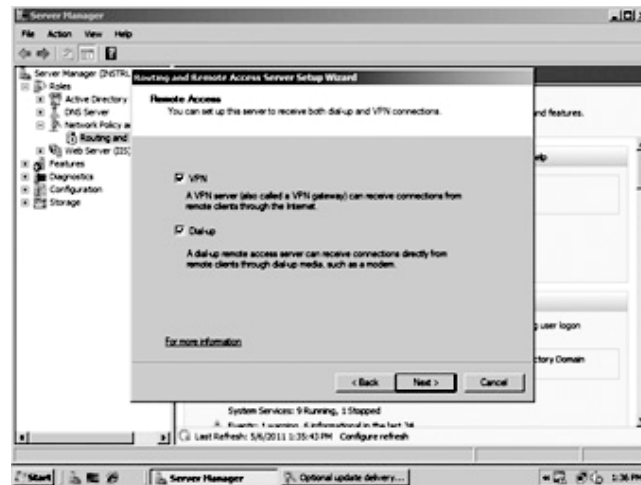
Figure 10-18: RRAS Setup Wizard

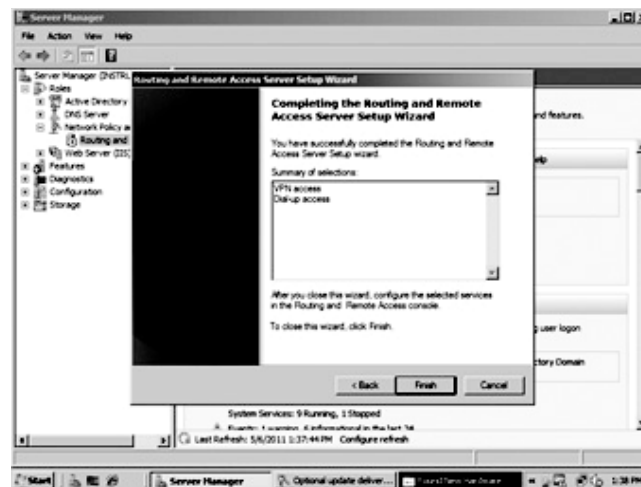5. Click *Finish*. Congratulations! You have installed RRAS. See Figure 10-19.

Figure 10-19: RRAS Setup Wizard Complete

Part C: Starting Routing and Remote Access Service

1. You can manage RRAS via **Start/Administration Tools/Routing and Remote Access**. See Figures 10-20 and 10-21.

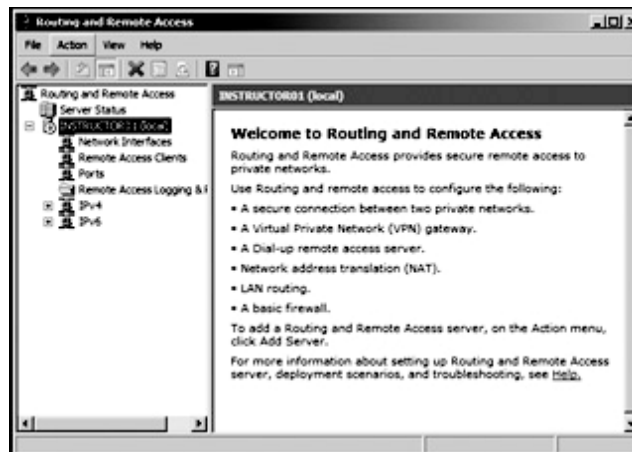

Figure 10-20: Open Manage RRAS

Figure 10-21: Manage RRAS Window

2. From the RRAS console, Choose **Actions/All Tasks** and **Start** as in Figure 10-22.
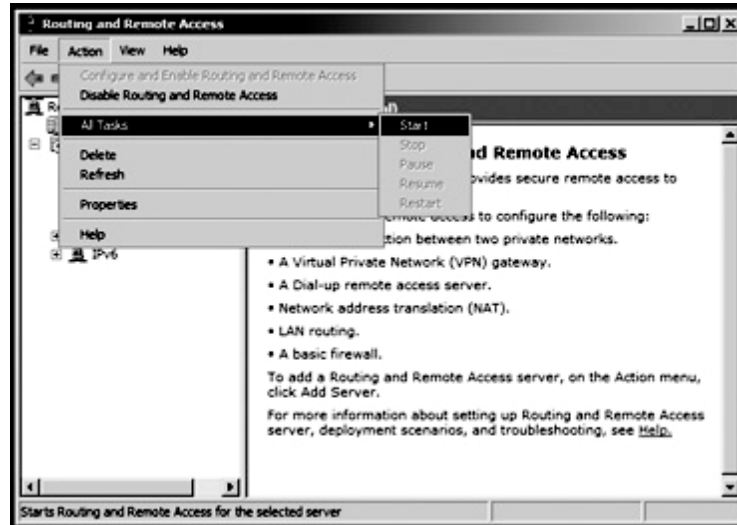

Figure 10-22: Start RRAS Service

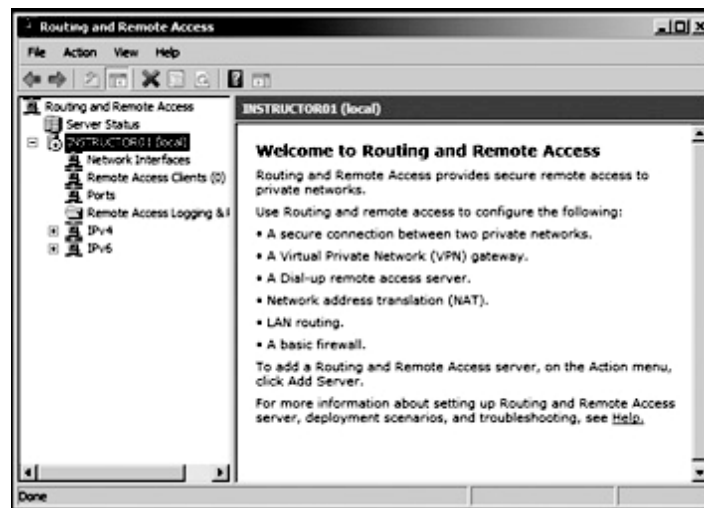3. You are now running RRAS. See Figure 10-23.

Figure 10-23: RRAS Service Welcome Screen

1. What benefit would you gain by using RADIUS?

_____

2. How does the **Routing and Remote Access** console visually indicate that the service is running?

_____

Project 10.4	Configuring a Dial-up Client
Overview	Windows 7 Professional or Windows 7 Enterprise can be configured to support both incoming and outgoing dial-up connections. You will want to be cautious when configuring an incoming dial-up connection because it is an entry point to your computer from anywhere with a phone line. This is particularly true if your computer is connected to a network.
	Part of the configuration process is configuring a network user account to enable dial-up access for that user. Only those users who need for remote access should be enabled. Each user for whom you allow remote access is a potential security hole if someone else gets the account information.
	In this project, you will configure a dial-up connection. You will not be able to test it unless you have a modem and another computer with a modem.
Outcomes	After completing this project, you will know how to:
	▲ configure a dial-up connection on Windows XP Professional
	▲ create and configure a user for dial-up access
What you'll need	To complete this project, you will need:
	▲ a domain controller running Windows Server 2008
	▲ a Windows 7 Professional or Windows 7 Enterprise domain member
Completion time	30 minutes
Precautions	The instructions in this project assume you are working on a two-node network with one computer running Windows 7 Professional or Windows 7 Enterprise and one computer running Windows Server 2008. If these computers are part of a larger classroom network, your instructor will provide you with alternate instructions for configuring network and domain parameters.
	If working on an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the instructions.

■ Part A: Set Dial-in Properties on a User Account

In this part of the project, you will create and configure a user account so that the user can dial in to the remote access server. You will perform this part of the project on the computer running Windows Server 2008.

1. Open the **Start** menu, point to **All Programs** and then to **Administrative Tools**, and select **Active Directory Users and Computers**.
2. If necessary, expand **BUSICORP.COM**.

3. Right-click **Users**, and select **New** and then **User** to display the **New Object-User** dialog box.

4. Complete the **New Object-User** dialog box, as shown in Figure 10-24, with user name **Ron User** and logon name **RUser**, and click *Next.*

Figure 10-24*: New user*

5. Enter **P@SSw0rd** in the **Password** and **Confirm password** fields, remove the check from **User must change password at next login**, and click *Next.*

6. Click *Finish.*

7. Select the **User OU**, locate and right-click **Ron User**, and select **Properties**.
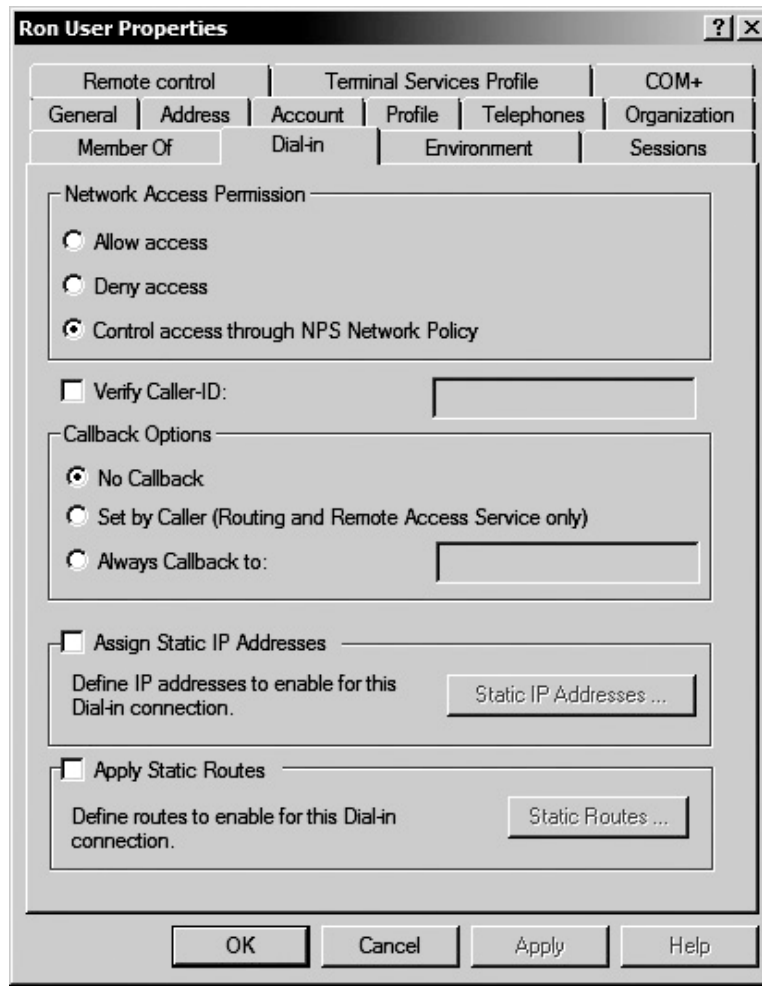
8. Display the **Dial-in** tab, as shown in Figure 10-25.

Figure 10-25: Dial-in tab

9. What is the default access setting?

_____

10. Select **Allow access**.
11. Click *OK* to close the **Properties** dialog box.
12. Close **Active Directory Users and Computers**.

■ Part B: Configure a Dial-up Connection

In this part of the project, you will view and configure a dial-up connection on the computer running Windows 7 Professional or Windows 7 Enterprise. You must perform this part of the project logged on as Administrator on the computer running Windows 7 Professional or Windows 7 Enterprise.

1. Open the **Start** menu and select **Control Panel/Network and Internet/View Network Status and Tasks**.

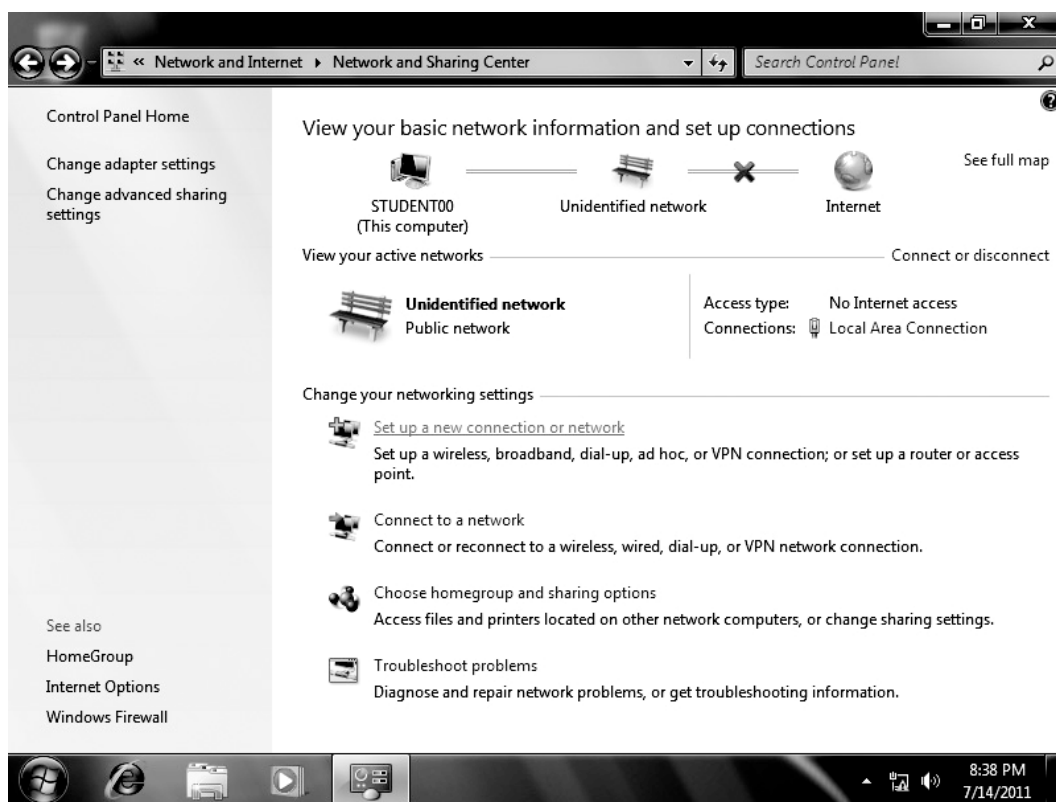2. Choose **Set up a new connection or network**, as shown in Figure 10-26.

Figure 10-26: Creating a new connection

3.   Choose **Set up a dial-up connection**, as shown in Figure 10-27.
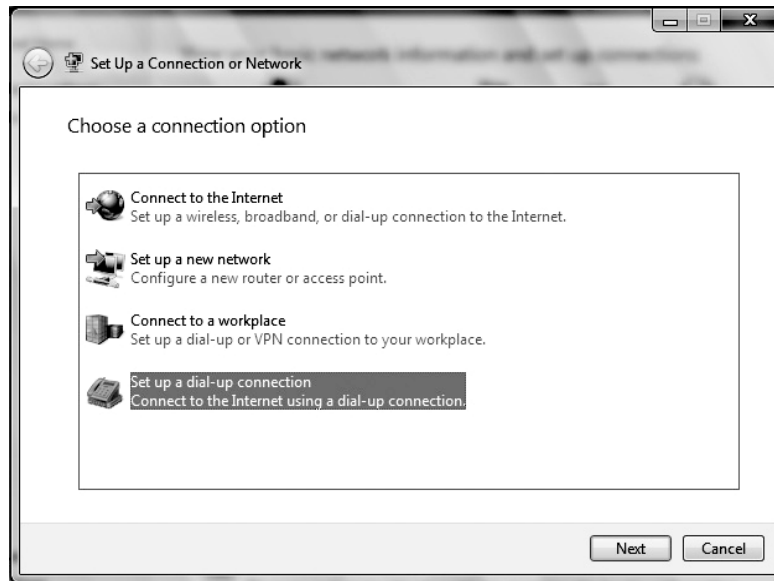

Figure 10-27: Set up a dial-up connection

4. If you have not set up a previous dial-up connection or configured phone and modem options, you will receive a notice; choose **Set up a conncetion anyway**, as shown in Figure 10-28. If you are not prompted for this information, continue with Step 7.
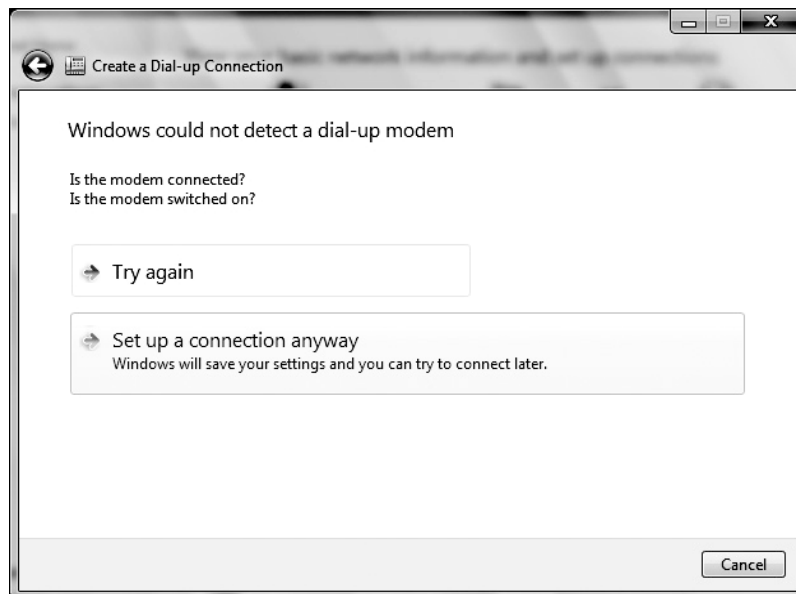

Figure 10-28: Set up a Connection

5. Fill in the required information. **18885551212** as the phone number, **Busicorp Office** as the name and **P@SSword** as the password, as shown in Figure 10-29.
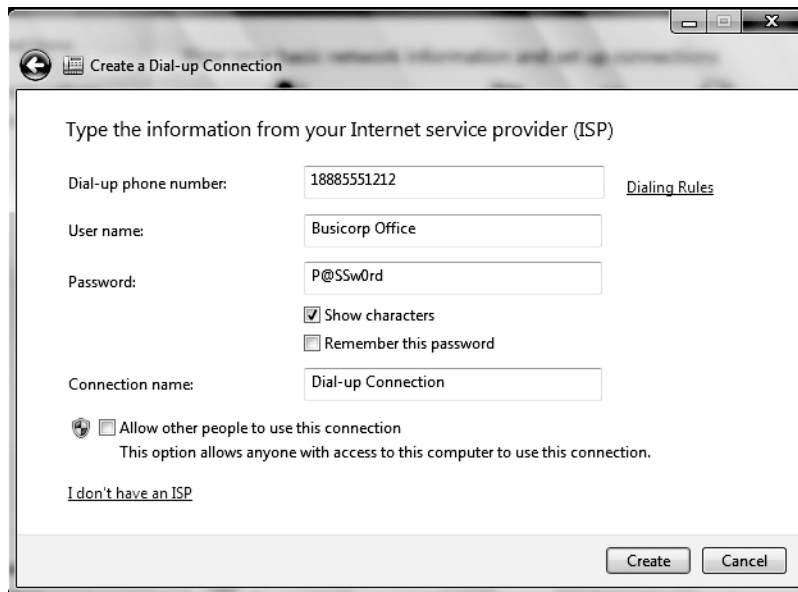
Figure 10-29: Create a Dial-up Connection

6. You will receive a notice that the connection is ready to use, so close this window.
7. Give an example of when you might select **My use only** instead.

_____

_____

8. Verify that your new connection is listed, as shown in Figure 10-30.
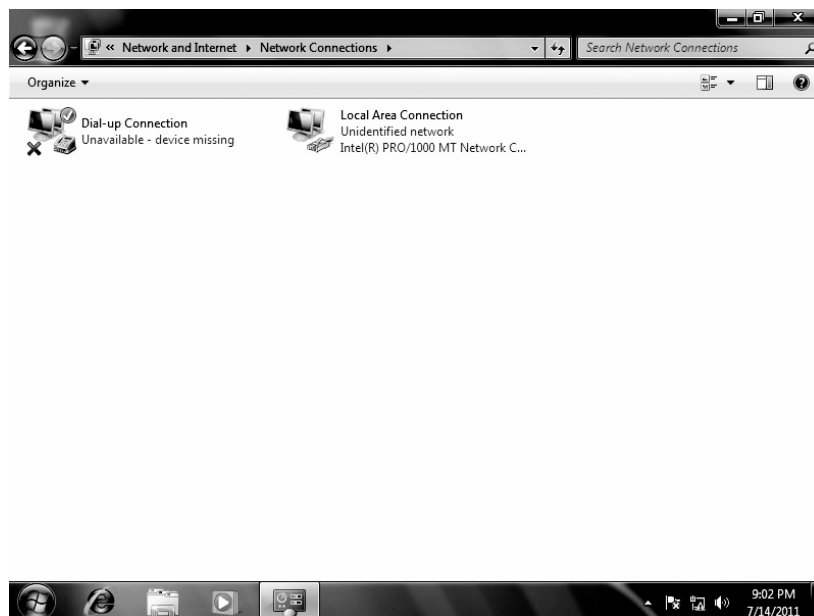

Figure 10-30: New dial-up connection

Note: If you do not have a modem installed, the dial-up connection will be created, but it will be marked as unavailable. Note the Red X.

17. Close **Network Connections**.

Project 10.5	Configuring a VPN Client
Overview	A remote user with a broadband Internet connection can be configured to connect to a LAN securely by tunneling through the Internet, which is known as a virtual private network (VPN). Windows 7 Professional or Windows 7 Enterprise supports both PPTP and L2TP/IPsec VPN connections. In this project, you will configure a VPN connection on the Windows 7 Professional or Windows 7 Enterprise computer.
Outcomes	After completing this project, you will know how to: ▲ configure a VPN connection ▲ connect using a VPN connection
What you'll need	To complete this project, you will need: ▲ domain controller running Windows Server 2008 ▲ domain member running Windows 7 Professional or Windows 7 Enterprise ▲ to have completed Project 8.3 and Project 8.4
Completion time	15 minutes
Precautions	The instructions in this project assume you are working on a two-node network with one computer running Windows7 Professional or Enterprise and one computer running Windows Server 2008. If these computers are part of a larger classroom network, your instructor will provide you with alternate instructions for configuring network and domain parameters. If working on an existing network, you must review the project steps with your network administrator. Your network administrator may need to make changes or additions to the instructions.

■ Part A: Create a VPN Connection

In this part of the project, you will create a VPN connection on the computer running Windows 7 Professional or Windows 7 Enterprise. You must be logged on as Administrator.

1. Open the **Start** menu and select **Control Panel/Network and Internet/View Network Status and Tasks**.

2. Choose **Set up a Connection or Network**.

3. In the **Set up a Connection or Network**, click **Connect to a workplace**. See Figure 10-31.
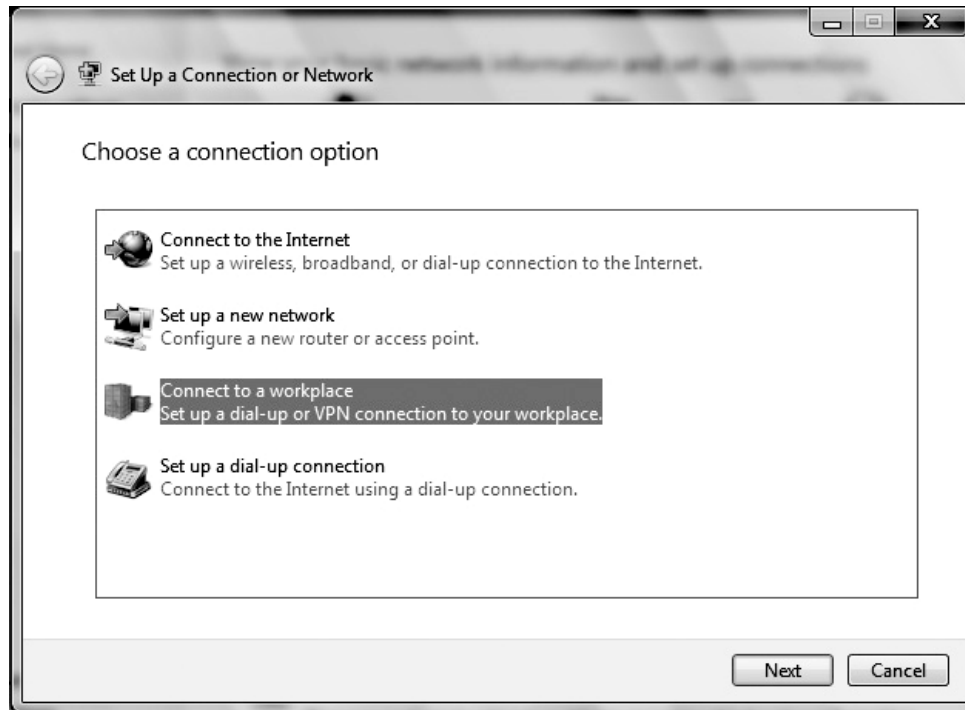
Figure 10-31: Connection Option

4. Choose **No**, **Create a new connection**, and **Next**.
5. Choose **Use My Internet connection (VPN)**. See Figure 10-32.

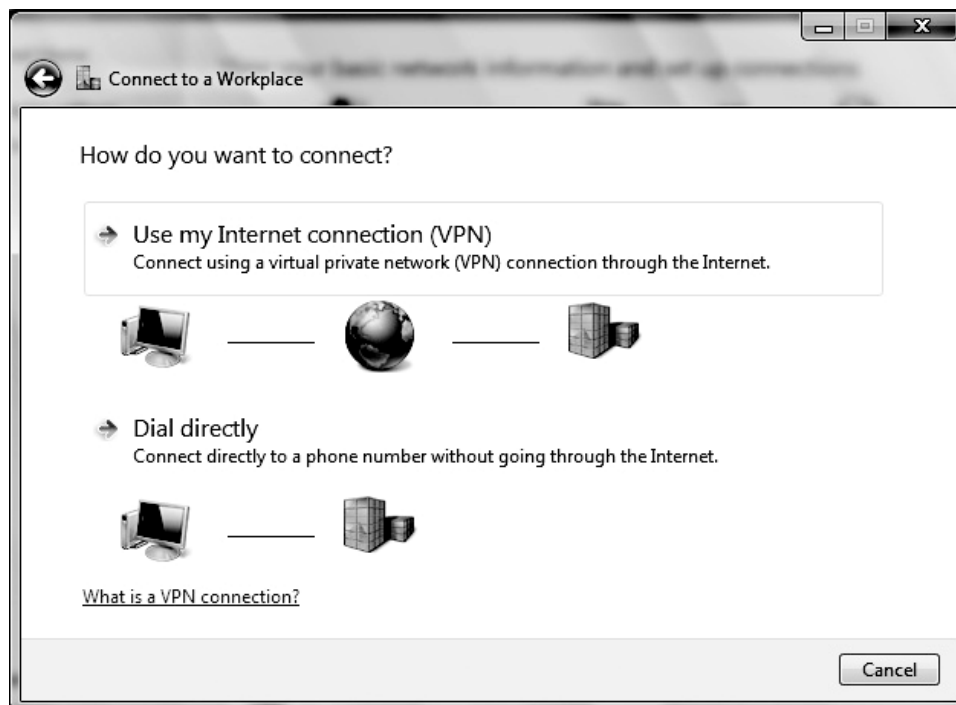**Figure 10-32: VPN option**

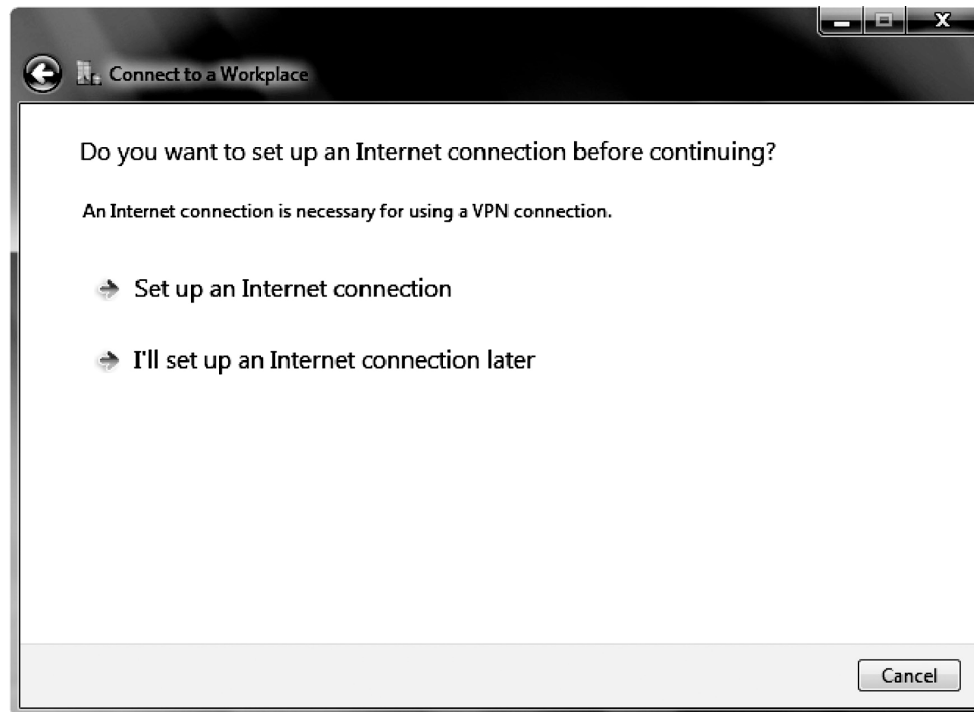6. Select **Set up an Internet connection** as in Figure 10-33.

Figure 10-33: Set up an Internet connection

7. Choose the **Broadband (PPPoE)** option as in Figure 10-34.

Figure 10-34: Connection type
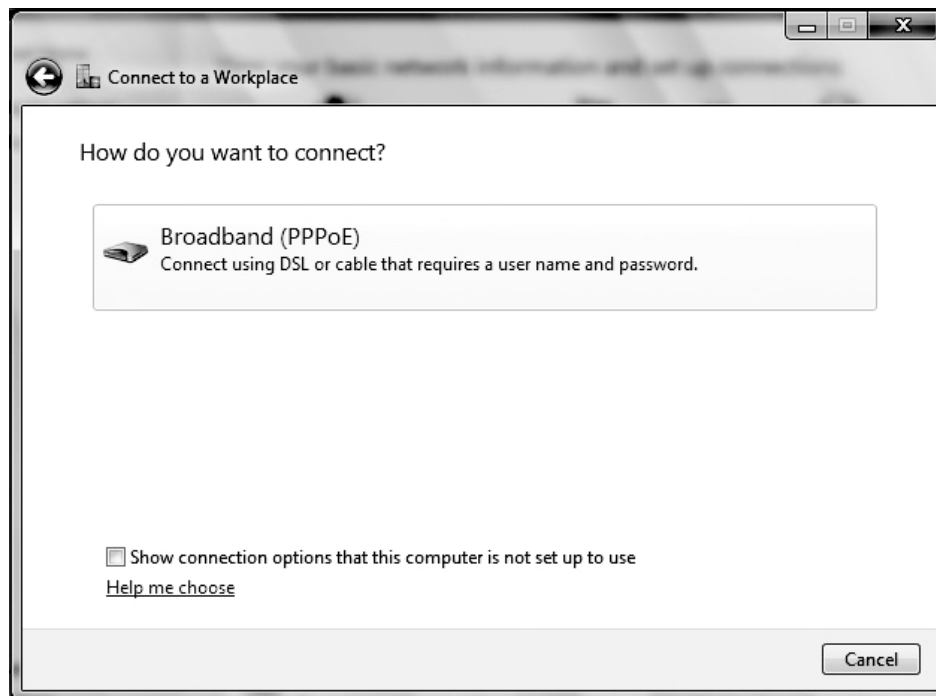
Fill in the appropriate information: **Busicorp via I-net** as the name and **P@SSw0rd** as the password leave the options unselected and click *Connect.*

8. Skip the attempt to connect via the miniport and close.
9. Verify that your new connection is listed from the Network and Internet panel, change **Adapter Settings** to see Figure 10-35.
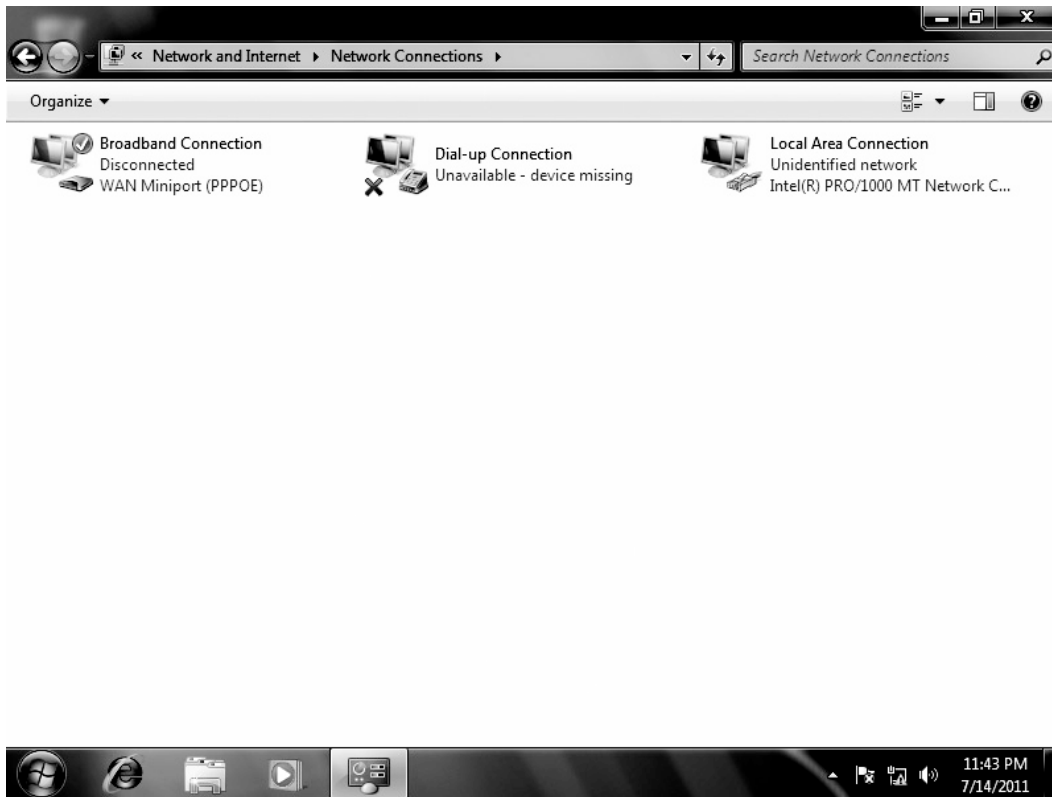

Figure 10-35: Network connections

10. In the **Connect Busicorp via I-net** dialog box, enter **adminstrator** as the **User name** and **P@SSw0rd** as the **Password**, as shown in Figure 10-36.

Figure 10-36: Connecting as administrator

11. What happens?

_____

_____

12. Why?

_____

_____

13. Click *Cancel.*

Project 10.6	Comparing WAN Requirements
Overview	An important part of WAN design is the type of connection you plan to use to connect the LANs. By classic definition, a LAN becomes a WAN as soon as data communications cross a public carrier.
	More companies are using the Internet as their WAN backbone, but this is far from the only connection option. Many established WANs continue to use other connection methods because they do a better job of meeting connection requirements, are more cost-effective, provide a known stable and secure connection, or any combination of the three.
	You will compare WAN connectivity options during this project.
Outcomes	After completing this project, you will know how to:
	▲ identify network categories
	▲ identify connection features
What you'll need	To complete this project, you will need:
	▲ the following worksheet
Completion time	20 minutes
Precautions	None

■ Part A: Carrier Networks

Table 10-1 lists the three WAN network categories. Place each WAN connection type under the appropriate category:

Carrier networks

T-carrier	ATM
PSTN	Frame Relay
X.25	SMDS
POTS	SONET
ISDN	

Table 10-1: WAN Network Categories

Circuit-switched	Dedicated-circuit	Packet-switched

■ Part B: Carrier service characteristics

Part B includes Table 10-2 with carrier service types and a list of statements that describe one or more of them. Check the boxes for the letters that best describe each access protocol. Each statement applies to at least one carrier. Some statements may apply to multiple carriers.

A. Based on a cloud architecture
B. Supports bus, ring, and mesh WAN topologies
C. Uses digital (B) channels and signaling (D) channels
D. Transmission speeds measured in multiples of OC-1, 51.84 Mbps
E. Network connections to the carrier are made using a PAD
F. Could be a dial-up connection to a home phone
G. Oldest packet-switched service still in use
H. Have a predictable route over public carriers
I. Fractional leased circuits are in 65-Kbps multiples
J. Based on published, generally accepted industry standards

Table 10-2: Carrier Service Types

Carrier type	A	B	C	D	E	F	G	H	I	J
PSTN										
ISDN										
SONET										
T-carrier										
ATM										
Frame Relay										
X.25										