Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**4**

**Networking**

* [Chapter Introduction](javascript://)
* **4-1**[Networking Overview](javascript://)
  + **4-1a**[Network and Internet Settings](javascript://)
  + **4-1b**[Network and Sharing Center](javascript://)
  + **4-1c**[Remembered Networks](javascript://)
  + **4-1d**[Connections](javascript://)
* **4-2**[IP Version 4](javascript://)
  + **4-2a**[IPv4 Addresses](javascript://)
  + **4-2b**[Subnet Masks](javascript://)
  + **4-2c**[Default Gateways](javascript://)
  + **4-2d**[DNS](javascript://)
  + **4-2e**[WINS](javascript://)
  + **4-2f**[Methods for Configuring IPv4](javascript://)
  + **4-2g**[Essential Networking Tools](javascript://)
  + **4-2h**[Troubleshooting IPv4](javascript://)
* **4-3**[IP Version 6](javascript://)
  + **4-3a**[IPv6 Address Notation](javascript://)
  + **4-3b**[IPv6 Address Types](javascript://)
  + **4-3c**[Methods for Configuring IPv6](javascript://)
  + **4-3d**[Troubleshooting IPv6 Settings](javascript://)
* **4-4**[Internet Connectivity](javascript://)
  + **4-4a**[Single-Computer Internet Connectivity](javascript://)
  + **4-4b**[Shared Internet Connectivity](javascript://)
* **4-5**[Wireless Networking](javascript://)
  + **4-5a**[Creating a Wireless Connection](javascript://)
  + **4-5b**[Managing Wireless Connections](javascript://)
  + **4-5c**[Troubleshooting Wireless Connections](javascript://)
* **4-6**[Windows Defender Firewall](javascript://)
  + **4-6a**[Basic Firewall Configuration](javascript://)
  + **4-6b**[Advanced Firewall Configuration](javascript://)
* **4-7**[Chapter Review](javascript://)
  + **4-7a**[Summary](javascript://)
  + **4-7b**[Key Terms](javascript://)
  + **4-7c**[Review Questions](javascript://)
  + **4-7d**[Case Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

Chapter Introduction

After reading this module and completing the exercises, you will be able to:

* **1**Understand Windows 10 network components
* **2**Describe and configure Internet Protocol version 4
* **3**Describe and configure Internet Protocol version 6
* **4**Connect Windows 10 to the Internet
* **5**Describe and configure wireless networking
* **6**Configure Windows Defender Firewall

The vast majority of computers are networked today. Many homes and businesses have multiple computers that are used to share files and access the Internet. In this module’s context, we examine how computers are linked to allow them to share data with other computers in an interactive way. People use applications on the computer to interact with other people and services to be productive, exchange information, and develop social connections. That can also be called networking in a human context, but networking in this module describes how to configure Windows 10 for computer-to-computer networking. Configuring those settings correctly will subsequently enable people’s access to information and services beyond the individual computer.

In this module, you learn how to configure networking in Windows 10, including both IPv4 and IPv6 protocols. Supported Internet connectivity technologies and sharing Internet connectivity are discussed. You learn about configuring connectivity to wireless networks, including managing wireless connections in Windows 10. You also learn to secure network connectivity by using Windows Defender Firewall.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**4-1**Networking Overview

Windows 10 includes the basic components of networking, such as clients, services, protocols, and network drivers; however, additional features have been added and evolved over time as computing needs have changed. The basic components of Windows 10 that support networking are as follows:

* Network and Internet Settings
* Network and Sharing Center
* Remembered Networks
* Connections

Go to pg.

[**help**](javascript://)

Application Opened

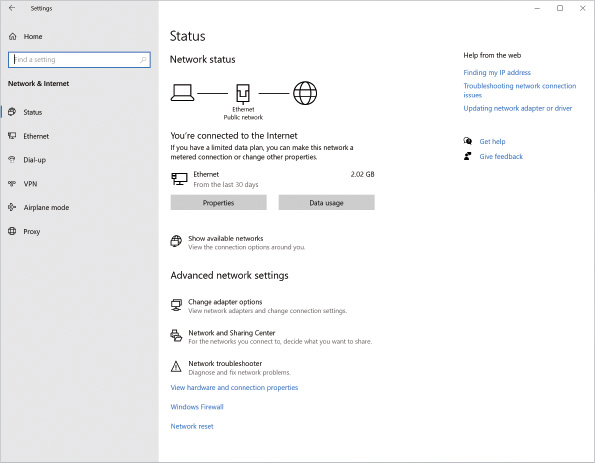
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-1aNetwork and Internet Settings

[**Network and Internet Settings**](javascript://) is the preferred way to manage the configuration of the network to which you are currently connected. The areas of Network and Internet Settings, as shown in [Figure 4-1](javascript://), are:

* Network Status—This area shows summary information for the network to which you are connected. It displays the network, the type of network it is (e.g., public/private), the type of access you have (e.g., wired/wireless), and the specific connection (i.e., network interface) used to access the network.
* Advanced network settings—This area shows links to advanced configuration and troubleshooting tools.
* Network and Internet settings categories—This area selects subsections of network and Internet settings, including overall status, settings by network technology (e.g., ethernet, Wi-Fi, Dial-up), as well as airplane mode and proxy settings.

**Figure 4-1Network and Internet Settings**



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

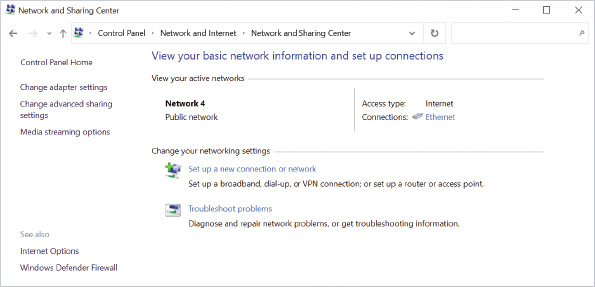
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-1bNetwork and Sharing Center

[**Network and Sharing Center**](javascript://) is a Control Panel tool that provides similar functionality to the Network and Internet Settings for Windows 10. Earlier Windows operating systems relied on the Network and Sharing Center as the primary interface for network configurations. The areas of Network and Sharing Center, as shown in [Figure 4-2](javascript://), are:

* View your active networks—This area shows summary information for the network to which you are connected. It displays the network you are connected to, the type of network it is, the type of access you have, and the connection being used to access the network.
* Change your networking settings—This area displays links to common configuration and troubleshooting wizards.

**Figure 4-2Network and Sharing Center**



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-1cRemembered Networks

In early versions of Windows, the operating system was simply aware of a network card being physically connected (or not connected) to a network. Windows 10 has been enhanced to be network location aware. When you move a computer from one network to another, Windows 10 is aware that it is connected to a different network. Windows 10 keeps track of enough network properties to profile the network to which it is connected. If the network is disconnected and reconnected later, Windows 10 may recognize the network from a list of stored network profiles and associate certain properties with that network profile, such as its assigned network [**location type**](javascript://).

[**Network location awareness**](javascript://) allows you to configure the security settings for each location differently. For example, for the network in your office, you might allow your computer to be discoverable by other computers on the network because you trust that network. When you are traveling on the road and using public networks in hotels and airports, however, you might want to restrict your computer’s capability to be discoverable. The configuration settings for each remembered network are saved so that you do not need to reconfigure your computer as you move from one frequently used network location to another. Each remembered network is assigned a network name and an associated location type.

**Tip**

The service called Network Location Awareness is set to automatically start when the computer is started and is responsible for collecting and storing information for the network, as well as notifying programs when this information is modified. If the service is stopped, remembered network connections’ configuration information might be unavailable.

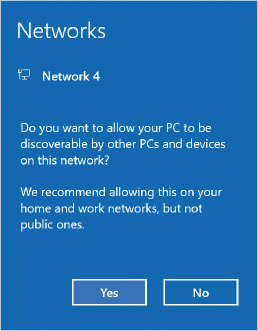
### Network Name

When you first connect to a network, the network is given a name to uniquely identify it as a remembered network to Windows 10. Wireless networks are named after the broadcast ID of the wireless access point. For example, connecting to the wireless network at work could create a network profile called Corp-Private. For Ethernet networks, the new network is assigned the prefix “Network” followed by a sequence number of the next available network number in the network profile history. For example, plugging into a new wired network at a hotel could create a network profile named Network 5.

### Location Types

Each remembered network location is assigned a location type. When you first connect to a network, Windows 10 prompts you if your computer should be visible, or discoverable, to other computers on the network, as shown in [Figure 4-3](javascript://). Depending on how you respond, different security settings are applied. Components that are configured include [**Windows Defender Firewall**](javascript://) and [**network discovery**](javascript://). Previous editions of Windows differentiated between home and work locations, but Windows 10 simplifies the location list to locations that are trusted for computer discovery and those that are not.

**Figure 4-3Confirming If You Want Your Computer Discoverable on a New Network**



The location types are:

* Private network—The [**private network**](javascript://) category is used when the computer is connected as part of a peer-to-peer network in a trusted location. Typically, this is used at home or at work for peer-to-peer networking. The computer is able to access other network computers, and you are able to share files and printers on your computer.
* Public network—[**Public network**](javascript://) is the default location type for a new network and is used when the computer is connected in an untrusted public location, such as an airport. In a public location, you cannot be sure of who else is using the network. Other network computers have limited or no visibility to your computer on the network.

Your computer can connect to publicly available network resources, but you are not able to share files and printers on your computer. Connections to your computer that are initiated from other computers on the public network are blocked by default.

**Caution**

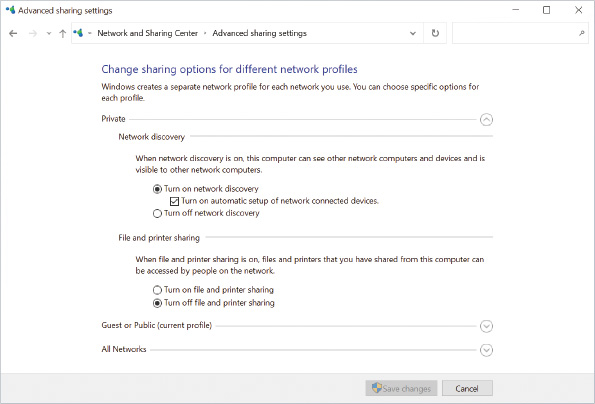
The level of visibility mentioned here is based on what shared files and printers are visible from your computer, but that does not hide your network connection and its traffic on the network.

* Domain network—The [**domain network**](javascript://) category is used in corporate environments when your computer is part of a domain network. When Windows 10 can communicate with a domain controller, the network connection is automatically placed in this location category. You cannot manually place a computer in this category. The computer settings for computers on a domain network are determined by Group Policy settings configured by the network administrator.

### Network Discovery

One of the network characteristics you can configure is network discovery. Network discovery provides you with an easy way to control how your computer views other computers on the network and advertises its presence on the network. Network discovery settings can be reviewed or modified by selecting the Change advanced sharing settings link in the Network and Sharing Center, as seen previously in [Figure 4-2](javascript://). This displays the Advanced sharing settings screen where for each type of network location, you can adjust the network discovery behavior of that type of location, as shown in [Figure 4-4](javascript://).

**Figure 4-4Advanced Sharing Settings, Network Discovery**



Enlarge Image

The options for network discovery are:

* Turn on network discovery—You can see and access other computers and devices on the network. Other computers can also see your computer on the network and access shared resources. This is the default configuration when the network is in the Private location type.
* Turn off network discovery—You cannot see or access other computers and devices on the network. Other computers also cannot see your computer on the network or access shared resources. This is the default configuration for networks in the Public location type.

**Activity 4-1**

### Exploring Network & Internet Settings

**Time Required:**5 minutes

**Objective:**Become familiar with the options that are available in Network & Internet Settings

**Description:**Network & Internet Settings provides you with an overview of the network configuration on your computer. In this activity, you explore a few of the options available to you.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click the **Start** button and then click **Settings**.

1. 3

Click **Network & Internet**. If not already selected, click **Status** in the left navigation pane to display the overall network status for your computer.

1. 4

In the Status page’s subsection titled Network Status, review the network connection listed there and note if it is a public or private network.

1. 5

Below the connection status, click the connection’s **Properties** button (which may be a link called Change connection properties in earlier Windows 10 editions). Click that to bring up the remembered connection’s settings.

1. 6

Scroll to the bottom of that window if necessary to observe the Properties section. Much of the same information is visible by running the ipconfig /all command from a command prompt window, but note that the user does not have to perform those extra steps because the settings summary view includes the detail. Note that key information such as DHCP enabled, Physical Address, IPv4 Address, IPv4 DNS servers, and Link-local IPv6 address are displayed.

1. 7

Click the back arrow in the upper-left corner of the connection’s settings window to return to the main Network & Internet settings. The highlighted subsection below Network & Internet has changed from Status to the subsection that matches that network connection’s type (typically one of these: Ethernet, Wi-Fi, Dial-Up, Cellular). Click **Status** in the left navigation pane to return to the status page.

1. 8

At the bottom of the Status page’s subsection Advanced network settings (which may be called Change your network settings in earlier Windows 10 editions), click **Network troubleshooter**.

1. 9

If no problems were found (none is expected in the lab environment), note the message that troubleshooting couldn’t identify the problem. Click **Close**.

1. 10

Close all open windows.

Go to pg.

[**help**](javascript://)

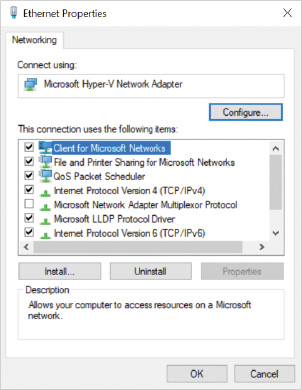
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-1dConnections

Connections in Windows 10 are fundamentally the same as in previous versions of Windows. For each network device installed in your computer, a connection is created to manage that network device. For example, if your computer has an Ethernet network card and a wireless network card, there will be two connections in Windows 10, one to manage each device. The properties of a connection are shown in [Figure 4-5](javascript://). If your computer has multiple network cards, you will see an additional Sharing tab when viewing connection properties.

**Figure 4-5Network and Sharing Center, Network Connection Properties**



Connections are composed of the following:

* Clients and services
* Protocols
* Network drivers

### Clients and Services

Clients and services are the applications that use the network to communicate. A [**client**](javascript://) allows you to connect to a particular service running on a remote computer. A service allows your computer to accept connections from and provide resources to a remote computer.

As shown in [Figure 4-5](javascript://), the clients and services included with Windows 10 are as follows:

* Client for Microsoft Networks—[**Client for Microsoft Networks**](javascript://) allows Windows 10 to access shared files and printers on other Windows computers.
* File and Printer Sharing for Microsoft Networks—[**File and Printer Sharing for Microsoft Networks**](javascript://) allows Windows 10 to share files and printers with other Windows computers.
* QoS Packet Scheduler—This service controls the flow of network traffic in Windows 10. It is responsible for optimizing network communication by controlling the [**Quality of Service (QoS)**](javascript://). Corporate environments can use QoS policies to give certain network content types higher priority within Windows 10. For private networks, QoS incorporates features to ensure that audio and video streams get higher network priority than data streams, which are more tolerant of network delays.

**Note 1**

All three client and service components in Windows 10 are installed by default.

Both the Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks use the [**Server Message Block (SMB)**](javascript://) protocol. Early versions of Windows included additional clients for accessing third-party server types, such as Novell NetWare networks. These third-party clients have been removed from Windows 10 but can be installed if you have a client installation disk from the other vendor.

### Protocols

A network [**protocol**](javascript://) is a set of rules for communicating across the network. For example, they define how much data can be sent and the format of the data as it crosses the network. Windows 10 includes several protocols for network communication.

* Internet Protocol Version 4 (TCP/IPv4)— [**Internet Protocol Version 4 (TCP/IPv4)**](javascript://) is the standard protocol used on corporate networks and the Internet. This protocol is installed by default and cannot be removed; however, it can be disabled.
* Internet Protocol Version 6 (TCP/IPv6)— [**Internet Protocol Version 6 (TCP/IPv6)**](javascript://) is an updated version of TCP/IPv4 with a larger address space and additional features. Windows 10 uses this protocol for some peer-to-peer networking applications. This protocol is installed by default and cannot be removed. However, it can be disabled.
* Link-Layer Topology Discovery Mapper I/O Driver—The Link-Layer Topology Discovery Mapper I/O Driver protocol is responsible for discovering network devices on the network, such as computers and routers. It is also responsible for determining the network speed.
* Link-Layer Topology Discovery Responder—The Link-Layer Topology Discovery Responder protocol is responsible for responding to discovery requests from other computers.
* Microsoft LLDP Protocol Driver—This protocol is used by network devices to advertise their identity, capabilities, and neighbors on a local network.

**Note 2**

Detailed information about TCP/IP v4 and v6 is found later in this module.

### Network Drivers

A [**network driver**](javascript://) is responsible for enabling communication between Windows 10 and the network device(s) in your computer. Each make and model of network device requires a driver specifically developed for that device, just as each printer requires a printer driver specific to that make and model of printer.

Windows 10 includes network drivers for network devices from a wide variety of manufacturers. If the network driver for your network device is not included with Windows 10, however, you can obtain the driver from the manufacturer’s website.

**Caution**

Windows will automatically look for and install network adapter drivers when it detects an unconfigured network adapter. If that doesn’t work and you need to manually install a driver, you will need to know the PC manufacturer name along with the associated model name or number. Some manufacturers will additionally require you to know the network adapter’s manufacturer name and its own associated model name or number to select the correct driver.

**Activity 4-2**

### Viewing a Network Connection

**Time Required:**5 minutes

**Objective:**View the properties and status of a network connection

**Description:**To configure Windows 10 for network connectivity, you need to understand the components of a network connection and how to view their status. In this activity, you view the status and properties of a network connection using the older Control Panel interface.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, in the search box type **control panel**, and then press **Enter**.

1. 3

Click **Network and Internet and then click Network and Sharing Center.**

1. 4

Below the View your active networks subheading, and to the right of Connections, click the named network connection. The name of the network connection will be different on different computers but will likely be called Ethernet. This shows the current connection status.

1. 5

Click the **Details…** button. Note that this will display the network connection’s configuration details, even if they were assigned automatically. Note that the list of details is like the connection properties listed when you browsed network connection details via Settings in [Activity 4-1](javascript://), but some of the miscellaneous properties listed are different between the two apps. As legacy control mechanisms like Control Panel are phased out, the Settings app’s functionality will expand and be the preferred control mechanism for network connections.

1. 6

Click **Close** to close the Network Connection Details dialog box.

1. 7

Click the **Properties** button in the network status dialog box. This displays all of the clients, services, and protocols that are installed as part of that network connection.

1. 8

Click the **Configure** button. This allows you to modify the configuration of the network adapter or an associated network adapter driver.

1. 9

Click the **Advanced** tab. This tab allows you to configure many settings for your network adapter. The options available here vary depending on the adapter; however, all adapters allow you to in some way configure the connection speed and duplex. These are important settings to ensure proper connectivity when connecting to some network switches in the event that **[autonegotiation](javascript://)** fails.

1. 10

Click the **Driver** tab. This tab lets you view driver details, update the driver, roll back the driver to a previous version, disable the device, and uninstall the device, as well as optionally uninstall the driver.

**Caution**

If you uninstall the driver without a backup copy of the driver to install and Windows cannot install its own version of the driver, you will need to download the correct driver from the manufacturer’s website, likely using a different PC that has a working network connection.

1. 11

Click the **Details** tab. This allows you to browse through additional information about the driver, such as its version and the company that provided the driver, its installation date, and a driver description among other details.

1. 12

Click the **Events** tab. This shows you a history of driver events that may assist with troubleshooting in the event of a problem.

1. 13

Close all open dialog boxes and windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**4-2**IP Version 4

TCP/IP is the most popular networking protocol to allow two computers to communicate in the world today. Although Windows 10 has the capability to use multiple protocols, only TCP/IP is included with Windows 10 for network communication, such as file sharing or accessing the Internet. IP version 4, also known as IPv4, is a standard first deployed in 1983. It defines how to specify and decipher the address of a computer that sent a piece of TCP/IP data, and the address of the computer that will receive it. The IPv4 addressing scheme works whether the computers are right next to each other or if they are located on opposite sides of the globe.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-2aIPv4 Addresses

Each computer must have a unique [**IP address**](javascript://) to communicate on a local area network. If any two computers on the same network have the same IP address, it is impossible for information to be correctly delivered to them.

IPv4 addresses are actually a binary number, 32 bits (binary digits) wide. Each bit can have the value 1 or 0. Computers work with bits and bytes, but people seldom do. IPv4 addresses are most commonly displayed in dotted decimal notation to make it easier for humans to work with the 32-bit address. In this format, an IP address is displayed as four decimal numbers, each decimal number representing an [**octet**](javascript://), separated by periods. An example of an IP address written in dotted decimal notation is 192.168.5.66. In this example, 192 is the first octet, 168 is the second, 5 is the third, and 66 is the fourth and last octet. Each octet represents the decimal number equivalent of the 8 binary bits in that portion of the 32-bit address. An octet value can range between 0 and 255.

The value of the first octet determines the general class of an IPv4 address, as shown in [Table 4-1](javascript://).

**Table 4-1**

### IPv4 Address Classes

| **First Octet Value Range** | **Corresponding Class** |
| --- | --- |
| 0 to 127 | A |
| 128 to 191 | B |
| 192 to 223 | C |
| 224 to 239 | D |
| 240 to 255 | E |

Special cases and considerations that are in the IPv4 class-based system include:

* If the first octet is zero, the remaining octets identify local machines on the same network as the computer sending data. The special IPv4 address 0.0.0.0 is used in routing logic to represent “all other computers.”
* A first octet value of 127 identifies a destination that is local to the computer sending data. The address in this range that is commonly seen is 127.0.0.1, or the loopback address.

**Tip**

Data sent to the [**loopback address**](javascript://) returns to the computer that sent it and does not appear on the actual network. This is useful for troubleshooting, which is covered later in this module.

* A first octet identifying a Class D address represents a multicast address. Computers that belong to the same multicast group have the same multicast address assigned to them. Data sent to that multicast address attempts to deliver copies of the data to all multicast members with the same address. This is useful for application services that run on servers within the network but the client doesn’t know their exact address to reach them, only the multicast address assigned to the service with which it is trying to connect. Class D addresses are not used to identify a single host computer with a unique IPv4 address.
* A first octet identifying a Class E address is reserved for future use and special purposes. Class E addresses are not used to identify a single host computer with a unique IPv4 address.

**Tip**

The special IPv4 address 255.255.255.255 is used as a [**broadcast address**](javascript://) that represents the destination “all computers in this network.” Data sent to this broadcast address cannot leave the local network through a router.

Several ranges of IP addresses are reserved for internal private network use and cannot be routed on the Internet; however, they can be routed internally on corporate networks. A proxy server or [**Network Address Translation (NAT)**](javascript://) must be used to provide Internet access to computers using these addresses. [Table 4-2](javascript://) shows the network addresses that are reserved for internal networks.

**Table 4-2**

### Addresses for Internal Networks

| **IP Address Range** | **Network (in CIDR Notation)** |
| --- | --- |
| 192.168.0.0.–192.168.255.255 | 192.168.0.0/16 |
| 172.16.0.0–172.31.255.255 | 172.16.0.0/12 |
| 10.0.0.0–10.255.255.255 | 10.0.0.0/8 |

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-2bSubnet Masks

An IP address is composed of two parts: a network ID followed by a host ID. Using the concept of a postal address for comparison, the network ID is similar to a street name and the host ID is similar to a house number. When a packet of information is being delivered on a corporate network, the network ID is used to get the packet to the proper area of the network through routers and the host ID is used to deliver the packet to the correct computer connected to a router responsible for its network ID. The total number of binary bits used to define a network ID plus the host ID must equal 32 bits exactly in order to fit in an IPv4 address. The number of bits used to specify the network ID can be variable, anywhere from 0 to 31 of the first bits in the 32-bit address. The host ID uses the bits left over that the network ID does not use. A network architect will decide where the split should happen based upon their design of the network, which is an advanced skill. The split is not arbitrary, so in addition to specifying an IPv4 address for a computer, you must identify where that computer will split its address into a network ID and a host ID.

A [**subnet mask**](javascript://) is another 32-bit address used to define which part of an IP address is the network ID and which part of the IP address is the host ID. If the subnet mask is configured incorrectly, Windows 10 might not be able to communicate with computers on other parts of the network.

The subnet mask is specified separately from the IP address itself. For discussion’s sake, consider this example of a subnet mask value in binary form (blank spaces inserted for readability):

* Subnet mask = 1111 1111 1111 1111 1111 1111 0000 0000

The subnet mask’s bits set to 1 identify what part of an assigned IPv4 address belongs to the network ID. The bits set to 0 in a subnet mask identify what part of an address belongs to the host ID. In this example, this would be interpreted by a computer as the first 24 bits of the IPv4 address identify the computer’s network ID; the last 8 bits of the IPv4 address identify the computer’s host ID.

For convenience, the dotted decimal notation is used to enter the subnet mask value into the IP settings of a network interface. Using dotted decimal notation, the preceding subnet mask binary value would be entered as 255.255.255.0.

The subnet mask octet value of 255 indicates that the corresponding IPv4 address octet belongs to the network ID. The subnet mask octet value of 0 indicates that the corresponding IPv4 address octet belongs to the host ID. For example, consider the following breakdown of an IPv4 address into its network and host ID components given a subnet mask:

* IPv4 address = 192.168.4.1 with subnet mask = 255.255.255.0
* Network ID = 192.168.4.0
* Host ID = 0.0.0.1

If two computers have the same network ID in their respective assigned IPv4 address, they should be able to directly communicate on the same local network through a common device, such as a network switch. If the network ID is not the same, routers must receive the data from one computer and pass it to the destination network for delivery to the target computer. For example, consider the following three IPv4 addresses and a given subnet mask:

* IPv4 address A = 172.16.4.254
* IPv4 address B = 192.168.4.254
* IPv4 address C = 172.16.4.1
* Subnet mask for all three computers = 255.255.0.0

If these three IP addresses are assigned to three different computers on the same local network, and all three computers have the same subnet mask assigned, then each computer would analyze their network ID portion as:

* Network ID portion of address A = 172.16.0.0
* Network ID portion of address B = 192.168.0.0
* Network ID portion of address C = 172.16.0.0

Address A and C have the same network ID; therefore, address C is considered directly reachable from address A. Those two computers will try to send data directly over the local network to each other. However, the computer assigned address A considers address B to be reachable only through a router because their network IDs do not match.

The computers assigned address A and B (and B and C) would not realize that they are on the same local network even though you know you put them on the same physical network. A router would need to be present and configured to relay data by routing traffic between the two network IDs. For example, a computer with address A trying to send to a computer with address B would send a packet to the router, the router would confirm it knew the path to send the packet to address B, then the router would send the packet to the computer with address B. That adds delays in communications, equipment cost, and administrative complexity—but it would work. In advanced networking scenarios, this may even be a required design for other reasons such as network segmentation and rule-based traffic controls, device categorization, and business requirements to name a few justifications. If setting up a router was not realistic and not required, and you just want all three computers to talk to each other, then you could fix the problem by changing address B to an IP address that shares the same network ID as address A and C.

**Note 3**

Analyzing subnet mask octet values other than 255 and 0 is an advanced TCP/IP design topic. See this link for more subnetting information: [https://support.microsoft.com/en-us/help/164015/understanding-tcp-ip-addressing-and-subnetting-basics](https://support.microsoft.com/en-us/help/164015/understanding-tcp-ip-addressing-and-subnetting-basics" \t "_blank).

Documenting subnet mask values with dotted decimal values is not the only way to write a subnet mask value using a shorthand notation. Another way to specify a subnet mask is to write the IPv4 address followed by a slash and a number that identifies the number of contiguous binary ones on the left-hand side of the subnet mask. For example, consider this subnet mask expressed in binary and dotted decimal notation:

* Subnet mask (binary) = 1111 1111 1111 1111 0000 0000 0000 0000
* Subnet mask (dotted decimal) = 255.255.0.0

In the case of the preceding example, there are 16 ones in the subnet mask value; therefore, the IP address and subnet mask value can be written as IPaddress/16. If this subnet mask was applied to the IP address 172.16.34.1, it would be written as 172.16.34.1/16. This notation is commonly referred to as [**classless interdomain routing (CIDR)**](javascript://) notation and is becoming more popular than the older dotted decimal notation.

Default subnet mask values were originally defined by the class of the IPv4 address, as shown in [Table 4-3](javascript://).

**Table 4-3**

### Class-Based Default Subnet Mask Values

| **Class** | **Default Subnet Mask Value** | **Default Subnet Mask Value (in CIDR Notation)** |
| --- | --- | --- |
| A | 255.0.0.0 | /8 |
| B | 255.255.0.0 | /16 |
| C | 255.255.255.0 | /24 |

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-2cDefault Gateways

The Internet and corporate networks are large networks that are composed of many smaller networks. Routers control the movement of packets through the networks. An individual computer is capable of delivering packets on the local network, but not to remote networks. To deliver packets to a remote network, the packet must be delivered to a router. The router sends the packet on toward its final destination.

A computer’s [**default gateway**](javascript://) is a router on the local network that is used to deliver packets to remote networks. The default gateway is identified in the computer’s IP settings by entering the IP address assigned to the router’s local network connection.

**Tip**

If a Windows 10 computer has multiple network interfaces configured, each with its own IPv4 settings, only one interface is typically configured with a default gateway setting to identify to where to send network traffic to communicate with computers beyond the local network.

If the default gateway is configured incorrectly, the computer cannot communicate outside the local network. This means Internet connectivity is not possible and the computer will likely not have access to all resources within a corporate routed environment.

Windows 10 stores the default gateway setting internally as part of a larger table, called the [**routing table**](javascript://). The routing table can be useful in advanced scenarios where the computer must track where to send data for multiple network interfaces with multiple gateways defined.

**Note 4**

Windows includes the route command-line tool to manage and view the routing table; for example, you can view the table with the route print command.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-2dDNS

[**Domain Name System (DNS)**](javascript://) is a part of TCP/IP and is essential to communicate on a TCP/IP network. The most common use for DNS is to resolve (i.e., translate) host names to IP addresses. When you access a website, you access a location, such as [www.microsoft.com](http://www.microsoft.com/" \t "_blank). This is a [**fully qualified domain name (FQDN)**](javascript://), which is a name useful to humans. Computers cannot connect to a service on the Internet directly using just the name. Instead, they convert the host name to an IP address and then access the service using the IP address.

DNS serves other functions beyond converting the name of a website to an IP address. In a corporate network, DNS is also required for Windows 10 computers in an Active Directory domain-based network to find domain services, controllers, and sign in.

Given how essential the DNS function can be to a workstation, you can specify a primary and secondary DNS server address for any network connection. To avoid operational problems, it must be clear how Windows 10 will use multiple DNS server entries if they are defined. When a program asks Windows 10 to translate a host name to an IP address, it picks the IP of one of the DNS servers and sends it a DNS query. There is no guarantee that the primary DNS server will always be the server queried first, but typically it is checked first.

When the computer receives a response from a DNS server telling it an answer has been found, or a response that no matching information is available, Windows 10 considers the DNS server active and functional. It is only when the DNS server fails to respond at all that Windows 10 sends the request to one of the other defined DNS servers. A response that a name couldn’t be translated into an IP address is still a valid response and the other DNS servers will not be queried for an answer to the same question.

Windows 10 also provides a text file called hosts in the folder C:\Windows\System32\drivers\etc\ that maps IP addresses to host names. Entries in the hosts file take precedence over data retrieved from DNS servers. Custom data can be entered into the hosts file to override DNS server data; however, this is a local file and can be difficult to remotely administer.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-2eWINS

[**Windows Internet Naming Service (WINS)**](javascript://) is a legacy technology used to resolve [**NetBIOS**](javascript://) names to IP addresses. In addition, it stores information about services such as domain controllers. WINS is primarily used for backward compatibility with older NetBIOS-based networks. NetBIOS names can be used to access network services, such as file shares. Windows 10 is capable of using WINS but uses DNS as its primary name-resolution mechanism. IPv6 does not support using WINS.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

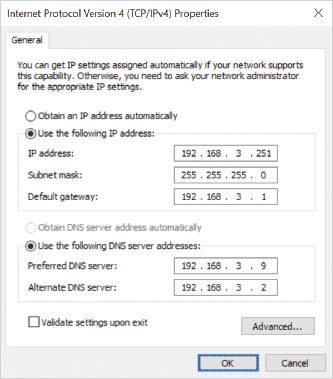
## 4-2fMethods for Configuring IPv4

Windows 10 supports configuring IPv4 settings with static configuration, automatic assignment, and IPv4 configuration commands.

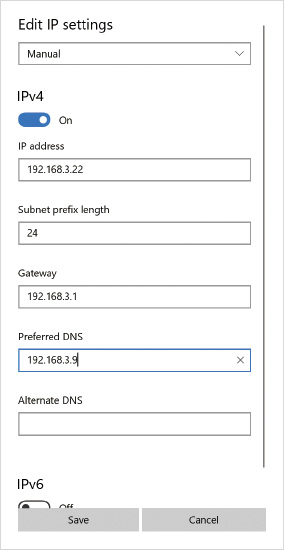
### Static Configuration

All IP configuration information can be manually entered on each Windows 10 computer, but this approach is not very efficient. With each manual entry, the risk of a typographical error arises. In addition, if the IP configuration changes, visiting each computer to modify the configuration can be an enormous task. Manually entering IP configuration information is called static configuration and can be done from Settings or from the Control Panel using different interfaces. [Figure 4-6](javascript://) shows TCP/IP version 4 configured with a static IP address using the Network and Internet Control Panel application. [Figure 4-7](javascript://) shows an IPv4 static address and settings being applied with the Network and Internet settings.

**Figure 4-6Network and Sharing Center, Network Connection IPv4 Properties, Static IPv4 Configuration**



**Figure 4-7Network and Internet Settings, Network Connection IPv4 Properties, Static IPv4 Configuration**



Enlarge Image

### Automatic Assignment

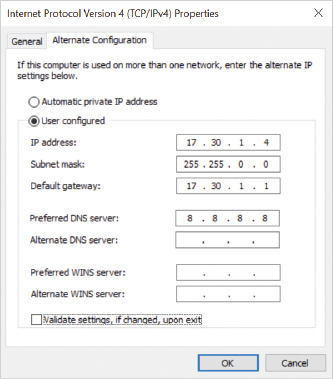
Automatic IPv4 configuration is usually preferred and accomplished with [**Dynamic Host Configuration Protocol (DHCP)**](javascript://) servers, which support an automated mechanism used to assign IP addresses, subnet masks, default gateways, DNS servers, WINS servers, and other IP configuration information to network devices. Automating this process avoids the problem of information being entered incorrectly. If a change needs to be made to the IP address information, you modify the configuration of the DHCP server. The DHCP server can be configured with a range of IP addresses to hand out, specific exclusions to never hand out, or specific reservations that are given out to DHCP client computers with specified MAC addresses. Obtaining IP configuration information automatically is called dynamic configuration.

If Windows 10 is configured to use dynamic IP configuration and is unable to contact a DHCP server, the default action is to use an [**Automatic Private IP Addressing (APIPA)**](javascript://) address. These addresses are on the 169.254.0.0/16 network.

APIPA is designed as a solution for very small networks with no Internet connectivity requirements. When two computers generate APIPA addresses, they are able to communicate with each other because they are considered to be on the same local network (i.e., 169.254.0.0), with a randomly generated unique host address in the last two octets. Unfortunately, APIPA addresses have little benefit in most scenarios because no default gateway is configured and no DNS server is assigned. This means that the computers cannot access the Internet. Consequently, a computer using an APIPA address is usually just a sign that the computer could not contact a DHCP server.

When a network connection is set to obtain its IP address automatically, Windows 10 also allows you to configure a static set of alternate IP configuration options from the Network and Internet control panel application. If a DHCP server cannot be contacted, the [**alternate IP configuration**](javascript://) is used instead of APIPA but only if the alternate IP configuration is defined ahead of time. One advantage to specifying the alternate IP configuration is that a gateway can be specified, which APIPA does not allow. [Figure 4-8](javascript://) shows the Alternate Configuration tab for Internet Protocol Version 4.

**Figure 4-8Network and Sharing Center, Network Connection IPv4 Alternate Configuration**



### IPv4 Configuration Commands

The administrator may optionally decide to use the **[netsh](javascript://)** command-line tool or Set-NetIPAddress PowerShell cmdlet to assign a static IP address to a network interface. For example, netsh interface ipv4 set address name=“Ethernet3” source=static address= 72.16.12.35 mask=255.255.0.0 gateway=172.16.0.1 tells the Network Shell utility to switch to the interface context and set the IPv4 address detail for the interface referenced with the name Ethernet3. The netsh utility has an interactive mode where these settings can be applied sequentially using its built-in menu system; however, netsh is commonly used by running one long command with the required command-line parameters. Some settings might require running the netsh command more than once. For example, the previous netsh command set the IP address, subnet mask, and default gateway, but the command netsh interface ipv4 set dnsservers name=“Ethernet3” source=dhcp is required to set the network interface Ethernet3 to obtain DNS server addresses from DHCP as a subsequent step.

**Activity 4-3**

### Viewing and Configuring IPv4

**Time Required:**10 minutes

**Objective:**View and configure IPv4 settings

**Description:**When you are troubleshooting network connectivity, it is essential that you understand how to view the existing IPv4 configuration to evaluate whether it is a problem. Basic IPv4 settings can be changed using the Settings app; however, the advanced settings are still accessed from the legacy Control Panel interface. In this activity, you view and configure IPv4 settings using the Settings app and the graphical interface from Control Panel.

**Note 5**

To avoid disrupting communications, the changes you are making in this activity are not saved and you will be asked to cancel your changes.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click the **Start** button and then click **Settings**.

1. 3

Click **Network & Internet**. If not already selected, click **Status** in the left navigation pane to display the overall network status for your computer.

1. 4

In the Status page’s subsection titled Network status, below the connection status, click the connection’s **Properties** button (which may be a link called Change connection properties in earlier Windows 10 editions) to display the connection’s settings.

1. 5

In the connection’s settings, locate a heading called IP settings and then click **Edit**.

1. 6

In the Edit IP settings window that opens, you should see Automatic (DHCP) is the current selection. Note that if you have already worked through later modules and their activities, you may already have your connection setting set to Manual. Click the arrow and then click **Manual**.

1. 7

Options to turn on and configure an IPv4 address and an IPv6 address will be displayed. Click to turn on IPv4, if it is not already on.

1. 8

In the IP address box, type **192.168.1.100**.

1. 9

In the Subnet prefix length box, type **24**. Note that you are specifying the subnet mask using a CIDR value and not a dotted decimal notation in this case.

1. 10

In the Gateway box, type **192.168.1.1**.

1. 11

In the Preferred DNS box, type **192.168.1.5**.

1. 12

Note that no advanced IPv4 settings option appears in this window.

1. 13

Click **Cancel**. If you saved these settings, the network interface would change to a static IP address. Because you do not want to disrupt activities in later modules, you will not save your changes and will leave the adapter configuration as Automatic (DHCP).

1. 14

Exit the Settings app.

1. 15

Click the **Start** button, in the search box type **control panel**, and then press **Enter**.

1. 16

Click **Network and Internet** and then click **Network and Sharing Center**.

1. 17

Below the View your active networks heading, and to the right of Connections, click the named network connection. The name of the network connection will be different on different computers but will likely be called Ethernet.

1. 18

Click the **Properties** button.

1. 19

Click to highlight **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**. This shows you the basic configuration of IPv4. By default, an IP address and DNS server address are obtained automatically through DHCP.

1. 20

Click **Use the following IP address**. This allows you to enter in a static IPv4 configuration.

1. 21

In the IP address box, type **192.168.1.100**.

1. 22

If necessary, in the Subnet mask box, type **255.255.255.0**. This is the same subnet mask you entered earlier in this activity, but this time you are specifying dotted decimal notation instead of CIDR notation.

1. 23

In the Default gateway box, type **192.168.1.1**.

1. 24

If necessary, click **Use the following DNS server addresses**.

1. 25

In the Preferred DNS server box, type **192.168.1.5**.

1. 26

Click the **Advanced** button. In the Advanced TCP/IP Settings, you can configure additional options. On the IP Settings tab, you can configure multiple IP addresses and default gateways for the network connection.

1. 27

Click the **DNS** tab. This tab allows you to control how DNS lookups are performed and whether this computer attempts to register its name with the DNS servers by using dynamic DNS.

1. 28

Click the **WINS** tab. This tab allows you to configure how WINS lookups are performed. Some networks prefer to disable NetBIOS over TCP/IP to reduce network broadcasts; however, some legacy applications require NetBIOS, so test your applications before disabling NetBIOS over TCP/IP.

1. 29

Click **Cancel** to close the Advanced TCP/IP Settings dialog box.

1. 30

Click **Cancel** to close the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box without saving any changes. If you saved these settings, the network interface would change to a static IP address. Because you do not want to disrupt activities in later modules, you will not save your changes and will leave the adapter configuration as automatic.

1. 31

Click **Cancel** to close the Ethernet Properties dialog box.

1. 32

Click **Close** to close the Ethernet Status dialog box.

1. 33

Close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-2gEssential Networking Tools

Several key utilities or PowerShell cmdlets can be used to configure and diagnose IP settings. Some of these utilities make low-level changes to the TCP/IP functionality. Some of these changes will be denied unless the utility or command is run from an administrator elevated prompt. [Table 4-4](javascript://) shows some of the common IP configuration and troubleshooting utilities.

**Table 4-4**

### Common Command-Line IP Troubleshooting Utilities

| **Utility** | **Description** |
| --- | --- |
| hostname | Displays the host name of the computer on which it is run. The [**hostname**](javascript://) utility is useful when you are at a computer and do not know the computer name. |
| ipconfig | Shows the current IPv4 and IPv6 configuration. You can also display some DNS information. |
| ping | Verifies connectivity to a destination by sending an ICMP request packet. |
| tracert | Provides similar information as the ping command but shows response times for every router on the path to the destination. Note that the routers consider ICMP requests low priority, which can provide unreliable latency information. |
| pathping | Provides similar information as **[tracert](javascript://)**; however, **[pathping](javascript://)** sends 100 ICMP requests per router in an attempt to identify packet loss. |
| route | Displays and modifies information in the local routing table. |
| netstat | Displays statistics and information about network connections. |
| nbtstat | Displays information about legacy NetBIOS over TCP/IP. **[Nbtstat](javascript://)** can display the NetBIOS names known to the computer and purge the cache. |
| getmac | Displays MAC addresses associated with network adapters. Use getmac /v to obtain a more detailed output that includes the adapter name in addition to the adapter identifier. Use getmac /s HostIP /u userid /p password to obtain MAC addresses from a remote system. |
| arp | Displays and modifies the contents of the address resolution protocol (ARP) table, which maps IP addresses to MAC addresses. Use arp -a or arp -g to display the contents of the ARP table. Uses arp -d HostIP to delete an entry from the ARP table. |
| netsh | Modifies network configuration. Most of this functionality is now replicated in Windows PowerShell cmdlets. |
| nslookup | Queries DNS records directly from a DNS server. This is used to verify whether DNS records on various servers are configured correctly. |

Enlarge Table

### Ipconfig

The [**ipconfig**](javascript://) command by itself displays basic TCP/IP settings of all active network connections at a command prompt. Several command-line options make the command versatile in troubleshooting TCP/IP settings, as well. [Table 4-5](javascript://) shows some of the most useful.

**Table 4-5**

### Common Ipconfig Options for Troubleshooting TCP/IP

| **Command** | **Description** |
| --- | --- |
| ipconfig /all | Displays all TCP/IP configuration settings in verbose detail. This includes DNS servers, the default gateway, and DHCP server (if applicable). |
| ipconfig /release | Removes dynamically assigned IP addresses from network connections. This disables TCP/IP operations on those interfaces. |
| ipconfig /renew | Attempts to renew IP addresses for all network connections that are configured to obtain an IP address automatically. If the renewal of a network connection’s current IP address is refused by the DHCP server, the IP address is lost and a new IP address must be assigned by the DHCP server. |
| ipconfig /registerdns | Forces Windows 10 to register its name and IP address with the DNS server defined on a network interface’s properties. This process is performed at startup. So, it is typically done manually only if the IP address has recently changed. |
| ipconfig /displaydns | Displays all cached DNS lookup data, including negative acknowledgements that a name was not found using DNS. |
| ipconfig /flushdns | Deletes the cached DNS lookup data, including wrong results or negative acknowledgements that may have been corrected at the DNS server since they were first cached. Useful if you don’t want to wait for the cached data to naturally expire based on the response’s [**time to live (TTL)**](javascript://). |

### Ping

The [**ping**](javascript://) command confirms basic IP connectivity between the computer that it is run on and a specified target host. The ping command tests the capability of network data to reach a target and return; it does not confirm that applications on the target computer are operating properly. The target host may be identified with an IP address or DNS name. The ping utility sends out a special type of packet called an ICMP request packet. The computer that receives this packet may reply with a response ICMP packet. The ping utility measures the total time it takes for the request to get to the destination and response packet to get back to the computer running the ping command. This latency time is measured in milliseconds (ms).

**Note 6**

Some network devices and firewall software, such as Windows Defender Firewall, may actively block ping ICMP traffic even though the network connection is perfectly healthy.

[Table 4-6](javascript://) shows some useful command-line switches for the ping command.

**Table 4-6**

### Common Ping Options for Troubleshooting

| **Command** | **Description** |
| --- | --- |
| ping -t | Continues pinging indefinitely |
| ping -a | Forces a reverse DNS lookup to identify the FQDN associated with an IP address |
| ping -n | Specifies the number of requests to send |
| ping -4 | Forces use of IPv4 |
| ping -6 | Forces use of IPv6 |

### Netstat

The [**netstat**](javascript://) command can display different types of TCP/IP statistics for active software and connections. Many options are available that can be reviewed by typing netstat /? at the command line. Several common netstat command-line options used in troubleshooting network connections are shown in [Table 4-7](javascript://).

**Table 4-7**

### Common Netstat Options for Network Troubleshooting

| **Command** | **Description** |
| --- | --- |
| netstat -a | Displays all connections including active and listening ports waiting for a connection |
| netstat -e | Displays statistics about total data sent and received |
| netstat -r | Displays the routing table |
| netstat -b | Displays the name of a program responsible for a connection or listening for one |
| netstat -o | For each active or waiting connection, displays the process ID of the process that owns the connection |

The netstat command is useful for documenting the network activity and connections at a moment in time. You can view the information on screen, but it is often easier to view if you direct the output to file.

### Nslookup

The **[nslookup](javascript://)** command can be used at the command prompt to look up a DNS entry from a specific DNS server, or it can provide an interactive text-based console for advanced DNS queries.

Nslookup is a powerful tool because it can query a DNS server directly, even if it is a different one than the network settings on a local computer are using right now. The debug feature allows the administrator to deeply diagnose what data can be returned to the Windows 10 client and why. Nslookup can be used to contrast answers from external Internet DNS servers and from local DNS servers that might be customized to serve LAN clients and Active Directory users and computers. Third-party web-based DNS lookup tools can be pretty, but they are limited in how deeply they can analyze responses from DNS servers, and they don’t report on internal DNS servers. Using nslookup can be an essential pro-level troubleshooting tool.

To fully appreciate the utility, the administrator must have knowledge of the type of records a DNS server includes, such as:

* A—Maps a host name to an IPv4 address
* AAAA—Maps a host name to an IPv6 address
* PTR—Maps an IPv4 or IPv6 address to a host name
* MX—Identifies the mail server(s) responsible for managing email for a domain
* NS—Identifies the DNS servers that authoritatively hold custom DNS data for a domain
* TXT—Text records associated with a domain that can be used for a variety of reasons, for example: vouch for domain ownership, implement Sender Policy Framework (SPF) to vouch for servers sending email on behalf of the domain, DomainKeys Identified Email (DKIM) to publish public SSL certificate records used to validate signed email messages and headers

**Note 7**

To review nslookup commands, start nslookup in interactive mode by entering nslookup on the command line and then pressing Enter. At the nslookup interactive prompt, >, type help.

### PowerShell Cmdlets for Networking

[Table 4-8](javascript://) shows some of the common IP configuration and troubleshooting PowerShell cmdlets.

**Table 4-8**

### PowerShell IP Configuration and Troubleshooting Cmdlets

| **PowerShell Cmdlet** | **Description** |
| --- | --- |
| Clear-DnsClientCache | Deletes all contents from the DNS client cache, similar to ipconfig /flushdns. |
| Get-DnsClientCache | Retrieves the contents of the DNS client cache, similar to ipconfig /displaydns. |
| Get-NetAdapter | Gets the basic network adapter properties. |
| Get-NetIPAddress | Gets IP address configuration, similar to ipconfig. |
| Get-NetIPConfiguration | Gets network configuration including network profile name, IP addresses, gateway address, and DNS servers; similar to ipconfig. |
| Get-NetIPv4Configuration | Gets global IPv4 settings, such as ICMP settings, default hop limit, neighbor cache limit, and the multicast configuration. Note that these are global IPv4 protocol settings and not IP address information. |
| Get-NetIPv6Configuration | Gets global IPv6 settings, such as ICMP settings, default hop limit, neighbor cache limit, values for temporary addresses, and the multicast configuration. Note that these are global IPv6 protocol settings and not IP address information. |
| Get-NetRoute | Gets routing table information, similar to the route command-line utility. |
| Get-NetTCPConnection | Gets current TCP/IP network connections including local and remote IP addresses, ports and connection state; similar to the netstat command-line utility. |
| New-NetIPAddress | Creates and configures an IP address. |
| Remove-NetIPAddress | Removes an IP address and its configuration. |
| Resolve-DnsName | Perform a DNS query for a specified name, similar to nslookup command-line utility. |
| Set-NetIPAddress | Modifies the configuration of an existing IP address. |
| Set-NetIPv4Configuration | Sets global IPv4 settings, such as ICMP settings, default hop limit, neighbor cache limit, and the multicast configuration. Note that these are global IPv4 protocol settings and not IP address information. |
| Set-NetIPv6Configuration | Sets global IPv6 settings, such as ICMP settings, default hop limit, neighbor cache limit, values for temporary addresses, and the multicast configuration. Note that these are global IPv6 protocol settings and not IP address information. |
| Test-NetConnection | Display diagnostic information for a connection, supports ping test, TCP test, route tracing, route selection diagnostics, similar to ping and tracert command-line utilities. |

Enlarge Table

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-2hTroubleshooting IPv4

To successfully troubleshoot IPv4-based communications, the technician should follow an incremental process that has proven successful in most situations. IPv4 has been in use for a very long time. Many problems actually have simple causes, such as a connection being in the wrong state or a feature turned off unexpectedly.

A common approach is to perform the following in order:

1. Confirm current settings.
2. Validate IPv4 connectivity.
3. Verify DNS name resolution.
4. Verify data connections.

### Confirm Current Settings

The existing IPv4 settings should be confirmed. Assumptions about what settings are active lead to incorrect troubleshooting progress. The ipconfig and netsh utilities can display the current settings from the command line; for example, netsh interface ipv4 show config will show all network interface IPv4 settings. The PowerShell cmdlets Get-NetIPAddress and Get-NetIPConfiguration can also display the current IP address settings. If the IPv4 address looks valid, it is possible that the default route (i.e., gateway) or routing table is incorrect. The default route can be displayed with the ipconfig or route command, or the Get-NetRoute and Get-NetIPConfiguration cmdlets. If all settings appear correct, the computer’s connectivity with those settings must be validated.

### Validate IPv4 Connectivity

If all settings appear correct, the ping utility (or Test-NetConnection cmdlet) can be used to confirm that the computer can ping its own loopback address. If the command is successful, the TCP/IP IPv4 protocol is functional on the computer.

The ping command can be used to ping a local host, such as the default gateway. If the local default gateway can be pinged, connectivity to the local network and the default gateway are validated in one attempt.

If the router can be pinged, attempt to ping a remote host using its IPv4 address. If this fails, confirm the path the traffic is taking with either the pathping or tracert commands.

### Verify DNS Name Resolution

If IPv4 communications to remote hosts work when the raw IP address is specified in a command, but not by name, a DNS issue likely exists. The nslookup utility or Resolve-DnsName cmdlet can be used to query DNS servers directly and confirm the lookup is working as expected.

Confirm the correct DNS servers are specified on network settings manually or automatically through DHCP with the ipconfig utility or the Get-NetIPConfiguration cmdlet. If the wrong servers were entered, that should be corrected first. While troubleshooting, if there are multiple DNS servers specified, consider simplifying the list to just one server that you expect has the correct data.

The DNS resolver caches data, and that data may contain obsolete data or invalid responses. The DNS data being cached can be displayed with ipconfig /displaydns or the Get-DnsClientCache cmdlet to confirm that expected answers are being correctly obtained by the Windows computer from either the local Hosts file or the DNS server(s). If the problem was with DNS data and it has been corrected, the cache data can be purged with ipconfig /flushdns or the Clear-DnsClientCache cmdlet to provide a clean start to name resolution.

The DNS cached data tells you what answer the workstation received, but not from which DNS server, and not if the data the DNS server is holding is correct.

A common but subtle mistake is configuring a domain-joined workstation with an ISP’s DNS server in addition to a corporate domain DNS server. When the workstation tries to look up DNS data to find corporate domain servers, it may ask the ISP’s DNS server where they are located instead of the domain DNS server. You can specify a preferred order for Windows 10 to query DNS servers, but you cannot restrict Windows 10 from using both interchangeably. The ISP DNS server sends back a valid response—the domain servers’ DNS data (e.g., where to find domain-specific Kerberos, global catalog, and LDAP services) does not exist in its database—and the client caches the response as a valid lookup result saying those services were not found. As a result, domain operations are disrupted and fail to operate correctly on the workstation. When the workstation is restarted by the user, it might go back to working with the correct domain DNS server. The workstation user might report intermittent overall failures and annoyance as a result.

### Verify Data Connections

If basic IP communications and name resolution appear healthy, the problem might be a result of data filtering by a firewall restriction or corruption. Any computer or device between the local client and the destination might be filtering data connections, disallowing them entirely. Windows 10 has a firewall component built in to filter inbound and outbound data connections, which is covered later in this module.

Many server-based data services listen on a specific data port. The Transmission Control Protocol (TCP) portion of TCP/IP allows an application to identify itself with a specific port value. The IP address identifies the computer itself; the TCP port identifies the listening application on that computer. Many third-party tools report the status of TCP ports for a given remote IP address. Windows 10 can report active port connections on the computer using the netstat command or the Get-NetTCPConnection cmdlet.

A crude test to check for connectivity to remote servers is to use the telnet application on the local computer to attempt a connection to a remote active TCP port. The telnet utility is available for installation as part of Windows, but it is not installed by default. It can be installed by opening Control Panel, Programs, Programs and Features, and selecting the task Turn Windows features on or off. The telnet client can then be selected and installed.

The telnet program provides an interactive interface that normally connects to a telnet server on its default TCP port number. A different port number can be specified on the command line, one that is used by a service other than telnet. For example, the mail server protocol for the Simple Mail Transfer Protocol (SMTP) is port 25. The telnet command telnet [mail.example.com](http://mail.example.com/" \t "_blank) 25 opens an interactive session with the mail server, identified by the name [mail.example.com](http://mail.example.com/" \t "_blank), which is listening for connections on TCP port 25. If the data connection is allowed, the mail server greeting should be displayed. If it is, this confirms some level of data connectivity is allowed.

Additional filtering or data corruption may happen after the initial TCP connection to give the impression of a data communication problem. To see the full network conversation between two computers, a utility that can capture the network conversation would have to be employed. Microsoft had previously created two such utilities called Message Analyzer and Network Monitor. These were not included by default with Windows 10 but used to be available as a free download. Both utilities have been retired, and Microsoft has not continued development of a similar network traffic capture tool. You may still find that someone has a download of the older free tools, but remember that they are no longer patched or developed. Network Monitor itself has been deprecated before Windows 10 and should definitely not be used with Windows 10.

Installing a full network monitoring tool isn’t always practical or desirable. Consider that Windows 7 introduced the capability to record network traffic using a network capture feature built into the operating system with the netsh utility (e.g., netsh trace). Windows 10 version 1809 also introduced a new packet-level monitoring tool called Packet Monitor (pktmon.exe) that runs from the command line and allows you to observe data in real-time or log data to a human readable or encoded data file (e.g., a data file with the .etl file extension) that can be opened in a tool like Message Analyzer.

**Note 8**

A popular open source alternative to a legacy tool like Message Analyzer is Wireshark, which is also supported by the Packet Monitor utility starting with Windows 10 version 2004. To learn more about Wireshark, see [https://wireshark.org](https://wireshark.org/" \t "_blank).

**Activity 4-4**

### Using Ipconfig, Netsh, and PowerShell to View Basic IPv4 Data

**Time Required:**15 minutes

**Objective:**Use ipconfig, netsh, and PowerShell to view and configure IPv4

**Description:**Windows 10 includes ipconfig, netsh, and PowerShell cmdlets to view and configure IPv4 information at the command line. These utilities and cmdlets can also be used for scripting. Ipconfig is used to view IPv4 configuration or release and renew IP configuration from a DHCP server. Netsh can be used to configure IPv4. PowerShell allows you to run cmdlets that can display and configure details using an object-based approach. In this activity, you use ipconfig and netsh to view and configure IPv4. Several PowerShell cmdlets are used to show IPv4 configuration details, test connectivity with ping/ICMP tests, and view resulting DNS cached data.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, in the search box type **cmd**, right-click **Command Prompt**, and then click **Run as administrator** on the shortcut menu.

1. 3

If you are prompted by a User Account Control window, click **Yes**.

1. 4

At the command prompt, type **ipconfig** and then press **Enter**. This command displays a summary of your IPv4 and IPv6 information.

1. 5

Type **ipconfig /all** and then press **Enter**. This command displays more detailed IP configuration information.

1. 6

Note that if you have completed later modules that have reset your network connection address to static instead of assigned automatically and you are repeating this activity, then skip this step and the next. Type **ipconfig /release** and then press **Enter**. This command releases the DHCP address on your computer. Notice that no IPv4 address is listed in the results.

1. 7

Type **ipconfig /renew** and then press **Enter**. This command renews a DHCP address on your computer or obtains a new one. Notice that the newly acquired IPv4 address is displayed. Note that the IPv4 address may be the same as the adapter had assigned previously. DHCP server implementations support the option of the client identifying the previous IP it had and asking for it again if it is still available.

1. 8

Type **netsh** and then press **Enter**. Netsh can be used in an interactive mode where you navigate through menu levels to view information.

1. 9

Type **interface** and then press **Enter**. This command changes to the interface context, where you can get more information about network interface configuration.

1. 10

Type **ipv4** and then press **Enter**. This command changes to the IPv4 context, where you can get more information about IPv4 configuration.

1. 11

Type **show** and then press **Enter**. This command displays a list of the information that can be displayed.

1. 12

Type **show addresses** and then press **Enter**. This command shows the IPv4 addresses that are used by this computer.

1. 13

Type **set address** and then press **Enter**. This command shows help information on how to configure an IP address for DHCP or as static. If a command is missing required information, the help screen for that command is automatically output.

1. 14

Type **..** and then press **Enter**. This will change the interactive context level back one level.

1. 15

Type **?** and then press **Enter**. This will display a long list of commands inherited from the netsh context in general, commands available in the current netsh context, and sub-contexts you can drill into.

1. 16

Type **exit** and then press **Enter**. This will exit the netsh interactive mode.

1. 17

Type the command **netsh interface ipv4 show addresses** and then press **Enter**. This noninteractive use of netsh will return the same result as the interactive commands you entered earlier.

1. 18

Close the command prompt and all other open windows.

1. 19

Right-click the **Start** button and then click **Windows PowerShell**.

1. 20

In the Windows PowerShell window that opens, type **Get-NetIPConfiguration** and then press **Enter**. Note the IPv4Address listed for any reported interfaces.

1. 21

Type **Resolve-DnsName -Name localhost** and then press **Enter**. Note the two loopback addresses that are reported in the results, one an IPv4 address and one an IPv6 address.

1. 22

Type **Test-NetConnection 127.0.0.1 -traceroute** and then press **Enter**. Note the reported value of PingSucceeded.

1. 23

To clear the DNS cache, type **ipconfig /flushdns** and then press **Enter**. This is not a PowerShell command but can be safely executed in a PowerShell window. This is not true for all legacy command-line utilities. Typically, PowerShell cmdlets can do the equivalent operation in a PowerShell script or window.

1. 24

Type **Clear-DnsClientCache** and then press **Enter**. This is the equivalent of the previous ipconfig /flushdns command.

1. 25

Type **Test-NetConenction** [www.novell.com](http://www.novell.com/" \t "_blank) and then press **Enter**. This will both ping the site [www.novell.com](http://www.novell.com/" \t "_blank) and populate the DNS cache with data that resolves the name [www.novell.com](http://www.novell.com/" \t "_blank) with its DNS equivalent data. Note that if you do not have Internet connectivity, this command will fail.

1. 26

Type **Get-DnsClientCache -Entry “**[www.novell.com](http://www.novell.com/" \t "_blank)**”** and then press **Enter**. If you have Internet connectivity, this will display the DNS client cache entry for only the name [www.novell.com](http://www.novell.com/" \t "_blank), unlike ipconfig /displaydns, which will display the entire DNS client cache.

1. 27

Type **Get-DnsClientCache -Entry “**[www.nothere.com](http://www.nothere.com/" \t "_blank)**”** and then press **Enter**. Note that PowerShell can report data that is not found with what appears as alarming red text when it really is just reporting only that it could not find a match.

1. 28

Close the Windows PowerShell window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**4-3**IP Version 6

IPv6 is the replacement for IPv4. The creators of IPv4 could not have anticipated the expansion of the Internet and, as a result, IPv4 has some serious shortcomings when used for global networking. IPv6 addresses these shortcomings.

Improvements found in IPv6 include:

* Increased address space
* Hierarchical routing to reduce the load on Internet backbone routers
* Simpler configuration through automatic address management
* Inclusion of encryption services for data security
* Quality of service
* Capability to add and extend new features

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-3aIPv6 Address Notation

The address space for IPv4 on the Internet has essentially been depleted; IPv6 has a significantly larger address space. IPv6 addresses are 128 bits long, while IPv4 addresses are only 32 bits long. IPv6 provides many more addresses than are available in IPv4.

IPv6 has many more addresses than would normally be required for computing devices, but it is designed for ease of use rather than efficiency of allocation. Many of these addresses will probably never be assigned to a host. In fact, only one-eighth of the total address space is allocated for Internet-accessible addresses.

IPv6 addresses are represented in hexadecimal for convenience, where each hexadecimal value actually represents the equivalent 4-bit binary value. Hexadecimal values are grouped into four-digit segments separated by colons for readability. The total address length is a maximum of 32 hexadecimal digits. An example of an IPv6 address is 222D:10B5:3355:00F3:8234:0000:32AC:099C.

At times, you will see shorter IPv6 addresses than the previous example, and there are some formatting rules to help understand why. To simplify the expression of IPv6 addresses, any group of four hexadecimal digits can drop leading zeros, leaving at least one digit visible. The IPv6 address in the previous example can be simplified to 222D:10B5:3355:F3:8234:0:32AC:99C.

When an IPv6 address contains a long set of zeros, the zeros can be compressed to a double colon — :: — to signify that the data is all zeros in that part of the IPv6 address. For example, the multicast address FF02:0:0:0:0:0:112A:CC87 could be shortened to FF02::112A:CC87. This type of zero compression can be used only once per address. In general, it doesn’t matter if the compression is done on the right or left side of the address; what really matters is that it can be done only once.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-3bIPv6 Address Types

The format of an IPv6 address is more complex than an IPv4 address. Depending on the purpose of the IPv6 address, analyzing the different parts of the address changes. Unlike IPv4 with its network and host ID with a subnet mask, IPv6 can be much more complicated and variable. The full decomposition of different address types is an advanced topic beyond the scope of this book. The numbers on the left side of a written IPv6 address provide a clue as to what type of address it is, which is covered in this module.

IPv6 uses the CIDR notation of adding a slash and a number after the slash to the end of the IPv6 address. That number indicates the number of bits on the left side of the written address that makes up the network portion of the address. This network portion of the address is referred to in general as the [**address prefix**](javascript://). For example, 10F0:0:0:6501::/64 is a possible IPv6 prefix. The address prefix contains information that helps devices, such as routers, decide how to move data among networks and the links between those networks.

It is important to recognize that IPv6 is a young standard and it is still evolving. Some of the format information current today may change over time.

Knowing the type of address helps to set expectations of how data can be delivered to an interface. The designers of IPv6 knew that the end point for delivery could be a physical device such as a network card, a wireless device, or some program that is receiving data and acting as an end point for IPv6 data. The end point for IPv6 data delivery is called an interface. A single computer is typically called a node, which is capable of running multiple interfaces. Each interface can have one or more IPv6 addresses assigned to it. Recognizing the address type by its address prefix (see [Table 4-9](javascript://)) is a required skill to analyze IPv6 addresses assigned to an interface.

**Table 4-9**

### Common IPv6 Address Prefixes

| **IPv6 Address Type** | **Address Prefix** |
| --- | --- |
| Link-local unicast | FE80::/64 |
| Global unicast | 2000::/3 |
| Unique local unicast | FC00::/7 |
| Site-local unicast (deprecated) | FEC0::/10 |
| Multicast | FF00::/8 |

### Link-Local Unicast

A [**unicast**](javascript://) address defines a delivery destination that identifies a specific single interface. Data sent to or from link-local unicast addresses is not allowed to pass through IPv6-aware routers. A link-local unicast address is automatically assigned to any active interface on the computer by Windows 10. A link-local address allows computers in a local network to communicate with one another without requiring the use of a router. In IPv4, this same link-local behavior is provided by Automatic Private IP Addressing (APIPA), which generates IP addresses in the range 169.254.0.0 to 169.254.255.255.

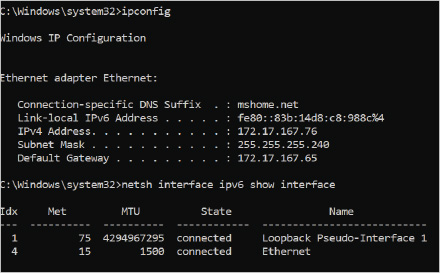
The address prefix of a link-local address in IPv6 is FE80::/64. The last 64 bits of the address are randomly generated by Windows 10 as the host ID. An example of a link-local unicast address is FE80::F9:1435:305E:DFF2.

A computer can have more than one link-local address if it has multiple network interfaces. The address prefix for each link-local address on that computer is exactly the same. When the computer is sending to a link-local address, the routing table cannot tell which interface to use to send data to a destination link-local address. If this causes a problem, the link-local address can be extended with a zone ID.

Each network interface in Windows 10 is assigned a network interface ID, otherwise known as a zone ID. The zone ID can be used to identify what network interface is used to send the data. The syntax to specify a zone ID is IPAddress%ZoneID, where IPAddress is the destination link-local address and ZoneID is the interface ID of the network interface.

To see the current identifier for each network interface, open a command window and issue the ipconfig command or netsh interface ipv6 show interface command. The output of the netsh command lists a column titled Idx (shown later in [Figure 4-9](javascript://)), which identifies the interface ID for each interface listed. The ipconfig output lists it at the end of each link-local address displayed below each connection.

**Figure 4-9Netsh and Ipconfig Output Displaying Interface Index ID**



**Tip**

If a command such as ping fe80::613a:325f:5e1b:d9b4 returns the error result “Destination host unreachable” or “PING: transmit failed. General failure,” it may be due to the command using the wrong interface to send the ping request. As an example, consider that the netsh command was issued to display the interface IDs and the correct interface to use was determined to be 15 on that computer. The ping command could be modified to include it as ping fe80::613a:325f:5e1b:d9b4%15.

### Global Unicast

A global address can be routed as a public address on the Internet through routers and networks. Global unicast IPv6 addresses are usually assigned by an ISP or public registration authority.

Note that a global unicast address can be generally identified with the address prefix 2000::/3. Even though that is the current block of IPv6 addresses being handed out to public end points, this may change in the future. Large portions of the IPv6 address space are still unused. An example of a global unicast address is: 2001:0:4137:9E76:F9:1435:304E:DFF2.

### Unique Local Unicast

The unique local unicast address type is intended for local communications within a private site. These addresses are similar in function to IPv4 internal private addresses (refer to [Table 4-2](javascript://)) in that they are not intended to be directly routable over the Internet.

The unique local address type allows an administrator to identify a site and route internally within that private site. Routers that connect to the global Internet will drop data with this address type if it is sent directly out to the Internet. Note that a unique local unicast address can be generally identified with the address prefix FC00::/7.

**Note 9**

Some references will mention a site-local unicast prefix as FEC0::/10 as an alternative to unique local unicast; however, these types of addresses were considered flawed in their design and application and therefore officially deprecated. See [https://tools.ietf.org/html/rfc3879](https://tools.ietf.org/html/rfc3879" \t "_blank) for further details.

### Multicast

An IPv6 [**multicast**](javascript://) address serves the same purpose as an IPv4 multicast address. One or more computers can be assigned a multicast address that identifies them as members of the same group of computers. When data is sent to a multicast address, all computers with an interface that belongs to that multicast group will receive a copy of the data.

The address prefix of a multicast address is FF00::/8. Managing multicast addresses is not a typical administration task for Windows 10, so these settings are not reviewed in detail here.

### Special Addresses

Two special addresses exist in IPv6: the loopback address and the unspecified address. The loopback address in IPv6 is specified as 0:0:0:0:0:0:0:1, otherwise written as ::1 or ::1/128. This is similar in function to the IPv4 loopback address 127.0.0.1. The loopback address is assigned only to a virtual interface, never to a physical one. Any data sent to the loopback address for a computer will deliver in software back to the computer that sent it. The data will not be sent out on the physical network; the entire process will happen in software using the virtual interface only.

The unspecified address is 0:0:0:0:0:0:0:0, otherwise written as :: or ::/128. The unspecified address is never assigned to a computer. It indicates the absence of an address. This can be observed when an IPv6 address is unspecified in a configuration window or when a computer is sending an IPv6 packet, but it doesn’t have a source address yet (i.e., it hasn’t learned its address yet).

### IPv6 Tunneling through IPv4

When IPv6 was still new, mechanisms like 6to4, Teredo, and Intra Site Automatic Tunneling Address Protocol (ISATAP) were included as part of Windows to carry IPv6 data over the existing IPv4 public networks. Best-practice advice is to not use these transition technologies as they are deprecated and disabled by default as Windows 10 evolves. Where possible, always use native IPv6 support instead.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-3cMethods for Configuring IPv6

A computer running Windows 10 automatically configures its network interfaces with a link-local address. These can be displayed by entering the ipconfig command at the command line, as shown in [Figure 4-9](javascript://). The link-local addresses allow the computer to interact with other computers on the local network but not through a router to other networks.

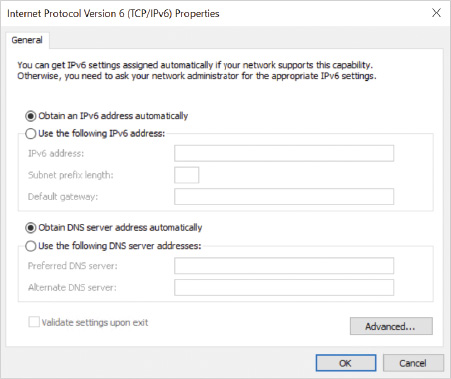
To configure IPv6, you can use:

* Static configuration
* Automatic configuration
* IPv6 Configuration Commands

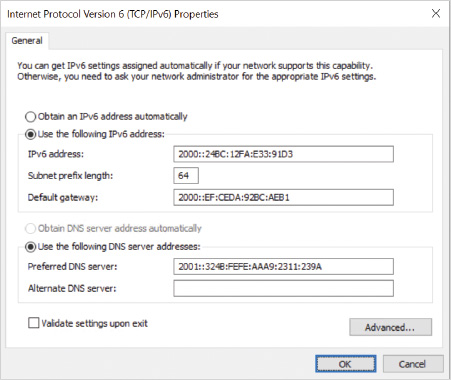
### Static Configuration

A network connection’s properties include settings for IPv6. By default, the properties are configured to obtain an IPv6 address automatically, as shown in [Figure 4-10](javascript://). It is not common to configure an IPv6 address statically. To configure a static address, a network interface’s IPv6 properties must be reconfigured to use a specific IPv6 address with a specified subnet prefix length, as shown in [Figure 4-11](javascript://).

**Figure 4-10Network and Sharing Center, Network Connection IPv6 Automatic Connection Properties**



**Figure 4-11Network and Sharing Center, Network Connection IPv6 Properties, Static IPv6 Configuration**



The Advanced button in the IPv6 Properties window allows the interface to be assigned one or more default gateways, multiple IPs, and custom DNS settings. IPv6 does not implement NetBIOS over TCP/IP, so there are no WINS configuration options.

### Automatic Configuration

Automatic configuration can be done in two ways: stateful and stateless. [**Stateful automatic address configuration**](javascript://) involves one or more devices that track the state of the client in internal data tables. Traditional IPv4 address allocation through DHCP is an example of stateful address allocation. IPv6 can also obtain an address from an IPv6 DHCP server (DHCPv6) if one is configured on the local network. Windows Server 2008 or later can support IPv6 configuration as a DHCP server, but earlier versions of Windows Server cannot. A compatible IPv6 DHCP relay can also be used with IPv6 addressing to enable a client to interact with a DHCPv6 server on a different network.

In stateful address allocation, the DHCPv6 server tracks details about the client while it is operational with a leased address assigned by that DHCP server. This can restrict the mobility of a client, as it has to coordinate its address assignment with servers and other devices while it moves from one network to another. The client and DHCP server present a DHCP Unique Identifier (DUID) to identify themselves when exchanging DHCPv6 messages. The clients DHCPv6 DUID can be seen by issuing the ipconfig /all command at a command prompt.

[**Stateless automatic address configuration**](javascript://) empowers the client to collect as many settings as possible from the network around it and have it create its own IPv6 address. The subnet address in use on a local network is advertised by an IPv6-aware router as the subnet ID. The client generates a random interface ID and combines it with the subnet ID to create its own IPv6 address. Configuration options, such as DNS server settings, are collected from DHCP servers or the router connected to the local network. If no router is connected, the interface can automatically configure only a link-local address. The advantage to stateless configuration is that less equipment and configuration effort is required to set up the IPv6 address for a network.

In small networks, even settings such as the DNS server settings may not be required. Windows 10 can resolve local client names using the [**Link-Local Multicast Name Resolution (LLMNR)**](javascript://) protocol and related supporting services. This allows a computer to query the names of other computers on the local network using IPv4 and IPv6 without relying on NetBIOS, WINS, or DNS name resolution. This can minimize the requirement to have name configuration servers defined ahead of time and configured for clients.

### IPv6 Configuration Commands

Script commands using netsh can be used to configure IPv6 settings on the computer. The netsh command is powerful and can be used to configure a variety of network settings; for example, netsh interface ipv6 add address “Ethernet4” 2001:EB8::8:801:20C4:2 will add the specified IPv6 address to the interface called Ethernet4.

PowerShell cmdlets like Set-NetIPAddress can also change the IPv6 settings for a network interface, for example, Set-IPAddress -InterfaceAlias Ethernet -IPAddress 2001:CCE:2025:61fC:B65:C216 -PrefixLength 64 will update the IPv6 address already assigned to the network interface identified with the alias Ethernet.

**Note 10**

If the network adapter does not already have an IPv6 address, then you would use the New-NetIPAddress cmdlet instead of Set-NetIPAddress.

**Note 11**

The PowerShell cmdlet Set-NetIPv6Protocol is designed to change global IPv6 parameters and not IPv6 address settings on a network interface.

Changes to a network interface’s settings may take multiple commands to completely configure the interface.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-3dTroubleshooting IPv6 Settings

Because IPv6 addressing is new and there are new details of how to configure it, many people assume that troubleshooting is different. The overall troubleshooting methodology is similar to IPv4 troubleshooting with the following notable considerations in each troubleshooting stage:

1. Confirm current settings.
2. Validate IPv6 connectivity.
3. Verify DNS name resolution.
4. Verify data connections.

### Confirm Current Settings

The existing IPv6 settings should be confirmed due to the default nature of IPv6 clients attempting to autoconfigure themselves. By default, Windows favors IPv6 global unicast addresses over IPv4 addresses, but this can be updated in the registry by an Administrator, either directly or using Group Policy.

**Caution**

Some administrators are tempted to disable IPv6 because it is new and unfamiliar; however, some Windows 10 components are designed to use only IPv6 and may not function correctly if the disabling occurs.

### Validate IPv6 Connectivity

If all settings appear correct, the ping utility can be used to confirm that the computer can ping its own loopback address by issuing the ping ::1 command or the Test-NetConnection ::1 PowerShell command. If either command is successful, the TCP/IP IPv6 protocol is functional on the computer.

The computer keeps track of which computers it communicated with recently, and some of that information can be out of date. The IPv4 system uses an ARP table to keep track of network devices to which it last connected. IPv6 uses a neighbor and destination cache to essentially do that, as well.

The neighbor and destination cache can be viewed and managed with the netsh utility or the Get-NetNeighbor/Set-NetNeighbor PowerShell cmdlets. The neighbor cache lists known computers on the same local network as the client computer. The destination cache lists the next IPv6 address the computer should send data to, to reach a particular destination.

If either the neighbor or destination cache data is in doubt, they can be cleared with the netsh utility or the Remove-NetNeighbor cmdlet. For example, the PowerShell command Remove-NetNeighbor -State Unreachable will remove all neighbor cache entries that are unreachable.

### Verify DNS Name Resolution

Different types of records are registered with the DNS server depending on the IP data the client is registering. An IPv4 address and host name are stored in the DNS server using an A record. The A record maps the name of the computer to its IP address. An IPv6 address and host name are stored in the DNS server using an AAAA record. The AAAA record maps the name of the computer to its IPv6 address.

A DNS server may be configured to map the IP address back to the name of the computer using PTR records, but this is not commonly implemented for IPv6. IPv4 addresses are stored in a DNS server data table called in-addr.arpa. IPv6 also uses a PTR record to match an IPv6 address to a name, but it uses a data table called ip6.arpa.

DNS servers may resolve a name to either an IPv4 address or an IPv6 address. There is no guarantee the DNS server will respond with IPv4 or IPv6 data in all cases. A computer may have a valid IPv4 A record stored in DNS but no IPv6 AAAA record. To restrict troubleshooting to IPv6 addresses, the ping command can be forced to only use IPv6 addresses by issuing the ping -6 TargetName command, where TargetName is the target name of the remote computer. If the DNS server cannot provide an answer that is a valid IPv6 address, the command reports that the host name could not be found.

### Verify Data Connections

Using the telnet application is a common tool for administrators to test application connectivity. The telnet utility does not guarantee it will use IPv6 to connect to a remote service unless the target address is specified as an IPv6 address. Carefully consider that specifying a target DNS host name to connect to does not guarantee that an IPv6 address will be used instead of an IPv4 address. This is true for any application you use to test data connections over the network.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**4-4**Internet Connectivity

Today, almost every computer is configured to communicate on the Internet; however, depending on your needs, how your computer connects to the Internet will vary. The way you connect to the Internet will also vary depending on whether a single computer or multiple computers are using an Internet connection.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-4aSingle-Computer Internet Connectivity

Many homes have one or more computers sharing the Internet. How a computer is configured to connect to the Internet depends on the type of Internet connection you have.

For some Internet connection types, the IP address provided to you is usually a fully routable IP address on the Internet. This means that anyone on the Internet can connect to and communicate with your computer. In those cases, it is important to enable Windows Defender Firewall to protect your computer.

**Note 12**

Detailed information about Windows Defender Firewall is provided later in this module.

### Cable

Almost all cable companies offer high-speed Internet connectivity as an option to their subscribers. In most cases, this is the simplest way to connect to the Internet.

When you subscribe to an Internet connection with your cable provider, you will be supplied with a cable modem that connects to the same cable that you hook up to your TV. The cable modem is responsible for converting signals from a format that travels properly over the cable provider network to standard Ethernet in your home using either a wired or wireless connection to your computer.

By default, Windows 10 networking is configured to use DHCP to obtain IP configuration information. When you connect your computer to the cable modem, the cable provider’s DHCP server provides IP configuration information to Windows 10. Moments after you plug in an Ethernet cable to the cable modem or connect to its WiFi access point, you should be able to access the Internet.

### DSL

Digital subscriber line (DSL) is a high-speed Internet connection over telephone lines. This type of Internet connectivity is often as fast as cable but can be slightly more difficult to configure.

When you subscribe to DSL, you are supplied with a DSL modem that connects to a phone line. The DSL modem is responsible for converting signals from a format that travels properly over the phone system to standard Ethernet in your home. The DSL modem is commonly combined with a router/firewall appliance in one physical box. You connect an Ethernet cable from your computer to the DSL modem or connect to its WiFi access point to connect to the Internet.

DSL connections usually use [**Point-to-Point Protocol over Ethernet (PPPoE)**](javascript://) to secure connections. Your DSL provider supplies you with a PPPoE user name and password to connect to the network. In a home situation, the installer can program this information into the DSL modem for you. Only after you are authenticated by using PPPoE will you be able to obtain IP configuration information from the DSL provider and connect to the Internet.

If the DSL provider has supplied only a DSL modem, and it does not have a router/firewall supplied with it, Windows 10 has built-in support to connect directly via PPPoE. You can connect to a network requiring PPPoE by creating a broadband connection from the Network and Sharing Center. The options in a broadband connection are similar to a dial-up connection.

### Dial-Up

Although progressively becoming much less common, some people still access the Internet using a dial-up connection over a phone line by using a modem. Although this is a much slower way to access the Internet, it is suitable when are no other options are available. Windows 10 includes support for dial-up connections.

### Cellular

Wireless wide area networks (WWANs) are fully supported by Windows 10 using cellular data network devices that connect through broadband cell towers and Wi-Fi hotspots for Internet data transfer. Those cellular data network devices can be built into the Windows 10 device, plugged in as an add-on device via USB, or a wired/wireless attached device, such as a smartphone. These devices have a Subscriber Identity Module commonly referred to as a [**SIM**](javascript://) card or **[eSIM](javascript://)** in them to identify the user to the cellular data network, enabling connectivity to the Internet.

Several requirements must be met in order for this option to work. The provider of the broadband service must enable this option for the portable device, typically for an extra fee. Most broadband vendors refer to this feature as “tethering” the computer to the mobile device. The mobile device must also be configured to recognize that this feature is active. The advantage of this technology is that broadband support for mobile devices is now widespread. The disadvantage is that the data plan contract to pay for the bandwidth used by the mobile device while it operates in this mode can be expensive. Windows 10 works with this type of connection fully aware that it is a WWAN service. Windows 10 includes options to control potentially expensive cellular usage, such as data roaming, using cellular instead of Wi-Fi for data, controlling which apps can use your cellular data, setting and managing a SIM PIN, and setting a data limit (i.e., metering).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-4bShared Internet Connectivity

It is possible for multiple computers to share a single Internet connection. This is not commonly done for dial-up connections, but is quite common for cable modem and DSL Internet connections. For multiple computers on your network to share a single Internet connection, a mechanism must be in place to share the single IP address given to you by your ISP. The two most common mechanisms for sharing an IP address are a router or [**Internet Connection Sharing (ICS)**](javascript://).

### Router Connection Sharing

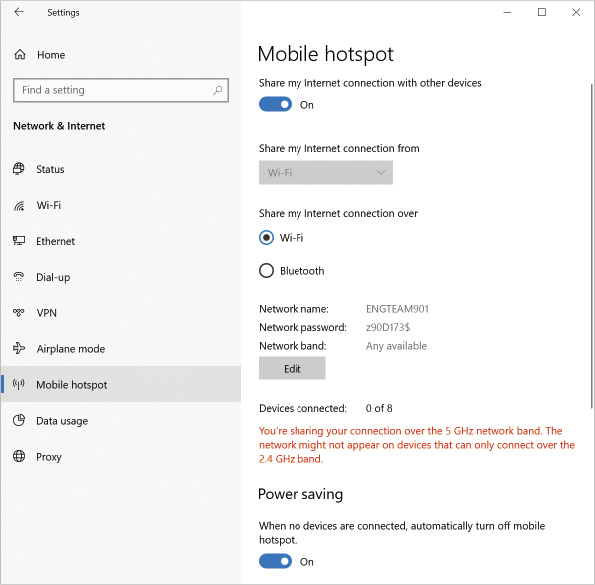
Multiple computers can share an Internet connection with a dedicated router appliance. The router is assigned an IP address from the ISP to connect to the public Internet. Computers on the router’s internal network are assigned private IP addresses that are not routable on the Internet. The computers on the internal network use the router as their default gateway, sending Internet-bound traffic to the router for delivery.

The hardware routers sold in retail stores, cable modems, and DSL modems are also simple firewalls that perform Network Address Translation (NAT). NAT is the process that allows multiple computers to effectively share the single IP address assigned by the ISP.

### Mobile Hotspot

If a Windows 10 computer has a wireless network adapter or Bluetooth adapter, it can be configured to act as a local hotspot that shares the computer’s Internet connection with other computers or devices over either one of those interfaces. The Mobile hotspot settings are found in the Network and Internet Settings, which include the settings shown in [Figure 4-12](javascript://).

**Figure 4-12Mobile Hotspot Settings**



Enlarge Image

Your mobile hotspot is shared using a selected local Wi-Fi or Bluetooth network interface and is given a name you can edit to identify it to others. The feature is protected with a simple password you manage as part of the mobile hotspot settings.

**Note 13**

Customize your mobile hotspot settings before turning on the Share my Internet connection with other devices option.

This feature is not designed to support large groups of users; rather, it’s designed to share with a few devices only (maximum of 8) as a convenience. To use it, the nearby computers or devices can open their Wi-Fi settings, find your network name, select it and enter the password that you share with them to connect.

### Internet Connection Sharing

Internet Connection Sharing (ICS) is an older technology that allows a Windows 10 computer with multiple network interfaces to act as an Internet router for other local computers. The ICS computer is called the host computer. To use ICS, the host computer must have an Internet connection (public interface) plus one additional network connection (private interface). The public interface obtains an IP address from your ISP or router. The private interface uses a private IP address to communicate with other computers with which you are sharing the Internet connection.

Using ICS to share an Ethernet based connection was popular when it was first introduced with Windows 98, but that is not a common use for it today. ICS is managed by the Internet Connection Sharing service, which requires you to set the service’s startup type to Automatic as well as configure the ICS settings manually.

**Caution**

It is not recommended that you use ICS manually, as the service is set by default to shut down after four minutes if no traffic passes through it and not restart automatically. Use a router or modern mobile hotspot technology instead of ICS.

Some Windows network features, such as wireless hosted networks (discussed later in this module), depend on using ICS in a custom fashion, but they will manage the service independently.

### Wireless Ad Hoc

Many standards are written by organizations such as the [**Institute of Electrical and Electronics Engineers (IEEE)**](javascript://) to guide the manufacturers of wireless network products and help make them functional and compatible with one another. The IEEE standard most commonly used for popular wireless networking products is IEEE [**802.11**](javascript://). The 802.11 is a collection of continuously evolving standards, so you will notice that different 802.11 specifications will add descriptive labels or letters to identify specific sections of the overall standard.

[**Wireless Ad Hoc**](javascript://) is based on the IEEE 802.11 ad hoc network standard to share wireless and was introduced with Windows Vista.

The use of wireless ad hoc networking is deprecated, and since the introduction of Windows 8.1, Microsoft’s recommendation has been to use Wi-Fi Direct (covered later in this module) or some other current wireless sharing technology instead.

**Note 14**

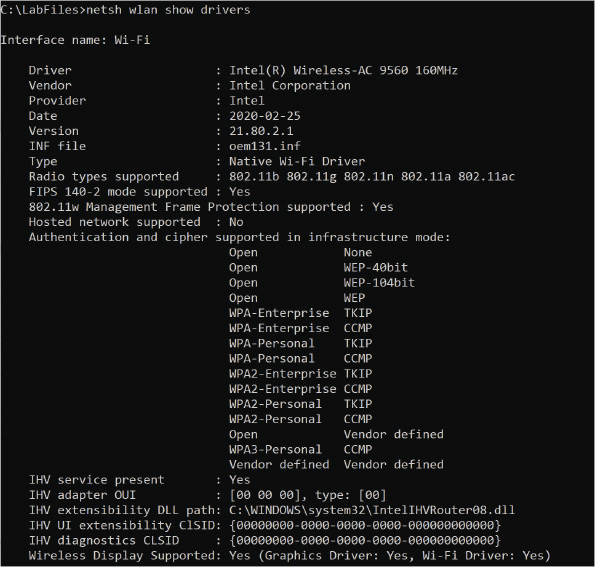
Wi-Fi Direct and the IEEE 802.11 Wi-Fi ad hoc network standard are not the same thing. Wi-Fi Direct has features, such as improved security and support for WPA2 encryption, where traditional Windows versions of Wi-Fi ad hoc networking support only weak WEP encryption.

### Wireless Hosted Network

[**Wireless Hosted network**](javascript://) was introduced with Windows 7 as another option to turn your Windows PC into a wireless hotspot you can share with others. The feature relies on legacy components, such as Internet Connection Sharing (ICS), to enable [**personal area network (PAN)**](javascript://) and Internet sharing scenarios. When it is enabled, one or more virtual wireless network adapters are created automatically to represent and manage a software access point for other wireless clients to connect to.

The physical wireless network adapter in the computer must have a driver that supports being used as a wireless hosted interface. Support for this feature has faded from some manufacturers as newer wireless hotspot technologies have become popular. If a Windows 10 computer was upgraded from an older operating system, say Windows 7, it is likely that the wireless network driver was retained after the upgrade and still supports this feature. If you decided to do a clean install of Windows 10 onto the same hardware, the newly installed wireless network driver may have dropped support. To determine if the current wireless network interface driver supports hosted networking, open a command prompt and run the netsh wlan show drivers command and look for the Hosted network supported value, as shown in [Figure 4-13](javascript://).

**Figure 4-13Netsh Output to Determine Wireless Adapter Driver’s Capabilities**



Enlarge Image

If the driver does not support hosted networks, you could try installing an older version of the wireless network card driver; however, you would be rolling back to an older driver that could limit the use of newer Windows 10 networking features and introduce instability.

If the driver does support hosted networks, you could configure the virtual access point by opening an administrative command prompt and run netsh to define basic settings like the advertised SSID and a passphrase, for example, netsh wlan set hostednetwork mode=allow ssid=myLocalPan key=9849897bw. You would continue to manage this virtual access point using netsh commands; for example, you could start that access point with the netsh wlan start hosted network command and stop it with netsh wlan stop hosted network.

### Wi-Fi Direct

[**Wi-Fi Direct**](javascript://) is a peer-to-peer wireless connection technology that allows devices certified for use with Wi-Fi Direct to securely discover, connect, and transfer information among one another. Wi-Fi Direct is a specification developed by the Wi-Fi Alliance. Wi-Fi Direct devices do not need to connect to a traditional Wi-Fi access point first or use existing Wi-Fi ad hoc mechanisms. Similar to other wireless sharing solutions, this feature will create Microsoft Wi-Fi Direct Virtual Adapters to support shared access.

**Tip**

A command like ipconfig /all will show the presence of the Microsoft Wi-Fi Direct Virtual Adapters in the command’s output, but you will not see the adapter in Device Manger. You can optionally turn on the display of hidden devices in Device Manager from its View menu, showing the hidden adapters in the Network adapters section. If you disable the virtual adapter for troubleshooting, note that it will most likely disable Wi-Fi Direct support as well.

Wi-Fi Direct is similar to Bluetooth technology and its capability to connect dynamically; however, the technology is faster than Bluetooth (up to 250 MBps) and has a greater range (currently up to 200 meters). Some common devices that can be certified for Wi-Fi Direct include wireless display adapters, Miracast display adapters, digital audio players, printers, televisions, projectors, cameras, phones, routers, computers, and tablets to name a few categories.

A computer that has a traditional Wi-Fi connection to a Wi-Fi network or hotspot can use that connection for traditional Internet access, what the Wi-Fi Direct program would call an infrastructure connection. Wi-Fi Direct allows that infrastructure connection to be shared with the Wi-Fi Direct connections, because the security of the Wi-Fi Direct peer-to-peer group is managed separately from the infrastructure network. Currently, most Wi-Fi Direct solutions use a custom vendor app or a third-party app you can purchase from the Windows Store to configure and use Wi-Fi Direct devices with Windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 4-5Wireless Networking

Network connections allow data to flow from the local computer to other computers that share that network. Many networking technologies rely on a wire-based physical data connection to the local computer. Different types of cables, connectors, and expansion equipment make up the wired network. Instead of relying on wires to connect computers, a wireless network transfers data without a physical connection. The most common type of wireless technology uses radios to transmit and receive data. Many different types of radios have been developed for wireless technology.

The [**Wireless Fidelity (Wi-Fi) Alliance**](javascript://) was created in 1999 as a nonprofit body to help manufacturers test and certify wireless products that would work together. These wireless standards are summarized in [Table 4-10](javascript://). IEEE 802.11n performance is fast and currently preferred because it is more tolerant of interference and supports a wide range of devices. Many portable devices, such as smartphones and newer laptops, include support for IEEE 802.11ac, which is becoming a popular alternative to 802.11n.

**Table 4-10**

### IEEE 802.11 Wireless Standard Comparison

| **Wireless Standard** | **Primary Radio Frequency** | **Maximum Data Throughput (MBps)** |
| --- | --- | --- |
| IEEE 802.11a | 5 GHz | 54 |
| IEEE 802.11b | 2.4 GHz | 11 |
| IEEE 802.11g | 2.4 GHz | 54 |
| IEEE 802.11n | 2.4 and 5 GHz | 600 |
| IEEE 802.11ac | 5 GHz | 3466 |
| IEEE 802.11ad | 60 GHz | 6757 |
| IEEE 802.11ax | 2.4, 5, 6 GHz | 9608 |

Enlarge Table

Windows 10 provides a strong foundation for wireless technology, leaving the manufacturer with less responsibility for code development and a smaller chance of creating unstable software. Wireless adapters now appear as their own media type, not as an Ethernet 802.3 connection.

Even though Windows 10 supports a range of IEEE 802.11 standards, several are becoming obsolete. For example, it is rare to find 802.11a and 802.11b hardware in use. Each standard defines limits on how many devices can interact at once, resistance to radio interference, how fast they transfer data, and over what range they can operate. Exceeding any of those limits can cause performance issues that Windows 10 cannot compensate for with software alone. For example, the 802.11ad standard can operate at a very high data rate but only for a short distance, typically within the same room (11 feet). Some newer standards, such as 802.11ax are not supported in older versions of Windows 10, being first introduced as supported in Windows 10 version 2004.

A computer running Windows 10 may have a wireless adapter installed in the computer. It may be installed as an add-on card, plugged into a USB port, or built into the system itself. If the wireless adapter is built in, such as in a laptop, there is often a power switch that toggles the adapter on or off to save power or ensure privacy.

The wireless adapter can communicate with a base station or other wireless adapters. A base station is commonly called a [**wireless access point (WAP)**](javascript://). The WAP itself connects to the wired network and allows wireless clients to ultimately use that wired connection. The WAP may be part of a firewall device sharing access to the Internet, or it may be a stand-alone unit. The WAP and wireless adapter in the Windows 10 computer must use the same 802.11 standard to communicate with each other. If they are not compatible, one or the other hardware component may need to be replaced. When a WAP is purchased, consider that many will support a combination of IEEE 802.11 standards, which can give them a price or feature set competitive advantage over other WAPs.

Most WAP devices have a web server built into them that allows the device to be configured initially using a wired network connection. The manufacturer’s instructions provide connection details and initial sign-in credentials. The manufacturer identifies a default management IP address, an initial connection URL (for example, http://192.168.0.1/admin), and a default administrator ID and password.

The most common configuration details for a WAP include:

* Security Set Identifier (SSID)—The [**Security Set Identifier (SSID)**](javascript://) is the name assigned to the WAP to identify itself to clients. The SSID may or may not be configured to broadcast its identity to all wireless clients. If the SSID is not broadcast, the wireless client can still connect if it knows the name ahead of time and has the right connection settings preconfigured.
* 802.11 mode—This includes the versions of 802.11 in which the radio operates, such as 802.11n. Choices will be limited to the modes supported by the WAP hardware.
* Security method—This includes the methods used to encrypt and restrict wireless client connections to the WAP.

Wireless encryption methods and client connection restrictions are required because the range of a wireless signal does not have a specific boundary. A private system may be detected by clients in unauthorized and unexpected areas. Newer technology has a greater range than ever before. Simply upgrading existing wireless hardware may expose companies to risks they did not think about before. A wireless client must be configured with correct security settings to enable it to communicate with a secured WAP. If the WAP is unsecured, it is referred to as an open or unsecured system.

Connecting to an open system may be dangerous because your computer may be connecting to an untrusted WAP that has been configured purposely to help unauthorized users gain access to your system or monitor the traffic you move through the WAP. If no choice is available, ensure that the connection is identified as a Public network connection to maximize the protection of Windows Defender Firewall and to disable your computer’s advertising of its identity.

Go to pg.

[**help**](javascript://)

Application Opened

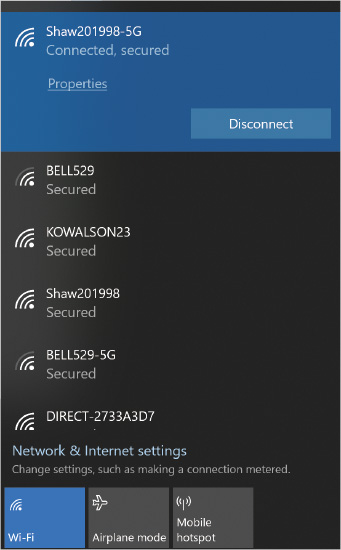
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-5aCreating a Wireless Connection

Wireless network connections can be created using several methods:

* Manually connect to a wireless network—This wizard is available by clicking Set up a new connection or network in Network and Sharing Center from Control Panel and selecting the Manually Connect to a Wireless Network option. All settings are manually configured.
* Connect to a network—By clicking the network icon in the notification area of the taskbar, a list of wireless networks is displayed, as shown in [Figure 4-14](javascript://). The list of visible networks shows the signal strength of each connection, if it is secure or open (no security), and if Windows 10 is connected to one of them. Selecting a network from the list and clicking the Connect button triggers the client to attempt a connection. If a security passphrase is requested, the user must enter a correct value before the connection is fully established.

**Figure 4-14Wireless Networks Displayed from Taskbar Notification Area**



Enlarge Image

* Use a command-line utility—The netsh command-line utility supports a command section for wireless LAN configuration, wlan. This advanced utility is not typically used in day-to-day network administration, but it is available for advanced management. More options can be seen by issuing the netsh wlan /? command.
* Configure in Group Policy—Wireless network settings can be applied to domain computers using Group Policy settings defined in Active Directory. A list of allowed or denied wireless networks can be specified.
* Provision via a website—Windows 10 version 2004 introduced the capability to configure a website so that a user can browse the website and provision a Wi-Fi profile for a **[Passpoint](javascript://)** or normal network. Passpoint is a [**Hotspot 2.0**](javascript://) technology term, covered later in this module.
* Use Wi-Fi Sense—Wireless network settings could be shared among contacts using [Outlook.com](http://outlook.com/" \t "_blank), Skype, and Facebook contacts who decide to share certain Wi-Fi connections with their contacts; however, this feature has been disabled by Microsoft due to its complexity and low demand for this feature.

Windows 10 keeps a list of SSIDs sorted by preference based on what you connected to in the past. The last used SSID is the preferred connection to connect to by default. If you are connected to one SSID in the list but you want to select a different one, simply select the other one from the list and connect to it. Windows 10 will remember that choice for next time.

### Wireless Connection Properties

When a new wireless connection is created, the key settings stored to describe it in Windows 10 are:

* Network name—The name of the wireless connection and its profile in the operating system
* Security type—The type of security methods the WAP expects the wireless client to use
* Encryption type—The method used to encrypt data, if a choice exists, as a customization of the selected security type
* Security key—A passphrase that acts as a password, allowing the wireless client to authenticate and connect
* Connect automatically when this connection is in range—The setting that identifies this SSID as preferred; tries to connect automatically once the client detects the WAP is operating in range
* Look for other wireless networks while connected to this network—A setting that allows the client to attempt to connect to a preferred wireless connection if it becomes available while connected to this SSID
* Connect even if the network is not broadcasting its name (SSID)—A setting that allows the client to attempt to connect even if it does not notice the WAP broadcasting its SSID wirelessly

Note that the last three connection settings enable a preference to be set for connecting to WAPs. A preferred connection can be set to automatically connect. A secondary connection can be used, but the client can change to a preferred WAP if it becomes available. If none of those is available, Windows can search for a specifically named WAP that is not broadcasting its name to clients. A WAP that is not configured to broadcast its name is sometimes seen as a security measure; however, applications are available that can spot the SSID from other types of packets the WAP generates, making the name known to others if they really want to look for it.

### Wireless Network Security

A wireless network connection has settings for both security type and encryption type. The security type defines how authentication is performed. The encryption type defines the algorithm that is used to encrypt data while in transit over the wireless network. In general, these settings are automatically detected when you connect to a wireless network for the first time.

The following security types are available:

* No authentication (open)—This service type is used by public Wi-Fi networks where you are not required to provide credentials.
* WPA3-Personal—[**WPA3-Personal**](javascript://) support was added with Windows 10 version 1903. Like WPA2, it also uses a pre-shared key exchange with improved 128-bit encryption and a new handshake protocol to make it harder to attack.

**Caution**

WPA3 security issues collectively called Dragonblood were discovered and allowed attackers to crack Wi-Fi network passwords and access encrypted network traffic exchanged among connected devices. Windows 10 version 2004 includes fixes to address those issues. As always, consider keeping device firmware and drivers up to date to ensure that the latest security patches are applied to all components of the wireless network.

* WPA2-Personal—[**WPA2-Personal**](javascript://) uses a pre-shared key (password) for authentication and is suitable only for small environments.
* WPA2-Enterprise—[**WPA2-Enterprise**](javascript://) uses 802.1x for authentication and is suitable for larger environments.
* 802.1x—This option defines port-based network access control that uses the physical characteristics of the LAN infrastructure to authenticate devices attached to a LAN port.

The [**802.1x**](javascript://) protocol is a standard for network devices, such as a Windows 10 computer, to be authenticated by switches or WAPs. Windows 10 provides authentication credentials to the WAP and then the WAP queries a [**RADIUS server**](javascript://) to verify the credentials. In a Windows-based environment, the RADIUS server can verify authentication for Active Directory user accounts or computer accounts.

The three encryption types available are as follows:

* None—Data is transmitted as cleartext. This option is available only for open networks.
* Wired Equivalent Privacy (WEP)—This older encryption protocol has known flaws and should be avoided whenever possible. This option is available only for open networks and 802.1x.
* Advanced Encryption Standard (AES)—This is the preferred encryption type and is used by WPA2-Personal and WPA2-Enterprise.

Go to pg.

[**help**](javascript://)

Application Opened

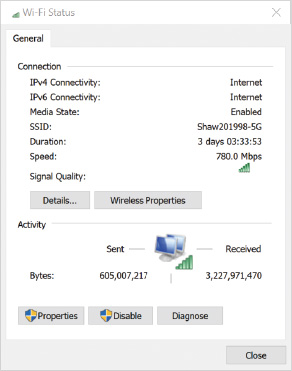
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-5bManaging Wireless Connections

Managing a wireless network connection is similar to managing a wired network connection. Typically, very few tasks are required to manage a wireless network after it is configured, except for troubleshooting when connectivity issues occur.

If connectivity issues occur, you can view the status of the wireless network, as shown in [Figure 4-15](javascript://). This shows which wireless network you are connected to and the signal strength. In the unlikely event you need to change the settings for the wireless network, you can do it manually in the wireless properties; however, it is typically faster and easier to forget the existing network and reconnect to autodetect the settings again.

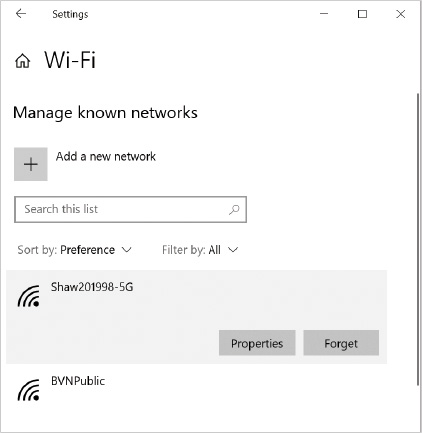
**Figure 4-15Network and Sharing Center, Wireless Connection Status**



### Forget Wireless Networks

Windows 10 keeps a record of all wireless networks that it has connected to, including the settings that were used. To delete older wireless networks that are no longer in use or you want to reset, you can choose to forget them from Network and Internet settings, Wi-Fi, Manage known networks, as shown in [Figure 4-16](javascript://).

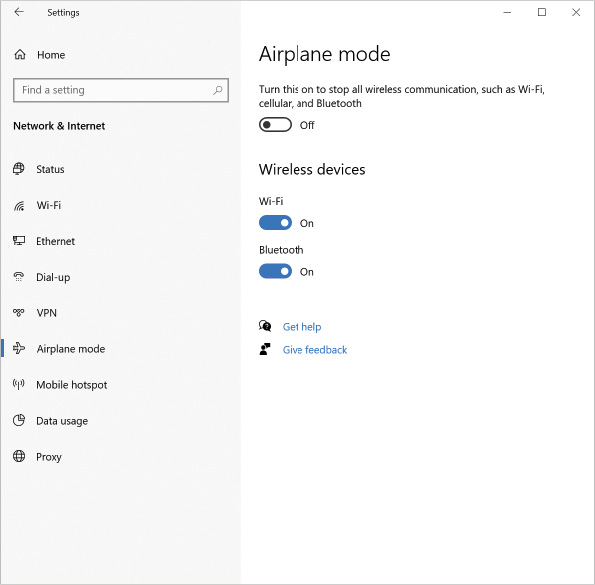
**Figure 4-16Manage Known Wi-Fi Networks**



### Airplane Mode

From a user perspective, temporarily disabling Wi-Fi can be useful for air travel. If you activate Airplane mode, it disables Wi-Fi and Bluetooth connectivity. You can enable Airplane mode in the Network and Internet Settings, as shown in [Figure 4-17](javascript://), or from the network icon on the taskbar, as shown previously in [Figure 4-14](javascript://).

**Figure 4-17Airplane Mode Settings**



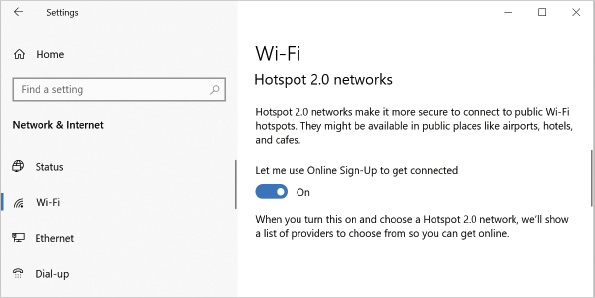
Enlarge Image

### Hotspot 2.0 Networks

Cellular networks have the convenience of working wherever a cell phone has reception from a compatible carrier’s tower and antennas. As you physically move away from one cell tower and approach another, your connection is handed off from one tower to the next, and you would likely not notice the temporary change in your voice call or browsing the network for data. Unlike typical Wi-Fi, you did not need to browse a list of local cell towers, pick one to login, and then enter credentials. Hotspot 2.0 is a technology that tries to provide a similar experience using public Wi-Fi provided by major carriers (i.e., the same companies most likely supplying your cell phone connection).

Hotspot 2.0 is a standard managed by the Wi-Fi Alliance and is based in large part on the IEEE 802.11u standard. Security on conversations between Windows 10 and the access point providing access to the hotspot network is based on end-to-end WPA2-Enterprise and WPA3 enhanced encryption. After the user signs up for a provider’s Hotspot 2.0 service and makes the first connection to a Hotspot 2.0 access point, the credentials and login process is remembered and automated for that service provider. For the user to connect to a hotspot network, [**Online Sign-Up**](javascript://) must be enabled in the Network and Internet settings, Wi-Fi settings, as shown in [Figure 4-18](javascript://).

**Figure 4-18Hotspot 2.0 Settings**



Enlarge Image

After the user activates the feature, this can potentially provide that cell-like experience but with Wi-Fi instead. For example, as the user moves from a hotel, to a café, and to an airport, his or her computer might find a compatible hotspot network at each location and seamlessly connect at each site to provide Internet connectivity. The user would not have to check which access point to use and configure a login at each location. Note that this would work only with access points that are set up to support that user’s carrier or service provider. The technology is designed to be secure and trusted so not just any access point could advertise and fake the secure connection.

Hotspot networks are supported by other computers and devices as well. If a device supports Hotspot 2.0, it will have a Passpoint certification to identify it as a compatible device.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-5cTroubleshooting Wireless Connections

Wireless technology is flexible, but several issues commonly arise. The first thing to check is whether the wireless radio on the device running Window 10 is turned on. This can be controlled by a switch, key, or just plugging in an antenna.

A common problem for travelers is that they forgot that they turned on airplane mode, which disables the Wi-Fi and Bluetooth radios on the computer. It’s also possible that the computer has a keyboard key combination that turns airplane mode on or off and somebody just pressed it by accident.

Before advanced wireless settings or configurations are changed, you should consider that the [**ISP**](javascript://) hardware or any hardware between that and the WAP could be malfunctioning to block access to Internet data. It is common to start with power cycling these devices (i.e., turning off a device, wait at least 30 seconds, then turn it back on again), working your way from the ISP modem, ISP router, firewall, network switch, to the wireless access point. If you are not sure about the impact to the network environment, for example in a client’s office, this needs to be planned out carefully. Some ISP support technicians may ask you to reset their equipment to factory default settings as part of troubleshooting Wi-Fi built into their equipment. If the configuration has been customized for an installation, be prepared to back up and reapply custom settings after a factory reset. A simple ping test between your computer and the default gateway could show if network traffic is getting at least that far.

Wireless technologies are typically radios restricted to specific radio frequencies as referenced in [Table 4-10](javascript://). Each of the 802.11 standards is designed to operate on one or perhaps more frequencies. Other devices, such as microwaves and cordless telephones, power lines, and nearby signal towers can interfere with the radio signal. If the interference cannot be eliminated, the signal between the computer and WAP might need to be improved with better antennas or better antenna placement. If that does not help enough, the WAP and wireless network adapter might have to be reconfigured to use a different frequency or IEEE 802.11 standard.

Some 802.11 standards are limited to what channels, in addition to specific frequencies, they can use to communicate. For example, the 802.11b standard works with 2.4 GHz radio frequencies. Each channel represents a small change of frequency from the original 2.4 GHz. Each channel is numbered, starting at 1, up to a maximum number of channels for that standard. Each country has rules about how many channels a standard can use on radios sold in that country. For example, IEEE 802.11b based radios can have up to 11 channels in North America and 14 in Japan.

Channels are designed to overlap in frequency ranges, so you may experience interference when someone else is also on your channel or close to it. For example, your computer may be on channel 1 and someone next door is on channel 2. The channel frequency ranges are very close together and the radio signal can experience overlap. Perhaps the person next door has a more powerful antenna and it is causing your radio to retry communications with your WAP. You have a working Wi-Fi connection, but it appears slow and maybe it even drops the connection occasionally. If the previous suggestions of upgrading antennas, or moving antennas did not help, you could change the Wi-Fi adapter to another channel in the advanced wireless adapter settings, picking a channel further away and eliminating the conflict. Channel selection may be limited by the number of active clients and sources of interference nearby. In a crowded environment like an office or apartment building, finding a free channel without heavy interference may be difficult. Making changes to the channel used might also require updates to the WAP configuration, as well.

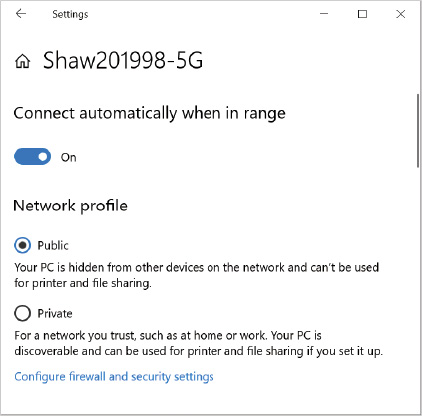
Note that channel interference is a dynamic problem. The nature of the interference can change over time. For example, someone moves into the office next door and installs a new Wi-Fi system that interferes with yours. How can you determine if channel competition and interference is a problem? There is no native utility in Windows 10 to analyze overall Wi-Fi channel use. Another option is trial and error, testing the use of a different channel and seeing if the situation improves, but that is not efficient. Best-practice advice to explore channel use is to use the Microsoft Store app to search for third-party Wi-Fi analyzers. Several are free and support basic features, but paid editions can be more elaborate and functional.

Purchasing new hardware might be a requirement in some situations where the existing hardware and its supported 802.11 settings fail to operate effectively. Options are limited by the manufacturer’s support for both the WAP and wireless network adapter, so you may have to replace both. If the device has built-in Wi-Fi, like a notebook, you may have to buy an updated notebook or add a new USB wireless network adapter.

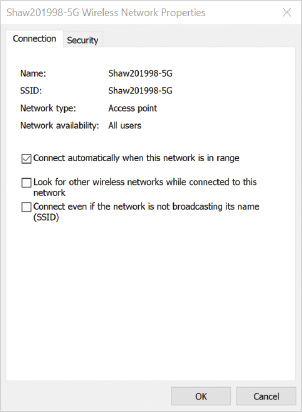
A Wi-Fi problem can also be caused by a misconfiguration of the WAP. For example, the SSID assigned to a WAP identifies that device, but there is no automatic method to force two WAP devices in the same area to have different SSID values assigned. If they have the same SSID, the wireless client may become confused about which one to connect to and unreliable connectivity will result. This is common when WAP devices are installed with factory settings in areas where multiple offices or homes are clustered together. A WAP’s SSID and administrator credentials (i.e., user ID and password) should always be changed when it is installed for the first time.

A Windows 10 client can be configured to connect to a WAP automatically when it is in range. This can be configured in Network and Internet Settings, Status, Change connection properties link, as shown in [Figure 4-19](javascript://). It can also be updated in the Network and Internet Control Panel app, wireless adapter’s wireless properties as shown in [Figure 4-20](javascript://).

**Figure 4-19Network and Internet Settings, Wi-Fi connection details**



**Figure 4-20Network and Sharing Center, Wireless Adapter Network Properties**



Note the advanced option in [Figure 4-20](javascript://) to look for other wireless networks while connected to this network. If the computer is configured for multiple WAPs and they are all active and in range, it may disconnect from one WAP and reconnect to another as the signal strength varies. This can cause the client to appear slow and unresponsive as the connection toggles. The wireless client can be moved closer to one of the WAPs to change the signal strength—the closer it is, the stronger the signal will appear. Another strategy is to set one wireless SSID as preferred and all others enabled with the option to connect to a more preferred network if it is available.

WAP devices in public places may be untrusted, even if they have a passphrase configured. If a computer is being connected to an untrusted network, always consider setting the network location type as Public and confirming that Windows Defender Firewall is up to date and configured without unsafe exceptions. Not all open WAPs are considered dangerous; some are designed to be open to allow devices to connect and access a paid secure wireless connection.

If the problem doesn’t seem to be the external wireless environment, the user can trigger the network troubleshooter by right-clicking the network icon in the taskbar and selecting Troubleshoot problems on the shortcut menu. This wizard is designed to work with users who are not as technically inclined; however, it should not be dismissed as a superficial troubleshooting tool. Microsoft has compiled a great deal of intelligence into the network troubleshooter, and it can correct many conditions with little effort from the user.

Windows 10 includes advanced troubleshooting tools for wireless connections that are used by network administrators and normally not by the average user. A history of wireless activity is collected by Windows 10 and can be used to generate a report called the Wireless LAN Report, or WlanReport for short. This is an .html and .xml file created by opening an elevated administrative command prompt and issuing the netsh wlan show wlanreport command. The report will be generated and include the date that the report was run in the file name. The location of the report will be reported by the command, but it is typically stored in the hidden folder C:\ProgramData\Microsoft\Windows\WlanReport.

The WlanReport.html file can be viewed in a browser and contains an interactive summary graph, general system information, user information, network adapter inventory details, output of an ipconfig /all command, ; and details of the wireless devices, drivers, and wireless profiles.

Some Windows 10 computers that have been updated from an earlier operating system might have an old device driver installed for the wireless network adapter that is not fully compatible with Windows 10. In that case, consider updating the device drivers for the wireless network driver using Device Manager.

If you are struggling to find a stable version of the device driver, look for a new device driver and advice from the wireless card manufacturer’s website. Ensure you are downloading the correct driver based on the manufacturer, make, and model number of the wireless adapter and its compatibility with the installed Windows version. Some embedded wireless adapters might even require a firmware update for the computer as well.

Even if a wireless network card driver is correct, the problem with connectivity can be caused by malicious software (malware), poorly written software, or people making low-level changes to network settings in the registry and making a mistake. This is not that common, but the attempted fix is fairly straightforward. Several command-line commands can reset the basic TCP/IP configuration of the computer. These commands should be run in the sequence listed below in an elevated administrative command prompt window:

* Netsh winsock reset—Reset the Winsock catalog tracking what applications are associated with ports linked to TCP/IP interfaces.
* Netsh int ip reset—Reset the TCP/IP protocol (i.e., re-install it).
* Ipconfig /release—Discard any previously obtained DHCP IP address information.
* Ipconfig /renew—Attempt to obtain new DHCP IP address information.
* Ipconfig /flushdns—Purge any previous DNS cached responses, which map names to IP addresses or “name not found” responses.
* Shutdown /r /f /t 60—Restart the computer (i.e., /r), forcing open applications to close (i.e., /f), waiting for 60 seconds to elapse before triggering the actual restart (i.e., /t 60).

If the network settings on the network adapter and the TCP/IP protocol are not the problem, it is possible that antivirus, Windows Defender Firewall settings, or anti-malware settings may have contributed to the problem. Antivirus and anti-malware performance and configuration issues should be escalated to their vendor for support. Windows Defender Firewall settings are reviewed in the next section.

As a last resort, consider the option of triggering a full network reset. This can be triggered by running the netcfg–d command from an elevated command prompt, or you can use the network reset feature introduced with Windows 10 version 1607. Network reset can be found in the Network and Internet settings, Status, Network reset link. This cleans up and removes all network devices plus customizations from the Windows 10 computer, and then triggers a restart. The Windows 10 computer detects the installed network devices it can see and attempts to reinstall drivers to default settings. This can help if the computer has been upgraded from an older operating system and old VPN software components or devices no longer used litter the system settings, causing a general network failure. Remember that after the network reset you will need to reconfigure network connections, reinstall custom VPN software, and update network discovery settings and network location profiles. Best practice is to document old settings if they are important before you trigger a network reset.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**4-6**Windows Defender Firewall

Many businesses have a firewall appliance at the network perimeter, managed by corporate administrators and beyond the control of a user within that site. Legacy network design assumed that the computers within the corporate site were static and did not move out of the building. The problem with this way of thinking is that attention is focused on the idea that network threats and their malicious traffic are outside the company site, not inside, and you should spend most of your focus protecting the site’s main data connection to the outside. The reality is that computers today are mobile, and the corporate boundary is extended to all the places you can take that computer—a café, a hotel, the airport, your car with shared Wi-Fi, Hotspot 2.0 networks, or even your home.

As ransomware and malware proliferate, attackers can sneak into corporate networks by infecting machines and using those infected machines to steal corporate intellectual property, as well as look for unprotected paths to elevate their access to other computers and systems within the corporate network. Having an active firewall on each computer is more important than ever.

A host-based firewall, like Windows Defender Firewall in Windows 10, protects your computer by restricting what network traffic (i.e., packets) comes in or goes out. It evaluates each packet as it arrives or leaves and determines whether that packet is allowed or denied. By default, all packets are denied when they arrive from external sources, and only a few are allowed for specific purposes. For example, when you join a domain, Windows 10 automatically configures Windows Defender Firewall to allow the correct packets through for domain-based communication, but other packets are denied.

The Windows Defender Firewall can be augmented with third-party firewall software that is certified to work with Windows Defender Firewall. Some parts of, or all of, the Windows Defender Firewall functionality could be turned off because the third-party firewall will provide the equivalent or enhanced function. This is by design; however, consider that turning off Windows Defender Firewall functions without an alternate firewall provider is a risky decision.

**Caution**

Stopping the Windows Defender Firewall service (i.e,. service name MpsSvc) associated with Windows Defender Firewall is not supported by Microsoft. Disabling Windows Defender Firewall profiles is not the same as turning off that service in the services snap-in. Turning off the actual service can result in newer applications failing to install or update, Start menu malfunctions, and trusted connection failures to back-end services among other unexpected issues. The proper way to disable the firewall is to disable the Windows Defender Firewall profiles and leave the service running.

Go to pg.

[**help**](javascript://)

Application Opened

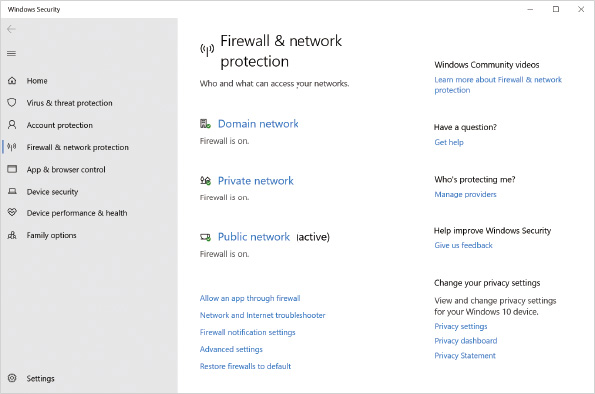
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-6aBasic Firewall Configuration

Microsoft has designed Windows Defender Firewall to be active on every Windows 10 computer right from the start and to support common programs. The user does not have to manage cryptic network traffic rules to be protected. When applications are installed, most installers are designed to update Windows Defender Firewall settings as required.

Basic controls for Windows Defender Firewall are found in the Settings app ([Figure 4-21](javascript://)). The Settings app is preferred to access these basic controls, navigated to by clicking Settings, Update and Security, Windows Security, then Firewall & network protection. The Windows Defender Firewall Control Panel app is becoming deprecated but is still used for some advanced operations.

**Figure 4-21Windows Security Settings, Firewall & Network Protection**

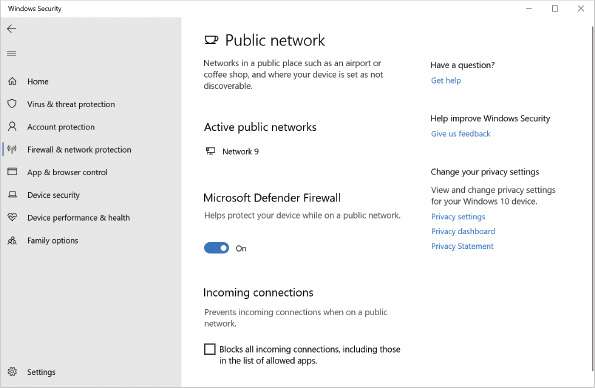


Enlarge Image

Windows 10 allows custom firewall settings for each type of network location (i.e., domain, private, or public), as was shown in [Figure 4-21](javascript://). When a network interface becomes active, it has a specified network location assigned to it. The matching firewall settings for that type of network location applies to traffic through that interface. If a Windows 10 computer has multiple network interfaces active, each can be assigned a different network location, each with different firewall settings based on that type of assigned network location.

If you select a network location profile from the Firewall & protection settings you will be shown which active network interfaces are using that type of network location, and you will have the option to turn Microsoft Defender Firewall on or off for that type of network location, as shown in [Figure 4-22](javascript://). Disabling Windows Defender Firewall should be done only for troubleshooting and not left as a permanent configuration. Many administrators regret the day they got lazy and left the firewall disabled on all local computers after a ransomware attack ran amok within a site.

**Figure 4-22Windows Security Settings, Firewall & Network Protection, Network Profile Settings**

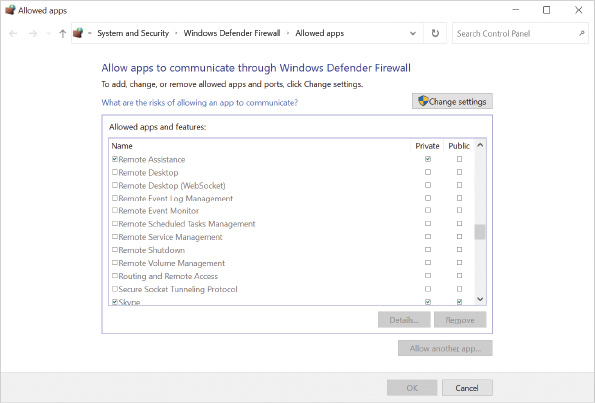


Enlarge Image

An option also is provided to block all incoming connections for that type of network location. When this option is selected, no exceptions are allowed. You are still able to initiate communication with other computers, but other computers cannot initiate communication with your computer. This is recommended only when you are connected directly to public networks, such as the wireless network in a café.

When you select Allow an app through Firewall in the Firewall & network protection settings, the Allowed apps window opens, as shown in [Figure 4-23](javascript://). This allows you to configure which programs are able to accept network communication requests. A program can be allowed access through the firewall depending on the network location type, private or public. The firewall exception can be enabled for one, both, or none of the network location categories.

**Figure 4-23Windows Defender Firewall, Allowed Apps**

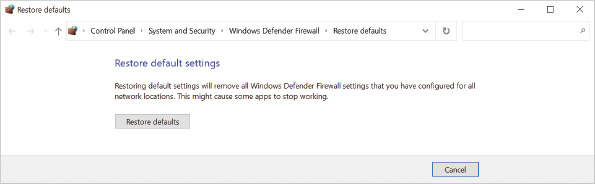


Enlarge Image

This allows some applications, such as Remote Assistance, to be available when the user is connected in supported situations. Many corporate offices do not want Remote Assistance enabled when the user is connected in unsupported locations or in locations where other support methods are available. The choice of what application to make an exception for and the type of network location to enable it for are defined by situational requirements. When you create an exception for a program, the exception applies to that program no matter what port number it uses. The exception is also valid only when the program is running. If the program is stopped, the exception poses no risk.

When Restore firewalls to default is selected from the Firewall & network protection settings (refer to [Figure 4-21](javascript://)), or Restore defaults is selected from the Windows Defender Firewall Control Panel window, the option to restore default settings for Windows Defender Firewall is presented, as shown in [Figure 4-24](javascript://). If you have performed many customized configurations and did not document them, you might want to reset Windows Defender Firewall back to the default configuration as part of the troubleshooting process.

**Figure 4-24Windows Defender Firewall, Restore Defaults**



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 4-6bAdvanced Firewall Configuration

Advanced firewall configuration allows you to configure more complex rules, outgoing filtering, and **[IPSec](javascript://)** rules. Advanced firewall configuration is useful in corporate and enterprise computing situations. The basic firewall settings are usually sufficient in home and small business situations. The tools available to perform advanced firewall configuration are:

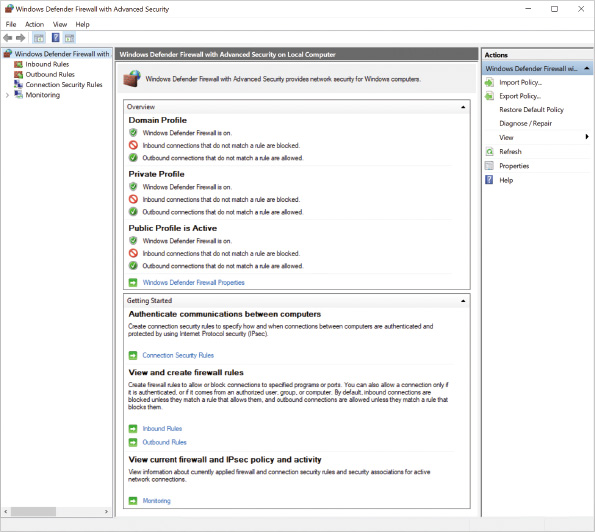
* Windows Defender Firewall with Advanced Security utility—This utility is a graphical tool to configure all of the Windows Defender Firewall features on a single computer.
* Netsh—This is a command-line utility for managing network configuration. It is also capable of configuring all of the Windows Defender Firewall features on the local computer. This tool can be used in a script that is run on multiple computers.
* Group Policy—To quickly and easily manage the Windows Defender Firewall settings in a corporate environment, you should use Group Policy. It allows firewall settings to be applied to hundreds or thousands of computers very quickly. Some Windows 10 Group Policy configuration options were not available for previous versions of Windows, and these settings are ignored by previous versions of Windows.
* Windows PowerShell—Windows PowerShell cmdlets can be used to configure advanced firewall settings. To view the list of cmdlets, use Get-Command \*firewall\* and Get-Command \*ipsec\*.
* Intune/Endpoint Configuration Manager—Settings that alter the Windows Defender Firewall are managed in the cloud by a tenant administrator and applied to a cloud-managed Windows 10 workstation. This topic is beyond the scope of this book and is not covered here.

**Tip**

If you find that Windows Defender Firewall is not enabled for all network location types, you can enable it using a script from an elevated command prompt with the netsh advfirewall set allprofiles state on command or from an elevated PowerShell prompt by running the Set-NetFirewallProfile -Name Domain,Public,Private -Enabled True command.

When Advanced settings is selected in the Firewall & network protection settings (refer to [Figure 4-21](javascript://)), or from the Windows Defender Firewall Control Panel window, the [**Windows Defender Firewall with Advanced Security utility**](javascript://) window opens, as shown in [Figure 4-25](javascript://).

**Figure 4-25Windows Defender Firewall with Advanced Security, Initial View**

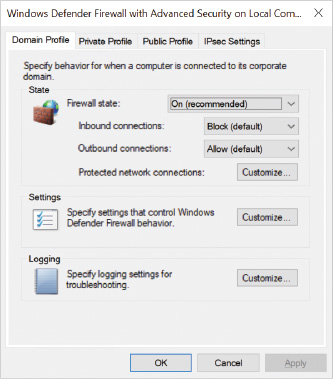


Enlarge Image

### Configuring Firewall Properties

When the Windows Defender Firewall with Advanced Security on Local Computer node is selected at the top of the left pane, a summary is displayed in the center pane showing the configuration of each network location profile. You can click Properties below Actions in the right pane or Windows Defender Firewall Properties in the center-pane to edit location profile settings and IPSec settings, as shown in [Figure 4-26](javascript://). The tabs for editing each profile have exactly the same options.

**Figure 4-26Windows Defender Firewall, Profile Settings for Network Locations**



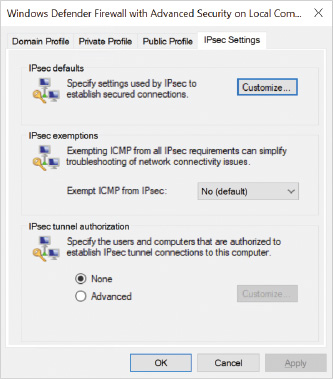
In each network location profile tab, you can:

* Enable or disable Windows Defender Firewall.
* Configure inbound connections.
  + Block (default)—All inbound connections are blocked unless specifically allowed by a rule.
  + Block all connections—All inbound connections are blocked regardless of the rules.
  + Allow—All inbound connections are allowed unless specifically blocked by a rule.
* Configure outbound connections.
  + Allow (default)—All outbound connections are allowed unless specifically blocked by a rule.
  + Block—All outbound connections are blocked unless specifically allowed by a rule.
* Customize protected network connections.
  + Select which network interfaces this firewall state applies to—All interface types (e.g., Ethernet) found on the computer are selected by default.
* Customize settings.
  + Display notifications to the user when a program is blocked from receiving inbound connections—This is useful for users to be notified when something unusual is happening on the network.
  + Allow unicast response to multicast or broadcast network traffic—Some network attackers use multicast and broadcast requests to map out the network and determine client IP addresses. Disabling this reduces that possibility.
  + Apply local firewall rules—This option allows firewall rules from Group Policy and the local computer to both be applied. If there is a conflict between Group Policy-based rules and local rules, the Group Policy-based rules are effective. You can configure this option only in Group Policy.
  + Apply local connection security rules—This option allows connection security rules from Group Policy and the local computer to both be applied. If there is a conflict between Group Policy-based rules and the local rules, the Group Policy-based rules are effective. You can configure this option only in Group Policy.
* Customize logging.
  + Name—This identifies the name and location of the Windows Defender Firewall log. By default, this is C:\Windows\system32\LogFiles\Firewall\pfirewall.log.
  + Size limit—This limits the size of the Windows Defender Firewall log to ensure you do not run out of disk space.
  + Log dropped packets—This specifies whether blocked packets are logged. By default, this option is turned off and blocked packets are not logged.
  + Log successful connections—This specifies whether successful connections are logged. By default, this option is turned off and successful connections are not logged.

### Configuring IPSec Settings

By using the Windows Defender Firewall with Advanced Security utility, you can configure IPSec settings, as shown in [Figure 4-27](javascript://). IPSec allows you to create connection security rules as a logical barrier between devices even if they are on the same local area network. Think of non-IPSec firewall rules as controlling traffic based on properties of the network traffic itself, for example, port numbers, which side started the conversation (e.g., inbound/outbound), and what network interface is involved, maybe even the application involved in the conversation. IPSec-based security connection rules are separate from the general traffic firewall rules, as they limit communication based on the identity of each computer involved in a conversation, each computer’s capability to prove that identity, as well as encrypt and authenticate the actual conversation among them. For a complete organization security solution, you would plan and deploy both types of rules. Due to the complexity of security connection rules and the ability to impact the ability of computers to talk to one another within an organization, it requires a lab environment and rigorous testing to ensure you get the results the situation demands.

**Figure 4-27Windows Defender Firewall, Global IPSec Settings**



**Note 15**

Creating and applying a secure isolation design with Windows Defender Firewall and Advanced Security is beyond the scope of this book. To learn more about advanced design and application for Windows Defender Firewall with Advanced Security, see: [https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security-design-guide](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security-design-guide" \t "_blank).

The IPSec default settings you can configure are:

* Key exchange—This setting controls which method is used to securely transmit the keys used for data encryption between both computers.
* Data protection—This setting controls which methods are used to encrypt and protect the integrity of data.
* Authentication method—This setting controls which method is used to authenticate the two computers creating an IPSec connection. The simplest method is a pre-shared key (password), but it is also the least secure and is not recommended. By default, Kerberos authentication is used.

**Note 16**

If the settings are configured as the value Default, they can be overridden by Group Policy-based settings. This is the preferred approach in a domain environment, while custom settings are preferred when the computer is not domain joined.

The IPSec exemption settings you can configure are:

* Exempt ICMP from IPsec—This is a Yes or No setting. ICMP packets are commonly used by troubleshooting tools (such as ping), and if they are exempted from IPSec by the network administrator, it could assist in diagnosing issues during troubleshooting. Note that exempting ICMP packets from IPSec doesn’t automatically allow them through the firewall. The Windows Defender Firewall rules must be enabled separately to allow ICMP traffic as well.

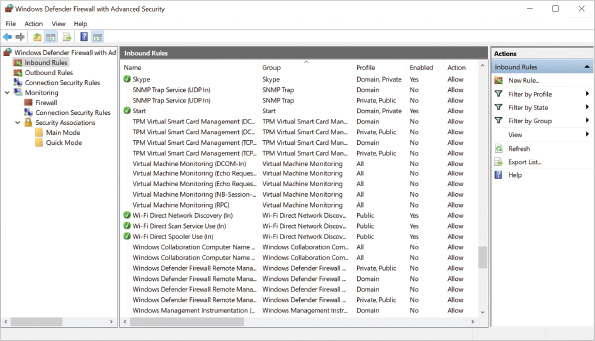
The IPSec tunnel authorization settings you can configure are:

* None—No user or computer authorization is required to use a tunnel mode connection from a remote computer to the local computer.
* Advanced, Custom—List specific users or computers that are either allowed (i.e., authorized) or denied (i.e., exceptions) the use of the tunnel mode connection from a remote computer to the local computer.

### Viewing and Editing Firewall Rules

A large number of inbound and outbound network traffic rules are created by default in Windows 10. [Figure 4-28](javascript://) shows a sample list of inbound rules. In the list of rules, you can see the name of the rule, a group of rules it belongs to, profiles the rule can belong to, if the rule is enabled, and whether the rule allows or denies packets. Additional columns can be added to the view by selecting more columns in the view options if desired.

**Figure 4-28Windows Defender Firewall, Sample Inbound Rule Listing**

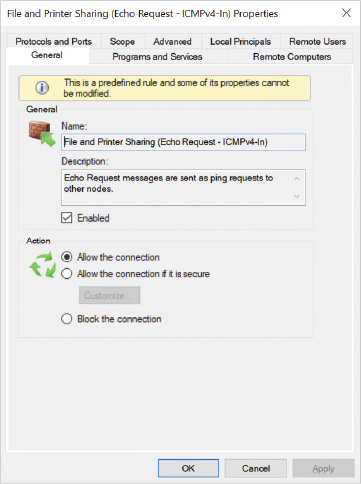


Enlarge Image

The icons for each rule also give you information about that rule. Rules that are enabled and allow packets have a green arrow icon. Rules that are enabled and deny packets have a red circle with a slash. If the icon is blank, the rule is disabled.

You modify an existing rule by changing its properties. [Figure 4-29](javascript://) shows the properties of the Echo Request ICMPv4-In rule.

**Figure 4-29Windows Defender Firewall, Sample Inbound Default Rule Properties**



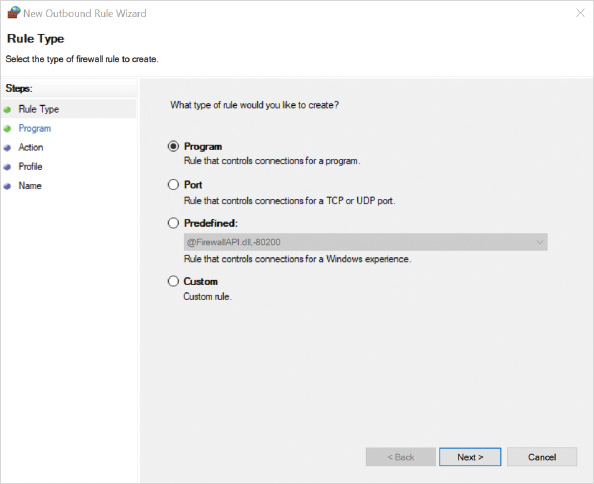
The tabs in the properties of an inbound rule are:

* General—This tab allows you to configure the rule name, configure the rule description, enable or disable the rule, and choose the rule action (e.g., allow, block, or allow if secured by user or computer identity).
* Programs and Services—This tab allows you to select programs, application packages, and services that this rule applies to.
* Remote Computers—This tab allows you to restrict connections to include or exclude specific computers or groups of computers. IPSec authentication is required.
* Remote Users—This tab allows you to restrict connections to include or exclude specific users or groups of users. IPSec authentication is required.
* Local Principals—This tab allows you to restrict connections to include or exclude specific users or application package properties.
* Protocols and Ports—This tab allows you to specify the protocol type this rule applies to, the local port this rule applies to, the remote port this rule applies to, and which ICMP packet types this rule applies to.
* Scope—This tab allows you to specify the source and destination IP addresses this rule applies to.
* Advanced—This tab allows you to specify which profiles (e.g., domain, private, public) and interface types (e.g., local area network, wireless, remote access) this rule applies to. Edge traversal settings enable you to allow or block traffic that came from the other side of a NAT router (i.e., most likely from the Internet) or let the user or an application decide if that’s acceptable.

### Creating New Firewall Rules

You can create firewall rules using all the methods mentioned at the start of this section. If you use the Windows Defender Firewall with Advanced Security interface to create a new firewall rule, a wizard guides you through the process. The wizard for creating an outbound rule is shown in [Figure 4-30](javascript://). Using a wizard simplifies the process of rule creation because it limits the options during the creation process to only those options you need for the particular type of rule you are creating.

**Figure 4-30Windows Defender Firewall, New Outbound Rule Wizard**



The rule types you can create with the Outbound Rule wizard are:

* Program—A program rule allows or denies traffic for a specific program that is specified by selecting an executable file. You can specify which profiles this rule applies to.
* Port—A port rule allows or denies traffic for a specific TCP or UDP port. You can specify which profiles this rule applies to.

**Tip**

You should know common TCP/IP application port numbers, with several common values listed in [Table 4-11](javascript://), or refer to a recent listing from IANA to understand which port numbers are used with common TCP/IP applications at [https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml](https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml" \t "_blank).

**Table 4-11**

### Common TCP/UDP Application Port Numbers

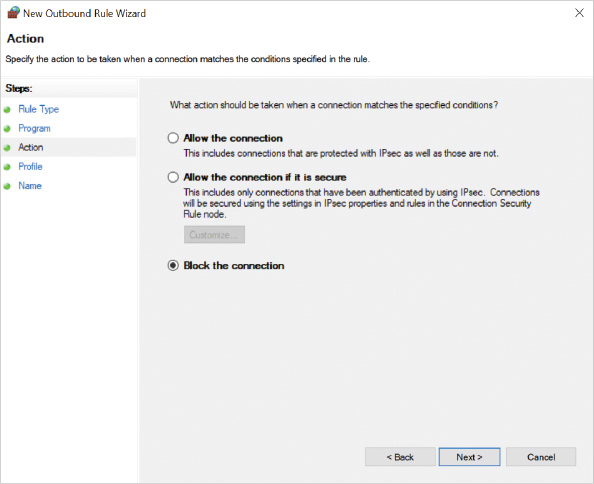
| **Program or Application** | **Server-Side Port Value** |
| --- | --- |
| echo | 7 |
| ftp-data | 20 |
| ftp | 21 |
| ssh | 22 |
| telnet | 23 |
| smtp | 25 |
| DNS | 53 |
| HTTP | 80 |
| POP3 | 110 |
| IMAP | 143 |
| HTTPS | 443 |

* Predefined—A predefined rule creates a group of rules to allow or deny Windows functions, such as file and printer sharing or Remote Assistance. In most cases, these rules are already created and do not need to be re-created. These rules allow you to define source and destination computers (endpoints) that the rule applies to. You can also specify to which profiles this rule applies.
* Custom—A custom rule lets you configure programs, ports, protocols, endpoints, and profiles. You can use this type of rule when the other rule types do not meet your needs.

When you define the actions for a rule, as shown in [Figure 4-31](javascript://), you can specify the following:

* Allow the connection—This option allows connections based on this rule.
* Allow the connection if it is secure—This option allows connections based on this rule only when an IPSec connection is configured. By default, this option requires that IPSec authenticates the connection and ensures integrity; however, you also have the option to require data encryption. Additionally, because a secure connection is based on an IPSec rule, you can select to have this rule override other block firewall rules.
* Block the connection—This option denies all connections based on this rule; however, a rule with this option selected can be overridden by another rule that allows only secure connections.

**Figure 4-31Windows Defender Firewall, New Outbound Rule Wizard, Rule Actions**

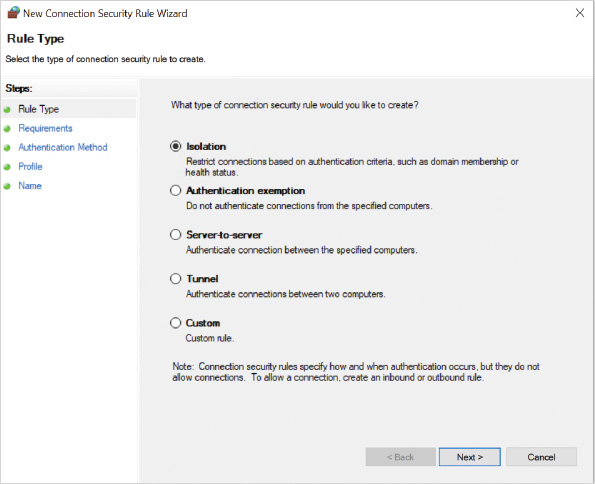


### Creating New Computer-Connection Security Rules

Computer-connection security rules use IPSec to authenticate and secure communication between two computers. Remember that these rules combine with the general inbound and outbound traffic rules to create a customized security experience at the firewall level. The computer-connection security rule types, shown in [Figure 4-32](javascript://), are:

* Isolation—An isolation rule restricts communication with other computers to only those that can be authenticated. You can specify the method of authentication. The rule can apply to inbound connections, outbound connections, or both.
* Authentication exemption—An authentication exemption rule specifies IP addresses or IP address ranges that do not need to be authenticated when communicating with this computer. Effectively, this creates exceptions to an isolation rule.
* Server-to-server—A server-to-server rule is used to enforce IPSec settings between two computers. Typically, this type of rule is used to require encryption between two computers, such as a client and server; however, it can also be configured to apply only for certain connection types, such as wireless connections.
* Tunnel—A tunnel rule is used to configure Windows 10 as the endpoint of a secure communication tunnel. Other computers use the Windows 10 computer as their default gateway to secure communication through the IPSec tunnel. This type of rule is seldom used.
* Custom—A custom rule allows you to configure a customized rule if the standard rule types do not meet your needs.

**Figure 4-32Windows Defender Firewall, New Connection Security Rule Wizard, Rule Types**



### PowerShell Cmdlets for Network Security

[Table 4-12](javascript://) shows some of the common IP network security PowerShell cmdlets that can be used to update the Windows Defender Firewall and the Advanced Security settings.

**Table 4-12**

### PowerShell Windows Defender Firewall and Related Network Security Cmdlets

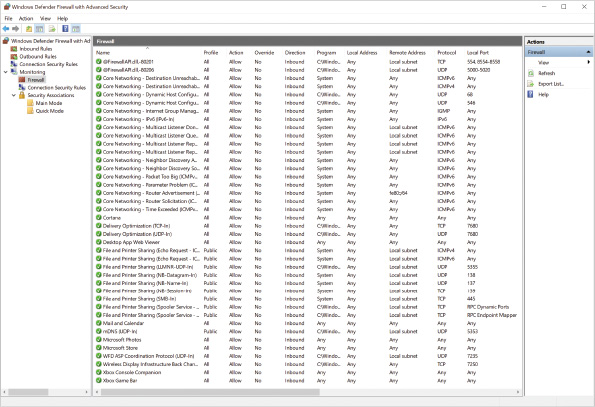
| **PowerShell Cmdlet** | **Description** |
| --- | --- |
| Copy-NetFirewallRule | Copies an entire firewall rule, and associated filters, to the same or to a different policy store. |
| Disable-NetFirewallRule | Disables a firewall rule. |
| Enable-NetFirewallRule | Enables a previously disabled firewall rule. |
| Get-NetFirewallProfile | Displays settings that apply to the per-profile configurations of the Windows Defender Firewall with Advanced Security. |
| Get-NetFirewallRule | Retrieves firewall rules from the target computer. |
| Get-NetFirewallSetting | Retrieves the global firewall settings of the target computer. |
| New-NetFirewallRule | Creates a new inbound or outbound firewall rule and adds the rule to the target computer. |
| Remove-NetFirewallRule | Deletes one or more firewall rules that match the specified criteria. |
| Rename-NetFirewallRule | Renames a single firewall rule. |
| Set-NetFirewallProfile | Configures settings that apply to the per-profile configurations of the Windows Defender Firewall with Advanced Security. |
| Set-NetFirewallRule | Modifies existing firewall rules. |
| Set-NetFirewallSetting | Modifies the global firewall settings of the target computer. |

Enlarge Table

### Monitoring Windows Defender Firewall Rules and Connections

When you view the inbound or outbound rules for Windows Defender Firewall, there is a large list of rules that includes enabled or disabled rules. The Firewall node below Monitoring in Windows Defender Firewall with Advanced Security, shown in [Figure 4-33](javascript://), allows you to see all of the rules that are enabled in one screen. This quickly shows you how your system is configured. This is also useful to see the rules that are being applied by Group Policy.

**Figure 4-33Windows Defender Firewall, Firewall Monitoring View**



Enlarge Image

The Connection Security Rules node below Monitoring allows you to see the computer connection security rules that are enabled and any security associations that are active. A security association is the set of rules for communication negotiated between two computers. If two computers have a security association, they are using IPSec to communicate.

Security associations are listed in the following two categories:

* Main Mode—Used for the initial configuration of an IPSec connection, including authentication
* Quick Mode—Signifies a secure IPSec communication channel has been negotiated

**Activity 4-5**

### Configuring Windows Defender Firewall

**Time Required: 15 minutes**

**Objective:**Configure Windows Defender Firewall by using the Windows Defender Firewall with Advanced Security utility

**Description:**Windows Defender Firewall in Windows 10 is capable of performing outbound filtering as well as inbound filtering. In this activity, you create a rule to block access to Internet websites and then disable the rule.

1. 1

If necessary, start your computer and sign in.

1. 2

On the taskbar, click **Microsoft Edge**.

1. 3

In the Search or enter web address box, type [http://www.microsoft.com](http://www.microsoft.com/" \t "_blank) and then press **Enter**. When the Microsoft website displays, it confirms that your computer is able to connect to the Internet properly right now.

1. 4

Exit Microsoft Edge.

1. 5

Click the **Start** button, in the search box type **firewall**, and then press **Enter**. This displays the Firewall and network protection system settings.

1. 6

Click the **Advanced settings** link in the left pane. This opens the Windows Defender Firewall with Advanced Security utility.

1. 7

If you are prompted with a User Account Control window, click **Yes**.

1. 8

Read the overview of Windows Defender Firewall configuration. Windows Defender Firewall is on for all network location profiles, inbound connections that do not match a rule are blocked by default, and outbound connections that do not match a rule are allowed by default. In the Overview pane, click the **Windows Defender Firewall Properties** link.

1. 9

Click the **Private Profile** tab. These settings apply for all Private networks.

1. 10

In the Settings area, click the **Customize** button. Here, you can configure whether notifications are displayed when inbound connections are blocked and how local firewall rules are combined with firewall rules defined in Group Policy.

1. 11

Click **Cancel** to close the Customize Settings for the Private Profile dialog box.

1. 12

In the Logging area, click the **Customize** button. Here, you can configure logging for Windows Defender Firewall.

1. 13

In the Log dropped packets box, select **Yes** and then click OK. Now all blocked connections will be logged to C:\Windows\system32\LogFiles\Firewall\pfirewall.log.

1. 14

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

1. 15

In the left pane, click **Outbound Rules**. These are the rules that control outbound communication. However, none of the default rules block outbound communication.

1. 16

In the left navigation pane, right-click **Outbound Rules** and then click **New Rule**.

1. 17

In the Rule Type window, click **Custom** and then click **Next**.

1. 18

In the Program window, if necessary click **All programs** and then click **Next**.

1. 19

In the Protocol type box, click TCP.

1. 20

In the Remote port box, click to select **Specific Ports** and then type **80,443**. This rule will apply to outbound packets addressed to port 80 and port 443. Ports 80 and 443 are used by web servers.

1. 21

Click **Next**.

1. 22

Click **Next** to select the default option of applying to all computers.

1. 23

If necessary, click **Block the connection** and then click **Next**. This rule will block connections to port 80 and port 443.

1. 24

Click **Next** to accept the default configuration of this rule applying to all profiles. You can also limit it to specific profiles.

1. 25

In the Name box, type **Block Web** and then click **Finish**. The Block Web rule is now at the top of the list of outbound rules. Notice that it is enabled and the action is block.

1. 26

On the taskbar, click **Microsoft Edge**. Note that some cached content may still be displayed; however, this is content that was downloaded before you created the rule blocking outbound connections to web servers.

1. 27

In the Search or enter web address box, type [http://www.microsoft.com](http://www.microsoft.com/" \t "_blank) and then press **Enter**. You are unable to load the Microsoft website because the Block Web rule is blocking access to all websites.

1. 28

Exit Microsoft Edge.

1. 29

Click the **Start** button, in the search box type **cmd**, right-click **Command Prompt**, and then click **Run as administrator** on the shortcut menu.

1. 30

If you are prompted with a User Account Control window, click **Yes**.

1. 31

At the command prompt, type **netsh advfirewall firewall set rule name=“Block Web” new enable=no** and then press **Enter**. This will disable the rule called “Block Web” that we created earlier using netsh instead of using the GUI interface to show the power of using netsh with advanced configurations.

1. 32

In Windows Defender Firewall with Advanced Security, below Actions click **Refresh** to refresh the view. Note that the “Block Web” rule is not enabled.

1. 33

On the taskbar, click **Microsoft Edge**.

1. 34

In the Search or enter web address box, type [http://www.microsoft.com](http://www.microsoft.com/" \t "_blank) and then press **Enter**. This verifies that web connectivity is working again.

1. 35

Close the Microsoft Edge window.

1. 36

Click the **Start** button, in the search box type **powershell**, right-click the result **Windows PowerShell**, and then click **Run as administrator** on the shortcut menu.

1. 37

If you are prompted with a User Account Control window, click **Yes**.

1. 38

At the PowerShell prompt, type **Remove-NetFirewallRule -DisplayName “Block Web”** and then press **Enter**. In the future, Microsoft will deprecate the netsh utility and use PowerShell cmdlets as a preference for script-based configurations. The netsh syntax and operation is specific to netsh, whereas PowerShell cmdlets have common programming behavior. For example, netsh has to refer to firewall rules by name; however, PowerShell logic can interact with rules based on their settings, using firewall properties to trigger updates.

1. 39

In the Windows Defender Firewall with Advanced Security window, below Actions in the right-most actions pane click **Refresh** to refresh the view. Note that the “Block Web“ rule is no longer listed.

1. 40

Close the Administrator Windows PowerShell window.

1. 41

Switch to the Administrator command prompt window. At the command prompt type **netsh advfirewall reset ?** and then press **Enter**. This will show the help screen for the netsh command to reset Windows Defender Firewall with Advanced Security policy to default values.

**Caution**

The netsh advfirewall reset command will reset default firewall rules and remove firewall customizations for previously installed applications and updated operating system components, which could result in broken functionality. Resetting firewall settings is a nontrivial decision but could be useful in a lab setting while you are testing custom settings for an organization.

1. 42

Close the Administrator Command Prompt window.

1. 43

Close the Windows Defender Firewall with Advanced Security window.

1. 44

Switch to the Windows Security window that is open to the Firewall & network protection settings. Click the **Restore firewalls to default** link at the bottom.

1. 45

This will open the Restore Defaults window for Windows Defender Firewall. This will have the same effect as the netsh advfirewall reset command but with less options than netsh. Click **Cancel** to abort the operation and close the window.

1. 46

Close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 4-7a**Summary**

* Network and Internet from the Settings app as well as Network and Sharing Center from Control Panel allow you to view and access networking information, such as viewing active networks, network status, and connection status, and to access configuration and troubleshooting wizards.
* Windows 10 is network-aware and can sense which type of network location it is connected to and change settings accordingly. Network location types are Private, Public, or Domain. These network location profiles can be applied to newly discovered and past remembered network locations.
* Network connections are composed of clients, services, protocols, and network drivers. Windows 10 includes both IPv4 and IPv6 protocols, neither of which can be removed.
* The important configuration concepts in IPv4 are IP addresses, subnet masks, default gateways, DNS, and WINS. If any of these components are configured incorrectly, network communication may be affected.
* Windows 10 can obtain IP configuration information from static configuration data, DHCP, APIPA, or an alternate IP configuration. DHCP is the most common.
* Windows 10 uses IPv6 to support peer-to-peer and general networking applications. IPv6 is becoming more common, and the address types can be recognized based on their prefix values. The most common method used for configuring IPv6 is based on stateful or stateless automatic configuration.
* The primary technologies for connecting a single computer or device to the Internet are cable, DSL, cellular, and dial-up. Cable and DSL are high-speed connection methods, while dial-up is slow. DSL commonly requires the configuration of PPPoE. Cellular requires a broadband device to supply Internet connectivity, potentially a cable to tether (connect) the computer to the mobile device, and a paid contract from the broadband supplier to use the feature.
* When an Internet connection is shared by multiple computers, there must be a mechanism to share the single IP address assigned by your ISP. You can use a router or Internet Connection Sharing (ICS). For sharing over Wi-Fi, the preferred standard is to configure your computer as a mobile hotspot or use Wi-Fi Direct technology. The older Wireless Ad Hoc feature has limited security and is difficult to configure in comparison. Windows also supports wireless hosted network as a similar but more advanced solution compared to wireless ad hoc, but it is still harder to configure and has weaker security than the preferred solutions.
* Wireless networking in Windows 10 supports different versions of the IEEE 802.11 standard that defines how a wireless adapter in a computer connects to a wireless access point (WAP). The WAP’s SSID and security settings must be correctly configured to enable the wireless client to connect. Wireless clients can automatically reconnect when they are in range of a WAP. Network location settings and Windows Defender Firewall can help secure the data connection. Cell-like convenience for public roaming WiFi is enabled by the newer Hotspot 2.0 technology.
* Windows Defender Firewall is a host-based firewall included with Windows 10 and can perform inbound and outbound filtering. Also, IPSec security connection rules are combined with firewall rules in Windows 10. Windows Defender Firewall can be configured by local settings and utilities, Group Policy, or cloud-based Intune.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 4-7b**Key Terms**

* [**802.11**](javascript://)
* [**802.1x**](javascript://)
* [**address prefix**](javascript://)
* [**alternate IP configuration**](javascript://)
* [**Automatic Private IP Addressing (APIPA)**](javascript://)
* [**autonegotiation**](javascript://)
* [**broadcast address**](javascript://)
* [**classless interdomain routing (CIDR)**](javascript://)
* [**client**](javascript://)
* [**Client for Microsoft Networks**](javascript://)
* [**default gateway**](javascript://)
* [**Domain Name System (DNS)**](javascript://)
* [**domain network**](javascript://)
* [**Dynamic Host Configuration Protocol (DHCP)**](javascript://)
* [**eSIM**](javascript://)
* [**File and Printer Sharing for Microsoft Networks**](javascript://)
* [**fully qualified domain name (FQDN)**](javascript://)
* [**hostname**](javascript://)
* [**Hotspot 2.0**](javascript://)
* [**Institute of Electrical and Electronics Engineers (IEEE)**](javascript://)
* [**Internet Connection Sharing (ICS)**](javascript://)
* [**Internet Protocol Version 4 (TCP/IPv4)**](javascript://)
* [**Internet Protocol Version 6 (TCP/IPv6)**](javascript://)
* [**IP address**](javascript://)
* [**ipconfig**](javascript://)

* **[IPSec](javascript://)**
* [**ISP**](javascript://)
* [**Link-Local Multicast Name Resolution (LLMNR)**](javascript://)
* [**location type**](javascript://)
* [**loopback address**](javascript://)
* [**multicast**](javascript://)
* [**nbtstat**](javascript://)
* [**NetBIOS**](javascript://)
* [**netsh**](javascript://)
* [**netstat**](javascript://)
* [**Network Address Translation (NAT)**](javascript://)
* [**Network and Internet Settings**](javascript://)
* [**Network and Sharing Center**](javascript://)
* [**network discovery**](javascript://)
* [**network driver**](javascript://)
* [**network location awareness**](javascript://)
* [**nslookup**](javascript://)
* [**octet**](javascript://)
* [**Online Sign-Up**](javascript://)
* [**Passpoint**](javascript://)
* [**pathping**](javascript://)
* [**Personal Area Network (PAN)**](javascript://)
* [**ping**](javascript://)
* [**Point-to-Point Protocol over Ethernet (PPPoE)**](javascript://)
* [**private network**](javascript://)
* [**protocol**](javascript://)
* [**public network**](javascript://)
* [**Quality of Service (QoS)**](javascript://)
* [**RADIUS server**](javascript://)
* [**route**](javascript://)
* [**routing table**](javascript://)
* [**Security Set Identifier (SSID)**](javascript://)
* [**Server Message Block (SMB)**](javascript://)
* [**SIM**](javascript://)
* [**stateful automatic address configuration**](javascript://)
* [**stateless automatic address configuration**](javascript://)
* [**subnet mask**](javascript://)
* [**Time To Live (TTL)**](javascript://)
* [**tracert**](javascript://)
* [**unicast**](javascript://)
* [**Wi-Fi Direct**](javascript://)
* [**Windows Defender Firewall**](javascript://)
* [**Windows Defender Firewall and Advanced Security utility**](javascript://)
* [**Windows Internet Naming Service (WINS)**](javascript://)
* [**wireless access point (WAP)**](javascript://)
* [**Wireless Ad Hoc**](javascript://)
* [**Wireless Fidelity (Wi-Fi) Alliance**](javascript://)
* [**Wireless Hosted network**](javascript://)
* [**WPA2-Enterprise**](javascript://)
* [**WPA2-Personal**](javascript://)
* [**WPA3-Personal**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 4-7c**Review Questions**

1. Your computer is configured to obtain an IPv4 address and DNS server address automatically. What utility will help you to find the IPv4 address of your computer? (Choose all that apply.)
   1. Get-NetIPAddress
   2. ipconfig
   3. Get-NetIPConfiguration
   4. netsh
   5. arp
2. provides you with a way to control how your computer views other computers on the network and advertises its presence on the network.
   1. Windows Defender Firewall
   2. SMB
   3. Network discovery
   4. IPv6
   5. Network location
3. Your computer is configured to obtain an IPv4 address and DNS server address automatically. Network traffic is not flowing as expected. You are asked by your manager to output the current IPv4 routing table. What commands can you use to display the IPv4 routing table? (Choose all that apply.)
   1. route
   2. netstat
   3. nslookup
   4. Get-NetRoute
   5. Get-RouteIPv4Table
4. Which protocol is used by the Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks to communicate with one another and share files?
   1. FTP
   2. IPv4
   3. IPv6
   4. HTTP
   5. SMB
5. For a Class C IPv4 address, what is the correct default subnet mask value, specified as either a dotted decimal address or a CIDR value? (Choose all that apply.)
   1. 255.0.0.0
   2. /24
   3. 255.255.255.0
   4. C::/24
   5. 255.255.256.0
6. Which of these addresses represents a valid IPv6 link-local address?
   1. 169.254.12.1
   2. ::1
   3. FE80::2cab:2a76:3f57:8499
   4. 2001:0:4137:9e74:2cab:2a76:3f57:8499
   5. FF::1:2
7. Which IPv4 configuration options must be configured properly to communicate with websites on the Internet? (Choose all that apply.)
   1. IP address
   2. subnet mask
   3. default gateway
   4. DNS
   5. WINS
8. Which of the following IP addresses is a valid IPv4 address and can be used by a host on the global Internet? (Choose all that apply.)
   1. 192.168.0.55
   2. 172.32.0.1
   3. 169.254.99.208
   4. 38.15.222.299
   5. 99.99.99.99
9. Which method can be used to assign IPv4 configuration settings when a DHCP server is not available? (Choose all that apply.)
   1. static configuration
   2. DNS
   3. WINS
   4. APIPA
   5. alternate IP configuration
10. To convert host names to IP addresses on the Internet,  is used.
11. Which of the following IPv4 addresses is a valid IPv4 address and has the same network ID as 192.168.112.45 given the subnet mask 255.255.255.0?
    1. 10.0.0.45
    2. 192.168.113.46
    3. 192.168.112.257
    4. 172.16.112.45
    5. 192.168.112.5
12. Your company is looking at securing connectivity between an internal server and workstations on the local area network. The network infrastructure does not support VLAN technology to compartmentalize network traffic, so they ask you for an overall design plan using Windows Defender Firewall with Advanced Security. Computers are required to confirm their identity when they communicate with one another using IPSec. For which of the following should your plan reference specific rules? (Select all that apply.)
    1. connection security rules
    2. IPSec token rules
    3. inbound rules
    4. outbound rules
    5. routing table rules
13. Which of the following IPv4 addresses have the same network ID as 10.16.112.45 given the subnet mask 255.255.0.0? (Choose all that apply.)
    1. 10.16.160.45
    2. 192.168.172.46
    3. 10.16.122.2
    4. 10.16.185.45
    5. 10.18.114.3
14. Your company requires computers to authenticate to one another and enforces this requirement with Windows Defender Firewall with advanced security rules. You are asked to customize exceptions based on specific IP ranges. This can be done with a(n)  connection security rule.
    1. isolation
    2. outbound
    3. authentication exemption
    4. server-to-server
    5. inbound
15. A Wi-Fi access point with a non-broadcasting SSID is not discoverable through any means unless a Wi-Fi client is configured to connect to it in advance. (True or False)?

True

False

1. Which Internet connection type is most likely to require the use of PPPoE?
   1. cable
   2. DSL
   3. dial-up
   4. wireless hotspot
2. Which of these addresses represents a valid IPv6 global unicast address?
   1. 169.254.12.1/64
   2. 2001::1::FEA
   3. FE80::2cab:2a76:3f57:8499
   4. 2001:0:4137:9e74:2cab:2a76:3f57:8499
   5. FF::1:2
3. Which of these addresses represents a valid loopback address? (Choose all that apply.)
   1. ::1
   2. ::/0
   3. FF::1
   4. 127.0.0.1
   5. 127::1/32
4. Which utilities can be used to perform advanced firewall configuration? (Choose all that apply.)
   1. Device security
   2. netsh
   3. Group Policy
   4. Windows Defender Firewall and Advanced Security
   5. Windows PowerShell
5. A computer has the IPv4 address 192.168.0.23 and a subnet mask of 255.255.255.0. Which of these addresses represents a possible default gateway address? (Choose all that apply.)
   1. 192.168.0.254
   2. 193.168.0.1
   3. 0.0.0.1
   4. 127.0.0.1
   5. 192.168.0.1

Go to pg.

[**help**](javascript://)