CHAPTER 6

Network Navigation

As a systems professional, there's one thing that is almost always on your mind: the network. It matters to you when it's down. It matters to you when it's up (it could be running better, of course…). And it matters to you when a new way to do an old trick comes around.

There's some good news. With Windows Vista, Microsoft has made big improvements on what have become old yet familiar technologies. In the process, they've made connecting to and navigating networks much easier. Have they invented the perfect operating system? No, of course not, but what they do offer is a lot better than what was there before.

This chapter is all about what's new in the Vista world of networking and also explains how to teach the new dog some old tricks. We'll talk about how you can navigate your network, and examine and manage its various and sundry settings. We'll also take a closer look at wireless networks, which takes a huge leap in accessibility and configuration in Windows Vista. Before we get into the nuts and bolts, let's take a quick look at some of the new technologies that promise to make your network a better place to work.

WHAT'S NEW IN VISTA NETWORKING

While the obvious differences between Windows XP and Vista are cosmetic, there's a lot going on under Vista's hood. Vista—along with its server partner, currently codenamed "Longhorn," but slated to be called Windows Server 2007—features a number of improvements in the way networking takes place. We have already talked about its Next Generation TCP/IP Stack, which uses both IPv4 and IPv6.

New and Improved

The first stop is to examine what is new to Windows Vista. Depending on your organization and its networking needs, some of these things may not be as important as others. On the other hand, some may be exactly the sorts of things you've needed to get the most out of your network.

QoS

Audio and video traversing a network is becoming more commonplace, both on home and corporate networks. Because audio and video packets generally need priority over other packets to avoid playback problems, Microsoft has enhanced Quality of Service (QoS) in Vista. Of course, it isn't just multimedia that benefits from Vista's policy-based QoS mechanisms. Networks of any complexity and with any need can prioritize which packets get preferential treatment.

For example, if yours is a network routinely used for transferring large files to workstations, you might use the new QoS tools to tell the network to give those packets priority over such packets as e-mail or Web traffic.

SMB

The Windows file-sharing protocol Server Message Block (SMB) 1.0 was introduced more than 15 years ago. As time has marched by and networks evolved, SMB's shortcomings needed to be addressed. With Vista, SMB is reintroduced with version 2.0, and it allows such enhancements as:

- Multiple commands can be handled within one packet. This reduces the amount of traffic that traverses the network between the server and client.
- Larger buffer sizes are allowed over SMB 1.0
- Support for symbolic links is provided
- It can handle short interruptions in network availability.

Http.sys

Http.sys, the kernel-mode driver that services Hypertext Transfer Protocol (HTTP), has also been improved over earlier versions. Ultimately, HTTP is enhanced for users, providing a smoother, more robust experience. Improvements include:

- Server-side authentication
- Logging
- Netsh commands, which will be examined later in this chapter
- Performance counters

Peer-to-Peer Networking

Initially introduced with the Advanced Networking Pack for Windows XP, Windows Peer-to-Peer Networking is an operating system platform and application programming interface (API) that allows the development of peer-to-peer (P2P) applications. In Vista, Windows Peer-to-Peer Networking includes:

- An easy-to-use API
- A new version of the Peer Name Resolution Protocol (PNRP)
- The dynamic discovery of other users on the local subnet
- Netsh configuration support
- Group Policy configuration support, that allows P2P settings to be managed from Group Policy

Retired Technologies

While Vista adds some new and interesting technologies, it removes several others. The following networking technologies were available up until Windows XP, but you won't find them in Vista:

- Bandwidth Allocation Protocol (BAP)
- X.25

- Serial Line Interface Protocol (SLIP)
- Asynchronous Transfer Mode (ATM)
- IP over IEEE 1394
- NWLink IPX/SPX/NetBios Compatible Transport Protocol
- Services for Macintosh (SFM)
- Open Shortest Path First (OSPF) routing protocol in Routing And Remote Access
- Basic Firewall in Routing And Remote Access
- Static IP filter APIs in Routing And Remote Access

This section gave just the quickest overview of what's brand new in Vista that was worth mentioning and what was removed. Let's take a closer look at the applications that you'll regularly come into contact with while using Vista on your network.

THE NETWORK AND SHARING CENTER

Unless you have intimate knowledge of a network's design, unless you've committed its topology to memory, and unless there have been no changes made to said design, just sitting down at a PC and trying to discern everything about that network can be difficult. Microsoft has tried to make network navigation easier in Windows Vista, thanks to a component called the Network And Sharing Center. The Center makes it a lot easier to gather information about how a workstation is connected to its network and how you can configure that workstation to work with the network.

Like so many other things in Vista, the Network And Sharing Center has its roots in earlier versions of Windows. If you hop in your time machine and set the dial for 1995, you might remember seeing Network Neighborhood in Windows 95. That tool gradually evolved into My Network Places in Windows XP. In Windows Vista, the tool is called simply Network. To start this option, simply click the Start button, and then click Network. The resulting screen looks like the one in Figure 6-1.

In many ways, Network behaves a lot like Network Neighborhood—clicking it displays all the computers in the current domain. By double-clicking any of the computers, you can access its shared resources.

By clicking the Network And Sharing Center option, a screen like the one in Figure 6-2 appears.

As you can see in the figure, the Network And Sharing Center is made up of a few components, which we will discuss in the next section.

Meet the Network And Sharing Center

There are several ways to access the Network And Sharing Center. In addition to the aforementioned method, you can start the Network And Sharing Center as follows:

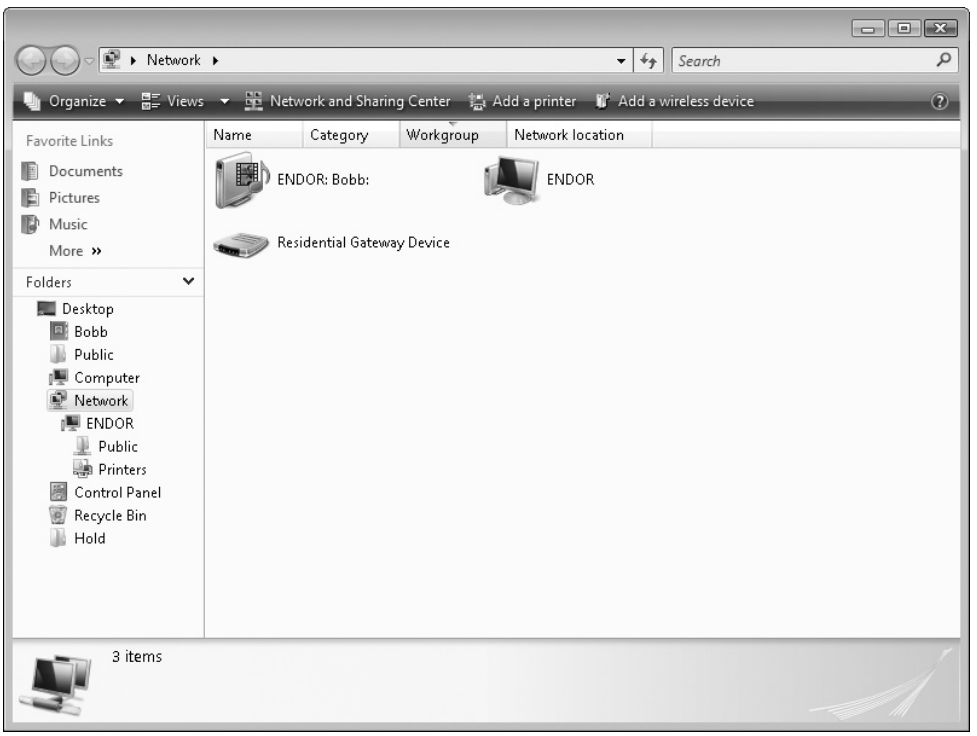

Figure 6-1. Windows Vista's Network is reminiscent of Network Neighborhood from Windows 95.

1. Click Start and then click Control Panel.
2. In Control Panel, under Network And Internet, click View Network Status And Tasks.

When you've started the Network And Sharing Center, you can use it to manage your network settings and status.

There are four areas within the Network And Sharing Center:

- **Network map** This presents a visual representation of the network's infrastructure. This map shows if you are connected to a network and whether you can access the Internet through that connection. If you click View Full Map, an extended network map is displayed.
- **Network details** This presents details about the network to which the computer is connected. By following the links, you can manage the connections and the networks to which they are linked.

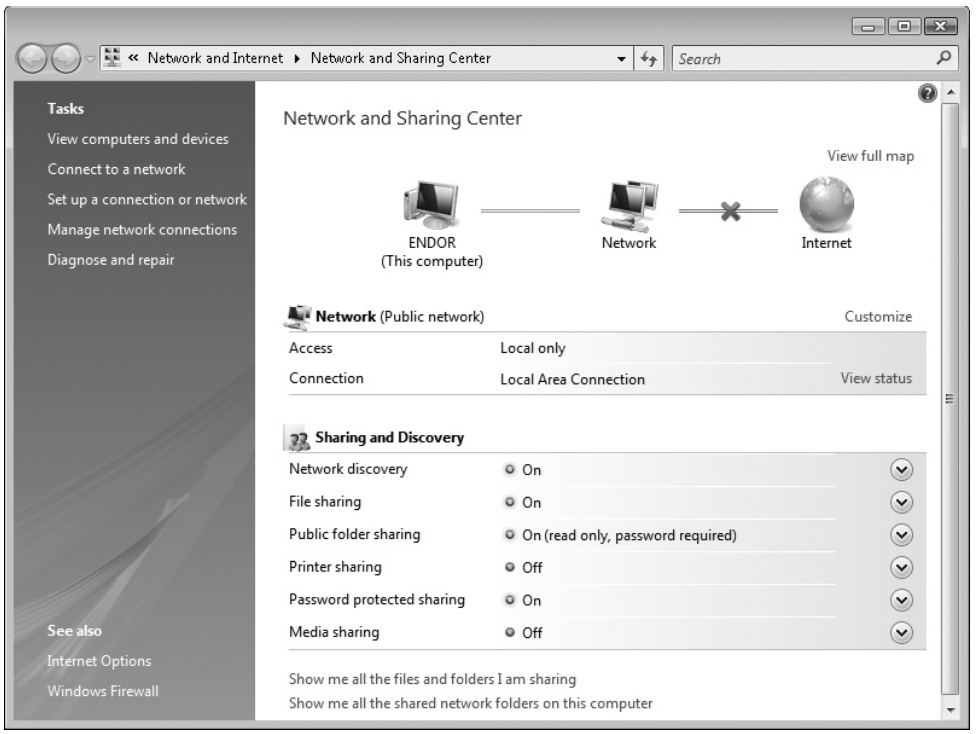

Figure 6-2. The Network And Sharing Center shows an overall look at network connectivity.

- **Sharing and discovery** This presents a summary of the computer's firewall, detection, and sharing settings. These options will vary, depending on the computer's configuration, and include Block, Allow, and View Sharing Settings.
- ▲ **Tasks** These are additional tasks, listed in the left pane, that can be started from elsewhere in Windows Vista, but are convenient to have handy in this context.

Let's examine these sections in more depth.

Network Map

Consider again the Network And Sharing Center. It shows the workstation you're using passing through a local network, with a subsequent connection to the Internet. Above the Internet icon, there is an option to view a full map of the network. If you click the View Full Map link, you'll see all the devices on your network. This is shown in Figure 6-3.

Vista does this by using Microsoft's link-layer protocol. As you may remember from Chapter 5, the protocol is used to both announce a device's presence on the network and map out devices on the network.

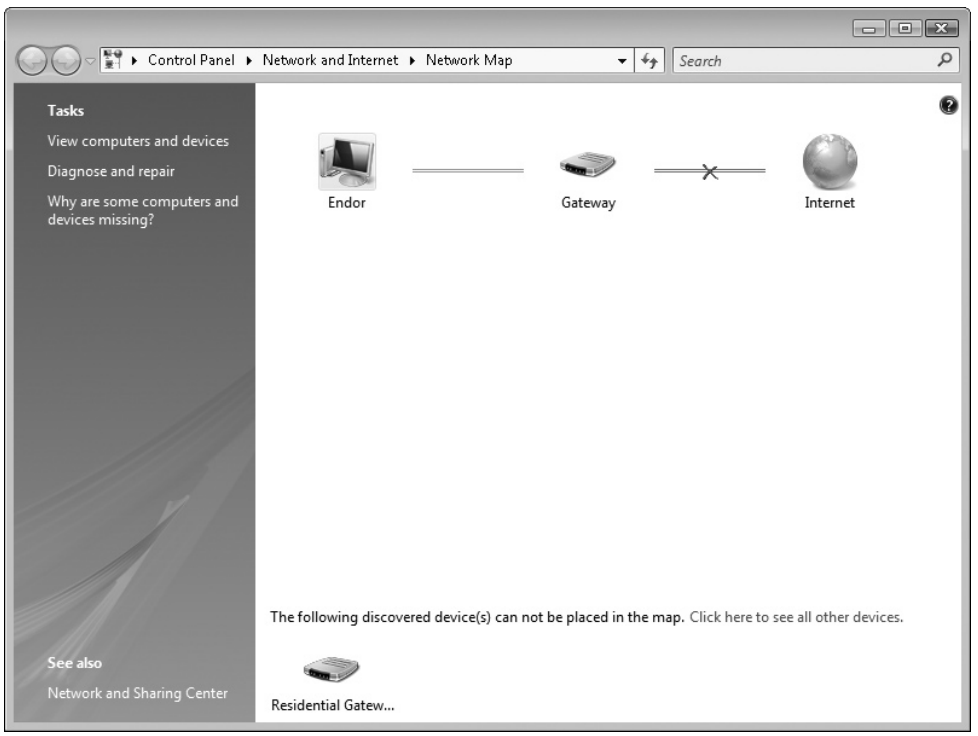

Figure 6-3. Clicking the View Full Map link gives a comprehensive overview of devices on your network.

NOTE If you have an Xbox plugged into your network, it will be shown on this map, as it also uses the link-layer protocol to announce its presence.

Network Details

By clicking the View Status link, you'll see a dialog box like the one shown in Figure 6-4.

The box should look familiar to Windows XP users—it's basically the Properties dialog box that so many of us have seen. However, here, it has been retooled for a Vista environment, including IPv6 details.

Sharing and Discovery

There are a couple of differences in how resource sharing works in Vista when compared to Windows 2000/XP. Vista uses the Public folder, unlike the user's Shared Documents folder in Windows XP, to simplify file sharing. In fact, simple file sharing is enabled by default in

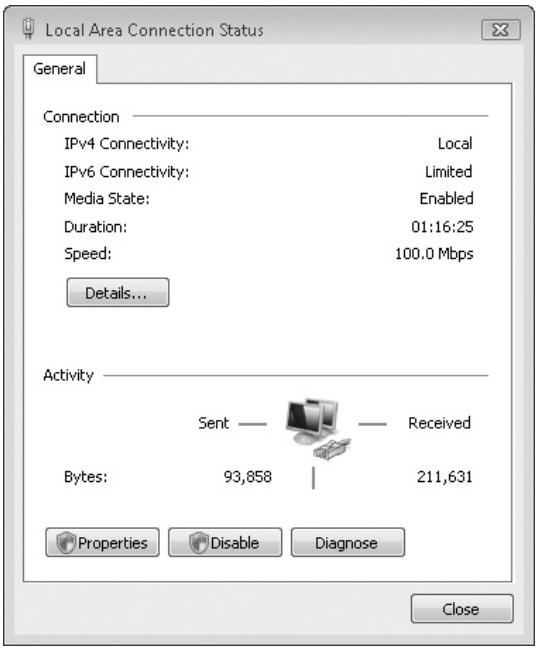

Figure 6-4. The View Status link takes you to a dialog box that shows current conditions for your connection.

Windows XP Home Edition and XP Professional when not joined to an Active Directory domain. By default, Vista does not allow simple file sharing. Access to shared folders requires a user name and password. The Sharing And Discovery area is shown in Figure 6-5.

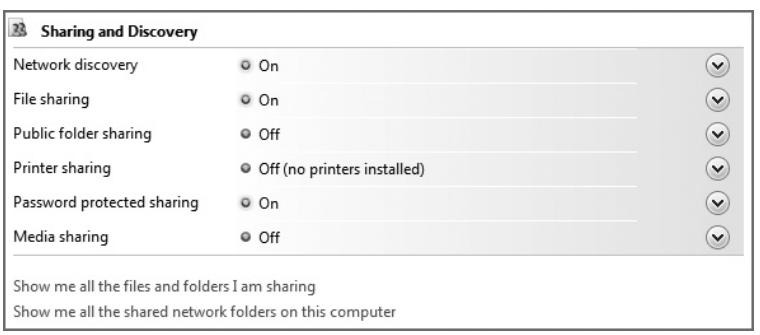

Figure 6-5. The Sharing And Discovery area centralizes resource-sharing configuration.

Your options for configuring resource sharing in the Sharing And Discovery area are explained in the following sections. Each area includes two or more options that are displayed by clicking the down arrow to the right of the option line.

Network Discovery By setting Network Discovery to "on," you activate the network map and make the workstation visible on the network maps of other workstations. The workstation can see other members of the workgroup or domain, and it can be seen by those other stations. Network Discovery is a requirement for sharing files and printers, as well as for accessing shared resources on other workstations. When connecting to a network, you choose the network location (domain, private, or public), and Vista sets Network Discovery to "on" or "off" based on your choice. For domain-controlled networks, Network Discovery is turned off by default and is managed by Group Policy. For private locations, Network Discovery is on by default.

When you select the network location, Windows Firewall will open the necessary ports to allow resource-sharing traffic. If you manage Windows Firewall using Group Policy, you will want to ensure that the ports in Table 6-1 are set according to your needs. If you use a firewall other than Windows Firewall, you must configure it to allow network discovery and file and printer-sharing traffic. The network ports used to support resource sharing include those listed in Table 6-1.

File Sharing Turn on file sharing to make files and printers that you have shared accessible to other workstations and devices on your network. You can access shared folders and devices on other workstations and servers, although the local sharing may be disabled. Turning file sharing on for the local workstation is not required if you wish to access network resources. The File Sharing option in the Network And Sharing Center affects whether the local workstation will advertise and allow access to local resources.

Purpose	Ports
For network discovery of other computers running Vista	UDP 3702 TCP 5357 TCP 5358
For network discovery of computers running Windows XP, as well as file and printer sharing for both Vista and Windows XP	UDP 137 UDP 138 TCP 139 TCP 445
For network discovery of network devices	UDP 1900 TCP 2869

Table 6-1. Resource Sharing Ports Managed by the Windows Firewall

The File Sharing feature is turned off by default. For domain network locations (domain member workstations), File Sharing is managed by Group Policy. To turn File Sharing on:

1. In the Sharing And Discovery section of the Network And Sharing Center window, click the down arrow next to File Sharing.
2. Within the File Sharing settings area, select Turn On File Sharing, and then click Apply.

After enabling file sharing, you then must configure each folder that you wish to share. Chapter 7 has more details on how to share files and devices.

Public Folder Sharing Vista provides a quick and easy way for all users that log on to a workstation to share files. Although it can be administratively disabled, by default, each installation of Vista includes a folder named "Public" that resides in the Users container. The Public folder is configured to enable all interactive, or locally logged on, users to read and write to a shared repository. By sharing it, the public folders and all of the folders within it are automatically shared.

Sharing files through the Public folder does not replace traditional file sharing. You can always share files directly from any folder on the workstation without copying or moving them to the Public folder (provided that file sharing is enabled). This method gives you more control over who you share files with on your network. It allows you to select people on an individual basis and set the level of sharing permissions for each person.

The Public folder (which is shown in Figure 6-6) contains no files by default. Any user who logs on locally can add files. The Public folder contains several subfolders to organize files, including:

- Public Documents
- Public Downloads
- Public Music
- Public Pictures
- Public Videos

As a shared storage area, no one should store files in the Public folder that they do not wish others to see. The Public folder is a good place for any file you want to share with the people who have given access to it. Settings for sharing the Public folder are shown in Figure 6-7.

You can control who will have access to the Public folder. You can also set the level of access by choosing between the three options:

- Turn On Sharing So Anyone With Network Access Can Open Files
- Turn On Sharing So Anyone With Network Access Can Open, Change, And Create Files
- Turn Off Sharing (People Logged On To This Computer Can Still Access This Folder)

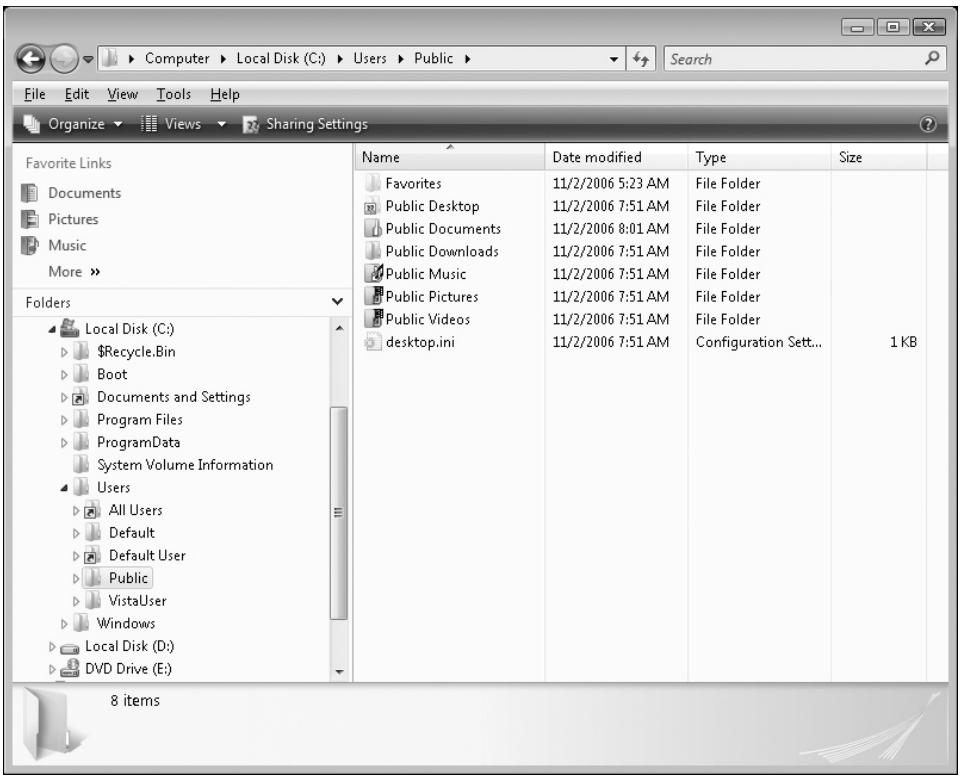

Figure 6-6. Public folder sharing gives you the option to share files quickly and simply.

Printer Sharing Until the Printer Sharing feature is enabled, no local printers can be shared. By enabling it, any personal or workgroup printers that are attached directly to the Vista workstation can be accessed by any user on your network. To enable printer sharing:

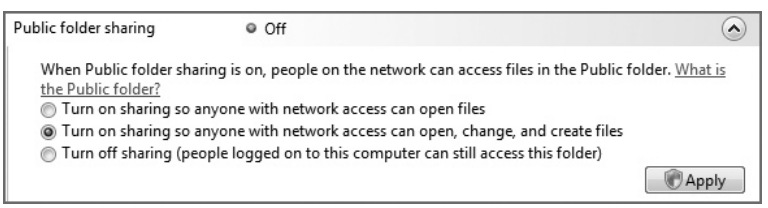

Figure 6-7. Turn on public folder sharing, and set the default level of access.

1. In the Sharing And Discovery section of the Network And Sharing Center window, click the down arrow next to Printer Sharing.
2. Within the Printer Sharing settings area, click Turn On Printer Sharing, and then click Apply.

None of your printers are shared at this point. However, the workstation is now configured to allow printer sharing. You have to visit each printer you wish to share and configure it, establishing with whom you wish to share the printer and what rights you wish to give them. Chapter 7 includes more details on how to share and access shared printers.

Password-Protected Sharing To require authentication to your shared folders and printers, enable the Password-Protected Sharing feature. Users will not be able to access your shared folders and printers without providing a user name or password that corresponds to an account that has been given permission to view, modify, or add to a folder or print to a printer. When a user on another workstation tries to connect to the shared folder or printer, he or she provides a user name and password of the account that they use to log on to their own computer.

When you disable password-protected sharing, the computer sharing the folder does not require a user account or password. Anyone on your network can access the shared folders of the computer (provided the folder was shared for the Guest or Everyone account). This behavior is equivalent to simple file sharing in Windows XP.

To disable password-protected sharing:

1. In the Sharing And Discovery section of the Network And Sharing Center window, click the down arrow next to Password-Protected Sharing.
2. Within the Password-Protected Sharing settings area, click Turn Off Password-Protected Sharing, and then click Apply.

Media Sharing Sharing music, video, and pictures may be appropriate for a workstation. You can stream these items from your workstation to devices that are connected to the wired or wireless home network. You may have a library of presentations for any number of business functions, such as product demonstrations, sales presentations, or other training. Windows Media Player 11 is specially enhanced to navigate media sharing on the Vista platform. By default, the Media Sharing feature is disabled in all network locations. To enable it:

1. In the Sharing And Discovery section of the Network And Sharing Center window, click the down arrow next to Media Sharing. This is shown in Figure 6-8.
2. Within the Media Sharing settings area, click Change.
3. In the new Media Sharing window that opens, select the Share My Media With check box, and click OK. Another new window opens, with any media player devices available on your network that can potentially access your files. Media player devices can be any workstation, personal digital assistant (PDA), or other handheld device with Windows Media Player 11 installed and configured accordingly.

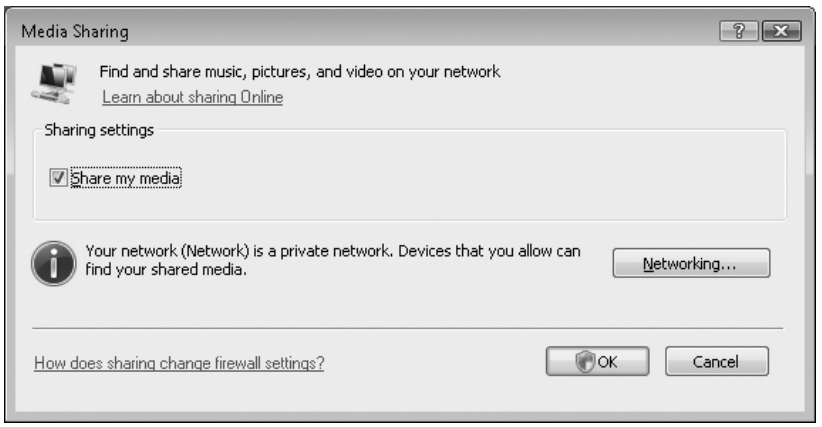

Figure 6-8. Windows Vista allows you to select whether you will share media content.

4. Among the items that appear in the box, select those that you wish to share media with, and click the Allow button. This is shown in Figure 6-9.
5. You can be more specific about what you would like to share by clicking the Customize button. You can choose to share only pictures, video, or music files. By selecting the Allow New Devices And Computers Automatically check box, you will open your media to all users on any network you may join. The types of media you can share are shown in Figure 6-10.

In addition to computers on your network, media devices attached to computers or the network will be able to access your content. Vista warns you about this, as Figure 6-11 shows.

You can share nearly any digital media file in your Media Player library, including protected Windows Media files that you have downloaded from online stores. To share a file in your library, the original file must be stored in one of your monitored folders (by default, the folders where digital media files are stored, including the My Music, My Pictures, and My Videos folders). For information about monitored folders, see Windows Media Player Help. In addition, the file must be of one of the following types:

- Music files, such as Windows Media Audio (.wma), MP3 (.mp3), and WAV (.wav) files. Note that audio CDs that are inserted into your workstation cannot be shared.
- Video files, such as Windows Media Video (.wmv), AVI (.avi), MPEG-1 (.mpeg, .mpg), and MPEG-2 (.mpeg, .mpg) files. Note that DVD-video discs that are inserted into your workstation cannot be shared.

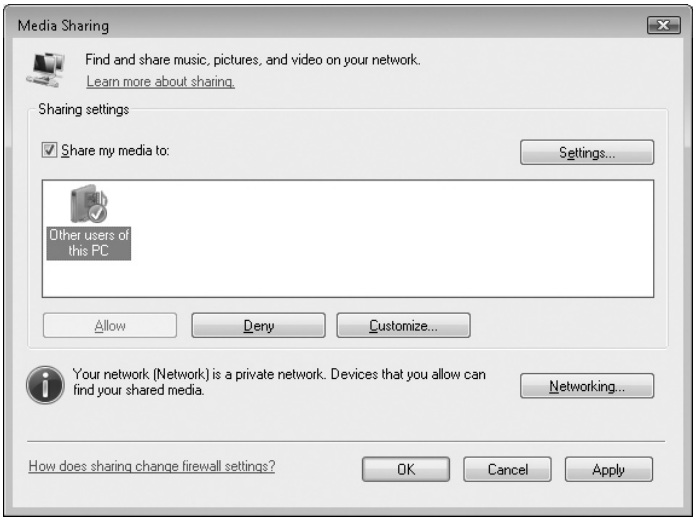

Figure 6-9. You can select with whom you will share media content.

- Picture files, such as JPEG (.jpeg, .jpg), portable network graphics (.png), and Windows Media Photo (.wpd) files.
- Playlists, such as Windows Media playlist (.wpl) and MP3 playlist (.m3u) files.

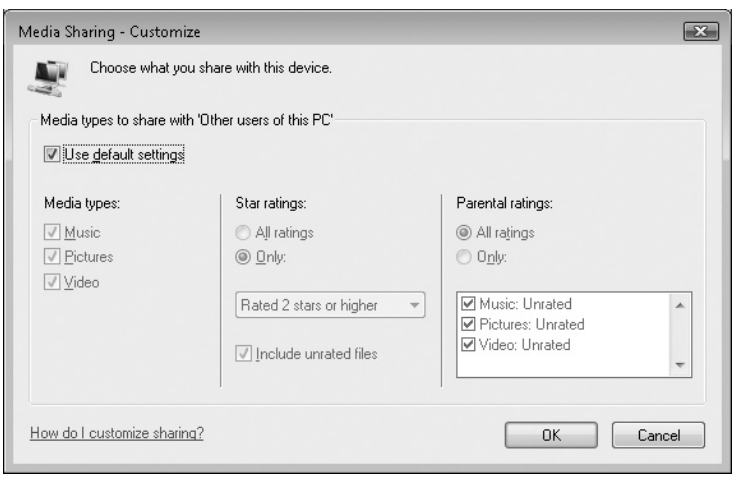

Figure 6-10. Customize access to your media for all workstations or per workstation.

Figure 6-11. Allow computers to automatically access your media only after careful consideration of the security implications.

Depending on how your computer is configured, Media Player might be able to share other music, video, and picture file types in addition to those listed here.

Windows Vista makes the process of configuring common network access and sharing tasks simple through its Sharing And Discovery settings area. The relevant settings are described in Table 6-2, along with their options.

At the bottom of the Network And Discovery section of the dialog box are two links that allow you to see which folders you are sharing on the network and all shared network folders that are on the computer (see Figure 6-12).

Tasks

In the leftmost pane of the Network And Sharing dialog box is a list of tasks that can be performed. We've already discussed a few of these tasks in Chapter 5—connect to a network, set up a connection or network, and manage network connections—but we'll touch on them a bit more in this section. However, there are a couple of other tasks that we haven't talked about yet.

By clicking Windows Firewall at the bottom of the pane, you can manage your computer's firewall settings. Clicking that link brings up a screen like the one shown in Figure 6-13.

To change the firewall's configuration, click the Change Settings link, and the resulting dialog box appears like the one shown in Figure 6-14.

By clicking Block, Windows Firewall blocks all access to the network, and you cannot access other computers on the network or the Internet. Likewise, no other computers will be able to access your computer.

You can unblock the computer by clicking Allow. This sets the computer's firewall to a normal configuration. In this mode, you can access other computers on the network or the Internet. Likewise, other computers can access your computer.

NOTE Windows Firewall can be configured from the Network And Sharing Center by clicking View Sharing Settings. This opens the Windows Firewall dialog box, which you can use to manage its configuration.

Setting	Description	Options
Network Discovery	When this setting is turned on, the computer can see other devices on the network, and this computer will be visible to other devices.	On or off.
File Sharing	When this setting is turned on, files and printers that you have designated as sharable will be available on the network.	On or off.
Public Folder Sharing	When turned on, people on the network can access files in the Public folder.	Turn on sharing so that anyone with network access can open files, change, or create files. Turn off sharing (anyone logged on to the computer can still access files).
Printer Sharing	When turned on, people connected to the network can access printers connected to this computer.	On or off.
Password-Protected Sharing	When turned on, only people with a user account on this computer can access shared files, printers attached to the computer, and the Public folder.	On or off.
Media Sharing	When turned on, others connected to the network can access shared music, pictures, and video, and this computer can find those types of files on the network.	On or off. If this setting has not already been configured, Vista will ask you whether you want to share your media and with whom you want to share it, as explained earlier.

Table 6-2. Network And Sharing Center Settings

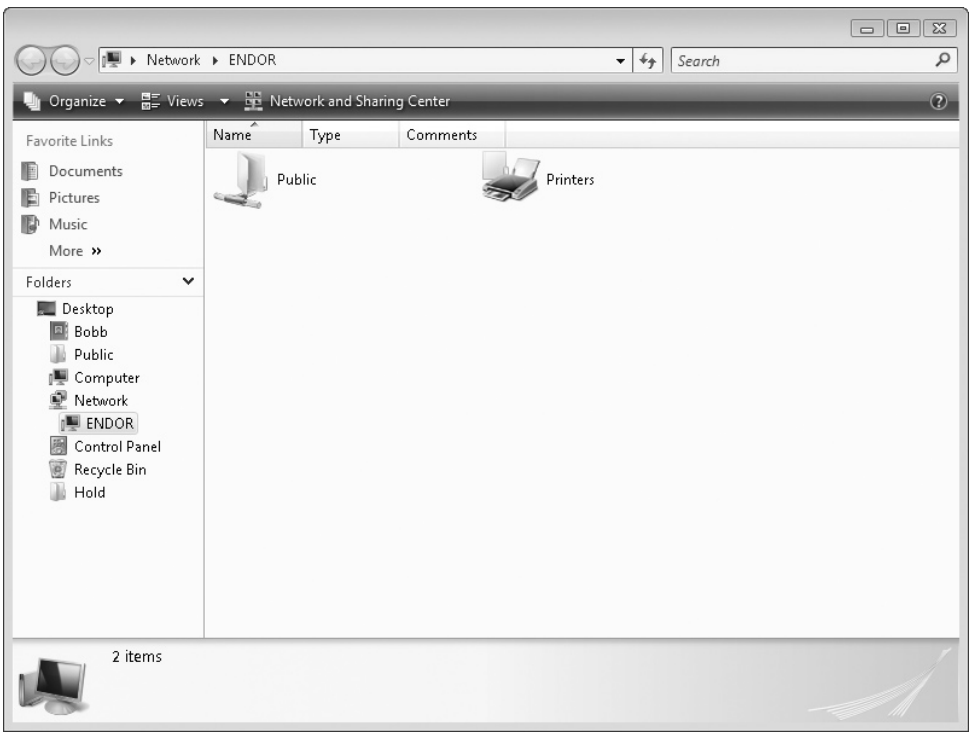

Figure 6-12. In the Network And Discovery area of the Network and Sharing dialog box, you can see which folders and printers are shared by your computer.

Troubleshooting

When your computer is disconnected from a network, the Network And Sharing Center shows an X through the connection. This is an obvious way of letting you know that you aren't connected to the Internet or a network.

To fix this problem, you start troubleshooting as you would with any other type of network—check network cables and wireless adapters. If they are appropriately plugged in, click Diagnose And Repair in the left pane to start the new Windows Network Diagnostics Tool, as shown in Figure 6-15.

This tool provides step-by-step instructions to fix your networking problem. For example, Figure 6-16 shows a window telling the user to connect a network cable to the network adapter. Once you plug in the cable and click the Diagnostics button, the tool will complete the repair. If the tool still detects a problem, it will continue troubleshooting the connection. Ideally, however, you'll see a message that the problem has been fixed.

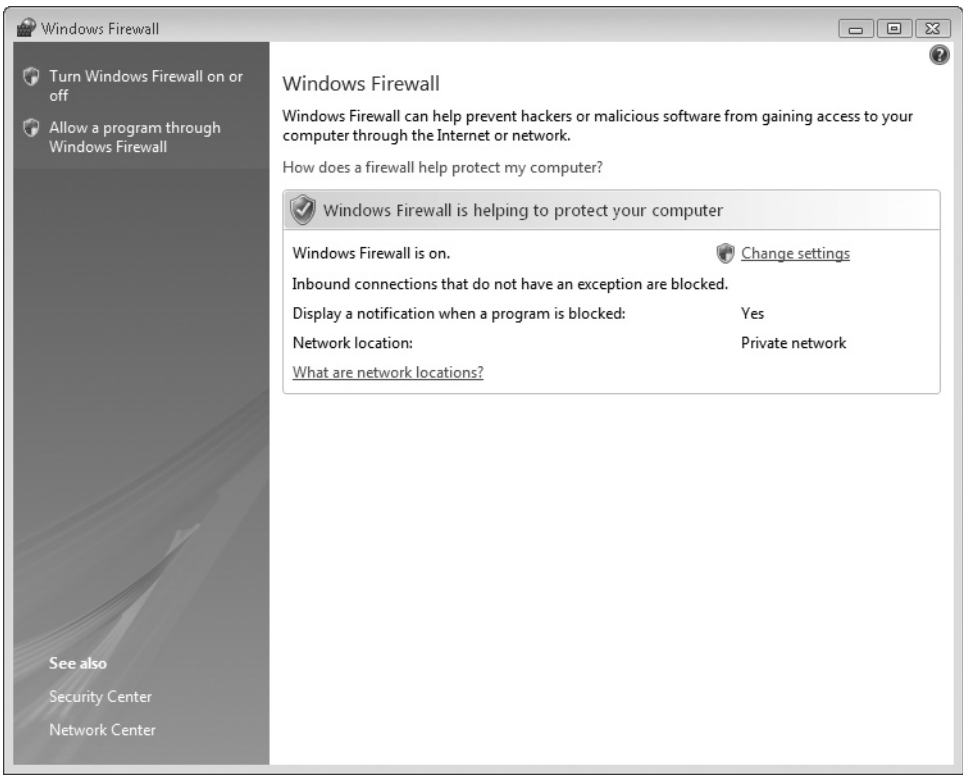

Figure 6-13. Windows Firewall settings can be managed from the Tasks pane on the Network and Sharing dialog box.

Managing Networks

Computers and devices in your network can be examined in the Network Center by clicking Browse The Network in the left pane. Depending on the type of network you have (domain or workgroup), your interaction will vary:

- ▼ If yours is an Active Directory domain, options in the Network View toolbar allow you to search Active Directory, connect to a domain, or return to Network Center.
- ▲ If yours is a workgroup, options in the Network View toolbar allow you to connect to a network or return to the Network Center.

Double-clicking a computer while browsing a network will allow you to see devices associated with the computer, like printers, external hard drives, and so forth.

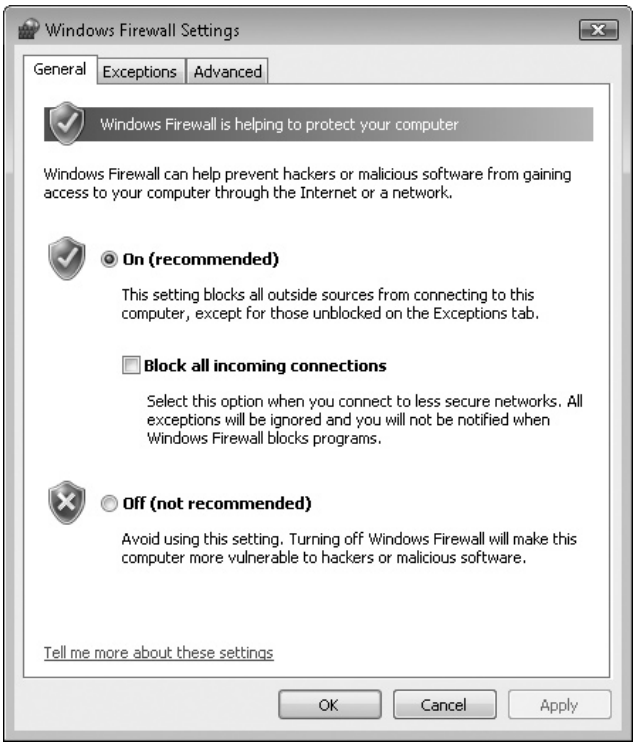

Figure 6-14. Windows Firewall Settings are easily managed through the various options.

Network connections can be created in the Network Center by clicking Connect To in the left pane and then clicking Create A New Connection in the Connect To A Network dialog box. This opens the Connect To A Network Wizard, which is shown in Figure 6-17.

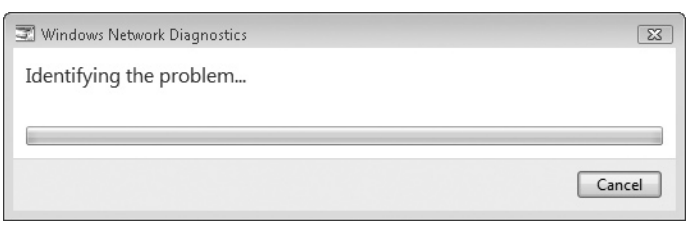

Figure 6-15. The Windows Network Diagnostics tool scans your computer to determine what's wrong with your network connection.

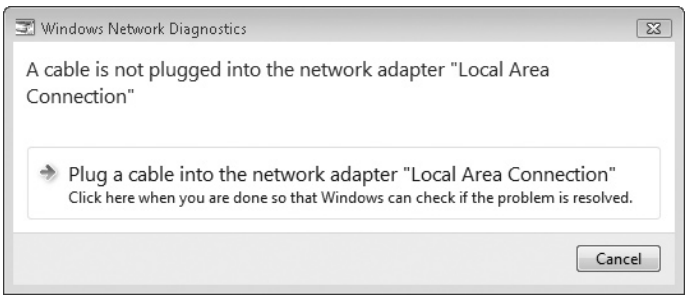

Figure 6-16. Windows Vista will give you suggestions to help fix the network connectivity problem.

This wizard is used to add a network, create virtual private network (VPN) connections, or make a dial-up connection.

NOTE For more detail on forming these connections, see Chapter 5.

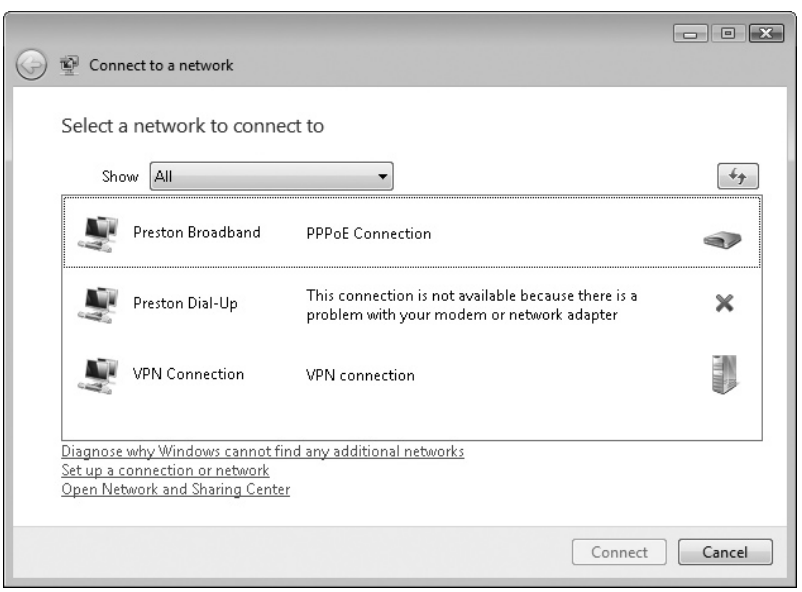

Figure 6-17. The Connect To A Network Wizard shows available network connections.

Network Connections

Connecting to a network in a new location creates a new network profile. Vista will automatically save this new network connection and settings, and will use them the next time you connect to this network.

Depending on how your computer is configured, there might be different ways in which you want to connect to the network. For instance, you might want to connect wirelessly, or you might have multiple network interface cards (NICs) installed but want to use a specific NIC for connection. You can configure which devices and connections are to be associated with the network.

1. Click Start and then click Control Panel.
2. In Control Panel, under the Network And Internet area, click View Network Status And Tasks.
3. If you have a working connection to the network, click the Customize link above the Network Details section of the dialog box.
4. The Set Network Location dialog box gives details about the network to which you're currently connected. This is shown in Figure 6-18.
5. The Network text box shows the name of the profile associated with the network. You can change it by typing a new name.

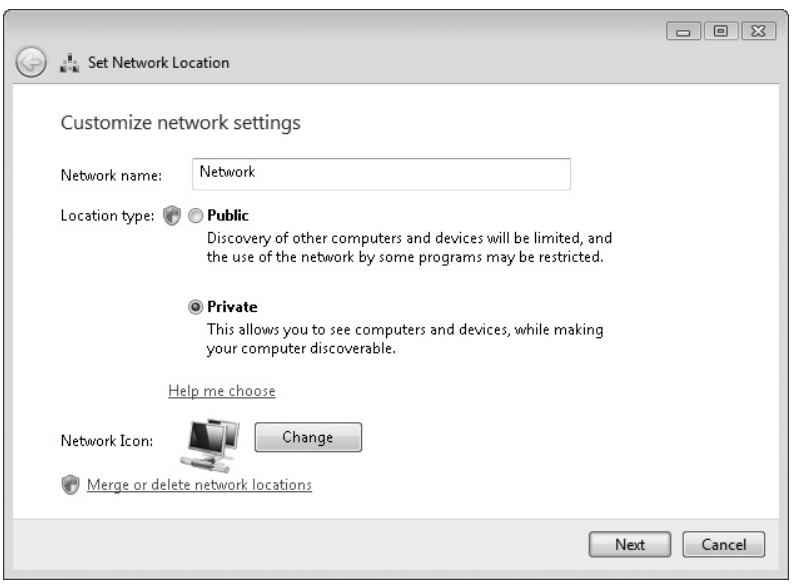

Figure 6-18. The Set Network Location dialog box offers many details that can be customized for a network connection.

6. The Location Type options indicate the category of the network. This is either public or private.
7. The Network Icon shows the current icon selected for the connection. You can change the icon by clicking the Change button next to this setting.
8. Click OK to close the Set Network Location dialog box.

Customization

The Set Network Location dialog box allows you to customize a network connection to meet your specific needs. It doesn't really sound like an earth-shattering achievement, but the idea behind it was to help people who are connecting to various wireless networks. This allows you to assign a specific name to each wireless network that you might connect to, rather than having to use whatever name is part of the network's Service Set Identification (SSID). For example, consider the laptop user in Figure 6-19.

NOTE If you're connecting to a "hidden" wireless network that is not broadcasting an SSID, this is a way to indicate—at least to yourself—which network it is.

As you can see from the example, there are five different networks to which our user, Kip, can connect. A couple of these don't really concern him; the rest have names that make sense to the network administrator or to the administrator's overall naming plan, but they aren't meaningful to Kip. As such, Kip can personalize the connection names in Network Details to make them relevant.

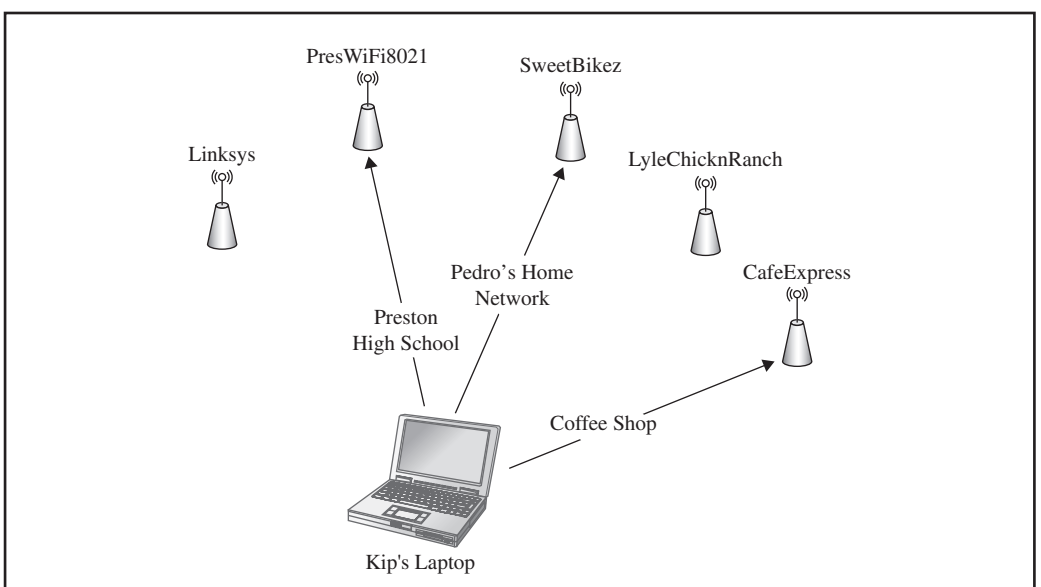

Figure 6-19. Users can give available wireless networks their own names to make the connections more meaningful.

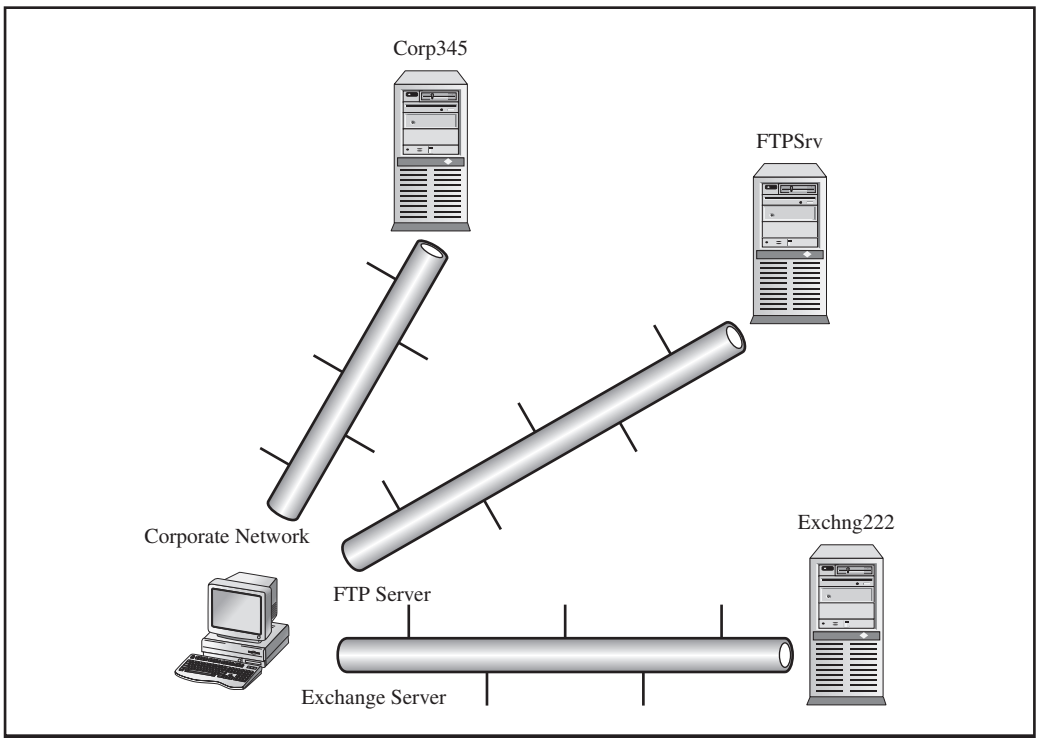

Figure 6-20. Users connecting to multiple wired networks can give those networks meaningful names.

Now, instead of names like PresWiFi8021, SweetBikez, and CafeExpress, Kip can rename them to be more readily understandable, like Preston High School, Pedro's Home Network, and Coffee Shop.

But the Personalize feature isn't just for wireless networks—it's also for wired connections. This isn't too crucial of a feature for computers with just one network connection, but laptop users or those who have more than one network to which they can connect will find this feature useful.

For example, consider the user in Figure 6-20. His workplace uses three networks to which he connects at various times during the day. The convenience of Vista, however, keeps him from having to remember which network is which. By giving the networks his own names, it's easier to keep track of what he's doing.

WIRELESS NETWORK CONFIGURATION

We touched on connecting to a wireless network in Chapter 5, but let's take a closer, more in-depth look at configuring a Windows Vista wireless network. This section looks at two ways you can configure your wireless connection: through the Connect To A Network dialog box and using the **`netsh`** command on the command line.

The Connect To A Network Dialog Box

The way most wireless local area networks (LANs) are configured is through the Connect To A Network dialog box. This is the standard, point-and-click way to configure such a connection. The dialog box can be called up in a number of ways, but for the sake of this exercise, click Start and select Connect To. This displays the Connect To A Network dialog box, which is used to select a wireless network to which you'll connect. An example is shown in Figure 6-21.

The dialog box is a somewhat retooled version of the wireless network dialog box from Windows XP Service Pack 2 (SP2). This dialog box not only handles wireless connections, but also VPN and dial-up connections.

To connect to a listed network, simply double-click its relevant icon.

If the network you wish to connect to is not listed, click Set Up A Connection Or Network, and Vista will display a dialog box. There are several options from which you can choose, including:

- Connect to the Internet
- Set up a wireless router or access point

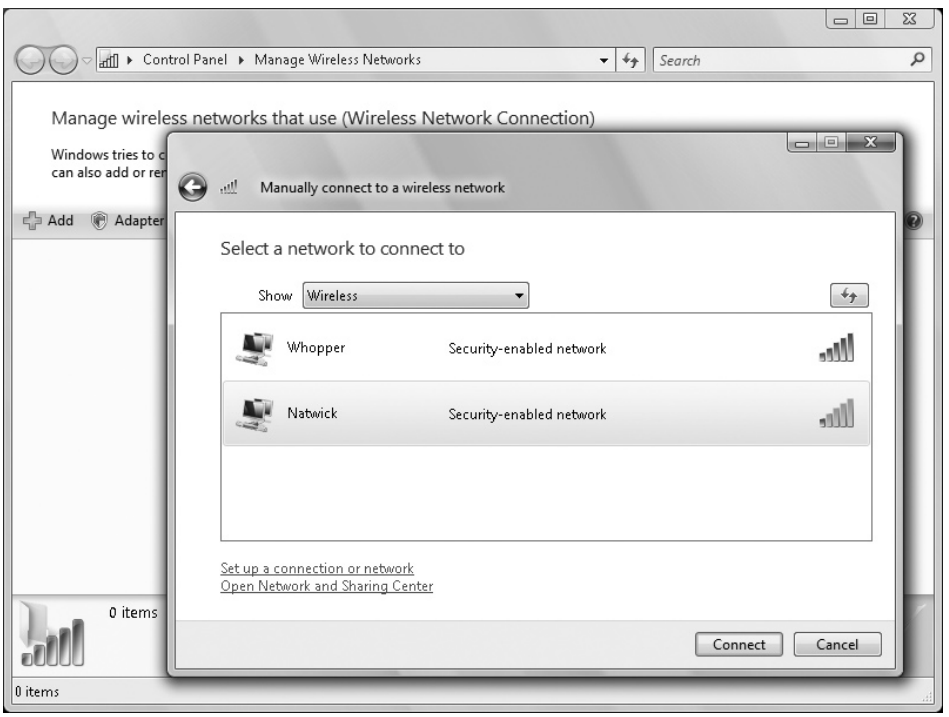

Figure 6-21. The Connect To A Network dialog box allows you to select the wireless network to which you'll connect.

- Manually connect to a wireless network
- Set up a wireless ad hoc (computer-to-computer) network
- Set up a dial-up connection
- Connect to a workplace

So, not only can you configure wireless connections, but other types as well. For more information on these other types of connections, see Chapter 5.

Manual Configuration

To manually configure a wireless connection, click Manually Connect To A Wireless Network, and then click Next. The resulting dialog box looks like the one shown in Figure 6-22.

Vista asks you various questions about the wireless network's configuration settings. The settings and requested information is listed in Table 6-3.

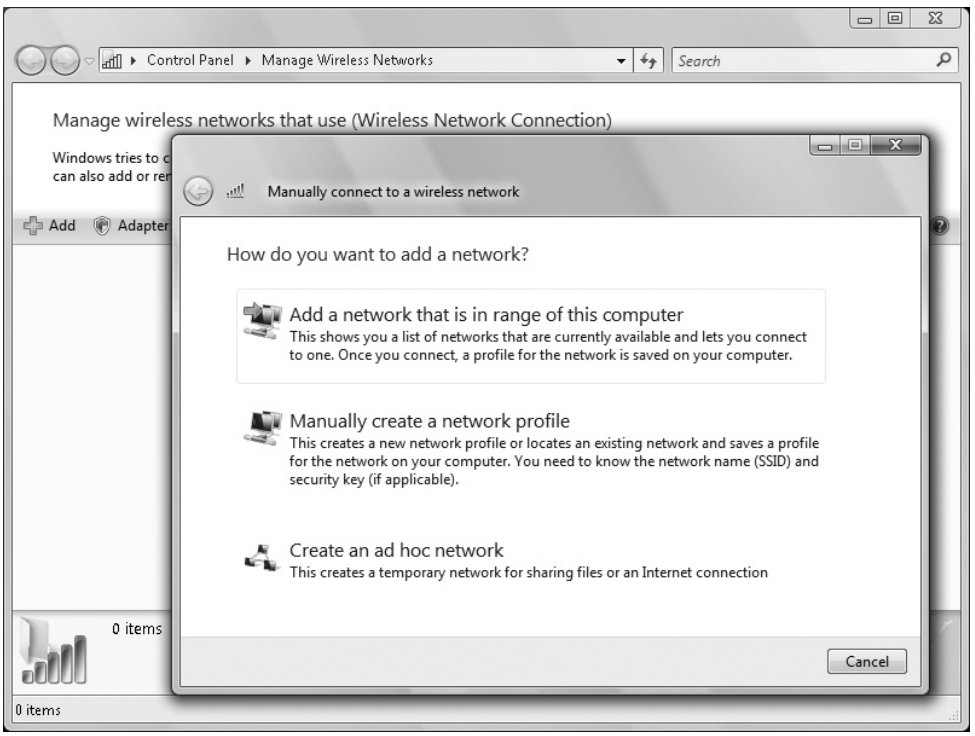

Figure 6-22. Connecting manually to a wireless network requires you to enter information about it.

Setting	Description
Network Name	Enter the name of the wireless network.
Security Type	Select the type of authentication you want to use to connect to the network. This is shown in Figure 6-23. Choices are: ■ No Authentication (Open) ■ WEP ■ WPA-Personal ■ WPA-Enterprise ■ WPA2-Personal ■ WPA2-Enterprise ■ 802.1x
Encryption Type	Select which method should be used to encrypt data sent over the network. The choices will depend on your security type. You can choose from: ■ None (when No Authentication is your security type) ■ WEP (when WEP is the security type) ■ TKIP or AES (when a form of WPA is the security type)
Security Key/Passphrase	Enter the WEP key (assuming WEP was chosen as the security type), the preshared key (if WPA-Personal was the security type), or the WPA2 preshared key (if you picked WPA2-Personal as the security type).
Display Characters	Indicates whether you want to view the security key characters as they are entered.
Save This Network For All Users Of This Computer/Save This Network For Me Only	Indicates whether this profile will be available for all users on the computer or just the current user.
Start This Connection Automatically	Indicates whether Vista will automatically connect to this network.
Connect Even If The Network Is Not Broadcasting	Indicates whether Vista should try to connect to the network even if it is not broadcasting its name.

Table 6-3. Configurable Settings for a Wireless Network

Figure 6-23. Depending on the type of security your network is using, you'll need the appropriate key or passphrase.

Connecting to the Network

You can connect to the network that you just configured by clicking Connect To and then double-clicking the network's icon in the Connect To A Network dialog box. Once the connection has been created, you can manage it right-clicking the connection icon and selecting Properties. You'll see a properties box like the one shown in Figure 6-24.

In this box, you can select:

- ▼ The Connection tab This allows you to view the wireless network's name, SSID, network type (access point for infrastructure networks or computer-to-computer for ad hoc networks), and availability. You can also opt to automatically connect when the network is in range, connect to a more preferred network, or connect if the network is not broadcasting. This tab is shown in Figure 6-25.
- ▲ The Security tab This allows you to manage the security settings that were detailed in Table 6-3. This tab is shown in Figure 6-26.

You can manage your wireless networks from the Manage Wireless Networks dialog box, as shown in Figure 6-27.

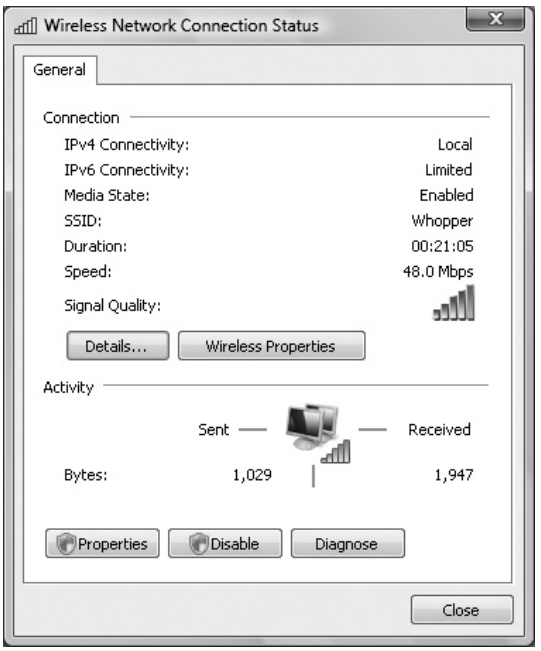

Figure 6-24. Managing wireless networks and their settings is accomplished in its Properties box.

To display this dialog box:

1. Click Start.
2. Click Control Panel.
3. Click Manage Wireless Networks.

This dialog box allows you to add and remove wireless networks and manage the properties of a connection.

COMMAND LINE

In addition to the very visual, easy-to-follow interface provided by the Vista graphical user interface (GUI), you can configure clients using the command line. Netsh—short for network shell—is a utility that was provided with Windows 2000 and XP. It allows for local or remote configuration of network settings. Netsh is commonly used to reset the TCP/IP stack to default settings that are known to be good.

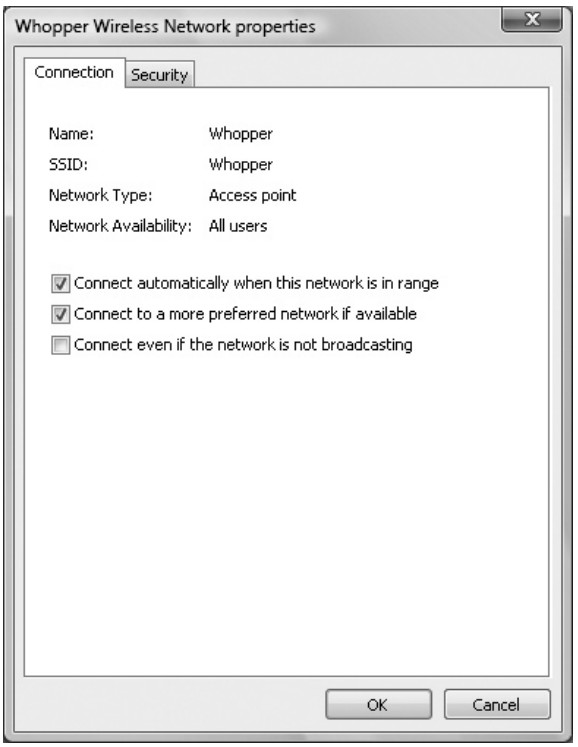

Figure 6-25. The Connection tab shows various connection details and allows you to manage them.

Netsh

Netsh is a powerful networking tool, but Window's flashier GUI brother seems to get more of the action than this frumpy command-line tool.

NOTE You can also use Netsh to connect remotely to other systems by using the –r parameter.

Contexts

Netsh is used in different *contexts*. Contexts are specific areas within the network that can be managed by Netsh. Commands are context-sensitive, and the same command can exist in different contexts. As such, it's important to know which context you're working in. Contexts include:

- Dynamic Host Configuration Protocol (DHCP) server administration
- LANs

- Wireless local area networks (WLANs)
- Routing and administrations
- Windows Internet Naming Service (WINS)

Netsh is a big topic, and not one we can cover in its entirety here. For the sake of our discussion, we're going to talk about two specific contexts: LAN (for wired networks) and WLAN (for wireless networks).

It's important to know that each context can have a subcontext. For example, the interface context includes these subcontexts:

- ip
- ipv6
- portproxy

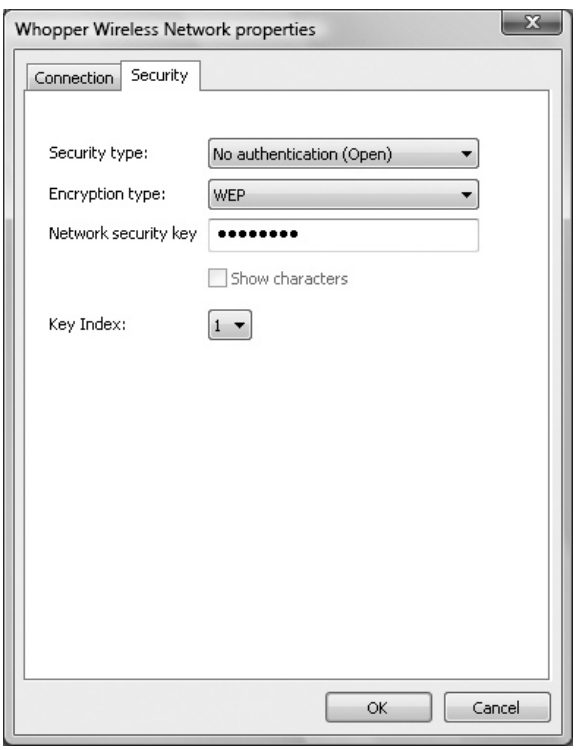

Figure 6-26. Security details for a wireless connection are managed via the Security tab.

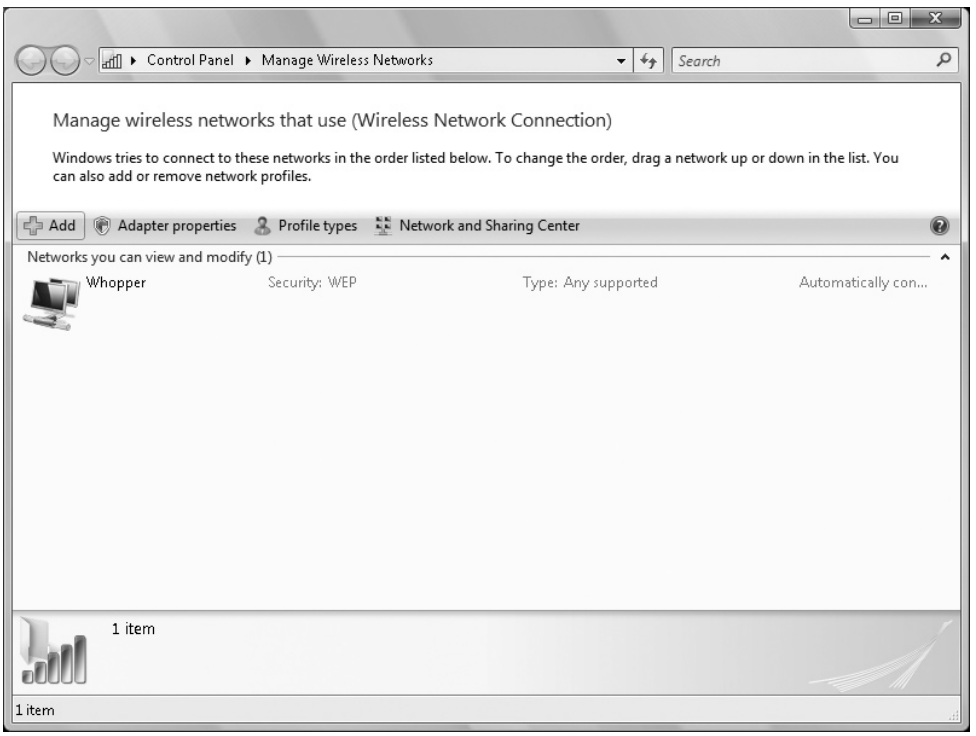

Figure 6-27. The Manage Wireless Networks dialog box helps you manage your wireless networks and gives at-a-glance information.

The point is that it is important to know which context you're working in so that you aren't issuing commands that are harming your system's configuration.

TCP/IP

Netsh can be used to make dynamic IP address changes from a static IP address to DHCP by importing a file. Netsh can also bring about the complete configuration, including:

- TCP/IP address
- DNS settings
- WINS settings
- IP aliases

This is helpful when you're working on different networks, some with DHCP servers, and others without. Although Automatic Private Internet Protocol Addressing (APIPA) is useful in such situations, Netsh is a far better tool.

Getting Around Netsh

Getting around Netsh can seem daunting, but there are some easy, basic rules that will help you once you understand them. Starting Netsh is easy—just open the command prompt window, and type **`netsh`**. Once you're there, follow these simple guidelines:

- To change the context you're in, simply type the name of it. For instance, typing `interface ip` will take you to the interface ip context from whichever context you're currently in.
- Typing `offline` or `online` will change what mode you're in. If you're in offline mode, you will be sent to an interactive session offline. In that mode, any changes you make won't be immediately applied. This is a good mode to be in if you're just starting to learn Netsh. Working in online mode will bring the session online, so changes will immediately be applied to your system.
- Typing `show mode` displays the current mode (online or offline).

NOTE The default mode is online, so if you're new to Netsh or just playing around, be sure to switch to offline mode.

- Type `?` or `help` to show the available commands for your current context.
- You can use global commands anywhere. These commands include `online`, `offline`, and `quit`.
- Within a context, typing **`set`** and **`show`** displays context-sensitive command options.

Wired

To use Netsh to manage your wired network connections, enter the **`netsh`** LAN context.

1. Click Start.
2. Click Run.
3. Type `cmd` and then click OK to open a command prompt window.
4. Type `netsh` and then press ENTER.
5. Type `lan` and then press ENTER.

Once you're in this context, you can use the commands listed in Table 6-4 to manage your wired connection.

Command	Description	Syntax	Usage Examples
?	Displays a list of commands or parameters	*CommandName*/?	? add /?
Add	Adds a profile to the specified interface on the computer	add profile filename=*PathAndProfileName*interface=*InterfaceName*	add profile filename=C:\configfiles\"lanprofile.xml" interface="LAN Connection"
Delete	Removes a LAN profile from the computer interface	delete profile interface=*InterfaceName*	delete profile interface="LAN Connection"
Dump	Creates and saves a script containing the current configuration	dump >*PathAndFileName*	dump >C:\configfiles\lanconfig.txt
Export	Saves LAN profiles as XML files	export profile folder=*PathAndFileName* [[interface=]*InterfaceName*]	export profile folder=C:\configfiles\ interface="Local Area Connection" export profile folder=C:\configfiles\
Help	Shows a list of commands	*CommandName*help	Add profile help
Reconnect	Reconnects to the network	reconnect[[interface=]*InterfaceName*]	reconnect interface="LAN Connection"
Set	Sets wired configuration	set autoconfig enabled={yes|no}interface=*InterfaceName*	set autoconfig enabled=yes interface="LAN Connection"

Table 6-4. Netsh Commands for a Wired Network

Command	Description	Syntax	Usage Examples
Show	Displays information for various settings	show interfaces show profiles[[interface =]*InterfaceName*] show settings show tracing	show interfaces show profiles interface="LAN Connection" show settings show tracing

Table 6-4. Netsh Commands for a Wired Network *(Continued)*

Wireless

To use Netsh to manage your wireless network connections, enter the netsh WLAN context.

1. Click Start.
2. Click Run.
3. Type `cmd` and then click OK to open a command prompt window.
4. Type `netsh` and then press ENTER.
5. Type `wlan` and then press ENTER.

Once you're in this context, you can use the commands listed in Table 6-5 to manage your wireless connection.

Networking your organization's computers is a crucial way to share information. With Windows Vista, users can access information on the network and on others' computers much more easily than they could with earlier versions of Windows. In addition, Vista introduces some exciting new ways to share information, such as integrated media sharing.

But while simply sharing information is the cornerstone of networking, the next level is actually being able to communicate and collaborate with coworkers. In Chapter 7, we'll show you how your users can collaborate using some tried and true Windows technologies, along with some new items introduced with Vista.

Command	Description	Syntax	Usage Examples
?	Displays a list of commands or parameters	*CommandName*/?	? add /?
Add filter	Adds a wireless network to an allowed or blocked list	add filter permission={allo w | block | denyall} ssid=*WirelessNetworkName* networktype={infrastructure | adhoc}	add filter permission=allow ssid="PrestonWiFi" networktype=infrastructure
Add profile	Adds a profile to the specified interface on the computer	add profile filename=*PathAndFileName* [[interface=]*InterfaceName*] [[user=]{all | current}]	add profile filename=C:\configfiles\"wlanprofile1.xml" Interface="Wireless Network Adapter"
Connect	Connects to a wireless network	connect[[ssid=]*SSIDName*] name=*ProfileName*interface= *InterfaceName*	connect ssid=PrestonWiFi name=Kip
Delete filter	Removes a wireless network from an allowed or blocked list	delete filter permission= {allow | block | denyall} ssid= *WirelessNetworkName*networkt ype={infrastructure | adhoc}]	delete filter permission=allow ssid=PrestonWiFi networktype=infrastructure

Table 6-5. Netsh Commands for Wireless Networks

Command	Description	Syntax	Usage Examples
Delete profile	Removes a LAN profile from the computer interface	delete profile name=*ProfileName* [[interface =]*InterfaceName*]	delete profile name="Kip" interface="WLAN Connection"
Disconnect	Disconnects from a wireless network	disconnect interface=*InterfaceName*	disconnect interface="WLAN Connection"
Dump	Creates and saves a script containing the current configuration	dump >*PathAndFileName*	dump >C:\configfiles\wlanconfig.txt
Export	Saves LAN profiles as XML files	export profile folder=*PathAndFileName* [[name=]*ProfileName*] [[interface=]*InterfaceName*]	export profile folder=C:\profiles name="Kip" interface="WLAN Connection"
Help	Shows a list of commands	*CommandName*help	Add profile help

Table 6-5. Netsh Commands for Wireless Networks *(Continued)*

Command	Description	Syntax	Usage Examples
Set	Sets configuration on interfaces	set autoconfig enabled={yes | no} interface=*InterfaceName* set blockednetworks display={show | hide} set profileorder name=*ProfileName*interface=*InterfaceName* priority=*integer* set tracing [[mode=]{yes | no | persistent}]	set autoconfig enabled=yes interface="WLAN Connection" set blockednetworks display=show set profileorder name="Kip" interface="WLAN Connection" priority=1 set tracing mode=persistent
Show	Displays information for various settings	show all show autoconfig show blockednetworks show drivers[[interface=]*InterfaceName*] show filters[[permission=]{allow | block}] show interfaces show networks[[interface=]*InterfaceName*] [[mode=]{ssid | bssid}] show profiles[[name=]*ProfileName*] [[interface=]*InterfaceName*] show settings show tracing	show all show autoconfig show blockednetworks show drivers interface="WLAN Connection" show filters permission=allow show interfaces show networks interface="WLAN Connection" show profiles name= "Kip" interface="WLAN Connection" show settings show tracing

Table 6-5. Netsh Commands for Wireless Networks *(Continued)*