In this chapter, you’ll 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’ll also learn to connect a computer to a network and how to set up and secure a small wired or wireless network.

This chapter prepares you to assume total responsibility for supporting both wired and wireless networks in a small-office-home-office (SOHO) environment. In Chapter 16, you learn more about the hardware used in networking, including network devices, connectors, and cabling, networking tools, and the types of networks used for Internet connections. In Chapter 17, you learn how to support applications using a network and how to troubleshoot networking problems. So let’s get started by looking at how TCP/IP works in the world of Windows networking.

⚠️ A+ Exam Tip ⚠️ Much of the content in this chapter applies to both the A+ 220-801 exam and the A+ 220-802 exam.
When two computers communicate using a local network or the Internet, communication happens at three levels (hardware, operating system, and application). The first step in communication is one computer must find the other computer. The second step is both computers must agree on the methods and rules for communication (called **protocols**). Then one computer takes on the role of making requests from the other computer. A computer making a request from another is called the client and the one answering the request is called the server. Most communication between computers on a network or the Internet uses this **client/server** model. For example, in Figure 15-1, someone uses a web browser to request a web page from a web server. To handle this request, the client computer must first find the web server, the protocols for communication are established, and then the request is made and answered. Hardware, the OS, and the applications on both computers are all involved in this process.

**Figure 15-1**   A web browser (client software) requests a web page from a web server (server software); the web server returns the requested data to the client

Let’s first look at the layers of communication that involve hardware, 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.

**LAYERS OF NETWORK COMMUNICATION**

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. For almost all networks today, including the Internet, the group or suite of protocols used is called **TCP/IP (Transmission Control Protocol/Internet Protocol)**.

Before data is transmitted on a network, it is first broken up into segments. Each data segment is put into a **packet**. The packet contains the data (called the payload) and information at the beginning of the packet (called the IP header) that identifies the type of data, where it came from, and where it’s going. If the data to be sent is large, it is first divided into several packets, each small enough to travel on the network.

Part of the information included in a packet header is the address information needed to find the computer that is to receive the packet. The address information includes three levels: the address at the hardware level (called a MAC address), the address at the OS level (called an IP address), and the address at the application level (called a port address).

Communication between two computers happens in layers. In Figure 15-2, you can see how communication starts with an application (browser) passing a request to the OS, which
passes the request to the network card and then onto the network. When the request reaches
the network card on the server, the network card passes it on to the OS and then the OS
passes it on to the application (the web server).

Listed next is a description of each level of communication:

**Level 1: Hardware level.** At the root level of communication is hardware. The hard-
ware or physical connection might be wireless or might use network cables, phone
lines (for DSL or dial-up), or TV cable lines (for a cable modem). For local wired or
wireless networks, a **network adapter** (also called a network card, a network interface
card, or a NIC) inside your computer is part of this physical network. Every network
adapter (including a network card, network port on a motherboard, onboard wireless,
or wireless NIC) has a 48-bit (6-byte) number hard-coded on the card by its
manufacturer that is unique for that device (see Figure 15-3). The number is written in
hex, and is called the **MAC (Media Access Control) address**, **hardware address**, **physical address**, **adapter address**, or Ethernet address. Part of the MAC address
identifies the manufacturer that is responsible for making sure that no two network
adapters have the same MAC address. MAC addresses are used to locate a computer
on a local area network (LAN). A **local area network (LAN)** is a network bound by
routers or other gateway devices. A **router** is a device that manages traffic between
two or more networks and can help find the best path for traffic to get from one net-
work to another. A **gateway** is any device or computer that network traffic can use to
leave one network and go to a different network.
Level 2: Operating system level. Operating systems use IP addresses to find other computers on a network. An IP address is a 32-bit or 128-bit string that is assigned to a network connection when the connection is first made. Whereas a MAC address is only used to find a computer on a local network, an IP address can be used to find a computer anywhere on the Internet (see Figure 15-4) or on an intranet. An intranet is
any private network that uses TCP/IP protocols. A large enterprise might support an intranet that is made up of several local networks. When several local networks are tied together in a subsystem of the larger intranet, this group of small local networks is called a subnetwork or subnet. IP addresses are used to find computers on subnets, an intranet, or the Internet.

**Level 3: Application level.** Most applications used on the Internet or a local network are client/server applications. Client applications, such as Internet Explorer, Google Chrome, or Outlook, communicate with server applications such as a web server or email server. Each client and server application installed on a computer listens at a predetermined address that uniquely identifies the application on the computer. This address is a number and is called a port number, port, or port address. For example, you can address a web server by entering into a browser address box an IP address followed by a colon and then the port number. These values are known as a socket. For example, an email server waiting to send email to a client listens at port 25, and a web server listens at port 80. Suppose a computer with an IP address of 136.60.30.5 is running both an email server and a web server application. If a client computer sends a request to 136.60.30.5:25, the email server that is listening at that port responds. On the other hand, if a request is sent to 136.60.30.5:80, the web server listening at port 80 responds (see Figure 15-5).

![Figure 15-5](image)

Figure 15-5  Each server running on a computer is addressed by a unique port number.

Figure 15-6 shows how communication moves from a browser to the OS to the hardware on one computer and on to the hardware, OS, and web server on a remote computer. As you connect a computer to a network, keep in mind that the connection must work at all three levels. And when things don’t work right, it helps to understand that you must solve the problem at one or more levels. In other words, the problem might be with the physical equipment, with the OS, or with the application.
HOW IP ADDRESSES GET ASSIGNED

A MAC address is embedded on a network adapter at the factory, but IP addresses are assigned manually or by software. In Chapter 7, you learned that an IP address can be a dynamic IP address (IP address is assigned by a server each time it connects to the network) or a static IP address (IP address is permanently assigned to the computer or device).

A+ Exam Tip

The A+ 220-801 and A+ 220-802 exams expect you to know what a DHCP server is and understand how to use static and dynamic IP addressing.

For dynamic IP addresses, a DHCP (dynamic host configuration protocol) server gives an IP address to a computer when it first attempts to initiate a connection to the network and requests an IP address. A computer or other device (such as a network printer) that requests an address from a DHCP server is called a DHCP client. It is said that the client is leasing an IP address. How to configure a Windows computer to use dynamic or static IP addressing is covered later in the chapter.

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 this standard, called Internet Protocol version 4 (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, Internet Protocol version 6 (IPv6), which uses an IP address with 128 bits, was developed. Currently, the Internet uses a mix of 32-bit and 128-bit IP addresses. The Internet Assigned Numbers Authority (IANA at iana.org) is responsible for keeping track of assigned IP addresses and has already released all its available 32-bit IP addresses. IP addresses leased from IANA today are all 128-bit addresses.
Understanding TCP/IP and Windows Networking

Next, let’s see how IPv4 IP addresses are used, and then you’ll learn about IPv6 addresses.

HOW IPV4 IP ADDRESSES ARE USED

A 32-bit IP address is organized into four groups of eight 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 IP 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 (for 8 bits) and can be any number from 0 to 255, making a total of about 4.3 billion IP addresses (256 * 256 * 256 * 256). Some IP addresses are reserved, so these numbers are approximations.

The first part of an IP address identifies the network, and the last part identifies the host. When data is routed over the Internet, the network portion of the IP address is used to locate the right network. After the data arrives at the local network, the host portion of the IP address is used to identify the one computer on the network that is to receive the data. Finally, the IP address of the host must be used to identify its MAC address so the data can travel on the host’s LAN to that host. The next section explains this in detail.

CLASSES OF IP ADDRESSES

IPv4 IP addresses are divided into three classes: Class A, Class B, and Class C. IP addresses belong in each class according to the scheme outlined in Table 15-1. When IPv4 addresses were available from IANA, a company would lease a Class A, Class B, or Class C license from IANA and from this license could generate multiple IP addresses.

<table>
<thead>
<tr>
<th>Class</th>
<th>Network Octets*</th>
<th>Approximate Number of Possible Networks or Licenses</th>
<th>Total Number of Possible IP Addresses in Each Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1.x.y.z to 126.x.y.z</td>
<td>126</td>
<td>16 million</td>
</tr>
<tr>
<td>B</td>
<td>128.0.x.y to 191.255.x.y</td>
<td>16,000</td>
<td>65,000</td>
</tr>
<tr>
<td>C</td>
<td>192.0.0.x to 223.255.255.x</td>
<td>2 million</td>
<td>254</td>
</tr>
</tbody>
</table>

*An x, y, or z in the IP address stands for an octet used to identify hosts.

Table 15-1  Classes of IP addresses

Recall that the first part of an IP address identifies the network, and the last part identifies the host. Figure 15-7 shows how each class of IP addresses is divided into the network and host portions.

Looking back at Table 15-1, you can see that a Class A license is for a single octet, which is the network portion of the IP addresses in that license. The remaining octets can be used for host addresses or to identify subnetworks in the larger network. For example, if a company is assigned 87 as its Class A license, then 87 is the network address and is used as the first octet for every host using this license (87.0.0.1, 87.0.0.2, 87.0.0.3, and so forth).
(In practice, such a large network is divided into subnets.) Because three octets can be used for Class A host addresses, one Class A license can have approximately $256 \times 256 \times 254$ host addresses, or about 16 million IP addresses. Only very large corporations with heavy communication needs were able to obtain a Class A license.

A Class B license leases the first two octets, and these first two octets are used for the network portion and the last two can be used for the host address or for subnetting the network. An example of a Class B license is 150.35, and examples of IP addresses in this network are 150.35.0.1, 150.35.0.2, and 150.35.0.3. How many host addresses are there in one Class B license? The number of possible values for two octets is about $256 \times 254$, or about 65,000 host addresses in a single Class B license.

A Class C license assigns three octets as the network address. With only one octet used for the host addresses, there can be only 254 host addresses on a Class C network or its subnetworks. For example, if a company is assigned a Class C license for its network with a network address of 200.80.15, some IP addresses on the network would be 200.80.15.1, 200.80.15.2, and 200.80.15.3.

Class D and Class E IP addresses are not available for general use. Class D addresses begin with octets 224 through 239 and are used for multicasting, in which one host sends messages to multiple hosts, such as when the host transmits a video conference over the Internet. Class E addresses begin with 240 through 254 and are reserved for research.

In addition to classes of IP addresses, a few IP addresses were reserved for special use by TCP/IP and should not be assigned to a device on a network. Table 15-2 lists these reserved IP addresses.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>How It Is Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>255.255.255.255</td>
<td>Used for broadcast messages by TCP/IP background processes</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Currently unassigned IP address</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Indicates your own computer and is called the loopback address</td>
</tr>
</tbody>
</table>

Table 15-2 Reserved IP addresses
SUBNETS USING IPV4

Looking back at Table 15-1, you can see that a single class license network might have millions of hosts. Managing a network with so many hosts is not practical unless you divide the network into subnets. To divide a network into subnets, you designate part of the host portion of the IP address as a subnet. For example, suppose you have a Class A license of 69. Without using subnets, you have one network: the first octet of all the IP addresses in this network is 69; the last three octets are used for host addresses; and the number of hosts in this one network is about 16 million. Suppose you divide this one network into 256 subnets by using the second octet for the subnet address. (The subnets are 69.0.x.y through 69.255.x.y.) The last two octets are used for host addresses in each subnet with a potential of about 65,000 hosts in each subnet (256 x 254).

The subnet mask used with IPv4 identifies which part of an IP address is the network portion and which part is the host portion. Using a subnet mask, a computer or other device can know if an IP address of another computer is on its network or another network (see Figure 15-8).

A subnet mask is a string of ones followed by a string of zeros. The ones in a subnet mask say, “On our network, this part of an IP address is the network part,” and the group of zeros says, “On our network, this part of an IP address is the host part.”

If you don’t divide a network into subnets, the default subnet mask is used, which is called a classful subnet mask because the network portion of the IP address aligns with the class license. For example, Table 15-3 shows the default subnet masks used for three IP addresses. In the table, the green numbers identify the network and the red numbers identify the host.
These three subnet masks would be displayed in a TCP/IP configuration window like this:

- Subnet mask of 11111111.00000000.00000000.00000000 is displayed as 255.0.0.0
- Subnet mask of 11111111.11111111.00000000.00000000 is displayed as 255.255.0.0
- Subnet mask of 11111111.11111111.11111111.00000000 is displayed as 255.255.255.0

A network is divided into subnets when the subnet mask takes some of the host portion of the IP address for the network ID. This classless subnet mask does not align the network ID with the network octets assigned by the class license. Using our earlier example, the classless subnet mask for a Class A license of 69 that uses two octets for the network ID rather than the one octet assigned by the class license would be 11111111.11111111.00000000.00000000 or 255.255.0.0. A classless subnet mask can also have a mix of zeros and ones in one octet such as 11111111.11111111.11110000.00000000, which can be written as 255.255.240.0. These classless subnet masks are used to subnet large corporate networks.

### Table 15-3 Default subnet masks for classes of IP addresses

<table>
<thead>
<tr>
<th>Class</th>
<th>Subnet Mask</th>
<th>Address</th>
<th>Network ID</th>
<th>Host ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td>11111111.00000000.00000000.00000000</td>
<td>89.100.13.78</td>
<td>89</td>
<td>100.13.78</td>
</tr>
<tr>
<td>Class B</td>
<td>11111111.11111111.00000000.00000000</td>
<td>190.78.13.250</td>
<td>190.78</td>
<td>13.250</td>
</tr>
<tr>
<td>Class C</td>
<td>11111111.11111111.11111111.00000000</td>
<td>201.18.20.208</td>
<td>201.18.20</td>
<td>208</td>
</tr>
</tbody>
</table>

### Applying Concepts

Larry is setting up a new computer on a network. He creates TCP/IP settings to use static IP addressing. He assigns a subnet mask of 255.255.240.0 and an IP address of 15.50.212.59 to this computer. Suppose this computer wants to communicate with a computer assigned an IP address of 15.50.235.80. Are these two computers in the same subnet? To find out, you can first compare the binary values of the first two octets and determine if they match. Then compare the binary values of the third octet, like this:

212 = 11010100
235 = 11101011

To be in the same subnet, the first four bits must match, which they don’t. Therefore, these two computers are not in the same subnet. However, an IP address that is in the same subnet as 15.50.212.59 is 15.50.220.100 because the first two octets match and the first four bits of the third octet match (comparing 11010100 to 11011100).

### Notes

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 subnet mask is written as 20 ones followed by enough zeros to complete the full 32 bits.
PUBLIC, PRIVATE, AND AUTOMATIC PRIVATE IP ADDRESSES

When a company applied for a Class A, B, or C license, it was assigned a group of IP addresses that are different from all other IP addresses and are available for use on the Internet. The IP addresses available to the Internet are called public IP addresses.

A company conserves its public IP addresses by using private IP addresses that are not allowed on the Internet. Within the company network, computers communicate with one another using these private IP addresses. A computer using a private IP address on a private network can still access the Internet if a router or other device that stands between the network and the Internet is using NAT (Network Address Translation). NAT is a TCP/IP protocol that substitutes the public IP address of the router for the private IP address of the other computer when these computers need to communicate on the Internet.

Because of NAT, a small company can rely solely on private IP addresses for its internal network and use only the one public IP address assigned to it by its ISP for Internet communication. 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
Connecting to and Setting Up a Network

If a computer first connects to the network and is unable to lease an IP address from the DHCP server, it uses an Automatic Private IP Address (APIPA) in the address range 169.254.x.y.

**HOW IPV6 IP ADDRESSES ARE USED**

Using 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 IP addresses are written and displayed:

- An IPv6 address has 128 bits that are written as 8 blocks of hexadecimal numbers separated by colons, like this: 2001:0000:B80:0000:D3:9C5A:CC.
- 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 zeros in a 4-character hex block can be eliminated. For example, the IP address above can be written as 2001:0000:B80:0000:D3:9C5A:CC.
- If blocks contain all zeros, 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 IP 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 zeros.

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**, sometimes called the local link, is a local area network (LAN) or wide area network (WAN) bounded by routers.
- An **interface** is a node’s attachment to a link. The attachment can be a logical attachment or a physical attachment using a network adapter or wireless connection. For example, a logical attachment can be used for tunneling. Tunnels are used by IPv6 to transport IPv6 packets over an IPv4 network.
- The last 64 bits or 4 blocks of an IP address identify the interface and are called the interface ID or interface identifier. These 64 bits uniquely identify an interface on the local link.
- **Neighbors** are two or more nodes on the same link.

Three tunneling protocols have been developed for IPv6 packets to travel over an IPv4 network:

- **ISATAP** (pronounced “eye-sa-tap”) stands for Intra-Site Automatic Tunnel Addressing Protocol).
- **Teredo** (pronounced “ter-EE-do”) is named after the Teredo worm that bores holes in wood. IPv6 addresses intended to be used by this protocol always begin with the same
32 bit-prefix (called fixed bits). Teredo IP addresses begin with 2001, and the prefix is written as 2001::/32.

6TO4 is an older tunneling protocol being replaced by the more powerful Teredo or ISATAP protocols.

IPv6 classifies IP addresses differently from that of IPv4. IPv6 supports these three types of IP addresses:

- Using a **unicast address**, packets are delivered to a single node on a network.
- Using a **multicast address**, packets are delivered to all nodes on a network.
- An **anycast address** is used by routers. The address identifies multiple destinations, and packets are delivered to the closest destination.

A unicast address identifies a single interface on a network. The three types of unicast addresses are global, link-local, and unique local addresses, which are graphically shown in Figure 15-10.

**Global Address**

<table>
<thead>
<tr>
<th>3 bits</th>
<th>45 bits</th>
<th>16 bits</th>
<th>64 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>Global Routing Prefix</td>
<td>Subnet ID</td>
<td>Interface ID</td>
</tr>
</tbody>
</table>

**Link Local Address**

<table>
<thead>
<tr>
<th>64 bits</th>
<th>64 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111 1110 1000 0000 0000 0000 0000 ... 0000 FE80::/64</td>
<td>Interface ID</td>
</tr>
</tbody>
</table>

**Unique Local Address**

<table>
<thead>
<tr>
<th>8 bits</th>
<th>40 bits</th>
<th>16 bits</th>
<th>64 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111 1100 = FC 1111 1101 = FD</td>
<td>Global ID</td>
<td>Subnet ID</td>
<td>Interface ID</td>
</tr>
</tbody>
</table>

Figure 15-10  Three types of IPv6 addresses

Here is a description of each of the three types:

- A **global unicast address**, also called a **global address**, can be routed on the Internet. These addresses are similar to IPv4 public IP addresses. Most global addresses begin with the prefix 2000::/3, although other prefixes are being released. The /3 indicates that the first three bits are fixed and are always 001.
- A **link-local unicast address**, also called a **link-local address** or local address, can be used for communicating with nodes in the same link. These addresses are similar to IPv4 private IP addresses and are sometimes called link-local addresses or local addresses and most begin with FE80::/64. (This prefix notation means the address begins with FE80 followed by enough zeros to make 64 bits.) Link-local addresses are not allowed on the Internet.
- A **unique local unicast address**, also called a **unique local address (ULA)**, is used to identify a specific site within a large organization. For example, an organization might have these two sites: employee.mycompany.com and support.mycompany.com. The
address prefixes used for unique local addresses are FC00::/7 and FD00::/8. The Global ID portion of the address is assigned by the organization. Unique local addresses are not allowed on the Internet. They are hybrid addresses between a global unicast address that works on the Internet and a link-local address that works on only one link.

Notice in Figure 15-10 that global and unique local addresses contain a block labeled the Subnet ID, which is the last block in the 64-bit prefix of an IP address. Recall that when using IPv4, the subnet could be identified by any number of bits at the beginning of the IP address. Using IPv6, a subnet is identified using some or all of the 16 bits in the Subnet ID block. Using IPv6, a subnet is, therefore, identified as one or more links that have the same 64 bits in the IP address prefix. This definition implies that a local link is itself a subnet.

Table 15-4 lists the currently used address prefixes for these types of IP addresses. In the future, we can expect more prefixes to be assigned as they are needed.

<table>
<thead>
<tr>
<th>IP Address Type</th>
<th>Address Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global unicast</td>
<td>2000::/3</td>
</tr>
<tr>
<td></td>
<td>(First 3 bits are always 001)</td>
</tr>
<tr>
<td>Link-local unicast</td>
<td>FE80::/64</td>
</tr>
<tr>
<td></td>
<td>(First 64 bits are always 1111 1110 1000 0000 0000 0000 .. 0000)</td>
</tr>
<tr>
<td>Unique local unicast</td>
<td>FC00::/7</td>
</tr>
<tr>
<td></td>
<td>(First 7 bits are always 1111 110)</td>
</tr>
<tr>
<td></td>
<td>FD00::/8</td>
</tr>
<tr>
<td></td>
<td>(First 8 bits are always 1111 1101)</td>
</tr>
<tr>
<td>Multicast</td>
<td>FF00::/8</td>
</tr>
<tr>
<td></td>
<td>(First 8 bits are always 1111 1111)</td>
</tr>
</tbody>
</table>

Table 15-4 Address prefixes for types of IPv6 addresses

A+ Exam Tip The A+ 220-801 exam expects you to know the prefixes listed in Table 15-4.

Notes An excellent resource for learning more about IPv6 and how it works is the ebook, TCP/IP Fundamentals for Microsoft Windows. To download the free PDF, search for it at www.microsoft.com/download.

VIEW IP ADDRESS SETTINGS

The Ipconfig command can be used in a command prompt window to show the IPv4 and IPv6 IP addresses assigned to all network connections (see Figure 15-11).

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

- Windows has assigned the wireless connection two IP addresses, one using IPv4 and one using IPv6.
- The Ethernet LAN connection has also been assigned an IPv4 address and an IPv6 address.

The IPv6 addresses are followed by a % sign and a number; for example, %13 follows the first 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.
IPv6 addressing is designed so that a computer can autoconfigure 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 randomly generating 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 router is present on the network to provide configuration information. If a router responds with DHCP information, the computer uses whatever information this might be, such as the IP addresses of DNS servers or its own IP address. Because a computer can generate its own link-local IP address, a DHCPv6 server usually serves up only global IPv6 addresses.

**CHARACTER-BASED NAMES IDENTIFY COMPUTERS AND NETWORKS**

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

- **A host name**, also called a **computer name**, is the name of a computer and can be used in place of its IP address. Examples of host names are www, ftp, Jean’s Computer, TestBox3, and PinkLaptop. You assign a host name to a computer when you first configure it for a network connection. The name can have up to 63 characters, including letters, numbers, and special characters. On a local network, you can use the computer name in the place of an IP address to identify a computer. To find out and change the computer name in Windows 7/Vista, click **Start**, right-click **Computer**, and select
Properties from the shortcut menu. In the System window, click Advanced system settings. In the System Properties box, click the Computer Name tab (see Figure 15-12).

To rename a computer, click Change. (For XP, click Start, right-click My Computer, and select Properties from the shortcut menu. Then click the Computer Name tab.)

![Figure 15-12 View and change the computer name](Source: Microsoft Windows 7)

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.

A domain name identifies a network. Examples of domain names are the names that appear before the period in microsoft.com, course.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) identifies a computer and the network to which it belongs. An example of an FQDN is www.course.com. The host name is www (a web server), course is the domain name, and com is the top-level domain name of the Course Technology network. Another FQDN is joesmith.mycompany.com.

On the Internet, a fully qualified domain name must be associated with an IP address before this computer can be found. This process of associating a character-based name with an IP address is called name resolution. The DNS (Domain Name System or Domain Name Service) protocol is used by a DNS server to find an IP address for a computer when the fully qualified domain name is known. Your ISP is responsible for providing you access to one or more DNS servers as part of the service it provides for Internet access. When a
When a web-hosting site first sets up your web site, IP address, and domain name, 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 your site.

A+ Exam Tip The A+ 220-802 exam expects you to be familiar with client-side DNS.

Notes When you enter a fully qualified domain name such as www.cengage.com in a browser address bar, that name is translated into an IP address followed by a port number. It's interesting to know that you can skip the translation step and enter the IP address and port number in the address box. See Figure 15-13.

Figure 15-13 A web site can be accessed by its IP address and port number: http://69.32.133.79:80

When Windows is trying to resolve a computer name to an IP address, it first looks in the DNS cache it holds in memory. Information in this cache includes what it loaded at startup from the Hosts file in the C:\Windows\System32\drivers\etc folder. This file, which has no file extension, contains computer names and their associated IP addresses on the local network. An administrator is responsible for manually editing the hosts file when the association is needed on the local network. If the computer name is not found in the hosts file, 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.

Notes For an entry in the Hosts file to work, the remote computer must always use the same IP address. One way to accomplish this is to assign a static IP address to the computer. Alternately, if your DHCP server supports this feature, you can configure it to assign the same IP address to this computer each time if you tell the DHCP server the computer’s MAC address. This method of computer name resolution is often used for intranet web servers, Telnet servers, and other servers.

TCP/IP Protocol Layers

Recall that a protocol is an agreed-to set of rules for communication between two parties. Operating systems and client/server applications on the Internet all use protocols that are supported by TCP/IP. The left side of Figure 15-14 shows these different layers of protocols and how they relate to one another. As you read this section, this figure can serve as your road map to the different protocols.
In the following sections, the more significant applications and operating system protocols are introduced. However, you should know that the TCP/IP protocol suite includes more protocols than just those mentioned in this chapter; only some of them are shown in Figure 15-14.

### TCP/IP Protocols Used by the OS

Looking back at Figure 15-14, you can see three layers of protocols between the applications and the hardware protocols. 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 shown underneath TCP and UDP, which control communication on the network.

Remember that all communication on a network happens by way of packets delivered from one location on the network to another. In TCP/IP, the protocol that guarantees packet delivery is TCP (Transmission Control Protocol). TCP makes a connection, checks whether the data is received, and resends it if it is not. TCP is, therefore, called a **connection-oriented protocol**. 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 IP layer to establish a session between client and server to verify that communication has taken place. When a TCP packet reaches its destination, an acknowledgment is sent back to the source (see Figure 15-15). 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 15-15** TCP guarantees delivery by requesting an acknowledgment

On the other hand, UDP (User Datagram Protocol) does not guarantee delivery by first connecting and checking whether data is received; thus, UDP is called a **connectionless protocol** or **best-effort protocol**. UDP is used for broadcasting, such as streaming video or sound over the web, where guaranteed delivery is not as important as fast transmission. UDP is also used to monitor network traffic.

**TCP/IP PROTOCOLS USED BY APPLICATIONS**

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 protocols used by these and other applications:

- **HTTP.** HTTP (Hypertext Transfer Protocol) is the protocol used for the World Wide Web and used 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 of a browser, such as http://www.microsoft.com.

- **HTTPS.** HTTPS (HTTP secure) is the HTTP protocol working with a security protocol such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), which is better than SSL, to create a secured socket. HTTPS is used by web browsers and servers to encrypt the data before it is sent and then decrypt it 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.

- **SMTP.** SMTP (Simple Mail Transfer Protocol) is used to send an email message to its destination (see Figure 15-16). An improved version of SMTP is **SMTP AUTH (SMTP Authentication)**. This protocol is used to authenticate a user to an email server when the
email client first tries to connect to the email server to send email. Using SMTP AUTH, an extra dialogue between the client and server happens before the client can fully connect that proves the client is authorized to use the service. After authentication, the client can then send email to the email server. The email server that takes care of sending email messages (using the SMTP protocol) is often referred to as the SMTP server.

![Figure 15-16](image.png) 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.

- **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)** or **IMAP4 (Internet Message Access Protocol, version 4)**. Using POP, email is downloaded to the client computer. Using IMAP, the client application manages the email stored on the server.

- **Telnet.** The **Telnet** protocol is used by the 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.

- **LDAP.** **Lightweight Directory Access Protocol (LDAP)** 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. Another example is when an application looks for a printer by querying a database of printers supported by an organization on the corporate network or Internet. Data sent and received using the LDAP protocol is not encrypted; therefore, an encryption layer is sometimes added to LDAP transmissions.

- **SMB.** **Server Message Block (SMB)** is the protocol used by Windows to share files and printers on a network.

- **FTP.** **FTP (File Transfer Protocol)** is used to transfer files between two computers. Web browsers can use the protocol. Also, special FTP client software such as CuteFTP by GlobalSCAPE (www.cuteftp.com), can be used, which offers more features for file transfer than does a browser. To use FTP in Internet Explorer version 9, enter the address of an FTP site in the address box, for example, ftp.cengage.com. A logon dialog box appears where you can enter a username and password (see Figure 15-17). When you click Log on, you can see folders on the
FTP site and the FTP protocol displays in the address bar, as in ftp://ftp.cengage.com. It’s easier to use Windows Explorer to transfer files rather than Internet Explorer. After you have located the FTP site, to use Windows Explorer for file transfers, press Alt, which causes the menu bar to appear. In the menu bar, click View, Open FTP site in Windows Explorer (see Figure 15-18). Then click Allow in the Internet Explorer Security box. Windows Explorer opens, showing files and folders on the FTP site. You can copy and paste files and folders from your computer to the site.

![Figure 15-17 Log on to an FTP site](Source: Microsoft Windows 7)

![Figure 15-18 Use Windows Explorer to transfer files using the FTP protocol](Source: Microsoft Windows 7)

**SSH.** The Secure Shell (SSH) protocol is used to pass login information to a remote computer and control that computer over a network. Transmissions are encrypted so they cannot be intercepted by a hacker.
**SFTP.** Secure FTP (SFTP) is used to transfer files from an FTP server to an FTP client using encryption. The encryption layer of the protocol used by Secure FTP is a variation of the SSH (Secure Shell) protocol.

**SNMP.** Simple Network Management Protocol (SNMP) is used to monitor network traffic. It is used by the Microsoft SNMP Agent application that monitors traffic on a network and helps balance that traffic.

**RDP.** Remote Desktop Protocol (RDP) is used by the Windows Remote Desktop and Remote Assistance utilities to connect to and control a remote computer.

---

**A+ Exam Tip** The A+ 220-801 exam expects you to know about the following application protocols: FTP, Telnet, SMTP, DNS, HTTP, POP3, IMAP, HTTPS, RDP, DHCP, LDAP, SNMP, SMB, SSH, and SFTP.

---

Recall that client/server applications use ports to address each other. Table 15-5 lists the port assignments for common applications.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol and App</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>FTP client</td>
<td>The FTP client receives data on port 20 from the FTP server.</td>
</tr>
<tr>
<td>21</td>
<td>FTP server</td>
<td>The FTP server listens on port 21 for commands from an FTP client.</td>
</tr>
<tr>
<td>22</td>
<td>SSH server</td>
<td>A server using the SSH protocol listens at port 22.</td>
</tr>
<tr>
<td>23</td>
<td>Telnet server</td>
<td>A Telnet server listens at port 23.</td>
</tr>
<tr>
<td>25</td>
<td>SMTP email server</td>
<td>An email server listens at port 25 to receive email from a client computer.</td>
</tr>
<tr>
<td>53</td>
<td>DNS server</td>
<td>A DNS server listens at port 53.</td>
</tr>
<tr>
<td>67</td>
<td>DHCP client</td>
<td>A DHCP client receives data from a DHCP server at port 67.</td>
</tr>
<tr>
<td>68</td>
<td>DHCP server</td>
<td>A DHCP server listens for requests at port 68.</td>
</tr>
<tr>
<td>80</td>
<td>Web server using HTTP</td>
<td>A web server listens at port 80 when receiving HTTP requests.</td>
</tr>
<tr>
<td>110</td>
<td>POP3 email client</td>
<td>An email client using POP3 receives email at port 110.</td>
</tr>
<tr>
<td>143</td>
<td>IMAP email client</td>
<td>An email client using IMAP receives email at port 143.</td>
</tr>
<tr>
<td>443</td>
<td>Web server using HTTPS</td>
<td>A web server listens at port 443 when receiving HTTPS transmissions.</td>
</tr>
<tr>
<td>3389</td>
<td>RDP apps, including Remote Desktop and</td>
<td>Remote Desktop and Remote Assistance listen at port 3389.</td>
</tr>
<tr>
<td></td>
<td>Remote Assistance</td>
<td></td>
</tr>
</tbody>
</table>

Table 15-5 Common TCP/IP port assignments for client/server applications

---

**A+ Exam Tip** The A+ 220-801 expects you to know the common port assignments of the FTP, Telnet, SMTP, DNS, HTTP, POP3, IMAP, HTTPS, and RDP protocols. Before sitting for this exam, be sure to memorize the ports listed in Table 15-5.
Now that you have an understanding of TCP/IP and Windows networking, let’s apply that knowledge to making network connections.

**Connecting a Computer to a Network**

Connecting a computer to a network is quick and easy in most situations. In this part of the chapter, you’ll learn to connect a computer to a network using Ethernet, wireless, and dial-up connections.

**Connect to a Wired Network**

To connect a computer to a network using a wired (Ethernet) connection, follow these steps:

1. If the network adapter is not yet installed, install it now. These steps include physically installing the card, installing drivers, and using Device Manager to verify that Windows recognizes the adapter without errors.
2. Connect a network cable to the Ethernet port (called an RJ-45 port) and to the network wall jack or directly to a switch or router. Indicator lights near the network port should light up to indicate connectivity and activity. If you connected the cable directly to a switch or router, verify the light at that port is also lit.
3. By default, Windows assumes dynamic IP addressing and automatically configures the network connection. To find out if the connection is working, open Windows Explorer and drill down into the Network group (see Figure 15-19). (For Windows XP, click **Start, My Network Places** to open the My Network Places window.) You should see icons that represent other computers on the network. Double-click a computer and drill down to shared folders and files to verify you can access these resources.
4. To verify you have Internet connectivity, open Internet Explorer and browse to a few web sites.

**Hands-on Project 15-1 Practice Using FTP**

Practice using FTP by downloading the latest version of Firefox, a web browser, using these methods. Do the following:

1. Using your current browser, go to the Mozilla web site at [www.mozilla.org](http://www.mozilla.org) and download the latest version of Firefox. What is the version number? What is the name of the downloaded file? In what folder on your hard drive did you put the file?
2. Using your current browser as an FTP client, locate the same version of Firefox and the same file at the Mozilla FTP site ([ftp.mozilla.org](http://ftp.mozilla.org)) and download it to your PC. What is the path to the Firefox file on the FTP site? In what folder on your hard drive did you put the file?

Now that you have an understanding of TCP/IP and Windows networking, let’s apply that knowledge to making network connections.
If the connection does not work, it’s time to verify that network settings are configured correctly. Follow these steps using Windows 7:

1. Verify that Device Manager recognizes the network adapter without errors. If you find an error, try updating the network adapter drivers. If that doesn’t work, then try uninstalling and reinstalling the drivers. Make sure Device Manager recognizes the network adapter without errors before you move on to the next step.

2. To open the Network and Sharing Center, open Control Panel and click Network and Sharing Center. (You can also click the network icon in the taskbar.) The Network and Sharing Center window opens (see Figure 15-20).
3. A red X indicates a problem. Click the X to get help and resolve the problem. Windows Network Diagnostics starts looking for problems, applying solutions, and making suggestions. You can also check these things:

- Is the network cable connected?
- Are status light indicators on the network port and router or switch lit or blinking appropriately to indicate connectivity and activity?

4. After Windows has resolved the problem, you should see a clear path from the computer to the Internet, as shown in Figure 15-21. Use Windows Explorer to try again to access resources on the local network, and use Internet Explorer to try to access the Internet.

If you still do not have connectivity, follow these steps to verify and change TCP/IP settings:

1. In the Network and Sharing Center, click Change adapter settings. In the Network Connections window, right-click the local area connection and select Properties from the shortcut menu. The properties box appears (see Figure 15-22).

2. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties. The properties box shown in Figure 15-23 (a) appears. Settings are correct for dynamic IP addressing.

Notes Notice in Figure 15-22 that you can uncheck Internet Protocol Version 6 (TCP/IPv6) to disable it. For most situations, you need to leave it enabled. A bug in Windows 7 prevents you from joining a homegroup if IPv6 is disabled.
3. To change the settings to static IP addressing, select **Use the following IP address**. Then enter the IP address, subnet mask, and default gateway. (A **default gateway** is the gateway a computer uses to access another network if it does not have a better option.)

4. If you have been given the IP addresses of DNS servers, check **Use the following DNS server addresses** and enter up to two IP addresses. If you have other DNS IP addresses, click **Advanced** and enter them on the **DNS** tab of the Advanced TCP/IP Settings box.
5. If the computer you are using is a laptop that moves from one network to another and one network uses static IP addressing, you can click the **Alternate Configuration** tab and configure an **alternate IP address** (see Figure 15-23 [b]). On this tab, select **User configured**. Then enter a static IP address, subnet mask, default gateway, and DNS server addresses. When you configure the General tab to use dynamic IP addressing, the computer will first try to use dynamic IP addressing. If that is not available on the network, it then applies the static IP address settings entered on the Alternate Configuration tab. If static IP address settings are not available on this tab, the computer uses an automatic private IP address (APIPA). This setup works well for a computer to receive a dynamic IP address while traveling, but use a static IP address when connected to the company network that uses static IP addressing.

![A+ Exam Tip](image)

**A+ Exam Tip** The A+ 220-802 exam expects you to know how to configure an alternate IP address, including setting the static IP address, subnet mask, DNS addresses, and gateway.

6. Close all boxes and windows and again try to access network resources. If you still don’t have connectivity, try to disable and enable the network connection. To do that, right-click the connection in the Network Connections window and select **Disable** (see Figure 15-24). For dynamic IP addressing, the IP address is released. Then right-click again and select **Enable**. The connection is remade and a new IP address is leased.

![Figure 15-24](image)

**Figure 15-24** To reset a network connection, disable and enable the connection

If you still don’t have local or Internet access, it’s time to dig a little deeper into the source of the problem. Troubleshooting network connections is covered in Chapter 17.

![Vista Differences](image)

**Vista Differences** To find out how to connect a Vista computer to a wired network, see Appendix B.

![XP Differences](image)

**XP Differences** To find out how to connect an XP computer to a wired network and how to verify TCP/IP settings for the connection, see Appendix C.
CONNECT TO A WIRELESS NETWORK

Wireless networks are either unsecured public hotspots or secured private hotspots. Even if you connect to a secured private hotspot, still be careful to protect your data and other Windows resources from attack. In this part of the chapter, you learn how to connect to unsecured and secured wireless networks.

Here are the steps to connect to a wireless network using Windows 7 and how to protect your computer on that network:

1. If necessary, install the wireless adapter. For external adapters such as the one shown in Figure 15-25, be sure to follow the manufacturer’s instructions for the installation. Most likely you’ll be asked to first install the software before installing the device. During the installation process, you will be given the opportunity to use the manufacturer’s configuration utility to manage the wireless adapter or to use Windows to do the job. For best results, use the utility provided by the manufacturer. In the following steps, we're using the Windows utility.

2. For embedded wireless, turn on your wireless device. For some laptops, that’s done by a switch on the keyboard (see Figure 15-26) or on the side of the laptop. The wireless antenna is usually in the lid of a notebook and gives best performance when the lid is fully raised. For a desktop computer, make sure the antenna is in an upright position (see Figure 15-27).

3. A yellow star in the network icon in the taskbar indicates hotspots are available. Double-click the network icon to see a list of networks. Click one to select it and then click Connect (see Figure 15-28).

4. If the network is secured, Windows asks for the security key the first time you connect (see Figure 15-29). Enter the security key or password to the network and click OK.

5. If the network is unsecured or you don’t trust all the users of the network, verify that Windows has configured the network as a Public network. To do so, open the Network and Sharing Center window (see Figure 15-30). If the network location says
Figure 15-26  Turn on the wireless switch on your laptop

Figure 15-27  Raise the antenna on a NIC to an upright position

Home network or Work network, click it. The Set Network Location box appears (see Figure 15-31). Click Public network and click Close. The Network and Sharing Center reports the network location as Public network.

6. Open your browser to test the connection. For some hotspots, a home page appears and you must enter a code or agree to the terms of use before you can use the network.

In addition to a security key used to access a secured wireless network, the network might be set up for even more security. A wireless network is created by a wireless device known
as the wireless access point. Here is a list of methods that the wireless access point might use to secure the wireless network:

- **A security key is required.** This is the most common method of securing a wireless network. A network that uses a security key encrypts data on the network using an encryption standard. You learn about these standards later in the chapter.
- **The SSID is not broadcasted.** The wireless device might not be broadcasting its name, which is called the Service Set Identifier (SSID). If the SSID is not broadcasting, the
The name of the wireless network will appear as Unnamed or Unknown Network. When you select this network, you are given the opportunity to enter the name. If you don’t enter the name correctly, you will not be able to connect.

**Only computers with registered MAC addresses are allowed to connect.** If MAC address filtering is used, you must give the network administrator the MAC address of your wireless adapter. This address is entered into a table of acceptable MAC addresses kept by the wireless access point.

To know the MAC address of your wireless adapter, for an external adapter, you can look on the back of the adapter itself (see Figure 15-32) or in the adapter documentation.
Also, if the adapter is installed on your computer, you can open a command prompt window and enter the command `ipconfig /all`, which displays your TCP/IP configuration for all network connections. In the results displayed, the MAC address is called the Physical Address (see Figure 15-33).

If you have problems connecting to a wireless network, here are the steps to follow to verify the network settings:

1. In the left pane of the Network and Sharing Center, click Manage wireless networks. The Manage Wireless Networks window appears (see the left side of Figure 15-34).
2. Using this window, you can change the order of networks that Windows uses to try to make a wireless connection. To view security settings, double-click a network in the list. The Properties box for the wireless network appears.

![Figure 15-34 Verify the Network security key for the wireless network is correct](source: Microsoft Windows 7)

3. On the Properties box, click the Security tab, which is shown in the right side of Figure 15-34. Check Show characters so that you can verify the Network security key is correct. Windows 7 should automatically sense the Security type and Encryption type for the wireless network, and these values should be correct. Change the Network security key, if necessary.

4. Click OK to close the Properties box. Windows should automatically connect to the network. If you still cannot connect, know that troubleshooting network connections is covered in Chapter 17.

**Vista Differences** To find out how to connect a Vista computer to a wireless network, see Appendix B.

**XP Differences** To find out how to connect an XP computer to a wireless network, see Appendix C.
CONNECT TO A WIRELESS WAN (CELLULAR) NETWORK

To connect a computer using mobile broadband to a wireless wide area network (WWAN), also called a cellular network, such as those provided by Verizon or AT&T, you need the hardware and software to connect and a SIM card. A SIM (Subscriber Identification Module) card is a small flash memory card that contains all the information you need to connect to a cellular network, including a password and other authentication information needed to access the network, encryption standards used, and the services that your subscription includes. SIM cards are used in cell phones, mobile broadband modems, and other devices that use a cellular network (see Figure 15-35).

**Hands-on Project 15-2 Investigate a Wireless Connection**

Using a computer connected to a wireless network, do the following:

1. In the Network and Sharing Center, click Manage wireless networks. Right-click the wireless connection and click Properties to view the Properties box for the wireless network. Is the network secured? If so, what is the security type? What is the encryption type?

2. Open the Properties box for the Wireless Network Connection. Is the connection using TCP/IPv4? TCP/IPv6?

3. View the TCP/IPv4 settings for the wireless adapter. Is the wireless connection using static or dynamic IP addressing?

4. Using the Ipconfig command, what is the IPv4 IP address for the wireless connection? What is the MAC address of the wireless adapter?

**Figure 15-35** A SIM card contains proof that your device can use a cellular network
Here are your options for hardware and software:

- **Use an embedded mobile broadband modem.** A laptop might have an embedded broadband modem. In this situation, you still need to subscribe to a mobile operator, which will provide you with a SIM card for your laptop.

- **Tether your cell phone to your computer.** You can tether your cell phone to your computer by way of a cable that connects your cell phone to a USB port. See Figure 15-36. (Some cell phones don’t have a USB port; in this situation, you have to purchase a special cable that works with your proprietary phone connector and a USB port on your computer.) A cell phone with Wi-Fi capabilities can be used to provide a Wi-Fi hotspot that your computer and other devices can connect to. In this situation, the cell phone acts like a wireless router. An app installed on the phone is used to configure the WLAN created by the phone.

- **Use a USB broadband modem.** For any computer, you can use a USB broadband modem (sometimes called an air card), such as the one shown in Figure 15-37. If you purchase the device from your mobile operator, a SIM card is included. If you purchase the modem from another source, you need to go to your mobile operator (for example, AT&T, Verizon, or Sprint) to obtain the SIM card the device will use to verify your subscription to the cellular network. A USB broadband modem is likely to give you access to a cellular network as well as a Wi-Fi network.

  Mobile operators and laptop manufacturers with embedded modems provide software and instructions for connecting to the cellular network. Follow those instructions rather than the generic ones presented here. Generally, here’s how you can connect to a cellular network:

- **Using an embedded broadband modem.** For a laptop with an embedded broadband modem, you must insert the SIM card provided by your mobile operator in the SIM card slot on the laptop. For some laptops, this slot might be in the battery bay, and...
you must remove the battery to find the slot. Then use a program installed on the laptop by the laptop manufacturer to connect to the cellular network. Look for a shortcut on the desktop or a program in the Start menu. In addition, the mobile operator might provide software for you to use.

▲ Using your cell phone. To tether your cell phone to your computer to use a cellular network, know that you need a subscription from your mobile operator to use this service. The mobile operator is likely to provide you software on CD, or you can download the software from the operator’s web site. Install the software first and then tether your cell phone to your computer. Use the software to make the connection.

▲ Use a USB broadband modem. When using a USB broadband modem, make sure the SIM card is inserted in the device (see Figure 15-38). When you insert the modem into a USB port, Windows finds the device, and the software stored on the device automatically installs and runs. A window then appears provided by the software that allows you to connect to the cellular network.

Here are more details of how to connect to a WWAN. In this example, we are using the Sierra Wireless modem shown earlier in Figure 15-37. Do the following to make the connection:

1. For best results, connect your computer to a wired network during the first part of the installation.

2. Insert the device into the USB port, and Windows automatically installs the device drivers stored on the device as well as the management software to use the device. Then the management software launches where you must accept the licensing agreement. A shortcut is added to your desktop and programs in the Start menu.

3. You must go to the web site of your mobile operator (AT&T in our example) and activate the phone number used by the modem. Then for best results, remove the modem and restart your computer.
4. After your computer restarts, plug in the modem. Wait until LED lights on the modem indicate the modem has found a network and is ready to connect. For this device, a solid blue light on the left indicates power is on, and a blinking green light on the right indicates the device has found a network and is ready to connect.

5. Start the Communication Manager software. When the software starts, it automatically connects to the network (see Figure 15-39). Note that if your computer is connected to a cellular network, it disconnects from a Wi-Fi network.

6. To test the connection, unplug your network cable and try to surf the web. The speed of the connection depends on the type of cellular network you are using, 2G, 3G, or 4G. The 4G networks are the fastest. For the device we are using, the color of the LED indicates the type of network (solid amber is 2G, solid blue is 3G or 4G, solid green is 4G LTE, which currently is the fastest type of cellular network).
To manage the broadband modem and the WWAN connection, you can do the following:

1. Open the Network and Sharing Center. You should see the Mobile Broadband Connection (see Figure 15-40). Make sure the network location is set to Public network.

2. Use Ipconfig to see the IP address assigned to the connection. In Figure 15-41, you can see the IPv4 IP address is a public IP address.

3. Device Manager should report the modem is installed with no errors. If you are having problems making the connection, start by checking Device Manager. If errors are reported here, update the device drivers.
CREATE A DIAL-UP CONNECTION

You never know when you might be called on to support an older dial-up connection. Here are the bare-bones steps you need to set up and support this type of connection:

1. Install an internal or external dial-up modem. Make sure Device Manager recognizes the card without errors.
2. Plug the phone line into the modem port on your computer and into the wall jack.
3. Open the Network and Sharing Center window and click Set up a new connection or network. In the dialog box that appears, select Set up a dial-up connection and click Next.
4. In the next box (see Figure 15-42), enter the phone number to your ISP, your ISP username and password, and the name you decide to give the dial-up connection, such as the name and city of your ISP. Then click Connect.

To use the connection, go to the Network and Sharing Center and click Connect to a network (see Figure 15-40). Alternately, you can click your network icon in the taskbar. A bubble appears above your taskbar (see Figure 15-43). Select the dial-up connection, and click Connect. The Connect dialog box appears, where you can enter your password (see Figure 15-44). Click Dial. You will hear the modem dial up the ISP and make the connection. (For XP, double-click the connection icon in the Network Connections window, and then click Dial.)
Figure 15-43  Select the dial-up connection and then click the Connect button that appears.

Figure 15-44  Enter the password to your ISP.
If the dial-up connection won’t work, here are some things you can try:

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

**CREATE A VPN CONNECTION**

A virtual private network (VPN) is often used by employees when they work away from the corporate network to connect to that network by way of the Internet. A VPN protects data by encrypting it from the time it leaves the remote computer until it reaches a server on the corporate network. The encryption technique is called a tunnel or tunneling (see Figure 15-45).
The VPN is often managed by client/server software such as Citrix Access Gateway by Citrix Systems (www.citrix.com). Also, Windows can create a VPN connection rather than using third-party software. A VPN connection is a virtual connection, which means you are really setting up the tunnel over an existing connection to the Internet. When creating a VPN connection on a personal computer, always follow directions given by the network administrator who set up the VPN. The company web site might provide VPN client software to download and install on your PC.

Here are the general steps to use Windows 7 to connect to a VPN:

1. In the Network and Sharing Center, click **Set up a new connection or network**. In the set up box, click **Connect to a workplace** and click **Next**.

2. In the **Connect to a Workplace** box, click **Use my Internet connection (VPN)**. In the next box, enter the IP address or domain name of the network (see Figure 15-46). Name the VPN connection and click **Next**.

3. Enter your username and password to the VPN and click **Connect**. If you want to just set up the connection without connecting to the VPN, in the next box, click **Skip**. The connection is ready to use. Click **Close** to close the wizard.

Whenever you want to use the VPN connection, click the network icon in the taskbar. In the list of available networks, click the VPN connection (see Figure 15-47) and then click **Connect**. A box similar to the one shown earlier in Figure 15-44 appears where you can enter your username and password and click **Connect**. After the connection is made, you can use your browser to access the corporate secured intranet web sites or other resources. The resources you can access depend on the permissions assigned the user account.
Setting Up a Multifunction Router for a SOHO Network

Hands-on Project 15-3  Investigate TCP/IP Settings

Using a computer connected to a network, answer these questions:

1. What is the hardware device used to make this connection (network card, onboard port, wireless)? List the device’s name as Windows sees it in the Device Manager window.

2. What is the MAC address of the wired or wireless network adapter? What command or window did you use to get your answer?

3. What is the IPv4 IP address of the network connection?

4. Are your TCP/IP version 4 settings using static or dynamic IP addressing?

5. What is the IPv6 IP address of your network connection?

6. Disable and enable your network connection. Now what is your IPv4 IP address?

Setting Up a Multifunction Router for a SOHO Network

A PC support technician is likely to be called on to set up a small office or home office network. As part of setting up a small network, you need to know how to configure a multipurpose router to stand between the network and the Internet. You also need to know how to set up and secure a wireless access point. Most SOHO routers are also a wireless access point.

A+ Exam Tip  The A+ 220-801 and A+ 220-802 exams expect you to be able to install, configure, and secure a SOHO wired and wireless router.
FUNCTIONS OF A SOHO ROUTER

Routers can range from small ones designed to manage a SOHO network connecting to an ISP (costing around $75 to $150) to those that manage multiple networks and extensive traffic (costing several thousand dollars). On a small office or home network, a router stands between the ISP network and the local network (see Figure 15-48), and the router is the gateway to the Internet. Note in the figure that computers can connect to the router using wired or wireless connections.

![Figure 15-48 A router stands between a local network and the ISP network and manages traffic between them](image)

This router is typical of many SOHO routers and is several devices in one:

- **Function 1:** As a router, it stands between the ISP network and the local network, routing traffic between the two networks.
- **Function 2:** As a switch, it manages several network ports that can be connected to wired computers or to a switch that provides more ports for more computers.
- **Function 3:** As a DHCP server, all computers can receive their IP address from this server.
- **Function 4:** As a wireless access point, a wireless computer can connect to the network. This wireless connection can be secured using wireless security features.
- **Function 5:** As a firewall, it blocks unwanted traffic initiated from the Internet and provides Network Address Translation (NAT) so that computers on the LAN can use private or link local IP addresses. Another firewall feature is to restrict Internet access for computers behind the firewall. Restrictions can apply to days of the week, time of day, keywords used, or certain web sites.
- **Function 6:** As an FTP server, you can connect an external hard drive to the router, and the FTP firmware on the router can be used to share files with network users.
An example of a multifunction router is the Linksys E4200 by Cisco shown in Figures 15-49 and 15-50. It has one port for the broadband modem (cable modem or DSL modem) and four ports for computers on the network. The USB port can be used to plug in a USB external hard drive for use by any computer on the network. The router is also a wireless access point having multiple antennas to increase speed and range using Multiple In, Multiple Out (MIMO) technology. The antennas are built in.

**Notes** The speed of a network depends on the speed of each device on the network and how well a router manages that traffic. Routers, switches, and network adapters currently run at three speeds: Gigabit Ethernet (1000 Mbps or 1 Gbps), Fast Ethernet (100 Mbps), or Ethernet (10 Mbps). If you want your entire network to run at the fastest speed, make sure all your devices are rated for Gigabit Ethernet.
INSTALL AND CONFIGURE THE ROUTER ON THE NETWORK

To install a router on the network, always follow the directions of the manufacturer rather than the general directions given here. Using the Linksys E4200 as our example router, here is how to install it on the network:

1. On one of your computers on the network (it doesn’t matter which one), launch the setup program on the CD that came bundled with the router. The setup program instructs you to use one network cable to connect the computer to the router and a second network cable to connect the router to the DSL or cable modem box using the Internet port on the router. After you have made the connections, click Next on the setup screen.

2. On the next screen, you are given the opportunity to change the SSID and password to the router. Be sure to change the password. On the next screen, you can decide to allow or not allow the router to receive automatic updates from Cisco.

3. The setup program says you should be connected to the Internet. Verify the connection by opening your browser and surfing the web. You can then close the router setup program.

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

Using any computer on the network, you can use your browser and the firmware on the router to configure it at any time. To do so, follow these steps:

1. Open your browser and enter the IP address of the router, 192.168.1.1, in the address box. The Windows Security box appears (see Figure 15-51). Enter admin as the username and the password is the one you set up when installing the router.

Figure 15-51 Enter the username and password to your router firmware utility
2. The main setup page of the router firmware appears in your browser window (see Figure 15-52). Use the menus near the top of the screen and items on each menu to change your router’s configuration. Each router utility is different, but you should be able to poke around and find the setting you need. When finished, click Save Settings and close the browser window.

![Router name or SSID]

**Figure 15-52** Use menus on the router firmware utility screens to configure your router

Following are some changes that you might need to make to the router’s configuration. If you make changes on a page, be sure to click Save Settings to save your changes. The first setting should always be done:

- **Change the router password.** It’s extremely important to protect access to your network and prevent others from hijacking your router. If you have not already done so, change the default password to your router firmware. If the firmware offers the option, disable the ability to configure the router from over the wireless network (see Figure 15-53).
- **Change the SSID and configure the DHCP server.** On the Basic Setup menu shown earlier in Figure 15-52, you can change the name of the router (the SSID), and you can enable or disable the DHCP server. For the DHCP server, you set the start IP address and set the number of IP addresses DHCP can serve up.
View assignments made by the ISP. The router belongs to both the local network and the ISP network. On the Status page shown in Figure 15-54, you can see the ISP has assigned the router a private IP address on its network. You can also use this page to release and renew this IP address, which might help solve a problem when you cannot connect to the ISP.

**Figure 15-53**  Prevent others from hijacking your router

**Figure 15-54**  The ISP has assigned the router a private IP address

**Notes**  If you are running a web server on the Internet, the web server must use a public and static IP address. For this situation, you can lease a public IP address from your ISP at an additional cost.
Assign static IP addresses. A computer or network printer might require a static IP address. For example, when a computer is running a web server on the local network, it needs a static IP address that you can add to the Hosts file for each computer on the network that needs to access this intranet web site. A network printer also needs a static IP address so computers will always be able to find the printer. To assign a static IP address to a client, click DHCP Reservation on the Setup page shown earlier in Figure 15-52. In the DHCP Reservation box, select a client from the DHCP table and click Add Clients. Then click Save Settings. In Figure 15-55, a Canon network printer is set to receive the IP address 192.168.1.118 each time it connects to the network.

Configure the firewall to disable all ports. On the Security page, you can enable SPI Firewall Protection (see Figure 15-56). SPI (stateful packet inspection) examines each data packet and rejects those unsolicited by the local network. Using this setting, all ports are disabled (closed) and no activity initiated from the Internet can get in. You can allow exceptions to this firewall rule by using port forwarding, port triggering, or a DMZ. How to do so is coming up in the next section.

Improve QoS for an application. As you use your network and notice that one application is not getting the best service, you can improve network performance for this application using the Quality of Service (QoS) feature. For example, suppose you routinely use Skype to share your desktop with collaborators over the Internet. To assign a high priority to Skype, go to the Applications & Gaming tab (see Figure 15-57). Under Internet Access Priority, select Enabled. Under Category, in the drop-down list of Applications, select Skype. Under Priority, select High and click Apply. Skype is added in the Summary area. If you don’t see your application listed, you can click Add a New Application in the drop-down list of applications and enter its name.

Now let’s look at the concepts and steps to allow certain activity initiated from the Internet past your firewall. Then we’ll look at how to set up a wireless network.
Figure 15-56 Configure the router’s firewall to prevent others on the Internet from seeing or accessing your network.

Figure 15-57 Use the QoS feature to assign a high priority to an application to improve its network service.
PORT FORWARDING, PORT TRIGGERING, AND A DMZ

Suppose you’re hosting an Internet game or want to use Remote Desktop to access your home computer from the Internet. In both situations, you need to enable (open) certain ports so that activity initiated from the Internet can get past your firewall.

Recall that a router uses NAT redirection to present its own IP address to the Internet in place of IP addresses of computers on the local network. The NAT protocol is also responsible for passing communication to the correct port on the correct local computer.

Here are the ways a router can use NAT to open or close certain ports:

- **Port filtering** is used to open or close certain ports so they can or cannot be used. Remember that applications are assigned these ports. Therefore, in effect, you are filtering or controlling what applications can or cannot get through the firewall. For example, in Figure 15-58a, all requests from the Internet to ports 20, 443, 450, and 3389 are filtered or disabled. These ports are closed.

- **Port forwarding** means that when the firewall receives a request for communication from the Internet to a specific computer and port, the request will be allowed and forwarded to that computer on the network. The computer is defined to the router by its static IP address. For example, in Figure 15-58a, port 80 is open and requests to
port 80 are forwarded to the web server that is listening at that port. This one computer on the network is the only one allowed to receive requests at port 80.

Port triggering opens a port when a PC on the network initiates communication through another port. For example, in Figure 15-58b, Computer C sends data to port 50 to a computer on the Internet. The router is configured to open port 80 for communication from this remote computer. Port 80 is closed until this trigger occurs. Port triggering does not require a static IP address for the computer inside the network, and any computer can initiate port triggering. The router will leave port 80 open for a time. If no more data is received from port 50, then it closes port 80.

To configure port forwarding or port triggering, use the Applications & Gaming tab shown in Figure 15-59. In the figure, the Remote Desktop application outside the network can use port forwarding to communicate with the computer whose IP address is 192.168.1.90 using port 3389. The situation is illustrated in Figure 15-60. This computer is set to support the Remote Desktop server application. You will learn to use Remote Desktop in Chapter 17.

To configure port triggering, click the Port Range Triggering tab and enter the two ranges of ports. For example, in Figure 15-61, the Triggered Range of ports will trigger the event to open the ports listed under Forwarded Range.

Here are some tips to keep in mind when using port forwarding or port triggering:

- You must lease a static IP address from your ISP so that people on the Internet can find you. Most ISPs will provide you a static IP address for an additional monthly fee.
- For port forwarding to work, the computer on your network must have a static IP address so that the router knows where to send the communication.
- If the computer using port triggering stops sending data, the router might close the triggered port before communication is complete. Also, if two computers on the network attempt to trigger the same port, the router will not allow data to pass to either computer.
Using port forwarding, your computer and network are more vulnerable because you are allowing external users directly into your private network. For better security, turn on port forwarding only when you know it’s being used.

A demilitarized zone (DMZ) in networking is a computer or network that is not protected by a firewall. You can drop all your shields protecting a computer by putting it in a DMZ and the firewall no longer protects it. If you are having problems getting port forwarding or port triggering to work, putting your computer in a DMZ can free it to receive any communication from the Internet. Enter its IP address or MAC address on the DMZ page of the router utility (see Figure 15-62) under Destination. You can also specify that any IP address on the Internet is allowed access or you can limit access to a specific IP address. It goes without saying to not leave the DMZ enabled unless you are using it.
CHAPTER 15754 Connecting to and Setting Up a Network

SET UP A WIRELESS NETWORK

The standards for a local wireless network are called Wi-Fi (Wireless Fidelity), and their technical name is IEEE 802.11. The IEEE 802.11 standards, collectively known as the 802.11 a/b/g/n standards, have evolved over the years and are summarized in Table 15-6.

**Table 15-6** Older and current Wi-Fi standards

<table>
<thead>
<tr>
<th>Wi-Fi Standard</th>
<th>Speeds, Distances, and Frequencies</th>
</tr>
</thead>
</table>
| IEEE 802.11a   | • Speeds up to 54 Mbps (megabits per second).  
                  • Short range up to 50 meters with radio frequency of 5.0 GHz.  
                  • 802.11a is no longer used. |
| IEEE 802.11b   | • Up to 11 Mbps with a range of up to 100 meters. (Indoor ranges are less than outdoor ranges.)  
                  • The radio frequency of 2.4 GHz experienced interference from cordless phones and microwaves. |
| IEEE 802.11g   | • Same as 802.11b, but with a speed up to 54 Mbps. |
| IEEE 802.11n   | • Up to 500 Mbps depending on the configuration.  
                  • Indoor range up to 70 meters and outdoor range up to 250 meters.  
                  • Can use either 5.0 GHz or 2.4 GHz radio frequency. |

---

Notes By the way, if you want to use a domain name rather than an IP address to access a computer on your network from the Internet, you’ll need to purchase the domain name and register it in the Internet name space to associate it with your static IP address assigned by your ISP. Several web sites on the Internet let you do both; one site is by Network Solutions at www.networksolutions.com.

**A+ Exam Tip** The A+ 220-801 exam expects you to know about 802.11 a/b/g/n standards, their speeds, distances, and frequencies.

**Figure 15-62** Put a computer in a DMZ so that the router firewall does not prevent it from receiving communication from the Internet
The latest Wi-Fi standard, 802.11n, uses **multiple input/multiple output (MIMO)**, which means a device can use two or more antennas to improve performance (see Figure 15-63). Most wireless devices today are 802.11 b/g/n compatible.

When setting up a wireless network, position your router or the stand-alone wireless access point in the center of where you want your hotspot and know that a higher position (near the ceiling) works better than a lower position (on the floor). Be sure to set the device in a physically secure place and not in a public area where it can be stolen.

When configuring an 802.11n network, consider these options:

- **The radio frequency (RF) the network will use.** Choices for radio frequency (RF) are 5 GHz and 2.4 GHz. The 5 GHz frequency yields faster speeds than the 2.4 GHz frequency, but the range is shorter. For best performance in a small space, use 5 GHz. Use 2.4 GHz if your hotspot must reach a longer distance. Use both frequencies so they can share the network traffic.
- **The older wireless devices that will use the network.** If your network must support older 802.11 b/g wireless devices, you must support the 2.4 GHz frequency.
- **The RF interference the network will experience.** Interference for 2.4 GHz frequency might come from cordless phones, microwaves, and other Wi-Fi networks. The 5 GHz frequency is less likely to experience this interference.
- **The channel the network will use.** A channel is a specific radio frequency within a broader frequency. For example, two channels in the 5 GHz band are 5.180 GHz and 5.200 GHz channels. In the United States, eleven channels are allowed for 5 GHz or 2.4 GHz bands (Channels 1 through 11). For most networks, you can allow auto channel selection so that any channel in the frequency range (5 GHz or 2.4 GHz) will work. The device scans for the least-busy channel. However, if you are trying to solve a problem with interference from a nearby wireless network, you can set each network to a different channel; make the channels far apart to reduce interference. For example, set one network to Channel 1 and set the other to Channel 11.
- **The channel width the network will use.** For a 5 GHz network, choices are 40 MHz and 20 MHz channel widths. For best performance, use 40 MHz. For less interference, use 20 MHz.
The radio power level the device will use. Some high-end access points allow you to adjust the radio power levels the device can use. To reduce interference, limit the range of the network, or to save on electricity, reduce the power level.

For the firmware utility of the Linksys E4200 wireless router, you can change wireless settings on the Wireless tab when you click Manual (see Figure 15-64). Notice in the figure the two wireless setting groups; one is for the 5 GHz range and the other is for the 2.4 GHz range. Unless you have a reason to do otherwise, you can leave the Network Mode for each group set to Mixed, which allows 801.11 b/g/n connections in the 5 GHz or 2.4 GHz band. Notice in the figure that the Channel and Channel Width for each band are set to Auto. If necessary, you can specify a channel or channel width. To force a device to use one band or the other, set a different passphrase for each band.

Figure 15-64 Configure settings for the wireless network

It is important to secure a wireless network from outside attack. Recall that securing a wireless network is generally done in three ways:

Method 1: Requiring a security key and using data encryption—If encryption is used when you connect to a wireless network, a security key is required. If no security key is required, the data on the wireless network is not encrypted. The three main protocols for encryption for 802.11 wireless networks are:

- **WEP.** WEP (Wired Equivalent Privacy) is no longer considered secure because the key used for encryption is static (it doesn’t change).
Setting Up a Multifunction Router for a SOHO Network

- **WPA.** WPA (Wi-Fi Protected Access) also called TKIP (Temporal Key Integrity Protocol) encryption, is stronger than WEP and was designed to replace it. With WPA encryption, encryption keys are constantly changing.
- **WPA2.** WPA2 (Wi-Fi Protected Access 2), also called the 802.11i standard, is the latest and best wireless encryption standard. It is based on the AES (Advanced Encryption Standard), which improved on the way TKIP generated encryption keys. All wireless devices sold today support the WPA2 standard.

To configure encryption for the Cisco router, select Manual in the Wireless Settings page shown in Figure 15-64 and select the Security Mode from the drop-down menu. For best security, enter a passphrase (security key) to the wireless network that is different from the password you use to the router utility.

**Notes**

To make the strongest passphrase or security key, use a random group of numbers, uppercase and lowercase letters, and, if allowed, at least one symbol. Also use at least eight characters in the passphrase.

- **Method 2: Disable SSID broadcasting**—You can disable SSID broadcasting and change the SSID on the Wireless page shown in Figure 15-64. This security method is not considered strong security because software can be used to discover an SSID that is not broadcasted.
- **Method 3: Filter MAC addresses**—A wireless access point can filter the MAC addresses of wireless adapters to either allow or not allow these MAC addresses access to the wireless network (see Figure 15-65). MAC address filtering is considered a weak security measure and does not use encryption.

You also need to know about **Wi-Fi Protected Setup (WPS)**, which is designed to make it easier for users to connect their computers to a wireless network when a hard-to-remember SSID and security key are used. WPS generates the SSID and security key using a random string of hard-to-guess letters and numbers. The SSID is not broadcasted, so both the SSID and security key must be entered to connect. Rather than having to enter these difficult strings,
a user presses a button on a wireless computer or the router’s PIN or computer’s PIN is used. All computers on the wireless network must support WPS for it to be used. WPS is enabled on the Wireless page of the router utility shown in Figure 15-66.

![Figure 15-66](image.png)

**Figure 15-66** Using WPS, it is easy for users to connect to a wireless network with strong security

*A+ Exam Tip* The A+ 220-801 exam expects you to know about installing and configuring a wireless network, including MAC filtering, Wi-Fi channels (1–11), SSID broadcasting, WEP, WPA, WPA2, TKIP, AES, and WPS.

The A+ 220-802 exam expects you to know about installing and configuring a wireless network, including changing default usernames and passwords, disabling and changing the SSID, using MAC filtering, antenna and access point placements, radio power levels, and assigning static IP addresses.

### Hands-on Project 15-4 Research a Wireless LAN

Suppose you have a DSL connection to the Internet in your home and you want to connect two laptops and a desktop computer in a wireless network to the Internet. You need to purchase a multifunction wireless router like the one you learned to configure in this chapter. You also need a wireless adapter for the desktop computer. (The two laptops have built-in wireless.) Use the web to research the equipment needed to create the wireless LAN and answer the following:

1. Print two web pages showing two different multifunctional wireless routers. What are the brand, model, and price of each router?

2. Print two web pages showing two different wireless adapters a desktop computer can use to connect to the wireless network. Include one external device that uses a USB port and one internal device. What are the brand, model, and price of each device?

3. Which router and wireless adapter would you select for your home network? What is the total cost of both devices?
Understanding TCP/IP and Windows Networking

- Networking communication happens at three levels: hardware, operating system, and application levels.
- At the hardware level, a network adapter has a MAC address that uniquely identifies it on the network.
- Using the TCP/IP protocols, the OS identifies a network connection by an IP address. At the application level, 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 IP address using IPv4 has 32 bits, and an IP address using IPv6 has 128 bits.
- Classes of IPv4 IP addresses used by the public are Class A, Class B, and Class C addresses. Some IP addresses are private IP addresses that can be used only on intranets.
- If a computer is unable to obtain an IP address from a DHCP server, Windows uses Automatic Private IP Addressing (APIPA) to assign the computer an IP address unless an alternate static IP address has been configured for the computer.
- Using IPv6, three types of IP addresses are a unicast address (used by a single node on a network), multicast address (used for one-to-many transmissions), and anycast address (used by routers).
- Three types of unicast addresses are a global unicast address (used on the Internet), a link local unicast address (used on a private network), and a unique local unicast address (used on subnets in a large enterprise).
- A computer can be assigned a computer name (also called a host 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 protocols at the application level (such as FTP, HTTP, and Telnet) and at the operating system level (such as TCP and UDP).

Connecting a Computer to a Network

- A PC support person needs to know how to configure TCP/IP settings and make a wired or wireless connection to an existing network.
- The best method to secure a wireless network is to use encryption (which requires you enter a security key to connect). Two other methods that are sometimes used to secure a network are to not broadcast the SSID (which requires you enter the SSID to connect) and MAC address filtering (which requires the network administrator enter the MAC address of your wireless adapter in a table). These last two methods provide weak security and are not recommended.
- To connect to a wireless WAN or cellular network, you need a mobile broadband modem, a SIM card, and a subscription to the cellular network. The mobile operator provides you a SIM card with your subscription. Your cell phone can serve as the mobile broadband modem when you tether it to your computer.
- A dial-up connection uses a telephone modem to make a connection to an ISP.
Setting Up a Multifunction Router for a SOHO Network

- A multifunction router for a small-office-home-office network might serve several functions, including a router, a switch, a DHCP server, a wireless access point, a firewall using NAT, and an FTP server.
- It’s extremely important to change the password to configure your router as soon as you install it, especially if the router is also a wireless access point.
- To allow certain network traffic initiated on the Internet past your firewall, you can use port forwarding, port triggering, and a DMZ.
- To secure a wireless access point, you can enable MAC address filtering, disable SSID broadcasting, and enable encryption (WPA2, WPA, or WEP).

>> KEY TERMS

For explanations of key terms, see the Glossary near the end of the book.

6TO4  
802.11 a/b/g/n  
adapter address  
AES (Advanced Encryption Standard)  
alternate IP address  
anycast address  
Automatic Private IP Address (APIPA)  
best-effort protocol  
channel  
Class A  
Class B  
Class C  
classful subnet mask  
classless subnet mask  
client/server  
computer name  
connectionless protocol  
connection-oriented protocol  
default gateway  
DHCP (dynamic host configuration protocol)  
DHCP client  
DMZ  
DNS (Domain Name System or Domain Name Service)  
DNS client  
DNS server  
domain name  
dynamic IP address  
FTP (File Transfer Protocol)  
fully qualified domain name (FQDN)  
gateway  
global address  
global unicast address  
hardware address  
host name  
Hosts file  
HTTP (Hypertext Transfer Protocol)  
HTTPS (HTTP secure)  
IMAP4 (Internet Message Access Protocol, version 4)  
interface  
interface ID  
Internet Protocol version 4 (IPv4)  
Internet Protocol version 6 (IPv6)  
intranet  
IP address  
ISATAP  
Lightweight Directory Access Protocol (LDAP)  
link  
link-local address  
link-local unicast address  
local area network (LAN)  
local link  
loopback address  
MAC (Media Access Control) address  
multicast address  
multicasting  
multiple input/multiple output (MIMO)  
name resolution  
NAT (Network Address Translation)  
eighbors  
network adapter  
octet  
packet  
physical address  
POP3 (Post Office Protocol, version 3)  
port  
port address  
port filtering  
port forwarding  
port number  
port triggering  
private IP addresses  
protocols  
public IP addresses  
Quality of Service (QoS)  
radio frequency (RF)  
Remote Desktop Protocol (RDP)  
router  
Secure FTP (SFTP)  
Secure Shell (SSH)  
Server Message Block (SMB)  
Service Set Identifier (SSID)  
SIM (Subscriber Identification Module) card  
Simple Network Management Protocol (SNMP)  
SMTP (Simple Mail Transfer Protocol)  
SMTP AUTH (SMTP Authentication)  
static IP address  
subnet  
subnet ID  
subnet mask  
TCP (Transmission Control Protocol)
TCP/IP (Transmission Control Protocol/Internet Protocol)  
Telnet  
Teredo  
TKIP (Temporal Key Integrity Protocol)  
UDP (User Datagram Protocol)  
unicast address  
unique local address (ULA)  
unique local unicast address  
virtual private network (VPN)  
WEP (Wired Equivalent Privacy)  
Wi-Fi (Wireless Fidelity)  
Wi-Fi Protected Setup (WPS)  
wireless access point  
wireless wide area network (WWAN)  
WPA (Wi-Fi Protected Access)  
WPA2 (Wi-Fi Protected Access 2)

1. How many bits are in a MAC address?
2. How many bits are in an IPv4 IP address? In an IPv6 IP address?
3. How does a client application identify a server application on another computer on the network?
4. What are IP addresses called that begin with 10, 172.16, or 192.168?
5. In what class is the IP address 185.75.255.10?
6. In what class is the IP address 193.200.30.5?
7. Describe the difference between public and private IP addresses. If a network is using private IP addresses, how can the computers on that network access the Internet?
8. Why is it unlikely that you will find the IP address 192.168.250.10 on the Internet?
9. In Figure 15-9, the subnet mask is four notches tall and is considered a classless subnet mask for this network of sticks. How many notches tall would be a classful subnet mask for the same network?
10. If no DHCP server is available when a computer configured for dynamic IP addressing connects to the network, what type of IP address is assigned to the computer?
11. If a computer is found to have an IP address of 169.254.1.1, what can you assume about how it received that IP address?
12. What are the last 64 bits of a IPv6 IP address called? How are these bits used?
13. Name at least three tunneling protocols that are used for IPv6 packets to travel over an IPv4 network.
14. How is an IPv6 IP address used that begins with 2000::? That begins with FE80::?
15. How many bits are in the Subnet ID block? What are the values of these bits for a link-local IP address?
16. Which type of IPv6 address is used to create multiple sites within a large organization?
17. What type of server serves up IP addresses to computers on a network?
18. Which TCP/IP protocol that manages packet delivery guarantees that delivery? Which protocol does not guarantee delivery, but is faster?
19. At what port does an SMTP email server listen to receive email from a client computer?
20. Which protocol does a web server use when transmissions are encrypted for security?
21. What type of server resolves fully qualified domain names to IP addresses?
22. Which email protocol allows a client application to manage email stored on an email server?

23. What type of protocol is used to present a public IP address to computers outside the LAN to handle requests to use the Internet from computers inside the LAN?

24. Which protocol is used when an application queries a database on a corporate network such as a database of printers?

25. What type of encryption protocol does Secure FTP (SFTP) use to secure FTP transmissions?

26. What two Windows applications use the RDP protocol and port 3389?

27. Which version of 802.11 technologies can use two antennas at both the access point and the network adapter?

28. Which wireless encryption standard is stronger, WEP or WPA?

29. When securing a Wi-Fi wireless network, which is considered better security: to filter MAC addresses, use encryption, or not broadcast the SSID?

30. Would you expect WPS to be used when a wireless network is using strong security, weak security, or no security (as in a public hotspot)?

**THINKING CRITICALLY**

1. You have just installed a network adapter and have booted up the system, installing the drivers. You open Windows Explorer on a remote computer and don’t see the computer on which you just installed the NIC. What is the first thing you check?
   a. Has TCP/IPv6 been enabled?
   b. Is the computer using dynamic or static IP addressing?
   c. Are the lights on the adapter functioning correctly?
   d. Has the computer been assigned a computer name?

2. 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 FTP server. Why is it not a good idea to use Telnet to reach the remote computer?
   a. Telnet transmissions are not encrypted.
   b. Telnet is not reliable and the file might arrive corrupted.
   c. FTP is faster than Telnet.
   d. FTP running on the same computer as Telnet causes Telnet to not work.

3. Your job is to support the desktop computers in a small company of 32 employees. A consulting firm is setting up a private web server to be used internally by company employees. The static IP address of the server is 192.168.45.200. Employees will open their web browser and enter personnel.mycompany.com in the URL address box to browse this web site. What steps do you take so that each computer in the company can browse the site using this URL?
REAL PROBLEM 15-1: Setting Up a Small Network

The simplest possible wired network is two computers connected together using a crossover cable. In a crossover cable, the send and receive wires are crossed so that one computer can send and the other computer receive on the same wire. At first glance, a crossover cable looks just like a regular network cable (also called a patch cable) except for the labeling (see Figure 15-67). (In Chapter 16, you learn how to distinguish between the cables by examining their connectors.)

Figure 15-67  A patch cable and crossover cable look the same but are labeled differently

Do the following to set up and test the network:

1. Connect two computers using a crossover cable. Using the Network and Sharing Center, verify your network is up. What is the IP address of Computer A? Of Computer B?
2. Join the two computers to the same homegroup. Then use Windows Explorer to view the files on the other computer shared with the homegroup.
3. Convert the TCP/IP configuration to static IP addressing. Assign a private IP address to each computer. What is the IP address of Computer A? Of Computer B?
4. Verify you can still see files shared with the homegroup on each computer.