Application Opened

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

**Chapter**

**8**

**Network Infrastructure and Troubleshooting**

* [Chapter Introduction](javascript://)
* **8-1**[Understanding TCP/IP and Windows Networking](javascript://)
  + **8-1a**[Layers of Network Communication](javascript://)
  + **8-1b**[How IPv4 Addresses Are Used](javascript://)
  + **8-1c**[How IPv6 Addresses Are Used](javascript://)
  + **8-1d**[Viewing IP Address Settings](javascript://)
  + **8-1e**[Character-Based Names Identify Computers and Networks](javascript://)
  + **8-1f**[TCP and UDP Delivery Methods](javascript://)
  + **8-1g**[TCP/IP Protocols Used by Applications](javascript://)
* **8-2**[Local Network Infrastructure](javascript://)
  + **8-2a**[Switches and Hubs](javascript://)
  + **8-2b**[Wireless Access Points and Bridges](javascript://)
  + **8-2c**[Network Servers](javascript://)
  + **8-2d**[Unified Threat Management (UTM) Appliance](javascript://)
  + **8-2e**[Ethernet Cables and Connectors](javascript://)
  + **8-2f**[Powerline Networking or Ethernet over Power (EoP)](javascript://)
  + **8-2g**[Power over Ethernet (PoE)](javascript://)
* **8-3**[Setting Up and Troubleshooting Network Wiring](javascript://)
  + **8-3a**[Designing a Wired Network](javascript://)
  + **8-3b**[Tools Used by Network Technicians](javascript://)
  + **8-3c**[How Twisted-Pair Cables and Connectors Are Wired](javascript://)
* **8-4**[Troubleshooting Network Connections](javascript://)
  + **8-4a**[Problems with No Connectivity or Intermittent Connectivity](javascript://)
  + **8-4b**[Problems with Internet Connectivity](javascript://)
  + **8-4c**[Using TCP/IP Utilities to Solve Connectivity Problems](javascript://)
  + **8-4d**[Slow Transfer Speeds](javascript://)
  + **8-4e**[Wi-Fi Network Not Found](javascript://)
* **8-5**[Chapter Review](javascript://)
  + **8-5a**[Chapter Summary](javascript://)
  + **8-5b**[Key Terms](javascript://)
  + **8-5c**[Thinking Critically](javascript://)
  + **8-5d**[Hands-On Projects](javascript://)
  + **8-5e**[Real Problems, Real Solutions](javascript://)
  + **8-5f**[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:

* Explain the TCP/IP protocols and standards Windows uses for networking
* Identify, compare, and contrast hardware used to build local networks
* Set up and troubleshoot the wiring in a small network
* Troubleshoot network connectivity problems caused by firmware, operating systems, and applications

You’ve already learned how to connect a computer to a network and how to set up and secure a wired and wireless router for a small network. This chapter takes you a step further in supporting networks. You learn how Windows uses TCP/IP protocols and standards to create and manage network connections, including how computers are identified and addressed on a network. You also learn about the hardware devices, cables, and connectors used to construct a network. Next, you learn about networking tools, how to terminate network cables, and how to troubleshoot problems with network hardware and software.

Go to pg.

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

Application Opened

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

**8-1**Understanding TCP/IP and Windows Networking

**A+ Core 1**

* 2.1

Compare and contrast TCP and UDP ports, protocols, and their purposes.

* 2.2

Compare and contrast common networking hardware devices.

* 2.3

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

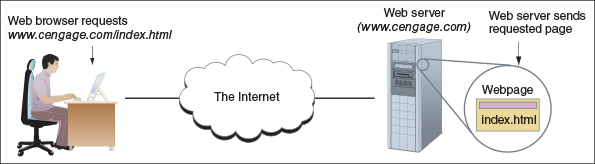
* 2.6

Explain common network configuration concepts.

The more you understand how networks work, the more likely you will be able to solve problems with network connections. This part of the chapter focuses on how a network works. When two computers communicate using a local network or the Internet, communication happens essentially at four levels: the hardware, the operating system, the application for each computer on the network, and the network itself. Communication begins when one computer tries to find the other computer on the local or remote network. For example, in [Figure 8-1](javascript://), someone uses a web browser on a client to request a webpage from a web server. To handle this request, the client computer looks for the web server, the protocols for communication are established, and then the request is made and answered. Hardware, network devices, the OS, and the applications on both computers are all involved in this process.

**Figure 8-1**

A web browser (client software) requests a webpage from a web server (server software); the web server returns the requested data to the client



Enlarge Image

Let’s first look at the layers of communication that involve hardware, network devices, the OS, and applications, and then see how computers are addressed and found on a network or the Internet. Then we’ll see how a client/server request is made by the client and answered by the server.

Go to pg.

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

Application Opened

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

## 8-1aLayers of Network Communication

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

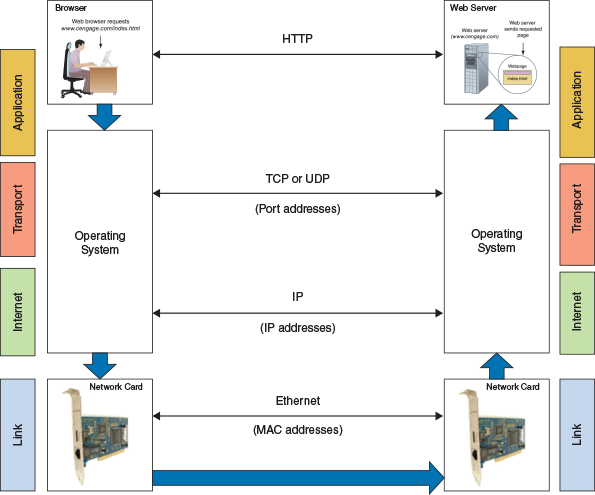
When your computer at home is connected to your Internet service provider (ISP) off somewhere in the distance, your computer and a computer on the Internet must be able to communicate. When two devices communicate, they must use the same protocols so that the communication makes sense. Recall that, for almost all networks today, including the Internet, the group or suite of protocols used is called **TCP/IP (Transmission Control Protocol/Internet Protocol)**.

### TCP/IP Model for Network Communication

Let’s consider network communication that starts when a browser (an application) requests a webpage from a web server (another application). The layers of communication are shown in [Figure 8-2](javascript://) with the blue arrows. The request is passed to the OS, which passes the request to the network card, which passes the request on to the network. When the request reaches the network card on the server, the network card passes the request on to the OS and then the OS passes it on to the application (the web server).

**Figure 8-2**

Network communication happens in layers



Enlarge Image

When studying networking theory, a simple model used to divide network communication into four layers is the [**TCP/IP model**](javascript://). In this model, protocols used by hardware function at the Link layer, and protocols used by the OS are divided into three layers (Internet, Transport, and Application layers). These four layers are shown on the left and right sides of [Figure 8-2](javascript://) and listed in [Table 8-1](javascript://).

**Table 8-1**

### TCP/IP Model Has Four Layers of Communication

| **Layer** | **Addressing** | **Description** |
| --- | --- | --- |
| Layer 4: Application layer |  | Application-to-application communication is managed by the OS, using protocols specific to the application (HTTP, Telnet, FTP, and so forth). This layer of communication happens after the OSs have made a connection at the Transport layer. |
| Layer 3: Transport layer | Port numbers | Host-to-host communication, managed by the OS, primarily using TCP and UDP protocols. |
| Layer 2: Internet layer | IP addresses | Host-to-host on the local network or network-to-network communication, managed by the OS and network devices. |
| Layer 1: Link layer | MAC addresses | Device-to-device on local network, managed by firmware on NICs. Layer 1 is also called the Network interface layer or Network access layer. |

Let’s follow a message from browser to web server, paying attention to each layer of communication:

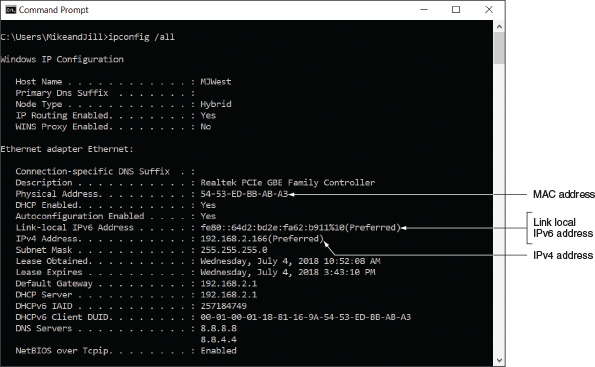
* **Source Step 1: Application layer**. Recall from [Chapter 7](javascript://) that most applications that use a network are client/server applications. When a browser client makes a request to a web server, the browser passes the request to the OS. The OS formats the message using the appropriate application protocol (for example, HTTP, FTP, Telnet, DNS, and SSH). In our example, an HTTP message is created and passed down in the TCP/IP stack of protocols to the Transport layer.
* **Source Step 2: Transport layer**. The Transport layer adds information to the message to address the correct server application. Depending on the type of application, the protocol TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) adds the port assigned to the server application (TCP uses port 80 for HTTP communication in our example). The message with Transport data added is then passed down to the Internet layer.
* **Source Step 3: Internet layer**. The Internet layer is responsible for getting the message to the destination computer or host on the local network, an intranet, or the Internet. An [**intranet**](javascript://) is any private network that uses TCP/IP protocols. A large enterprise might support an intranet that is made up of several local networks. The primary protocol used at the Internet layer is [**IP (Internet Protocol)**](javascript://), which uses a 32-bit and/or 128-bit IP address to identify each host. (Other Internet layer protocols include EIGRP, OSPF, BGP, and ICMP.) IP adds address information to the message and then passes it down to the Link layer.
* **Source Step 4: Link layer**. The Link layer is the physical network, including the hardware and its firmware for every device connected to the network. A computer’s network interface card (NIC) is part of this physical network. As you know, each NIC is able to communicate with other NICs on the local network using each NIC’s MAC address. The MAC address is a 48-bit (6-byte) unique number hard-coded on the card by its manufacturer. Part of the MAC address identifies the manufacturer, who is responsible for making sure that no two network adapters have the same MAC address. Every device on a network (for example, computers, printers, smart thermostats, refrigerators, and smartphones) connects to the network by way of its NIC and MAC address. For a local network, recall the hardware or physical connection might be wireless (most likely using Wi-Fi) or wired (most likely using Ethernet). The NIC receives the message from IP, adds information for Ethernet or Wi-Fi transmission, and places the message on the network.

**Notes**

You can have Windows tell you the MAC address of an installed NIC by entering the ipconfig /all command in a command prompt window (see [Figure 8-3](javascript://)).

**Figure 8-3**

Use the ipconfig /all command to show the MAC address, also called the physical address, of a network adapter

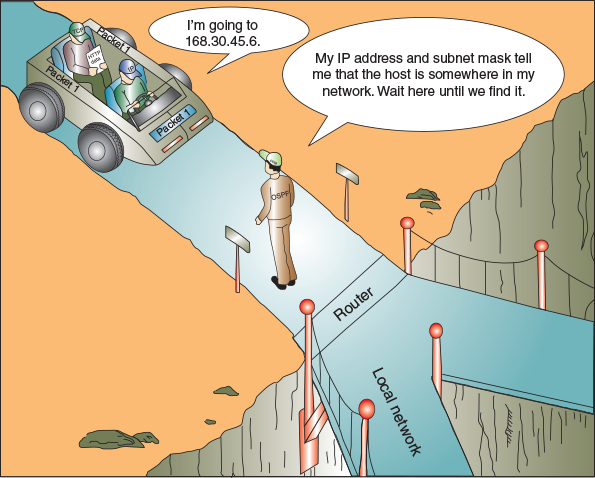


Enlarge Image

* **Step 5: Network transmission**. IP at the Internet layer is responsible to make sure the message gets from one network to the next until it reaches its destination network (see [Figure 8-4](javascript://)) and destination computer on that network. Whereas a MAC address at the hardware Link layer is only used to find a computer or other host on a local network, an IP address can be used to find a computer on a local network, anywhere on the Internet (see [Figure 8-5](javascript://)), or on an intranet.

**Figure 8-4**

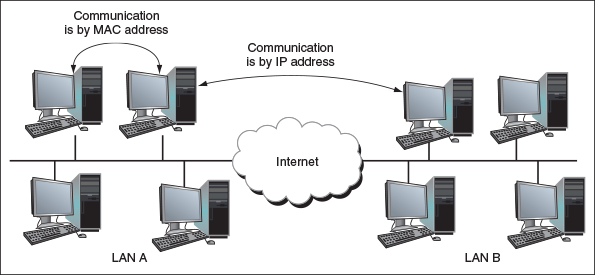
A host (router, in this case) can always determine if an IP address is on its network



Enlarge Image

**Figure 8-5**

Computers on the same LAN can use MAC addresses to communicate, but computers on different LANs use IP addresses to communicate over the Internet

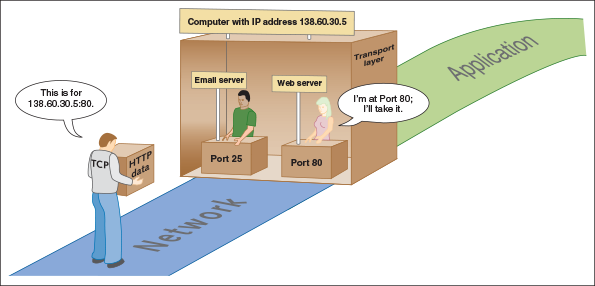


Enlarge Image

* **Step 6: Destination**. On the destination computer, its NIC receives the message, strips off Ethernet or Wi-Fi information at the Link layer, and passes the message up to the Internet layer. The Internet layer strips off IP address information and passes the message up to the Transport layer. The Transport layer strips off TCP or UDP information and passes the message to the correct port (see [Figure 8-6](javascript://)) and on to the Application layer. The Application layer passes the message to the web server application.

**Figure 8-6**

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



Enlarge Image

**Notes**

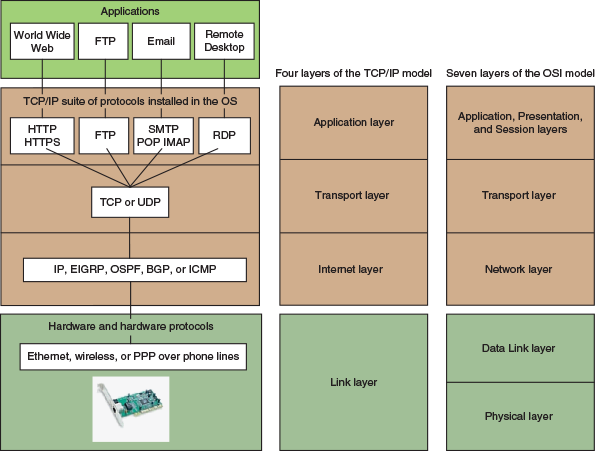
Messages on a TCP/IP network might have different names depending on which layer’s protocols have added information to the message, either at the beginning of the message (called a header) or at the end (called a trailer). For example, messages with IP address header information added are called packets. Messages with source and destination MAC addresses are called frames. In general, all of these messages can be referred to with the more technical term [**protocol data unit (PDU)**](javascript://).

### Compare the TCP/IP Model and OSI Model

Besides the TCP/IP model, a more complicated model is the [**OSI (Open Systems Interconnection) model**](javascript://), which has seven layers of communication and is shown on the right side of [Figure 8-7](javascript://). The figure also shows many of the TCP/IP protocols used by operating systems and client/server applications and how they relate to one another at the different layers. As you continue reading the chapter, this figure can serve as your road map to the different protocols. Three of the most important protocols in the TCP/IP suite are IP at the Internet layer, and TCP and UDP at the Transport layer. Let’s first look at IP along with its IP addresses, beginning with IPv4, and then we’ll examine TCP and UDP with their port numbers, followed by a discussion of several other important protocols.

**Figure 8-7**

How software, protocols, and technology on a TCP/IP network relate to each other



Enlarge Image

**Notes**

In the following sections, the more significant application and operating system protocols are introduced. However, you should know that the TCP/IP protocol suite includes many more protocols than just those mentioned in this chapter; only some of them are shown in [Figure 8-7](javascript://).

Go to pg.

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

Application Opened

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

## 8-1bHow IPv4 Addresses Are Used

**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 MAC address is embedded on every NIC at the factory, but each time a computer connects to a network, the interface with the network is assigned an IP address. Recall from [Chapter 7](javascript://) that an IP address can be a dynamic IP address assigned by a DHCP server or a static IP address manually assigned by the user or a technician. An IP address has 32 bits or 128 bits. When the Internet and TCP/IP were first invented, it seemed that 32 bits were more than enough to satisfy any needs we might have for IP addresses because IPv4 created about four billion potential IP addresses. Today we need many more than four billion IP addresses over the world. Partly because of a shortage of 32-bit IP addresses, IPv6 was designed to use an IP address with 128 bits. Currently, the Internet uses a mix of 32-bit and 128-bit IP addresses. The Internet Assigned Numbers Authority (IANA at [iana.org](http://iana.org/" \t "_blank)) is responsible for keeping track of assigned IP addresses and has already released all of its available 32-bit IPv4 addresses. IPv6 addresses leased from IANA today are all 128-bit addresses.

A 32-bit IPv4 address is organized into four groups of 8 bits each, which are presented as four decimal numbers separated by periods, such as 72.56.105.12. The largest possible 8-bit number is 11111111, which is equal to 255 in decimal, so the largest possible IPv4 address in decimal is 255.255.255.255, which in binary is 11111111.11111111.11111111.11111111. Each of the four numbers separated by periods is called an [**octet**](javascript://) (for 8 bits) and can be any decimal value from 0 to 255, making a total of about 4.3 billion IPv4 addresses (256 × 256 × 256 × 256). Some IP addresses are reserved, so these numbers are approximations. IP addresses that are reserved for special use by TCP/IP and should not be assigned to a device on a network are listed in [Table 8-2](javascript://).

**Table 8-2**

### Reserved IP Addresses

| **IP Address** | **How It Is Used** |
| --- | --- |
| 127.0.0.1 | Indicates your own computer and is called the [**loopback address**](javascript://). |
| 0.0.0.0 | Currently unassigned IP address. |
| 255.255.255.255 | Used for [**broadcast messages**](javascript://) by TCP/IP background processes to communicate with all devices on a network at the same time or without needing specific recipient information, such as when a device uses DHCP to send out a request to any host that might be running a DHCP server to get an IP address. Broadcasting can cause a lot of network chatter; to reduce the chatter, [**subnets**](javascript://) are created to subdivide a network into smaller networks so that fewer devices receive and respond to broadcast messages. |

The first part of an IP address identifies the network, and the last part identifies the host. When messages are routed over the Internet, the network portion of the IP address is used to locate the right local network. After the message arrives at the local network, the host portion of the IP address is used to identify the one computer on the network that will receive the message. How does a computer or other network device know what part of an IP address identifies the network and what part identifies the host? It relies on a subnet mask for this information.

### Subnet Masks

Recall that when a computer first connects to a network, it is assigned an IP address, subnet mask, and IP address of its default gateway. All the IP addresses assigned to a local network or subnet have matching bits in the first part of the IP address; these bits identify the network and are called the [**network ID**](javascript://). For example, the range of IP addresses assigned to a local network might be 192.168.80.1-100. The first three octets (192.168.80) identify the network and the last octet (1 through 100) identifies each host. The last bits in each IP address that identify the host must be unique for each IP address on the network.

Before a computer can send a message to another computer, it must decide whether it can communicate directly with the computer on its local network or must go through the default gateway to a remote network. To decide, the computer compares the network ID portion of its IP address to the network ID portion of the remote computer’s IP address. How does it know how many bits in its IP address identify its network? That’s the job of the **subnet mask**.

A subnet mask has 32 bits and is a string of 1s followed by a string of 0s—for example, 11111111.11111111.11110000.00000000. The 1s in a subnet mask say, “On our network, this part of an IP address identifies our network,” and the group of 0s says, “On our network, this part of an IP address identifies the host.” Usually a subnet mask is displayed in decimal—for example, the subnet mask of 11111111.11111111.00000000.00000000 is 255.255.0.0 in decimal.

[Figure 8-8](javascript://) shows how a subnet mask serves as a type of filter to decide whether a destination IP address is on the local network or a remote network. In the figure, you can see that the subnet mask has 24 ones. Therefore, the computer compares the first 24 bits of the destination IP address to its own first 24 bits. If they match, it directs the message to the computer on its local network. If they don’t match, it sends the message to its default gateway.

**Figure 8-8**

The subnet mask serves as a filter to decide whether a destination IP address is on its own or another network

Diagram

Description automatically generated

Enlarge Image

In another example, suppose the IP address of a computer is 201.18.20.160 and the subnet mask is 255.255.0.0, which is 11111111.11111111.00000000.00000000 in binary. The subnet mask tells Windows that the first 16 bits, or two octets (201.18), of the IP address is the network ID. Therefore, when Windows is deciding how to communicate with a computer that has an IP address of 201.18.20.208, it knows the computer is on its own network, but a computer with an IP address of 201.19.23.160 is on a different network.

Let’s look at one more example. Suppose the IP address of a computer is 19.200.60.6 and its subnet mask is 255.255.240.0. Is a computer with the IP address 19.200.51.100 on its network? [Table 8-3](javascript://) shows the logic to find out:

**Table 8-3**

### Logic of a Subnet Mask

| **Question** | **Answer** |
| --- | --- |
| * 1.   What is my IP address in binary? | 19.200.60.6 in binary is:  00010011.11001000.00111100.00000110. |
| * 2.   What is my subnet mask in binary? | 255.255.240.0 in binary is:  11111111.11111111.11110000.00000000. |
| * 3.   How many bits in my IP address identify my network? | There are 20 ones in the subnet mask. Therefore, 20 bits identify the network. |
| * 4.   What is the other IP address in binary? | 19.200.51.100 in binary is:  00010011.11001000.00110011.01100100. |
| * 5.   Do the first 20 bits in my IP address match the first 20 bits in the other IP address? | Compare the 20 red bits in the two IP addresses:  00010011.11001000.00111100.00000110  00010011.11001000.00110011.01100100  Yes, they match. |
| * 6.   Is the other IP address on my network? | Yes. |

Sometimes an IP address and subnet mask are written using a shorthand notation like 15.50.212.59/20, where the /20 means that the first 20 bits in the IP address identify the network. This notation is sometimes called slash notation or [**CIDR notation**](javascript://) (pronounced “cider notation”), named after the CIDR (Classless Interdomain Routing) standards that were written in 1993 about subnetting.

### Public, Private, and Automatic Private IP Addresses

There are a few more special ranges of IP addresses you need to know about. IP addresses available to the Internet are called [**public IP addresses**](javascript://). To conserve the number of public IP addresses, some blocks of IP addresses have been designated as [**private IP addresses**](javascript://) that are not allowed on the Internet. Private IP addresses are used within a company’s private network, and computers on this network can communicate with one another using these private addresses.

IEEE recommends that the following IP addresses be used for private networks:

* 10.0.0.0 through 10.255.255.255
* 172.16.0.0 through 172.31.255.255
* 192.168.0.0 through 192.168.255.255

**A+ Exam Tip**

The A+ Core 1 exam expects you to have memorized the private network IP address ranges.

There’s also a special type of private IP address range. If a computer first connects to a network that is using dynamic IP addressing and is unable to lease an IP address from the DHCP server, it generates its own Automatic Private IP Address (APIPA) in the address range 169.254.x.y.

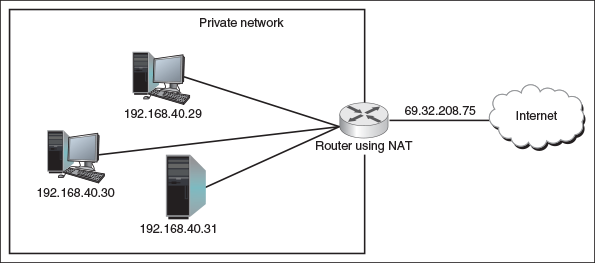
**Notes**

If you are running a web server on the Internet, you will need a public IP address for your router and either a static or reserved private IP address for the web server. For this situation, you can lease a public IP address from your ISP at an additional cost. You will also need to enable port forwarding to the server, which is discussed in [Chapter 7](javascript://).

[**NAT (Network Address Translation)**](javascript://) is a technique designed to conserve the number of public IP addresses needed by a network. A router stands between a private network and the Internet. It substitutes the private IP addresses used by computers on the private network with its own public IP address when these computers need access to the Internet. See [Figure 8-9](javascript://). Besides conserving public IP addresses, another advantage of NAT is security; the router hides the entire private network behind this one address. For a SOHO router, expect that NAT is enabled by default.

**Figure 8-9**

NAT allows computers with private IP addresses to access the Internet



Enlarge Image

**Notes**

IEEE, a nonprofit organization, is responsible for many Internet standards. Standards are proposed to the networking community in the form of an RFC (Request for Comment). RFC 1918 outlines recommendations for private IP addresses. To view an RFC, visit the website [rfc-editor.org](http://rfc-editor.org/" \t "_blank).

Go to pg.

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

Application Opened

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

## 8-1cHow IPv6 Addresses Are Used

**A+ Core 1**

* 2.6

Explain common network configuration concepts.

Moving on to the IPv6 standards, more has changed than just the number of bits in an IP address. To improve routing capabilities and speed of communication, IPv6 changed the way IP addresses are used to find computers on the Internet. Let’s begin our discussion of IPv6 by looking at how IPv6 addresses are written and displayed:

* An IPv6 address has 128 bits that are written as eight blocks of hexadecimal numbers separated by colons, like this: 2001:0000:0B80:0000:0000:00D3:9C5A:00CC.
* Each block is 16 bits. For example, the first block in the address above is 2001 in hex, which can be written as 0010 0000 0000 0001 in binary.
* Leading zeroes in a four-character hex block can be eliminated. For example, the IP address above can be written as 2001:0000:B80:0000:0000:D3:9C5A:CC, where leading zeroes have been removed from three of the hex blocks.
* If blocks contain all zeroes, they can be written as double colons (::). The IP address above can be written two ways:
  + 2001::B80:0000:0000:D3:9C5A:CC
  + 2001:0000:B80::D3:9C5A:CC

To avoid confusion, only one set of double colons is used in an IPv6 address. In this example, the preferred method is the second one: 2001:0000:B80::D3:9C5A:CC because the address is written with the fewest zeroes.

The way computers communicate using IPv6 has changed the terminology used to describe TCP/IP communication. Here are a few terms used in the IPv6 standards:

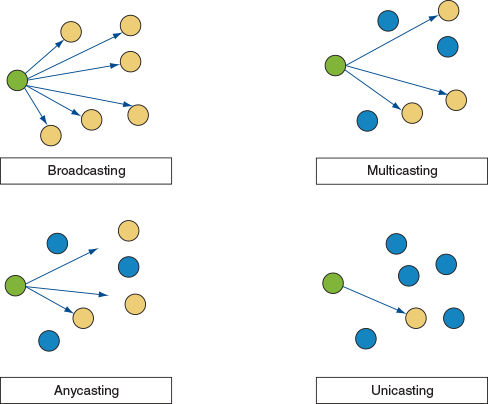
* A [**link**](javascript://) is a local area network (LAN) or wide area network (WAN).
* A [**node**](javascript://) is any device that connects to the network, such as a computer, printer, or router. The connection can be a logical attachment, such as when a virtual machine connects to the network, or a physical attachment, such as when a network adapter connects to the wired network.
* The last 64 bits or 4 blocks of an IPv6 address identify the interface and are called the [**interface ID**](javascript://) or interface identifier. These 64 bits uniquely identify an interface on the local network.
* [**Neighbors**](javascript://) are nodes on the same local network.

Recall that with IPv4 broadcasting, messages are sent to every node on a local network. However, IPv6 doesn’t use broadcasting, thereby reducing network traffic. Instead, IPv6 uses multicasting, anycasting, and unicasting, as illustrated in [Figure 8-10](javascript://) and described next:

* A [**multicast address**](javascript://) is used to deliver messages to all nodes in a targeted, multicast group, such as when video is streaming from a server to multiple nodes on a network.
* An [**anycast address**](javascript://) is used by routers and can identify multiple destinations; a message is delivered only to the closest destination.
* A [**unicast address**](javascript://) is used to send messages to a single node on a network. Three types of unicast addresses are link local addresses, unique local addresses, and global addresses. A single interface might have more than one unicast address assigned to it at any given time:
  + A [**link local address**](javascript://), also called a link local unicast address or local address, can be used for limited communication with neighboring nodes in the same link (the local network). These local addresses are similar to IPv4 APIPA addresses in that they are assigned to the computer by itself as opposed to coming from a DHCPv6 server, and are not guaranteed to be unique on the network. Most link local addresses begin with FE80::/64. This prefix notation means the address begins with FE80 followed by enough zeroes to make 64 bits, as shown in [Figure 8-11](javascript://). Link local addresses are not allowed on the Internet or allowed to travel outside private networks. Look back at [Figure 8-3](javascript://) to see an example of a link local address where the wired interface has the IPv6 address of fe80::64d2:bd2e:fa62:b911%10. The first 64 bits are fe80::, and the interface ID is 64d2:bd2e:fa62:b911. IPv6 addresses are followed by a % sign and a number; for example, %10 follows this IP address. This number is called the zone ID or scope ID and is used to identify the interface in a list of interfaces for this computer.
  + A [**unique local address**](javascript://) is a private address assigned by a DHCPv6 server that can communicate across subnets within the private network. They’re used by network administrators when subnetting a large network. A unique local address always begins with FC or FD and is usually assigned to an interface in addition to its self-assigned link local address.
  + A [**global address**](javascript://), also called a global unicast address, can be routed on the Internet. These addresses are similar to IPv4 public IP addresses. The first 48 bits of the address is the Global Routing Prefix. When an ISP assigns a global address to a customer, it’s these 48 bits that are assigned. An organization that leases one Global Routing Prefix from its ISP can use it to generate many IPv6 global addresses.

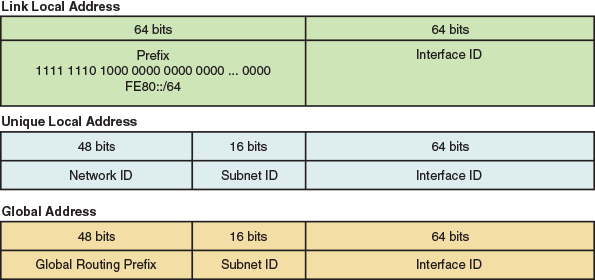
**Figure 8-10**

Concepts of broadcasting, multicasting, anycasting, and unicasting



**Figure 8-11**

Three types of IPv6 addresses: A link local address has a 64-bit prefix followed by 64 bits to identify the host



Enlarge Image

[Table 8-4](javascript://) lists the currently used address prefixes for these types of IPv6 addresses. In the future, we can expect more prefixes to be assigned as they are needed.

**Table 8-4**

### Address Prefixes for Types of IPv6 Addresses

| **IP Address Type** | **Address Prefix** |
| --- | --- |
| Multicast | FF00::/8  (The first 8 bits are always 1111 1111) |
| Link local address | FE80::/64  (The first 64 bits are always 1111 1110 1000 0000…) |
| Unique local address | FC00::/7  (The first 7 bits are always 1111 110; today’s local networks assign 1 for the 8th bit, so the prefix typically shows as FD00::/8) |
| Global address | 2000::/3  (The first 3 bits are always 001) |
| Unassigned address | 0::0  (All zeroes) |
| Loopback address | 0::1, also written as ::1  (127 zeroes followed by 1) |

**A+ Exam Tip**

The A+ Core 1 exam expects you to understand what a link local address is and how it’s used.

**Notes**

IPv6 uses subnetting but doesn’t need a subnet mask because the subnet ID is part of the IPv6 address. The [**subnet ID**](javascript://) is the 16 bits following the first 48 bits of the address. When a large IPv6 network is subnetted, a DHCPv6 server assigns a node in a subnet a global address or unique local address that contains the correct subnet ID for the node’s subnet.

An excellent resource for learning more about IPv6 and how it works is the e-book, TCP/IP Fundamentals for Microsoft Windows. To download the free PDF, search for it at [microsoft.com/download](http://microsoft.com/download" \t "_blank).

Go to pg.

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

Application Opened

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

## 8-1dViewing IP Address Settings

**A+ Core 1**

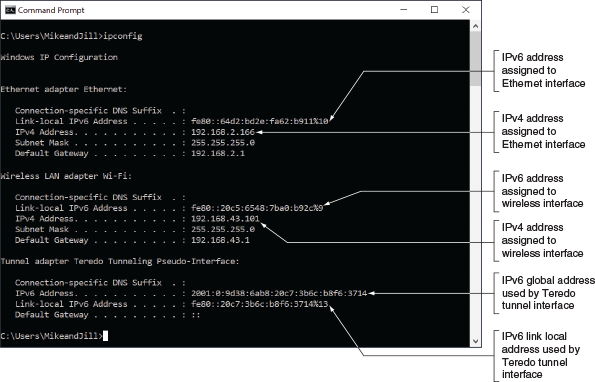
* 2.6

Explain common network configuration concepts.

In summary, let’s use the ipconfig command to take a look at the IPv4 and IPv6 addresses assigned to all network connections on a computer (see [Figure 8-12](javascript://)).

**Figure 8-12**

The ipconfig command showing IPv4 and IPv6 addresses assigned to this computer



Enlarge Image

Notice in the figure the four IP addresses that have been assigned to the physical connections:

* TCP/IP has assigned the Ethernet connection two IP addresses: one IPv4 address and one IPv6 address.
* The wireless LAN connection on a different subnet has also been assigned an IPv4 address and an IPv6 address.

**Notes**

Very few networks solely use IPv6. Tunneling is used to allow IPv6 messages to traverse IPv4 networks. A tunnel works by encapsulating an IPv6 message inside an IPv4 message. [Figure 8-12](javascript://) shows a Teredo (pronounced “ter-EE-do”) tunnel that is assigned IPv6 global and link local addresses. Teredo is named after the Teredo worm that bores holes in wood.

IPv6 addressing is designed so that a computer can self-configure its own link local IP address, which is similar to how IPv4 uses an Automatic Private IP Address (APIPA). Here’s what happens when a computer using IPv6 first makes a network connection:

1. The computer creates its IPv6 address by using the FE80::/64 prefix and uses its MAC address to generate an interface ID for the last 64 bits.
2. It then performs a duplicate address detection process to make sure its IP address is unique on the network.
3. Next, it asks if a DHCPv6 server is present on the network to provide configuration information. If a server responds with DHCP information, such as the IP addresses of DNS servers or the default gateway’s IP address, the computer uses it. It also keeps its original link local address. Because a computer can generate its own link local IP address, a DHCPv6 server usually serves up only global or unique local addresses.

Go to pg.

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

Application Opened

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

## 8-1eCharacter-Based Names Identify Computers and Networks

**A+ Core 1**

* 2.6

Explain common network configuration concepts.

Remembering an IP address is not always easy for humans, so character-based names are used to substitute for IP addresses. Here are the possibilities:

* A [**host name**](javascript://) is the name of a computer and can be used in place of its IP address. The name can have up to 63 characters, including letters, numbers, and special characters. Examples of computer names are www, ftp, Jean’s Computer, TestBox3, and PinkLaptop. You can assign a computer name while installing Windows. In addition, you can change the computer name at any time using the System window.
* A workgroup is a group of computers on a peer-to-peer network that are sharing resources. The workgroup name assigned to this group is only recognized within the local network. In a peer-to-peer network, each computer is responsible for sharing and securing its own resources.
* A [**domain name**](javascript://) identifies a network. Examples of domain names are the names that appear before the period in microsoft.com, cengage.com, and mycompany.com. The letters after the period are called the top-level domain and tell you something about the domain. Examples are .com (commercial), .org (nonprofit), .gov (government), and .info (general use).
* A [**fully qualified domain name (FQDN)**](javascript://) identifies a computer and the network to which it belongs. An example of an FQDN is www.cengage.com. The host name is www (a web server), cengage is the domain name, and com is the top-level domain name of the Cengage network. Another FQDN is joesmith.mycompany.com.

On the Internet, a fully qualified domain name must be associated with an IP address before the computer can be found. Recall that this process of associating a character-based name with an IP address is called name resolution; DNS services and protocols manage name resolution. On home or small company networks, the ISP is responsible for providing access to one or more DNS servers as part of its Internet service. (Recall from [Chapter 7](javascript://) that a DNS server looks up and returns an IP address for a computer name when a DNS client requests this namespace lookup.) Larger corporations have their own DNS servers to perform name resolution for the enterprise network. When an individual or organization, which has its own DNS servers, leases a public IP address and domain name and sets up a website, it is responsible for entering the name resolution information into its primary DNS server. This server can present the information to other DNS servers on the web and is called the authoritative name server for the website.

**A+ Exam Tip**

The A+ Core 1 exam expects you to understand the purpose of DNS servers and be familiar with client-side DNS.

When Windows is trying to resolve a computer name to an IP address, it first looks in the DNS cache it holds in memory. If the computer name is not found in the cache, Windows then turns to a DNS server if it has the IP address of the server. When Windows queries the DNS server for a name resolution, it is called the [**DNS client**](javascript://).

**Applying Concepts**

### Viewing and Clearing the DNS Cache

Suppose a user is unable to reach a website on her computer but you can access it from your help-desk computer. One good step to use when troubleshooting name resolution problems is to clear the DNS cache. Open a command prompt window and use the **ipconfig /displaydns** command to view the DNS cache on your computer. Then use the **ipconfig /flushdns** command to clear the DNS cache. Windows will rebuild its cache by collecting up-to-date DNS information from the DNS servers you’ve configured Windows to use.

Go to pg.

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

Application Opened

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

## 8-1fTCP and UDP Delivery Methods

**A+ Core 1**

* 2.1

Compare and contrast TCP and UDP ports, protocols, and their purposes.

Looking back at [Figure 8-7](javascript://), you can see three layers of protocols working at the Application, Transport, and Internet layers. These three layers make up the heart of TCP/IP communication. In the figure, TCP or UDP manages communication with the applications protocols above them as well as the protocols in the lower layers, which control communication on the network. There are a few key differences between TCP and UDP that determine which of these two protocols is most appropriate for each situation.

**A+ Exam Tip**

The A+ Core 1 exam expects you to be able to contrast the TCP and UDP protocols.

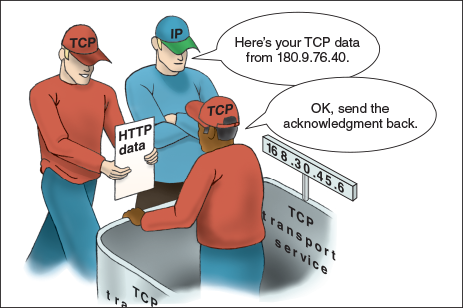
### TCP Guarantees Delivery

Remember that all communication on a network happens by way of messages delivered from one location on a network to another. [**TCP (Transmission Control Protocol)**](javascript://) guarantees message delivery. TCP makes a connection, sends the data, checks whether the data is received, and resends it if it is not. TCP is therefore called a [**connection-oriented protocol**](javascript://). TCP is used by applications such as web browsers and email. Guaranteed delivery takes longer and is used when it is important to know that the data reached its destination.

For TCP to guarantee delivery, it uses protocols at the Internet layer to establish a session between client and server to verify that communication has taken place. When a TCP message reaches its destination, an acknowledgment is sent back to the source (see [Figure 8-13](javascript://)). If the source TCP does not receive the acknowledgment, it resends the data or passes an error message back to the higher-level application protocol.

**Figure 8-13**

TCP guarantees delivery by requesting an acknowledgment



### UDP Provides Fast Transmissions

On the other hand, [**UDP (User Datagram Protocol)**](javascript://) does not guarantee delivery by first establishing a connection or by checking whether data is received; thus, UDP is called a [**connectionless protocol**](javascript://) or [**best-effort protocol**](javascript://). UDP is used for broadcasting, such as streaming live video or sound over the web, where guaranteed delivery is not as important as fast transmission; however, TCP is preferred for video on demand. UDP is also used to monitor network traffic.

Go to pg.

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

Application Opened

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

## 8-1gTCP/IP Protocols Used by Applications

**A+ Core 1**

* 2.1

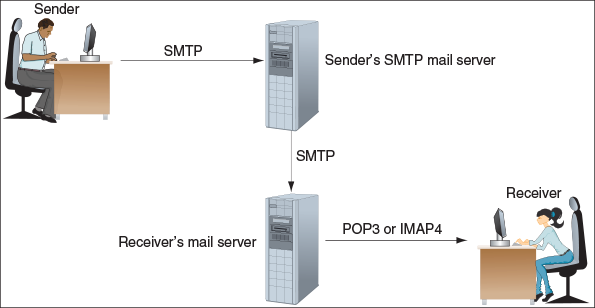
Compare and contrast TCP and UDP ports, protocols, and their purposes.

Some common applications that use the Internet are web browsers, email, chat, FTP, Telnet, Remote Desktop, and Remote Assistance. Here is a bit of information about several of the Application-layer protocols used by these applications and others:

* **HTTP**. [**HTTP (Hypertext Transfer Protocol)**](javascript://) is the protocol used for the World Wide Web and by web browsers and web servers to communicate. You can see when a browser is using this protocol by looking for “http” at the beginning of a URL in the address bar, such as [http://www.microsoft.com](http://www.microsoft.com/" \t "_blank).
* **HTTPS**. [**HTTPS (HTTP secure)**](javascript://) refers to the HTTP protocol working with a security protocol such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to create a secured socket. (TLS is better than SSL.) A **socket** is a connection between a browser and web server. HTTPS is used by web browsers and servers to secure the socket by encrypting the data before it is sent and then decrypting it on the receiving end before the data is processed. To know a secured protocol is being used, look for “https” in the URL, as in [https://www.wellsfargo.com](https://www.wellsfargo.com/" \t "_blank).
* **SMTP**. [**SMTP (Simple Mail Transfer Protocol)**](javascript://) is used to send an email message to its destination (see [Figure 8-14](javascript://)). The email server that takes care of sending email messages (using the SMTP protocol) is often referred to as the SMTP server.
* **POP and IMAP**. After an email message arrives at the destination email server, it remains there until the recipient requests delivery. The recipient’s email server uses one of two protocols to deliver the message: [**POP3 (Post Office Protocol, version 3)**](javascript://) or [**IMAP4 (Internet Message Access Protocol, version 4)**](javascript://). Using POP3, email is downloaded to the client computer and, unless the default setting is changed, the email is then deleted from the email server. Using IMAP4, the client application manages the email while it is still stored on the server.
* **RDP**. [**Remote Desktop Protocol (RDP)**](javascript://) is used by the Windows Remote Desktop and Remote Assistance utilities to connect to and control a remote computer.
* **Telnet**. The [**Telnet**](javascript://) protocol is used by Telnet client/server applications to allow an administrator or other user to control a computer remotely. Telnet is not considered secure because transmissions in Telnet are not encrypted.
* **SSH**. The [**Secure Shell (SSH)**](javascript://) protocol encrypts communications so hackers can’t read the data if they intercept a transmission. SSH is used in various situations for encryption, such as when remotely controlling a computer or when communicating with a web server. SSH is commonly used in Linux to pass sign-in information to a remote computer and control that computer over a network. Because it’s secure, SSH is preferred over Telnet.
* **FTP**. [**FTP (File Transfer Protocol)**](javascript://) is used to transfer files between two computers over a WAN or LAN connection. Web browsers can use the protocol, as can File Explorer in Windows. Also, third-party FTP client software, such as CuteFTP by GlobalSCAPE ([cuteftp.com](http://cuteftp.com/" \t "_blank)) or open source FileZilla ([filezilla-project.org](http://filezilla-project.org/" \t "_blank)), offer additional features. By default, FTP transmissions are not secure. Two protocols that encrypt FTP transmissions are FTPS (FTP Secure), which uses SSL encryption, and SFTP (SSH FTP), which uses SSH encryption.
* **SMB**. [**Server Message Block (SMB)**](javascript://) is a file access protocol originally developed by IBM and used by Windows to share files and printers on a network. The current release of the SMB protocol is SMB 3; older versions include SMB 2 and a spinoff protocol called [**CIFS (Common Internet File System)**](javascript://).
* **AFP**. [**AFP (Apple Filing Protocol)**](javascript://) is a file access protocol used by early editions of the Mac operating system by Apple and is one protocol in the old suite of Apple networking protocols called AppleTalk. (TCP/IP has replaced AppleTalk for most networking protocols in the macOS.) Current macOS releases use SMB 3 for file access, and support both AFP and CIFS for backward compatibility.
* **LDAP**. [**Lightweight Directory Access Protocol (LDAP**](javascript://), often pronounced “l-dap”) is used by various client applications when the application needs to query a database. For example, an email client on a corporate network might query a database that contains the email addresses for all employees, or an application might query a database of printers looking for a printer on the corporate network or the Internet. Data sent and received using the LDAP protocol is not encrypted; therefore, an encryption layer using SSL is sometimes added to LDAP transmissions.
* **SNMP**. [**Simple Network Management Protocol (SNMP)**](javascript://) is a versatile protocol used to monitor network traffic and manage network devices. It can help create logs for monitoring device and network performance, it can make some automatic changes to devices being monitored, and it can be used to alert network technicians when a bottleneck or other performance issues are causing problems on the network. The SNMP server is called the manager, and a small application called an agent is installed on devices being managed by SNMP.

**Figure 8-14**

The SMTP protocol is used to send email to a recipient’s mail server, and the POP3 or IMAP4 protocol is used by the client to receive email



Enlarge Image

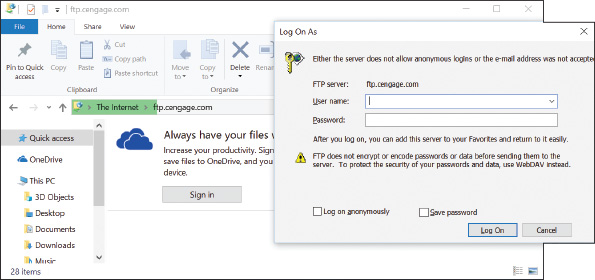
**Applying Concepts**

### File Explorer and FTP

To use FTP in File Explorer, enter the address of an FTP site in the address bar—for example, ftp.cengage.com. A logon dialog box appears where you can enter a user name and password (see [Figure 8-15](javascript://)). When you click **Log On**, you can see folders on the FTP site and the FTP protocol displays in the address bar, as in The Internet > ftp.cengage.com. You can copy and paste files and folders between your computer and the FTP server.

**Figure 8-15**

Log on to an FTP site



Enlarge Image

Recall that client/server applications use ports to address each other. [Table 8-5](javascript://) lists the port assignments for common applications.

**Table 8-5**

### Common TCP/IP Port Assignments for Client/Server Applications

|  |  |  |
| --- | --- | --- |
| **Port** | **Protocol and Role** | **Description** |
| 20 | FTP client | The FTP client receives data on port 20 from the FTP server. |
| 21 | FTP server | The FTP server listens on port 21 for commands from an FTP client. |
| 22 | SSH server | A server using the SSH protocol listens at port 22. |
| 23 | Telnet server | A Telnet server listens at port 23. |
| 53 | DNS server | A DNS server listens at port 53. |
| 67 | DHCP server | A DHCP server listens on port 67. |
| 68 | DHCP client | A DHCP client receives messages on port 68. |
| 80 | Web server using HTTP | A web server listens at port 80 when receiving HTTP requests. |
| 443 | Web server using HTTPS | A web server listens at port 443 when receiving HTTPS transmissions. |
| 25 | SMTP email server | An email server listens at port 25 to receive email from an email client. |
| 465 | SMTP secure | An email client sends secured email to an SMTP server listening at port 465. SMTP secure is also known as SMTPS and uses SSL/TLS to secure transmissions. |
| 110 | POP3 email server | An email client requests email from a POP3 server listening at port 110. |
| 995 | POP3 secure | An email client requests secured email from a POP3 server listening at port 995. POP3 secured is also known as POP3S and uses SSL/TLS to secure transmissions. |
| 143 | IMAP email server | An email client requests email from an IMAP server listening at port 143. |
| 993 | IMAP secure | An email client requests secured email from an IMAP server listening at port 993. IMAP secure is also known as IMAPS and uses SSL/TLS to secure transmissions. |
| 137, 138, and 139 | SMB over NetBIOS | [**NetBIOS**](javascript://) is a legacy suite of protocols used by Windows before TCP/IP. To support legacy NetBIOS applications on a TCP/IP network, Windows offers **[NetBT (NetBIOS over TCP/IP)](javascript://)**. Earlier versions of SMB required NetBT to be enabled. Ports used on these networks are:   * SMB over UDP uses ports 137 and 138. * SMB over TCP uses ports 137 and 139.   Current versions of SMB don’t require NetBT. |
| 445 | SMB direct over TCP/IP | SMB 3, SMB 2, and closely related CIFS use port 445 for both TCP and UDP traffic. |
| 161 | SNMP agent | An SNMP-managed device receives requests from the manager on port 161. |
| 162 | SNMP manager | An SNMP manager listens on port 162. |
| 389 | LDAP | A database or directory service listens at port 389 for LDAP communication from a client. LDAP (or its secure version, LDAPS, at port 636) is often used for network authentication services. |
| 427 | SLP and AFP | [**Service Location Protocol (SLP)**](javascript://) uses port 427 to find printers and file sharing devices on a network. AFP relies on SLP and port 427 to find resources on a local network. |
| 548 | AFP | AFP over TCP/IP is used for file sharing and file services. |
| 3389 | RDP apps, including Remote Desktop and Remote Assistance | Remote Desktop and Remote Assistance services listen at port 3389. |

Enlarge Table

**A+ Exam Tip**

The A+ Core 1 exam expects you to know the common port assignments of the FTP, SSH, Telnet, SMTP, DNS, HTTP, POP3, IMAP, HTTPS, RDP, NetBIOS, SMB, CIFS, SLP, AFP, DHCP, LDAP, and SNMP protocols, and to understand the purposes of these protocols. Before sitting for this exam, be sure to memorize the ports listed in Table 8-5. You also might be given a scenario that requires you to put this information to use.

As you work with network connections, keep in mind that the connections must work at all layers. When things don’t work right, it helps to understand that you must solve the problem at one or more layers. In other words, the problem might be with the NIC, with the OS or application on the host, or with a router or other device on the local or remote network.

Now that you have an understanding of TCP/IP and Windows networking, let’s apply that knowledge to manage, set up, and troubleshoot networks.

Go to pg.

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

Application Opened

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

**8-2**Local Network Infrastructure

**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.

* 2.5

Summarize the properties and purposes of services provided by networked hosts.

* 3.1

Explain basic cable types, features, and their purposes.

In this part of the chapter, you learn about the hardware devices that create and connect to networks. We discuss desktop and laptop devices, hubs, switches, bridges, and other network devices, and the cables and connectors these devices use.

Go to pg.

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

Application Opened

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

## 8-2aSwitches and Hubs

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

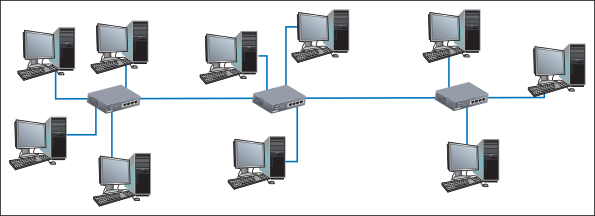
* 2.3

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

Today’s Ethernet networks use a design called a star bus topology, which means that nodes are connected to one or more centralized devices, which are connected to each other (see [Figure 8-16](javascript://)). A centralized device can be a switch or a hub. Each of these devices handles a network message differently.

**Figure 8-16**

A star bus network formed by nodes connected to multiple switches



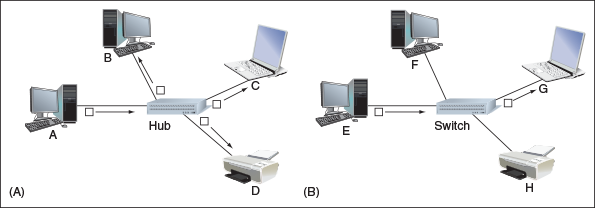
Enlarge Image

Here are the differences between a hub and a switch:

* An Ethernet [**hub**](javascript://) transmits the message to every device except the device that sent the message, as shown in [Figure 8-17A](javascript://). A hub is just a pass-through and distribution point for every device connected to it, without regard for what kind of data is passing through and where the data might be going. Hubs are outdated technology, having been replaced by switches. [Figure 8-18](javascript://) shows a hub that supports 10-Mbps and 100-Mbps Ethernet speeds. (You can’t find hubs these days to support faster networks.)

**Figure 8-17**

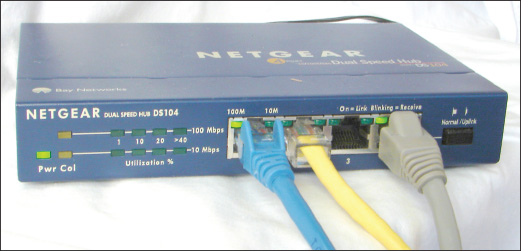
(A) A hub is a simple pass-through device to connect nodes on a network, and (B) a switch sends a message to the destination node based on its MAC address



Enlarge Image

**Figure 8-18**

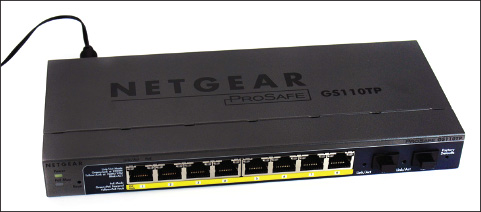
This hub supports 10-Mbps and 100-Mbps Ethernet speeds



* A **switch** (see [Figure 8-19](javascript://)) is smarter and more efficient than a hub because it keeps a table of all the MAC addresses for devices connected to it. When the switch receives a message, it searches its MAC address table for the destination MAC address of the message and sends the message only to the interface for the device using this MAC address (see [Figure 8-17B](javascript://)). At first, a switch does not know the MAC addresses of every device connected to it. It learns this information as it receives messages and records each source MAC address in its MAC address table. When it receives a message destined to a MAC address not in its table, the switch acts like a hub and broadcasts the message to all devices except the one that sent it.

**Figure 8-19**

This Gigabit Ethernet switch by NETGEAR has eight Ethernet ports

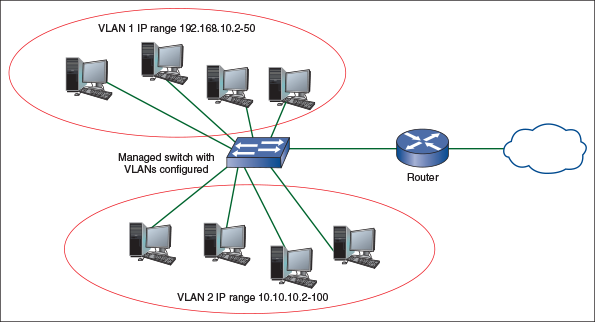


Two types of switches are managed and unmanaged switches. An [**unmanaged switch**](javascript://) requires no setup or configuration other than connecting network cables to its ports. It does not require an IP address and is appropriate for SOHO networks. A [**managed switch**](javascript://) has firmware that can be configured to monitor and manage network traffic. It’s appropriate for larger networks and can be used to manage QoS for prioritizing network traffic and to control speeds for specific ports.

You can also use a managed switch to subnet a large LAN into smaller subnets called [**virtual LANs (VLANs)**](javascript://), which can reduce network traffic. Subnetting is done by assigning a group of ports on the switch to a different VLAN and directing the router as a DHCP server to assign a unique range of IP addresses to each VLAN to create a subnet. In [Figure 8-20](javascript://), the one physical LAN is subnetted into two virtual LANs. With subnetting, broadcast traffic is reduced because it is limited to each VLAN. The firmware on a managed switch is accessed through a browser using the switch’s IP address, which is similar to how you access the firmware on a router. A switch requires an IP address only for the purpose of accessing its firmware.

**Figure 8-20**

Ports on a managed switch can be assigned to a VLAN to subnet a network



Enlarge Image

Here are reasons you might add switches to your network:

* **To add network connections**. A SOHO router usually has four to eight ports in a built-in switch. When you need more connections, add a switch in a location where you have multiple workstations or printers that need to connect to the network. In practice, a small network might begin as one switch and three or four computers. As the need for more computers grows, new switches are added to provide these extra connections.
* **To regenerate the network signal**. An Ethernet cable should not exceed 100 meters (about 328 feet) in length. If you need to reach distances greater than that, you can add a switch in the line, which regenerates the signal.
* **To manage network traffic**. Managed switches can be installed in strategic places on the network to subnet the network and manage network traffic to improve performance.

[Figure 8-16](javascript://), shown earlier in the chapter, uses three switches in sequence. Physically, the network cables that run between two switches or between a switch and a computer might be inside a building’s walls, with a network jack on the wall providing an RJ-45 connector. You plug a network cable into the jack 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)

## 8-2bWireless Access Points and Bridges

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

You’ve already learned that a router can also be a wireless access point. In addition, a wireless access point can be a dedicated device. The wireless access point can also serve as a bridge, as shown in [Figure 8-21](javascript://). A [**bridge**](javascript://) is a device that stands between two segments of a network and manages network traffic between them. For example, one network segment might be a wireless network and the other segment might be a wired network; the wireless access point (AP) connects these two segments. Functioning as a bridge, the AP helps to reduce the overall volume of network traffic by not allowing messages across the bridge if it knows that the messages are addressed to a destination on its own segment. [Figure 8-22](javascript://) demonstrates the concept of a network bridge. (Logically, you can think of a switch as a multiport bridge.)

**Figure 8-21**

A ceiling-mount wireless access point by TP-Link



**Figure 8-22**

A bridge is an intelligent device that makes decisions concerning network traffic



Enlarge Image

Similar to a switch, a bridge at first doesn’t know which nodes are on each network segment. It learns that information by maintaining a table of MAC addresses from information it collects from each message that arrives at the bridge. Eventually, it learns which nodes are on which network segment and becomes more efficient at preventing messages from getting on the wrong segment, which can bog down network traffic.

**Notes**

If your wireless access point does not reach the entire area you need to cover, you can add a [**repeater**](javascript://) or an extender, which amplifies and retransmits the signal to a wider coverage area. Repeaters and extenders capture the Wi-Fi signal, boost it, and retransmit it to the new area. The difference between a repeater and an extender is that a repeater rebroadcasts the signal using a new network name, whereas an extender keeps the original network name.

**A+ Exam Tip**

The A+ Core 1 exam expects you to know the functions and features of a hub, switch, router, access point, bridge, repeater, firewall, and modem.

Go to pg.

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

Application Opened

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

## 8-2cNetwork Servers

**A+ Core 1**

* 2.5

Summarize the properties and purposes of services provided by networked hosts.

Recall that a client computer contacts a server in order to request information or perform a task, such as when a web browser connects with a web server and requests a webpage. Many other types of server resources exist on a typical network. Some of these servers are stand-alone devices, but often multiple network services are provided by a single server computer, or servers might be embedded in other devices. For example, servers are sometimes embedded in router firmware (such as a SOHO router providing DHCP services) or in an operating system (such as web server capabilities embedded in Windows Server). On large networks, network services are often provided by multiple servers so that if one goes down, others can fill in the gap. This is called redundancy. It adds reliability but also adds complexity. Each time any of these components is updated, any legacy technology present on the network must be taken into consideration, which can result in a complex web of network server resources. Here’s a brief list of several popular client/server resources used on networks and the Internet:

* **Web server**. A web server serves up webpages to clients. Many corporations have their own web servers, which are available privately on the corporate network. Other web servers are public, accessible from anywhere on the Internet. The most popular web server application is Apache (see [apache.org](http://apache.org/" \t "_blank)), which primarily runs on UNIX or Linux systems and can also run on Windows. The second most popular web server is Internet Information Services (IIS), which is embedded in the Windows Server operating system.
* **Mail server**. Email is a client/server application that involves two mail servers. Recall that SMTP is used to send email messages, and either POP3 or IMAP4 is used to deliver an email message to a client. An example of a popular email server application is Microsoft Exchange Server. Outlook, an application in the Microsoft Office suite of applications, is a popular email client application.
* **File server**. A [**file server**](javascript://) stores files and makes them available to other computers. A network administrator can make sure this data is backed up regularly and kept secure.
* **Print server**. A [**print server**](javascript://) manages network printers and makes them available to computers throughout the network. Expensive network printers can handle high-capacity print jobs from many sources, eliminating the need for a desktop printer at each workstation. If a network printer fails, a technician can sometimes diagnose and solve the problem from her workstation. Windows business and professional versions include the Print Management console for this purpose.
* **DHCP server**. Recall from [Chapter 7](javascript://) that a DHCP server leases an IP address to a computer when it first attempts to initiate a connection to the network and requests an IP address. The DHCP server is configured to pull from a range of IP addresses, which is called the DHCP scope.
* **DNS server**. DNS servers, as you’ve learned, store domain names and their associated IP addresses for computers on the Internet or a large enterprise network. DNS servers are responsible for name resolution, which happens when a client computer sends an FQDN (fully qualified domain name) to a DNS server and requests the IP address associated with this character-based name.

**Notes**

A telltale sign that the network’s DNS server is malfunctioning is when you can reach a website by its IP address, but not by its FQDN.

* **Proxy server**. A [**proxy server**](javascript://) is a computer that intercepts requests that a client, such as a browser, makes of another server, such as a web server. The proxy server substitutes its own IP address for the request using NAT protocols. It might also store data that is used frequently by its clients. An example of using a proxy server is when an ISP caches webpages to speed up requests for the same pages. After it caches a page and another browser requests the same content, the proxy server can provide the content that it has cached. In addition, a proxy server sometimes acts as a router to the Internet, a firewall to protect the network, a filter for email, and to restrict Internet access by employees to prevent them from violating company policies.
* **Authentication server**. An [**authentication server**](javascript://) authenticates users or computers to the network so that they can access network resources. Active Directory, which is a directory service included in Windows Server, is often used for this purpose on a Windows domain. The authentication server stores user or device credentials such as user names and passwords, validates an authentication request, and determines the permissions assigned to each user, device, or group.
* **Syslog server**. [**Syslog**](javascript://) is a protocol that gathers event information about various network devices, such as errors, failures, maintenance tasks, and users logging in or out. The messages about these events are sent to a central location called a [**Syslog server**](javascript://), which collects the events into a database. Some Syslog servers can generate alerts or notifications to inform network administrators of problems that might need attention.

Go to pg.

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

Application Opened

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

## 8-2dUnified Threat Management (UTM) Appliance

**A+ Core 1**

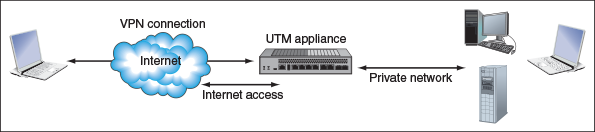
* 2.5

Summarize the properties and purposes of services provided by networked hosts.

Recall that a router stands between the Internet and a private network to route traffic between the two networks. It can also serve as a firewall to protect the network. A [**next-generation firewall (NGFW)**](javascript://) combines firewall functions with antivirus/anti-malware functions and perhaps other functions as well. NGFW components might be installed on a dedicated appliance, a router, servers, or even in the cloud. In addition, an NGFW device can offer comprehensive [**Unified Threat Management (UTM)**](javascript://) services. A UTM appliance, also called a security appliance, network appliance, or Internet appliance, stands between the Internet and a private network, as does a router, and protects the network (see [Figure 8-23](javascript://)).

**Figure 8-23**

A UTM appliance is considered a next-generation firewall that can protect a private network



Enlarge Image

A UTM appliance might offer these types of protections and services:

* **Firewall.** The firewall software filters incoming and outgoing network traffic according to IP addresses, ports, the type of messages the traffic contains, and how the message was initiated.
* **Antivirus and anti-malware software.** This software is usually much more advanced than what might be installed on a server or workstation.
* **Identity-based access control lists.** These lists control access of users or user groups and can log and report activity of these users and groups to reveal misuse, data leaks, or unauthorized access to resources. The company can use this feature to satisfy legal auditing requirements for detecting and controlling data leaks.
* **Intrusion detection system.** An [**intrusion detection system (IDS)**](javascript://) monitors all network traffic and creates alerts when suspicious activity happens. IDS software can run on a UTM appliance, router, server, or workstation.
* **Intrusion prevention system.** An [**intrusion prevention system (IPS)**](javascript://) not only monitors and logs suspicious activity, it can prevent the threatening traffic from burrowing into the system.
* **Endpoint management server.** Also called an endpoint security management system, an [**endpoint management server**](javascript://) provides monitoring of various [**endpoint devices**](javascript://) on the network, from computers and laptops to mobile devices like smartphones, tablets, or even barcode readers. The service can ensure that endpoints are kept up to date with current anti-malware requirements, operating system patches, and application updates. The system will restrict the device’s access to the network until that device meets the security requirements, which gives an additional layer of protection to other network resources.
* **VPN.** The appliance can provide a VPN (virtual private network) to remote users of the network. You learned how to create a VPN connection in [Chapter 7](javascript://).

[Figure 8-24](javascript://) shows a UTM appliance by NETGEAR.

**Figure 8-24**

The ProSECURE UTM appliance by NETGEAR



Source: [Fortinet.com](http://fortinet.com/" \t "_blank)

**A+ Exam Tip**

The A+ Core 1 exam expects you to be able to summarize the purposes of services provided by a UTM Internet appliance, including an IDS, IPS, and endpoint management server.

Go to pg.

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

Application Opened

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

## 8-2eEthernet Cables and Connectors

**A+ Core 1**

* 3.1

Explain basic cable types, features, and their purposes.

Several variations of Ethernet cables and connectors have evolved over the years. They are primarily identified by their speeds and the types of connectors used to wire the networks. [Table 8-6](javascript://) compares cable types and Ethernet versions.

**A+ Exam Tip**

The A+ Core 1 exam expects you to know the details listed in [Table 8-6](javascript://). Given a scenario, you need to recognize that when a cable exceeds its recommended maximum length, limited connectivity problems can result.

**Table 8-6**

### Variations of Ethernet and Ethernet Cabling

| **Cable System** | **Speed** | **Cables and Connectors** | **Example of Connectors** | **Maximum Cable Length** |
| --- | --- | --- | --- | --- |
| 10Base2 (ThinNet) | 10 Mbps | Coaxial cable, an older cable typically used for cable TV, uses a **BNC connector**. | Source: Courtesy of [Cables4Computer.com](http://cables4computer.com/" \t "_blank) | 185 meters or 607 feet |
| 10BaseT, 100BaseT (Fast Ethernet), 1000BaseT (Gigabit Ethernet), and 10GBaseT (10-Gigabit Ethernet) | 10 Mbps, 100 Mbps, 1 Gbps, or 10 Gbps | Twisted-pair (UTP or STP) uses an RJ-45 connector. | Source: Courtesy of Tyco Electronics | 100 meters or 328 feet |
| 100BaseFL, 100BaseFX, 1000BaseFX, or 1000BaseX (fiber optic) | 100 Mbps, 1 Gbps, or 10 Gbps | Fiber-optic cable uses ST or SC connectors (shown to the right) or LC and MT-RJ connectors (not shown). | Source: Courtesy of Black Box Corporation | Up to 2 kilometers (6562 feet) |

### Ethernet Standards and Cables

Ethernet can run at four speeds. Each version of Ethernet can use more than one cabling method. Here is a brief description of the transmission speeds and the cabling methods they use:

* **10-Mbps Ethernet.** This first Ethernet specification was invented by Xerox Corporation in the 1970s, and later became known as Ethernet.
* **100-Mbps Ethernet or Fast Ethernet.** This improved version of Ethernet, called [**Fast Ethernet**](javascript://), operates at 100 Mbps and typically uses copper cabling rated CAT-5 or higher. Fast Ethernet networks can support slower speeds of 10 Mbps so devices that run at either 10 Mbps or 100 Mbps can coexist on the same LAN.
* **1000-Mbps Ethernet or Gigabit Ethernet.** This version of Ethernet operates at 1000 Mbps (1 Gbps) and uses twisted-pair cable and fiber-optic cable. [**Gigabit Ethernet**](javascript://) is becoming the most popular choice for LAN technology. Because it can use the same cabling and connectors as Fast Ethernet, a company can upgrade from Fast Ethernet to Gigabit without rewiring the network.
* **10-Gigabit Ethernet.** This version of Ethernet operates at 10 billion bits per second (10 Gbps) and typically uses fiber-optic cable. It can be used on LANs, MANs, and WANs, and is also a good choice for network backbones. (A network backbone is a channel whereby local networks can connect to wide area networks or to each other.)

### Twisted-Pair Cable

As you can see from [Table 8-6](javascript://), the three main types of cabling used by Ethernet are twisted-pair, coaxial, and fiber optic. [**Twisted-pair cabling**](javascript://) uses pairs of wires twisted together to reduce crosstalk, which is interference that degrades a signal on the wire. It’s the most popular cabling method for local networks and uses an RJ-45 connector. The cable comes in two varieties: [**unshielded twisted-pair (UTP) cable**](javascript://) and [**shielded twisted-pair (STP) cable**](javascript://). UTP cable is less expensive than STP and is commonly used on LANs. STP cable uses a covering or shield around each pair of wires inside the cable that protects it from electromagnetic interference caused by electrical motors, transmitters, or high-tension lines. It costs more than unshielded cable, so it’s used only when the situation demands it. Twisted-pair cable is rated by category (cat), as listed in [Table 8-7](javascript://).

**Table 8-7**

### Twisted-Pair Categories

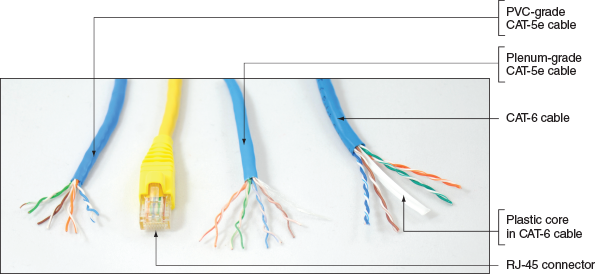
| **Twisted-Pair Category** | **Cable System** | **Frequency** | **Shielded or Unshielded** | **Comment** |
| --- | --- | --- | --- | --- |
| [**CAT-5**](javascript://) | 10/100BaseT | Up to 100 MHz | Either | Has two wire pairs and is seldom used today |
| [**CAT-5e**](javascript://) (Enhanced) | 10/100BaseT, Gigabit Ethernet | Up to 350 MHz | Either | Has four twisted pairs and a heavy-duty sheath to help reduce crosstalk |
| [**CAT-6**](javascript://) | 10/100BaseT, Gigabit Ethernet, 10Gig Ethernet at shorter distances | Up to 250 MHz | Either | Less crosstalk because it has a plastic core that keeps the twisted pairs separated |

Enlarge Table

[Figure 8-25](javascript://) shows unshielded twisted-pair cables and the RJ-45 connector. Twisted-pair cable has four pairs of twisted wires for a total of eight wires. You learn more about how the eight wires are arranged later in this chapter.

**Figure 8-25**

Unshielded twisted-pair cables and an RJ-45 connector used for local wired networks



Enlarge Image

**Notes**

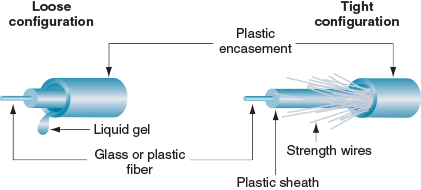
Normally, the plastic covering of a cable is made of [**PVC (polyvinyl chloride)**](javascript://), which is not safe when used inside [**plenums**](javascript://) (areas between the floors of buildings). In these situations, plenum cable covered with Teflon is used because it does not give off toxic fumes when burned. Plenum cable is two or three times more expensive than PVC cable. [Figure 8-25](javascript://) shows plenum cable and PVC cable. Because they can look essentially the same, check for labels printed on the cable to determine whether it’s PVC or plenum-rated.

### Fiber Optic

Fiber-optic cables transmit signals as pulses of light over glass or plastic strands inside protective tubing, as illustrated in [Figure 8-26](javascript://). Fiber-optic cable comes in two types: single-mode (thin, difficult to connect, expensive, and best performing) and multimode (most popular). A single-mode cable uses a single path for light to travel through it and multimode cable uses multiple paths for light. Both single-mode and multimode fiber-optic cables can be constructed as loose-tube cables for outdoor use or tight-buffered cables for indoor or outdoor use. Loose-tube cables are filled with gel to prevent water from soaking into the cable, and tight-buffered cables are filled with synthetic or glass yarn, called strength wires, to protect the fiber-optic strands, as shown in [Figure 8-26](javascript://).

**Figure 8-26**

Fiber-optic cables contain a glass or plastic core for transmitting light



**A+ Exam Tip**

The A+ Core 1 exam expects you to know about these cables and connectors: BNC, RJ-45, RJ-11, coaxial, Ethernet, STP, UTP, CAT-5, CAT-5e, CAT-6, plenum, and fiber.

Go to pg.

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

Application Opened

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

## 8-2fPowerline Networking or Ethernet over Power (EoP)

**A+ Core 1**

* 2.2

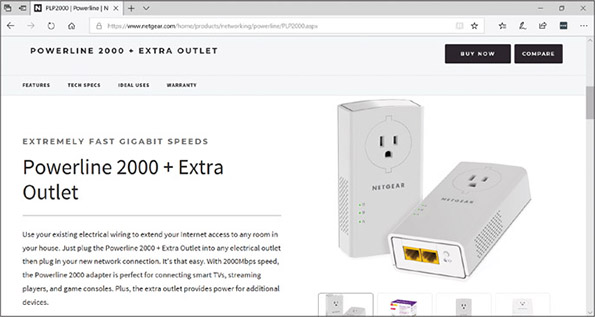
Compare and contrast common networking hardware devices.

If you need network access to a remote location in a building where network cabling and Wi-Fi cannot reach, you have another option. The HomePlug standard introduced in 2001, called [**powerline networking**](javascript://) or [**Ethernet over Power (EoP)**](javascript://), uses power lines in a building to transmit data. Powerline networking is simple to set up, inexpensive, and can run at Gigabit speeds. Like Wi-Fi, the data is sent out on a network that you cannot necessarily contain because power lines are not confined to a single building. If a building or apartment is sharing a phase (electrical signal) with another building or apartment, the data might leak and be intercepted by a neighbor. For this reason, powerline adapters offer 128-bit AES encryption that is activated by pairing the adapters to each other. Alternately, you can install the manufacturer’s utility on your computer to create a network key.

To use powerline networking, you need at least two powerline adapters (see [Figure 8-27](javascript://)), which can be bought in pairs called a kit.

**Figure 8-27**

A starter kit for powerline networking includes two adapters



Enlarge Image

Source: [NETGEAR.com](http://netgear.com/" \t "_blank)

Powerline networks are not without problems. Consider the following issues powerline networking presents:

* Powerline adapters must be plugged directly into a wall outlet. Plugging a powerline adapter into a power strip or surge protector or sharing an outlet with an energy hog like a space heater hinders the function of the device.
* Powerline adapters might be large and cover both outlets on a single wall plate. A few powerline adapters offer a pass-through outlet, but most do not.
* Sometimes people forget to use the encryption options and end up with an unsecured network.
* Distance degrades quality. If you have a map of the building’s circuits, try to keep the two adapters as close on the same circuit as possible. Jumping circuits decreases signal strength.

When shopping for powerline adapters, consider these things:

* Most powerline manufacturers belong to the HomePlug Alliance group ([homeplug.org](http://homeplug.org/" \t "_blank)). Make sure the adapter you are considering is HomePlug certified.
* Make sure the adapter is rated for the latest HomePlug AV2 speed standard for Gigabit-class data transfers.
* If you have limited wall outlets, you might need a powerline adapter that offers a pass-through outlet.

Go to pg.

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

Application Opened

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

## 8-2gPower over Ethernet (PoE)

**A+ Core 1**

* 2.2

Compare and contrast common networking hardware devices.

If you have the opposite problem of needing to get power where your network cabling has gone, you can use **Power over Ethernet (PoE)**, a feature that might be available on high-end wired network adapters to allow power to be transmitted over Ethernet cable. Using this feature, you can place a wireless access point, webcam, IP phone, or other device that needs power in a position in a building where you don’t have an electrical outlet. The Ethernet cable to the device provides both power and data transmissions. PoE can provide up to 25.5 W from a single Ethernet port, although the amount of power that reaches a device degrades with the length of the cable. Most high-quality switches provide PoE. If your switch doesn’t offer PoE, you can attach a [**PoE injector**](javascript://) (see [Figure 8-28](javascript://)), which adds power to an Ethernet cable.

**Figure 8-28**

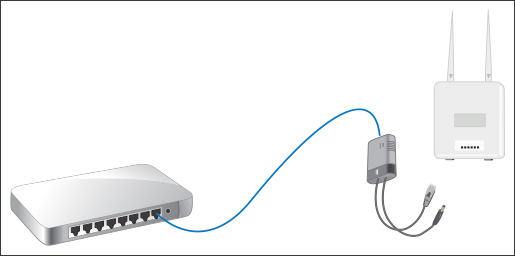
A PoE injector introduces power to an Ethernet cable



Some devices, such as a webcam, are designed to receive both power and data from the Ethernet cable. For other devices, you must use a splitter that splits the data and power transmissions before connecting to the non-PoE device. [Figure 8-29](javascript://)shows a PoE switch and a splitter used to provide power to a non-PoE access point. When setting up a device to receive power by PoE, make sure the device sending the power, the splitter, and the device receiving the power are all compatible. Pay special attention to the voltage and wattage requirements and the type of power connector of the receiving device.

**Figure 8-29**

Use a PoE splitter if the receiving device is not PoE compatible



Go to pg.

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

Application Opened

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

**8-3**Setting Up and Troubleshooting Network Wiring

**A+ Core 1**

* 2.3

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

* 2.8

Given a scenario, use appropriate networking tools.

* 3.1

Explain basic cable types, features, and their purposes.

In [Chapter 7](javascript://) you learned to configure a workstation and SOHO router to create a small network and connect it to a device (for example, a DSL or cable modem) that provides Internet access. If your network is not strictly a wireless network, you also need cabling and perhaps one or more switches to create a wired network. This section covers what you need to know to set up and troubleshoot a wired network.

Go to pg.

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

Application Opened

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

## 8-3aDesigning a Wired Network

**A+ Core 1**

* 2.3

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

Begin your network design by deciding where to place your router. If the router is also your wireless access point, take care in where you place it. Recall from [Chapter 7](javascript://) that a wireless access point should be placed near the center of the area where you want your wireless hotspot to maximize its range for users and minimize your Wi-Fi network’s exposure to unauthorized users outside your building. The router also needs to have access to your cable modem or DSL modem. The modem needs access to the cable TV or phone jack where it receives service. For a business, the router, modem, and servers are often placed in an electrical closet that can be locked for security and additional wireless access points are placed where hotspots are needed. Next, consider where the wired workstations will be placed. Position switches in strategic locations to provide extra network drops to multiple workstations.

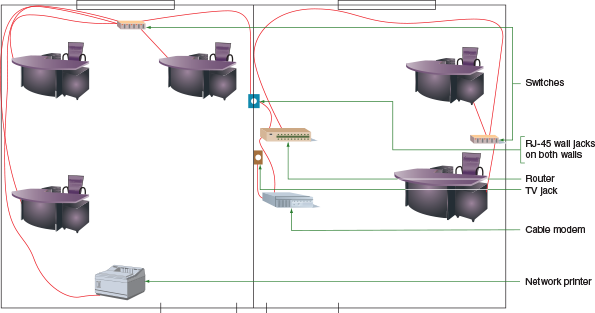
Some network cables might be wired inside walls of your building with wall jacks that use RJ-45 ports. These cables might converge in an electrical closet or server room to connect to switches. If network cables are lying on the floor, be sure to install them against the wall so they won’t be a trip hazard. To get the best performance from your network, follow these tips:

* Make sure cables don’t exceed the recommended length (100 meters for twisted pair).
* Use twisted-pair cables rated at CAT-5e or higher. (CAT-6 gives better performance than CAT-5e for Gigabit Ethernet, but it’s harder to wire and more expensive.)
* Use switches rated at the same speed as your router and network adapters.
* For Gigabit speed on the entire network, use all Gigabit switches, network adapters, and router. However, if some devices run at slower speeds, most likely a switch or router can still support the higher speeds for other devices on the network.

[Figure 8-30](javascript://) shows a possible inexpensive wiring job where two switches and a router are used to wire two rooms for five workstations and a network printer. The only inside-wall wiring that is required is two back-to-back RJ-45 wall jacks on either side of the wall between the two rooms. The plan allows for all five desktop computers and a network printer to be wired with cabling neatly attached to the baseboards of the office without being a trip hazard.

**Figure 8-30**

Plan the physical configuration of a small network



Enlarge Image

Now let’s look at the tools you need to solve problems with network cabling, the details of how a network cable is wired, and how you can create your own network cables by installing RJ-45 connectors on twisted-pair cables.

Go to pg.

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

Application Opened

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

## 8-3bTools Used by Network Technicians

**A+ Core 1**

* 2.8

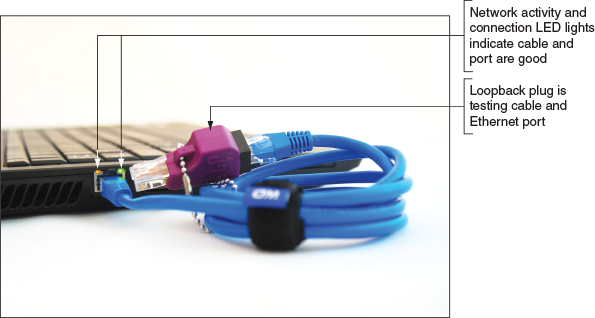
Given a scenario, use appropriate networking tools.

Here’s a list of tools a network technician might want in his or her toolbox:

* **Loopback plug.** A loopback plug can be used to test a network cable or port. To test a port, insert the loopback plug into the port; to test a cable, connect one end of the cable to a network port on a computer or other device, and connect the loopback plug to the other end of the cable (see [Figure 8-31](javascript://)). If the LED lights on the network port light up, the cable and port are good. Another way to use a loopback plug is to find out which port on a switch in an electrical closet matches up with a wall jack. Plug the loopback plug into the wall jack. The connecting port on the switch in the closet lights up. When buying a loopback plug, pay attention to the Ethernet speeds it supports. Some only support 100 Mbps; others support 100 Mbps and 1000 Mbps.

**Figure 8-31**

A loopback plug verifies that the cable and network port are good



Enlarge Image

* **Cable tester.** A [**cable tester**](javascript://) is used to determine if a cable is good or to find out what type it is if the cable is not labeled. You can also use a cable tester to locate the ends of a network cable in a building. A cable tester has two components, the remote and the base (see [Figure 8-32](javascript://)).

**Figure 8-32**

Use a cable tester pair to determine the type of cable and/or if the cable is good



Enlarge Image

To test a cable, connect each component to the ends of the cable and turn on the tester. Lights on the tester will show you if the cable is good and what type of cable you have. You’ll need to read the user manual that comes with the cable tester to know how to interpret the lights.

You can also use the cable tester to find the two ends of a network cable installed in a building. Suppose you see several network jacks on walls in a building, but you don’t know which jacks connect back to the switch. Install a short cable in each of the two jacks or a jack and a port in a patch panel. A [**patch panel**](javascript://) (see [Figure 8-33](javascript://)) provides multiple network ports for cables that converge in one location such as an electrical closet or server room. Each port is numbered on the front of the panel. Use the cable tester base and remote to test the continuity between remote wall jacks and ports in the patch panel, as shown in [Figure 8-34](javascript://). Whereas a loopback plug works with live cables and ports, a cable tester works on cables that are not live. You might damage a cable tester if you connect it to a live circuit, so before you start connecting the cable tester to wall jacks, be sure that you turn off all devices on the network.

**Figure 8-33**

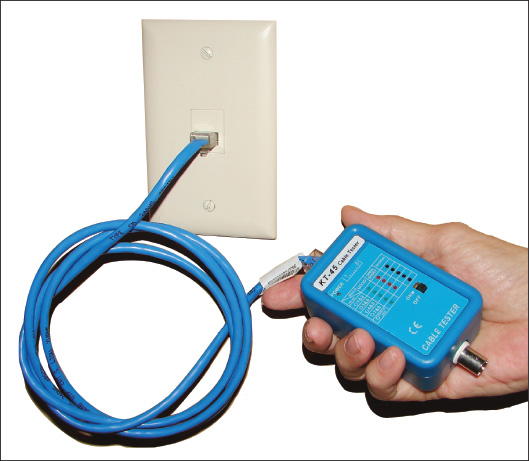
A patch panel provides Ethernet ports for cables converging in an electrical closet



Source: Courtesy of Tripp Lite

**Figure 8-34**

Use cable testers to find the two ends of a network cable in a building



* **Network multimeter.** You’ve already learned about multimeters. A [**network multimeter**](javascript://) (see [Figure 8-35](javascript://)) is a multifunctional tool that can test cables, ports, and network adapters. When you connect it to your network, it can also detect the Ethernet speed, duplex status, default router on the network, lengths of cables, voltage levels of PoE, and other network statistics and details. Many network multimeters can document test results and upload results to a computer. Good network multimeters can cost several hundred dollars.

**Figure 8-35**

The LinkRunner Pro network multimeter by Fluke Corporation works on Gigabit Ethernet networks using twisted-pair copper cabling



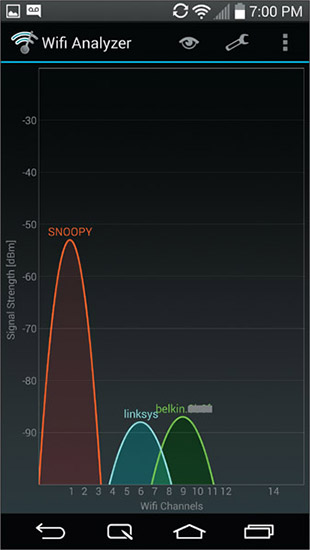
Enlarge Image

Source: Courtesy of Fluke Corporation

* **Wi-Fi analyzer.** A [**Wi-Fi analyzer**](javascript://) is software that can find Wi-Fi networks, determine signal strengths, help optimize Wi-Fi signal settings, and help identify Wi-Fi security threats. For example, you can use a Wi-Fi analyzer to find out which Wi-Fi channels are being used before you pick your channels. You can turn your smartphone into a Wi-Fi analyzer by installing a free or inexpensive app through your phone’s app store (see [Figure 8-36](javascript://)).

**Figure 8-36**

This Wi-Fi Analyzer app detected three wireless networks



Enlarge Image

Source: Wi-Fi Analyzer app for Android

* **Toner probe.** A [**tone generator and probe**](javascript://), sometimes called a [**toner probe**](javascript://), is a two-part kit that is used to find cables in the walls of a building. See [Figure 8-37](javascript://). The toner connects to one end of the cable and puts out a continuous or pulsating tone on the cable. While the toner is putting out the tone, you use the probe to search the walls for the tone. The probe amplifies the tone so you hear it as a continuous or pulsating beep. The beeps get louder when you are close to the cable and weaker when you move the probe away from the cable. With a little patience, you can trace the cable through the walls. Some toners can put out tones up to 10 miles on a cable and offer a variety of ways to connect to the cable, such as clips and RJ-45 and RJ-11 connectors.

**Figure 8-37**

A toner probe kit by Fluke Corporation

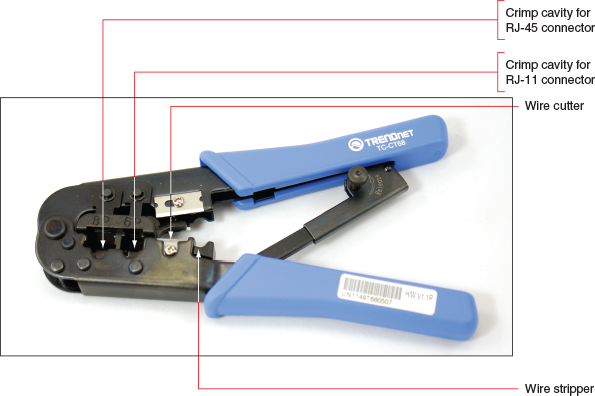


Enlarge Image

* **Cable stripper.** A [**cable stripper**](javascript://) is used to build your own network cable or repair a cable. Use the cable stripper to cut away the plastic jacket or coating around the wires inside a twisted-pair cable so that you can install a connector on the end of the cable. How to use cable strippers is covered later in the chapter.
* **Crimper.** A [**crimper**](javascript://) is used to attach a terminator or connector to the end of a cable. It applies force to pinch the connector to the wires in the cable to securely make a solid connection. [Figure 8-38](javascript://) shows a multifunctional crimper that can crimp an RJ-45 or RJ-11 connector. It also serves double duty as a wire cutter and wire stripper.

**Figure 8-38**

This crimper can crimp RJ-45 and RJ-11 connectors



Enlarge Image

* **Punchdown tool.** A **[punchdown tool](javascript://)** (see [Figure 8-39](javascript://)) is used to punch individual wires in a network cable into their slots in a keystone RJ-45 jack that is used in an RJ-45 wall jack. In a project at the end of this chapter, you practice using the tool with a keystone jack.

**Figure 8-39**

A punchdown tool forces a wire into a slot and cuts off the wire



Enlarge Image

Now that you know about the tools you’ll need to wire networks, let’s see how the cables and connectors are wired.

Go to pg.

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

Application OpenedApplication Opened

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

**8-4**Troubleshooting Network Connections

**A+ Core 1**

* 2.8

Given a scenario, use appropriate networking tools.

* 5.7

Given a scenario, troubleshoot common wired and wireless network problems.

With tools in hand, including hardware tools described in this chapter and software tools you learned about in [Chapter 7](javascript://), you’re now ready to tackle network troubleshooting, including problem solving when there is no connectivity or it is limited or intermittent. Some guidelines to follow when troubleshooting a network problem are outlined in [Figure 8-50](javascript://) and listed here:

1. To check for local connectivity, ping the local router, then try pinging other devices on the network. No connectivity to any network devices might be caused by the network cable or its connection, a wireless switch not turned on, a bad network adapter, or network settings in Windows.

**Figure 8-50**

A flowchart to troubleshoot networking problems related to hardware

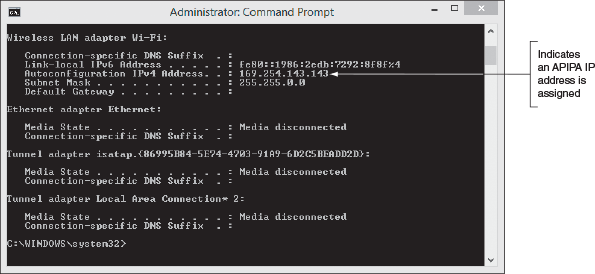
The image shows a flowchart to troubleshoot networking problems related to hardware. "Begin troubleshooting the network" goes to "Can you ping devices on the local network?" by an arrow. It then goes to "Are other computers experiencing the same problem?" and "Can you access network resources?" by two different arrows No and yes respectively. Now, the first option "Are other computers experiencing the same problem?" leads to Check network cables, router, and switches." and "Are the status indicator lights on the network port lit?" by two different arrows Yes and No respectively. Again, "Are the status indicator lights on the network port lit?" goes to "Check network settings in Windows" and "Does a loopback plug indicate the network port is good?" by two different arrows Yes and No respectively. Again, "Does a loopback plug indicate the network port is good?" leads to "Troubleshoot the network adapter" and "Does a loopback plug indicate the wall jack port is good?" by two different arrows No and Yes respectively. "Does a loopback plug indicate the wall jack port is good?" goes to "Test the cable or try a known good cable" and "Does a cable tester indicate the cable from the wall jack port to the patch panel port is good?" by two different arrows Yes and No respectively. "Does a cable tester indicate the cable from the wall jack port to the patch panel port is good?" goes to "You might need to rewire the keystone jack in the patch panel. Also look for signs of damage to the cable from the wall jack to the patch panel" and "The source of the problem is some other device on the network. Use a network multimeter to locate the problem" by two different arrows No and Yes respectively. Both this option then goes to "Can you ping devices on the local network?". The second option "Can you access network resources?" goes to "Can you access the Internet?", "Check network cables and switches along the path to that resource", and "Check higher T C P/I P layers, such as permissions or hosts of those services" by three different arrows Yes, Some, and No respectively. "Can you access the Internet?" option leads to "You have full network access" and "Check the router and modem, and the I S P’s service" by two arrows Yes and No respectively. Lastly, "Check the router and modem, and the I S P’s service", "Check network cables and switches along the path to that resource", and "Check higher T C P/I P layers, such as permissions or hosts of those services"go to the option "Can you ping devices on the local network?".

Enlarge Image

1. Determine whether other computers on the network are experiencing the same problem you’ve noticed on the first computer. If the entire network is down, the problem is not isolated to the computer you are working on.
2. To find out if a computer with limited or no connectivity was able to initially connect to a DHCP server on the network, check for an Automatic Private IP Address (APIPA) on an IPv4 network. On an IPv6 network, check for a link local address for the interface with no unique local address. Recall that on an IPv4 network, a computer assigns itself an APIPA if it is unable to find a DHCP server when it first connects to the network. On an IPv6 network, the computer always assigns itself a link local address, but it will only have a unique local address if it can get one from a DHCPv6 server. Use the ipconfig command to find out the IP addresses (see [Figure 8-51](javascript://)). In the results, an APIPA presents itself as the Autoconfiguration IPv4 Address, and the address begins with 169.254. An IPv6 link local address begins with FE80 and a unique local address, if obtained successfully from the DHCPv6 server, will begin with FC or FD.

**Figure 8-51**

The network connection was not able to lease an IP address



Enlarge Image

1. Check the status indicator lights on the network ports for connectivity and activity.
2. Use a loopback plug to verify that each port is working. The loopback plug can test ports on a computer, wall jack, patch panel, switch, router, or other device that is turned on. If you find a bad port, try a different port on a switch, router, or patch panel. Try resetting a switch or router. For a router, try updating its firmware. You might need to replace the device.
3. For short, straight-through cables that connect a computer to a wall jack or other nearby device, exchanging the straight-through cable for a known good one might be easier and quicker than using a cable tester to test the cable. For longer cables, especially those inside walls, ceilings, and raised floors, consider that the cable length might exceed the recommended maximum length.
4. Use a cable tester to verify that a cable permanently installed along or inside a wall is good. To test the cable, you have to first disconnect it from a computer, patch panel, switch, or other device at both ends of the cable. Common problems with networks are poorly wired termination in patch panels and wall jacks. If the cable proves bad, first try reinstalling the two jacks before you replace the cable.
5. Test for access to other network resources, such as file shares, network printers, or email services. If you can successfully ping the devices hosting those resources, but you can’t access the resources themselves, this indicates a problem at a higher TCP/IP layer, such as permission configurations, or problems at the host for that network service.
6. If you can access some but not all devices on the network, the limited connectivity might be caused by cables or a switch on the network or a problem at the other computers you’re trying to reach.
7. To test for Internet access, use a browser to surf the web. Problems with no Internet access can be caused by cables, a SOHO router, a broadband modem, or problems at the ISP.

Now let’s see how to handle problems with no connectivity or intermittent connectivity and then we’ll look at problems with Internet access.

**A+ Exam Tip**

The A+ Core 1 exam might give you a scenario that requires you to troubleshoot a network with no connectivity, limited connectivity, intermittent connectivity, or unavailable resources. You might be given some network commands and be asked to order the commands correctly to solve the problem.

Go to pg.

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

Application Opened

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

## 8-4aProblems with No Connectivity or Intermittent Connectivity

**A+ Core 1**

* 2.8

Given a scenario, use appropriate networking tools.

* 5.7

Given a scenario, troubleshoot common wired and wireless network problems.

When a computer has no network connectivity or intermittent connectivity, begin by checking hardware and then move on to checking Windows network settings.

Follow these steps to solve problems with hardware:

1. Check the status indicator lights on the NIC or the motherboard Ethernet port. A steady light indicates connectivity and a blinking light indicates activity (see [Figure 8-52](javascript://)). Check the indicator lights on the router or switch at the other end. Try a different port on the device. If the router or switch is in a server closet and the ports are not well labeled, you can use a loopback plug to find out which port the computer is using. If you don’t see either light, this problem must be resolved before you consider OS or application problems.

**Figure 8-52**

Status indicator lights verify connectivity for a network port



1. Check the network cable connection at both ends. Is the cable connected to a port on the motherboard that is disabled? It might need to be connected to the network port provided by a network card. A cable tester can verify that the cable is good or if it is the correct cable (patch cable or crossover cable). Try a different network cable.
2. For wireless networking, make sure the wireless radio on the computer is turned on. If you have no connectivity, limited connectivity, or intermittent connectivity, consider moving the computer to a new position in the hotspot or shift the wireless access point’s location. Use a wireless locator to find the best position. Try turning the wireless connection off, wait a few seconds, then turn it back on. Rebooting a computer might solve the problem of not receiving a signal. Problems with a low RF (radio frequency) signal can sometimes be solved by moving the laptop or connecting to a different wireless access point that has a stronger RF signal.
3. If the problem still persists after you’ve checked cable connections and the wireless radio, turn to Windows to repair the network connection. Use one of these methods:
   * In a command prompt window, use these two commands: **ipconfig /release** followed by **ipconfig /renew**.
   * In the Network and Sharing Center, click **Troubleshoot problems** to access a diagnostic tool for Windows network connectivity (see [Figure 8-53](javascript://)).

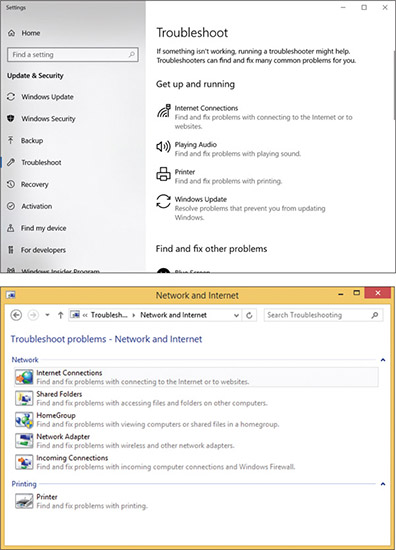
**Notes**

In Windows 10, you can also access the troubleshooter tools by right-clicking the network connection icon in the taskbar, clicking **Open Network & Internet settings**, and then clicking **Network troubleshooter**.

* + If that doesn’t work, return to the Network and Sharing Center, click **Change adapter settings**, right-click the connection, and click **Disable**. Then right-click the connection again and click **Enable**.

**Figure 8-53**

Windows 10 and Windows 8/7 troubleshooter tools



Enlarge Image

If the problem is still not resolved, you need to dig deeper. Perhaps the problem is with the network adapter drivers. To solve problems with device drivers, which might also be related to a problem with the NIC, follow these steps:

1. Make sure the network adapter and its drivers are installed by checking for the adapter in Device Manager. Device Manager should report the device is working with no problems.
2. If errors are reported, try updating the device drivers. (Use another computer to download new drivers to a USB flash drive and then move the flash drive to this computer.) If the drivers still install with errors, look on the manufacturer’s website or the installation CD that came bundled with the adapter for diagnostic software that might help diagnose the problem.
3. Try uninstalling and reinstalling the network adapter.
4. If Device Manager still reports errors, try running anti-malware software and updating Windows. Then try replacing your network adapter. If that doesn’t work, the problem might be a corrupted Windows installation.

Go to pg.

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

Application Opened

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

## 8-4bProblems with Internet Connectivity

**A+ Core 1**

* 5.7

Given a scenario, troubleshoot common wired and wireless network problems.

If you have local connectivity, but not Internet access, do the following:

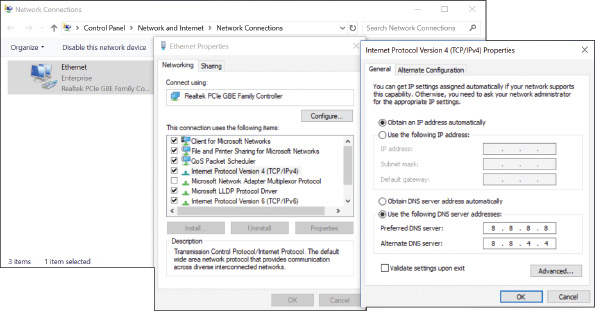
1. Try recycling the connection to the ISP. Follow these steps:
   * Go to the power source of the cable modem, DSL modem, or other device that you use to connect to your ISP, and unplug the power. Unplug the router. Wait about five minutes for the connection to break at the ISP.
   * Plug in the cable modem, DSL modem, or other ISP device. Wait until the lights settle. Then plug in your router.
   * On any computer on your network, use the Network and Sharing Center to repair the network connection. Open your browser and try to browse to some websites.
2. For a cable modem, check to make sure your television works. The service might be down. For a DSL connection, check to make sure your landline phone gives a dial tone. The phone lines might be down.
3. To eliminate the router as the source of the problem, connect one computer directly to the broadband modem. If you can access the Internet, you have proven the problem is with the router or cables going to it. Connect the router back into the network and check all the router settings. The problem might be with DHCP, the firewall settings, or port forwarding. Try updating the firmware on the router. If you are convinced all settings on the router are correct, but the connection to your ISP works without the router and does not work with the router, it’s time to replace the router.
4. To eliminate DNS as the problem, follow these steps:
   * Try substituting a domain name for the IP address in a ping command. First ping an IP address, such as Google’s DNS server:
     + **ping 8.8.8.8**
     + Then ping a domain name:
     + **ping google.com**

If both pings work, then you can conclude that DNS works. If an IP address works but the domain name does not work, the problem lies with DNS.

* + Try pinging your DNS server. To find out the IP address of your DNS server, use the nslookup command with no parameters or open the firmware utility of your router and look on a status screen.
  + Try changing your DNS servers to public DNS servers, such as Google’s (see [Figure 8-54](javascript://)). In the Network Connections window, right-click the active connection and click **Properties**. Click **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. Select **Use the following DNS server addresses**. Google’s DNS servers are 8.8.8.8 and 8.8.4.4, and there are several other public DNS servers available. You can use a different computer to search for other DNS services as well.

**Figure 8-54**

Several organizations offer public DNS services if your ISP’s DNS servers are down



Enlarge Image

1. If you’re having a problem accessing a particular computer on the Internet, try using the tracert command. For example:

**tracert cengage.com**

The results show computers along the route that might be giving delays.

1. If one computer on the network cannot access the Internet but other computers can, make sure MAC address filtering on the router is disabled or the computer is allowed access.
2. Perhaps the problem is with your router firewall or Windows Firewall. How to verify router firewall settings is covered in [Chapter 7](javascript://). Windows Firewall is covered in [Chapter 16](javascript://).
3. If you still cannot access the Internet, contact your ISP.

If some computers on the network have both local and Internet connectivity, but one computer does not, move on to checking problems on that computer, which can include TCP/IP settings and problems with applications.

Go to pg.

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

Application Opened

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

## 8-4cUsing TCP/IP Utilities to Solve Connectivity Problems

**A+ Core 1**

* 5.7

Given a scenario, troubleshoot common wired and wireless network problems.

The problem of no connectivity or no Internet access can be caused by Windows TCP/IP configuration and can be solved using Windows TCP/IP utilities. Follow these steps to verify that the local computer is communicating over the network:

1. Using the Network and Sharing Center or the ipconfig command, try to release the current IP address and lease a new address. This process solves the problem of an IP conflict with other computers on the network when using DHCP and dynamic IP addresses or your computer’s failure to connect to the network.
2. For static IP addressing, consider that duplicate static IP addresses may have been assigned to hosts on the network. You need to go to each computer or device that is using static IP addresses and verify that no two addresses are the same.
3. To find out if you have local connectivity, try to ping another computer on the network. To find out if you have Internet connectivity and DNS is working, try to ping a computer on the Internet using its host address. Enter **ping cengage.com**. If this last command doesn’t work, try the tracert command to find out if the problem is outside or inside your local network. Enter **tracert cengage.com**.
4. In a command prompt window, enter **ipconfig /all**. Verify the IP address, subnet mask, and default gateway. For dynamic IP addressing, if the computer cannot reach the DHCP server, it assigns itself an APIPA, which is listed as an Autoconfiguration IPv4 Address that begins with 169.254 (refer back to [Figure 8-51](javascript://)). In this case, suspect that the computer is not able to reach the network or the DHCP server is down.
5. Next, try the loopback address test. Use the **ping 127.0.0.1** command. Your computer should respond. If you get an error, assume the problem is TCP/IP settings on your computer. Compare the configuration with that of a working computer on the same network.
6. If you’re having a problem with slow transfer speeds, suspect a process is hogging network resources. Use the **netstat –b** command to find out if the program you want to use to access the network is actually running. In [Chapter 14](javascript://), you learn to use Resource Monitor to look for processes hogging network resources. Recall from [Chapter 7](javascript://) that you can use QoS features in Windows and on the router to give priority to an application or device that needs to perform better on the network.
7. Firewall settings might be wrong. Are port forwarding settings on the router and in Windows Firewall set correctly? You learn to configure Windows Firewall in [Chapter 16](javascript://).
8. If you’re having problems getting a network drive map to work, try making the connection with the net use command, like this:
   * **net use z: \\computername\folder**
   * To disconnect a mapped network drive, use this command:
   * **net use z: /delete**

Go to pg.

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

Application Opened

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

## 8-4dSlow Transfer Speeds

**A+ Core 1**

* 5.7

Given a scenario, troubleshoot common wired and wireless network problems.

Perhaps you have network connectivity, but the network seems sluggish with slow file transfer speeds, lagging websites or network-based applications, and possibly a variety of error messages. It’s best to look first for simple problems causing these delays. Using your critical thinking skills, start at the hardware level of the TCP/IP model and work your way up the layers:

* There’s an unofficial layer affectionately called the User layer. If the user is present, interview the user and have the user reproduce the problem while you watch. Ask questions such as, “When did the problem start?” and “What has changed since the problem started?” Determine if you might have some tips for how to access network resources more efficiently and effectively.
* **Link layer**. Check cables for secure connections, status lights for consistent connectivity, and network devices for indications of errors being reported. Also use Device Manager to check the NIC’s speed and duplex settings on Ethernet connections, ensuring that Auto Negotiation is selected.
* **Internet layer**. Ping the computer’s loopback address, default gateway, another device on the network, and a server on the Internet. Watch for indications of delayed responses, and use tracert if needed to help identify the exact location of the slowdown.
* **Transport layer**. Check firewall settings for blocked ports. Also confirm that QoS settings are configured as expected, and consider experimenting with different settings to see if that improves network performance.
* **Application layer**. If everything below the Application layer is working, you’ll know to focus your troubleshooting efforts on application installation, configuration, and compatibility concerns. Try the same operations using different but similar applications. For example, try using a different browser, or use a different FTP client application. Keep in mind that both the server and the client might need some troubleshooting to identify and solve an Application-layer problem.

Now we move on to problems with wireless connectivity.

Go to pg.

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

Application Opened

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

## 8-4eWi-Fi Network Not Found

**A+ Core 1**

* 5.7

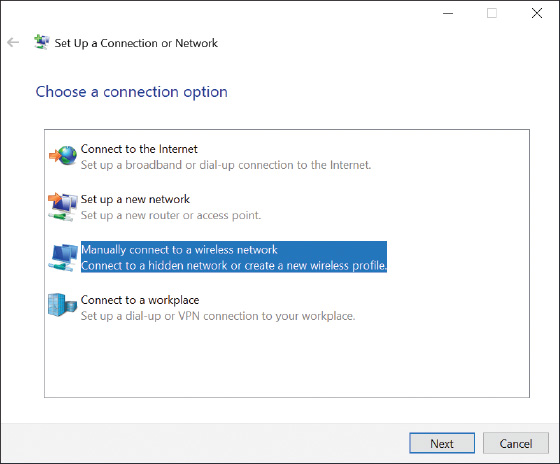
Given a scenario, troubleshoot common wired and wireless network problems.

Recall that a wireless access point broadcasts an SSID. Your computer should easily find the SSID of a Wi-Fi network and connect after entering the security key, if one is needed. If your computer does not detect an SSID that you know should be available, it might be because the SSID is hidden. If you know the SSID name and the security key, you can still connect to the network by following these steps:

1. Open the Network and Sharing Center.
2. Click **Set up a new connection or network**.
3. Select **Manually connect to a wireless network** (see [Figure 8-55](javascript://)), and click **Next**.

**Figure 8-55**

Set up a manual connection to a hidden SSID



1. Enter the network name, choose the security type, and enter the security key. Click **Next**.
2. Your wireless network is set up and you should be connected. Click **Close**.

Go to pg.

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

Application Opened

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

# Chapter Review

## 8-5a**Chapter Summary**

### Understanding TCP/IP and Windows Networking

* According to the TCP/IP model, networking communication must happen at four layers: Link, Internet, Transport, and Application.
* At the Link layer, a network adapter has a MAC address that uniquely identifies it on the network.
* At the Internet layer, the OS identifies a network connection by an IP address. At the Transport layer, a port address identifies an application.
* IP addresses can be dynamic or static. A dynamic IP address is assigned by a DHCP server when the computer first connects to a network. A static IP address is manually assigned.
* An IPv4 address has 32 bits, and an IPv6 address has 128 bits. Some IP addresses are private and can only be used on a local network.
* Using IPv4, the string of 1s in a subnet mask determines the number of left-most bits in an IP address that identify the local network. The string of 0s determines the number of right-most bits in the IP address that identify the host.
* Using IPv6, three types of IP addresses are a multicast address (used for one-to-many transmissions), anycast address (used by routers), and unicast address (used by a single node on a network).
* Types of unicast addresses are a link local address (used on a private network), unique local address (used on subnets in a large enterprise), and global address (used on the Internet).
* A computer can be assigned a computer name, and a network can be assigned a domain name. A fully qualified domain name (FQDN) includes the computer name and the domain name. An FQDN can be used to find a computer on the Internet if this name is associated with an IP address kept by DNS servers.
* TCP/IP uses several protocols at the Application layer (such as FTP, HTTP, and Telnet) and at the Transport layer (such as TCP and UDP). The Internet layer primarily relies on IP, and the Link layer mostly uses Ethernet and Wi-Fi protocols.

### Local Network Infrastructure

* Networking hardware used on local networks can include hubs, switches, routers, wireless access points, bridges, cables, and connectors.
* Switches and older hubs are used as centralized connection points for devices on a wired network. A bridge stands between two network segments and controls traffic between them.
* A client computer contacts a server to request information or to perform a task. Examples of network servers are a web server, mail server, file server, print server, DHCP server, DNS server, proxy server, authentication server, and Syslog server.
* Most wired local networks use twisted-pair cabling that can be unshielded twisted-pair (UTP) cable or shielded twisted-pair (STP) cable. Twisted-pair cable is rated by category, with the most common being CAT-5, CAT-5e, and CAT-6.
* Fiber-optic cables can use one of four connectors: ST, SC, LC, or MT-RJ. Any one of the four connectors can be used with single-mode or multimode fiber-optic cable.
* Powerline networking, also called Ethernet over Power (EoP), sends Ethernet transmissions over the power lines of a building or house. Power over Ethernet (PoE) sends power over Ethernet cables.

### Setting Up and Troubleshooting Network Wiring

* Tools used to manage and troubleshoot network wiring and connectors are a loopback plug, cable tester, network multimeter, Wi-Fi analyzer, toner probe, cable stripper, crimper, and punchdown tool.
* The RJ-45 connector has eight pins. Four pins (pins 1, 2, 3, and 6) are used to transmit and receive data using the 10BaseT and 100BaseT speeds. Using 1000BaseT speed, all eight pins are used for transmitting and receiving data.
* Two standards used to wire network cables are T568A and T568B. The difference between the two standards is that the orange twisted-pair wires are reversed in the RJ-45 connector from the green twisted-pair wires.
* Either T568A or T568B can be used to wire a network. To avoid confusion, don’t mix the two standards in a building.
* Use wire strippers, wire cutters, and a crimper to make network cables. A punchdown tool is used to terminate cables in a patch panel or keystone RJ-45 jack. Be sure to use a cable tester to test or certify a cable you have just made.

### Troubleshooting Network Connections

* When troubleshooting network problems, check hardware, device drivers, Windows, and the client or server application, in that order.
* Use the ping command to verify connectivity and the tracert command to solve problems with connecting to a particular host on the Internet. The nslookup command can verify that DNS is working. Use ipconfig to verify that the computer leased an IP address from the DHCP server. The netstat command can verify a process that uses the network is running. The net use command can be used to map a network drive.
* Use the Network and Sharing Center to connect to a Wi-Fi network when the SSID is hidden.

Go to pg.

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

Application Opened

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

# Chapter Review

## 8-5b**Key Terms**

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

* [**AFP (Apple Filing Protocol)**](javascript://)
* [**anycast address**](javascript://)
* [**authentication server**](javascript://)
* [**best-effort protocol**](javascript://)
* **BNC connector**
* [**bridge**](javascript://)
* [**broadcast message**](javascript://)
* [**cable stripper**](javascript://)
* [**cable tester**](javascript://)
* [**CAT-5**](javascript://)
* [**CAT-5e**](javascript://)
* [**CAT-6**](javascript://)
* [**CIDR (Classless Interdomain Routing) notation**](javascript://)
* [**CIFS (Common Internet File System)**](javascript://)
* [**connectionless protocol**](javascript://)
* [**connection-oriented protocol**](javascript://)
* [**crimper**](javascript://)
* [**crossover cable**](javascript://)
* [**DNS client**](javascript://)
* [**domain name**](javascript://)
* [**endpoint device**](javascript://)
* [**endpoint management server**](javascript://)
* [**EoP (Ethernet over Power)**](javascript://)
* [**Fast Ethernet**](javascript://)
* [**file server**](javascript://)
* [**FQDN (fully qualified domain name)**](javascript://)
* [**FTP (File Transfer Protocol)**](javascript://)
* [**Gigabit Ethernet**](javascript://)
* [**global address**](javascript://)
* [**host name**](javascript://)
* [**HTTP (Hypertext Transfer Protocol)**](javascript://)
* [**HTTPS (HTTP secure)**](javascript://)
* [**hub**](javascript://)
* [**IDS (intrusion detection system)**](javascript://)
* [**IMAP4 (Internet Message Access Protocol, version 4)**](javascript://)
* [**interface ID**](javascript://)
* [**intranet**](javascript://)
* [**IP (Internet Protocol)**](javascript://)
* [**IPS (intrusion prevention system)**](javascript://)
* [**LDAP (Lightweight Directory Access Protocol)**](javascript://)
* [**link**](javascript://)
* [**link local address**](javascript://)
* [**loopback address**](javascript://)
* [**managed switch**](javascript://)
* [**multicast address**](javascript://)
* [**NAT (Network Address Translation)**](javascript://)
* [**neighbor**](javascript://)
* [**NetBIOS**](javascript://)
* [**NetBT (NetBIOS over TCP/IP)**](javascript://)
* [**network ID**](javascript://)
* [**network multimeter**](javascript://)
* [**NGFW (next-generation firewall)**](javascript://)

* **[node](javascript://)**
* [**octet**](javascript://)
* [**OSI (Open Systems Interconnection) model**](javascript://)
* [**patch cable**](javascript://)
* [**patch panel**](javascript://)
* [**PDU (protocol data unit)**](javascript://)
* [**plenum**](javascript://)
* **PoE (Power over Ethernet)**
* [**PoE injector**](javascript://)
* [**POP3 (Post Office Protocol, version 3)**](javascript://)
* [**powerline networking**](javascript://)
* [**print server**](javascript://)
* [**private IP address**](javascript://)
* [**proxy server**](javascript://)
* [**public IP address**](javascript://)
* [**punchdown tool**](javascript://)
* [**PVC (polyvinyl chloride)**](javascript://)
* [**RDP (Remote Desktop Protocol)**](javascript://)
* [**repeater**](javascript://)
* [**SLP (Service Location Protocol)**](javascript://)
* [**SMB (Server Message Block)**](javascript://)
* [**SMTP (Simple Mail Transfer Protocol)**](javascript://)
* [**SNMP (Simple Network Management Protocol)**](javascript://)
* **socket**
* [**SSH (Secure Shell)**](javascript://)
* [**STP (shielded twisted-pair) cable**](javascript://)
* [**straight-through cable**](javascript://)
* [**subnet**](javascript://)
* [**subnet ID**](javascript://)
* **subnet mask**
* **switch**
* [**Syslog**](javascript://)
* [**Syslog server**](javascript://)
* [**T568A**](javascript://)
* [**T568B**](javascript://)
* [**TCP (Transmission Control Protocol)**](javascript://)
* **TCP/IP (Transmission Control Protocol/Internet Protocol)**
* [**TCP/IP model**](javascript://)
* [**Telnet**](javascript://)
* [**tone generator and probe**](javascript://)
* [**toner probe**](javascript://)
* [**twisted-pair cabling**](javascript://)
* [**UDP (User Datagram Protocol)**](javascript://)
* [**unicast address**](javascript://)
* [**unique local address**](javascript://)
* [**unmanaged switch**](javascript://)
* [**UTM (Unified Threat Management)**](javascript://)
* [**UTP (unshielded twisted-pair) cable**](javascript://)
* [**virtual LAN (VLAN)**](javascript://)
* [**Wi-Fi analyzer**](javascript://)

Go to pg.

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

Application Opened

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

# Chapter Review

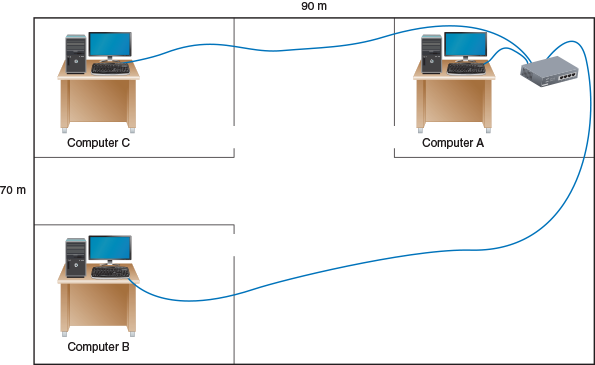
## 8-5c**Thinking Critically**

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. While investigating the settings on your SOHO router, you find two IP addresses reported on the device’s routing table, which is used to determine where to send incoming data. The two IP addresses are 192.168.2.1 and 71.9.200.235. Which of these IP addresses would you see listed as the default gateway on the devices in your local network? How do you know?
2. Different network devices function at different network communication layers, depending on their purpose. Using the TCP/IP model, identify the highest layer accessed by each of the following devices:
   1. Router
   2. Unmanaged switch
   3. Wireless access point
   4. Firewall
3. Your boss asks you to transmit a small file that includes sensitive personnel data to a server on the network. The server is running a Telnet server and an FTPS server. Why is it not a good idea to use Telnet to reach the remote computer?
   1. Telnet transmissions are not encrypted.
   2. Telnet is not reliable and the file might arrive corrupted.
   3. FTP is faster than Telnet.
   4. FTP running on the same computer as Telnet causes Telnet not to work.
4. While troubleshooting an IPv4 network connection problem, you start to wonder if the local computer’s NIC is working correctly. What command should you enter at the command prompt to test your theory?
5. Which of the following are valid IPv6 addresses? Select all that apply.
   1. fe80::64d2:bd2e:fa62:b911
   2. fe80::g90p:bd2e:fa62:b911
   3. fe80::64d2:bd2e::b911
   4. ::1
6. You’re setting up a secure email server on your local network that you want clients to be able to access from the Internet using IMAP4 and SMTP. Which ports should you open in your firewall?
   1. 25 and 143
   2. 587 and 993
   3. 80 and 443
   4. 25 and 110
7. Lately your IPv6 network has experienced problems connecting new clients to the network. As part of your troubleshooting, you run an ipconfig command on one of the client computers and find two IPv6 addresses reported on the Ethernet interface: fe80::894d:c173:fef2 and fdb9::75f8:e30c:7cf4. Which one indicates the DHCPv6 server is probably working correctly? How do you know?
8. FTP requires confirmation that a file was successfully transmitted to a client, but it has no built-in mechanism to track this information for itself. What protocol does FTP rely on at the Transport layer of the TCP/IP model to ensure delivery is complete?
   1. UDP
   2. HTTP
   3. SSH
   4. TCP
9. A hub transmits all incoming messages to all of its ports except the port where the messages came in. A switch usually sends messages only to the destination computer. What information does a switch collect from messages crossing its interfaces so it knows where to send data in future transmissions?
   1. IP address
   2. MAC address
   3. Port number
   4. FQDN
10. Your customer recently installed a new router in her dance studio, as shown in the diagram in [Figure 8-56](javascript://). She then ran Ethernet cables through the drop ceiling to computers in various offices. Without any further testing, which computers do you suspect are experiencing connection problems? Choose all that apply.
    1. Computer A
    2. Computer B
    3. Computer C
    4. None of them

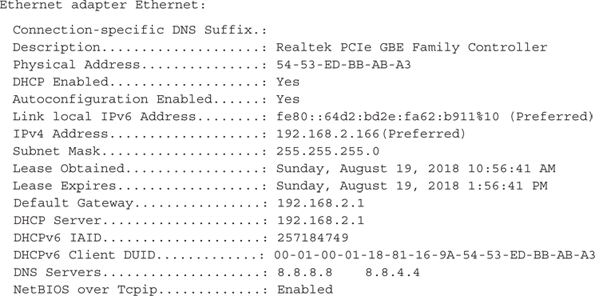
**Figure 8-56**

A diagram of a dance studio



Enlarge Image

1. Your SOHO router has failed and you have installed a new router. The old router’s static IP address on the network is 192.168.0.1. The new router has a static IP address of 10.0.0.1. You go to a computer to configure the new router and enter 10.0.0.1 in the browser address box. The router does not respond. You open a command prompt window and try to ping the router, which does not work. Next, you verify that the router has connectivity and you see that its local connection light is blinking, indicating connectivity. What is the most likely problem and its best solution?
   1. The computer you are using to configure the router has a corrupted TCP/IP configuration. Restart the computer.
   2. The router is defective. Return it for a full refund.
   3. The computer and the router are not in the same subnet. Release and renew the IP address of the computer.
   4. The computer and the router are not in the same subnet. Change the subnet mask assigned to the computer.
2. While troubleshooting a network connection problem, you run the command ipconfig /all in a command prompt window and get the following output:



Enlarge Image

Is the computer using a wired or wireless network connection? What is the local computer’s MAC address? What is the IP address of the router on the local network?

1. Which two of the following hosts on a corporate intranet are on the same subnet?
   1. 192.168.2.143 255.255.255.0
   2. 172.54.98.3 255.255.0.0
   3. 192.168.5.57 255.255.255.0
   4. 172.54.72.89 255.255.0.0
2. You are configuring email on a customer’s computer. Which port should you configure for [pop.companymail.com](http://pop.companymail.com/" \t "_blank)? For [smtp.companymail.com](http://smtp.companymail.com/" \t "_blank)?
   1. 143, 25
   2. 110, 143
   3. 110, 25
   4. 25, 110
3. Which of the following tools can be used to determine if a network cable is good? Choose all that apply.
   1. Cable tester
   2. Crimper
   3. Loopback plug
   4. Network multimeter
4. You’ve been hired to help with installing cable at a new office building for the local branch of the Social Security Administration. You’re wiring a connection into the first room on your list. List the colors of the wires in the order you should place them into the connector, starting with pin 1.

Go to pg.

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

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

## 8-3cHow Twisted-Pair Cables and Connectors Are Wired

**A+ Core 1**

* 2.8

Given a scenario, use appropriate networking tools.

* 3.1

Explain basic cable types, features, and their purposes.

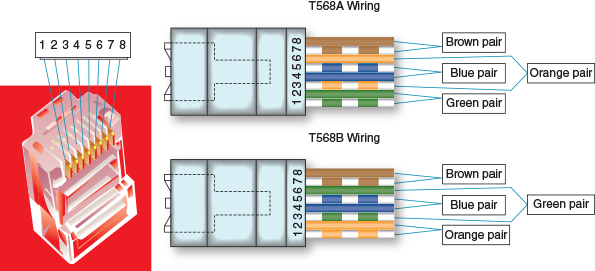
Two types of network cables can be used when building a network: a straight-through cable and a crossover cable. A [**straight-through cable**](javascript://) (also called a [**patch cable**](javascript://)) is used to connect a computer to a switch or other network device. A [**crossover cable**](javascript://) is used to connect two like devices such as a switch to a switch or a computer to a computer (to make the simplest network of all).

The difference between a straight-through cable and a crossover cable is the way the transmit and receive lines are wired in the connectors at each end of the cables. A crossover cable has the transmit and receive lines reversed so that one device receives off the line on which the other device transmits. Before the introduction of Gigabit Ethernet, 10BaseT and 100BaseT required that a crossover cable be used to connect two like devices such as a switch to a switch. Today’s devices that support Gigabit Ethernet use auto-uplinking, which means you can connect a switch to a switch using a straight-through cable and the devices will negotiate the transmit and receive links so data crosses the connection successfully. Crossover cables are seldom used today except to connect a computer to a computer to create a simple two-node network.

Twisted-pair copper wire cabling uses an RJ-45 connector that has eight pins, as shown in [Figure 8-40](javascript://). 10BaseT and 100BaseT Ethernet use only four of these pins: pins 1 and 2 for transmitting data and pins 3 and 6 for receiving data. The other pins can be used for phone lines or for power (using PoE). Gigabit Ethernet uses all eight pins to transmit and receive data and can also transmit power on these same lines.

**Figure 8-40**

Pinouts for an RJ-45 connector



Enlarge Image

Twisted-pair cabling used with RJ-45 connectors is color-coded in four pairs: blue, orange, green, and brown, as shown in [Figure 8-40](javascript://). Each pair has one solid wire and one striped wire. Two standards have been established in the industry for wiring twisted-pair cabling and RJ-45 connectors: T568A and T568B. Both are diagrammed in [Figure 8-40](javascript://) and listed in [Table 8-8](javascript://). The [**T568A**](javascript://) standard has the green pair connected to pins 1 and 2 and the orange pair connected to pins 3 and 6. The [**T568B**](javascript://) standard has the orange pair using pins 1 and 2 and the green pair using pins 3 and 6, as shown in the diagram and the table. For both standards, the blue pair uses pins 4 and 5, and the brown pair uses pins 7 and 8.

**Table 8-8**

### The T568A and T568B Ethernet Standards for Wiring RJ-45 Connectors

| **Pin** | **100BaseT Purpose** | **T568A Wiring** | **T568B Wiring** |
| --- | --- | --- | --- |
| 1 | Transmit+ | White/green | White/orange |
| 2 | Transmit- | Green | Orange |
| 3 | Receive+ | White/orange | White/green |
| 4 | (Used only on Gigabit Ethernet) | Blue | Blue |
| 5 | (Used only on Gigabit Ethernet) | White/blue | White/blue |
| 6 | Receive- | Orange | Green |
| 7 | (Used only on Gigabit Ethernet) | White/brown | White/brown |
| 8 | (Used only on Gigabit Ethernet) | Brown | Brown |

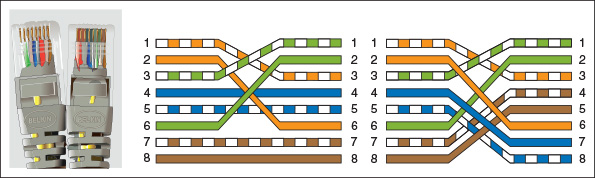
**Notes**

The T568A and T568B standards as well as other network wiring standards and recommendations are overseen by the Telecommunications Industry Association (TIA), Electronics Industries Alliance (EIA), and American National Standards Institute (ANSI).

If the wiring on one end of the cable matches the wiring on the other end, be it the T568A or T568B standard, you have a straight-through cable. If you’re working on a 10BaseT or 100BaseT network and you use T568A wiring on one end of the cable and T568B on the other end, you have a crossover cable (see the diagram on the left side of [Figure 8-41](javascript://)). For Gigabit Ethernet (1000BaseT) that transmits data on all four pairs, you must cross the green and orange pairs as well as the blue and brown pairs to make a crossover cable (see the diagram on the right side of [Figure 8-41](javascript://)). Recall, however, that crossover cables are seldom used on Gigabit Ethernet. When you buy a crossover cable, most likely it is wired only for 10BaseT or 100BaseT networks. If you ever find yourself needing to make a crossover cable, be sure to cross all four pairs so the cable will work on 10BaseT, 100BaseT, and 1000BaseT networks. You can also buy an adapter to convert a straight-through cable to a crossover cable, but most likely the adapter only crosses two pairs and works only for 10BaseT or 100BaseT networks, such as the adapter shown in [Figure 8-42](javascript://).

**Figure 8-41**

Two crossed pairs in a crossover cable is compatible with 10BaseT or 100BaseT Ethernet; four crossed pairs in a crossover cable is compatible with Gigabit Ethernet



Enlarge Image

**Figure 8-42**

A crossover adapter converts a patch cable to a crossover cable for a 10BaseT or 100BaseT network



Although it’s possible to mix standards on the same network, you should always be consistent with which standard you use. When you are wiring a network in a building that already has network wiring, be sure to find out if the wiring is using T568A or T568B, and then be sure you always use that standard. If you don’t know which to use, use T568B because it’s the most common. However, if you are working for the U.S. government, know that it requires T568A for all its networking needs.

**Applying Concepts**

### Making a Straight-Through Cable Using T568B Wiring

It takes a little practice to make a good network straight-through cable, but you’ll get the hang of it after doing only a couple of cables. [Figure 8-43](javascript://) shows the materials and tools you’ll need to make a network cable.

**Figure 8-43**

Tools and materials to make a network cable



Enlarge Image

Here are the steps to make a straight-through cable using the T568B standard:

1. Use wire cutters to cut the twisted-pair cable the correct length plus a few extra inches.
2. If your RJ-45 connectors include boots, slide two boots onto the cable. Be sure they’re each facing the correct direction.
3. Use wire strippers to strip off about two inches of the plastic jacket from the end of the wire. To do that, put the wire in the stripper and rotate the stripper around the wire to score the jacket (see [Figure 8-44](javascript://)). You can then pull off the jacket.

**Figure 8-44**

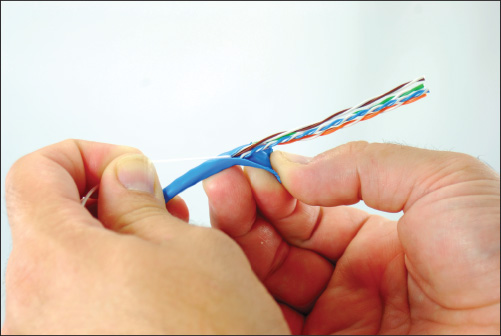
Rotate a wire stripper around the jacket to score it so you can slide it off the wire



1. Use wire cutters to start a cut into the jacket, and then use the rip cord to pull the jacket back a couple of inches (see [Figure 8-45](javascript://)). Next, cut off the rip cord and the jacket. You take the extra precaution of removing the jacket because you might have nicked the wires with the wire strippers.

**Figure 8-45**

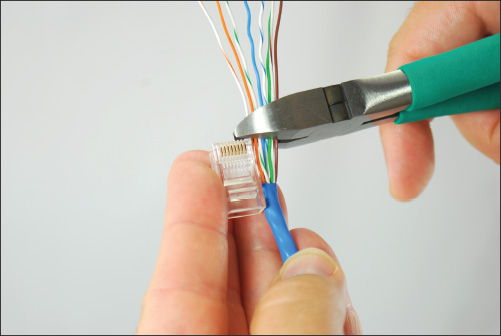
Rip back the jacket, and then cut off the extra jacket and rip cord



1. Untwist each pair of wires so you have eight separate wires. Smooth each wire to straighten out the kinks. Line up the wires in the T568B configuration (refer to [Table 8-8](javascript://)).
2. Holding the tightly lined-up wires between your fingers, use wire cutters to cut the wires off evenly, leaving a little over an inch of wire. See [Figure 8-46](javascript://). To know how short to cut the wires, hold the RJ-45 connector up to the wires. The wires must go all the way to the front of the connector. The jacket must go far enough into the connector so that the crimp at the back of the connector will be able to solidly pinch the jacket.

**Figure 8-46**

Evenly cut off wires measured to fit in the RJ-45 connector with the jacket protruding into the connector



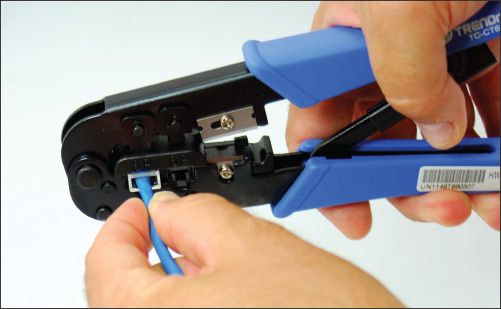
**Notes**

You’ll find several YouTube videos on network wiring. An excellent video by Ferrules Direct for making a straight-through cable is posted at [youtube.com/watch?v=WvP0D0jiyLg](http://youtube.com/watch?v=WvP0D0jiyLg" \t "_blank).

1. Be sure you have pin 1 of the connector lined up with the orange-and-white wire. Then insert the eight wires in the RJ-45 connector. Guide the wires into the connector, making sure they reach all the way to the front. (It helps to push up a bit as you push the wires into the connector.) You can jam the jacket firmly into the connector. Look through the clear plastic connector to make sure the wires are lined up correctly, that they all reach the front, and that the jacket goes past the crimp.
2. Insert the connector into the crimper tool. Use one hand to push the connector firmly into the crimper as you use the other hand to crimp the connector. See [Figure 8-47](javascript://). Use plenty of force to crimp. The eight blades at the front of the connector must pierce through to each copper wire to complete each of the eight connections, and the crimp at the back of the connector must solidly crimp the cable jacket to secure the cable to the connector (see [Figure 8-48](javascript://)). Remove the connector from the crimper and make sure you can’t pull the connector off the wire.

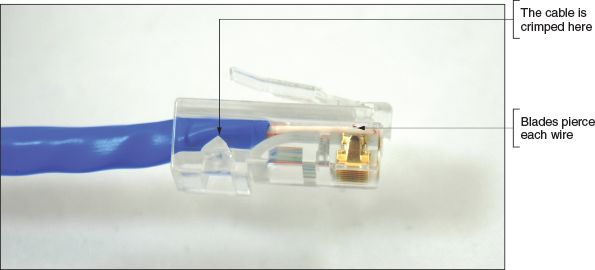
**Figure 8-47**

Use the crimper to crimp the connector to the cable



**Figure 8-48**

The crimper crimps the cable and cable jacket, and eight blades pierce the jacket of each individual copper wire



Enlarge Image

1. Slide the boot into place over the connector. Now you’re ready to terminate the other end of the cable. Configure it to also use the T568B wiring arrangement. [Figure 8-49](javascript://) shows the straight-through cable with only one boot in place.

**Figure 8-49**

A finished patch cable with one boot in place



1. Use a cable tester to make sure the cable is good.

**Notes**

According to networking standards for wiring a keystone RJ-45 jack and a straight-through cable, you can avoid crosstalk by removing the cable jacket to expose no more than three inches of twisted-pair wires, and you should untwist exposed twisted-pair wires no more than a half inch.

Go to pg.

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