Mastering Microsoft® Windows® 7 Administration
by William Panek and Tylor Wentworth

Chapter 11

Configuring Network Connectivity

To successfully establish network connectivity, you must have a properly installed and configured network interface card (NIC) and network protocol. The first step is to physically install and configure the network adapter that you will use and verify that Windows 7 recognizes the hardware. The installation of the hardware might go smoothly, but you need to be able to troubleshoot any issues that arise. Today, a big part of most networks is wireless connectivity that presents a whole new and interesting set of challenges. Not only does wireless connectivity present challenges in physical connectivity, but it requires a more thorough understanding of the physical connectivity to ensure a secure network.

The second step is to install, configure, and test the network protocol you have installed. In most home networks, network protocol connectivity seems automatic, but as an administrator, you need to understand the protocols like TCP/IPv4 as well as TCP/IPv6.

From here, you need to connect to other resources you have on your network, including shared resources on other machines, whether it's servers or other users' machines. You might also need to connect to printers, cameras, or other data-supplying devices needed for you or your users' productivity or pleasure. Setting up peer-to-peer networking is a big part of connecting to other devices as most users will want to be able to browse to the resources.

In this chapter, you'll learn how to:

- Set up hardware to provide network connectivity
- Connect to network devices
- Set up peer-to-peer networking
- Configure network protocols

Connecting Network Devices

NICs are hardware components used to connect computers or other devices to the network. NICs are responsible for providing the physical connection that recognizes the physical address of the device where they are installed.

PHYSICAL ADDRESSES VS. LOGICAL ADDRESSES

The Open System Interconnect (OSI) model defines the encapsulation technique that builds the basic data structure for data transport across an internetwork. The OSI model provides interoperability between hardware vendors, network protocols, and applications. The physical address is the OSI address, or for Ethernet technologies, the Media Access Control address (MAC address). This is not the IP address, which is the OSI Layer 3 or Network Layer address, also generically defined as the Logical Address. We'll discuss logical addressing later in this chapter in the section, ''Basics of IP Addressing and Configuration.''

The most common place you see network adapters installed are computers, but you also see NICs installed in network printers and specialized devices like intrusion detection systems (IDSs) and firewalls. We generically refer to the interface between our network devices and the software components of the machines as network adapters. Network adapters do not need to be separate cards; they can be built in as in the case of most PCs today or other network-ready devices such as network cameras or network media players. These adapters (and all other hardware devices) need a driver to communicate with the Windows 7 operating system.

Installing a Network Adapter

Before you physically install a NIC or network adapter, it's important to read the vendor's instructions that come with the hardware. Most network adapters you get today should be self-configuring using Plug and Play capabilities. After you install a network adapter that supports Plug and Play, it should work following the installation procedure (which should be automated if the vendor says it is). You might have to restart, but our operating systems are getting much better with this, and you might just get lucky and be all right immediately.

If you happen to have a network adapter that is not Plug and Play, the operating system should detect the new piece of hardware and start a wizard that leads you through the process of loading the adapter's driver and sets initial configuration parameters. You can see your network connection and manage the network connection properties through the Network And Sharing Center. We'll explore this applet in the ''Connecting Wireless Devices'' section later in this chapter.

Configuring a Network Adapter

After you have installed the network adapter, you configure it through its Properties dialog box. There are several ways to access the properties: by using the Network And Sharing Center, through the Computer Management MMC, or via Device Manager. We'll look at the Network And Sharing Center later in the section, ''Viewing the Network And Sharing Center.'' Let's use the Device Manager applet for the network adapter configuration here. To access the Properties dialog box, choose Start and type **Device Manager** in the Start menu's search box to launch Device Manager. Alternatively, you can right-click Computer on the Start menu and choose Manage from the context menu to access Computer Management, which lets you access Device Manager, as shown in Figure 11.1.

Figure 11.1 shows the Network Adapters item expanded. Having Computer Management open is a great way to open Device Manager; this MMC has numerous other installed plug-ins available that might be helpful as you work with your machines.

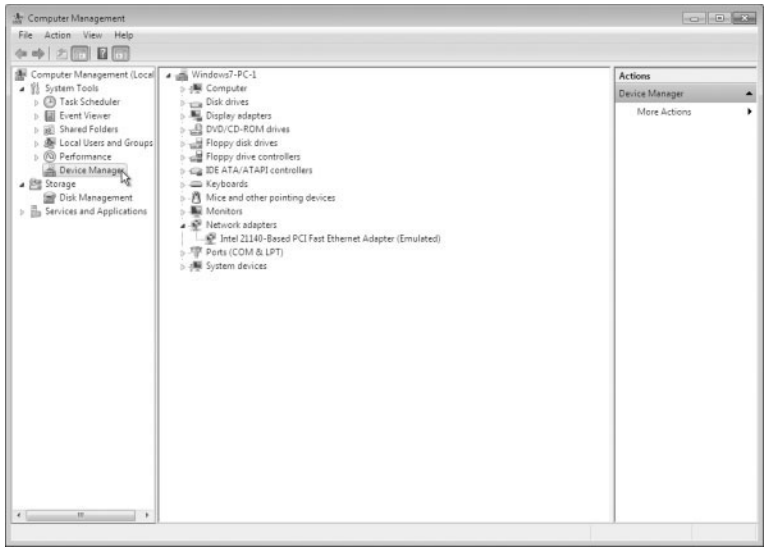


FIGURE 11.1
Accessing Device Manager from the Computer Management MMC

NETWORK ADAPTER PROPERTIES

Accessing the network adapter properties allows you to view and change configuration parameters of the adapter. You do this by right-clicking the adapter in Device Manager and selecting Properties from the context menu. Figure 11.2 shows the Properties dialog box and the tabs available for a network adapter. The available tabs depend on the hardware manufacturer:

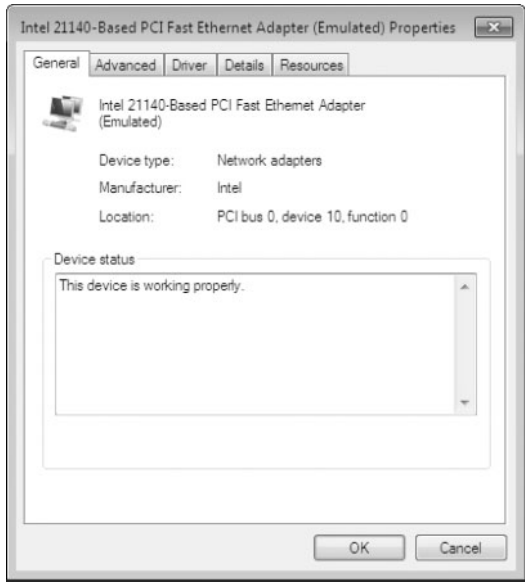
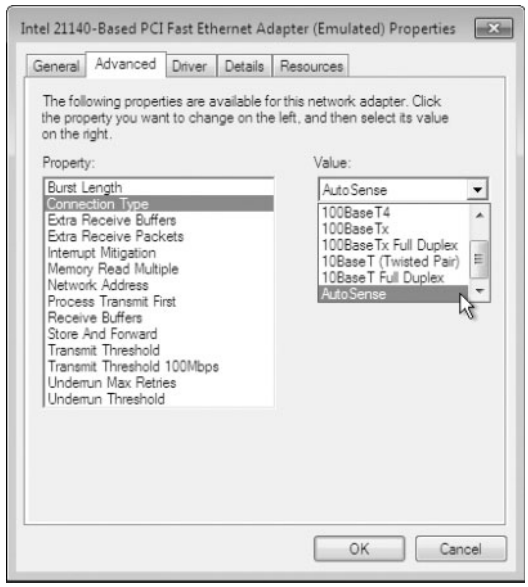


FIGURE 11.2
Network adapter Properties dialog box

The General Tab The General tab of the network adapter Properties dialog box (the tab open in Figure 11.2) shows the name of the adapter, the device type, the manufacturer, and the location. The Device Status box reports whether or not the device is working properly. If a device is not working, the Device Status box gives you an error code and a brief description of what Windows 7 identifies as the issue. You can perform an Internet search for the error code(s) if the text is not sufficient.

The Advanced Tab The contents of the Advanced tab of a network adapter's Properties dialog box vary depending on the network adapter and driver that you are using. Figure 11.3 shows an example of the Advanced tab for a Fast Ethernet adapter. To configure options in this dialog box, choose the property you want to modify in the Property list box and specify the desired value for the property in the Value box on the right. We have selected the Connection Type property and opened the Value drop-down list to show you the options for this network adapter.

FIGURE 11.3
The Advanced tab of a network adapter's Properties dialog box

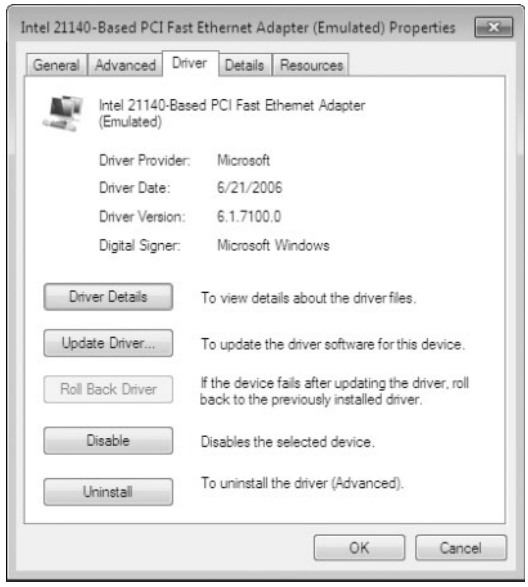


The Driver Tab The Driver tab of the network adapter's Properties dialog box provides the following information about your driver:

- The driver provider
- The date the driver was released
- The driver version (useful in determining whether you have the latest driver installed)
- The digital signer (the company that provides the digital signature for driver signing)

The Driver tab for our adapter is shown in Figure 11.4. The information here varies from driver to driver and even from vendor to vendor.

FIGURE 11.4
The Driver tab of a network adapter's Properties dialog box



Clicking the Driver Details button on the Driver tab opens the Driver File Details dialog box, which provides the following details about the driver:

- The location of the driver file (useful for troubleshooting)
- The original provider of the driver
- The file version (useful for troubleshooting)
- Copyright information about the driver
- The digital signer for the driver

The Update Driver button starts a wizard to step you through upgrading the driver for an existing device.

The Roll Back Driver button allows you to roll back to the previously installed driver if you update your network driver and encounter problems. In Figure 11.4, the Roll Back Driver button is unavailable because we have not updated the driver or a previous driver is not available.

The Disable button is used to disable the device. After you disable the device, the Disable button changes into an Enable button, which you can use to enable the device.

The Uninstall button removes the driver from your computer's configuration. You would uninstall the driver if you were going to remove the device from your system or if you wanted to completely remove the driver configuration from your system so that you could reinstall it from scratch either automatically or manually.

The Details Tab The Details tab of the network adapter's Properties dialog box lists the resource settings for your network adapter. Information found on the Details tab varies by hardware device. Figure 11.5 shows the Details tab for our adapter in Figure 11.5 with the Property drop-down list open to show the options.

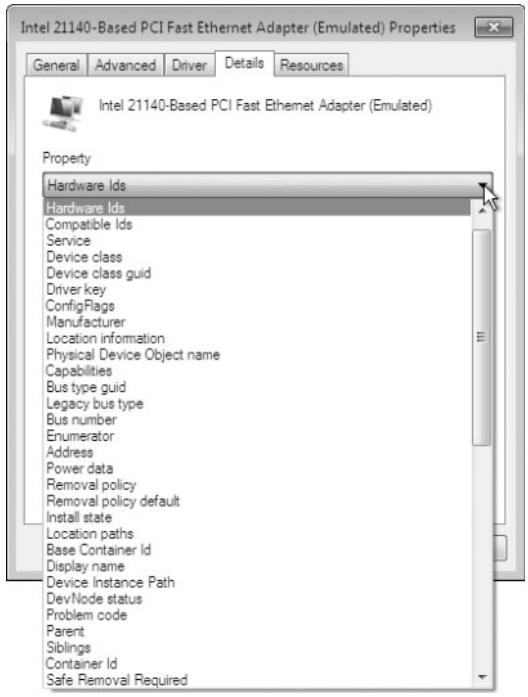


FIGURE 11.5
The Details tab of a network adapter's Properties dialog box

The Resources Tab The Resources tab of a network adapter's Properties dialog box lists the resource settings for your network adapter. Resources include interrupt request (IRQ), memory, and input/output (I/O) resources. This information can be important for troubleshooting if other devices are trying to use the same resource settings. This is not normally the case as Windows 7 and the Plug and Play specification should set up nonconflicting parameters. If there are issues, the Conflicting Device list box at the bottom of the Resources tab shows the conflicts.

NAVIGATING TO THE ADVANCED TAB AND ASSIGNING A CONNECTION TYPE

There might be times when you, as a network administrator, need to manually assign a connection type for one of your servers' NICs. For example, suppose the hardware switch to which you are connecting does not seem to negotiate with the NIC in your server and you want to set up the best connection. When you view the NIC parameters, it seems to be set up for half duplex and you know the switch is set to full duplex.

Perform the following steps to navigate to the Advanced tab and assign the connection type to 100 Mbps and Full Duplex for the most efficient connection for your server and switch connection:

1. Click Start and type **Device Manager** in the Start menu's search box.
2. Double-click Network Adapters in Device Manager to expand the Network Adapters item.
3. Right-click your NIC in the Network Adapters list and select Properties from the context menu.
4. Click the Advanced tab of your NIC's Properties dialog box.

5. Choose Connection Type in the Property list box.
6. Click the drop-down list box and select the choice that allows you to have Full Duplex at 100 Mbps. This item will probably be set at Auto Sense by default, which is not working in this scenario.
7. Click OK to save your changes and close your NIC's Properties dialog box.
8. Close Device Manager.

Troubleshooting a Network Adapter

If your network adapter is not working, the problem might be with the hardware, the driver software, or the network protocols. We discuss the Layer 3 (network protocol) issues later in this chapter in the section, ''Basics of IP Addressing and Configuration.'' The following list gives some common causes for network adapter problems related to Layer 1 and Layer 2:

Network Adapter Not on the HCL If the device is not on the Hardware Compatibility List (HCL), use Internet resources to see if others have discovered a solution or contact the hardware vendor for advice.

Outdated Driver Make sure that you have the most current driver for your adapter. You can check for an updated driver by selecting the Driver tab of the adapter's Properties dialog box and clicking the Update Driver button. Windows 7 searches for a better driver or checks for the latest driver on the hardware vendor's website.

Network Adapter Not Recognized by Windows 7 Check Device Manager to see if Windows 7 recognizes the adapter. If you don't see your adapter, you can try to manually install it.

Improperly Configured Network Card Verify that the settings for the network card are correct for the parameters known within your network and the hardware device the machine is connected to.

Cabling Problem Make sure that all network cables are functioning and are the correct type. This includes making sure the connector is properly seated, the cable is straight or crossed (depending on where it's plugged into), and the cable is not broken. You can do this by looking at the little green light (LGL) for the link and activity on the NIC. This does not guarantee a good connection even if the LGLs are illuminated. A single conductor failure in a cable can still have a link light on but that doesn't mean data is passing.

Bad Network Connection Device Verify that all network connectivity hardware is properly working. For example, on a Fast Ethernet network, make sure the switch and port being used are functioning properly.

Real World Scenario

Cabling Issues Can Be a Pain to Discover

Today, cabling issues should not be nearly as hard to deal with as they were in the past. We have so much autosensing now in our hardware that just about any cable should work. We have been in many situations where we were using the latest hardware but still ran into issues.

Autosensing covers the speed the hardware communicates with, whether it's 10 Mbps, 100 Mbps, or in the Gigabit range. Some IT departments choose to hard-code or define the speed at which communication occurs. If both sides are not set to the same value, problems will exist. We have seen several instances where autospeed settings have the devices swapping between transfer speeds intermittently, thus causing random failures and periodic problems on the network. We have set the speed parameters manually and have found this to be the solution (and actually the troubleshooting step that identified the issue).

When we use autosensing, the hardware negotiates half or full duplex, which is either only transmitting data or receiving data (half duplex) or allowing the hardware to transmit and receive at the same time (full duplex). The original Ethernet specification was based on a contention-based system using a single coaxial cable for data distribution, where all devices connected shared the same distribution wire; only one device could talk at a time. Every device had to listen for data to know if two devices tried to communicate at the same time. When two devices did attempt to transmit data at the same time, a collision occurred and all data had to stop; all devices had to regroup and attempt to communicate again following the one-at-a-time method. With the implementation of twisted-pair wiring and the use of switches, we have hardware (the switch) that controls which devices hear what and can effectively eliminate the potential for collisions. If there are no collisions, there is no need to listen to the media to see if someone else is talking, so talking and listening (transmitting and receiving) at the same time is all right (full duplex). Both devices at the end of the cable must be set up to allow transmitting and receiving at the same time, or intermittent problems will exist. We have run into this many times as well; a switch port was set up as full duplex and the autosensing NIC of our server decided half duplex was the choice. We started seeing collisions increasing within the switch!

One of the more bothersome issues we had to address was the use of either straight-through or cross-over cabling. Autosensing now uses auto MDI/MDX to determine straight (I) or crossed (X), the port type, and lets us always use a straight-through cable. Before, you could go with the old LGL trick for link status and just change the cable if the LED didn't come on. Now, the autosensing takes care of it, but we still seem to have issues with some devices and need to disable auto MDI/MDX and use the correct cable.

Let autosensing be your friend, but don't assume everything is going to just work because all your hardware is new. We find cabling still accounts for a large percentage of our issues, even when just changing a network adapter. Moving a cable in and out of a jack might be just enough to fracture a conductor and cause grief. Start with Layer 1 and verify physical connections before going crazy with the software components.

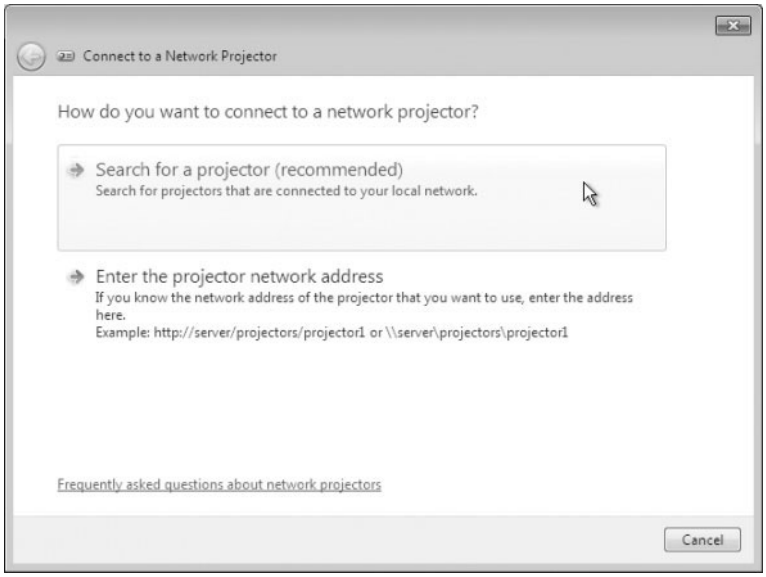
Connecting to a Network Projector

Windows 7 includes network projector support. We use a projector to display presentations, and it's normally connected with a video cable. Today many projectors come with a network interface, wireless or wired, to provide a convenient way to get video output to the projector. If the projector is configured properly for the network, you can use Windows 7 to provide the video to it as a networked display. The projector functionality is designed to use the Remote

Desktop Protocol (RDP) to send the video stream of a machine to a remote device via the network.

Select Start and then type **Network Projector** into the Start menu's search box (you can also choose Start ➢ All Programs ➢ Accessories ➢ Connect To A Network Projector) to initiate the connection process. The Connect To A Network Projector Wizard launches, as shown in Figure 11.6.

FIGURE 11.6
The Connect To A Network Projector Wizard



Click Search For A Projector to locate a projector connected to your wired or wireless network. If no projectors are found, you can go back and enter the name or IP address of a projector. If you know the name or IP address, you can simply choose Enter The Projector Address during the initial wizard screens. You might also need the password of the projector if a password has been configured, as shown in Figure 11.7.

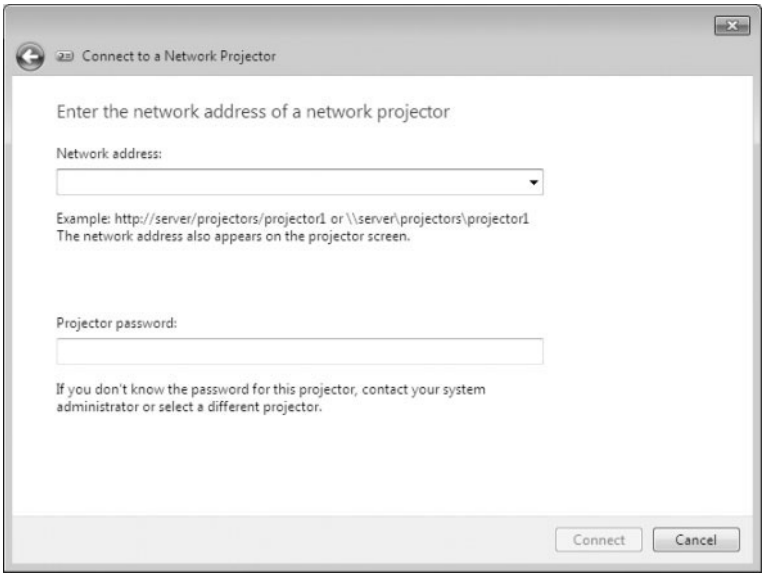
Connecting to a Network Printer

Adding a network printer to Windows 7 is even easier than it was in Vista (which was much easier than previous versions). There is new functionality in Windows 7 for devices and printers known as Device Stage (discussed in Chapter 10). To add a network printer, select Start ➢ Devices And Printers. When the Devices And Printers applet launches, choose the Add A Printer menu item.

Next, select Add A Network, Wireless Or Bluetooth Printer. Windows 7 searches for available printers and allows you to install them. If your printer isn't found, you can select The Printer That I Want Isn't Listed and browse for a printer, or you can select a printer by name or IP address. Chapter 10 has more details and examples about printers.

We have been using wired connections since the beginning of networking. Today, we are transitioning to a wireless network infrastructure, and Windows 7 is well versed to integrate into the wireless world.

FIGURE 11.7
You might have to enter a projector password.



Connecting Wireless Devices

Wireless technology has matured to the point of becoming cost-effective and secure. The use of wireless network adapters is increasingly popular, scaling well out of the home and into the workplace. Windows 7 supports wireless autoconfiguration, which makes wireless network connections easy to use. Windows 7 will automatically discover the wireless networks available and connect your machine to the preferred network. Although this connection is convenient, you must still take certain considerations into account, such as security.

Configuring Wireless Network Settings

If you have a wireless network adapter compatible with Windows 7, it will be automatically recognized by the operating system. This can be a built-in adapter (which most modern laptops come with), a wireless card you install in the machine, or even a wireless USB adapter. After it is installed, it is recognized and shown in Device Manager as well as the Network And Sharing Center in the View Your Active Networks section. We used Device Manager in the previous section for the network adapter configuration, so let's use the Network And Sharing Center for the wireless network configuration. Figure 11.8 shows the Network And Sharing Center with two active networks: the wireless network connection and the wired local area connection.

VIEWING THE NETWORK AND SHARING CENTER

Perform the following step to access the Network and Sharing Center:

- Choose Start and type **Network and Sharing Center** into the Start menu's search box.

or

- Choose Start ➢ Control Panel ➢ Network And Internet ➢ Network And Sharing Center.

or

- Choose Start, and then right-click Network and select Properties from the context menu.

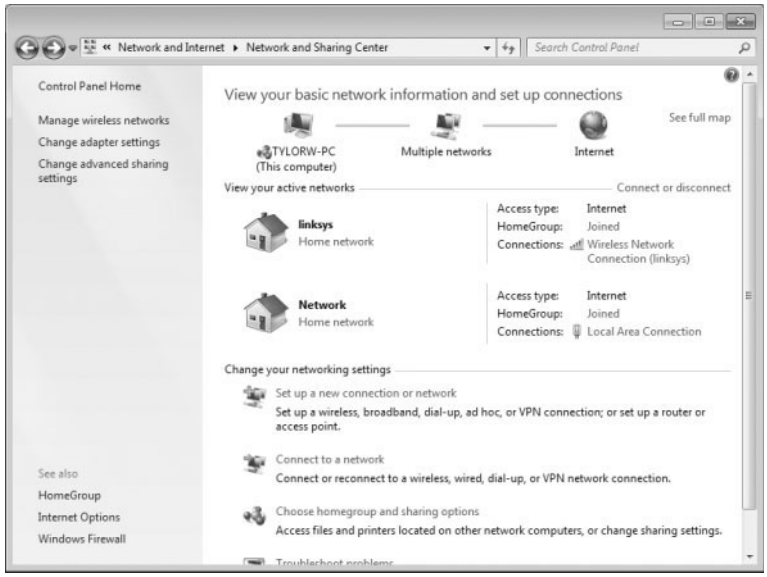
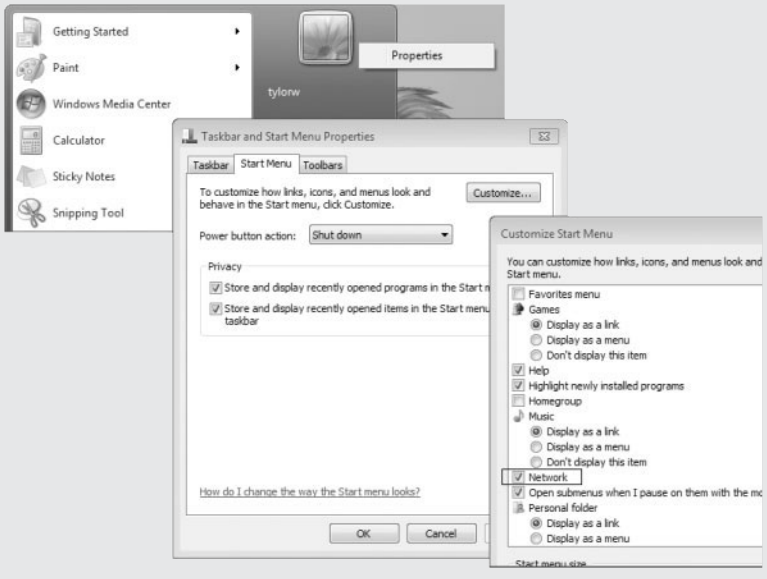


FIGURE 11.8
Network And Sharing Center

The Network Option in the Start Menu

The caveat to this choice is the Network option on the Start menu is not available by default in Windows 7 (the same as in previous Windows versions) and must be added as a customized option to your Start menu using its properties dialog box. You can see all three windows open showing the Network option selected in the following graphic:



Viewing the Wireless Network Connection Status

From the Network And Sharing Center you have easy access to the Wireless Network Connection Status window. This window gives you an initial look at the status by providing the Layer 3 connectivity status (IPv4 and IPv6), media state, Service Set Identifier (SSID) being used, how long the connection has been active (Duration), the negotiated speed of the connection, and the signal quality. The Wireless Network Connection Status window is shown in Figure 11.9.

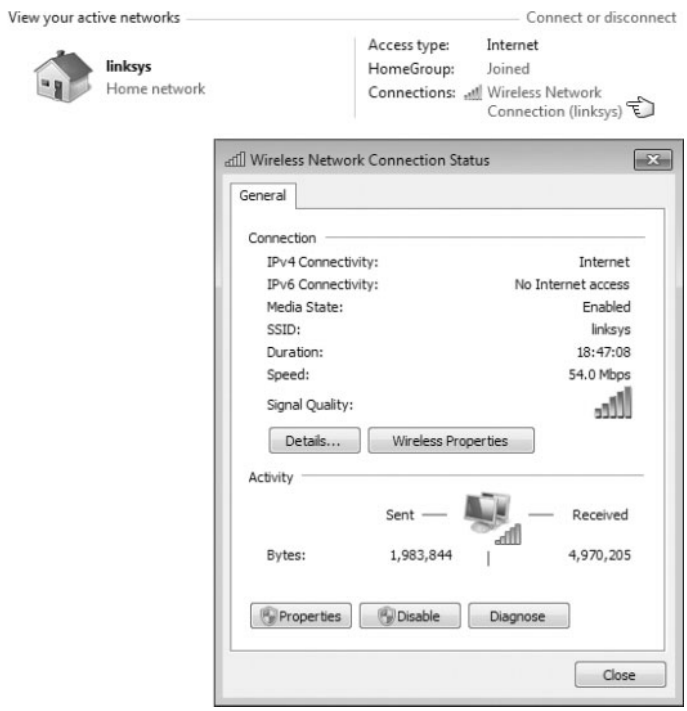


Figure 11.9
The Wireless Network Connection Status window

The Details button in the Wireless Network Connection Status window provides detailed information, including the physical address (Layer 2), logical address (Layer 3), dynamic addressing parameters (DHCP), name resolution items, and more. After you verify physical layer parameters, this area of properties and status is a great place to verify and troubleshoot logical (driver and software) issues.

Viewing Wireless Network Connection Details

If you have a wireless adapter in your machine, perform the following steps to view the network connection details for your wireless network connection:

1. Choose Start and type **Network and Sharing Center** into the Start menu's search box; press Enter.
2. Select the Wireless Network Connection option in the View Your Active Networks section.
3. Click the Details button.
4. Review the network connection details for this connection.

The Wireless Network Connection Status window has an Activity section showing real-time traffic (in bytes) being sent from and received by the wireless network. In this window, you also have access to the wireless network connection properties, which includes access to the wireless adapter configuration pages. You access the Properties dialog box by clicking the Properties button in the Activity section (not the Wireless Properties button in the Connection section; you can identify these buttons, as shown previously in Figure 11.9). The Wireless Network Connection Properties window is shown in Figure 11.10.

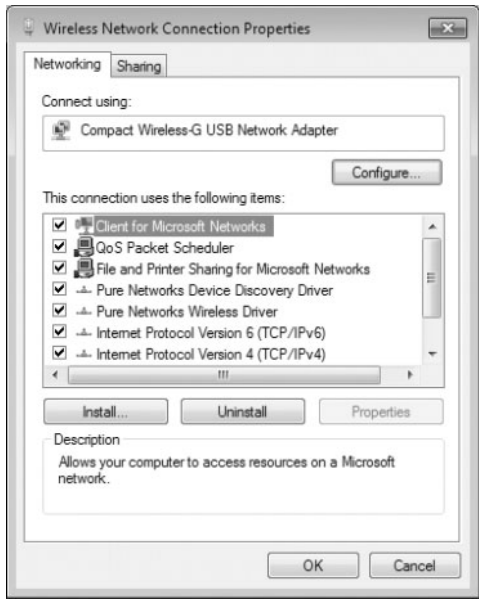


FIGURE 11.10
Wireless Network Connection Properties window

The Wireless Network Connection Properties window has a Networking tab that shows which network adapter is being used for this connection (which you can change if you have more than one available). There is also a tab to allow you to configure Internet Connection Sharing (ICS), which allows other users on your network to access resources through this machine's connection. The This Connection Uses The Following Items section displays the various client, service, and protocols that are currently available for this connection. You can install or uninstall network clients, network services, and network protocols by choosing the appropriate button. You can also view the client, service, or protocol properties if they are available by clicking the Properties button for the selected item (if the Properties button is gray, a properties window is not available for the item). From the Wireless Network Connection Properties window, you have access to the network adapters' hardware configuration properties pages. These would be the same pages you have access to from Device Manager.

Accessing the Wireless Network Adapter Properties Page from the Network And Sharing Center

Perform the following steps to access the network adapter properties from the Wireless Network Connection Properties window:

1. Choose Start and type **Network and Sharing Center** into the Start menu's search box; press Enter.
2. Select Wireless Network Connection in the View Your Active Networks section.

3. Click the Properties button in the Activity section.
4. Click the Configure button.
5. View the various tabs regarding the network adapter properties.
6. Choose Cancel to return to the Wireless Network Connection Status window.

Configuring Wireless Network Security

Wireless network security is a very large part of setting up our wireless networks. The focal point for this is the wireless access point or wireless router to which we connect.

Wireless Connection: Infrastructure or Ad Hoc?

You might not always be connecting to an access point or router; these connections are considered infrastructure mode connections. Infrastructure mode connections are similar to our wired connection of a PC to a switch. You might connect in an ad hoc fashion that could be a computer-to-computer connection to share information with other wireless network devices without another wireless device acting as an intermediary. Ad hoc connections exist in our wired environment as well where we would connect two PCs' NICs together using an Ethernet crossover cable. Securing data transfer in an ad hoc setup is equally important as it is in infrastructure mode where the data is still traversing between devices using radio frequency (RF). Network sniffers today running the wireless adapter promiscuously (in monitor mode) have no problem viewing the RF data stream. If the data stream is not encrypted, the sniffers will have access to it.

Whether you are using a small wireless network or large wireless infrastructure, you should have a plan for ensuring secure communications and configuring wireless network security. There are several basic parameters you can configure on your network access devices that you should increase the security of your wireless network:

- Disable broadcast of the SSID, which is the name of the wireless network. When SSID broadcast is disabled, the wireless network cannot be detected automatically until you manually configure your wireless network card to connect to that SSID.
- Create a Media Access Control (MAC) address filter list so only specifically allowed wireless devices are allowed to connect to the wireless network, or require users attempting to connect to supply connection credentials.
- Enable encryption such as Wi-Fi Protected Access (WPA) or WPA2.

For large implementations, there are several vendors supplying wireless access points under the control of a wireless director, offering software-based controllers that allow access points on the network, providing user access control, and enforcing encryption policies. For smaller implementations, this control functionality is done manually when the wireless routers or access points are set up. The security policies put in place are configured on the wireless access device and the wireless client. The Windows 7 client components in our case must be set up to match the security settings of the wireless network access devices.

During the setup of the most wireless access devices that the hardware vendor provides, the administrator will configure the security parameters. Configuring can be done during the setup program and/or when accessing the wireless access device configuration pages through

a web browser. Most of our current devices have a built-in web server to allow the HTTP connection from a web browser. Windows 7 also has the ability to configure the wireless access device if the hardware vendor makes it available. If there is no specific component written, you can launch the web browser–based configuration from a convenient location: the Network And Sharing Center.

Configuring a Network And Sharing Center Wireless Access Device

Perform the following steps to see how to initiate a Windows 7 wireless access point configuration:

1. Choose Start and type **Network and Sharing Center** into the Start menu's search box; press Enter.
2. Choose the Set Up A New Connection Or Network option.
3. Choose Set Up A New Network to configure a new router or access point, as shown in Figure 11.11, and then click Next.

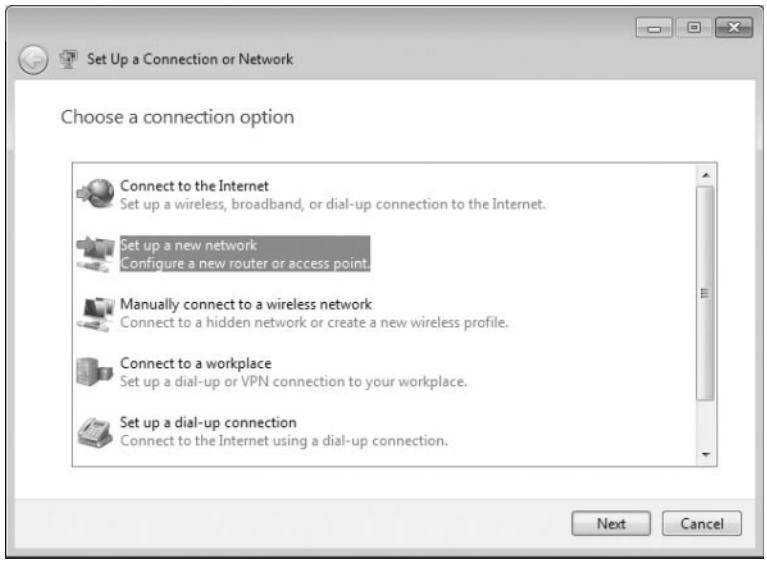


Figure 11.11
Setting up a new network

4. Select the wireless access device you want to configure, as shown in Figure 11.12, from the Set Up A Network window and click Next.
5. Depending on your device, you might be asked to enter a PIN or other identifying parameter to access the device. Enter the PIN and click Next.
6. On the next screen, as shown in Figure 11.13, you will be able to configure the security settings dictated by the wireless security policy to be implemented. The settings defined here need to be configured for each client machine connecting to the wireless network. After making the setting choices, click Next.
7. The configuration of the wireless network device completes and you are shown a confirmation window. Click Finish to close the window.

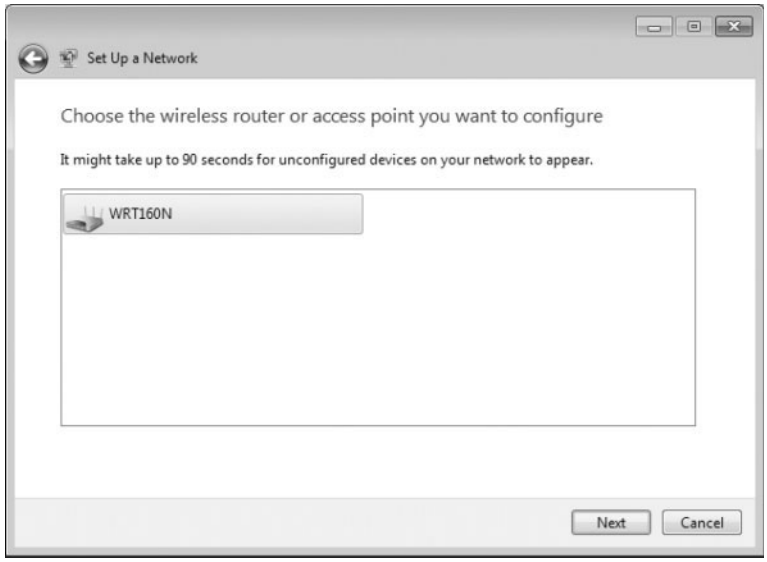


FIGURE 11.12
Choosing the wireless router

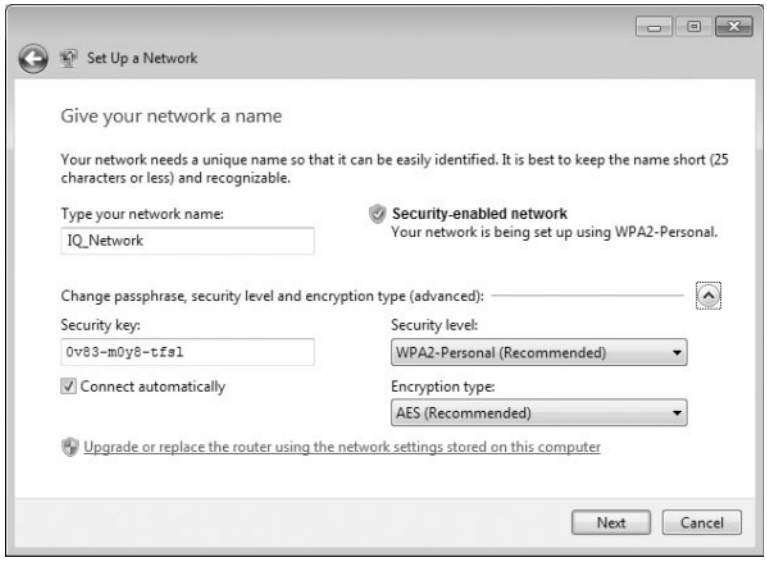


FIGURE 11.13
Wireless security configuration

Whether you had Windows 7 configure the wireless network connection or you performed the setup through the manufacturer's process, you still need to configure your Windows 7 client access. If you have performed the simplest configuration, and there are no security parameters configured (bad idea, by the way), Windows 7 will connect automatically with a quick window showing the wireless network it's connecting to and providing access without much user intervention. Even canceling through the screens will produce a successful (non-secure) connection. This simple configuration process makes connecting a home or small network easy and straightforward for nontechnical users, but this is not a good solution.

If you have configured wireless network security (a good idea), then you need to configure the Windows 7 client with the correct settings. Once again, the configuration screens are available from a convenient location known as the Network And Sharing Center.

Configuring the Network And Sharing Center Wireless Network Client

Perform the following steps to access the Windows 7 client wireless network properties:

1. Choose Start and type **Network and Sharing Center** into the Start menu's search box; then press Enter.
2. Choose Wireless Network Connection item in the View Your Active Networks section of the Network And Sharing Center.
3. Click the Wireless Properties button in the Connection area of the Wireless Network Connection Status window, as shown in Figure 11.14.

Figure 11.14
Click Wireless Properties.

The Wireless Network Properties dialog box opens, displaying the current setup for the wireless network.

Figure 11.15 shows the Connection tab of the Wireless Network Properties dialog box. Here, you have the ability to set or change the Windows 7 client configuration.

The Connection tab displays the following information:

Name The name assigned to the wireless network.

SSID The Service Set Identifier (SSID) of the wireless connection. This defines a friendly name for the wireless network. This is normally an ASCII string and is usually broadcast by default, allowing a machine or users to select a wireless network with which to connect. Some wireless access devices will allow more than one SSID to be available (or broadcast) at the same time, thus creating more than one wireless network within the same device.

Network Type Displays the mode in which the wireless network is operating. If the wireless network is in infrastructure mode, this parameter will be Access Point. If the wireless network is ad hoc, this field will display Computer-To-Computer.

Network Availability Displays to whom the wireless network is available — All Users or Me Only, for example.

You can configure the following information:

Connect Automatically When This Network Is In Range This option, when checked, allows automatic connection for this wireless network. If this option is deselected, the user has to select this wireless network for connection.

FIGURE 11.15
The Connection tab of the Wireless Network Properties dialog box

Connect To A More Preferred Network If Available Windows 7 will attempt to connect to a preferred network (if the Connect Automatically option is selected). If there is more than one preferred network, Windows 7 might switch back and forth if they are both available at the same time. Clearing this option allows the currently connected network to stay connected until it is no longer available, possibly preventing the dropping of data or even dropped connections.

Connect Even If The Network Is Not Broadcasting Its Name (SSID) If the wireless network you are attempting to connect to is not broadcasting its SSID, you must select this option to allow Windows 7 to automatically connect.

There is one more option on the Connection tab of the Wireless Network Properties tab: Copy This Network Profile To A USB Flash Drive. Selecting this link launches the Copy Network Settings Wizard, as shown in Figure 11.16. After you insert a USB flash drive, Windows 7 saves the currently configured wireless network configuration in the form of a `setupSNK.exe` program and a folder named `SMRTNTKY` with the configuration parameters. Exercise caution to protect this information as all the configuration parameters (including security keys) are stored in clear text.

After the files and folder are created and saved, you are presented with a confirmation screen with simple instructions and a link for the detailed information about wireless network configuration. The confirmation page is shown in Figure 11.17.

The second tab of the Wireless Network Properties dialog box is the Security tab. This tab allows you to configure the security parameters as defined in your security policy and configured on your wireless network access devices. Figure 11.18 shows the Security tab with the Security Type and Encryption Type drop-down lists open. You can also see the Network Security Key entry as clear text as the Show Characters option is enabled.

FIGURE 11.16
Copy Network Settings Wizard for the wireless connection

FIGURE 11.17
Wireless connection copy confirmation window

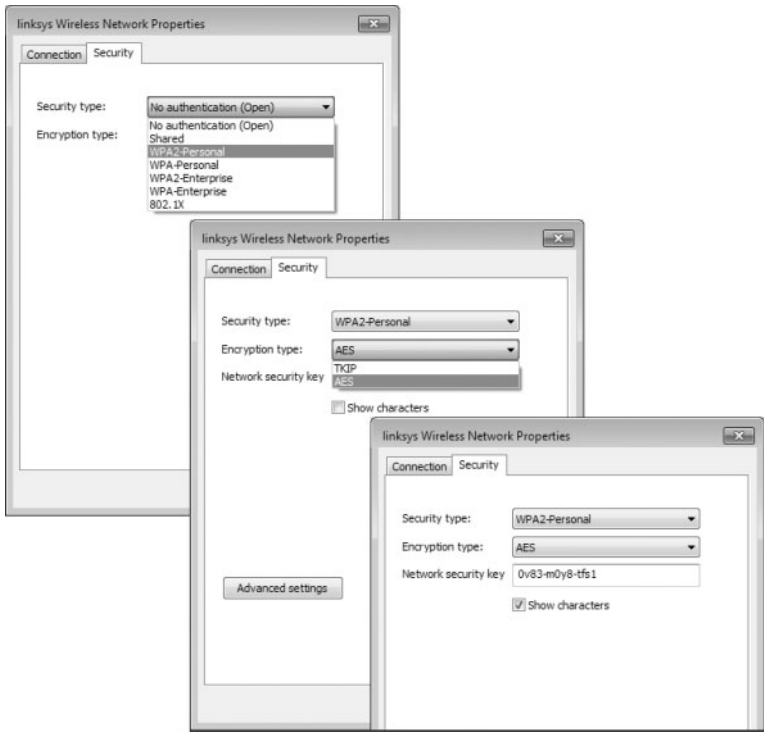


FIGURE 11.18
Wireless Network Properties, Security tab

TROUBLESHOOTING WIRELESS CONNECTIVITY

If you're having problems connecting to your wireless network, check this list:

Ensure that your wireless card and the access device are compatible. Cards that are compatible with the 802.11b standard can only connect to 802.11b or an 802.11b/g access device configured to accept 802.11b. Cards using 802.11a can only connect to 802.11a or 802.11 a/b/g access devices configured to accept 802,11a. An 802.11n card needs to connect to an 802.11n access device for efficiency (although most will auto-negotiate to the best spec available). The specification you're using on the card has to be available and turned on in the wireless access device.

Ensure that your wireless network card is enabled. Many newer laptops and tablets have either a switch or a hotkey setting that enables and disables the wireless device. A laptop switch may be turned off, or the user has unintentionally pressed the key sequence to shut off the PC's wireless radio. The Physical layer always seems to be a good place to start looking.

Ensure that the access point signal is available. The output power of the signal might be fine, but the radio frequency (RF) power is attenuated as it goes through walls, insulation, or water. You need to make sure there is nothing that might be causing interference of the wireless signal.

Ensure the security parameters are configured alike. The SSID, encryption type, encryption algorithm, and passphrase/security key have to be set the same on both the wireless access

device as well as the wireless client. In the desire to make the initial setup and the secure setup easier for end users, some hardware vendors have an ''easy'' button to allow the network access device to negotiate a secure set of parameters with the client. After the wireless network has been working correctly for a while, a failure shows the parameters to now be incompatible, thanks in large part to someone pressing the easy button just before the failure.

Ensure automatic connections if the SSID is not being broadcast. If you are having trouble connecting to a network that does not broadcast its SSID, select the Connect Even If The Network Is Not Broadcasting check box in the Wireless Network Properties dialog box.

One final thought on troubleshooting in the wireless world: wireless routers are quite technologically sophisticated. They have switch ports for connecting hard-wired devices on the private network as well as an Internet port to connect to the outside world. The wireless portion of the device is like another switch port on the private side, thus allowing the wireless devices to interact with the hard-wires. When you troubleshoot, start with the hard-wired devices and see if they can communicate with one another and the outside (the other side of your wireless router). Try to communicate between the hard-wired and wireless as well to eliminate the router components. Also, never use the wireless network to configure the wireless devices. If you do, you will undoubtedly lose connectivity in the middle of a configuration and be forced to connect with the cable, leaving the access point unusable until you complete the task you started wirelessly.

Joining and Sharing HomeGroups in Windows 7

Have you ever wanted to share your music or pictures and found it difficult? HomeGroup is a new functionality of Windows 7 that simplifies the sharing of music, pictures, and documents in your small office or home network between Windows 7 PCs. HomeGroup allows you to share USB connected printers, too. If you have a printer installed on a Windows 7 computer and it's shared by HomeGroup, it is automatically installed onto the other HomeGroup-enabled Windows 7 PCs. This even extends to domain-joined computers; they can be part of a HomeGroup as well.

The first step in the process of using HomeGroup for sharing is to create a new HomeGroup or join an existing one. If the Windows 7 Network Discovery feature is not enabled, you will be asked to create a HomeGroup. In the Network And Sharing Center select Choose Homegroup And Sharing Options and then click the Create A Homegroup button (both items are shown in Figure 11.19).

With Windows 7 Network Discovery turned on (the default), HomeGroup is created automatically. You still need to join the HomeGroup to make use of the other shared resources and to share yours. In the Network And Sharing Center, you can join an existing HomeGroup by clicking the Join Now button, as shown in Figure 11.20.

Part of joining a HomeGroup setup is to define the resources that you want to make available to the other members of HomeGroup. The next screen in the setup, as shown in Figure 11.21, lets you choose which resources you want to share.

The next step is to enter the HomeGroup password. Windows 7, by default, will recognize a HomeGroup on the network. However, the other Windows 7 machines will not have access to the resources. Allowing any Windows 7 machine connecting to the network to automatically have shared resource access would be a huge security hole. To protect the Windows 7 user resources, a password must be entered to join HomeGroup. Figure 11.22 shows the screen where you enter the password.

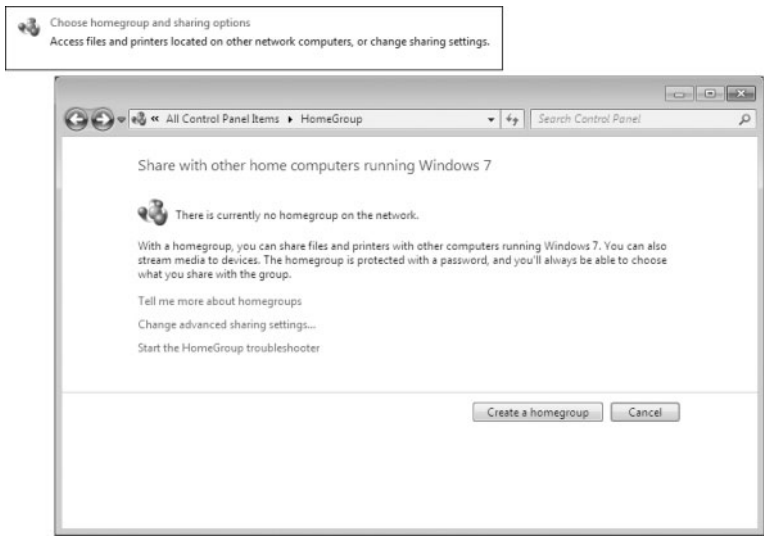


FIGURE 11.19
Creating a HomeGroup

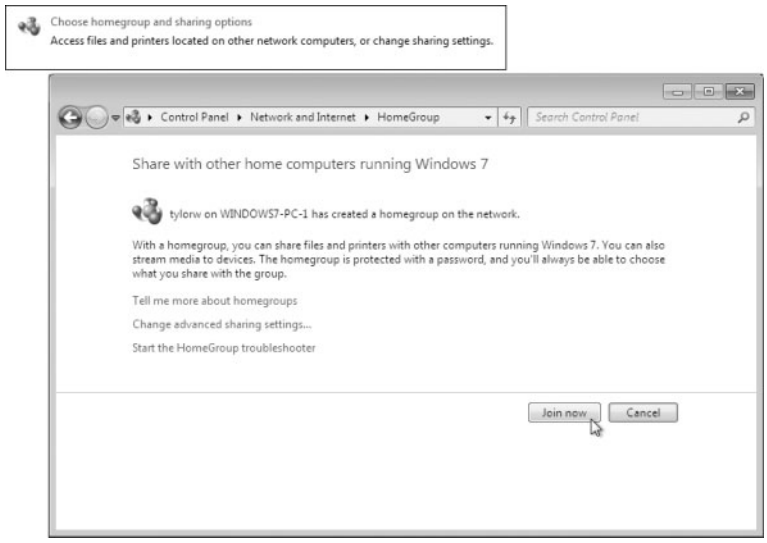


FIGURE 11.20
Joining an existing HomeGroup

FIGURE 11.21
HomeGroup sharing selections

FIGURE 11.22
HomeGroup password screen

The password for the HomeGroup can be found or changed on the machine that established the HomeGroup. After other machines have joined, each machine has the ability to view or change the password, but they must join the HomeGroup first. The initial machine in the HomeGroup will create a random secure password. To view and/or print the HomeGroup password, select Choose Homegroup And Sharing Options in the Network And Sharing Center and then choose View Or Print The Homegroup Password, as shown in Figure 11.23. Again, this can be done from any Windows 7 machine that is already a member of the HomeGroup, but not from one that wants to join.

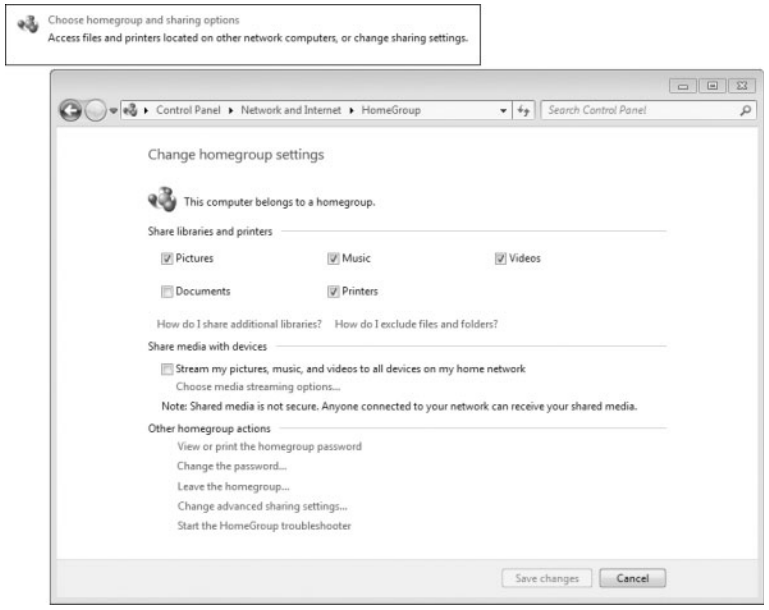


FIGURE 11.23 Changing the HomeGroup settings

Figure 11.24 shows the View And Print Your Homegroup Password screen. We have changed the password to ''password'' (not recommended for your network).

Remember that Windows 7 will initially create a random secure password for the HomeGroup, and you need to visit the View And Print Your Homegroup Password screen to find out what it is. You will probably want to change it. To change the password, choose the Change The Password option on the Change Homegroup Settings screen and then select Change The Password on the Change Your Homegroup Password screen, as shown in Figure 11.25. When you change the HomeGroup password, you need to go to each of the other Windows 7 machines that are members of the HomeGroup and change the password if you still want the others to share resources.

After the HomeGroup is set up, you can see the other members' resources by choosing the HomeGroup option in Windows Explorer. You can also add the HomeGroup option to your Start menu, as shown in Figure 11.26.

Choosing the HomeGroup option from the Start menu (or choosing Computer and selecting HomeGroup in the Explorer window) allows you to access the other members of your HomeGroup. Figure 11.27 shows the HomeGroup item expanded and another Windows 7 machine's resources that has joined the HomeGroup.

FIGURE 11.24
View And Print Your Homegroup Password screen

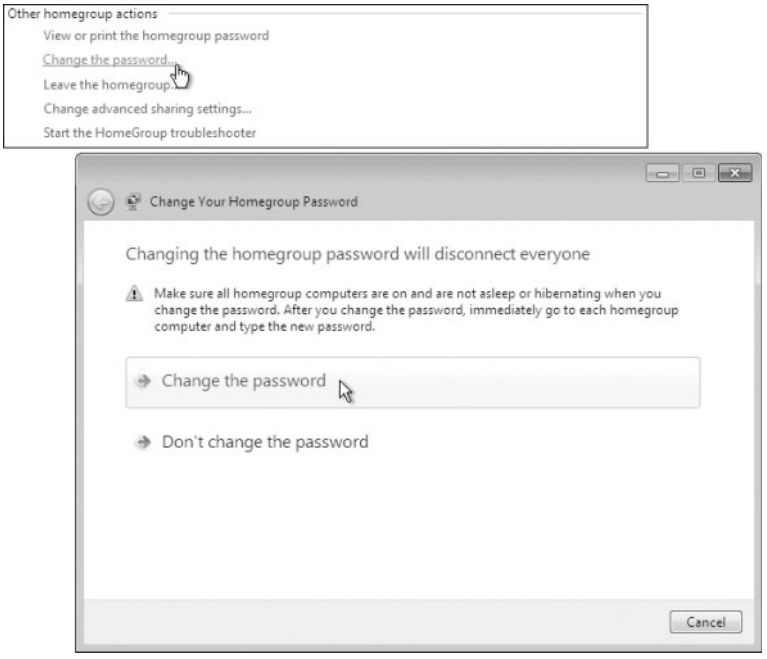


FIGURE 11.25
Changing the HomeGroup password

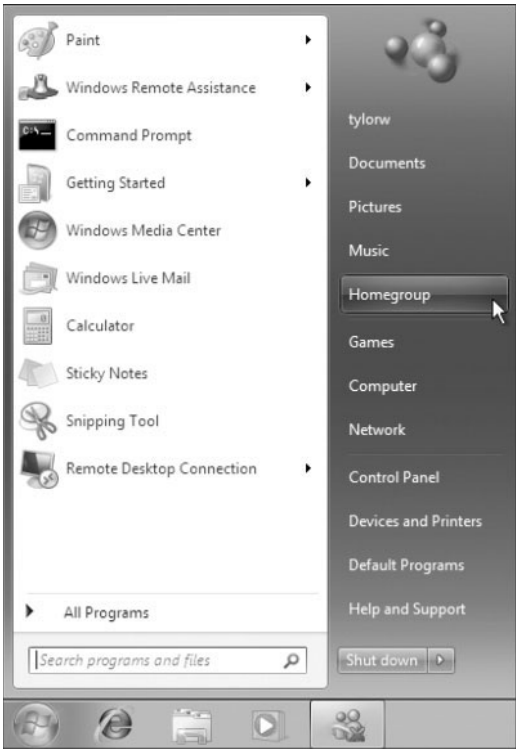


FIGURE 11.26
HomeGroup in the Start menu

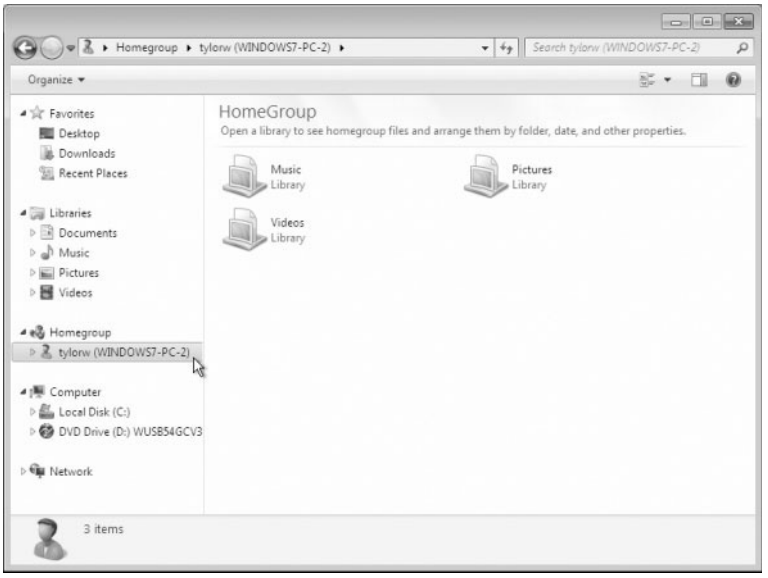


FIGURE 11.27
Viewing HomeGroup resources from Explorer

HomeGroups are a great option for users in the Windows 7 environment for sharing resources. But what if you still have non–Windows 7 machines? The legacy function of simply sharing resources and setting permissions still works for Windows 7 and will allow older operating systems to have access to resources shared on Windows 7 machines. It also allows users running Windows 7 to have access to the shared resources on Vista and XP.

To connect to other network devices, having a network protocol configured correctly is a key process. TCP/IP is the default network protocol for Windows 7.

Understanding Network Protocols

Network protocols function at the OSI model Layer 3 (the Network layer) and Layer 4 (the Transport layer). Network protocols are responsible for transporting data across an internetwork. They are responsible for reliable communication as well. The only network protocol installed by default in Windows 7 is TCP/IP, both version 4 and version 6 (called IPv4 and IPv6).

A solid understanding of TCP/IP and the configuration required for network communication is a substantial piece of the Windows 7 setup.

Overview of TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is the most commonly used network protocol. It is a suite of protocols that have evolved into the industry standard for network, internetwork, and Internet connectivity. The main protocols providing basic TCP/IP services include Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP).

Benefits of Using TCP/IP

TCP/IP as a protocol suite was accepted as an industry standard in the 1980s and continues to be the primary internetworking protocol today. For a default installation of Windows 7, IPv4 and IPv6 are both installed by default. TCP/IP has the following benefits:

- TCP/IP is the most common protocol and is supported by almost all network operating systems. It is the required protocol for Internet access.
- TCP/IP is dependable and scalable for use in small and large networks.
- Support is provided for connectivity across interconnected networks, independent of the operating systems being used at the upper end of the OSI model or the physical components at the lower end of the OSI model.
- TCP/IP provides standard routing services for moving packets over interconnected network segments. Dividing networks into multiple subnetworks (or subnets) optimizes network traffic and facilitates network management.
- TCP/IP is designed to provide data reliability by providing a connection at the transport layer and verifying each data segment is received and passed to the application requiring the data by retransmitting lost information.
- TCP/IP allows for the classification of data in regard to its importance (quality of service). This allows important time-sensitive streams of data to get preferential treatment (like Voice over IP).

- TCP/IP is designed to be fault tolerant. It is able to dynamically reroute packets if network links become unavailable (assuming alternate paths exist).
- Protocol applications can provide services such as *Dynamic Host Configuration Protocol (DHCP)* for TCP/IP configuration and Domain Name System (DNS) for hostname-to-IP address resolution.
- Windows 7 continues to support *Automatic Private IP Addressing (APIPA)* used by small local connection–only networks without a DHCP server to allow Windows 7 to automatically assign an IP address to itself.
- Support for *NetBIOS* over TCP/IP (NetBT) is included in Windows 7. NetBIOS is a software specification used for identifying computer resources by name as opposed to IP address. We still use TCP/IP as the network protocol, so we map the NetBIOS name to an IP address.
- The inclusion of *Alternate IP Configuration* allows users to have a static and a DHCP-assigned IP address mapped to a single network adapter, which is used to support mobile users who roam between different network segments.
- IPv6 incorporates a much larger address space and, more importantly, incorporates many of the additional features of TCP/IP into a standardized protocol. This is important because if a vendor says they support TCP/IP, they only have to support the 1980s version and may not support additional features like the Internet protocol security features of IPSec. IPv6 as a standard includes these features and is thus a more robust network protocol.

FEATURES OF TCP/IP

One of the main features of TCP/IP is that it allows a common structure for network communications across a wide variety of diverse hardware and operating systems and a lot of applications, specifically written to configure and control it. Several of the features of TCP/IP included with Windows 7 are:

- TCP/IP connectivity tools allowing access to a variety of hosts across a TCP/IP network. TCP/IP tools in Windows 7 include clients for HTTP, FTP, TFTP, Telnet, and finger, among others. Server components for the tools are available.
- Inclusion of a Simple Network Management Protocol (SNMP) agent that can be used to monitor performance and resource use of a TCP/IP host, server, or network hardware devices.
- TCP/IP management and diagnostic tools are provided for maintenance and diagnostic support. TCP/IP management and diagnostic commands include `ipconfig`, `arp`, `ping`, `nbtstat`, `netsh`, `route`, `nslookup`, `tracert`, and `pathping`.
- Support for TCP/IP network printing, allowing you to print to networked print devices.
- Logical and physical multihoming, allowing multiple IP addresses on a single computer for single or multiple network adapters. Multiple network adapters installed on a single computer are normally associated with routing for internetwork connectivity.

- Support for internal IP routing, which allows a Windows 7 computer to route packets between multiple network adapters installed in one machine.
- Support for virtual private networks, which allows you to transmit data securely across a public network via encapsulated and encrypted packets.

Basics of IP Addressing and Configuration

Before you can configure TCP/IP, you should have a basic understanding of TCP/IP configuration and addressing. Let's review TCP/IP addressing. To configure a TCP/IP client, you must specify an IP address (also known as the logical address), subnet mask, and default gateway (if you're going to communicate outside your local network). Depending on your network, you might want to configure a DNS server, domain name, or maybe even a WINS server.

You can see the Windows 7 TCP/IP version 4 properties window in Figure 11.28. We will go through the configuration steps and show you how to access this window later in this section.

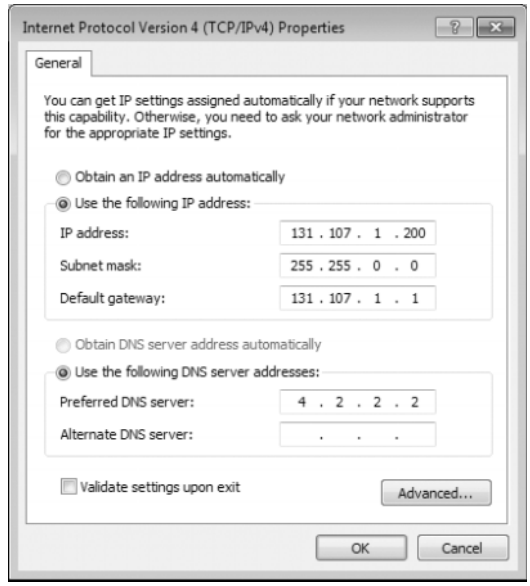


Figure 11.28
Windows 7 TCP/IP version 4 properties

IPv4 Address Types

There are three types of IPv4 addresses: broadcast, multicast, and unicast.

A broadcast address is read by all hosts that hear it (the broadcast will not go across a router, so only local devices hear the broadcast). The IPv4 broadcast address is 255.255.255.255; every single bit is a one.

A multicast address is a special address that one or more devices will listen for by joining a multicast group. Not all the local devices respond and process the data in the multicast packet; only the devices configured to listen for it respond. A multicast address will have a

value between 224 and 239 in the first octet (the leftmost number in the dotted decimal representation). A multicast example is 224.0.0.5.

A unicast IP address uniquely identifies a computer or device on the network. An IPv4 unicast address is a four-octet, 32-bit address represented as dotted decimal (an example is 131.107.1.200). Each number in the dotted decimal notation is a decimal representation of 8 bits, and the value of each is going to be between 0 and 255 (255 is the numerically largest value that 8 bits can represent). A portion of the IPv4 unicast address is used to identify the network the device is on (or the network of a destination device), and part is used to identify the individual host on the local network or the unique host on a remote network. The IPv4 address scheme is the only address space that the Internet uses today, and TCP/IP is the only network protocol that the Internet uses today.

IPv4 Address Classes

When the TCP/IP suite was accepted as a standard in the 1980s, three classes of unicast IP addresses were defined. Depending on the class you use, different parts of the address show the default network portion of the address and the host address. We still refer to these addresses by class, but we no longer really utilize this class structure; we'll explain shortly.

Table 11.1 shows the three classes of network addresses and the number of networks and hosts available for each network class as defined by the original TCP/IP version 4 standard.

TABLE 11.1: IPv4 Class Assignments

Network Class	Address Range of First Octet	Number of Unique Networks Available	Number of Unique Hosts Per Network
A	1–126	126	16,777,214
B	128–191	16,384	65,534
C	192–223	2,097,152	254

The values are based on the number of bits that can be changed (or used) by the network portion for the number of networks available or by the host portion for the number of hosts available. A quick example: if you have 8 bits to work with, 2 raised to the 8th power are the total number of different combination (of 8 bits) you can make. 2 raised to the 8th power is 256. So, if you have 8 bits available to you in the host portion of an IP address, you can have 256 possible addresses. The catch here is that the first address in the range is not assignable to a host (we use the first address to define the network ID) and the last address is not assignable to a host (we use the last address as the subnetwork broadcast address). If you have 8 bits to use, you can only assign 254 to unique unicast IPv4 addresses to devices. It just so happens that the original IPv4 specification for a Class C address space allocated 24 bits to the network portion and 8 bits for the host portion. How many unique addresses are available? Yes: 254.

IPv4 Subnet Mask

The *subnet mask* is used to specify which portion of the unicast IPv4 address defines the network value and which portion of the unicast IPv4 address defines the unique host value. The subnet mask can be shown as dotted decimal, as with 255.255.255.0, or as slash notation, as

in /24. The 1980s standard for classful network addressing defined subnet masks for each class, as shown in Table 11.2.

TABLE 11.2: IPv4 Classful Subnet Masks

CLASS	DEFAULT MASK	SLASH NOTATION
Class A	255.0.0.0	Slash 8 (/8)
Class B	255.255.0.0	Slash 16 (/16)
Class C	255.255.255.0	Slash 24 (/24)

The slash notation is easier to use as it defines the same information in a more convenient format. If you look at the Class A default (or natural) mask or 255.0.0.0, you can say that 255 is 8 ones (converting a decimal 255 to binary yields 1111 1111). Slash 8 simply means there are 8 ones in the subnet mask (or 255.0.0.0). By using 255, you are selecting the octet or octets (or, in some cases, the piece of an octet) used to identify the network address. For example, in the Class B network address 192.168.2.1, with the default subnet mask for a Class B space being 255.255.0.0, then 192.168 is the network address and 2.1 is the unicast host address.

IPv4 Default Gateway

For each machine to communicate to other devices, the machine evaluates the network portion of the IP address it desires to communicate with (the destination device) and the network portion of its IP address. If the two network values are the same, the machine attempts to communicate directly with the destination machine. If the network portions of the two IP addresses are different, then the local machine sends the packet to the default gateway. The default gateway will then decide where the destination is by evaluating the network portion of the IP address and send it to the next device. You configure a *default gateway* if the network contains routers (the default gateway is a router). A *router* is a device that connects two or more network segments (IP subnetworks) together. Routers function at the Network layer of the OSI model.

You can configure a Windows 7 computer or Windows Server 2008 to act as a router by installing two or more network cards in the server, attaching each network card to a different network segment, and then configuring each network card for the segment to which it will attach. You can also use third-party routers, which typically offer more features than Windows 7 computers or Windows Server 2008 configured as a router. Many times in our network we use the first available IP address as the address of our default gateway (for example, 131.107.1.1). You do not send packets to the default gateway; the network protocol does by getting the physical address (MAC) or the default gateway and inserting it as the destination MAC address with the actual destination IP or the remote device.

DNS Servers

Domain Name System (DNS) servers are used to resolve hostnames to IP addresses. Name resolution makes it easier for people to access other IP hosts. For example, do you know what the IP address is for Google? No? Do you know the hostname of Google server? Yes, you would use `www.google.com`. From your computer, pinging www.google.com actually sends the request to 66.102.1.147, the IP address returned by your DNS server. You can understand why many

people might not know the IP address but would know the domain hostname. Windows 7 asks the DNS server configured on the machine for the resolution of the hostname to an IP address. Most companies and Internet service providers (ISPs) have their own DNS servers that know how to resolve any valid request. There are public DNS servers that can be used as well.

> ***FULLY QUALIFIED DOMAIN NAME***
>
> The name you use to access the Google server, www.google.com, is an example of a fully qualified domain name (FQDN). This notation has a domain component, which is google.com. The ''dot com'' is the top-level domain that parents most company names. You will see ''dot gov'' for government agencies and ''dot edu'' for educational institutions, along with a lot more. The ''google'' of the google.com domain is the organization who is logically responsible for the resource. Finally, the ''www'' is the unique identifier within the organization for the resource. We have become very familiar with this notation, but it is not guaranteed to be the name (nor does it have to be). You might well have seen your browser go to www1.acme.com or even bob.jester.edu. As long as the name resolves to the correct IP address, all is good.

If you do not have access to a properly configured DNS server or simply don't want your machine to resolve an IP address dynamically, you can statically configure a hostname to an IP address by editing the HOSTS file on your Windows 7 machine. Why would you do this? Perhaps there is more than one server available with the same name (do you think there is only one Google server?), and you want to use one of the addresses specifically. You can edit your local host's file, as shown in Figure 11.29, with a FQDN and the configured IP address will be used.

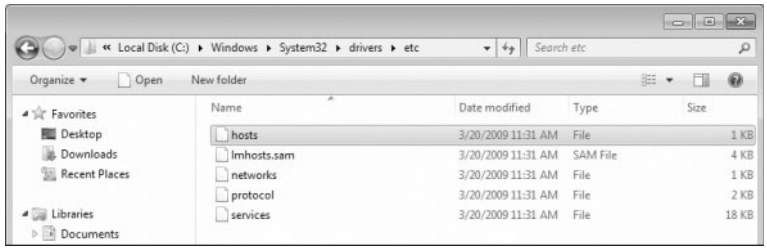


FIGURE 11.29
HOSTS file location in Windows 7

WINS Servers

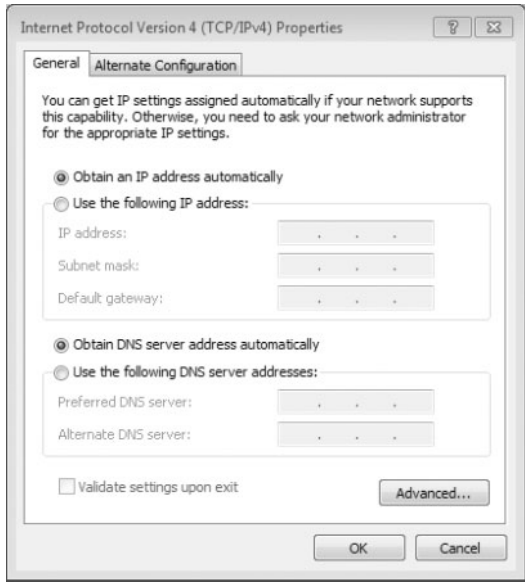
Windows Internet Name Service (WINS) servers are used to resolve NetBIOS (Network Basic Input/Output System) names to IP addresses. Windows 7 uses NetBIOS names in addition to hostnames to identify network computers. This is mainly for backward compatibility with legacy Windows operating systems, which used this addressing scheme extensively. When you attempt to access a computer using the NetBIOS name, the computer must be able to resolve the NetBIOS name to an IP address. This address resolution can be accomplished by using one of the following methods:

- Through a broadcast (if the computer you are trying to reach is on the same network segment)
- Through a WINS server
- Through an LMHOSTS (LAN Manager HOSTS) file, which is a static mapping of IP addresses to NetBIOS computer names

Dynamic Host Configuration Protocol (DHCP)

Each device that will use TCP/IP on your network must have a valid, unique IP address. This address can be manually configured or better yet can be automated through *Dynamic Host Configuration Protocol (DHCP)*. DHCP is implemented as a client/server application. The server is configured with a pool of IP addresses and other IP-related configuration settings, such as subnet mask, default gateway, DNS server address, and WINS server address. The client is configured to automatically request IP configuration information from the DHCP server and use it for a given period of time (the lease length). Figure 11.30 shows the TCP/IP version 4 properties pages set up to use DHCP.

FIGURE 11.30
TCP/IP properties using DHCP



DHCP works in the following manner:

1. When the client computer starts up, it sends a broadcast DHCPDISCOVER message, requesting a DHCP server. The request includes the hardware address of the client computer.
2. Any DHCP server receiving the broadcast that has available IP addresses will send a DHCPOFFER message to the client. This message offers an IP address for a set period of time (called a *lease*), a subnet mask, and a server identifier (the IP address of the DHCP server). The address that is offered by the server is marked as unavailable and will not be offered to any other clients during the DHCP negotiation period.
3. The client selects one of the offers and broadcasts a DHCPREQUEST message, indicating its selection. This allows any DHCP offers that were not accepted to be returned to the pool of available IP addresses.
4. The DHCP server that was selected sends back a DHCPACK message as an acknowledgment, indicating the IP address, subnet mask, and duration of the lease that the client computer will use. It might also send additional configuration information, such as the address of the default gateway and the DNS server address.

Using Deployment Options for TCP/IP Configurations

Windows 7 has four methods available for configuring TCP/IP:

- Static IP addressing
- Dynamic Host Configuration Protocol (DHCP)
- Automatic Private IP Addressing (APIPA)
- Alternate IP configuration

Although DHCP is the most common method for configuring an IP address on the machines in a network, the other methods are used as well.

Configuring Static IP Addressing

You can manually configure IP addressing if you know your IP address and subnet mask. If you are using optional components such as a default gateway or a DNS server, you will need to know the IP addresses of the computers that host these services as well. This option is not typically used in large networks because it is time consuming and prone to user error.

Statically Configuring a Windows 7 IPv4 address and DNS Server

Perform the following steps to manually configure a static IP address for a Windows 7 machine:

1. Select Start and type **Network and Sharing Center** into the Start menu's search box.
2. In the Network And Sharing Center window, click Local Area Connection in the View Your Active Networks section.
3. Click the Properties button in the Activity section of the Local Area Connection Status box.
4. In the Local Area Connection Properties dialog box, select Internet Protocol Version 4 (TCP/IPv4), as shown in Figure 11.31, and click the Properties button.

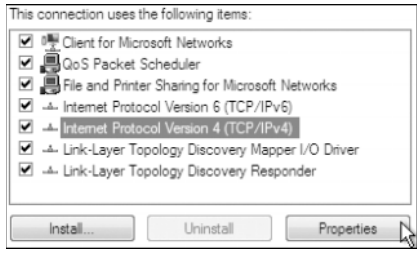


FIGURE 11.31
Select Internet Protocol Version 4 (TCP/IPv4).

5. Choose Use The Following IP Address in the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
6. In the IP Address box, enter **131.200.1.200**; in the Subnet Mask box, enter **255.255.0.0**; and in the Default Gateway box, enter **131.107.1.1**.

USE A VALID ADDRESS FOR YOUR NETWORK

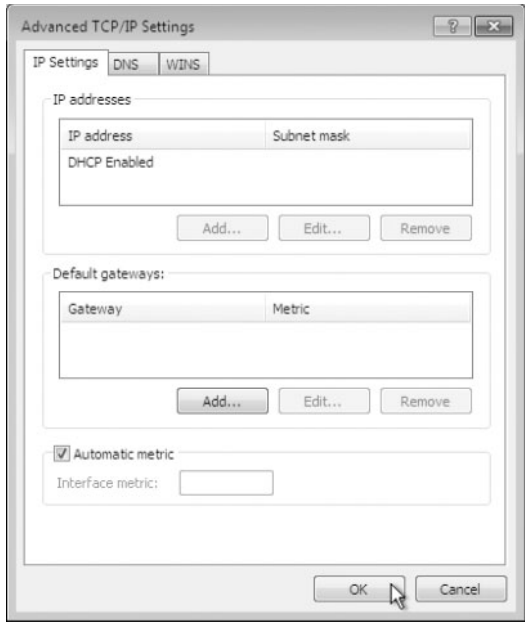
The example in step 6 is likely not a valid IP address on your network. You can substitute a valid address, subnet mask, and default gateway if you know them. If you click OK and see this is not a valid IP address for your network, you will lose connectivity!

7. Choose Use The Following DNS Server Addresses in the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
8. Enter **4.2.2.2** in the Preferred DNS Server box. You can leave the Alternate DNS Server box blank.
9. If you have entered valid information in steps 6 and 8, you can click OK to save your settings and close the dialog box; otherwise, click Cancel to revoke your changes.

Access Advanced Configuration TCP/IPv4 Properties

Clicking the Advanced button in the Internet Protocol Version 4 (TCP/IPv4) dialog box opens the Advanced TCP/IP Settings dialog box, as shown in Figure 11.32. In this dialog box, you can configure advanced IP, DNS, and WINS settings.

FIGURE 11.32
Advanced TCP/IPv4 Properties dialog box



You can edit or add multiple addresses to the same machine in the Advanced TCP/IP Settings windows as well as edit or add default gateways here. You also have access to the advanced DNS and WINS tabs, where you can modify specific parameters for both hostname resolution (DNS) and NetBIOS name resolution (WINS). Figure 11.33 shows both the DNS and WINS tabs of the Advanced TCP/IP Settings dialog box.

Table 11.3 shows the DNS advanced configuration properties and outlines the functionality.

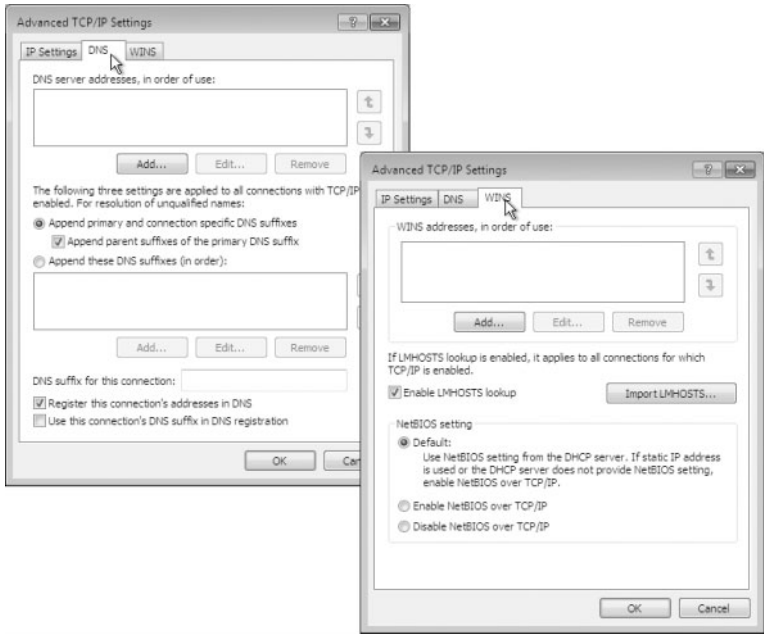


FIGURE 11.33
Advanced DNS and WINS properties tabs

TABLE 11.3: Advanced DNS TCP/IP Settings Options

OPTION	DESCRIPTION
DNS Server Addresses, In Order Of Use	Specifies the DNS servers that are used to resolve DNS queries. Use the arrow buttons on the right side of the list box to move a server up or down in the list.
Append Primary And Connection Specific DNS Suffixes	Specifies how unqualified domain names are resolved by DNS. For example, if your primary DNS suffix is `iq.com` and you type **`ping bob`**, DNS will try to resolve the address as `bob.iq.com`.
Append Parent Suffixes Of The Primary DNS Suffix	Specifies whether name resolution includes the parent suffix for the primary domain DNS suffix, up to the second level of the domain name. For example, if your primary DNS suffix is `maine.iq.com` and you type **`ping bob`**, DNS will try to resolve the address as `bob.maine.iq.com`. If this doesn't work, DNS will try to resolve the address as `bob.iq.com`.
Append These DNS Suffixes (In Order):	Specifies the DNS suffixes that will be used to attempt to resolve unqualified name resolution. For example, if your primary DNS suffix is `iq.com` and you type **`ping bob`**, DNS will try to resolve the address as `bob.iq.com`. If you append the additional DNS suffix `Corp.com` and type **`ping bob`**, DNS will try to resolve the address as `bob.iq.com` and `bob.Corp.com`.

TABLE 11.3: Advanced DNS TCP/IP Settings Options (*CONTINUED*)

OPTION	DESCRIPTION
DNS Suffix For This Connection:	Specifies the DNS suffix for the computer. If this value is configured by a DHCP server and you specify a DNS suffix, it will override the value set by DHCP.
Register This Connection's Addresses In DNS	Specifies that the connection will try to register its addresses dynamically using the computer name that was specified through the System Properties dialog box (accessed through the System icon in Control Panel).
Use This Connection's DNS Suffix In DNS Registration	Specifies that when the computer registers automatically with the DNS server, it should use the combination of the computer name and the DNS suffix.

Table 11.4 shows the WINS advanced configuration properties and outlines the functionality.

TABLE 11.4: Advanced WINS TCP/IP Settings Options

OPTION	DESCRIPTION
WINS Addresses, In Order Of Use	Specifies the WINS servers that are used to resolve WINS queries. You can use the arrow buttons on the right side of the list box to move a server up or down in the list.
Enable LMHOSTS Lookup	Specifies whether an LMHOSTS file can be used for name resolution. If you configure this option, you can use the Import LMHOSTS button to import an LMHOSTS file to the computer.
Default: Use NetBIOS Setting From The DHCP Server	Specifies that the computer should obtain its NetBIOS-over-TCP/IP and WINS settings from the DHCP server.
Enable NetBIOS Over TCP/IP	Allows you to use statically configured IP addresses so that the computer is able to communicate with pre–Windows XP computers (NetBIOS was discontinued with XP).
Disable NetBIOS Over TCP/IP	Allows you to disable NetBIOS over TCP/IP. Use this option only if your network includes only Windows XP clients, Windows Vista clients, or DNS-enabled clients.

SETTING UP DHCP

Dynamic IP configuration assumes that you have a DHCP server on your network that is reachable by the DHCP clients. DHCP servers are configured to automatically provide DHCP clients with all their IP configuration information, including IP address, subnet mask, and DNS server. For large networks, DHCP is the easiest and most reliable way of managing IP configurations. By default, a Windows 7 machine is configured as a DHCP client for dynamic IP configuration.

Perform the following steps if your computer is configured for manual IP configuration and you want to use dynamic IP configuration:

1. Select Start and type **`Network and Sharing Center`** into the Start menu's search box.
2. In the Network And Sharing Center window, click Local Area Connection in the View Your Active Networks section.
3. Click the Properties button in the Activity section of the Local Area Connection Status box.
4. In the Local Area Connection Properties dialog box, select Internet Protocol Version 4 (TCP/IPv4) and click the Properties button.
5. Choose Obtain An IP Address Automatically on the General tab of the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
6. Choose Obtain DNS Server Address Automatically on the General tab.
7. To use this configuration, click OK to accept the selection and close the dialog box. To exit without saving (if you had a valid static configuration), click Cancel.

Using APIPA

Automatic Private IP Addressing (APIPA) is used to automatically assign private IP addresses for home or small business networks that contain a single subnet, have no DHCP server, and are not using static IP addressing. If APIPA is being used, clients will be able to communicate only with other clients on the same subnet that are also using APIPA. The benefit of using APIPA in small networks is that it is less tedious and has less chance of configuration errors than statically assigning IP addresses and configuration.

APIPA is used with Windows 7 under the following conditions:

- When the client is configured as a DHCP client, but no DHCP server is available to service the DHCP request.
- When the client originally obtained a DHCP lease from a DHCP server, but when the client tried to renew the DHCP lease, the DHCP server was unavailable and the lease period expired.

APIPA uses a Class B network addresses space that has been reserved for its use. The address space is the 169.254.0.0 network where the range of 169.254.0.1–169.254.255.254 is available for host to assign to themselves.

The steps that APIPA uses are as follows:

1. The Windows 7 client attempts to use a DHCP server for its configuration, but no DHCP servers respond.
2. The Windows 7 client selects a random address from the 169.254.0.1–169.254.255.254 range of addresses and uses a subnet mask of 255.255.0.0.

   The client uses a duplicate-address detection method to verify the address it selected is not already in use on the network.
3. If the address is already in use, the client repeats steps 1 and 2. If the address is not already in use, the client configures its network interface with the address it randomly selected. If you note the number of the address the APIPA client can select from (65536 addresses), the odds of selecting a duplicate is very slim.

4. The Windows 7 network client continues to search for a DHCP server every five minutes. If a DHCP server replies to the request, the APIPA configuration is dropped and the client receives new IP configuration settings from the DHCP server.

You can determine if your network interface has been configured using APIPA by looking at your IP address. You can do this easily from the command interpreter using the `ipconfig /all` command.

Perform the following steps to view your IP address this way:

1. Click Start and enter **`cmd`** into the Start menu's search box.
2. Type **`ipconfig /all`** into the command interpreter.
3. Look at the Local Area Connection IP address. If your IP address is in the range of 169.254.0.1–169.254.255.254 and the text Autoconfiguration Enabled is present, as shown in Figure 11.34, your machine is using APIPA.

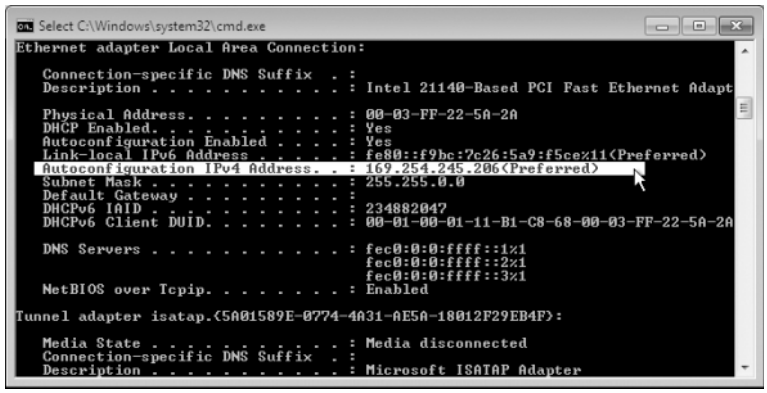


FIGURE 11.34
Autoconfigured IP address

USING MULTIPLE IP ADDRESSES

Windows 7 allows you to configure more than one network adapter in a single computer, an approach known as *multihoming*. You can also configure multiple IP addresses on the same network adapter in Windows 7, an approach known as logical multihoming. You would use logical multihoming if you had a single physical network logically divided into subnets and you wanted your computer to be connected with more than one subnet.

Perform the following steps to configure multiple IP addresses for a single network adapter:

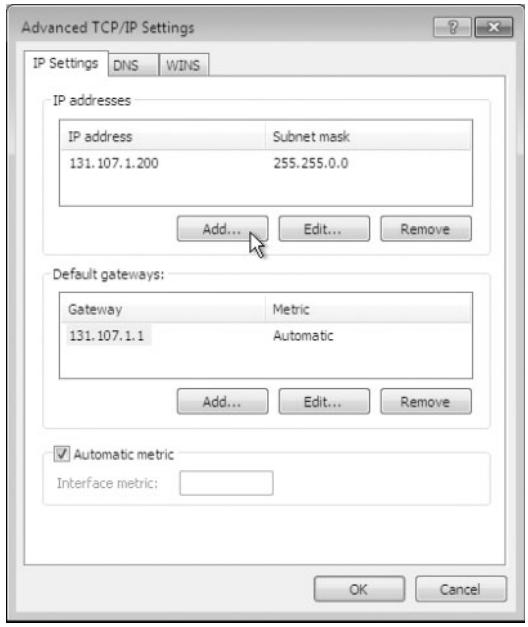
1. Select Start and type **Network and Sharing Center** in the Start menu's search box.
2. In the Network and Sharing Center window, click Local Area Connection in the View Your Active Networks section.
3. Click the Properties button in the Activity section of the Local Area Connection Status box.
4. In the Local Area Connection Properties dialog box, select Internet Protocol Version 4 (TCP/IPv4) and click the Properties button.
5. You will need to have a static IP address to use multihoming. Choose Use The Following IP Address in the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.

6. In the IP Address box, enter **131.200.1.200**; in the Subnet Mask box, enter **255.255.0.0**; and in the Default Gateway box, enter **131.107.1.1**.

> **USE A VALID ADDRESS FOR YOUR NETWORK**
>
> The example in step 6 is likely not a valid IP address on your network. You can substitute a valid address, subnet mask, and default gateway if you know them. If you click OK and see this is not a valid IP address for your network, you will lose connectivity!

7. Click the Advanced button to access the Advanced TCP/IP Settings dialog box. On the IP Settings tab in the IP Addresses section, click the Add button, as shown in Figure 11.35.

FIGURE 11.35
Advanced TCP/IP Settings dialog box



8. You add additional IP addresses by entering them into the TCP/IP address window launched in step 5 along with their subnet mask and then clicking Add. You can repeat this step to add additional IP addresses.

9. If you need to assign more than one default gateway to your IP configuration, use the Default Gateways section of Advanced IP Settings.

USING ALTERNATE CONFIGURATION

Alternate Configuration is designed to be used by laptops and other mobile computers to manage IP configurations when the computer is used in multiple locations and one location requires a static IP address and the other location(s) require dynamic IP addressing. For example, a user with a laptop might need a static IP address to connect to their broadband ISP at home, and then use DHCP when connected to the corporate network.

Alternate Configuration works by allowing the user to configure the computer so that it will initially try to connect to a network using DHCP; if the DHCP attempt fails (for example, when the user is at home), the alternate static IP configuration is used. The alternate IP address can be an APIPA or a manually configured IP address.

Perform the following steps to configure Alternate Configuration:

1. Select Start and type **Network and Sharing Center** in the Start menu's search box.
2. In the Network and Sharing Center window, click Local Area Connection in the View Your Active Networks section.
3. Click the Properties button in the Activity section of the Local Area Connection Status box.
4. In the Local Area Connection Properties dialog box, select Internet Protocol Version 4 (TCP/IPv4) and click the Properties button.
5. Select the Alternate Configuration tab in the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
6. The Automatic Private IP address radio button is selected by default. To create a static configuration if the DHCP server is unavailable, choose the User Configured radio button and enter the values for your Alternate Configuration.
7. Click OK to save your Alternate Configuration or reset to the default Automatic Private IP Address radio button and click OK, or click Cancel to abandon your changes and close the window.

Using IPv6 Addresses

Though most of this section we've been referencing TCP/IP as the network protocol, but you should remember that it is really a suite of protocols running in Layer 3 and Layer 4 of the OSI model. Internet Protocol (IP) is the Layer 3 protocol responsible for assigning end devices globally unique addresses (and we mean the whole company for private addresses to the whole Internet for public addresses). Back in the 1980s, it was unimaginable that we would ever need more than 4 billion addresses, but we do. They (the keepers of the Internet) realized in the 1990s that we were going to have a problem and decided that a new Layer 3 would be needed. This was not an easy task, and integration into the existing infrastructure was going to be long as well. They (the keepers of the Internet) came up with an interim solution while the new Layer 3 protocol became standardized. The interim solution is known as NAT and PAT. NAT/PAT allowed more than one device to use the same IP address on a private network as long as there was one Internet address available. Cool enough, but this is not the real solution.

IPv6 is the solution to the IPv4 address depletion. As time has progressed from the IPv4 standard acceptance in the 1980s, we have needed new and better functionality. However, given the way the standards process works around the world, you can add functionality but it may or may not be supported in any vendor's TCP/IPv4 network stack. What happened in IPv6 is not only did the address space increase in size, but the additional functionality that may or may not have been included before has become part of the IPv6 standard. For example, IPv4 is defined as having a variable-length header, which is cumbersome as we need to read an additional piece of data to see how big the header is. Most of the time it stays the same, so why not just fix its length and add perhaps an extension to the header if we need to carry more information? IPv6 uses a fixed-length IP header with the capability of carrying more information in an extension to the header known as an ''extension header.''

What about the Layer 4 piece, TCP and UDP? Those don't need to change; we're only changing Layer 3. What about the MAC address and the Ethernet specification? Those don't need to change, either; we're only changing Layer 3 (We'll have to add a new identifier for the Layer 2 header so we know to hand the data to IPv6.).

Microsoft has been including IPv6 in its operating systems since NT 4.0; it just has not been enabled by default. Windows 7 (as did Vista) natively supports both IPv4 and IPv6. The main differences you will notice between IPv4 and IPv6 is the format and size of the IP address. IPv6 addresses are 128 bits (IPv4 is 32 bits) and typically written as eight groups of four hex characters. IPv4 as you saw earlier is four decimal representations of 8 bits. Each of the eight groups of characters is separated by a colon. An example of a valid IPv6 address is 2001:4860:0000:0000:0012:10FF:FECD:00EF.

Leading zeroes can be omitted, so we can write our example address as 2001:4860:0:0:12:10FF:FECD:EF. Additionally, a double colon can be used to compress a set of consecutive zeroes, so we can write our example address as 2001:4860::12:10FF:FECD:EF. The IPv6 address is 128 bits; when you see a double colon, it's a variable that says fill enough zeros within the colons to make the address 128 bits. You can only have one set of double colon — two variables in one address is not going to work.

Will we see IPv6 take over the Global Address space soon? Even with IPv4's lack of address space, we are going to continue to use it for many years. The integration of IPv6 into the infrastructure is going to happen as a joint venture, with IPv4 and IPv6 running at the same time in the devices and on some networks.

There are many mechanisms for enabling IPv6 communications over an IPv4 network, including the following:

- Dual Stack, which involves a computer or device running both the IPv4 and IPv6 protocol stacks at the same time
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)
- 6to4, which is an encapsulation technique for putting IPv6 addresses inside IPv4 addresses
- Toredo Tunneling, which is another encapsulation technique for putting IPv6 traffic inside an IPv4 packet

Some IPv6-to-IPv4 dynamic translation techniques require that a computer's IPv4 address be used as the last 32 bits of the IPv6 address. When these translation techniques are used, it is common to write the last 32 bits as you would typically write an IPv4 address, such as 2001:4850::F8:192.168.122.26.

Testing IP Configuration

After you have installed and configured the TCP/IP settings, you can test the IP configuration using the `ipconfig`, `ping`, and `nbtstat` commands. These commands are also useful in troubleshooting IP configuration errors. You can graphically view connection details through the Local Area Connection Status of the Network And Sharing Center.

Using the `ipconfig` Command

The `ipconfig` command displays your IP configuration. Table 11.5 lists the command switches that you can use with the `ipconfig` command.

TABLE 11.5: `ipconfig` Switches

SWITCH	DESCRIPTION
/?	Shows all of the help options for `ipconfig`
/all	Shows verbose information about your IP configuration, including your computer's physical address, the DNS server you are using, and whether you are using DHCP
/allcompartments	Shows IP information for all compartments
/release	Releases an IPv4 address that has been assigned through DHCP
/release6	Releases an IPv6 address that has been assigned through DHCP
/renew	Renews an IPv4 address through DHCP
/renew6	Renews an IPv6 address through DHCP
/flushdns	Purges the DNS Resolver cache
/registerdns	Refreshes DHCP leases and re-registers DNS names
/displaydns	Displays the contents of the DNS Resolver Cache
/showclassid	Lists the DHCP class IDs allowed by the computer
/setclassID	Allows you to modify the DHCP class ID

Perform the following steps to use `ipconfig` to view your IP address configuration:

1. Select Start and type **cmd** into the Start menu's search box or choose Start ➢ All Programs ➢ Accessories ➢ Command Prompt.
2. In the Command Prompt dialog window, type **ipconfig** and press Enter. Note the IPv4 address as well as the IPv6 address.
3. In the Command Prompt dialog box, type **ipconfig /all** and press Enter. You now see more information such as the Ethernet address, IPv6 tunnel parameters, and their interface identifiers. Close the Command Prompt window when you have finished viewing the information by typing **exit** or closing the window.

Using the `ping` Command

The `ping` command is useful for verifying connectivity between two IP devices. The command sends an Internet Control Message Protocol (ICMP) Echo Request message to a remote machine and receives an ICMP Echo Reply message back if the remote device is able to respond.

You can ping a computer based on the computer's IPv4 address, IPv6 address, hostname (DNS resolves), or NetBIOS name (WINS resolves). The following list shows examples of `ping`:

- `ping 131.107.1.200`
- `ping 2001:4860::12:10FF:FECD:EF`
- `ping www.google.com`
- `ping windows7-pc-1`

If you are having trouble connecting to a host on another network, `ping` could help you verify that a valid communication path exists. You might ping the following addresses:

- The IPv4 loopback address, 127.0.0.1
- The IPv6 loopback address, ::1
- The local computer's IP address
- The local router's (default gateway's) IP address
- The remote computer's IP address

If `ping` failed to get a reply from any of these addresses, you would have a starting point for troubleshooting the connection error. The error messages that can be returned from a ping request include the following:

Request Timed Out Means that the Echo Reply message was not received from the destination computer within the time allotted. By default, destination computers have 4 seconds to respond.

TTL Expired In Transit Means the packet exceeded the number of hops specified to reach the destination device. Each time a packet passes through a router, the Time To Live (TTL) counter is decremented and reflects the pass through the router as a hop. If the TTL reaches 0, this message is returned.

Destination Host Unreachable Generated when a local or remote route path does not exist between the sending host and the specified destination computer. This error could occur because the router is misconfigured or the target computer is not available.

Ping Request Could Not Find Host Indicates the destination hostname couldn't be resolved. You should verify the destination hostname was properly specified, that all DNS and WINS settings are correct, and that the DNS and WINS servers are available.

Using the `nbtstat` Command

NBT is NetBIOS over TCP/IP, and the `nbtstat` command is used to display TCP/IP connection protocol statistics over NBT. Table 11.6 lists the command-line options that you can use.

TCP/IP Troubleshooting

If you are having trouble connecting to network resources, you might want to check the following:

- If you can access resources on your local subnet but not on a remote subnet, you should check the default gateway settings on your computer. Pinging a remote host and receiving a Destination Unreachable message is also related to default gateway misconfiguration.

- If you can access some but not all resources on your local subnet or remote subnet, you should check your subnet mask settings, the wiring to those resources, or the devices between your computer and those resources.
- Use the `ipconfig` command to ensure you are not configured with an APIPA address. If so, determine why you are not receiving IP settings from your DHCP server.
- If you can access a resource (for example, by pinging a computer) by IP address, but not by name, you should check the DNS settings on your computer.

TABLE 11.6: `nbtstat` Command-Line Options

SWITCH	OPTION	DESCRIPTION
/?	Help	Shows all of the help options for `nbtstat`
-a	adapter Status	Shows adapter status and lists the remote computer's name, based on the hostname you specify
-A	Adapter Status	Shows adapter status and lists the remote computer's name, based on the IP address you specify
-c	cache	Displays the NBT cache of remote computers through their names and IP addresses
-n	names	Shows a list of the local computer's NetBIOS names
-r	resolved	Shows a list of computer names that have been resolved through either broadcast or WINS
-R	Reload	Causes the NBT remote cache name table to be purged and reloaded (must be logged on as an administrator with privilege elevation)
-S	Sessions	Shows the current sessions table with the destination IP addresses
-s	sessions	Shows the current sessions table and the converted destination IP address to the computer's NetBIOS name
-RR	Release Refresh	Sends a Name Release packet to the WINS server and then starts a refresh

The Bottom Line

Set up hardware to provide network connectivity. After installing a new piece of hardware into Windows 7, the operating system goes through a process of discovery and installation. This goes smoothly most of the time, although occasionally, you must step in as the administrator and correct an issue.

Master It You have just installed a new network adapter into one of your Windows 7 machines. The operating system discovered the new device and installed the driver, but the

adapter doesn't work. You checked Device Manager and the network adapter appears to have been installed with a generic network adapter driver. You have a disk with the correct driver for Windows 7. How do you install a network adapter driver from a disk supplied by the hardware vendor to allow Windows 7 to use the NIC to connect to the network?

Connect to network devices. Windows 7 offers many enhancements for administrators to connect to network devices. One option that can make implementation easier is to connect to a network capable projector.

Master It One of your training rooms has a new overhead projector that has the capability of being connected to the network and displaying information from the connection. Tim, the instructor, just received a new machine in the classroom running Windows 7 and has asked you to configure the machine to use the network projector to present his PowerPoint presentations. The projector has an IP address of 172.25.2.100. How will you set up a network projector option in Windows 7 to allow PowerPoint to display using the current network infrastructure rather than a video cable in your classroom?

Set up peer-to-peer networking. Having the ability to share resources has been one of Windows' main features since network capability was added to the operating system. Each release of Windows has added new or enhanced functionality to peer-to-peer networking and Windows 7 is no exception with the addition of HomeGroups.

Master It How can you use the HomeGroup functionality in Windows 7 to allow users in the remote office to share file and printer resources with each other.

Configure network protocols. In order to allow machines to communicate through a network, network protocols must be installed and configured on each device. As administrators, we can use dynamic methods to configure our users machines, but sometimes we may need to manually configure the network protocol.

Master It As a network administrator, you are responsible for ensuring users have a proper network configuration to access the network. Your network is setup for DHCP for the client machines. One of your users currently set up as a DHCP client needs to have a static IP address due to the use of a specific application. How do you configure a Windows 7 client machine that is set up as a DHCP client to have a Static IPv4 address of 172.16.1.50 with a subnet mask of 255.255.255.0 and a default gateway of 172.16.1.1?