Introducing TCP/IP Networking for Windows Vista

The networking components in Windows Vista have been extensively reworked. In this section, you’ll look at the changes to these components and how they are used to improve reliability while reducing transfer times. You’ll learn about:

- The next generation of networking components.
- The dual stack and the IP management enhancements.

Getting to Know the Next Generation TCP/IP Stack

Whether they are using wired or wireless technology, most networks use TCP/IP. TCP/IP is a protocol suite consisting of Transmission Control Protocol (TCP) and Internet Protocol (IP). TCP is a connection-oriented protocol designed for reliable end-to-end communications. IP is
Part III: Securing Windows Vista

an internetworking protocol that is used to route packets of data over a network. Two versions of IP are in use:

- **IP version 4 (IPv4)**  IPv4 is the primary version of IP used today on networks, including the Internet. IPv4 has 32-bit addresses.
- **IP version 6 (IPv6)**  IPv6 is the next-generation version of IP. IPv6 has 128-bit addresses.

While many computers use only IPv4, IPv6 is increasingly being used, and eventually IPv4 may be phased out in favor of IPv6. Why? IPv4 allows only \(2^{32}\) unique addresses to be used. While 4,294,967,296 unique addresses might seem like a huge amount, it really isn’t when you look at the number of computing devices in our connected world. This is why we need IPv6, with its virtually unlimited address space, and why computers running Windows Vista have both IPv4 and IPv6 configured by default.

Windows Vista includes many other changes to the core networking components as well. Windows Vista provides a new implementation of the TCP/IP protocol stack known as the Next Generation TCP/IP stack. This stack is a complete redesign of TCP/IP functionality for both IPv4 and IPv6. The Next Generation TCP/IP stack supports:

- **Receive Window Auto Tuning**  Optimizes TCP transfers for the host receiving data by automatically managing the size of the memory buffer (the receive windows) to use for storing incoming data based on the current network conditions.
- **Compound TCP (CTCP)**  Optimizes TCP transfers for the sending host by aggressively increasing the amount of data sent in a connection while ensuring that other TCP connections are not impacted.
- **Neighbor Unreachability Detection**  Determines when neighboring nodes, including routers, are no longer reachable and reports the condition.
- **Automatic Dead Gateway Retry**  Ensures that an unreachable gateway is tried again periodically to determine whether it has become available.
- **Automatic Black Hole Router Detection**  Prevents TCP connections from terminating due to intermediate routers silently discarding large TCP segments, retransmissions, or error messages.
- **Routing Compartments**  Prevents unwanted forwarding of traffic between interfaces by associating an interface or a set of interfaces with a login session that has its own routing tables.
- **Network Diagnostics Framework**  Provides an extensible architecture that helps users recover from and troubleshoot problems with network connections.
- **TCP Extended Statistics**  Helps determine whether a performance bottleneck for a connection is the sending application, the receiving application, or the network.
- **Windows Filtering Platform**  Provides application programming interfaces (APIs) for extending the TCP/IP filtering architecture so that it can support additional features.
To optimize throughput in high-loss environments, the Next Generation TCP/IP stack supports industry standard Requests For Comments (RFCs) 2582, 2883, 3517, and 4138. These changes allow the Next Generation TCP/IP stack to:

- Modify how the TCP fast recovery algorithm is used. The new algorithm provides faster throughput by changing the way that a sender can increase its sending rate when multiple segments in a window of data are lost and the sender receives an acknowledgement stating that only part of the data has been successfully received. The old algorithm worked well for single lost segments, but it did not perform well when multiple lost segments were involved.

- Extend the use of the Selective Acknowledgement (SACK) option for TCP. This option now allows a receiver to indicate up to four noncontiguous blocks of received data and to acknowledge duplicate packets. The sender can then determine when it has retransmitted a segment unnecessarily and adjust its behavior to prevent future retransmissions.

- Introduce a conservative SACK-based loss recovery algorithm for TCP. This new algorithm makes it possible to use SACK information to perform loss recovery when TCP senders receive duplicate acknowledgements and to recover more effectively and quickly when multiple segments are not received at the destination.

- Detect spurious retransmission time-outs (RTOs) with TCP. This provides correction for sudden, temporary increases in RTOs and prevents unnecessary retransmission of segments.

**Learning About the Dual Stack and the IP Management Enhancements**

As mentioned earlier, computers running Windows Vista have both IPv4 and IPv6 configured by default. This is a major change from earlier versions of Microsoft Windows, in which only IPv4 is used by default.

Windows Vista supports IPv4 and IPv6 by using the dual-layer Next Generation TCP/IP stack. This stack features an implementation of IP in which IPv4 and IPv6 share common transport and framing layers. Because Windows Vista enables IPv4 and IPv6 by default, there is no need to install a separate component to obtain IPv6 support.

To make IPv6 more dynamic, Windows Vista includes a number of enhancements. These enhancements include support for:

- **Symmetric network address translators (NATs)** A symmetric NAT maps the internal (private) address and port number to different external (public) addresses and ports, depending on the external destination address. This new behavior allows an IPv6 feature called Teredo to act as the go-between for a larger set of Internet-connected host computers.
Part III: Securing Windows Vista

- **IP Security in IPv6**  Windows Vista supports IP Security for IPv6 traffic in the same way it supports IPv4 traffic. As a result, IPv6 can use Internet Key Exchange (IKE) and data encryption in the same way as IPv4. This ensures IPv6 traffic can be as secured as IPv4 traffic. When you configure an IP filter as part of an IP filter list in the IP Security Policies snap-in, you can now specify IPv6 addresses and address prefixes in IP Address or Subnet when specifying a specific source or destination IP address.

- **IPv6 over Point-to-Point Protocol (PPPo6)**  PPPv6 allows native IPv6 traffic to be sent over PPP-based connections. This means that remote access clients can connect with an IPv6-based Internet service provider (ISP) through dial-up or PPP over Ethernet (PPPoE)-based connections.

- **Multicast Listener Discovery version 2 (MLDv2)**  IPv6 routers use MLDv2 to identify the presence of multicast listeners and to provide support for source-specific multicast traffic. MLDv2 is equivalent to Internet Group Management Protocol version 3 (IGMPv3) for IPv4. (Multicast listeners are nodes that are configured to receive multicast packets.)

- **Link-Local Multicast Name Resolution (LLMNR)**  LLMNR allows IPv6 hosts on a single subnet without a DNS server to resolve each other’s names. This feature is useful for single-subnet home networks and ad hoc wireless networks.

- **Random Interface IDs**  Random Interface IDs prevent address scanning of IPv6 addresses based on the known company IDs of network adapter manufacturers. By default, Windows Vista generates Random Interface IDs for nontemporary autoconfigured IPv6 addresses, including public and local link addresses.

- **Dynamic Host Configuration Protocol version 6 (DHCPv6)**  Windows Vista includes a DHCPv6-capable DHCP client. This client can use stateful address autoconfiguration with a DHCPv6 server. Or, the client can use stateless address autoconfiguration when a DHCPv6 server is not present.

---

**From the experts**

**Configuring IPv4 and IPv6 settings**

In Windows Vista, you can manually configure both IPv4 and IPv6 settings through a set of dialog boxes accessible from the Network Connections console. Click Start, and then click Control Panel. In Control Panel, under the Network And Internet heading, click View Network Status And Tasks. In the left pane in Network Center, click Manage Network Connections. Right-click a connection and then select Properties. In the connection’s Properties dialog box, double-click Internet Protocol Version 6 (TCP/IPv6) or Internet Protocol Version 4 (TCP/IPv4) as appropriate.

You configure IPv4 settings through the Properties dialog box of the Internet Protocol version 4 (TCP/IPv4) component and through commands in the Netsh Interface IPv4 context. You can disable IPv4 for connections by clearing the check box next to the Internet Protocol version 4 (TCP/IPv4) component from the properties of a connection.
You configure IPv6 settings through the Properties dialog box of the Internet Protocol version 6 (TCP/IPv6) component and through commands in the Netsh Interface IPv6 context. You can disable IPv6 for connections by clearing the check box next to the Internet Protocol version 6 (TCP/IPv6) component from the properties of a connection. For more information about configuring IPv4 and IPv6, refer to the *Microsoft Windows Vista Administrator’s Pocket Consultant* (Microsoft Press, 2006).

William Stanek  
*Author, MVP, and series editor for the Microsoft Press Administrator’s Pocket Consultants*

### Mapping Your Networking Capabilities and Infrastructure

Windows Vista provides a whole new way to navigate and manage the networking features of your computer. In this section, you’ll learn about these features, including Network Center, Network List, Network Map, and Network Connections.

#### Using Network Center

When you want to work with the networking features of your computer, you’ll start with Network Center. You can access Network Center by following these steps:

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

This displays Network Center, as shown in Figure 12-1.

![Figure 12-1](image.png)  
*Network Center shows that you are connected to a network that in turn has connectivity to the Internet.*
Once you’ve accessed Network Center, you can use it to manage your general network settings and network status. When you are connected to a network, Network Center provides an overview of your networking configuration and allows you to determine your network status and view or change settings.

The three main areas in Network Center are:

- **Status** Provides a visual overview of the network infrastructure. The map depicts whether you are connected to a network and whether you can access the Internet on that network. Clicking View Full Map displays an expanded Network Map, as described in the “Using Network Map” section later in this chapter.

- **Network Details** Provides details about the network to which the computer is currently connected. These details include the connections being used and whether the network has Internet access. Using the links provided, you can manage the connections in use and the networks to which those connections are linked, as described in the “Viewing and Managing Your Networks” section later in this chapter.

- **General** Provides a summary of the computer’s firewall, detection, and sharing settings. Depending on the configuration, several options are provided, including Block, Allow, and View Sharing Settings. You’ll learn how to manage general settings in the next section, “Managing General Networking Settings.”

The sections that follow discuss using Network Center to manage settings, diagnose and repair connectivity issues, and manage your network status.

**Managing General Networking Settings**

In Network Center, the settings in the General panel allow you to block or allow connections to your computer. If you click Block, the computer’s firewall blocks all access to the network. While access is blocked, you will be unable to access other computers on the network or on the Internet, and other computers will be unable to access your computer.

To unblock the computer, you need to click Allow. Clicking Allow sets the computer’s firewall to its normal configuration. In this configuration, you can access other computers on the network or on the Internet, and other computers can access your computer, if allowed by the firewall configuration.

**Tip** To configure Windows Firewall from Network Center, click View Sharing Settings. This link opens the Windows Firewall dialog box, which you can use to manage the Windows Firewall configuration.

**Diagnosing and Resolving Network Connectivity Issues**

When you are disconnected from a network, Network Center displays a modified view, as shown in Figure 12-2. Based on this view of your network configuration, you know at a glance that you are not connected to a network or the Internet.
Chapter 12: Networking Your Computer

Figure 12-2  Network Center shows that you are not connected to a network or the Internet.

To resolve this problem, you should check the network cable that connects to your computer as well as any wireless adapters. If your network cable or wireless adapters are properly connected, you can click Diagnose Internet Connection in the left pane to start the new Windows Networks Diagnostics Tool. This tool uses the Network Diagnostics Framework to help you recover from and troubleshoot problems with network connections.

The Windows Networks Diagnostics Tool offers step-by-step advice on resolving your network connectivity problem. For example, in Figure 12-3, the tool advises that you should connect a network cable to the computer’s network adapter. When you plug in the cable and then click the diagnostics box, the tool will validate the repair. If a problem is detected, the tool continues troubleshooting the connection. Otherwise, you’ll see a prompt confirming that the problem has been repaired.

Figure 12-3  The Windows Networks Diagnostics Tool offers step-by-step advice.

Viewing and Managing Your Networks

In Network Center, you can browse computers and devices on the network by clicking Browse The Network in the left pane. While browsing the network, you use Network view. In a domain, options on the Network view toolbar allow you to search Active Directory, connect to a network,
194 Part III: Securing Windows Vista

or return to Network Center. In a workgroup, options on the Network view toolbar allow you to connect to a network or return to Network Center. If you double-click a computer while browsing, you’ll be able to see devices associated with the computer, such as printers.

In Network Center, you can create network connections 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, shown in Figure 12-4. You can use this wizard to add a network, create a virtual private network (VPN) connection or create a dial-up connection.

![Figure 12-4](image)

Connecting to a new network

When you connect to a network in a new location, a network profile is created. Windows can save settings in this location and automatically use these settings the next time you connect to this network. Sometimes, you can connect to one network in multiple ways. For example, you might be able to connect to a network by plugging in a cable, by using a wireless connection, or both. Or your computer might have multiple network adapters and those adapters might be connected to different networks or to the same network. You can determine the devices and connections associated with the current network by following these steps:

1. Click Start, and then click Control Panel.
2. In Control Panel, under the Network And Internet heading, click View Network Status And Tasks.
3. If you have a valid connection to the network, click Personalize under Network Details.
4. The Personalize Settings dialog box, shown in Figure 12-5, provides details about the network to which you are currently connected.
Figure 12-5  The Personalize Settings dialog box

5. The Network text box shows the name of the profile associated with the network. You can change the profile name by typing a new name.

6. The Category text box shows the category of the network to which you are connected as either private or public. You can switch the category from private to public or vice versa by clicking Switch Category.

7. The Connections In Use list shows the connections being used to connect to the current network.

8. You can manage connections by selecting them and then clicking one of these buttons:
   - **Disconnect**  Allows you to disconnect a wireless connection from a network. This button is available only when you are using a wireless connection.
   - **Properties**  Displays the connection’s Status dialog box, which you use to get details about the TCP/IP configuration and to manage the TCP/IP configuration.
   - **Diagnose**  Starts the Windows Networks Diagnostics Tool for troubleshooting.

9. Click OK to close the Status dialog box.

**Using Network List**

Network List displays a list of all the networks you’ve accessed from the computer. Managed and unmanaged networks are listed separately, as shown in Figure 12-6. You can access Network List by following these steps:

1. Click Start, and then click Control Panel.

2. In Control Panel, under the Network And Internet heading, click View Network Status And Tasks.

3. In Network Center, click Network List under See Also in the left pane.
Part III: Securing Windows Vista

Network List has several different views. You can access these views by clicking the Views button and then selecting the desired view. The view you'll use most often is the Details view.

Using the Details view of the Network List, you can quickly determine the following information:

- **Name**: The name of the profile associated with the network.
- **Status**: The status of your connection to the network as either connected (and active) or disconnected (and inactive).
- **Last Connected**: The date and time you last connected to the network.
- **Type**: The type of network, such as managed or unmanaged.

The Network List toolbar allows you to work with networks in several different ways. The option buttons are used as follows:

- **Reorder Wireless Networks**: Click Reorder Wireless Networks to set the preference order for using wireless networks. To change the order, drag a network entry up or down the list. You can also add or remove network profiles.

- **View Status And Properties**: Click View Status And Properties to display a Status dialog box for a selected network. As discussed in the “Viewing and Managing Your Networks” section of this chapter, you can then manage the network’s profile name and connection configuration.

- **Remove Network**: Click Remove Network to remove and delete the profile associated with the network. When prompted, confirm that you want to delete this information by clicking OK.
Using Network Map

Network Map uses the neighbor detection functionality built into the Next Generation TCP/IP stack to display an expanded view of your network. As Figure 12-7 shows, the expanded Network Map view includes your computer, the computers near your computer, and the devices near your computer. You can access Network Map by following these steps:

1. Click Start, and then click Control Panel.
2. In Control Panel, under the Network And Internet heading, click View Network Status And Tasks.
3. In Network Center, under Network Map, click View Full Map.

If you have questions about your network infrastructure and have permission to browse the network, you can use Network Map to get a better understanding of how you are connected to the network and what devices are near you.

Note Sometimes Network Map will detect devices or computers near you but will not be able to place the devices on the map. If this happens, you’ll see a list of discovered but not mapped devices in the lower portion of the Network Map window.
Part III: Securing Windows Vista

Viewing and Managing Network Connections

Network Connections displays a list of all network connections configured for use on the computer, as shown in Figure 12-8. You can quickly obtain a list of open network connections by completing the following steps:

1. Click Start, and then click Control Panel.
2. In Control Panel, under the Network And Internet heading, click View Network Status And Tasks.
3. In the left pane in Network Center, click Manage Network Connections.

Using Network Connections

Network Connections has several different views. You can access these views by clicking the Views button and then selecting the desired view. The view you’ll use most often is the Details view.

Using the Details view of Network Connections, you can quickly determine the following information:

- **Name** The name of the network connection.
- **Type** The type of connection, such as LAN or High-Speed Internet.
- **Status** The status of the connection, such as Connected or Disabled.
- **Device Name** The manufacturer and type of network adapter.
- **Phone # Or Host Address** The phone number associated with a dial-up connection or the host address associated with a remote access connection.
- **Owner** The owner of the connection, such as System.

If you select a connection, the Network Connection toolbar allows you to work with connections in several different ways. The option buttons are used as follows:

- **Diagnose This Connection** Starts the Windows Networks Diagnostics Tool for troubleshooting.
Chapter 12: Networking Your Computer

■ View Status Of This Connection  Displays the connection’s Status dialog box, which can be used to get details about the TCP/IP configuration and to manage the TCP/IP configuration.

■ Change Settings Of This Connection  Displays the connection’s Properties dialog box, which can be used to manage the TCP/IP configuration.

Tip  If you right-click a connection, a shortcut menu will provide an expanded set of options.

Introducing Wireless Networking for Windows Vista

The wireless components in Windows Vista have been extensively reworked. In this section, you’ll look at the changes to these components and how they are used to improve flexibility and security. You’ll learn about:

■ Wireless networking changes.
■ New ways of connecting to wireless networks.
■ Fast roaming and auto configuration.

Exploring Wireless Networking Changes

Wireless connections in earlier versions of Windows are designed to emulate Ethernet connections and can be extended only when using additional Extensible Authentication Protocol (EAP) types for IEEE 802.1X authentication. Wireless connections in Windows Vista use a software infrastructure for 802.11 wireless connections called the Native Wireless Fidelity (Wi-Fi) architecture.

Native Wi-Fi architecture has many benefits. It allows:

■ Windows Vista to represent wireless (IEEE 802.11) as a media type separate from Ethernet (IEEE 802.3). This increases flexibility by allowing hardware vendors to support advanced features specific to IEEE 802.11 networks, such as larger frame sizes than Ethernet.

■ Windows Vista to include the authentication, authorization, and management components necessary for 802.11 connections. This streamlines the development of miniport drivers that expose a native 802.11 interface and makes it easier for hardware vendors to develop wireless network adapter drivers.

■ Hardware vendors to extend the built-in wireless client for additional wireless services and custom capabilities. This allows vendors to create extensible components and also makes it possible for vendors to provide customized configuration dialog boxes and wizards.
You can configure wireless networking by using the Wireless Network Setup Wizard. This wizard retrieves the security capabilities of the wireless network adapter and recommends the strongest security setting that is supported by the wireless network adapter as the default configuration. For example, if a wireless network adapter supports both Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA), the Wireless Network Setup Wizard will configure settings for WPA by default.

Learning New Ways to Connect to Wireless Networks

Wireless clients can connect to three different types of networks:

- **Secure**  Secure wireless networks transmit passwords and data securely. Typically, they use some form of encryption, and the stronger the encryption, the more protection offered.

- **Unsecured**  Unsecured wireless networks do not transmit passwords or data securely. While they may require a password to establish a connection, they typically transmit all data without encryption or protection.

- **Hidden**  Hidden wireless networks do not advertise their network names and can be either secured or unsecured. You can connect to a hidden network only if you know its network name.

Windows Vista works with hidden and unsecured networks in different ways than earlier versions of Windows. Because of the many changes, keep the following information in mind:

- Wireless access points used by hidden wireless networks can be configured to use non-broadcast Service Set Identifiers (SSIDs). In this configuration, the wireless access points either do not send Beacon frames, which announce their network names, or they send Beacon frames with an SSID set to NULL. Although earlier versions of Windows do not allow you to mark a preferred wireless network as hidden, Windows Vista allows you to indicate that a preferred wireless network is hidden by configuring it as a non-broadcast network.

- Wireless access points used by unsecured networks are at high risk of being compromised. To help improve awareness about unsecured networks, Windows Vista displays a prompt when you connect to an unsecured wireless network and allows you to confirm or cancel the connection attempt.

When connecting to wireless networks, if preferred wireless networks are not found or if connections to detected preferred wireless networks are not successful, the wireless client in earlier versions of Windows prompts you to connect to any detected wireless network. Wireless clients running earlier versions of Windows cannot be configured to prompt you to connect only to specific wireless networks or to never prompt you to connect to specific wireless networks.
Group Policy settings in Windows Vista allow administrators to configure lists of allowed and denied wireless network names. With an *allow* list, administrators can specify by name the set of wireless networks to which wireless clients are allowed to connect, thereby limiting wireless connections to a specific set of wireless networks. With a *deny* list, administrators can specify by name the set of wireless networks to which wireless clients are not allowed to connect and in this way prevent connections to known unsecured wireless networks as well as to any other wireless networks that might be available but should not be used.

**Using Fast Roaming and Auto Configuration with Wireless Connections**

Through Group Policy settings, administrators can also configure fast roaming and automatic connections on preferred wireless networks. With fast roaming, wireless clients can more quickly roam from one wireless access point to another by using preauthentication and Pairwise Master Key (PMK) caching. With automatic connections, wireless clients can establish connections automatically when preferred networks are detected. If you don’t want to use automatic connections, you can specify that manual connections should be used instead.

Wireless Auto Configuration is a service that dynamically selects the wireless network to which the computer will automatically connect, based either on your preferences or on default settings. This includes automatically selecting and connecting to a more preferred wireless network when it becomes available.

Wireless Auto Configuration in Windows Vista helps to protect computers running Windows Vista from attackers. As with earlier versions of Windows, a computer running Windows Vista uses a randomly named wireless network if no preferred network is available and periodically scans for a preferred network to become available. Unlike earlier versions of Windows, Windows Vista prevents a wireless connection to a wireless network matching the random wireless network name. Further, because Windows Vista attempts to connect preferred networks in the order specified, you can connect to a hidden network before a nonhidden network if the hidden network is higher in the preferred network list.

Wireless connections also support integration with Network Access Protection (NAP) when using 802.1X authentication and Single Sign-On profiles. Using Network Access Protection and 802.1X authentication, administrators can prevent wireless clients that do not comply with system health requirements from gaining unlimited access to a private network. With Single Sign-On profiles, administrators can ensure that only an appropriate user or device is allowed on the protected network and that their data is secure when establishing the connection as well as once the connection is established.

When a Single Sign-On profile is configured, 802.1X authentication is used prior to the computer logon to the domain and users are prompted for credential information only if needed. This ensures that the wireless connection is established prior to the computer domain logon, which enables scenarios that require network connectivity prior to user logon such as Group Policy updates, wireless client domain joins, and execution of logon scripts.
Mapping Your Wireless Networking Capabilities and Infrastructure

The same features that can be used to work with wired connections can be used to work with wireless connections. This means that everything you’ve learned about Network Center, Network List, Network Map, and Network Connections can be used to help you work with wireless connections. Because Windows Vista represents wireless (IEEE 802.11) as a media type separate from Ethernet (IEEE 802.3), there are a few differences that should be noted. These differences are explored in the sections that follow.

Listing and Connecting to Available Wireless Networks

These days, most laptops and portable computers have wireless network adapters, and so do some workstations. No matter where you are, you can get a list of available wireless networks in your area and connect to one by using your wireless network adapter.

To view and connect to an available wireless network, follow these steps:

1. Click Start, and then click Connect To.
2. A list of the wireless networks currently available is displayed.
3. Select a network, and then click Connect.

The network list is available only if your computer has a wireless network adapter installed, the adapter is turned on, and there are no policy settings blocking your computer from browsing for available wireless networks. If you don’t see the network to which you want to connect, click the I Don’t See The Networks I Am Looking For link. On the Select A Connection Option page, select the Show All Connection Options check box. Select the type of connection that you are trying to use, and then follow the prompts to configure the connection.

Tip Some networks are protected with a network security key. To connect to one of these networks, you must obtain the key from your network administrator or the service provider.

Connecting to Public Wireless Networks

When connecting to public networks, you might be asked to set up an account and save files to your computer. Before you do this, however, make sure that you understand which files, if any, are saved to your computer and what type of information the network provider collects from your computer. Read the service provider’s privacy statement carefully, and keep in mind that even if the service provider requires you to create an account, that doesn’t mean that the connection you are using is secure.
Caution You should be wary of working on company-sensitive information or accessing password-protected areas of your business network while you are connected to a public network. If you connect to a network that is not secure, anyone with the right tools can intercept the data being transmitted from your computer, and they would see any user names and passwords you use, the Web sites you visit, the documents you work on, and the messages you send.

You can view and connect to a public wireless network in the same way as you can connect to an available wireless network:

1. Click Start, and then click Connect To.
2. A list of the wireless networks currently available is displayed.
3. Select a network, and then click Connect.

When you connect to a wireless network that supports Wireless Provisioning Service (WPS) technology, you are prompted to download provisioning files that will allow your computer to connect to the network. While these files are generally safe to download, you should verify that the Web site from which the files will be downloaded is one that you expected based on your location or one that you trust to provide you with the information. If you choose to download provisioning files, you download the files from the provider and then store them on your computer for as long as you want to use the wireless network. The files do not contain any personal information about you or your computer. Instead, they provide details on the network configuration and on how you can access the network. If you choose not to download the files, you will not be able to connect to the wireless network.

When the provisioning files are downloaded, the Wireless Network Registration Wizard requests additional information from you. At this point, you might have to enter your credit card information to provide payment or you might simply have to acknowledge the service provider’s usage policy. Follow the instructions in the Wireless Network Registration Wizard to provide the appropriate information to the network provider.

After you have signed up with a wireless network that supports WPS, the provisioning files stored on your computer can be updated automatically. If you choose this option, your computer will connect to the wireless network provider’s computers and update the information stored on your computer according to the schedule set by the wireless network provider. Typically, the provider schedules an update once a week or once a month. The update process will occur only while you are already connected to the Internet and will not interfere with your use of your Internet connection. If you choose not to update the provisioning files automatically, the files will be updated the next time you connect to the wireless network. Updating the files is required to ensure that your computer has the correct information for the network.
Disconnecting a Wireless Connection

When you no longer need a wireless connection, you should disconnect the connection. To disconnect a wireless connection to the current network, follow these steps:

1. Click Start, and then click Control Panel.
2. In Control Panel, under the Network And Internet heading, click View Network Status And Tasks.
3. If you have a valid connection to the network, click Personalize under Network Details. The Status dialog box appears.
4. The Connections In Use list show the connections you are using. Click the wireless connection, and then click Disconnect.

To disconnect an open wireless connection when your computer has multiple active connections, follow these steps:

1. Click Start, and then click Control Panel.
2. In Control Panel, under the Network And Internet heading, click View Network Status And Tasks.
3. In the left pane in Network Center, click Open Connections.
4. Right-click the wireless connection, and then select Disable.