Application Opened

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

**Chapter**

**7**

**Setting Up a Local Network**

* [Chapter Introduction](javascript://)
* **7-1**[Types of Networks and Network Connections](javascript://)
  + **7-1a**[Internet Connection Technologies](javascript://)
* **7-2**[Connecting a Computer to a Local Network](javascript://)
  + **7-2a**[Connecting to an Ethernet Wired or Wi-Fi Wireless Local Network](javascript://)
  + **7-2b**[Creating a VPN Connection](javascript://)
  + **7-2c**[Creating a Dial-Up Connection](javascript://)
  + **7-2d**[Dynamic and Static IP Configurations](javascript://)
  + **7-2e**[Alternate IP Address Configuration](javascript://)
  + **7-2f**[Managing Network Adapters](javascript://)
* **7-3**[Setting Up a Multifunction Router for a SOHO Network](javascript://)
  + **7-3a**[Functions of a SOHO Router](javascript://)
  + **7-3b**[Installing and Configuring a Router on the Local Network](javascript://)
  + **7-3c**[Limiting Internet Traffic on Your Network](javascript://)
  + **7-3d**[Setting up a Wireless Network](javascript://)
* **7-4**[Troubleshooting Network Connections](javascript://)
  + **7-4a**[Ping [-A] [-T] [*TargetName*]](javascript://)
  + **7-4b**[Ipconfig [/All] [/Release] [/Renew] [/Displaydns] [/Flushdns]](javascript://)
  + **7-4c**[Nslookup [*ComputerName*]](javascript://)
  + **7-4d**[Tracert [*TargetName*]](javascript://)
  + **7-4e**[The net Commands](javascript://)
  + **7-4f**[Netstat [-A] [-B] [-O]](javascript://)
* **7-5**[Chapter Review](javascript://)
  + **7-5a**[Chapter Summary](javascript://)
  + **7-5b**[Key Terms](javascript://)
  + **7-5c**[Thinking Critically](javascript://)
  + **7-5d**[Hands-On Projects](javascript://)
  + **7-5e**[Real Problems, Real Solutions](javascript://)
  + **7-5f**[Exam Tips](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 completing this chapter, you will be able to:

* Describe network types and the Internet connections they use
* Connect a computer to a wired or wireless network
* Configure and secure a multifunction router on a local network
* Troubleshoot network connections using the command line

In this chapter, you learn about the types of networks and the technologies used to build networks. You also learn to connect a computer to a network and how to set up and secure a small wired or wireless network.

This chapter prepares you to assume total responsibility for supporting both wired and wireless networks in a small office/home office (SOHO) environment. Later, you’ll learn more about the hardware used in networking, including network devices, connectors, cabling, networking tools, and the types of networks used for Internet connections. Let’s get started by looking at the types of networks you might encounter as an IT support technician and the types of connections they might use to connect to the Internet.

**A+ Exam Tip**

Much of the content in this chapter applies to both the A+ Core 1 220-1001 exam and the A+ Core 2 220-1002 exam.

Go to pg.

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

Application Opened

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

**7-1**Types of Networks and Network Connections

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

* 2.4

Compare and contrast wireless networking protocols.

* 2.7

Compare and contrast Internet connection types, network types, and their features.

A computer network is created when two or more computers can communicate with each other. Networks can be categorized by several methods, including the technology used and the size of the network. When networks are categorized by their size or physical area they cover, these are the categories used, listed from smallest to largest:

**A+ Core 2**

* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

* ***PAN***. A [**PAN (personal area network)**](javascript://) consists of personal devices such as cell phones and laptop computers communicating at close range. PANs can use wired connections (such as USB or Lightning) or wireless connections (such as Bluetooth or Wi-Fi, also called 802.11).
* ***LAN***. A [**LAN (local area network)**](javascript://) covers a small local area, such as a home, office, or a small group of buildings. LANs can use wired (most likely Ethernet) or wireless technologies (most likely Wi-Fi). A LAN allows workstations, servers, printers, and other devices to communicate and share resources.
* ***WMN***. A [**WMN (wireless mesh network)**](javascript://) consists of many wireless devices communicating directly with each other rather than through a single, central device. Some or all of the devices on the WMN can serve as connection points for other devices to communicate across longer distances. This technology is commonly used in IoT (Internet of Things) wireless networks, where many types of devices, such as thermostats, light switches, door locks, and security cameras, are connected to the network and on to the Internet.
* ***MAN***. A [**MAN (metropolitan area network)**](javascript://) covers multiple buildings in a large campus or a portion of a city, such as a downtown area. It’s usually the result of a cooperative effort to improve service to its users. Network technologies used can be wireless (most likely LTE) and/or wired (for example, Ethernet with fiber-optic cabling).
* ***WAN.*** A [**WAN (wide area network)**](javascript://) covers a large geographical area and is made up of many smaller networks. The best-known WAN is the Internet. Some technologies that connect a single computer or LAN to the Internet include DSL, cable Internet, satellite, cellular WAN, and fiber optic.

**A+ Exam Tip**

The A+ Core 1 exam expects you to be able to compare LAN, WAN, PAN, MAN, and WMN networks.

Now let’s look at network technologies used for Internet connections.

Go to pg.

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

Application Opened

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

## 7-1aInternet Connection Technologies

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

* 2.4

Compare and contrast wireless networking protocols.

* 2.7

Compare and contrast Internet connection types, network types, and their features.

**A+ Core 2**

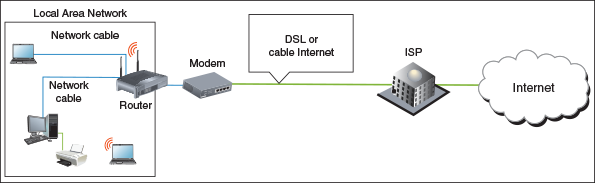
* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

To connect to the Internet, a device or a network first connects to an [**Internet service provider (ISP)**](javascript://), such as Xfinity or Spectrum. The most common types of connections for SOHO networks are DSL and cable Internet (commonly called cable or cable modem). See [Figure 7-1](javascript://). When connecting to an ISP, know that upload speeds are generally slower than download speeds. These rates differ because users typically download more data than they upload. Therefore, an ISP devotes more of the available bandwidth to downloading and less of it to uploading.

**Figure 7-1**

An ISP stands between a LAN and the Internet



Enlarge Image

Networks are built using one or more technologies that provide varying degrees of bandwidth. [**Bandwidth**](javascript://) is the theoretical number of bits that can be transmitted over a network connection at one time, similar to the number of lanes on a highway. The networking industry refers to bandwidth as a measure of the maximum rate of data transmission in bits per second (bps), thousands of bits per second (Kbps), millions of bits per second (Mbps), or billions of bits per second (Gbps). Bandwidth is the theoretical or potential speed of a network, whereas [**data throughput**](javascript://) is the average of the actual speed. In practice, network transmissions experience delays, called [**latency**](javascript://), that result in slower network performance. For example, wired signals traveling across long cables or wireless signals crossing long distances through the air can cause signal strength degradation, resulting in latency. Latency is measured by the round-trip time it takes for a message to travel from source to destination and back to source.

[Table 7-1](javascript://) lists network technologies used by local networks to connect to the Internet. The table is more or less ordered from slowest to fastest maximum bandwidth within each category, although latency can affect the actual bandwidth of any particular network. We’ll explore each of these technologies in more depth throughout this chapter.

**Table 7-1**

### Networking technologies (continues)

| **Technology (Wireless or Wired)** | **Maximum Speed** | **Description** |
| --- | --- | --- |
| **Wireless Internet connection: Satellite and WiMAX** | | |
| Satellite | Up to 15 Mbps | Requires a dish to send to and receive from a satellite, which is in a relative fixed position with the Earth. |
| WiMAX | Up to 30 Mbps | Requires a transmitter to send to and receive from a WiMAX tower up to 30 miles away. WiMAX was once popular in rural areas for wireless Internet connections, but it is losing this market space to cellular solutions such as LTE. |
| **Wireless Internet connection: Cellular** | | |
| [**3G**](javascript://) cellular (third-generation cellular) | At least 200 Kbps, but can be up to 4 Mbps | Improved over earlier technologies and allows for transmitting data and video. Uses either CDMA or GSM mobile phone services. Speeds vary widely according to the revision standards used. |
| [**4G**](javascript://) cellular (fourth-generation cellular) | 100 Mbps to 1 Gbps | Higher speeds are achieved when the mobile device stays in a fixed position. A 4G network typically uses LTE (Long Term Evolution) technology. |
| [**5G**](javascript://) cellular (fifth-generation cellular) | 10–50 Gbps and beyond | At the time of this writing, 5G devices are expected on the market as soon as 2019 with more widespread use beginning in 2020, and additional improvements to the technology in later years. |
| **Wired Internet connection: Telephone** | | |
| Dial-up or regular telephone (POTS, for plain old telephone service) | Up to 56 Kbps | Slow access to an ISP using a modem and dial-up connection over phone lines. |
| ISDN | 64 Kbps or 128 Kbps | [**ISDN (Integrated Services Digital Network)**](javascript://) is an outdated business-use connection to an ISP over dial-up phone lines. |
| SDSL (Symmetric Digital Subscriber Line) | Up to 22 Mbps | Equal bandwidth in both directions. SDSL is a type of broadband technology. ([**Broadband**](javascript://) refers to a networking technology that carries more than one type of signal on the same cabling infrastructure, such as DSL and telephone or cable Internet and TV.) DSL uses regular phone lines and is an always-up or always-on connection that does not require a dial-up. |
| ADSL (Asymmetric DSL) | 640 Kbps upstream and up to 24 Mbps downstream | Most bandwidth is allocated for data coming from the ISP to the user. Slower versions of ADSL are called ADSL Lite or DSL Lite. ISP customers pay according to a bandwidth scale. |
| VDSL (very-high-bit-rate DSL) | Up to 70 Mbps | A type of asymmetric DSL that works only over a short distance. |
| **Other wired Internet connections** | | |
| Cable Internet | Up to 160 Mbps, depending on the type of cable | Connects a home or small business to an ISP, usually comes with a cable television subscription, and shares cable TV lines. If available, fiber-optic cable gives highest speeds. |
| Dedicated line using fiber optic | Up to 43 Tbps | Dedicated fiber-optic line from ISP to business or home. Speeds vary widely with price. |
| **Wired local network: Ethernet** | | |
| Fast Ethernet (100BaseT) | 100 Mbps | Used for local networks. |
| Gigabit Ethernet (1000BaseT) | 1000 Mbps or 1 Gbps | Fastest Ethernet standard for small, local networks. |
| 10-Gigabit Ethernet (10GBaseT) | 10 Gbps | Typically requires fiber media, is mostly used on the backbone of larger enterprise networks, and can also be used on WAN connections. |
| **Wireless local network: Wi-Fi** | | |
| [**802.11a**](javascript://) | Up to 54 Mbps | No longer used. |
| [**802.11b**](javascript://) | Up to 11 Mbps | Experiences interference from cordless phones and microwaves. |
| [**802.11g**](javascript://) | Up to 54 Mbps | Compatible with and has replaced 802.11b. |
| [**802.11n**](javascript://) | Up to 600 Mbps | Uses [**multiple input/multiple output (MIMO)**](javascript://), which means an access point can have up to four antennas to improve performance. |
| [**802.11ac**](javascript://) | Theoretically up to 7 Gbps, but currently at 1.3 Gbps | Supports up to eight antennas and supports [**beamforming**](javascript://), which detects the locations of connected devices and increases signal strength in those directions. |
| 802.11ad | Up to 7 Gbps | This throughput can only be achieved when the device is within 3.3 m of the access point. |

Enlarge Table

**Notes**

Pending Wi-Fi standards include 802.11 ax, which is designed to improve performance in highly populated areas, and 802.11 ay, which is expected to achieve maximum throughput of 20 Gbps and extend the range of 802.11 ad. Approval of both standards is expected in 2019.

Currently, cable Internet and DSL are the two most popular ways to make an Internet connection for a home network. Let’s first compare these two technologies and then we’ll look at fiber-optic dedicated lines, satellite, dial-up, and cellular WAN connections.

**A+ Exam Tip**

The A+ Core 1 exam expects you to be able to compare these network types used for Internet connections: cable, DSL, dial-up, fiber, satellite, ISDN, and cellular (tethering and mobile hotspot).

### Compare Cable Internet and DSL

Here are the important facts about cable Internet and DSL:

* [**Cable Internet**](javascript://) is a broadband technology that uses cable TV lines and is always connected (always up). With cable Internet, the TV signal to your television and the data signals to your computer or LAN share the same **coaxial (coax) cable**, an older cable form that is rarely used today in a local area network. The [**cable modem**](javascript://) converts a computer’s digital signals to analog when sending them and converts incoming analog data to digital.

* **[DSL (Digital Subscriber Line)](javascript://)** is a group of broadband technologies that covers a wide range of speeds. DSL uses ordinary copper phone lines and a range of frequencies on the copper wire that are not used by voice, making it possible for you to use the same phone line for voice and DSL at the same time. When you make a regular phone call, you dial in as usual. However, the DSL part of the line is always connected (always up) for most DSL services.

When deciding between cable Internet and DSL, consider these points:

* Both cable Internet and DSL can sometimes be purchased on a sliding scale, depending on the bandwidth you want to buy. Subscriptions offer residential and more expensive business plans. Business plans are likely to have increased bandwidth and better support when problems arise.
* With cable Internet, you share the TV cable infrastructure with your neighbors, which can result in service becoming degraded if many people in your neighborhood are using cable Internet at the same time. With DSL, you’re using a dedicated phone line, so your neighbors’ surfing habits are not important.
* With DSL, static over phone lines in your house can be a problem. The DSL company provides filters to install at each phone jack (see [Figure 7-2](javascript://)), but still the problem might not be fully solved. Also, your phone line must qualify for DSL; some lines are too dirty (too much static or noise) to support DSL. [Figure 7-3](javascript://) shows a [**DSL modem**](javascript://) that can connect directly to a computer or to a router on your network.

**Figure 7-2**

When DSL is used in your home, filters are needed on every phone jack except the one used by the DSL modem



**Figure 7-3**

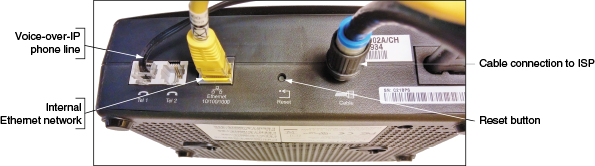
This DSL modem connects to a phone jack and a computer or router to provide a broadband connection to an ISP



* Both cable and DSL connections typically require a modem device at the entry to your SOHO network. Although you might be able to find the modem’s default login instructions online, you’ll likely never have to change any settings on the modem itself. Configuring a DSL or cable modem consists of plugging the correct cables into the correct ports. For example, [Figure 7-4](javascript://) shows a cable modem with the ISP cable connected on the right. The yellow Ethernet cable connects to the local network, and a phone line is plugged into the Voice-over-IP (VoIP) phone service provided by the ISP over the Internet. Also notice the Reset button in the figure, which you can use to reset a modem to its factory default settings. When troubleshooting a modem, try rebooting it first, and only use the reset as a last resort.

**Figure 7-4**

Use a cable modem to connect the ISP’s coaxial cable to the LAN’s Ethernet cable



Enlarge Image

### Dedicated Line Using Fiber Optic

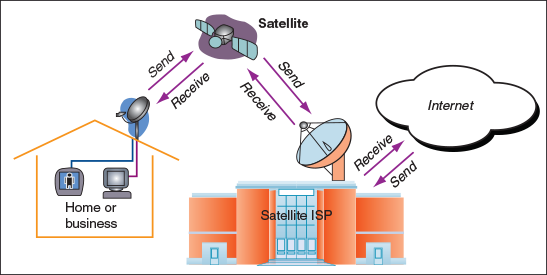
Another broadband technology used for Internet access is [**fiber optic**](javascript://). The technology connects a dedicated line from your ISP to your place of business or residence. This dedicated line is called a point-to-point (PTP) connection because no other business or residence shares the line with you. Television, Internet data, and voice communication all share the broadband [**fiber-optic cable**](javascript://), which reaches all the way from the ISP to your home. Alternatively, the provider might install fiber-optic cabling up to your neighborhood and then run coaxial cable (similar to that used in cable Internet connections) for the last leg of the connection to your business or residence. Upstream and downstream speeds and prices vary.

### Satellite

People who live in remote areas and want high-speed Internet connections often have limited choices. DSL and cable options might not be available where they live, but satellite access is available from pretty much anywhere. Internet access by satellite is available even on airplanes. Passengers can connect to the Internet using a wireless hotspot and satellite dish on the plane. A satellite dish mounted on top of your house or office building communicates with a satellite used by an ISP offering the satellite service (see [Figure 7-5](javascript://)). One disadvantage of satellite is that it requires [**line-of-sight wireless connectivity**](javascript://) without obstruction from mountains, trees, and tall buildings. Another disadvantage is that it experiences higher delays in transmission (called latency), especially when uploading, and is therefore not a good solution for an Internet connection that will be used for videoconferencing or voice over Internet.

**Figure 7-5**

Communication by satellite can include television and Internet access



### Dial-up

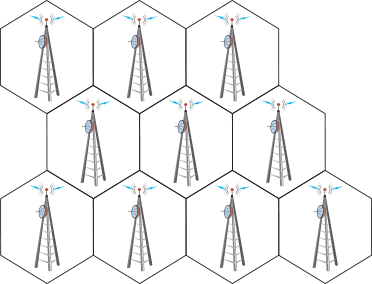
Of all the types of networking connections, dial-up or POTS (plain old telephone service) is the least expensive and slowest connection to the Internet. Dial-up connections are painfully slow, but you might still need them when traveling, and they’re good at home when your broadband connection is down.

### Cellular WAN

A [**wireless wide area network (WWAN)**](javascript://), also called a **cellular network** or cellular WAN because it consists of cells, is provided by companies such as Verizon and AT&T. Each cell is controlled by a base station (see [Figure 7-6](javascript://)), which might include more than one transceiver and antenna on the same tower to support various technologies for both voice and data transmission. Two established cellular technologies are GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access). In the United States, Sprint and Verizon use CDMA, while AT&T and T-Mobile—along with most of the rest of the world—use GSM. [**Long Term Evolution (LTE)**](javascript://) and Voice over LTE (VoLTE) provide both data and voice transmissions and are expected to ultimately replace both GSM and CDMA.

**Figure 7-6**

A cellular WAN is made up of many cells that provide coverage over a wide area



Cellular devices that use GSM or LTE require a [**SIM (Subscriber Identification Module) card**](javascript://) to be installed in the device; the card contains the information that identifies your device to the carrier (see [Figure 7-7](javascript://)). CDMA networks don’t require SIM cards unless they also use LTE. Most carriers today use a combination of GSM and LTE or CDMA and LTE.

**Figure 7-7**

A SIM card contains proof that your device can use a cellular network



Enlarge Image

Most smartphones are linked by the manufacturer to a specific cellular provider and will need to be validated on that provider’s network to connect to it. To connect a computer using mobile broadband to a cellular network, you need the hardware and software to connect and, for most networks, a SIM card. Here are your options for software and hardware devices that can connect to a cellular network, and general steps for how to create each connection. Keep in mind that when you purchase any of these devices from a carrier or manufacturer, detailed instructions are most likely included for connecting to the cellular network.

* **Embedded mobile broadband modem**. A laptop or other mobile device might have an embedded broadband modem. In this situation, you still need to subscribe to a carrier. If a SIM card is required, insert the card in the device. For some laptops, the card slot might be in the battery bay, and you must remove the battery to find the slot. Then use a setting or application installed on the device to connect to the cellular network.
* **Cell phone tethering**. You can [**tether**](javascript://) your computer or another device to your cell phone. The cell phone connects to the cellular network and provides communication to the tethered device. To use your phone for tethering, your carrier contract must allow it. The phone and other device can connect by way of a USB cable (see [Figure 7-8](javascript://)), a proprietary cable provided by your cell phone manufacturer, or a Bluetooth or Wi-Fi wireless connection. Your carrier is likely to provide you software to make the connection, or the setting might be embedded in the phone’s OS. If software is provided, install the software first and then use the software to make the connection. Otherwise, enable the tether in your phone’s OS.

**Figure 7-8**

Tether your laptop to your cell phone using a USB cable



* **USB broadband modem**. For any computer, you can use a USB broadband modem (sometimes called an air card), such as the one shown in [Figure 7-9](javascript://). The device requires a contract with a cellular carrier. If needed when using a USB broadband modem, insert the SIM card in the modem (see [Figure 7-10](javascript://)). When you insert the modem into a USB port, Windows finds the device, and the software stored on the device automatically installs and runs. A window provided by the software then appears and allows you to connect to the cellular network.

**Figure 7-9**

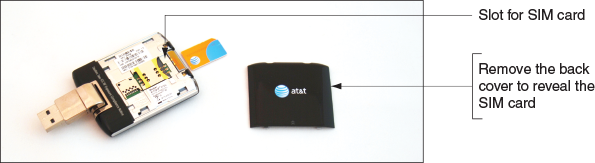
A USB broadband modem by Sierra Wireless



Enlarge Image

**Figure 7-10**

A SIM card with subscription information on it might be required to use a cellular network



Enlarge Image

* **LTE installed Internet**. Some cellular companies offer home Internet service through their cellular WAN infrastructure. Verizon calls its service LTE Internet Installed, and AT&T calls its service FWI (Fixed Wireless Internet). The ISP installs an LTE router at the home, possibly with an external antenna, which then connects wirelessly to the ISP’s cellular network. The router provides a Wi-Fi hotspot as well as a few Ethernet ports for wired devices. Typically, the router can’t be moved to other locations like a smartphone can—it’s designed to be used only at the location where the subscription is established. Data usage caps also may apply.
* **Mobile hotspot**. Some mobile devices can create a [**mobile hotspot**](javascript://) that computers and other mobile devices can connect by Wi-Fi to your device and on to the Internet. Some cellular ISPs, such as AT&T, also offer devices dedicated to this purpose.

Now that you understand some basics about the different types of networks and methods of connecting those networks to the Internet, you’re ready to learn about different ways to connect computers to local networks.

Go to pg.

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

Application Opened

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

**7-2**Connecting a Computer to a Local Network

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

* 2.6

Explain common network configuration concepts.

* 3.2

Identify common connector types.

Connecting a laptop or desktop computer to a network is quick and easy in most situations. Here, we begin with a summary of how to connect to a wired or wireless network, and then you learn how to connect to a VPN. (In [Chapter 9](javascript://), you learn how to connect smartphones and tablets to networks.)

**A+ Core 2**

* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

**A+ Exam Tip**

The A+ Core 2 exam expects you to know which type of network connection (VPN, wired, wireless, cellular, or dial-up) is appropriate for a given scenario and to know how to make the connection.

Go to pg.

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

Application Opened

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

## 7-2aConnecting to an Ethernet Wired or Wi-Fi Wireless Local Network

**A+ Core 1**

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

* 3.2

Identify common connector types.

To connect a computer to a network using an Ethernet wired or Wi-Fi wireless connection, follow these steps:

1. In general, before you connect to any network, the network adapter and its drivers must be installed and Device Manager should report no errors.

**A+ Core 2**

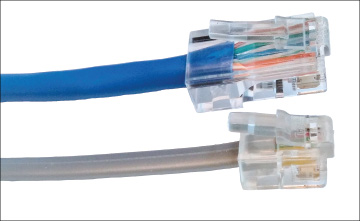
* + 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

1. Do one of the following to connect to the network:
   * For a wired network, plug in the network cable to the Ethernet port. The port is also called an [**RJ-45**](javascript://) port and looks like a large phone jack. An RJ-45 connector looks similar to an RJ-11 connector, only larger (see [Figure 7-11](javascript://)). Indicator lights near the network port should light up to indicate connectivity and activity. For Ethernet, Windows should automatically configure the connection.

**Figure 7-11**

RJ-45 and RJ-11 connectors



* + For a wireless network, click the **Network** icon in the taskbar on the desktop and select a wireless network. Click **Connect**. If the network is secured, you must enter the security key to the wireless network to connect.

1. If this is the first time you’ve connected to a local network, you’ll be asked if you want to make the PC discoverable. For private networks (such as your home or business), click **Yes**, and for public networks (such as a coffee shop hotspot), click **No**.
2. Open your browser and make sure you can access the web. For wireless connections, some hotspots provide an initial page called a captive portal, where you must enter a code or agree to the terms of use before you can use the network. On a private network, open File Explorer or Windows Explorer and drill down into the Network group to verify that network resources are available (see [Figure 7-12](javascript://)).

**Figure 7-12**

File Explorer shows resources on the network



Enlarge Image

**Notes**

For a private corporate or enterprise network, Windows Server or Microsoft Azure is likely to manage access to the network using a Windows domain. You must sign in to the Windows domain with a user name and password. Press **Ctrl+Alt+Del** to access the sign-on screen. The user name might be text such as Jane Smith or an email address such as [JSmith@mycompany.com](http://JSmith@mycompany.com/" \t "_blank). You learn more about private networks, public networks, and Windows domains in [Chapter 11](javascript://).

To view and change network security settings in Windows 10, open the Settings app and click **Network & Internet**. Click **Change connection properties**, and then select either **Public** or **Private**.

**OS Differences**

To verify or change security settings in Windows 8, click the **Settings** charm and click **Change PC settings**. On the PC settings screen, click **Network**. On the Network screen, if necessary, click **Connections**. To set the network security to Private, turn on **Find devices and content**. To set the network security to Public, turn this setting off.

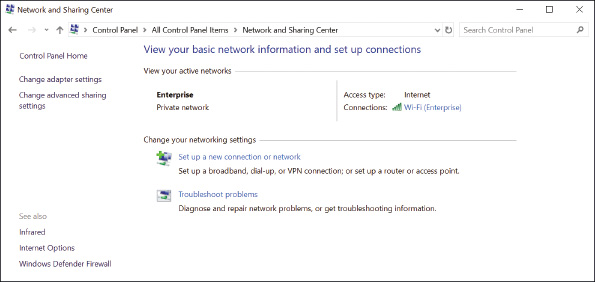
In Windows 7, open the **Network and Sharing Center** window. If the network location is **Home network** or **Work network**, click it. The Set Network Location box appears. Select a network type and click **Close**.

For wireless connections, you can view the status of the connection, including the security key used to make the connection. Do the following:

1. Open **Control Panel** and open the **Network and Sharing Center**. Alternately, you can right-click the **Network** icon in the desktop taskbar in Windows 10 and click **Open Network & Internet settings**, which opens the Network & Internet group in the Settings app. In Windows 8/7, click **Open Network****and Sharing Center**. In the Network and Sharing Center (see [Figure 7-13](javascript://)), click **Change adapter settings**, or in the Network & Internet window, click **Change adapter options**. The Network Connections window appears (see [Figure 7-14](javascript://)).

**Figure 7-13**

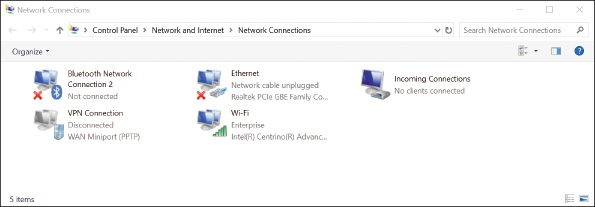
The Network and Sharing Center reports a healthy wireless network connection



Enlarge Image

**Figure 7-14**

The Network Connections window can be used to repair broken connections



Enlarge Image

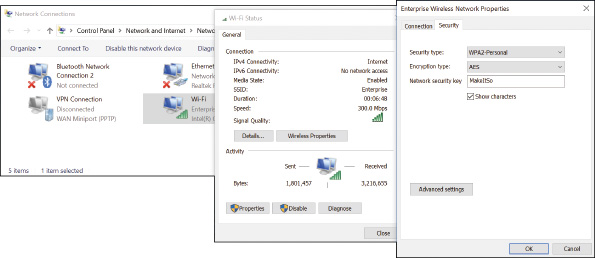
**Notes**

For Windows 10, a shortcut to open the Network & Internet window in the Settings app is to press **Win+X** and click **Network Connections.** For Windows 8, the same shortcut will open the Network Connections window.

1. In the Network Connections window, right-click the **Wi-Fi** connection and click **Status**. In the Wi-Fi Status box (see [Figure 7-15](javascript://)), click **Wireless Properties**. In the Wireless Network Properties box, select the **Security** tab. To view the security key, check **Show characters**. You can also see the security and encryption types that Windows automatically detected and applied when it made the connection.

**Figure 7-15**

Verify that the Network security key for the wireless network is correct

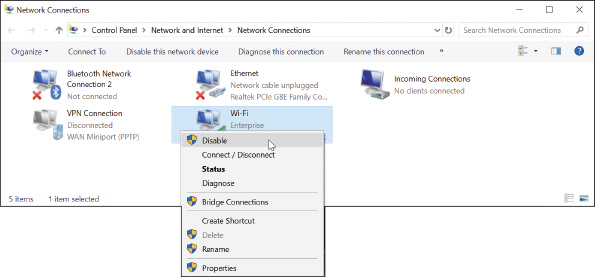


Enlarge Image

If you have a problem making a network connection, you can reset the connection. Open the Network Connections window and right-click the network connection. Select **Disable** from the shortcut menu, as shown in [Figure 7-16](javascript://). Right-click the connection again and select **Enable**. The connection is reset. Try again to browse the web or access resources on the network. If you still don’t have local or Internet access, it’s time to dig a little deeper into the source of the problem. More network troubleshooting tools and solutions are covered later in this chapter.

**Figure 7-16**

To repair a connection, disable and then enable the connection



Enlarge Image

Go to pg.

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

Application Opened

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

## 7-2bCreating a VPN Connection

**A+ Core 1**

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

* 2.6

Explain common network configuration concepts.

**A+ Core 2**

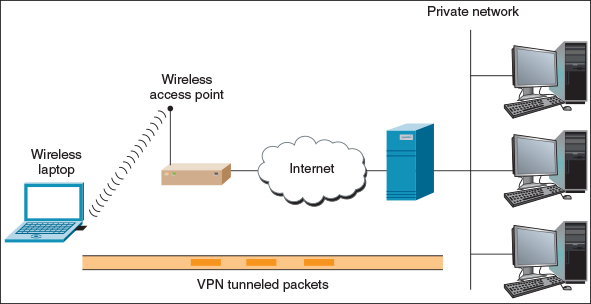
* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

A [**virtual private network (VPN)**](javascript://) is often used by telecommuting employees to connect to the corporate network by way of the Internet. A VPN protects data by encrypting it from the time it leaves the remote computer until it reaches a server on the corporate network, and vice versa. The encryption technique is called a tunnel or tunneling (see [Figure 7-17](javascript://)).

**Figure 7-17**

With a VPN, tunneling is used to send encrypted data over wired and wireless networks and the Internet



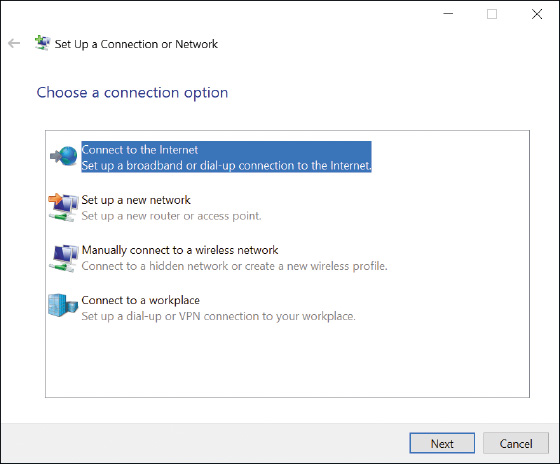
A VPN can be managed by operating systems, routers, or third-party software such as OpenVPN ([openvpn.net](http://openvpn.net/" \t "_blank)). A VPN connection is a virtual connection, which means you are setting up the tunnel over an existing connection to the Internet. When creating a VPN connection on a personal computer, always follow directions given by the network administrator who hosts the VPN. The company website might provide VPN client software to download and install on your computer. Then you might be expected to double-click a configuration file to complete the VPN connection. OpenVPN uses an .ovpn file for this purpose.

Here are the general steps using Windows to connect to a VPN:

1. In the Network and Sharing Center (refer back to [Figure 7-13](javascript://)), click **Set up a new connection or network**. Then select **Connect to a workplace - Set up a dial-up or VPN connection to your workplace** (see [Figure 7-18](javascript://)) and click **Next**.

**Figure 7-18**

Create a dial-up connection to an ISP



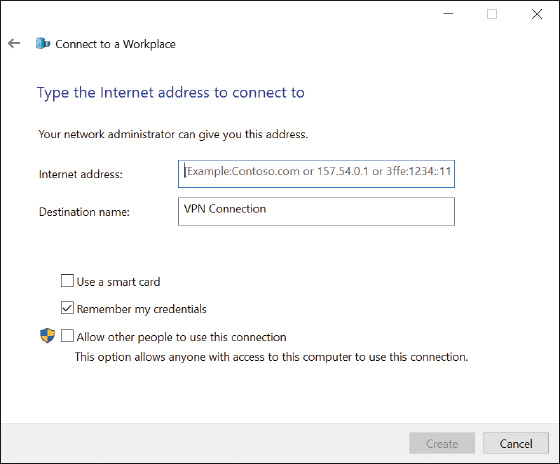
**Notes**

In Windows 10, you can accomplish the first part of this step in the Settings app. Open the Network & Internet group in the Settings app, click **Dial-up**, and then click **Set up a new connection**. The dialog box shown in [Figure 7-18](javascript://) appears.

1. In the Connect to a Workplace dialog box, click **Use my Internet connection (VPN)**. In the next dialog box, enter the IP address or domain name of the network (see [Figure 7-19](javascript://)). Your network administrator can provide this information. Name the VPN connection and click **Create**.

**Figure 7-19**

Enter connection information to the VPN



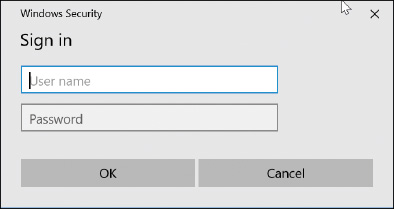
**OS Differences**

Windows 10/8 requires you to enter your user name and password at the time you connect to a VPN. Windows 7 gives you the option to enter this information when you set up the VPN or as you connect to it.

Whenever you want to use the VPN connection, click the **Network** icon in the taskbar. In the list of available networks, click the **VPN connection** and click **Connect**. Enter your user name and password (see [Figure 7-20](javascript://)) and click **OK**. Your user name and password are likely to be the same network ID and password to your user account on the Windows domain on the corporate network.

**Figure 7-20**

Enter your user name and password to connect to your VPN

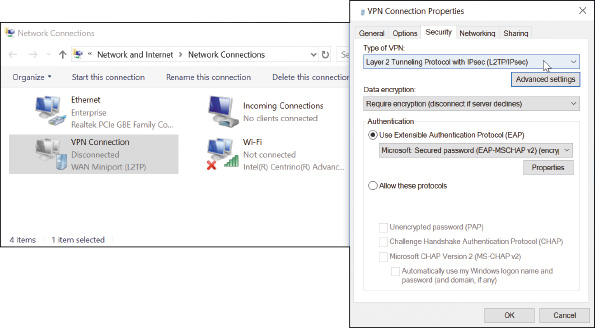


After the connection is made, you can use your browser to access the corporate secured intranet websites or other resources. The resources you can access depend on the permissions assigned to your user account.

Problems connecting to a VPN can be caused by the wrong authentication protocols used when passing the user name and password to the VPN. To configure these settings, return to the Network and Sharing Center and click **Change adapter settings**. In the Network Connections window, right-click **VPN Connection** and click **Properties**. In the Properties box, select the **Security** tab (see [Figure 7-21](javascript://)). Here you can select security settings for the type of VPN, encryption requirements, and authentication protocols given to you by the network administrator.

**Figure 7-21**

Configure the VPN’s security settings



Enlarge Image

Go to pg.

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

Application Opened

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

## 7-2cCreating a Dial-Up Connection

Here are the bare-bones steps you need to set up and support a dial-up connection:

1. Install an internal or external dial-up modem in your computer. Make sure Device Manager recognizes the card without errors.
2. Plug the phone line into the dial-up modem port on your computer and into the wall jack. Phone lines use **RJ-11** connectors (RJ stands for registered jack), which are the same connectors used for wired telephones.
3. Open the **Network and Sharing Center** window. In Windows 10/8/7, open the Control Panel and click **Network and Sharing Center**.

**A+ Exam Tip**

Windows 10 includes many options for accessing the Network and Sharing Center, and the A+ Core 2 exam expects you to be familiar with multiple methods for accessing any of the common utilities. One of the quickest ways to get to the Network and Sharing Center is to right-click **Start**, click **Network Connections**, then click **Network and Sharing Center**.

1. In the Network and Sharing Center window, click **Set up a new connection or network**. In the dialog box that appears (refer back to [Figure 7-18](javascript://)), select **Connect to the Internet - Set up a broadband or dial-up connection to the Internet** and click **Next**.
2. In the next dialog box, click **Dial-up**. In the next box (see [Figure 7-22](javascript://)), enter the phone number to your ISP, your ISP user name and password, and the name you decide to give the dial-up connection. Then click **Create**.

**Figure 7-22**

Enter a phone number and account information to your ISP

Graphical user interface, text, application, email

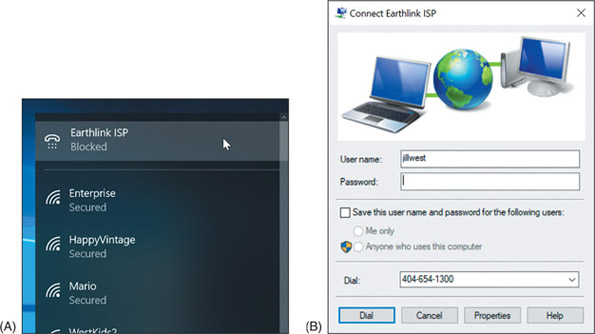
Description automatically generated

Enlarge Image

To use the connection, click your **Network** icon in the taskbar. In the list of available connections, select your dial-up connection (see [Figure 7-23A](javascript://)). In Windows 10, this opens the Dial-up page in the Settings app, where you click the dial-up connection again and click **Connect**. In Windows 8/7, click **Connect**. The Connect dialog box appears, where you can enter your password (see [Figure 7-23B](javascript://)). Click **Dial**. You will hear the modem dial the ISP and make the connection.

**Figure 7-23**

(A) Select your dial-up connection, and (B) enter the password to your ISP



Enlarge Image

If the dial-up connection won’t work, here are some things you can try:

* Is the phone line working? Plug in a regular phone and check for a dial tone. Is the phone cord securely connected to the computer and the wall jack?
* Does the modem work? Check Device Manager for reported errors about the modem. Does the modem work when making a call to another phone number (not your ISP)?
* Check the Dial-up Connection Properties box for errors. To do so, click **Change adapter settings** in the Network and Sharing Center, and then right-click the dial-up connection and select **Properties** from the shortcut menu. Is the phone number correct? Has a 1 been added in front of the number by mistake? Does the number need to start with a 9 to get an outside line? If you need to add a 9, you can put a comma in the field (for example, “9,4045661200”), which causes a slight pause after the 9 is dialed.
* Try dialing the number manually from a phone. Do you hear beeps on the other end? Try another phone number.
* When you try to connect, do you hear the number being dialed? If so, the problem is most likely with the phone number, the phone line, or the user name and password.
* Try removing and reinstalling the dial-up connection.

Now let’s turn our attention to how to configure settings for a network connection, including dynamic, static, and alternate address configurations.

Go to pg.

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

Application Opened

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

## 7-2dDynamic and Static IP Configurations

**A+ Core 1**

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

Computers use IP addresses to find each other on a network. An [**IP address**](javascript://) is assigned to a network connection when the connection is first made and can be:

* A 32-bit string, written as four decimal numbers called octets and separated by periods, such as 192.168.100.4

**A+ Core 2**

* + 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

* A 128-bit string, written as eight hexadecimal numbers separated by colons, such as 2001:0000:B80:0000:0000:D3:9C5A:CC

Most networks use 32-bit IP addresses, which are defined by [**IPv4 (Internet Protocol version 4)**](javascript://). Some networks use both 32-bit addresses and 128-bit addresses, which are defined by [**IPv6 (Internet Protocol version 6)**](javascript://).

**Notes**

The suite of rules that define network communication is called [**TCP/IP (Transmission Control Protocol/Internet Protocol)**](javascript://). IP (Internet Protocol) is a set of rules for IP addressing. IPv4 is an earlier version of IP, and IPv6 is the latest version. A **protocol** is a set of rules computers must follow in order to communicate.

A [**host**](javascript://) is any device, such as a desktop computer, laptop, or printer, on a network that requests or serves up data or services to other devices. To communicate on a network or the Internet, a host needs this TCP/IP information:

* Its own IP address—for example, 192.168.100.4.
* A [**subnet mask**](javascript://), which is four decimal numbers separated by periods—for example, 255.255.255.0. When a computer wants to send a message to a destination computer, it uses its subnet mask to decide whether the destination computer is on its own network or another network.
* The IP address of a [**default gateway**](javascript://). Computers can communicate directly with each other on the same network. However, when a computer sends a message to a computer on a different network, it sends the message to its default gateway, which is connected to the local network and at least one other network. The gateway sends the message on its way to other networks. For small businesses and homes, the default gateway is a router.
* The IP addresses of one or more [**DNS (Domain Name System or Domain Name Service) servers**](javascript://). Computers use IP addresses to communicate, but people use computer names, such as www.cengage.com, to address a computer. When you enter www.cengage.com in your browser address box, your computer must find the IP address of the www.cengage.com web server and does so by querying a DNS server. DNS servers can access databases spread all over the Internet that maintain lists of computer names (such as www.cengage.com) and their IP address assignments. This group of databases is called the Internet namespace and finding the IP address for a computer name is called [**name resolution**](javascript://). In the Internet namespace, cengage.com is the name of the Cengage domain and www.cengage.com is the name of a web server in that domain. You’ll learn more about these concepts in [Chapter 8](javascript://).

The IP address, subnet mask, default gateway, and DNS server addresses can be manually assigned to a computer’s network connection; the computer’s IP address is called a [**static IP address**](javascript://). Alternately, all of this information can be requested from a server on the network when a computer first connects to the network. The IP address it receives is called a [**dynamic IP address**](javascript://), and the server that assigns the address from a pool of addresses it maintains is called a [**DHCP (Dynamic Host Configuration Protocol) server**](javascript://). A computer or other device (such as a network printer) that requests address information from a DHCP server is called a [**DHCP client**](javascript://). It is said that the client is leasing an IP address. A DHCP server that serves up IPv6 addresses is often called a [**DHCPv6 server**](javascript://). You’ll learn more about DHCP in [Chapter 8](javascript://).

**A+ Exam Tip**

The A+ Core 1 exam expects you to know what a DHCP server is and may give you a scenario that requires you to use static and dynamic IP addressing.

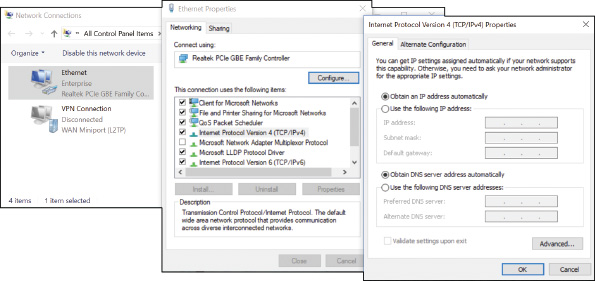
Most networks use dynamic IP addressing. By default, Windows requests dynamic IP configuration from the DHCP server and there is nothing for you to configure. In some situations, however, a computer must have a static IP address, so as an IT support technician, you need to know how to configure static IP addressing.

Follow these steps to configure static IP addressing:

1. Open the **Network Connections** window. Right-click the network connection and click **Properties**. In the Properties box on the **Networking** tab (as shown in the middle box of [Figure 7-24](javascript://)), select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. The TCP/IPv4 Properties box appears (see the right side of [Figure 7-24](javascript://)).

**Figure 7-24**

Configure TCP/IPv4 for static or dynamic addressing



Enlarge Image

1. By default, dynamic IP addressing is used, which selects Obtain an IP address automatically and Obtain DNS server address automatically. To change the settings to static IP addressing, select **Use the following IP address**. Then enter the IP address, subnet mask, and default gateway.
2. If your network administrator has given you the IP addresses of DNS servers, select **Use the following DNS server addresses** and enter up to two IP addresses. If you have additional DNS IP addresses, click **Advanced** and enter them on the **DNS** tab of the Advanced TCP/IP Settings box.

**Notes**

As an IT support technician, it’s unlikely you’ll ever be called on to configure static IPv6 addressing. However, to do so, use the Ethernet Properties box in the middle of [Figure 7-24](javascript://). Select **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**.

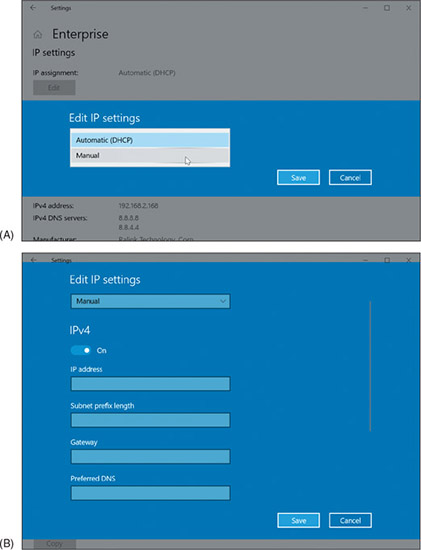
You can also uncheck **Internet Protocol Version 6 (TCP/IPv6)** to disable it. For most situations, you need to leave it enabled. A bug in Windows 7 might prevent you from joining a homegroup if IPv6 is disabled. You’ll learn more about IPv6 in [Chapter 8](javascript://).

**Notes**

In Windows 10, you can use the Settings app to configure static IP addressing. On the Status page in the Network & Internet group, click **Change connection properties**. Scroll down and click **Edit** under IP settings. Automatic (DHCP) is the default setting (see [Figure 7-25A](javascript://)). To enter static IP address information, click **Manual**. In the Edit IP settings box (see [Figure 7-25B](javascript://)), turn on IPv4 and enter the information.

**Figure 7-25**

Set static IP addressing information in the Settings app



Enlarge Image

Go to pg.

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

Application Opened

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

## 7-2eAlternate IP Address Configuration

**A+ Core 1**

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

**A+ Core 2**

* 1.8

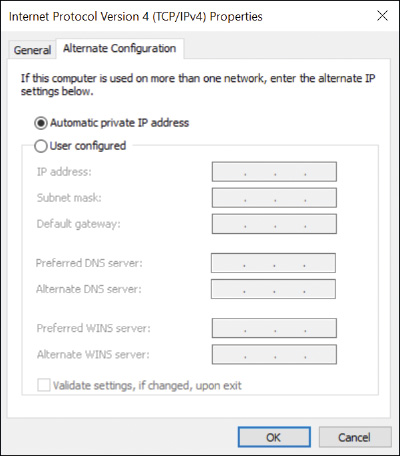
Given a scenario, configure Microsoft Windows networking on a client/desktop.

Suppose an employee with a laptop often travels, and her work network uses static IP addressing, even though most public networks use dynamic IP addressing. How do you configure her computer’s network connection settings? For travel, you would configure the computer to use dynamic IP addressing in order to connect to public networks. However, when the computer attempts to connect to the corporate network, it needs a static IP address. The solution is to create an alternate configuration that the computer will use only if needed.

To create an alternate configuration, first use the General tab of the TCP/IPv4 Properties box shown earlier in [Figure 7-24](javascript://) to set the configuration for dynamic IP addressing. Then click the **Alternate Configuration** tab. As you can see in [Figure 7-26](javascript://), by default Windows sets an [**Automatic private IP address (APIPA)**](javascript://), which is an IP address beginning with 169.254, when it cannot find a DHCP server. Select **User configured**. Then enter a static IP address, subnet mask, default gateway, and DNS server addresses for the alternate configuration to be used on the company network. Click **OK** and close all boxes. Now the computer will first attempt to gather network connection settings from a DHCP server. If a DHCP server is not available on the network, the computer will instead use the new static IP settings you just entered.

**Figure 7-26**

Create an alternate static IP address configuration



**A+ Exam Tip**

The A+ Core 2 exam expects you to know in a scenario when it is appropriate to configure an alternate IP address, including setting the static IP address, subnet mask, DNS addresses, and gateway address.

Go to pg.

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

Application Opened

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

## 7-2fManaging Network Adapters

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

**A+ Core 2**

* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

A computer makes a wired or wireless connection to a local network by way of a network adapter, which might be a network port embedded on the motherboard or a [**network interface card (NIC)**](javascript://) installed in an expansion slot on the motherboard. In addition, the adapter might be an external device plugged into a USB port (see [Figure 7-27](javascript://)). A network adapter is often called a network interface card or NIC even when it’s not really a card but a USB device or a device embedded on the motherboard. It might also be called a network controller or network adapter.

**Figure 7-27**

USB devices provide wired and wireless network connections



**A+ Exam Tip**

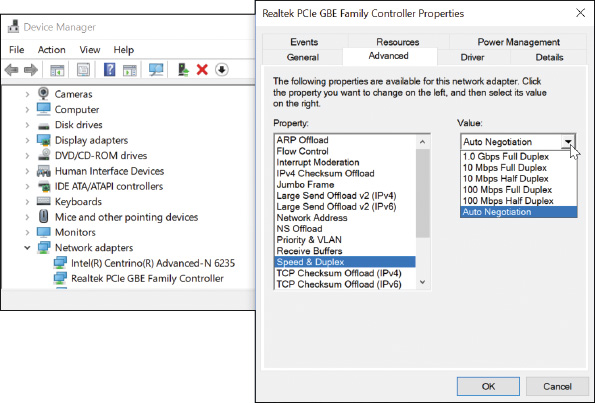
The A+ Core 2 exam expects you, when given a scenario, to be able to resolve a problem by configuring the features of a network adapter, including speed, half duplex, full duplex, Wake-on-LAN, QoS, and available BIOS/ UEFI settings for onboard NICs.

Here are a network adapter’s features you need to be aware of:

* **The drivers a NIC uses.** A NIC usually comes bundled with drivers on CD or the drivers can be downloaded from the web. Windows has several embedded NIC drivers. After you install a NIC, you install its drivers. Problems with the network adapter can sometimes be solved by using Device Manager to update the drivers or uninstall the drivers and then reinstall them.
* **Ethernet speeds.** For wired networks, the four speeds for Ethernet are 10 Mbps, 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), and 10 Gbps (10-gigabit Ethernet). Most network adapters sold today for local networks use Gigabit Ethernet and support the two slower speeds. To see the speeds a NIC supports, open its Properties box in **Device Manager**. Select the **Advanced** tab. In the list of properties, select **Speed & Duplex**. You can then see available speeds in the Value drop-down list (see the right side of [Figure 7-28](javascript://)). If the adapter connects with slower network devices on the network, the adapter works at the slower speed. Notice that the drop-down list has options for half duplex or full duplex. [**Full duplex**](javascript://) sends and receives transmissions at the same time. [**Half duplex**](javascript://) works in only one direction at a time. Select **Auto Negotiation** for Windows to use the best possible speed and duplex for a particular connection.

**Figure 7-28**

Set the speed and duplex for the network adapter



Enlarge Image

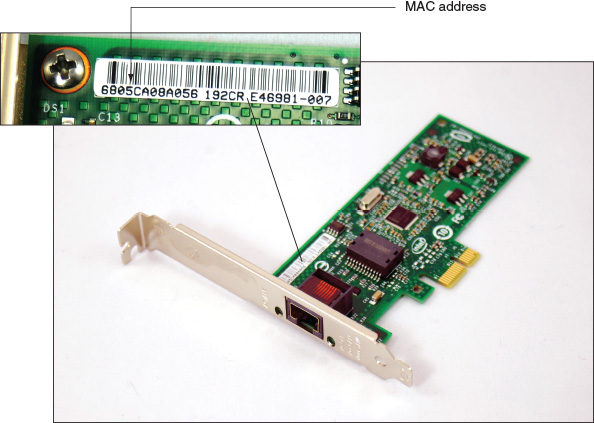
**Notes**

The speed of a network depends on the speed of each device on the network and how well a router or switch manages that traffic. SOHO network devices typically offer three speeds: Gigabit Ethernet (1000 Mbps or 1 Gbps), Fast Ethernet (100 Mbps), or Ethernet (10 Mbps). If you want your entire network to run at the fastest speed, make sure all your devices are rated for Gigabit Ethernet.

* **MAC address.** Every NIC (wired or wireless) has a 48-bit (6-byte) identification number, called the [**MAC address**](javascript://) or [**physical address**](javascript://), hard-coded on the card by its manufacturer. The MAC address is unique for that adapter and is used to identify the adapter on the local network. An example of a MAC address is 00-0C-6E-4E-AB-A5. Most likely, the MAC address is printed on the device (see [Figure 7-29](javascript://)).

**Figure 7-29**

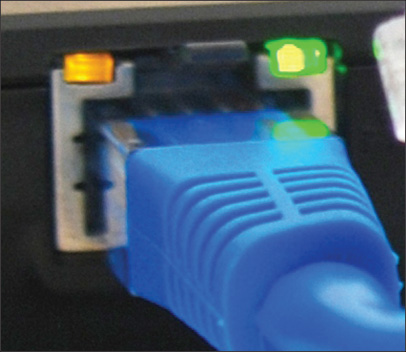
This Gigabit Ethernet adapter by Intel uses a PCIe ×1 slot



* **Status indicator lights.** A wired network adapter might provide indicator lights on the side of the RJ-45 port that indicate connectivity and activity (see [Figure 7-30](javascript://)). When you first discover you have a problem with a computer not connecting to a network, be sure to check the status indicator lights to verify that you have connectivity and activity. If not, then the problem is related to hardware. Next, check the cable connections to make sure they are solid.

**Figure 7-30**

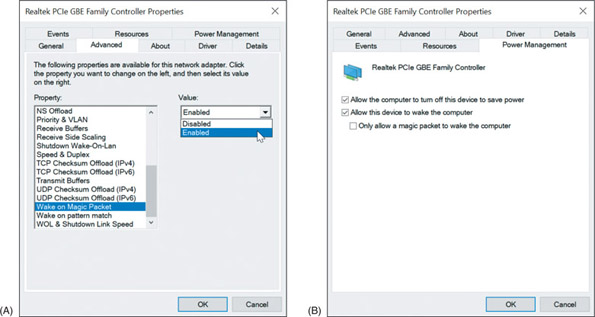
Status indicator lights for the onboard network port



* **Wake-on-LAN.** A NIC might support [**Wake-on-LAN**](javascript://), which allows it to wake up the computer when it receives certain communication on the network. To use the feature, it must be enabled on the NIC. Open the NIC’s Properties box in Device Manager and click the **Advanced** tab. Make sure **Wake on Magic Packet** and **Wake on pattern match** are both enabled (see [Figure 7-31A](javascript://)).

**Figure 7-31**

Enable Wake-on-LAN (A) using the Advanced tab, or (B) using the Power Management tab of the network adapter’s Properties box



Enlarge Image

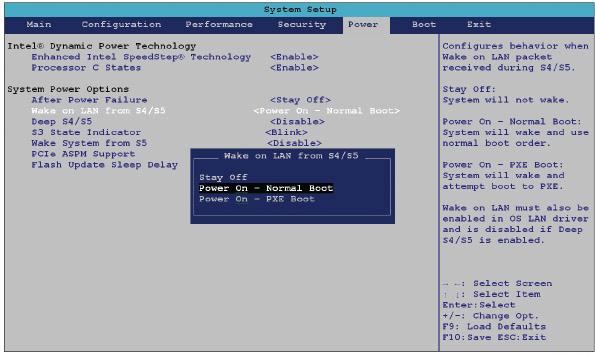
**Notes**

Some NICs provide a Power Management tab in the Properties box. To use the Power Management tab to enable Wake-on-LAN, check **Allow this device to wake the computer** (see [Figure 7-31B](javascript://)).

For an onboard NIC, you must also enable Wake-on-LAN in BIOS/UEFI setup. Reboot the computer, enter BIOS/UEFI setup, and look for the option on a power-management screen. [Figure 7-32](javascript://) shows the BIOS/UEFI screen for one onboard NIC. It is not recommended that you enable Wake-on-LAN for a wireless network adapter.

**Figure 7-32**

Use the Power screen in the BIOS/UEFI setup to enable Wake-on-LAN



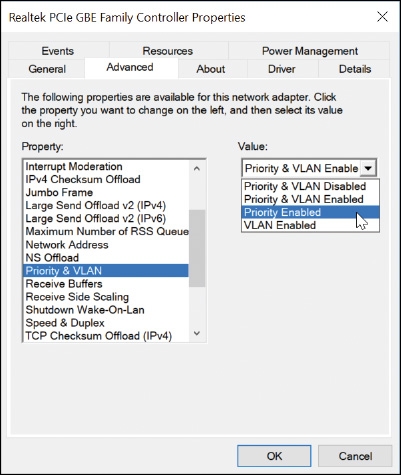
Enlarge Image

Source: Intel

* **Quality of Service (QoS).** Another feature on a network adapter is [**Quality of Service (QoS)**](javascript://), the ability to control which applications’ traffic have priority on the network. The feature must be enabled and configured on the router, enabled on the network adapters, and configured in Windows for every computer on the network that uses the high-priority applications. Later in this chapter, you learn how to configure a router to use QoS. To enable QoS on a Windows computer’s NIC, open the network adapter Properties box in Device Manager. On the Advanced tab, make sure **Priority Enabled** or **Priority & VLAN Enabled** is selected, as shown in [Figure 7-33](javascript://). If the option is not listed, the adapter does not support QoS.

**Figure 7-33**

Select Priority Enabled to allow the network adapter to support QoS on the network



**Notes**

A VLAN is a virtual LAN, and QoS is sometimes implemented using VLAN technology. You’ll learn more about VLANs when you study virtualization.

Now that you know how to connect a computer to a network, let’s look at how to set up the network itself. The process of building and maintaining a large, corporate network is outside the scope of this text. However, working with smaller networks, such as those used in homes and small businesses, helps prepare you to work in larger network environments.

Go to pg.

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

Application Opened

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

**7-3**Setting Up a Multifunction Router for a SOHO Network

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

* 2.4

Compare and contrast wireless networking protocols.

* 2.6

Explain common network configuration concepts.

An IT support technician is likely to be called on to set up a small office or home office (SOHO) network. As part of setting up a small network, you need to know how to configure a multipurpose router to stand between the network and the Internet. A [**router**](javascript://) (see [Figure 7-34](javascript://)) is a device that manages traffic between two or more networks and can help find the best path for traffic to get from one network to another.

**Figure 7-34**

A router connects the local network to the Internet



**A+ Exam Tip**

The A+ Core 1 and A+ Core 2 exams may require you to evaluate the needs of a business or residence in a given scenario and to install, configure, and secure a SOHO wired and wireless router based on these needs.

**A+ Core 2**

* 2.2

Explain logical security concepts.

* 2.3

Compare and contrast wireless security protocols and authentication methods.

* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

* 2.10

Given a scenario, configure security on SOHO wireless and wired networks.

Go to pg.

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

Application Opened

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

## 7-3aFunctions of a SOHO Router

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

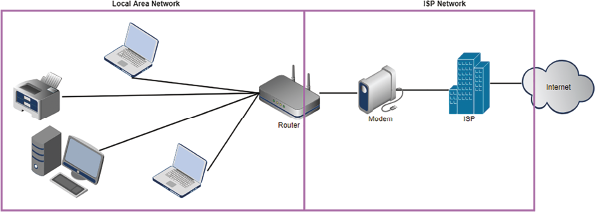
* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

Routers can range from small ones designed to manage a SOHO network that connects to an ISP (costing around $50 to $300) to those that manage multiple networks and extensive traffic (costing several thousand dollars). On a small office or home network, a router stands between the ISP network and the local network (see [Figure 7-35](javascript://)), and the router is the local network’s gateway to the Internet.

**Figure 7-35**

A router stands between a local network and the ISP network and manages traffic between them



Enlarge Image

Note in the figure that computers can connect to this router using wired or wireless connections. This is because a SOHO router often serves different functions in a single device. A typical SOHO router usually combines these functions:

* As a router, it stands between two networks—the ISP network and the local network—and routes traffic between the two networks.
* As a [**switch**](javascript://), it manages several network ports that can be connected to wired computers on the local network or to a dedicated switch that provides even more ports for locally networked computers.
* As a DHCP server, it can provide IP addresses to computers and other devices on the local network.
* As a [**wireless access point (WAP)**](javascript://), it enables wireless devices to connect to the network. These wireless connections can be secured using wireless security features.
* As a [**firewall**](javascript://), it blocks unwanted traffic from the Internet and can restrict Internet access for local devices behind the firewall. Restrictions on local devices can apply to days of the week, time of day, keywords used, certain websites, and specific applications. It can also limit network and Internet access to specified computers, based on their MAC addresses.
* If the router is used as an [**FTP (File Transfer Protocol) server**](javascript://), you can connect an external hard drive to the router, and the FTP firmware on the router can be used to share files with network users.

An example of a multifunction router is the Nighthawk AC1900 by NETGEAR, shown in [Figures 7-36](javascript://) and [7-37](javascript://). It has one Internet port for the broadband modem (cable modem or DSL modem) and four ports for devices on the network. The USB port can be used to plug in a USB external hard drive for file sharing on the network. The router is also a wireless access point with multiple antennas to increase speed and range.

**Figure 7-36**

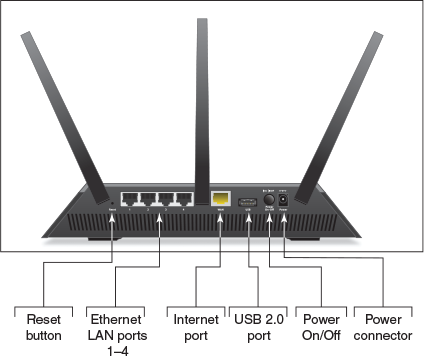
The NETGEAR Nighthawk AC1900 dual band Wi-Fi Gigabit router



Source: [Amazon.com](http://amazon.com/" \t "_blank)

**Figure 7-37**

Connections and ports on the back of the NETGEAR router



Source: NETGEAR

Go to pg.

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

Application Opened

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

## 7-3bInstalling and Configuring a Router on the Local Network

**A+ Core 1**

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

* 2.6

Explain common network configuration concepts.

**A+ Core 2**

* 2.2

Explain logical security concepts.

* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

* 2.10

Given a scenario, configure security on SOHO wireless and wired networks.

When deciding where to physically place a router, consider its physical security. If the router will be used as a wireless access point, make sure it is centrally located to create the best Wi-Fi hotspot for users. For physical security in a small business, don’t place the router in a public location, such as the lobby. For best security, place the router behind a locked door accessible only to authorized personnel in a location with access to network cabling. The indoor range for a Wi-Fi hotspot is up to 70 meters; this range is affected by many factors, including interference from walls, furniture, electrical equipment, and other nearby hotspots. For the best Wi-Fi strength, position your router or a stand-alone wireless access point in the center of where you want your hotspot, and know that a higher position (near the ceiling) works better than a lower position (on the floor).

For routers that have external antennas, raise the antennas to vertical positions. Plug in the router and connect network cables to devices on the local network. Connect the network cable from the ISP modem or other device to the uplink port on the router.

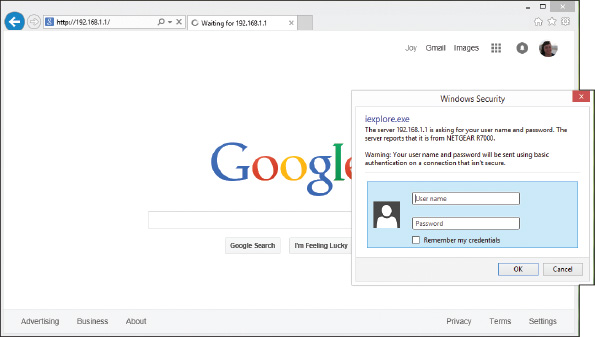
To configure a router for the first time or change its configuration, always follow the directions of the manufacturer. You can use any computer on the network that uses a wired connection (it doesn’t matter which computer) to configure the firmware on the router. You’ll need the IP address of the router and the default user name and password to the router setup. To find this information, look in the router documentation or search online for your model and brand of router.

Here are the general steps for one router, the Nighthawk AC1900 by NETGEAR, although the setup screens for your router may be different:

1. Open your browser and enter the IP address of the router in the address box. In our example, the address is 192.168.1.1. The Windows Security box appears (see [Figure 7-38](javascript://)). For our router, the default user name and password are both **admin**, although yours might be different.

**Figure 7-38**

Enter the user name and password to the router firmware utility

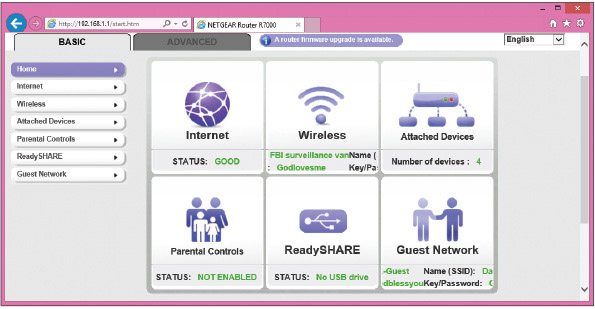


Enlarge Image

1. The main setup page of the router firmware appears in your browser window. [Figure 7-39](javascript://) shows the main page for a router that has already been configured. Notice the BASIC tab is selected. Most of the settings you’ll need are on the ADVANCED tab. Begin by poking around to see what’s available and to find the settings you need. If you make changes, be sure to save them. When finished, click **Logout** and close the browser window.

**Figure 7-39**

The main screen for router firmware setup



Enlarge Image

Source: NETGEAR

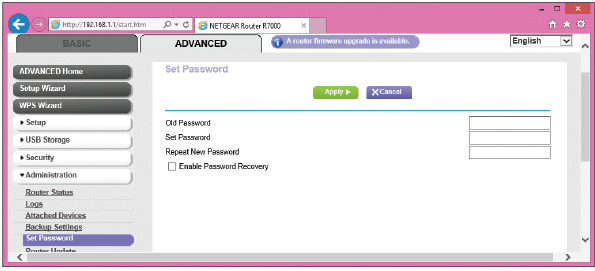
Following are some changes you might need to make to the router’s configuration. To secure your router, always change the router password, which is described next.

### Change the Router Password

It’s extremely important to protect access to your network and prevent others from hijacking your router. If you have not already done so, change the router’s default administrative password. For our router, click the **ADVANCED** tab, click **Administration**, and click **Set Password** (see [Figure 7-40](javascript://)). Change the password and click **Apply**. If the firmware offers the option, disable the ability to configure the router over the wireless network. Know that this password to configure the router firmware is different from the password needed to access the router’s wireless network.

**Figure 7-40**

Change the router firmware password



Enlarge Image

Source: NETGEAR

**Caution**

Changing the router password is especially important if the router is a wireless router. Unless you have disabled or secured the wireless access point, anyone within its range—even outside your building—can use your wireless network. If they guess the default password to the router, they can change the password to hijack your router. Also, your wireless network can be used for criminal activity. After you first install a router and before you do anything else, change your router password and disable the wireless network until you have time to set up and test the wireless security. To give even more security, change the default user name if the router utility allows that option.

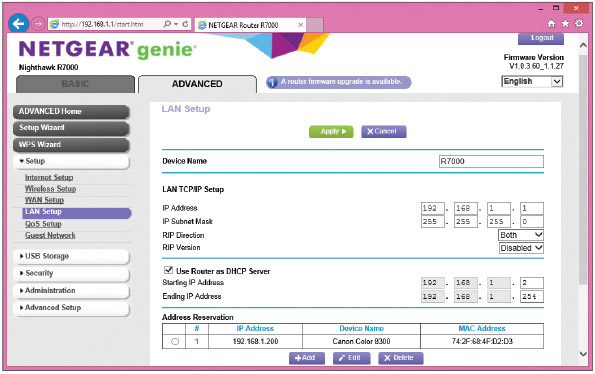
For best security, get in the habit of always changing the default administrative password for any wireless device, such as a Roku or security camera, that you might connect to a wireless network.

### Configure the DHCP Server

To configure the DHCP server for our sample router, click the **ADVANCED** tab and then click **LAN Setup** in the Setup group (see [Figure 7-41](javascript://)). On this page, you can enable or disable the DHCP server and set the IP address of the router and subnet mask for the network. For the DHCP server, set the starting and ending IP addresses, which determines the range of IP addresses DHCP can serve up. After making changes on this page, click **Apply** to save your changes.

**Figure 7-41**

Configure the DHCP server in the router firmware



Enlarge Image

Source: NETGEAR

**Notes**

As you advance in your networking skills, you’ll learn how to choose subnet masks and ranges of IP addresses to divide a large network into more manageable subnets. For now, know that if your range of IP addresses varies only in the last octet, the subnet mask is 255.255.255.0. If the range of IP addresses varies in the last two octets, the subnet mask is 255.255.0.0. You’ll learn more about subnets in [Chapter 8](javascript://).

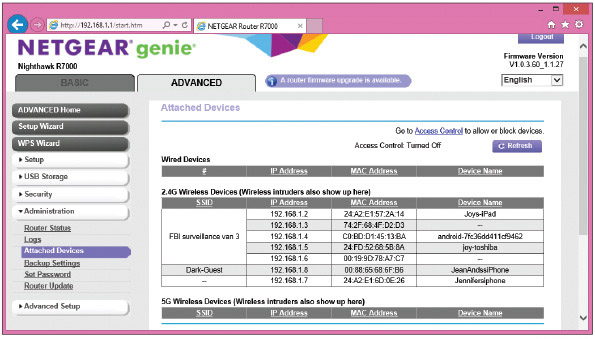
### Reserve IP Addresses

A network device such as a printer needs a consistent IP address at all times so computers that access the printer don’t need to be told its new IP address each time it reconnects to the network. In addition, a computer that is running a service, such as a web server for other computers on the network, needs a consistent IP address so that other computers can consistently find the web server. You could assign the printer and web server IP addresses by configuring the device or computer for static IP addressing. Alternately, you can assign static IP addresses to a device or computer by creating an [**address reservation**](javascript://) on the DHCP server so that the DHCP client receives the same IP address from the server every time it connects to the network. Do the following to reserve an IP address:

1. To identify the computer or printer, you’ll need its MAC address. When the client is connected to the network, click the **ADVANCED** tab and click **Attached Devices** in the Administration group (see [Figure 7-42](javascript://)). Copy the MAC address (select it and press **CTRL+C**) or write it down.

**Figure 7-42**

View the MAC addresses of devices connected to the network



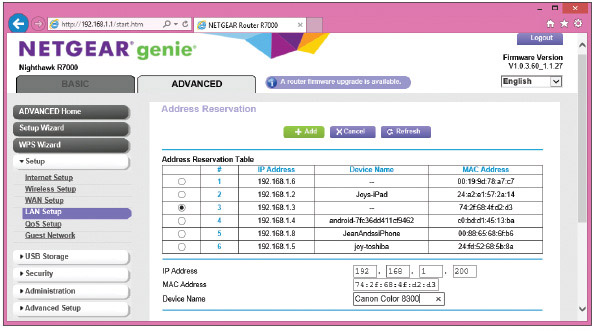
Enlarge Image

Source: NETGEAR

1. To assign a reserved IP address to the client, go to the LAN Setup page shown in [Figure 7-41](javascript://) and click **Add** under **Address Reservation**. In the IP address field, enter the IP address to assign to the computer or printer. Be sure to use an IP address in the range of IP addresses assigned by the DHCP server. Select the MAC address from the list of attached devices or copy or type the MAC address in the field. Click **Apply** to save your changes. In [Figure 7-43](javascript://), a Canon network printer is set to receive the IP address 192.168.1.200 each time it connects to the network. It’s helpful to network users to write this IP address on a label taped in plain sight on the printer or web server.

**Figure 7-43**

Use address reservation to assign a reserved IP address to a computer or other device



Enlarge Image

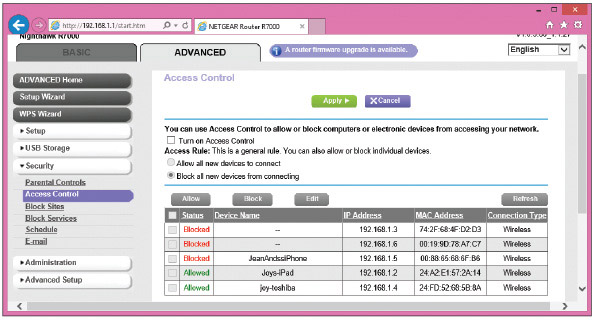
Source: NETGEAR

### MAC Address Filtering

**MAC address filtering** allows you to restrict access to your network to certain computers or devices. If a MAC address is not entered in the table of MAC addresses, the device is not allowed to connect to the network. For our sample router, the MAC address table can be viewed and edited on the ADVANCED tab of the Access Control page in the Security group (see [Figure 7-44](javascript://)). To turn on Access Control, check the **Turn on Access Control** check box and then allow or block each MAC address in the table.

**Figure 7-44**

Use MAC address filtering to allow and block devices on the network



Enlarge Image

Source: NETGEAR

**Notes**

It’s fairly easy to fake a MAC address when attacking a network. Therefore, MAC address filtering is not considered an effective security measure.

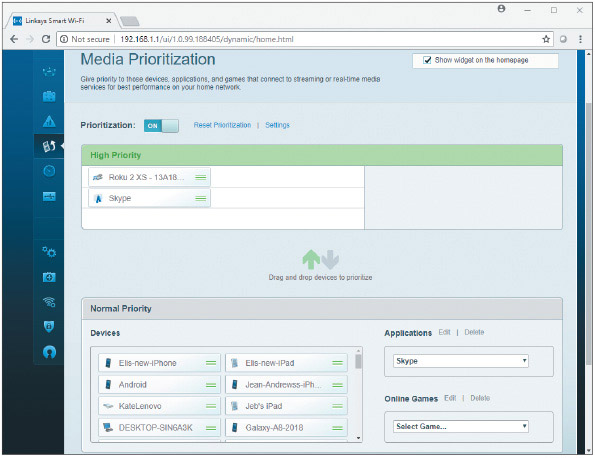
### QOS for an Application or Device

As you use your network and notice that one application or device is not getting the best service, you can improve its network performance using the Quality of Service (QoS) feature discussed earlier in this chapter. Wireless devices used for streaming multimedia (for example, a Roku) and applications used for video conferencing (for example, Skype) might need a high priority. For one sample router, do the following:

1. Sign in to the router firmware and go to the **Media Prioritization** page (see [Figure 7-45](javascript://)). Turn on **Prioritization**. Then you can drag a device into the High Priority list. You can also select an application or online game from one of the two drop-down lists on the right and drag it to the High Priority list.
2. Notice in the figure that a Roku device is listed for the highest priority, followed by the Skype application. Click **OK** to save your changes.

**Figure 7-45**

High priority is given to a device or app for best QoS



Enlarge Image

Source: Linksys

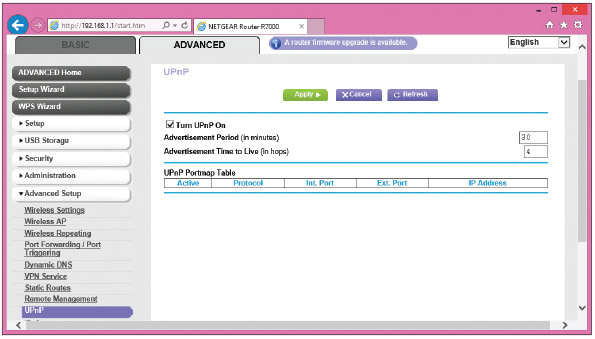
### Universal Plug and Play

[**Universal Plug and Play (UPnP)**](javascript://) helps computers on the local network automatically discover and communicate with services provided by other computers on the local network. Enable UPnP if computers on the network use applications, such as messaging, gaming, or Windows Remote Assistance, which run on other local computers and there is a problem establishing communication. Basically, a computer can use the router to advertise its service and automatically communicate with other computers on the network. UPnP is considered a security risk because shields between computers are dropped, which hackers might exploit. Therefore, use UPnP with caution.

For our sample router, UPnP is enabled on the UPnP page in the Advanced Setup group on the ADVANCED tab (see [Figure 7-46](javascript://)). Any computers and their ports that are currently using UPnP are listed.

**Figure 7-46**

Turn on UPnP



Enlarge Image

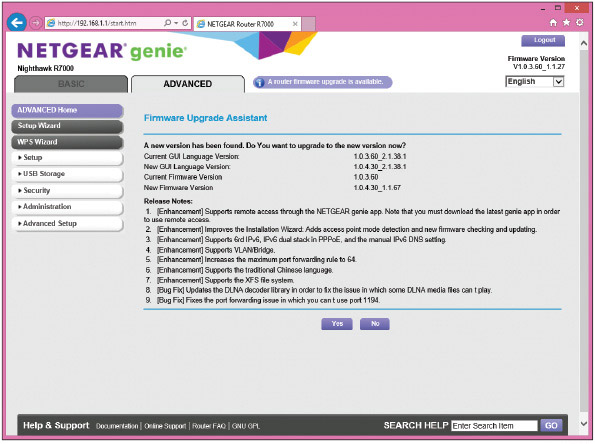
Source: NETGEAR

### Update Router Firmware

As part of maintaining a router, know that router manufacturers occasionally release updates to the router firmware. The router setup utility can be used to download and apply these updates. For our sample router, you can click **A router firmware upgrade is available** on any of the setup screens (for example, see [Figure 7-46](javascript://)) to see the Firmware Upgrade Assistant page (see [Figure 7-47](javascript://)). Use this page to perform the upgrade.

**Figure 7-47**

Update router firmware



Enlarge Image

Source: NETGEAR

Now let’s look at the concepts and steps to put up a firewall to control traffic to and from your network and the Internet. Then we’ll look at how to set up a wireless network.

Go to pg.

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

Application Opened

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

## 7-3cLimiting Internet Traffic on Your Network

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

To protect resources on the network, a router’s firewall can examine each message coming from the Internet and decide if the message is allowed onto the local network. A message is directed to a particular computer (identified by its IP address) and to a particular application running on that computer. The application is identified by a port number, also called a port or [**port address**](javascript://).

**A+ Core 2**

* 2.10

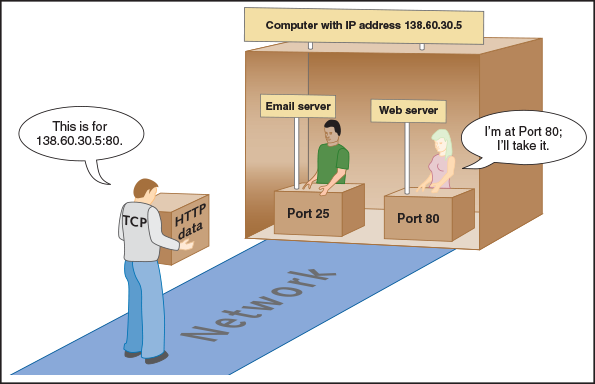
Given a scenario, configure security on SOHO wireless and wired networks.

Most applications used on the Internet or a local network are [**client/server applications**](javascript://). Client applications, such as Internet Explorer, Google Chrome, or Outlook, communicate with server applications such as a web server or email server. Each client and server application installed on a computer listens at a predetermined port that uniquely identifies the application on the computer.

Suppose a computer with an IP address of 138.60.30.5 is running an email server listening at port 25 and a web server application listening at port 80. If a client computer sends a request to 138.60.30.5:25 (IP address and port 25), the email server listening at that port responds. On the other hand, if a request is sent to 138.60.30.5:80 (IP address and port 80), the web server listening at port 80 responds (see [Figure 7-48](javascript://)). You’ll learn more about ports in [Chapter 8](javascript://), including the common port numbers used by several popular applications.

**Figure 7-48**

Each server application running on a computer is addressed by a unique port number



Enlarge Image

Routers offer the option to disable (close) all ports, which means that no activity initiated from the Internet can get in. For some routers, you must explicitly disable all ports. For the NETGEAR router in our example, all ports are disabled (closed) by default. You must specify exceptions to this firewall rule in order to allow unsolicited traffic from the Internet. Exceptions are allowed using port forwarding or a DMZ. In addition to managing ports, you can also limit Internet traffic by filtering content. All these techniques are discussed next.

**A+ Exam Tip**

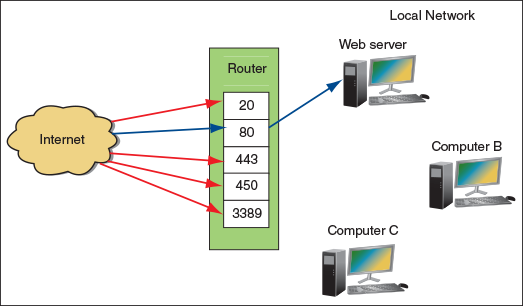
The A+ Core 1 and A+ Core 2 exams may give a scenario that expects you to resolve a problem by implementing port forwarding/mapping, whitelists, blacklists, content filtering, parental controls, and a DMZ.

### Port Forwarding

Suppose you’re hosting an Internet game or website or want to use Remote Desktop to access your home computer from the Internet. In these situations, you need to enable (open) certain ports to certain computers so that activity initiated from the Internet can get past your firewall. This technique, called [**port forwarding**](javascript://) or port mapping, means that when the firewall receives a request for communication from the Internet to the specific computer and port, the request will be allowed and forwarded to that computer on the network. The computer is defined to the router by its static IP address. For example, in [Figure 7-49](javascript://), port 80 is open and requests to port 80 are forwarded to the web server listening at that port. This one computer on the network is the only one allowed to receive requests at port 80.

**Figure 7-49**

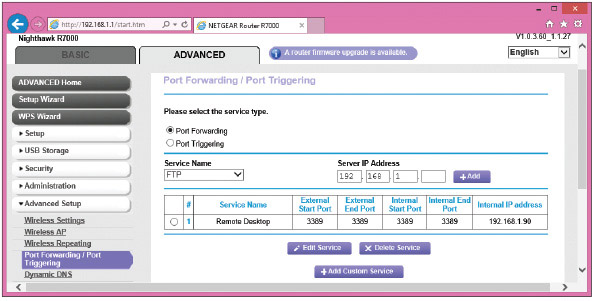
Port forwarding on a network



To configure port forwarding for our sample router, click the **ADVANCED** tab, click **Port Forwarding/Port Triggering** in the Advanced Setup group (see [Figure 7-50](javascript://)), and verify that **Port Forwarding** is selected. Select the **Service Name**, enter the static IP address of the computer providing the service in the Server IP Address field, and click **Add**. Notice in the figure that the Remote Desktop application on a device outside the network can use port forwarding to communicate with the computer whose IP address is 192.168.1.90 using port 3389. The situation is illustrated in [Figure 7-51](javascript://). This computer is set to support the Remote Desktop server application.

**Figure 7-50**

Using port forwarding, activity initiated from the Internet is allowed access to a computer on the network

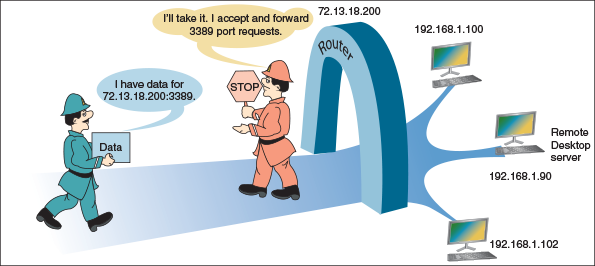


Enlarge Image

Source: NETGEAR

**Figure 7-51**

With port forwarding, a router allows messages past the firewall that are initiated outside the network



Enlarge Image

**Notes**

If you want to use a domain name rather than an IP address to access a computer on your network from the Internet, you’ll need to purchase the domain name and register it in the Internet namespace to associate it with your static IP address assigned by your ISP. Several websites on the Internet let you do both; one site is by Network Solutions at [networksolutions.com](http://networksolutions.com/" \t "_blank).

Also notice the IP address for the message in [Figure 7-51](javascript://) is directed to the router’s IP address. With port forwarding, the router forwards all traffic to port 3389 to the one computer with this open port, even through traffic is directed to the router’s IP address. Here are some tips to keep in mind when using port forwarding:

* You must lease a static IP address for your router from your ISP so that people on the Internet can find you. Most ISPs will provide you a static IP address for an additional monthly fee.
* For port forwarding to work, the computer on your network must have a static IP address so that the router knows where to send the communication.
* Using port forwarding, your computer and network are more vulnerable because you are allowing external users directly into your private network. For better security, turn on port forwarding only when you know it’s being used.

### DMZ

A [**DMZ (demilitarized zone)**](javascript://) in networking is a computer or network that is not protected by a firewall or has limited protection. You can drop all your shields protecting a computer by putting it in a DMZ, and the firewall no longer protects it. If you are having problems getting port forwarding to work, putting a computer in a DMZ can free it to receive any communication from the Internet. All unsolicited traffic from the Internet that the router would normally drop is forwarded to the computer designated as the DMZ server.

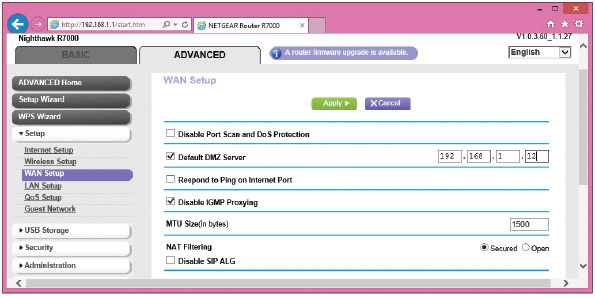
**Caution**

If a DMZ computer is compromised, it can be used to attack other computers on the network. Use it only as a last resort when you cannot get port forwarding to work. It goes without saying you should not leave the DMZ enabled unless you are using it.

To set up a DMZ server for our sample router, click the **ADVANCED** tab and select **WAN Setup** in the Setup group (see [Figure 7-52](javascript://)). Check **Default DMZ Server** and enter the static IP address of the computer.

**Figure 7-52**

Set up an unprotected DMZ server for the network



Enlarge Image

Source: NETGEAR

### Content Filtering and Parental Controls

Routers normally provide a way for employers or parents to limit the content that computers on the local network can access on the Internet. Filtering can apply to specific computers, users, websites, categories of websites, keywords, services, time of day, and day of the week. Criteria for filtering can draw from [**blacklists**](javascript://) (lists of what cannot be accessed) or [**whitelists**](javascript://) (lists of what can be accessed).

For our sample router, content filtering and parental controls are managed in the Security group on the ADVANCED tab. Here are the options:

* The Parental Controls page provides access to the Live Parental Controls application and website at [netgear.com/lpc](http://netgear.com/lpc" \t "_blank), where parents can manage content allowed from the Internet and monitor websites and content accessed.
* The Block Sites page (see [Figure 7-53](javascript://)) allows you to create a blacklist of keywords or websites to block. Notice you can also specify a trusted IP address of a computer on the network that is allowed access to this content.

**Figure 7-53**

Block sites by keyword or domain names



Enlarge Image

Source: NETGEAR

* The Block Services page can block services on the Internet. For example, you can block Internet gaming services or email services, or allow the service based on a schedule. You will need to know the ports these services use. You can also specify the IP addresses of computers to which the block applies.
* The Schedule page allows you to specify a schedule of times and days a blocked service can be used.
* The E-mail page gives you the option to have the router email you a log of router activities.

Now let’s turn our attention to configuring a wireless access point provided by a router.

Go to pg.

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

Application Opened

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

## 7-3dSetting up a Wireless Network

**A+ Core 1**

* 2.3

Given a scenario, install and configure a basic wired/wireless SOHO network.

* 2.4

Compare and contrast wireless networking protocols.

**A+ Core 2**

* 2.3

Compare and contrast wireless security protocols and authentication methods.

* 2.10

Given a scenario, configure security on SOHO wireless and wired networks.

A wireless network is created by a wireless access point. The standards for a local wireless network are called **Wi-Fi (Wireless Fidelity)**, and their technical name is IEEE 802.11. The IEEE 802.11 standards, collectively known as the 802.11 a/b/g/n/ac standards, have evolved over the years. This list details the progression of ranges and frequencies for each standard:

* **802.11a.** Short range up to 50 meters with radio frequency of 5.0 GHz
* **802.11b.** Longer range of 100 meters (indoor ranges are less than outdoor ranges) and radio frequency of 2.4 GHz
* **802.11g.** Same range and frequency as 802.11b but with faster speeds up to 54 Mbps
* **802.11n.** Can use either 5.0-GHz or 2.4-GHz radio frequency with an indoor range up to 70 meters and an outdoor range up to 250 meters
* **802.11ac.** Uses the 5.0-GHz radio frequency and has the same ranges as 802.11n, except performance stays stronger at the edges of its reach

**A+ Exam Tip**

The A+ Core 1 exam expects you to be able to compare and contrast the 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac standards, including their frequencies and channels. Study this list carefully, and refer back to [Table 7-1](javascript://) for additional information.

Wireless computers and other devices on the [**wireless LAN (WLAN)**](javascript://) must support the latest wireless standard for it to be used. If not, the connection uses the latest standard both the WAP and client support. [Figure 7-54](javascript://) shows a wireless adapter that has two antennas and supports the 802.11ac standard. Most new adapters, wireless computers, and mobile devices support 802.11ac and are backward compatible with older standards.

**Figure 7-54**

A wireless network adapter with two antennas supports 802.11a/b/g/n/ac Wi-Fi standards



Now let’s look at the various features and settings of a wireless access point and how to configure them.

**Notes**

When configuring your wireless access point, it’s important you are connected to the router using a wired connection. If you change a wireless setting and you are connected wirelessly, your wireless connection will be dropped immediately and you cannot continue configuring the router until you connect again.

### Security Key

The most common and effective method of securing a wireless network is to require a security key before a client can connect to the network. By default, a network that uses a security key encrypts data traversing the network. Use the router firmware to set the security key. For best security, enter a security key that is different from the password for the router’s configuration utility.

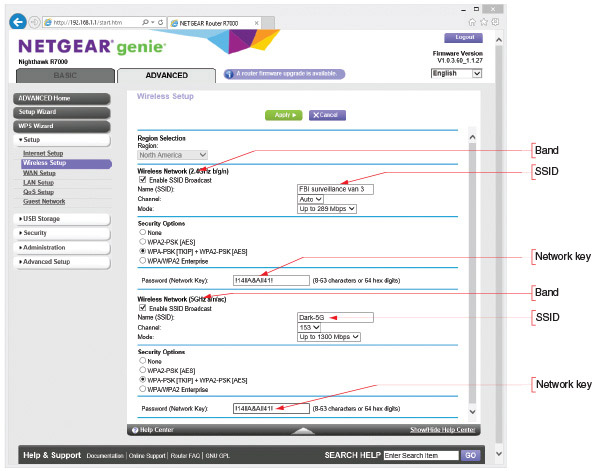
**Notes**

When it comes to making secure passwords and passphrases, longer is better and randomness is crucial. To make the strongest passphrase or security key, use a random group of numbers, uppercase and lowercase letters, and, if allowed, at least one symbol. At the bare minimum, use at least eight characters in the passphrase.

For our sample router, the security key can be set on the ADVANCED tab of the Wireless Setup page in the Setup group (see [Figure 7-55](javascript://)). Here, the security key is called the Password or Network Key. Click **Apply** to save your changes.

**Figure 7-55**

Configure the router’s wireless access point



Enlarge Image

Source: NETGEAR

### Set Encryption

When you set a security key, routers by default encrypt wireless transmissions. You can change the encryption protocols used or disable encryption. (Encrypting transmissions increases security but slows down the network; disabling encryption can improve performance and might be appropriate when you are not concerned about transmissions being hacked.) The three main security standards for 802.11 wireless networks are:

* **WEP.** [**WEP (Wired Equivalent Privacy)**](javascript://) is no longer considered secure because the key used for encryption is static (it doesn’t change).
* **WPA.** [**WPA (Wi-Fi Protected Access)**](javascript://) is stronger than WEP and was designed to replace it. WPA typically uses [**TKIP (Temporal Key Integrity Protocol**](javascript://), pronounced tee-kip) for encryption. TKIP generates a different key for every transmission; however, the encryption algorithm used for its calculations is no longer considered secure.
* **WPA2.** [**WPA2 (Wi-Fi Protected Access 2)**](javascript://), also called the 802.11i standard, is the current wireless security standard. WPA2 typically uses [**AES (Advanced Encryption Standard)**](javascript://) for encryption, which provides faster and more secure encryption than TKIP. All wireless devices sold today support the WPA2 standard.
* **WPA3.** [**WPA3 (Wi-Fi Protected Access 3)**](javascript://) offers better encryption and additional features over WPA2. For example, you can securely configure a nearby wireless device, such as a wireless webcam or motion sensor, over the wireless network, eliminating the need to connect the device with a wired connection to configure it. Another feature is Individual Data Encryption, which allows a secure connection for your laptop or other wireless device over a public, unsecured Wi-Fi network.

To configure Wi-Fi encryption for our sample router, first notice in [Figure 7-55](javascript://) that this router supports two wireless frequencies or bands: 2.4 GHz used by 802.11 b/g/n standards and 5 GHz used by 802.11 a/n/ac. Each band can have its own encryption type and security key. For the most flexibility, set both bands to allow any encryption standard the router supports. For our router, that’s **WPA-PSK [TKIP] + WPA2-PSK [AES]** encryption. This setting means a wireless connection will use WPA2 encryption unless an older device does not support it, in which case the connection reverts to WPA encryption. Alternately, for best security, set both bands to require the highest standard the router supports. For our router, that’s **WPA2-PSK [AES]**. Using this setting, the router will reject any older devices not capable of supporting this encryption standard. Click **Apply** to save your changes.

**Notes**

WPA/WPA2 Enterprise is more secure than WPA/WPA2 PSK, also known as WPA/WPA2 Personal. PSK (pre-shared key) relies on a passphrase shared with all network users, which could be compromised. Enterprise relies on a secure authentication server to manage all users on the network. However, very few SOHO networks have the resources to set up and host an authentication service. In most cases, when setting up a SOHO network, your most secure option is WPA2-PSK or, better yet, WPA2 Personal with AES encryption.

### Change the Default SSID and Disable SSID Broadcasting

The [**Service Set Identifier (SSID)**](javascript://) is the name of a wireless network. When you look at [Figure 7-55](javascript://), you can see that each frequency band has its own SSID and you can change that name. Each band is its own wireless network, which the access point (router) connects to the local wired network. When you give each band its own SSID and connect a wireless computer to your network, you can select the band by selecting the appropriate SSID. If your computer supports 802.11ac, you would want to select the SSID for the 5-GHz band in order to get the faster speeds of the 802.11ac standard. If you selected the SSID for the 2.4-GHz band, the connection would revert to the slower 802.11n standard.

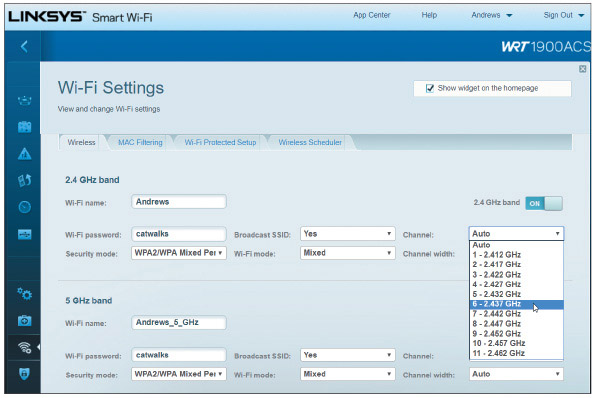
Also notice in [Figure 7-55](javascript://) the option to Enable SSID Broadcast. When you disable SSID broadcasting, the wireless network will appear as Unnamed or Unknown Network on an end user’s device. When a client selects this network, she is given the opportunity to enter the SSID. If she doesn’t enter the name correctly, she will not be able to connect. This security method is not considered strong because software can be used to discover an SSID that is not being broadcast.

### Select Channels for the WLAN

A [**channel**](javascript://) is a specific radio frequency within a broader frequency. For example, two channels in the 2.4-GHz band are 2.412 GHz and 2.437 GHz. In the United States, eleven channels are available for wireless communication in the 2.4-GHz band. In order to avoid channel overlap, however, devices in the 2.4-GHz band select channels 1, 6, or 11, resulting in three nonoverlapping channels available for use. The 5-GHz band offers up to 24 nonoverlapping channels in the United States, although some of those channels are restricted in certain areas, such as near an airport. For most networks, you can allow auto channel selection so the device scans for the least busy channel. However, if you are trying to solve a problem with interference from a nearby wireless network, you can manually set each network to a different channel and make the channels far apart to reduce interference. For example, in the 2.4-GHz band, set the network on one WAP to channel 1 and set a nearby WAP’s network to channel 11. For one router, the Wi-Fi Settings page provides a drop-down menu to select a specific channel or allow the router to automatically select the least busy channel (see [Figure 7-56](javascript://)).

**Figure 7-56**

Select a channel in the 2.4-GHz band



Enlarge Image

Source: Linksys

### Radio Power Levels and WAP Placement

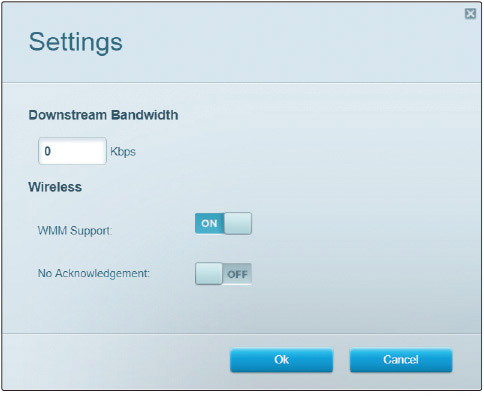
You’ve already learned that an access point should be placed in a central location to maximize its range in the target area. This also minimizes the signal’s reach outside of the target area, which increases security. A wireless signal that reaches to public areas, such as a parking lot or the street, invites unauthorized users to park nearby and take their time attempting to crack your wireless security measures. Some high-end access points allow you to adjust the radio power levels the wireless network can use. To reduce interference, save on electricity, or limit the range of the network to your own property, reduce the power level.

### Wireless QOS

Earlier, you learned you can improve QoS for a device, online game, or other application by assigning it to a high-priority list. In addition, for wireless devices, you can further improve QoS by enabling WMM (Wi-Fi Multimedia). When WMM is enabled, the wireless access point will prioritize wireless traffic for audio, video, and voice over other types of wireless network traffic. For one sample router, look back at [Figure 7-45](javascript://). When you click **Settings** on this router firmware page, the Settings box shown in [Figure 7-57](javascript://) appears. Turn on **WMM Support** and click **OK**. The Roku shown in [Figure 7-45](javascript://) is already prioritized as a device. Now multimedia traffic on the Wi-Fi network has priority.

**Figure 7-57**

Prioritize multimedia traffic over the wireless portion of the network



Source: Linksys

### Wi-Fi Protected Setup (WPS)

You also need to know about [**Wi-Fi Protected Setup (WPS)**](javascript://), which is designed to make it easier for users to connect their computers to a wireless network when a hard-to-remember SSID and security key are used. WPS generates the SSID and security key using a random string of hard-to-guess letters and numbers. The SSID is not broadcast, so both the SSID and security key must be entered correctly to connect. Rather than having to enter these difficult strings, a user presses a button on a wireless computer or on the router, or enters an eight-digit PIN assigned to the router (see [Figure 7-58](javascript://)). All computers on the wireless network must support WPS for it to be used, and you must enable WPS on the router, as shown in the figure.

**Figure 7-58**

Enable WPS and decide how the router’s PIN is used

Graphical user interface, text, application, email

Description automatically generated

Enlarge Image

Source: NETGEAR

WPS might be a security risk if it’s not managed well. To improve WPS security, turn on auto disable so that WPS will be disabled after a few failed PIN entries. If the router doesn’t have the auto disable feature, don’t use WPS—an eight-digit PIN is easy to hack with repeated attempts. In addition, if the router has a WPS button to push, don’t use WPS unless the router is in a secured physical location. For improved security, turn on WPS only when you are working with a user to connect to the wireless network, and then turn it off.

**A+ Exam Tip**

The A+ Core 1 exam may give you a scenario that requires you to install and configure a wireless network, including Wi-Fi 802.11 standards, frequencies, channels (1–11), and encryption.

**A+ Exam Tip**

The A+ Core 2 exam expects you to compare and contrast wireless security protocols (including WEP, WPA, WPA2, TKIP encryption, and AES encryption). Also, given a scenario, you are expected to know when it is appropriate to use SOHO router features, including changing the default SSID and password, setting encryption, disabling SSID broadcasting, antenna and access point placements, radio power levels, and WPS.

Go to pg.

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

Application Opened

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

**7-4**Troubleshooting Network Connections

**A+ Core 2**

* 1.4

Given a scenario, use appropriate Microsoft command line tools.

Windows includes several utilities you can use to troubleshoot networking problems. In this part of the chapter, you learn to use ping, ipconfig, nslookup, tracert, two net commands, and netstat. Most of these program files are found in the \Windows\System32 folder.

**Notes**

Only the more commonly used parameters or switches for each command are discussed in this part of the chapter. For several of these commands, you can use the /? or /help parameter to get more information. For even more information about each command, search the [technet.microsoft.com](http://technet.microsoft.com/" \t "_blank) site.

**A+ Exam Tip**

The A+ Core 2 exam expects you, when given a scenario, to know when and how to use these network utilities: ping, ipconfig, ifconfig, tracert, netstat, net use, net user, and nslookup. You should know when and how to use each utility and how to interpret results.

Now let’s see how to use each utility.

Go to pg.

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

Application Opened

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

## 7-4aPing [-A] [-T] [TargetName]

**A+ Core 2**

* 1.4

Given a scenario, use appropriate Microsoft command line tools.

The [**ping**](javascript://) command tests connectivity by sending an echo request to a remote computer. If the remote computer is online, detects the signal, and is configured to respond to a ping, it responds. (Responding to a ping is the default Windows setting.) Use ping to test for connectivity or to verify that DNS is working. A few examples of ping are discussed in [Table 7-2](javascript://). Two examples are shown in [Figure 7-59](javascript://).

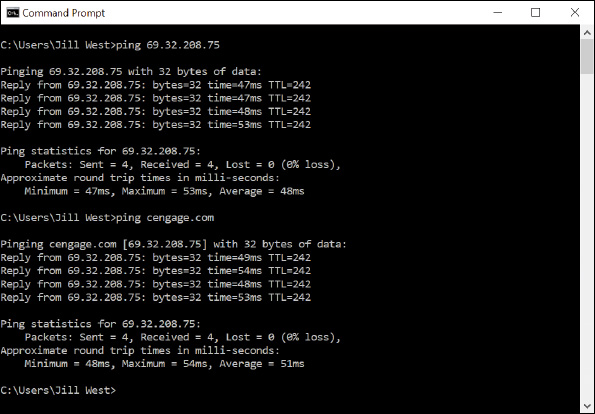
**Table 7-2**

### Examples of the ping command

| **Ping Command** | **Description** |
| --- | --- |
| ping 69.32.208.75 | Ping tests for connectivity using an IP address. If the remote computer responds, the round-trip times are displayed. |
| ping –a 69.32.208.75 | The –a parameter tests for name resolution. Use it to display the host name and verify that DNS is working. |
| ping –t 69.32.208.75 | The –t parameter causes pinging to continue until interrupted. To display statistics, press **Ctrl+Break**. To stop pinging, press **Ctrl+C**. |
| ping 127.0.0.1 | This is called a loopback address test. The IP address 127.0.0.1 always refers to the local computer. If the local computer does not respond, you can assume there is a problem with the network connection’s configuration. |
| ping cengage.com | Use a host name to find out the IP address of a remote computer. If the computer does not respond, suspect there is a problem with DNS. On the other hand, some computers are not configured to respond to pings. |

**Figure 7-59**

Use ping to test for connectivity and name resolution



Enlarge Image

Go to pg.

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

Application Opened

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

## 7-4bIpconfig [/All] [/Release] [/Renew] [/Displaydns] [/Flushdns]

**A+ Core 2**

* 1.4

Given a scenario, use appropriate Microsoft command line tools.

The [**ipconfig (IP configuration)**](javascript://) command can display network configuration information and refresh the TCP/IP assignments for a connection, including its IP address. Some examples of the command are listed in [Table 7-3](javascript://).

**Table 7-3**

### Examples of the ipconfig command

| **Ipconfig Command** | **Description** |
| --- | --- |
| ipconfig /all | Displays a network connection’s configuration information, including the MAC address. |
| ipconfig /release | Releases the IP address and other TCP/IP assignments when dynamic IP addressing is being used. |
| ipconfig /release6 | Releases an IPv6 address and other TCP/IP assignments. |
| ipconfig /renew | Leases a new IP address from a DHCP server. Make sure you release the IP address before you renew it. |
| ipconfig /renew6 | Leases a new IPv6 address from a DHCP IPv6 server. Make sure you release the IPv6 address before you renew it. |
| ipconfig /displaydns | Displays information about name resolutions that Windows currently holds in the DNS resolver cache. |
| ipconfig /flushdns | Flushes the name resolver cache, which might solve a problem when the browser cannot find a host on the Internet. |

**Notes**

The **[ifconfig (interface configuration)](javascript://)** command is similar to ipconfig, and is used on UNIX, Linux, and macOS operating systems. You’ll learn more about how to use Linux and macOS in [Chapter 18](javascript://).

Go to pg.

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

Application Opened

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

## 7-4cNslookup [ComputerName]

**A+ Core 2**

* 1.4

Given a scenario, use appropriate Microsoft command line tools.

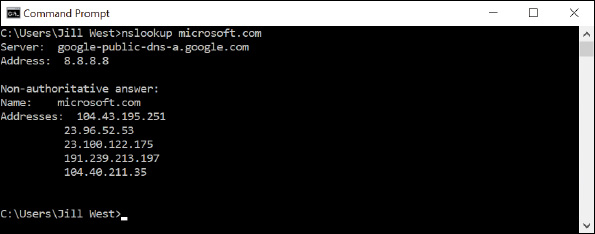
The **[nslookup (namespace lookup](javascript://)** or **name server lookup)** command is used to test name resolution problems with DNS servers by allowing you to request information from a DNS server’s zone data. Zone data is the portion of the DNS namespace that the server knows about. For example, to find out what your DNS server knows about the domain name [microsoft.com](http://microsoft.com/" \t "_blank), use this command:

nslookup microsoft.com

[Figure 7-60](javascript://) shows the results. Notice in the figure that the DNS server reports five different IPv4 addresses assigned to [microsoft.com](http://microsoft.com/" \t "_blank). It also reports that this information is nonauthoritative, meaning that it is not the authoritative, or final, name server for the [microsoft.com](http://microsoft.com/" \t "_blank) domain name.

**Figure 7-60**

The nslookup command reports information about the Internet namespace



Enlarge Image

A [**reverse lookup**](javascript://) is when you use the nslookup command to find the host name when you know a computer’s IP address, such as:

nslookup 69.32.208.75

To find out the default DNS server for a network, enter the nslookup command with no parameters.

Go to pg.

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

Application Opened

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

## 7-4dTracert [TargetName]

**A+ Core 2**

* 1.4

Given a scenario, use appropriate Microsoft command line tools.

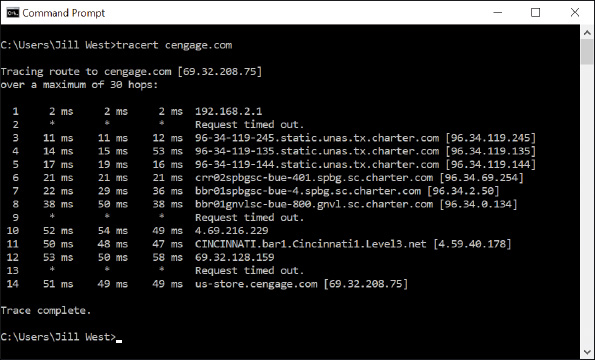
The **[tracert (trace route)](javascript://)** command can be useful when you’re trying to resolve a problem reaching a destination host such as an FTP site or website. The command sends a series of requests to the destination computer and displays each hop to the destination. (A hop happens when a message moves from one router to another.) For example, to trace the route to the cengage.com web server, enter this command in a command prompt window:

tracert cengage.com

The results of this command for one location are shown in [Figure 7-61](javascript://); your results will be different. A message is assigned a Time to Live (TTL), which is the number of hops it can make before a router drops the message and sends an error message back to the host that sent the original message (see [Figure 7-62](javascript://)). The tracert command creates its report from these messages. If a router doesn’t respond, the Request timed out message appears.

**Figure 7-61**

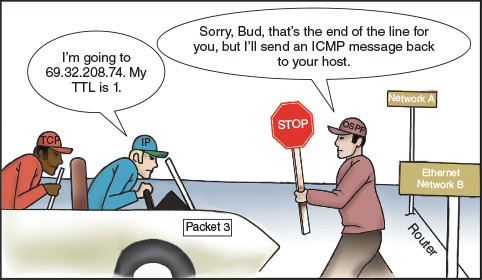
The tracert command traces a path to a destination computer



Enlarge Image

**Figure 7-62**

A router eliminates a message that has exceeded its TTL



Go to pg.

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

Application Opened

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

## 7-4eThe net Commands

**A+ Core 2**

* 1.4

Given a scenario, use appropriate Microsoft command line tools.

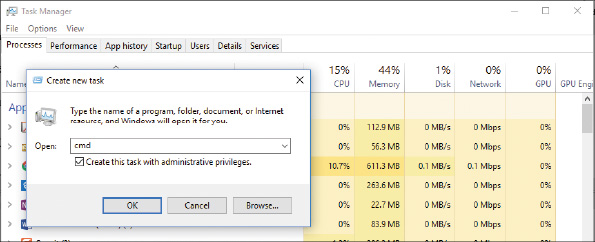
The net command is several commands in one, and most of the net commands require an [**elevated command prompt window**](javascript://), which allows commands that require administrator privileges in Windows. In this section, you learn about the net use and net user commands. The [**net use**](javascript://) command connects or disconnects a computer from a shared resource or can display information about connections.

**Notes**

One way to get an elevated command prompt window is to open **Task Manager**, click **File**, click **Run new task**, type **cmd**, check **Create this task with administrative privileges**, and click **OK**. See [Figure 7-63](javascript://). The command prompt window that appears has Administrator in the title bar.

**Figure 7-63**

Open an elevated command prompt window



Enlarge Image

Use the following commands to pass a user name and password to the \\bluelight remote computer, and then map a network drive to the \Medical folder on that computer:

net use \\bluelight\Medical /user:“Jean Andrews” mypassword

net use z: \\bluelight\Medical

The double quotation marks are needed in the first command above because the user name has a space in it.

A persistent network connection is one that happens at each logon. To make the two commands persistent, add the /persistent parameter like this:

The [**net user**](javascript://) command manages user accounts. For example, the built-in administrator account is disabled by default. To activate the account, use this net user command:

net user administrator /active:yes

**Notes**

Other important net commands are net localgroup, net accounts, net config, net print, net share, and net view. Consider doing a Google search on these commands to find out how they work.

Go to pg.

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

Application Opened

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

## 7-4fNetstat [-A] [-B] [-O]

**A+ Core 2**

* 1.4

Given a scenario, use appropriate Microsoft command line tools.

The [**netstat (network statistics)**](javascript://) command gives statistics about network activity and includes several parameters. [Table 7-4](javascript://) lists a few netstat commands.

**Table 7-4**

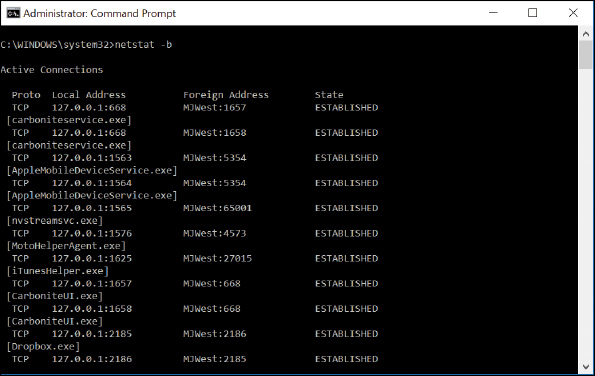
### Netstat commands

| **Netstat Command** | **Description** |
| --- | --- |
| netstat | Lists statistics about the network connection, including the IP addresses of active connections. |
| netstat >>netlog.txt | Directs output to a text file. |
| netstat –b | Lists programs that are using the connection (see [Figure 7-64](javascript://)) and is useful for finding malware that might be using the network. The –b switch requires an elevated command prompt. |
| netstat –b -o | Includes the process ID of each program listed. When you know the process ID, you can use the taskkill command to kill the process. |
| netstat –a | Lists statistics about all active connections and the ports the computer is listening on. |

Enlarge Table

**Figure 7-64**

Netstat -b lists programs that are using a network connection



Enlarge Image

**Notes**

Many commands other than netstat can use the >> parameter to redirect output to a text file. For example, try the ping or tracert command with this parameter:

tracert cengage.com >>C:\Users\“Jill West”\Documents\testfile.txt

Go to pg.

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

Application Opened

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

# Chapter Review

## 7-5a**Chapter Summary**

### Types of Networks and Network Connections

* Networks are categorized by size as a PAN, LAN, WMN, MAN, or WAN.
* Performance of a network technology is measured in bandwidth and latency.
* The two most popular ways to connect to the Internet are cable Internet and DSL. Other methods used include dedicated fiber optic, satellite, dial-up, and cellular wireless technologies (3G, 4G, 5G, and/or LTE).

### Connecting a Computer to a Local Network

* A VPN protects data by encrypting it from the time it leaves the remote computer until it reaches a server on the corporate network, and vice versa.
* A host needs an IP address, subnet mask, default gateway, and IP addresses for DNS servers to communicate with other hosts on the local or remote networks.
* Network adapters, commonly called NICs, are rated by speed and each has a MAC address. Some NICs have status indicator lights and wake-on-LAN and QoS features.

### Setting Up a Multifunction Router for a SOHO Network

* A multifunction router for a small office/home office network might serve several functions, including router, switch, DHCP server, wireless access point, firewall, and FTP server.
* It’s extremely important to change the administrative password on a router as soon as you install it, especially if the router also serves as a wireless access point.
* To allow certain network traffic initiated from the Internet past your firewall, you can use port forwarding, a DMZ, and content filtering with whitelists or blacklists. Access to the network can be controlled by MAC address filtering.
* To secure a wireless access point, you can require a security key, enable encryption (WEP, WPA, WPA2, or WPA3), disable SSID broadcasting, and adjust radio power levels. You can also set wireless channels and wireless QoS to maximize the efficiency of a wireless network.

### Troubleshooting Network Connections

* Useful Windows command-line utilities for network troubleshooting are ping, ipconfig, nslookup, tracert, net use, net user, and netstat. The Linux ifconfig command is similar to the Windows ipconfig command.

Go to pg.

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

Application Opened

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

# Chapter Review

## 7-5b**Key Terms**

For explanations of key terms, see the Glossary for this text.

* [**3G**](javascript://)
* [**4G**](javascript://)
* [**5G**](javascript://)
* [**802.11a**](javascript://)
* [**802.11ac**](javascript://)
* [**802.11b**](javascript://)
* [**802.11g**](javascript://)
* [**802.11n**](javascript://)
* [**address reservation**](javascript://)
* [**AES (Advanced Encryption Standard)**](javascript://)
* [**APIPA (Automatic private IP address)**](javascript://)
* [**bandwidth**](javascript://)
* [**beamforming**](javascript://)
* [**blacklist**](javascript://)
* [**broadband**](javascript://)
* [**cable Internet**](javascript://)
* [**cable modem**](javascript://)
* **cellular network**
* [**channel**](javascript://)
* [**client/server application**](javascript://)
* **coaxial (coax) cable**
* [**data throughput**](javascript://)
* [**default gateway**](javascript://)
* [**DHCP (Dynamic Host Configuration Protocol)**](javascript://)
* [**DHCP client**](javascript://)
* **DHCP server**
* [**DHCPv6 server**](javascript://)
* [**DMZ (demilitarized zone)**](javascript://)
* [**DNS (Domain Name System or Domain Name Service)**](javascript://)
* [**DNS server**](javascript://)
* [**DSL (Digital Subscriber Line)**](javascript://)
* [**DSL modem**](javascript://)
* [**dynamic IP address**](javascript://)
* [**elevated command prompt window**](javascript://)
* [**fiber optic**](javascript://)
* [**fiber-optic cable**](javascript://)
* [**firewall**](javascript://)
* **FTP (File Transfer Protocol)**
* [**FTP server**](javascript://)
* [**full duplex**](javascript://)
* [**half duplex**](javascript://)
* [**host**](javascript://)
* [**ifconfig (interface configuration)**](javascript://)
* [**IP address**](javascript://)
* [**ipconfig (IP configuration)**](javascript://)
* [**IPv4 (Internet Protocol version 4)**](javascript://)
* [**IPv6 (Internet Protocol version 6)**](javascript://)
* [**ISDN (Integrated Services Digital Network)**](javascript://)
* [**ISP (Internet service provider)**](javascript://)
* [**LAN (local area network)**](javascript://)
* [**latency**](javascript://)
* [**line-of-sight wireless connectivity**](javascript://)
* [**LTE (Long Term Evolution)**](javascript://)
* [**MAC address**](javascript://)
* **MAC address filtering**
* [**MAN (metropolitan area network)**](javascript://)
* [**MIMO (multiple input/multiple output)**](javascript://)
* [**mobile hotspot**](javascript://)
* [**name resolution**](javascript://)
* [**net use**](javascript://)
* [**net user**](javascript://)
* [**netstat (network statistics)**](javascript://)
* [**NIC (network interface card)**](javascript://)
* [**nslookup (namespace lookup or name server lookup)**](javascript://)
* [**PAN (personal area network)**](javascript://)
* [**physical address**](javascript://)
* [**ping**](javascript://)
* [**port address**](javascript://)
* [**port forwarding**](javascript://)
* **protocol**
* [**QoS (Quality of Service)**](javascript://)
* [**reverse lookup**](javascript://)
* **RJ-11**
* [**RJ-45**](javascript://)
* [**router**](javascript://)
* [**SIM (Subscriber Identification Module) card**](javascript://)
* [**SSID (Service Set Identifier)**](javascript://)
* [**static IP address**](javascript://)
* [**subnet mask**](javascript://)
* [**switch**](javascript://)
* [**TCP/IP (Transmission Control Protocol/Internet Protocol)**](javascript://)
* [**tether**](javascript://)
* [**TKIP (Temporal Key Integrity Protocol)**](javascript://)
* [**tracert (trace route)**](javascript://)
* [**UPnP (Universal Plug and Play)**](javascript://)
* [**VPN (virtual private network)**](javascript://)
* [**Wake-on-LAN**](javascript://)
* [**WAN (wide area network)**](javascript://)
* [**WAP (wireless access point)**](javascript://)
* [**WEP (Wired Equivalent Privacy)**](javascript://)
* [**whitelist**](javascript://)
* **Wi-Fi (Wireless Fidelity)**
* [**WLAN (wireless LAN)**](javascript://)
* [**WMN (wireless mesh network)**](javascript://)
* [**WPA (Wi-Fi Protected Access)**](javascript://)
* [**WPA2 (Wi-Fi Protected Access 2)**](javascript://)
* [**WPA3 (Wi-Fi Protected Access 3)**](javascript://)
* [**WPS (Wi-Fi Protected Setup)**](javascript://)
* [**WWAN (wireless wide area network)**](javascript://)

Go to pg.

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

Application Opened

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

# Chapter Review

## 7-5c**Thinking Critically**

These questions are designed to prepare you for the critical thinking required for the A+ exams and may use content from other chapters and the web.

1. You have just finished installing a network adapter and booted up the system, installing the drivers. You open File Explorer on a remote computer and don’t see the computer on which you installed the new NIC. What is the first thing you check? The second thing?
   1. Has IPv6 addressing been enabled?
   2. Is the computer using dynamic or static IP addressing?
   3. Do the lights on the adapter indicate it’s functioning correctly?
   4. Has the computer been assigned a computer name?
2. As an IT technician, you arrive at a customer’s home office to troubleshoot problems he’s experiencing with his printer. While questioning the customer to get an understanding of his network, you find that he has a new Wi-Fi router that connects wirelessly to a new desktop and two new laptops, in addition to multiple smartphones, tablets, and the network printer. He also has several smart home devices, including security cameras, light switches, door locks, and a thermostat supported by an IoT controller hub. To work on the printer, which type of network will you be interacting with?
   1. PAN
   2. WAN
   3. WMN
   4. LAN
3. While you work on the customer’s printer, he continues chatting about his network and problems he’s been experiencing. One complaint is that his Internet service slows down considerably in the evening. You suspect you know the cause of this problem: His neighbors arrive home in the evening and bog down the ISP’s local infrastructure. To be sure, you take a quick look at the back of his modem. What type of cable connected to the WAN port would confirm your suspicions and why?
4. Your customer then asks you if it would be worth the investment for him to have Ethernet cabling installed to reach each of his workstations, instead of connecting them by Wi-Fi to his network. Specifically, he wants to know if that would speed up communications for the workstations. You examine his router and find that it’s using 802.11ac Wi-Fi. Would you advise him to upgrade to Ethernet? Why or why not?
   1. Yes, because Ethernet is faster than 802.11ac.
   2. Yes, because wired connections are always faster than wireless connections.
   3. No, because installing Ethernet cabling is more expensive than the increased speed is worth.
   4. No, because 802.11ac speeds are faster than Ethernet.
5. You run the ipconfig command on your computer, and it reports an IP address of 169.254.75.10 on the Ethernet interface. Which device assigned this IP address to the interface?
   1. The ISP’s DNS server
   2. The local network’s DHCP server on the SOHO router
   3. The cable modem
   4. The local computer
6. A friend of yours is having trouble getting good Internet service. He says his house is too remote for cable TV—he doesn’t even have a telephone line to his house. He’s also really frustrated with satellite service because cloudy skies or storms often disrupt the signal. You ask him what provider he uses for his cell phone. He says he has Verizon for his cell, which gets a good signal at his house. What Internet service will you recommend he look into getting for his home network?
   1. Dial-up
   2. LTE installed Internet
   3. DSL
   4. Cable Internet
7. You’ve just received a call from Human Resources asking for assistance with a problem. One of your company’s employees, Renee, has recently undergone extensive surgery and will be homebound for 3–5 months. She plans on working from home and needs a solution to enable frequent and extended access to the company network’s resources. Which WAN technology will you need to configure for Renee and which tool will you use to configure it?
   1. WWAN using the Network Connections window
   2. Dial-up using the Network and Sharing Center
   3. Ethernet using the Network Connections window
   4. VPN using the Network and Sharing Center
8. Describe two different methods of opening the Network and Sharing Center in Windows 10.
9. In this chapter, you learned how to set a static IP address in Windows. Most Linux OSs allow these settings to be changed from the command line. Search online to see how to do this. What Linux command is used to set the interface to a static IP address?
10. Your boss has asked you to configure a DHCP reservation on the network for a Windows computer that is used to configure other devices on a network. To do this, you need the computer’s MAC address. What command can you enter at the command line to access this information?
11. You’re setting up a Minecraft gaming server so that you and several of your friends can share a realm during your gameplay. To do this, your friends will need to access your server over the Internet, which means you must configure your router to send this traffic to your game server. Which router feature will you use and which port must you open?
12. While troubleshooting an Internet connection problem for your network, you restarted the modem and then the router. The router is now communicating with the Internet, which you can confirm by observing the blinking light on the router’s WAN indicator. However, now your laptop is not communicating with the router. Order the commands below to fix the problem and confirm connectivity.
    1. ping
    2. ipconfig /renew
    3. nslookup [microsoft.com](http://microsoft.com/" \t "_blank)
    4. ipconfig /release
13. You have just installed a SOHO router in a customer’s home and the owner has called to say his son is complaining that Internet gaming is too slow. His son is using a wireless laptop. Which possibilities should you consider to speed up the son’s gaming experience? Select all that apply.
    1. Verify that the wireless connection is using the fastest wireless standard the router supports.
    2. Disable encryption on the wireless network to speed up transmissions.
    3. Suggest the son use a wired Gigabit Ethernet connection to the network.
    4. Enable QoS for the gaming applications on the router and on the son’s computer.
14. You need a VPN to connect to a private, remote network in order to access some files. You click the network icon in your taskbar to establish the connection, and realize there is no VPN option available on the menu. What tool do you need to use to fix this problem?
    1. net command
    2. netstat command
    3. Network and Sharing Center
    4. Network Connections window
15. You’re troubleshooting a network connection for a client at her home office. After pinging the network’s default gateway, you discovered that the cable connecting the desktop to the router had been damaged by foot traffic and was no longer providing a reliable signal. You replaced the cable, this time running the cable along the wall so it won’t be stepped on. What do you do next?

Go to pg.

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