7-1 Understanding TCP/IP and Windows Networking

Core 1 Objectives

- 2.1

  Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

- 2.4

  Summarize services provided by networked hosts.

- 2.5

  Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

- 2.6

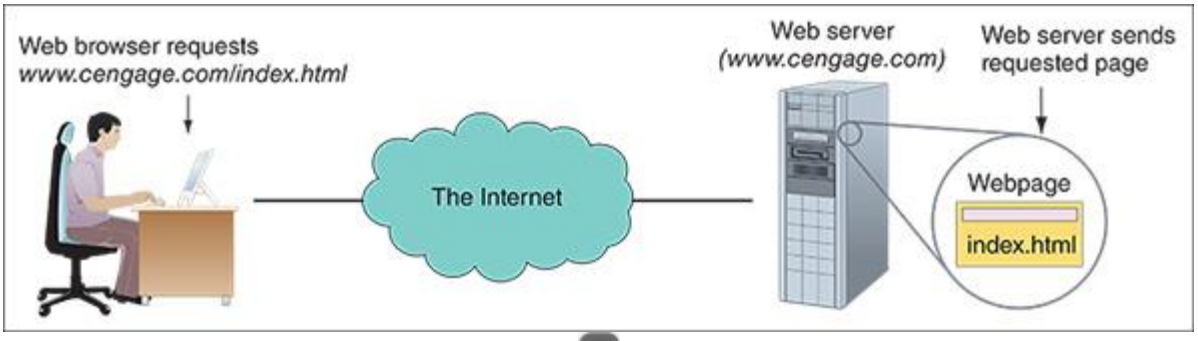
  Compare and contrast common network configuration concepts.

This section of the module focuses on how a network works. Network communication begins when one application on one computer tries to find another application on another computer on a local or remote network. Most applications used on the Internet or a local network are **client/server applications**. Client applications—such as Microsoft Edge, Google Chrome, or Outlook—usually initiate communication with server applications such as a web server or email server.

For example, in Figure 7-1, someone uses a web browser (the client) to request a webpage from a **web server**. To handle this request, the client computer looks for the web server, the protocols (or rules for communication) are established, and then the request is made and answered. The application, the OS and hardware on both computers, and the network are all involved in this process.

Figure 7-1

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



Both computers are called hosts or nodes on the network:

- A **host** is a computer that can be either the client or the server using client/server applications.
- A **node** is any computer, printer, smart thermostat, or other networked device that can be addressed on the network. Every host is a node, but not every node is a host.

Let's see how computers and networking devices can be addressed on a network.

7-1a Addresses Used on a Network

Core 1 Objectives

- 2.1

Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

- 2.5

Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

The following three types of numeric addresses are used for communication on a network:

- **Port address identifies an application.** Each client or server application running on a computer is identified by a **port address**, also called a port or a port number. For example, a web server receives communication from a browser at port 80 using the HTTP protocol for unsecured communication and at port 443 using the HTTPS protocol for secured communication.
- **IP address identifies a node and its network connection.** An **IP address** is assigned to a node when the device first connects to the network, and it identifies the network connection. The following are two types of IP addresses:

- A 32-bit string, written as four decimal numbers called octets and separated by periods, such as 192.168.100.4
- A 128-bit string, written as eight hexadecimal numbers separated by colons, such as 2001:0000:B80:0000:0000:D3:9C5A:CC

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

- **MAC address identifies a network adapter.** Every wired or wireless network adapter, also called a network interface card (NIC), has a 48-bit (6-byte) identification number—called the **MAC address**, physical address, or network adapter address—hard-coded on the card by its manufacturer. Part of the MAC address identifies the manufacturer, who is responsible for making sure that no two network adapters have the same MAC address. Every device on a network (for example, computers, printers, smart thermostats, refrigerators, and smartphones) connects to the network by way of its NIC and its MAC address. An example of a MAC address, written in hexadecimal or hex, is 00-0C-6E-4E-AB-A5. Most likely, the MAC address is printed on the device (see Figure 7-2). Later in the module, you learn to use the ipconfig command to find out the MAC address of your installed NIC.

Figure 7-2

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

7-1b TCP/IP Model for Network Communication

Core 1 Objective

- 2.1

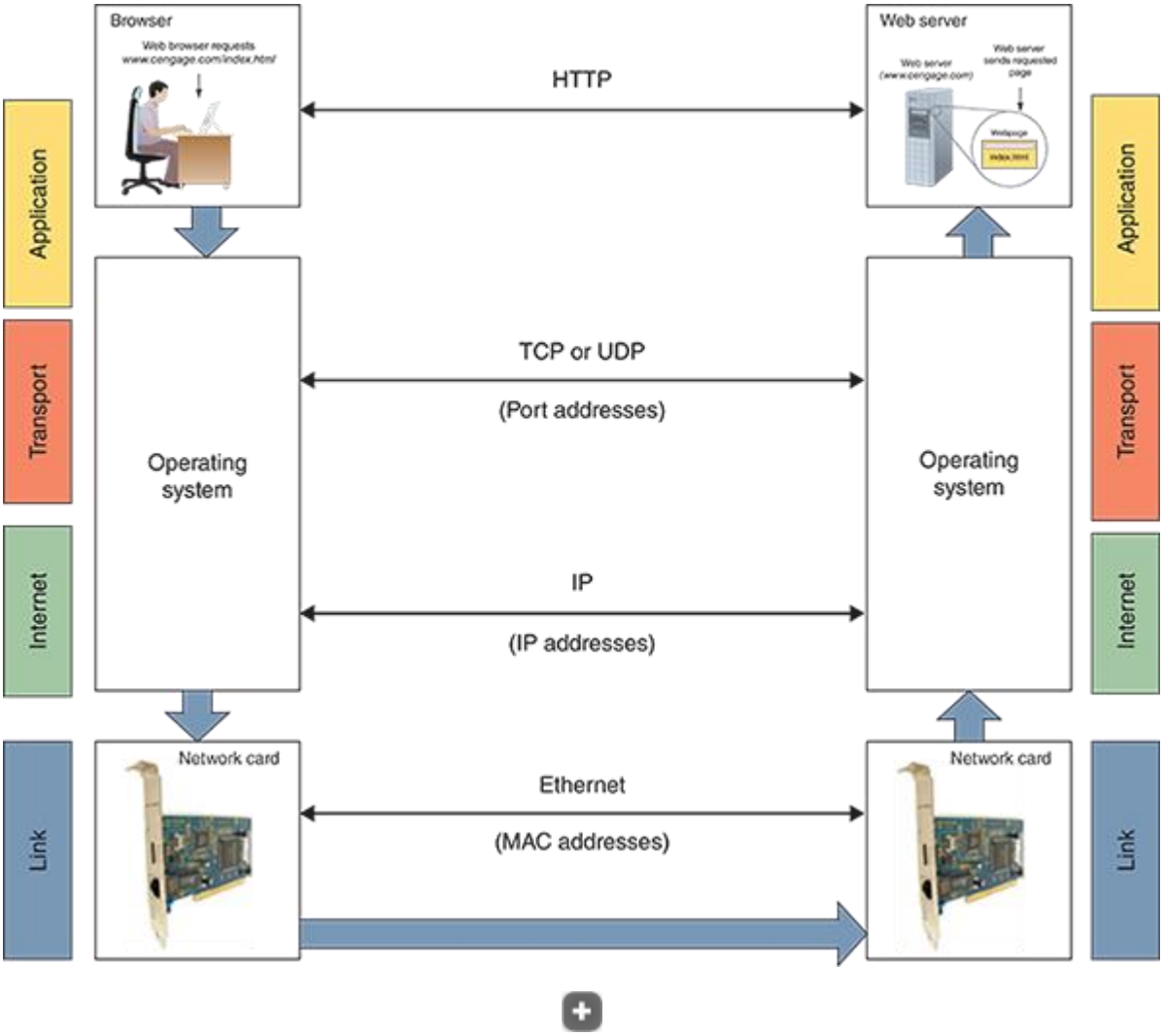
Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

The suite of protocols or rules that define network communication is called **TCP/IP (Transmission Control Protocol/Internet Protocol)**. Let's consider network communication that starts when a browser (an application) requests a webpage from a web server (another application). As you follow the blue arrows through the diagram, shown in Figure 7-4, you can see the layers of communication. The browser app passes the request to the OS, which passes the request to the network card, which passes the request on to the network. When the request reaches the network card on

the server, the network card passes the request on to the OS, and then the OS passes it on to the web server application.

Figure 7-4

Network communication happens in layers



When studying networking theory, a simple model used to divide network communication into four layers is the **TCP/IP model**. In this model, protocols used by hardware function at the Link layer, and protocols used by the OS are divided into three layers (Internet, Transport, and Application layers). These four layers are shown on the left and right sides of Figure 7-4 and listed in Table 7-1.

Table 7-1

TCP/IP Model Has Four Layers of Communication

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

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

- **Source Step 1: Application layer.** Recall that most applications that use a network are client/server applications. When a browser client makes a request to a web server, the browser passes the request to the OS. The OS formats the message using the appropriate application protocol (for example, HTTP, FTP, Telnet, DNS, and SSH). In our example, an HTTP message is created and passed down in the TCP/IP stack of protocols to the Transport layer.
- **Source Step 2: Transport layer.** The Transport layer adds information to the message to address the correct server application. Depending on the type of application, the protocol TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) adds the port assigned to the server application (TCP uses port 80 for HTTP communication in our example). The message with Transport data added is then passed down to the Internet layer.
- **Source Step 3: Internet layer.** The Internet layer is responsible for getting the message to the destination computer or host on the local network, an intranet, or the Internet. An **intranet** is any private network that uses TCP/IP protocols. A large enterprise might support an intranet that is made up of several local networks. The primary protocol used at the Internet layer is **IP (Internet Protocol)**, which uses an IP address to identify each host. (Other Internet layer protocols include EIGRP, OSPF, BGP, and ICMP.) IP adds address information to the message and then passes it down to the Link layer.
- **Source Step 4: Link layer.** The Link layer is the physical network, including the hardware and its firmware for every device connected to the network. A computer's network interface card (NIC) is part of this physical network. As you know, each NIC is able to communicate with other NICs on the local network using each NIC's MAC address. For a

local network, the physical connection might be wireless (most likely using Wi-Fi) or wired (most likely using Ethernet). The NIC receives the message from IP, adds information for Ethernet or Wi-Fi transmission, and places the message on the network.

- **Step 5: Network transmission.** IP at the Internet layer is responsible for making sure the message gets from one network to the next until it reaches its destination network (see Figure 7-5) and destination computer on that network. Whereas a MAC address at the hardware Link layer is only used to find a computer or other host on a local area network (LAN), an IP address can be used to find a computer on a local network, anywhere on the Internet (see Figure 7-6), or on an intranet.

Figure 7-5

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

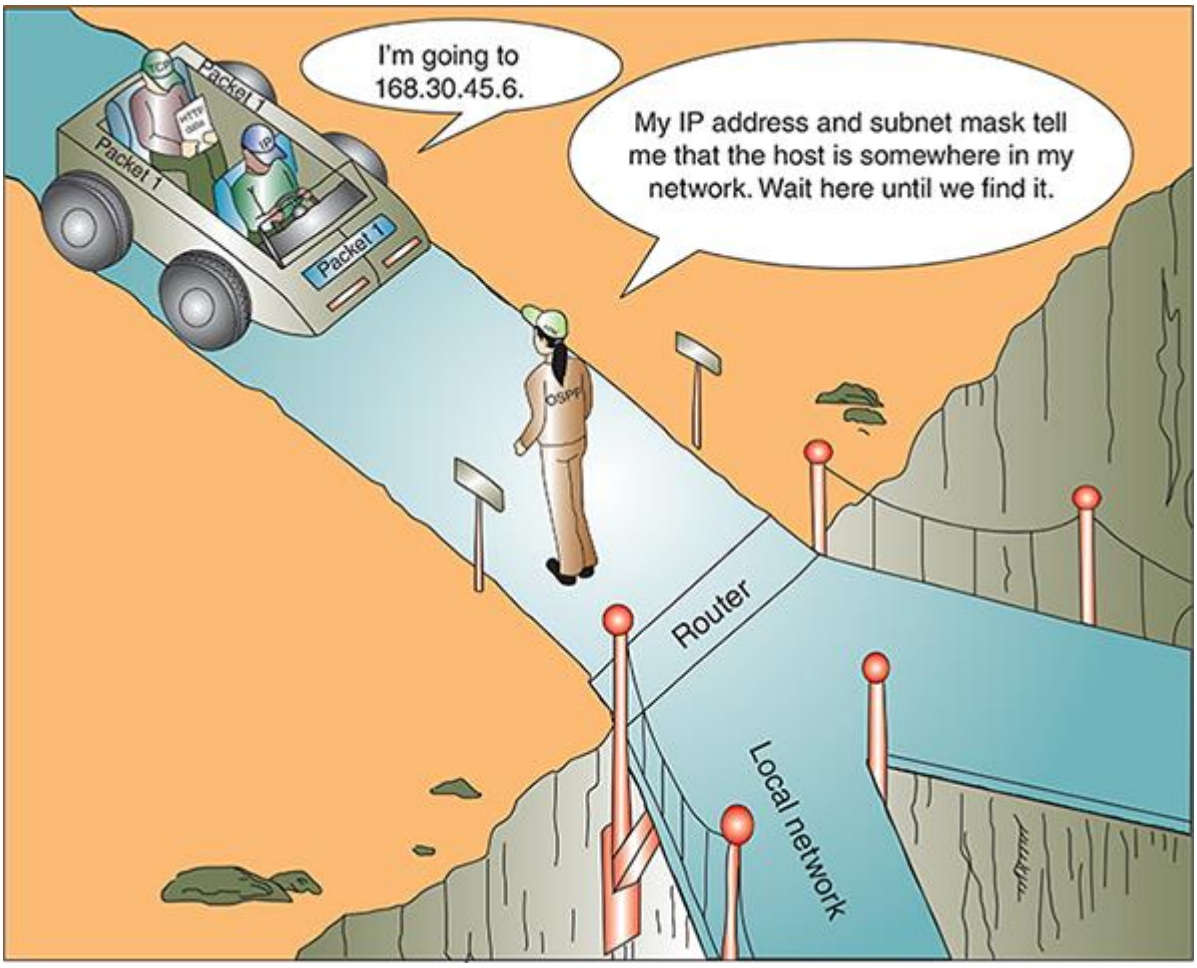
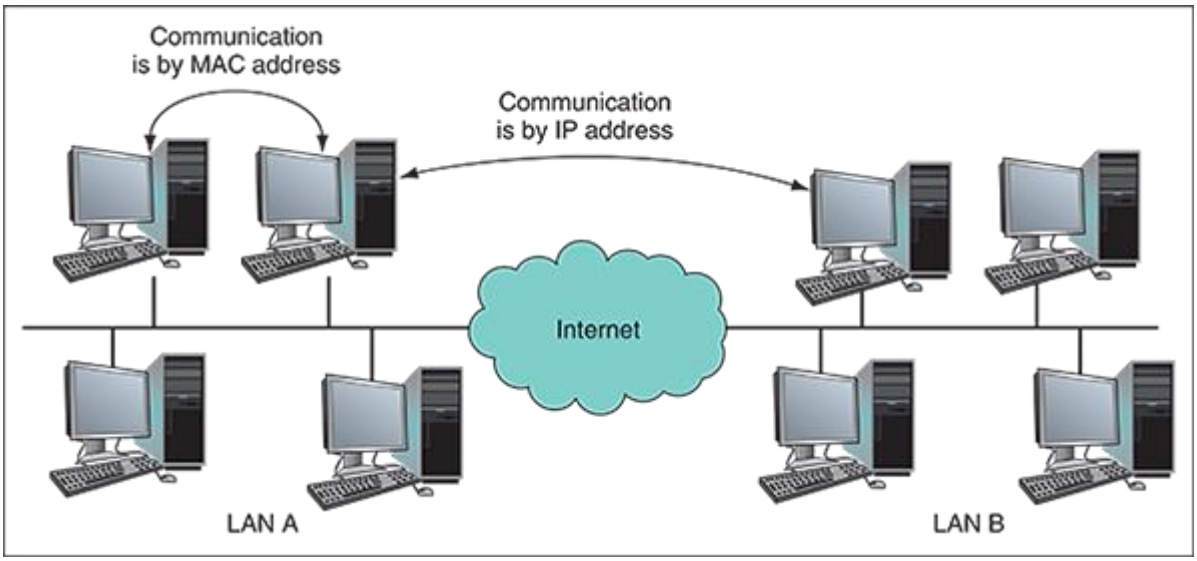


Figure 7-6

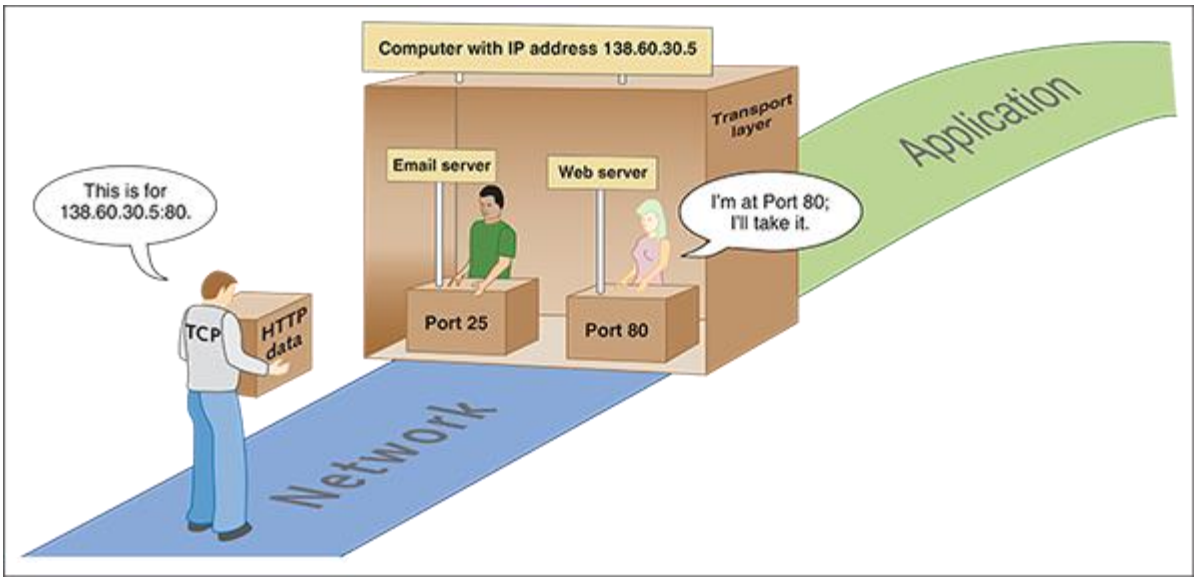
Computers on the same LAN can use MAC addresses to communicate, but computers on different LANs use IP addresses to communicate over the Internet



- **Step 6: Destination.** On the destination computer, its NIC receives the message, strips off Ethernet or Wi-Fi information at the Link layer, and passes the message up to the Internet layer. The Internet layer strips off IP address information and passes the message up to the Transport layer. The Transport layer strips off TCP or UDP information and passes the message to the correct port (see Figure 7-7) and on to the Application layer. The Application layer passes the message to the web server application.

Figure 7-7

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



Note 1

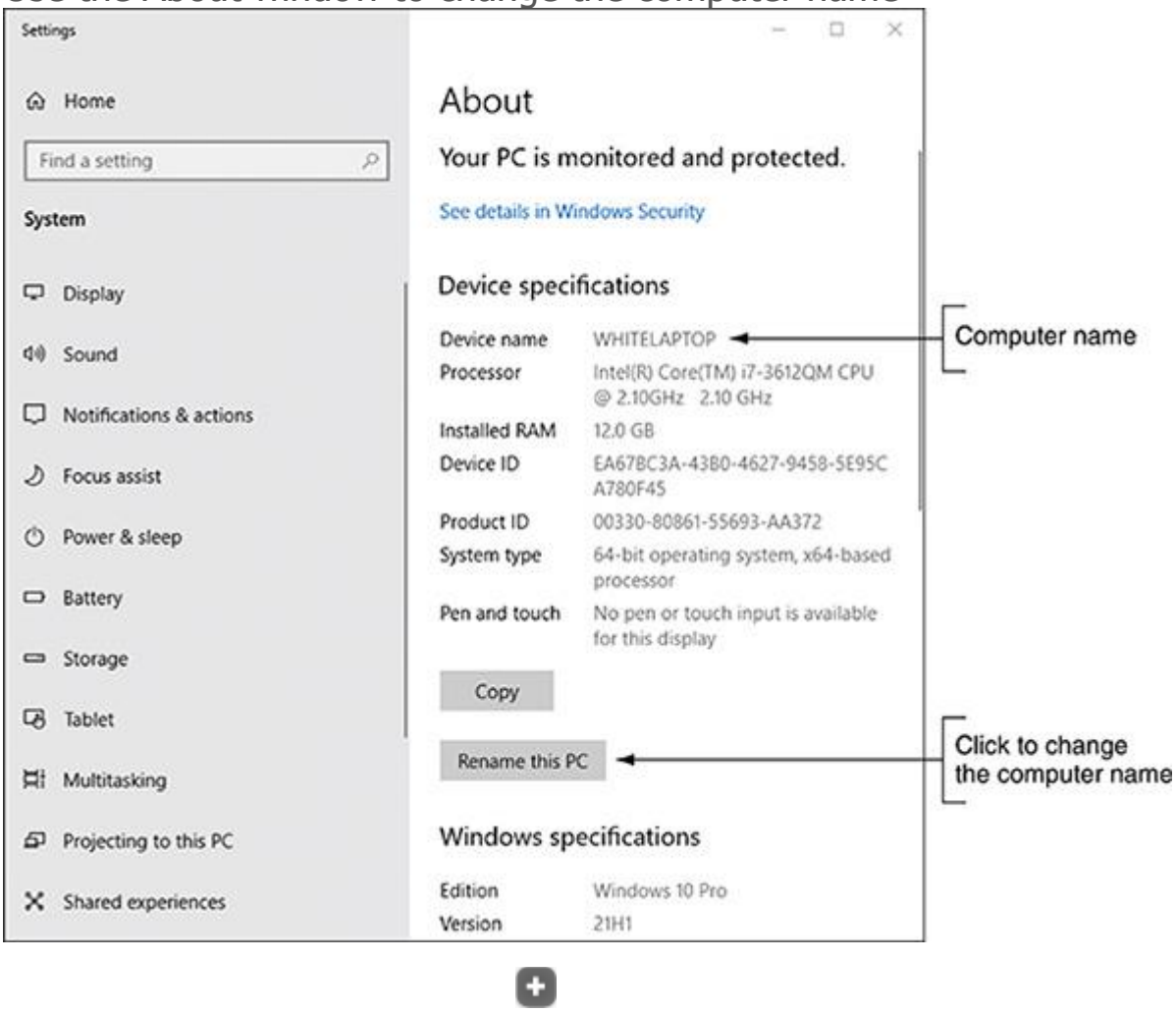
Messages on a TCP/IP network might have different names depending on which layer's protocols have added information to the message, either at the beginning of the message (called a header) or at the end (called a trailer). For example, messages with IP address header information added are called packets.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

Although IP addresses can always be used to identify hosts on a network or the Internet, they are difficult for humans to remember. Therefore, character-based addresses are preferred:

- A **host name** or computer name identifies a host and can be used in place of its IP address on the local network. The name can have up to 63 characters, including letters, numbers, and special characters. Examples of computer names are www, ftp, JeanAndrews, TestBox3, and RedLaptop. You can assign a computer name while installing Windows. In addition, you can change the computer name at any time using the About window in the Settings app. See Figure 7-3.

Figure 7-3

Use the About window to change the computer name



- A **domain name** identifies a network. Examples of domain names are the names that appear before the period in microsoft.com, *cengage.com*, and mycompany.com. The letters after the period are called the top-level domain and tell you something about the domain. Examples are .com (commercial), .org (nonprofit), .gov (government), .edu (education), 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.cengage.com*. The host name is *www* (a web server), *cengage* is the domain name, and *com* is the top-level domain name of the Cengage network. Another FQDN is joesmith.mycompany.com.

A fully qualified domain name must be associated with an IP address before the computer can be found on the Internet. The process of associating a character-based name with an IP address is done via DNS services and is covered later in this module.

7-1c The OSI Model for Network Communication

Core 1 Objective

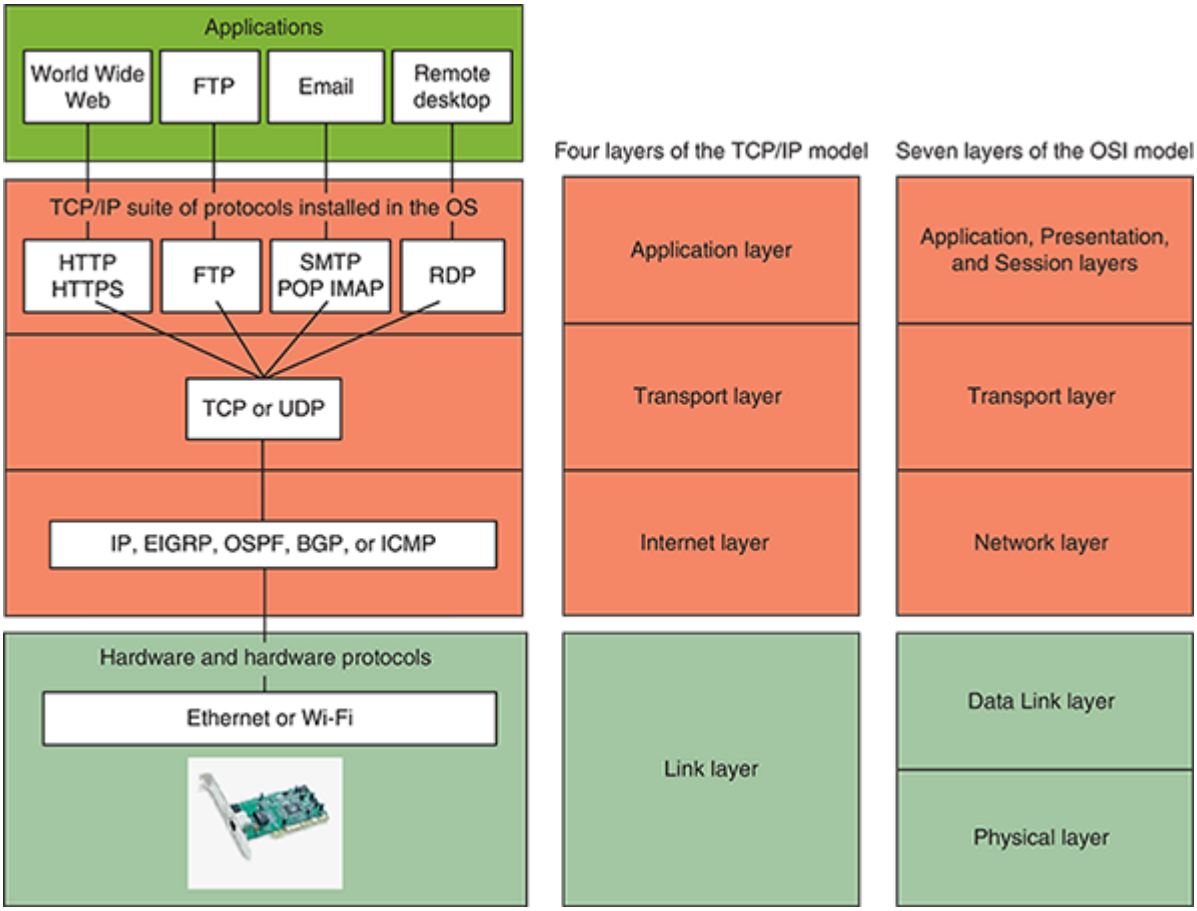
- 2.1

Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

A more detailed model for network communication is the **OSI (Open Systems Interconnection) model**, which has seven layers of communication and is shown on the right side of Figure 7-8. The figure also shows many of the TCP/IP protocols used by client/server applications, the operating systems, and hardware and how they relate to one another at the different layers.

Figure 7-8

How software, protocols, and technology on a TCP/IP network relate to each other using the seven-layer OSI model



Note 2

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

As you continue reading the module, Figure 7-8 can serve as your road map to the different protocols. Let's begin with the higher-layer application protocols used by server applications.

7-1d Server Applications, Their Protocols and Ports

Core 1 Objectives

- 2.1

  Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

- 2.4

  Summarize services provided by networked hosts.

Recall that a client computer contacts a server in order to request information or perform a task, such as when a web browser connects with a web server and requests a webpage. Many other types of server resources exist on a typical network. A server application might be installed on a computer as a stand-alone application or embedded as firmware in other network devices such as a router. (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 network to another. You learn more about routers later in this module.)

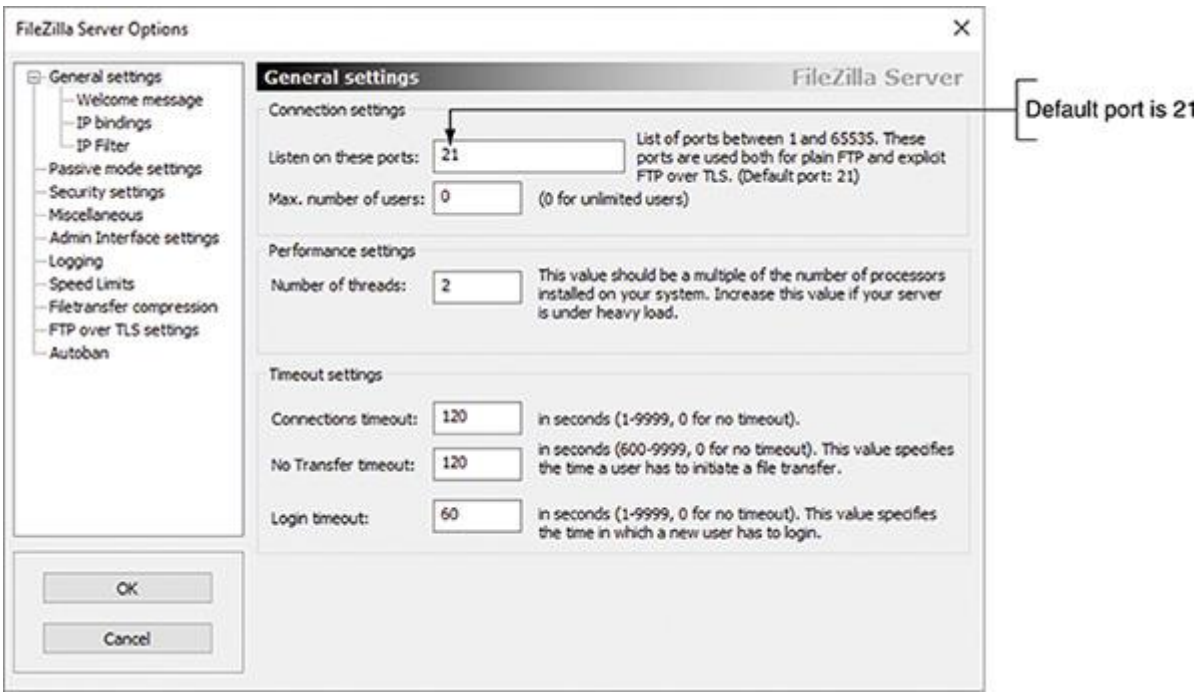
Exam Tip

The A+ Core 1 exam expects you to know the port addresses used by many server applications. As you read the list that follows, pay close attention and even memorize the port addresses used by each server application.

Ports are usually assigned to a client or server app when the app is first installed or configured later after the installation. For example, Figure 7-9 shows a settings window where the port for an FTP server is set to 21.

Figure 7-9

Configure an FTP server to use the default port 21 or any port between 1 and 65535



Here's a brief list of several popular client/server resources used on networks and the Internet along with the protocols and ports they use:

- **Web server.** A web server serves up webpages to clients. Many corporations have their own web servers, which are available privately on the corporate network. Other web servers are public, accessible from anywhere on the Internet. The most popular web server applications are Apache (see apache.org) and Nginx *(*nginx.org*)*. The most popular OSs for running a web server are UNIX and Linux. A web server uses the following ports and protocols:
    - **Port 80. HTTP (Hypertext Transfer Protocol)** is used by a browser and web server for unsecured communication. You can see when a browser is using this protocol by looking for "http" at the beginning of a URL in the address bar, such as http://www.microsoft.com. The web server listens at port 80.
    - **Port 443. HTTPS (HTTP secure)** refers to the HTTP protocol working with a security protocol such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to create a secured socket. (TLS is better than SSL.) A socket is a connection between a browser and web server. HTTPS is used by web browsers and servers to secure the socket by encrypting the data before it is sent and then decrypting it on the receiving end

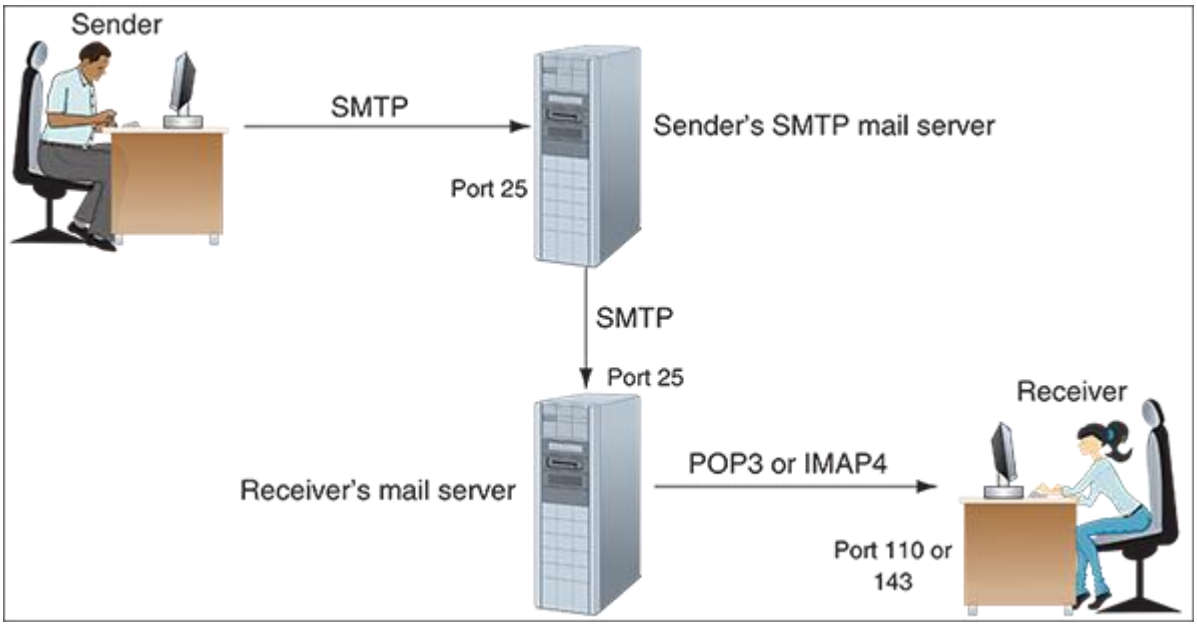
before the data is processed. To know a secured protocol is being used, look for "https" in the URL, as in https://www.wellsfargo.com. Most websites today use secure protocols.

- **Mail server.** Email is a client/server application that involves two mail servers, one to send the mail and another to deliver an email message to a client app. A mail server uses the following ports and protocols:

  - **Port 25. SMTP (Simple Mail Transfer Protocol)** is used to send an email message to its destination (see Figure 7-10). The email server that takes care of sending email messages (using the SMTP protocol) is often referred to as the SMTP server. The SMTP server listens at port 25.

Figure 7-10

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



  - **Port 110 or port 143.** 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 **IMAP (Internet Mail Access Protocol)**. Using POP3, email is downloaded to the client computer, and unless the default setting is changed, the email is then deleted from the email server. The client requests email from a POP3 server listening at port 110. Using IMAP, the client application

manages the email while it is still stored on the server. An IMAP server listens at port 143.

- **File server.** A **file server**, also called a file share server, stores files and makes them available to other computers. Windows uses the **Server Message Block (SMB)** protocol to share files and printers on a network. The current release of the SMB protocol is SMB 3; older versions include SMB 2 and a spin-off protocol called **CIFS (Common Internet File System)**. SMB might use the following ports:
  - **Ports 137 and 139.** SMB originally worked with **NetBIOS (Network Basic Input/Output System)**, an older protocol used by Windows for network communication. To support legacy NetBIOS applications on a TCP/IP network, Windows offered **NetBT (NetBIOS over TCP/IP)**. Earlier versions of SMB require NetBT to be enabled and use these ports:
    - SMB over UDP uses ports 137 and 138.
    - SMB over TCP uses ports 137 and 139.
  - **Port 445.** Current versions of SMB and CIFS don't require NetBT and use port 445.

Core to Core

You learn how to manage a file server in the A+ Core 2 module "Securing and Sharing Windows Resources."

- **Print server.** A **print server** manages network printers and makes them available to computers throughout the network. You learn more about print servers in the module "Supporting Printers."
- **DHCP server.** When a device first connects to a network, its IP address can have already been manually assigned; this type of IP address is called a **static IP address**. Alternately, the device can request an IP address from a **DHCP (Dynamic Host Configuration Protocol) server** that assigns the address from a pool of addresses it maintains; this type of IP address is called a **dynamic IP address**. A device that requests an IP address and other information from a DHCP server is called a **DHCP client**. It is said that the client is leasing an IP address. A DHCP server that serves up IPv6 addresses is often called a **DHCPv6 server**. Later in this module, you learn how to configure a DHCP server embedded in a SOHO router. DHCP uses the following ports:
  - **Port 67.** A DHCP server listens at port 67.
  - **Port 68.** A DHCP client receives messages on port 68.
- **DNS server. DNS servers** are part of a client/server system that associates FQDNs such as *www.cengage.com* with IP addresses. The process is called **name resolution**, and it begins when a DNS client,

such as a laptop or workstation, makes a query to its DNS server. The server might turn to other DNS servers to find the IP address of a given domain name. A DNS server listens at port 53.

- **Proxy server.** A **proxy server** is a computer that intercepts requests that a client, such as a browser, makes of another server, such as a web server. The proxy server substitutes its own IP address for the request. It might also store, or cache, data that is used frequently by its clients. An example of using a proxy server is when an ISP caches webpages to speed up requests for the same pages. After it caches a page and another browser requests the same content, the proxy server can provide the content that it has cached. In addition, a proxy server sometimes acts as a router to the Internet, a firewall to protect the network, a filter for email, and to restrict Internet access by employees to prevent them from violating company policies. When functioning in these ways to give easy access to the Internet, a proxy server is known as an Internet appliance.
- **Authentication, authorization, and accounting (AAA) server.** An **authentication, authorization, and accounting (AAA) server** (pronounced a "triple-A server") is used to secure and control access to the network and its resources. Active Directory, which is a directory service included in Windows Server, is often used for these purposes on a Windows domain. AAA servers perform the following tasks:

    - Authenticate users or computers to the network so they can access network resources and stores user or device credentials, such as user names and passwords.
    - Authorize what a user or computer can do after they have access, including the resources they can access and what they can do with these resources.
    - Account for what a user or computer did with the resources and the time they took. These logs can be useful when users and computers are billed for services they used.

  One protocol a AAA server can use for communication is LDAP. The **Lightweight Directory Access Protocol** (**LDAP**, often pronounced "l-dap") uses port 389. LDAPS is the secure version of LDAP, and it listens at port 636.

Core to Core

You learn about other protocols a AAA server can use in the Core 2 module "Network Security and Troubleshooting."

- **Syslog server. Syslog** is a protocol that gathers event information about various network devices, such as errors, failures, maintenance tasks, and users logging in or out. The messages about these events

are sent to a central location called a **syslog server**, which collects the events into a database. Some syslog servers can generate alerts or notifications to inform network administrators of problems that might need attention.

Exam Tip

The A+ Core 1 exam expects you to be able to summarize services provided by several server applications, including AAA, DNS, DHCP, file share, mail, print, syslog, and web servers.

- **FTP server.** An **FTP (File Transfer Protocol)** server and the FTP protocol is used to transfer files between two computers on a network or the Internet. Web browsers can use the protocol, as can File Explorer in Windows. Also, third-party FTP client software, such as CuteFTP by GlobalSCAPE (globalscape.com/cuteftp) or open-source FileZilla (filezilla-project.org), offer additional features. By default, FTP transmissions are not secure. Two protocols that encrypt FTP transmissions are FTPS (FTP Secure), which uses SSL encryption, and SFTP (SSH FTP), which uses SSH encryption. FTP uses the following ports:
  - **Port 20.** The FTP client receives data on port 20 from the FTP server.
  - **Port 21.** The FTP server listens at port 21 for commands from an FTP client.

Exam Tip

FTP has been largely replaced by other technologies, such as the BitTorrent and Streaming Sync protocols, for file transfers. However, the A+ Core 1 exam still expects you to be familiar with FTP.

- **Telnet server. Telnet** server and protocol can be used by an administrator or other user to control a computer remotely. Telnet is not considered secure because transmissions in Telnet are not encrypted. The Telnet server listens at port 23.
- **SSH server.** An SSH server and **Secure Shell (SSH)** protocol encrypt communications so hackers can't read the data if they intercept a transmission. The SSH protocol is used in various situations for encryption, such as when remotely controlling a computer or when communicating with a web server. SSH is commonly used in Linux to pass sign-in information to a remote computer and control that computer over a network. Because it's secure, SSH is preferred over Telnet. SSH uses port 22.
- **Remote Desktop and Remote Assistance. Remote Desktop Protocol (RDP)** is used by the Windows Remote Desktop and Remote Assistance utilities to connect to and control a remote computer. These two RDP servers both listen at port 3389.

Core to Core

You learn more about remotely controlling a computer, including how to use Remote Desktop and Remote Assistance, in the Core 2 module "Network Security and Troubleshooting."

- **SNMP server and agent. Simple Network Management Protocol (SNMP)** is a versatile service and protocol used to monitor network traffic and manage network devices. The SNMP server is called the manager, and a small application called an agent is installed on devices being managed by SNMP. The service can help create logs for monitoring device and network performance, make some automatic changes to devices being monitored, and alert network technicians when a bottleneck or other performance issues are causing problems on the network. SNMP uses the following ports:
  - **Port 161.** The SNMP agent on the monitored device listens at port 161.
  - **Port 162.** The SNMP server or manager listens at port 162.

In summary, Table 7-2 lists all the ports you are expected to have memorized in preparation for the A+ Core 1 exam. You need to know the app that uses each port, the purpose of the app, and whether the app uses TCP or UDP at the Transport layer. TCP and UDP are discussed next.

Table 7-2

Common TCP/IP Port Assignments for Client/Server Applications

Port	Protocol and Role	TCP, UDP or Both	Description
20	FTP client	TCP	The FTP client receives data on port 20 from the FTP server.
21	FTP server	TCP	The FTP server listens at port 21 for commands from an FTP client.
22	SSH server	TCP	A server using the SSH protocol listens at port 22.
23	Telnet server	TCP	A Telnet server listens at port 23.
25	SMTP email server	TCP	An email server listens at port 25 to receive email from an email clien
53	DNS server	TCP/UDP	A DNS server listens at port 53.
67	DHCP server	UDP	A DHCP server listens at port 67.
68	DHCP client	UDP	A DHCP client receives messages on port 68.
80	HTTP	TCP	A web server listens at port 80 when receiving HTTP requests.
110	POP3 email server	TCP	An email client requests email from a POP3 server listening at port 11
143	IMAP email server	TCP	An email client requests email from an IMAP server listening at port 1
161	SNMP agent	UDP	An SNMP agent listens at port 161.
162	SNMP manager	UDP	An SNMP manager listens at port 162.

Port	Protocol and Role	TCP, UDP or Both	Description
137 and 139	SMB with NetBT	TCP/UDP	SMB with NetBT uses ports 137 and 139 (for TCP traffic).
389	LDAP	TCP/UDP	AAA servers using LDAP listen at port 389.
443	HTTPS	TCP	A web server listens at port 443 when receiving HTTPS transmissions
445	SMB and CIFS	TCP/UDP	SMB and CIFS use port 445 for both TCP and UDP traffic.
3389	RDP	TCP/UDP	Remote Desktop and Remote Assistance services listen at port 3389.

Exam Tip

In preparation for the A+ Core 1 exam, memorize the details in Table 7-2. Questions at the end of this module will help you.

7-1e TCP and UDP Delivery Methods

Core 1 Objective

- 2.1

Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

Looking back at Figure 7-8, you can see three layers of protocols working at the Application, Transport, and Internet layers. These three layers make up the heart of TCP/IP communication. As illustrated in the figure, TCP or UDP manages communication with the applications protocols in the layers above as well as those in the lower layers, which control communication on the network. TCP and UDP at the Transport layer are both charged with delivering an application's message to the destination host (refer back to Figure 7-5), but they do their jobs differently. Let's discuss next a few key differences between TCP and UDP that determine which of these two protocols is most appropriate for each situation.

Exam Tip

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

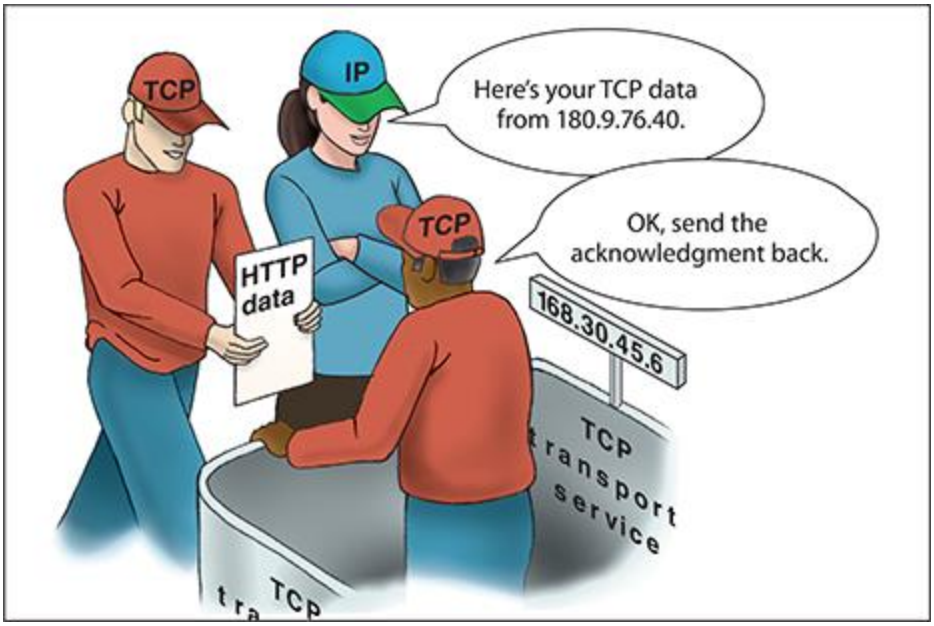
TCP Guarantees Delivery

Remember that all communication on a network happens by way of messages delivered from one location on a network to another. **TCP (Transmission Control Protocol)** guarantees message delivery. TCP uses IP addresses to make a connection between a sending and destination host,

sends the data, 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 (using HTTP and HTTPS protocols), email (using SMTP, POP3, and IMAP protocols), FTP file transfer apps (using FTP protocol), and SSH apps used to make secure connections to a server (using SSH protocol). Guaranteed delivery takes longer and is used when it is important to know that the data reached its destination. When a TCP message reaches its destination, an acknowledgment is sent back to the source (see Figure 7-11).

Figure 7-11

TCP guarantees delivery by requesting an acknowledgment



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.

UDP Provides Fast Transmissions

On the other hand, **UDP (User Datagram Protocol)** does not guarantee delivery by first establishing a connection or by checking whether data is received; thus, UDP is called a **connectionless protocol** or **best-effort protocol** and is used where guaranteed delivery is not as important as fast transmission. Here are some example uses of UDP:

- **Broadcasting, such as streaming live video or sound over the web.** (TCP, however, is preferred for video on demand where quality is an issue.)
- **Monitoring network traffic.** Notice in Table 7-2 the SNMP agent and manager use UDP.

- **Completing simple file transfers.** **Trivial FTP (TFTP)** is a small, simple app often used to transfer BIOS updates to firmware on routers and smartphones. It's also used to transfer a lean pre-execution environment (PXE) operating system from a server to BIOS/UEFI on a computer to boot the computer when it does not have a working OS. TFTP over UDP is preferred in these situations because the program is small enough to store on firmware, and it is simple to implement and use.
- **Communicating between DHCP clients and servers.** DHCP uses UDP rather than TCP primarily because DHCP clients and servers use broadcasting to communicate on a local network; UDP supports broadcasting, but TCP does not.

TCP and UDP are responsible for delivering an application's message, and the IP protocol is responsible for finding the right destination host. Let's see how that's done.

7-1f How Computers Find Each Other

Core 1 Objective

- 2.5

Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

To learn how computers use the IP protocol to find each other on a local network or the Internet, let's first discuss how IPv4 addresses are constructed and used. A 32-bit IPv4 address is organized into four groups of 8 bits each, which are presented as four decimal numbers separated by periods, such as 72.56.105.12. The largest possible 8-bit number is 11111111, which is equal to 255 in decimal, so the largest possible IPv4 address in decimal is 255.255.255.255, which in binary is 11111111.11111111.11111111.11111111. Each of the four numbers separated by periods is called an **octet** (for 8 bits) and can be any decimal value from 0 to 255, making a total of about 4.3 billion possible IPv4 addresses (256 × 256 × 256 × 256). Some IP addresses are reserved, so these numbers are approximations. IP addresses that are reserved for special use by TCP/IP and should not be assigned to a device on a network are listed in Table 7-3.

Table 7-3

Reserved IP Addresses

IP Address	How It Is Used
127.0.0.1	Indicates your own computer and is called the **loopback address**.
0.0.0.0	Currently unassigned IP address.
255.255.255.255	Used for **broadcast messages** by TCP/IP background processes to communicate with all devices on a network at the same time or without needing specific recipient information, such as when a device broadcasts a message on the local network looking for a DHCP server from which it can lease an IP address. Broadcasting can cause a lot of network chatter; to reduce the chatter, **subnets** are created to subdivide a network into smaller networks so fewer devices receive and respond to broadcast messages.

To communicate on a network or the Internet, a host needs this TCP/IP information:

- Its own IP address—for example, 192.168.100.4. The first part of an IP address identifies the network, and the last part identifies the host.
- A **subnet mask**, which is four decimal numbers separated by periods—for example, 255.255.255.0. When a computer wants to send a message to a destination computer, it uses its subnet mask to decide whether the destination computer is on its own network or another network.
- The IP address of a **default gateway**. Computers can communicate directly with each other on the same network. However, when a computer sends a message to a computer on a different network, it sends the message to its default gateway, which is connected to the local network and at least one other network. The gateway sends the message on its way to other networks. For small businesses and homes, the default gateway is a router.
- The IP addresses of one or more DNS servers. It queries a DNS server to find out the IP address of the destination host when it knows only the domain name of the host.

Applying Concepts

Viewing TCP/IP Settings

- **Est. Time:** 15 minutes
- **Core 1 Objective:** 2.5

The IP address, subnet mask, default gateway, and DNS server addresses can be manually assigned to a computer's network connection, or this information can be requested from a DHCP server on the network when a computer first connects to the network. Follow these steps to view the current TCP/IP settings on a Windows 10 computer:

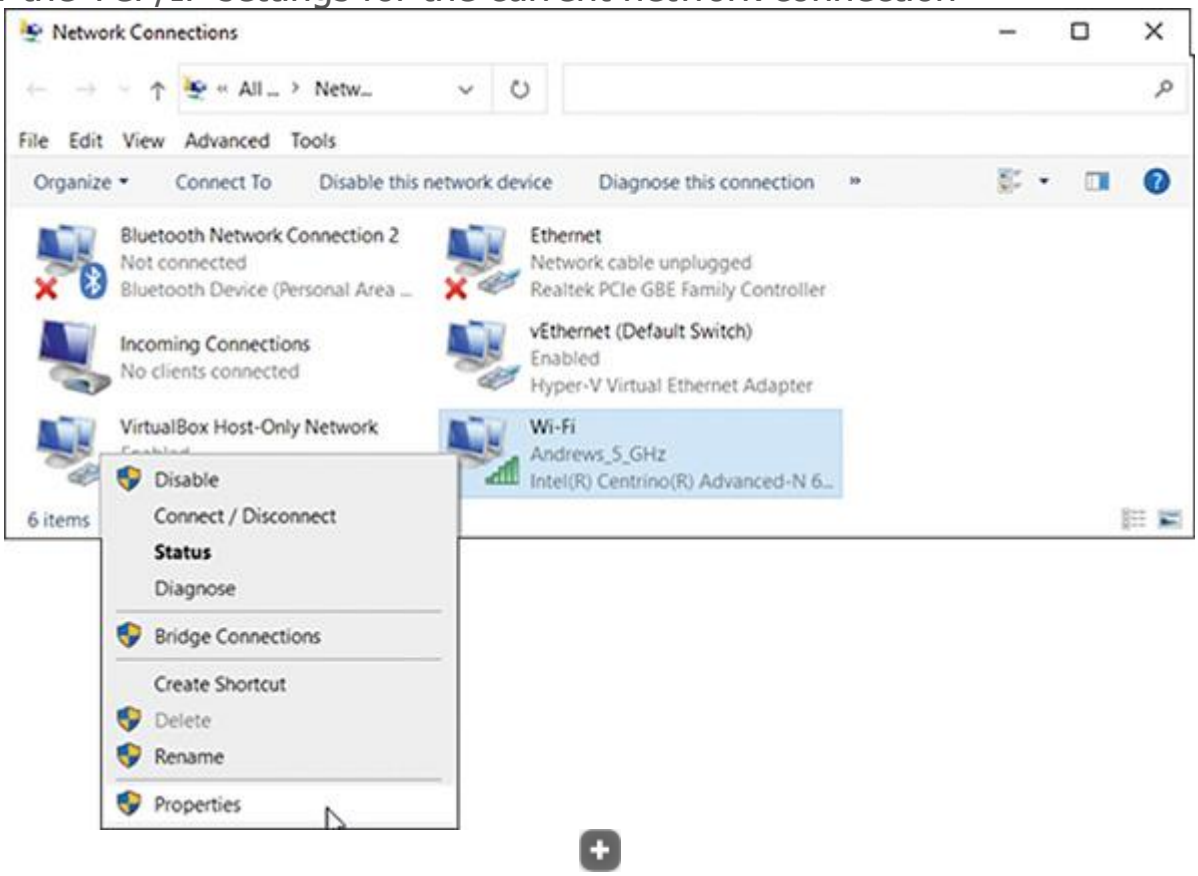
1. 1

Right-click **Start** and click **Network Connections**. In the Status window, click **Change adapter options**.

2. 2
In the Network Connections window, you can see all your connections. Right-click your current connection, and click **Properties** (see Figure 7-12).

Figure 7-12

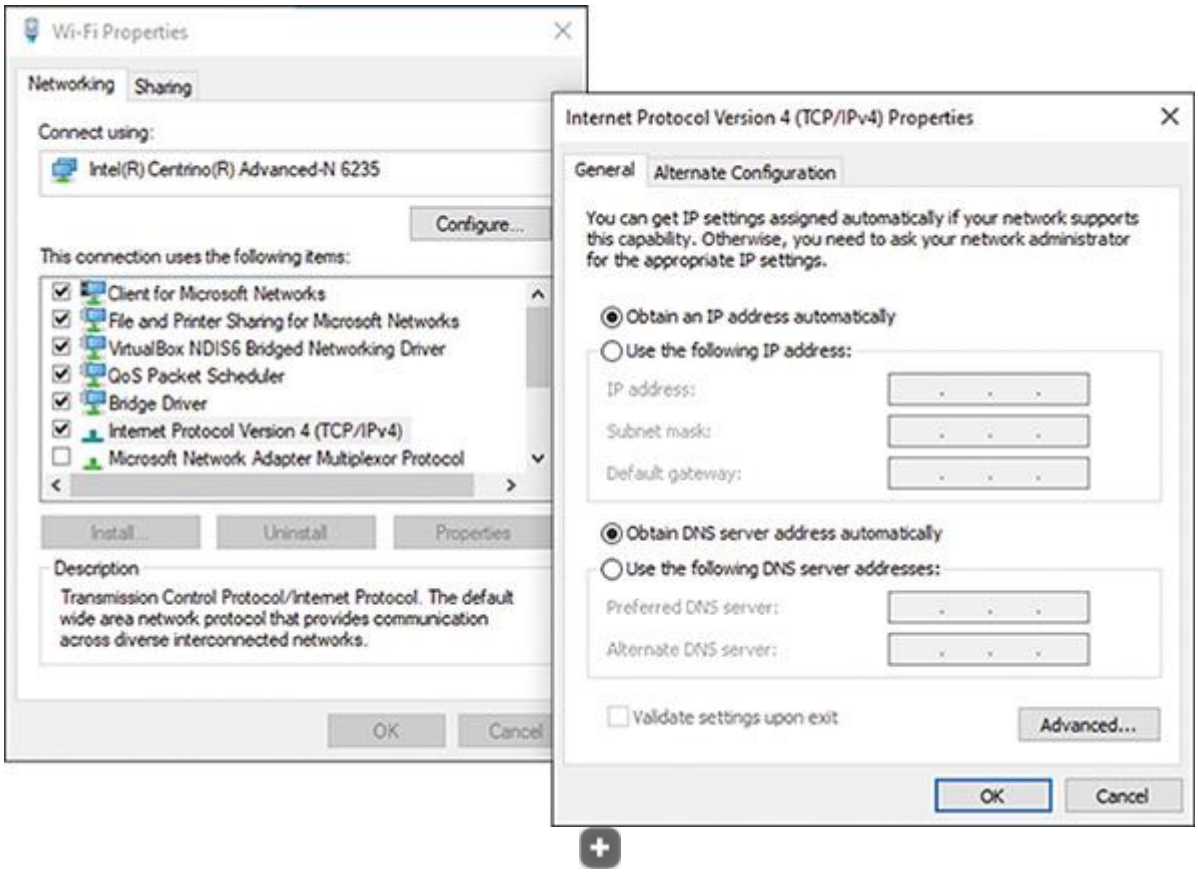
View the TCP/IP settings for the current network connection



3. 3
In the Properties dialog box, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. In Figure 7-13, you can see the host is configured to request its IP address, subnet mask, default gateway and DNS server addresses from a DHCP server on the network.

Figure 7-13

This network connection is configured for dynamic IP addressing



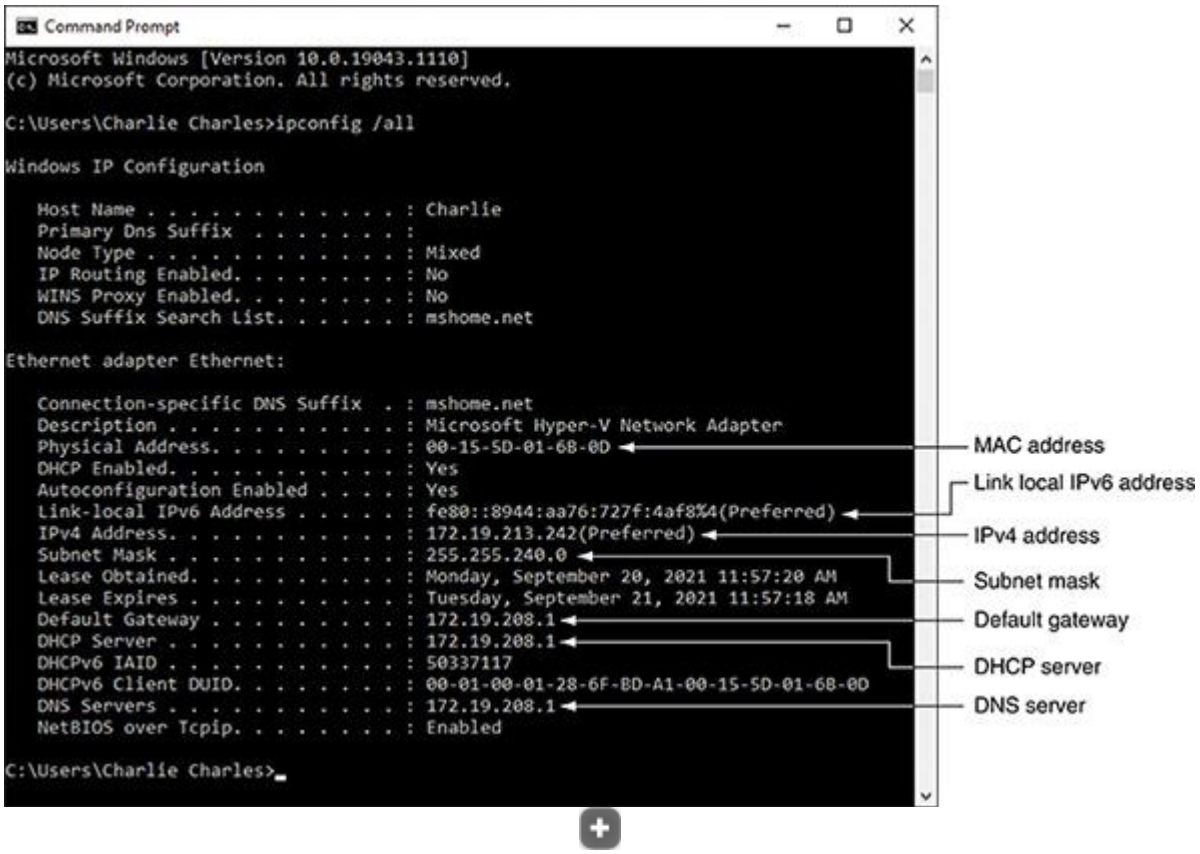
4. 4
   To find out what values have been assigned to this computer, enter **cmd** in the Windows search box. The Command Prompt window opens. In the window, enter the following:

   ```
   ipconfig /all
   ```

5. 5
   Scroll through the results to locate information similar to that shown in Figure 7-14. Is your current network connection a wired or wireless connection? What is its MAC address (physical address)? IPv4 address? Subnet mask? Default gateway? DHCP server? DNS server?

Figure 7-14

Use the ipconfig /all command to show the MAC address and other information about the current network connections

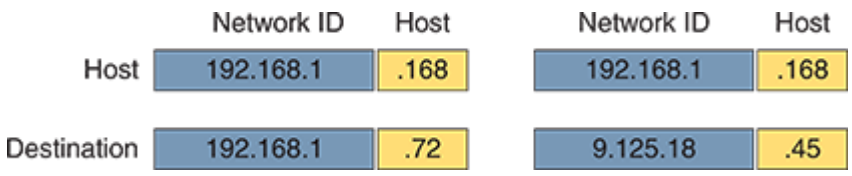


6. 6
Close all open windows.

When TCP/IP receives a message to send to a destination computer, it first looks at the beginning or left part of its own IP address that identifies the network (called the **network ID**) and compares it to the network ID of the destination IP address. On the left side of Figure 7-15, the network ID of the host (192.168.1) matches the network ID of the destination (192.168.1); therefore, the two computers are on the same network. On the right side of Figure 7-15, the network ID (192.168.1) of the host does not match the network ID of the destination (9.125.18); therefore, the host sends the message to its default gateway, which sends the message to a different network.

Figure 7-15

A computer uses network IDs to determine whether a destination computer is on the same network



The network ID of the destination IP address is used to locate the destination host's local network. After the message arrives at the local

network, the host portion of the IP address is used to identify the one computer on the network that will receive the message.

Subnet Masks

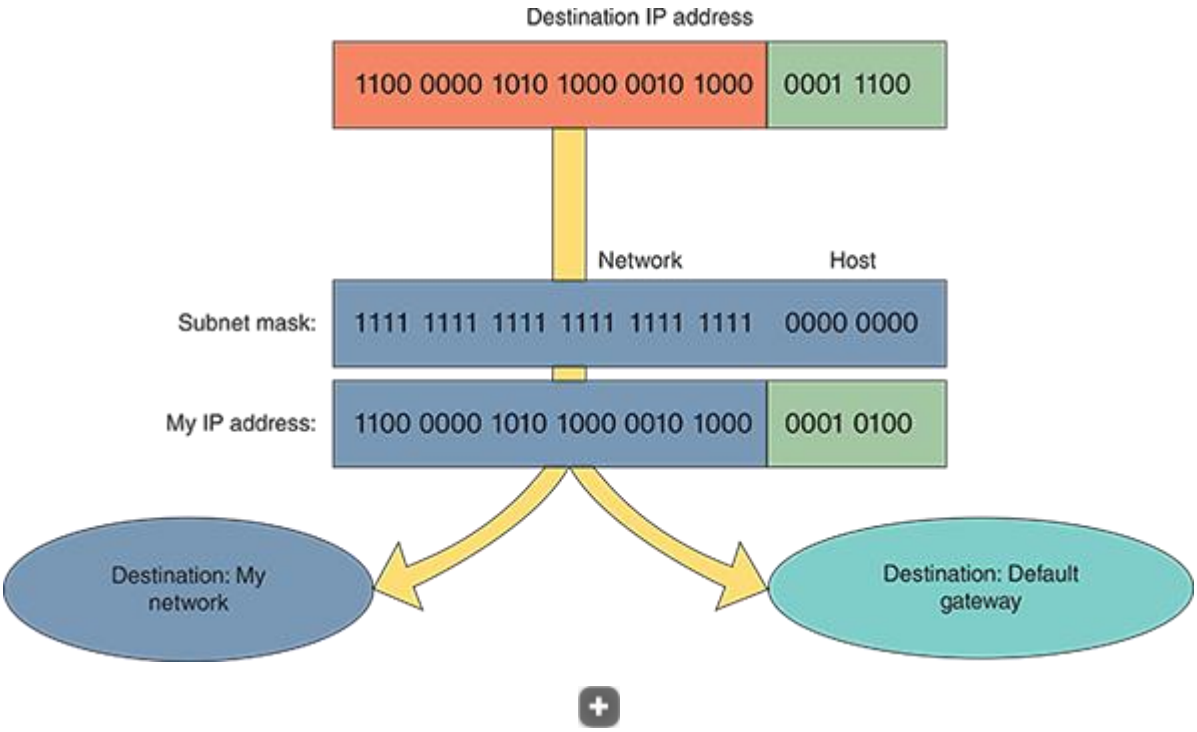
How does a computer or other network device know what part of an IP address identifies the network and what part identifies the host? It relies on a subnet mask for this information. All the IP addresses assigned to a local network or subnet have matching bits in the leftmost part of the IP address; these bits that identify the network are called the network ID. For example, the range of IP addresses assigned to a local network might be 192.168.80.1–100. The first three octets (192.168.80) identify the network and the last octet (1 through 100) identifies each host. The last bits in each IP address that identify the host must be unique for each IP address on the network.

A subnet mask has 32 bits and is a string of 1s followed by a string of 0s—for example, 11111111.11111 111.11110000.00000000. The 1s in a subnet mask say, "On our network, this part of an IP address identifies our network," and the group of 0s says, "On our network, this part of an IP address identifies each host." Usually, a subnet mask is displayed in decimal—for example, the subnet mask of 11111111.11111111.00000000.00000000 is 255.255.0.0 in decimal.

Figure 7-16 shows how a subnet mask serves as a type of filter to decide whether a destination IP address is on the local network or a remote network. In the figure, you can see that the subnet mask has 24 ones. Therefore, the computer compares the first 24 bits of the destination IP address to its own first 24 bits. If they match, it directs the message to the computer on its local network. If they don't match, it sends the message to its default gateway.

Figure 7-16

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



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

Let's look at one more example. Suppose the IP address of a computer is 19.200.60.6 and its subnet mask is 255.255.240.0. Is a computer with the IP address 19.200.51.100 on its network? Table 7-4 shows the logic to find out:

Table 7-4

Logic of a Subnet Mask

Question	Answer
1. What is my IP address in binary?	19.200.60.6 in binary is 00010011.11001000.00111100.00000110.
2. What is my subnet mask in binary?	255.255.240.0 in binary is 11111111.11111111.11110000.00000000.
3. How many bits in my IP address identify my network?	There are 20 ones in the subnet mask. Therefore, 20 bits identi the network.

Question	Answer
4. What is the other IP address in binary?	19.200.51.100 in binary is 00010011.11001000.00110011.01100100.
5. Do the first 20 bits in my IP address match the first 20 bits in the other IP address?	Compare the 20 red bits in the two IP addresses 00010011.11001000.00111100.00000110 00010011.11001000.00110011.01100100. Yes, they match.
6. Is the other IP address on my network?	Yes.

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

Public, Private, and Automatic Private IP Addresses

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

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

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

Note 3

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

Exam Tip

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

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

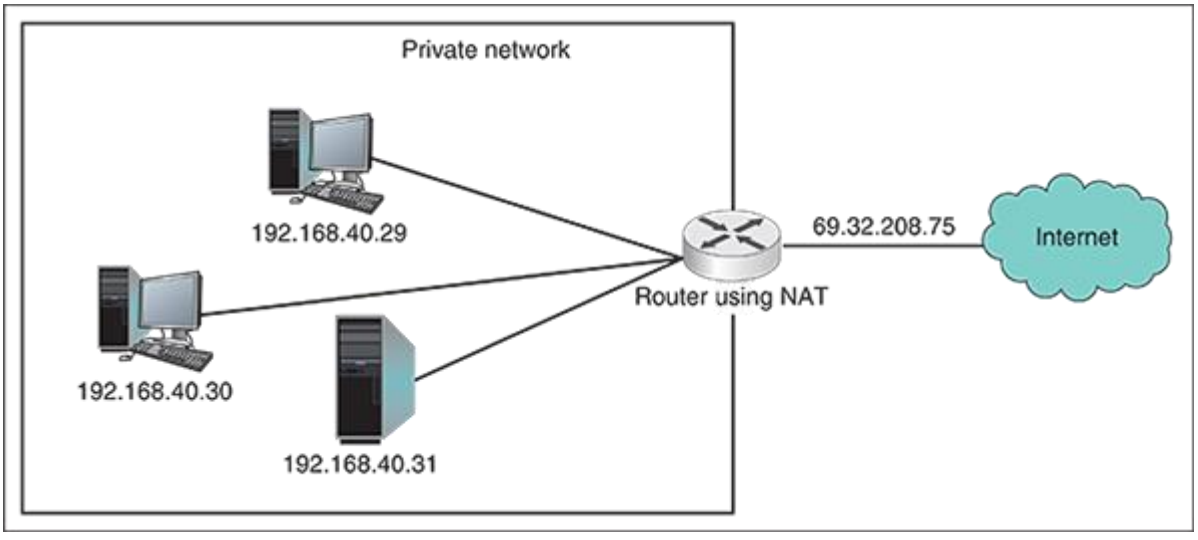
Core to Core

If you are running a web server on the Internet, you will need a public IP address for your router and either a static or reserved private IP address for the web server. For this situation, you can lease a public IP address from your ISP at an additional cost. You will also need to enable port forwarding to the server, which is discussed in the Core 2 module "Network Security and Troubleshooting".

NAT (Network Address Translation) is a technique designed to conserve the number of public IP addresses needed by a network. A router stands between a private network and the Internet. It substitutes the private IP addresses used by computers on the private network with its own public IP address when these computers need access to the Internet. See Figure 7-17. Besides conserving public IP addresses, another advantage of NAT is security; the router hides the entire private network behind this one address. For a small office/home office (SOHO) router, expect that NAT is enabled by default.

Figure 7-17

NAT allows computers with private IP addresses to access the Internet



7-1g How IPv6 Addresses Are Used

Core 1 Objective

- 2.5

Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

When the Internet and TCP/IP were first invented, it seemed that 32 bits were more than enough to satisfy any needs we might have for IP addresses because IPv4 created about four billion potential IP addresses. Today we need many more than four billion IP addresses over the world. Partly because of a shortage of 32-bit IP addresses, IPv6 was designed to use an IP address with 128 bits. Currently, the Internet uses a mix of 32-bit and 128-bit IP addresses. The Internet Assigned Numbers Authority (IANA at iana.org) is responsible for keeping track of assigned IP addresses and has already released all of its available 32-bit IPv4 addresses. IPv6 addresses leased from IANA today are all 128-bit addresses.

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

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

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

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

- A **link** is a local area network (LAN) or wide area network (WAN).
- The last 64 bits or four blocks of an IPv6 address identify the interface and are called the **interface ID** or interface identifier. These 64 bits uniquely identify an interface on the local network.
- **Neighbors** are nodes on the same local network.

Recall that with IPv4 broadcasting, messages are sent to every node on a local network. However, IPv6 doesn't use broadcasting, thereby reducing network traffic. Instead, IPv6 uses multicasting, anycasting, and unicasting, as illustrated in Figure 7-18 and described next:

Figure 7-18

Concepts of broadcasting, multicasting, anycasting, and unicasting

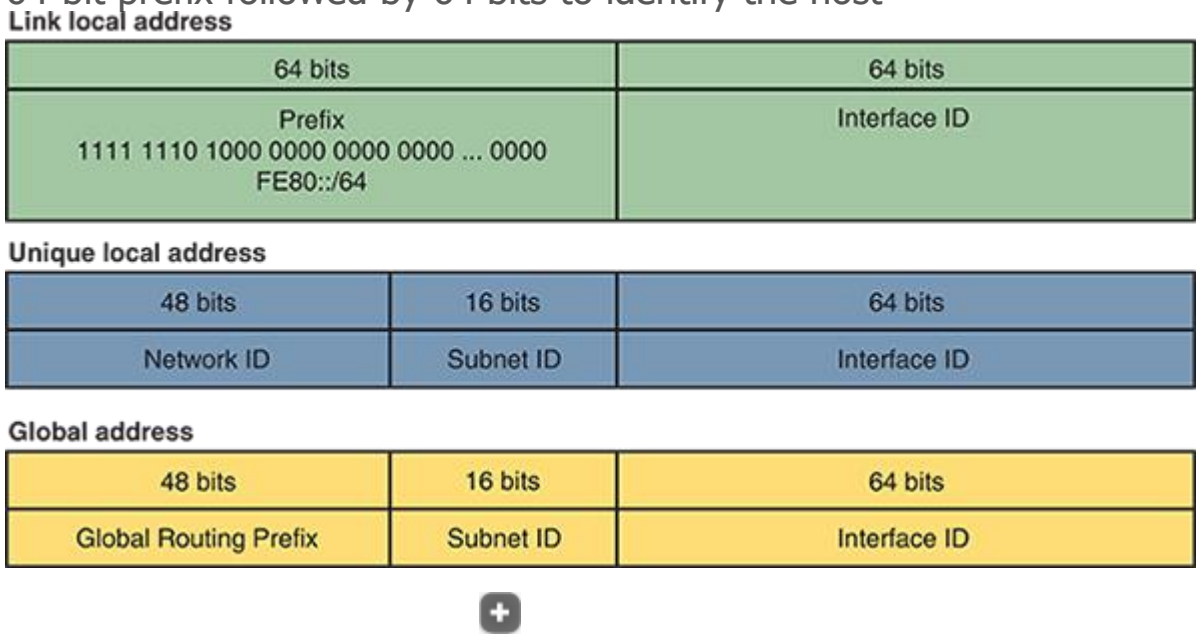
- A **multicast address** is used to deliver messages to all nodes in a targeted, multicast group, such as when video is streaming from a server to multiple nodes on a network.
- An **anycast address** is used by routers and can identify multiple destinations; a message is delivered only to the closest destination.
- A **unicast address** is used to send messages to a single node on a network. Three types of unicast addresses are link local addresses,

unique local addresses, and global addresses. A single interface might have more than one unicast address assigned to it at any given time:

- A **link local address**, also called a link local unicast address or local address, can be used for limited communication with neighboring nodes in the same link (the local network). These local addresses are similar to IPv4 APIPA addresses in that they are assigned to the computer by itself, as opposed to coming from a DHCPv6 server, and are not guaranteed to be unique on the network. Most link local addresses begin with FE80::/64. This prefix notation means the address begins with FE80 followed by enough zeroes to make 64 bits, as shown in Figure 7-19. Link local addresses are not allowed on the Internet or allowed to travel outside private networks.

Figure 7-19

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



- Look back at Figure 7-14 to see an example of a link local address where the wired interface has the IPv6 address of fe80::8944:aa76:727f:4af8%4. The first 64 bits are fe80::, and the interface ID is 8944:aa76:727f:4af8. IPv6 addresses are followed by a % sign and a number; for example, %4 follows this sample IP address. This number is called the zone ID or scope ID and is used to identify the interface in a list of interfaces for this computer.
- A **unique local address** is a private address assigned by a DHCPv6 server that can communicate across subnets within the private network. They're used by network administrators when

subnetting a large network. A unique local address always begins with FC or FD and is usually assigned to an interface in addition to its self-assigned link local address.

- A **global address**, also called a global unicast address, can be routed on the Internet. These addresses are similar to IPv4 public IP addresses. The first 48 bits of the address is the Global Routing Prefix. When an ISP assigns a global address to a customer, it's these 48 bits that are assigned. An organization that leases one Global Routing Prefix from its ISP can use it to generate many IPv6 global addresses.

Table 7-5 lists the currently used address prefixes for these types of IPv6 addresses. In the future, we can expect more prefixes to be assigned as they are needed.

Table 7-5

Address Prefixes for Types of IPv6 Addresses

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

Exam Tip

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

Note 4

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

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

Now that you have an understanding of TCP/IP and Windows networking, let's turn our attention to the hardware used for local networks.

7-2 Network Hardware

Core 1 Objective

- 2.2

Compare and contrast common networking hardware.

In this section of the module, you learn about the hardware devices used to create local networks in homes and small businesses, including network adapters, switches, hubs, cable modems, and SOHO routers.

7-2a Network Adapters

Core 1 Objective

- 2.2

Compare and contrast common networking hardware.

A computer makes a wired or wireless connection to a local network by way of a network adapter, which might be a network port embedded on the motherboard or a **network interface card (NIC)** installed in an expansion slot on the motherboard. In addition, the adapter might be an external device plugged into a USB port (see Figure 7-20). A network adapter is often called a network interface card or NIC even when it's not really a card but rather a USB device or a device embedded on the motherboard. It might also be called a network controller or network adapter.

Figure 7-20

USB devices provide wired and wireless network connections

Exam Tip

The A+ Core 1 exam expects you to be able to compare and contrast network interface cards, cable modems, routers, switches and hubs—all discussed in this section of the module.

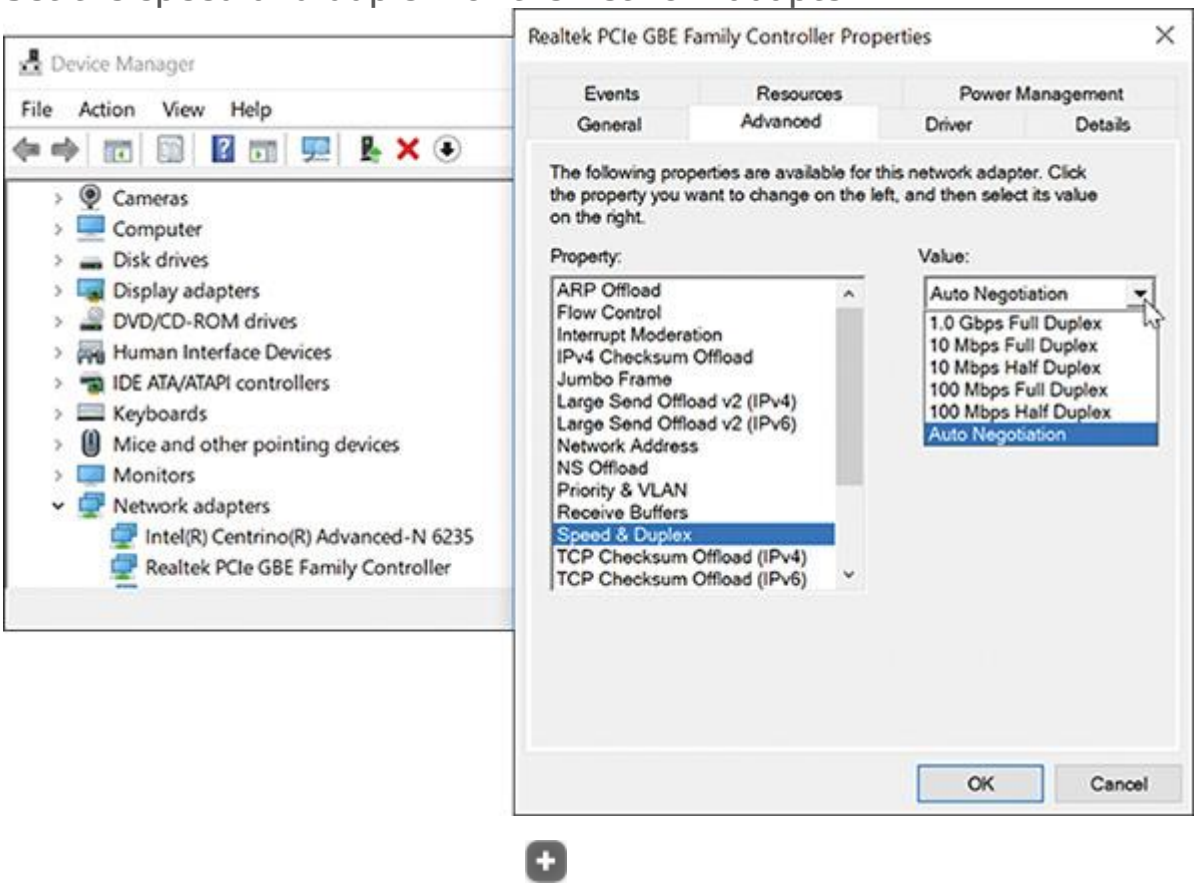
Here are a network adapter's features you need to be aware of:

- **NIC drivers.** A NIC usually comes bundled with drivers on CD or the drivers can be downloaded from the web. Windows has several embedded NIC drivers. After you install a NIC, you install its drivers. For best functionality and security, always use the latest drivers. Problems with the network adapter can sometimes be solved by using Device Manager to update the drivers or uninstall the drivers and then reinstall them.
- **Ethernet speeds.** A NIC supports wired Ethernet transmissions or wireless Wi-Fi transmissions. For wired networks, the four speeds for Ethernet are 10 Mbps, 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), and 10 Gbps (10-gigabit Ethernet). Most network adapters sold today for local networks use Gigabit Ethernet and support the two slower speeds. To see the speeds a NIC supports, open its **Properties** dialog box in **Device Manager**. Select the **Advanced** tab. In the list of properties, select **Speed & Duplex**. You can then see available speeds in the Value drop-down list (see the right side of Figure 7-21). If the adapter connects with slower network devices on the network, the adapter works at the slower speed.

Select **Auto Negotiation** for Windows to use the best possible speed for a particular connection.

Figure 7-21

Set the speed and duplex for the network adapter



Note 5

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

- **RJ-45 port and status indicator lights.** A network port is called an **RJ-45** port, and it looks like a large phone jack. The RJ-45 Ethernet connector is similar to but larger than the RJ-11 phone connector (see Figure 7-22). A wired network adapter might provide indicator lights on the side of the network port that indicate connectivity and activity (see Figure 7-23). When you first discover you have a problem with a computer not connecting to a network, be sure to check the status indicator lights to verify you have connectivity and activity. If not, then the problem is related to hardware. Next, check the cable connections to make sure they are solid.

Figure 7-22

RJ-45 and RJ-11 connectors

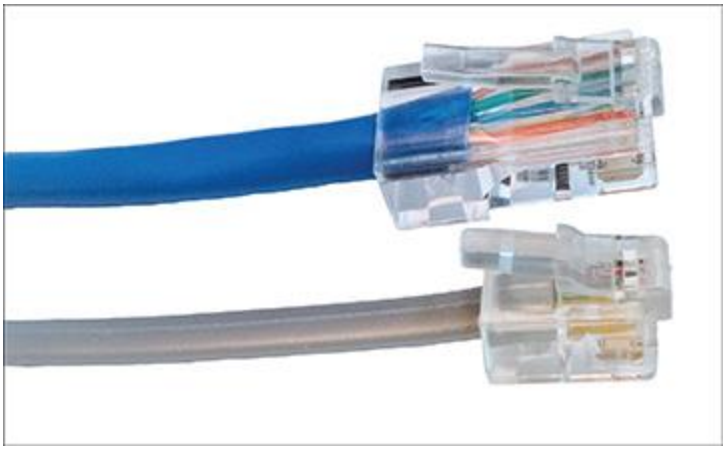


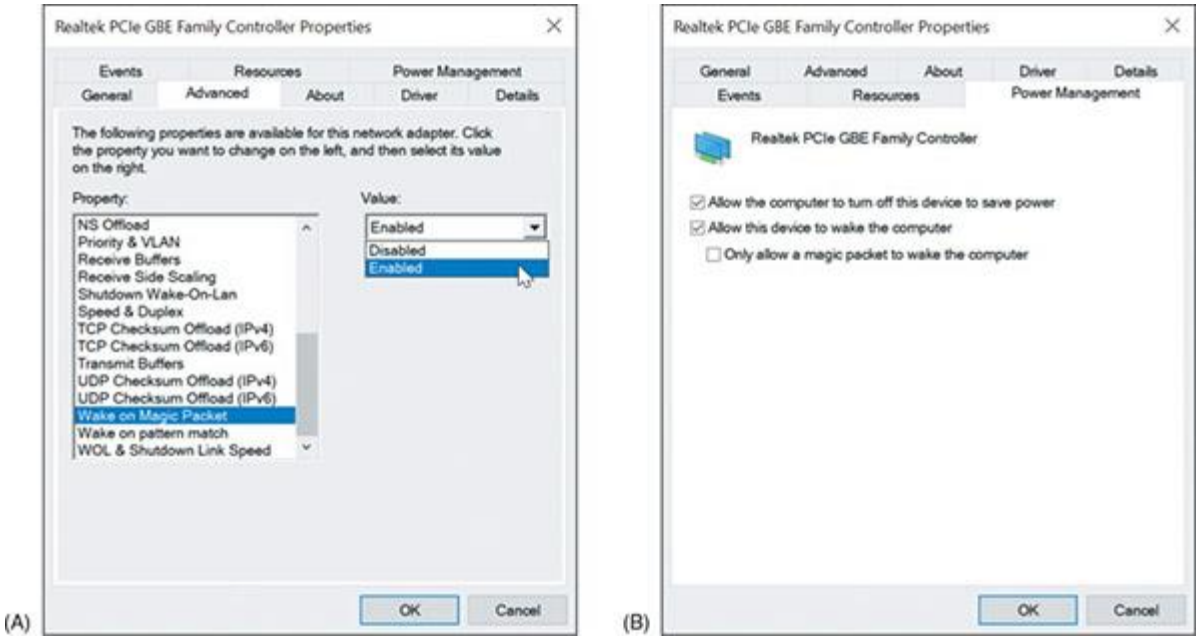
Figure 7-23

Status indicator lights for the onboard network port

- **Wake-on-LAN.** A NIC might support **Wake-on-LAN**, which allows it to wake up the computer when it receives certain communication on the network. To use the feature, it must be enabled on the NIC. Open the NIC's **Properties** dialog box in Device Manager, and click the **Advanced** tab. Make sure **Wake on Magic Packet** and **Wake on pattern match** are both enabled (see Figure 7-24A).

Figure 7-24

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



- For an onboard NIC, you must also enable Wake-on-LAN in BIOS/UEFI setup. Reboot the computer, enter BIOS/UEFI setup, and look for the option on a power-management or advanced screen. For some systems, such as the one shown in Figure 7-25, you enable power-on by the PCI-E bus because the NIC communicates via this bus. It is not recommended that you enable Wake-on-LAN for a wireless network adapter.

Figure 7-25

For this system, use the Advanced screen in the BIOS/UEFI setup to enable Wake-on-LAN by enabling power-on by the PCIe bus

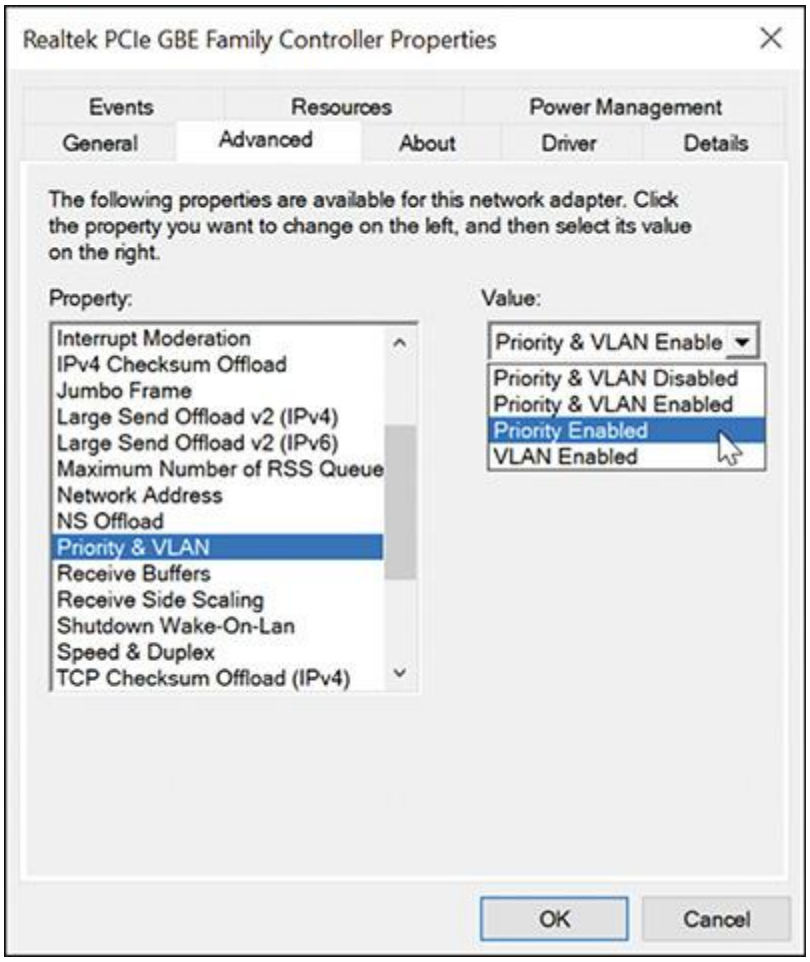
Note 6

Some NICs provide a Power Management tab in the Properties dialog box. To use the Power Management tab to enable Wake-on-LAN, check **Allow this device to wake the computer** (see Figure 7-24B).

- **Quality of Service (QoS).** Another feature of a network adapter is **Quality of Service (QoS)**, the ability to control which applications' traffic have priority on the network. The feature must be enabled and configured on the router, enabled on the network adapters, and configured in Windows for every computer on the network that uses the high-priority applications. In the Core 2 module "Network Security and Troubleshooting," you learn how to configure a router to use QoS. To enable QoS on a Windows computer's NIC, open the network adapter **Properties** dialog box in Device Manager. On the **Advanced** tab, make sure **Priority Enabled** or **Priority & VLAN Enabled** is selected, as shown in Figure 7-26. If the option is not listed, the adapter does not support QoS.

Figure 7-26

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



Note 7

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

7-2b Switches and Hubs

Core 1 Objective

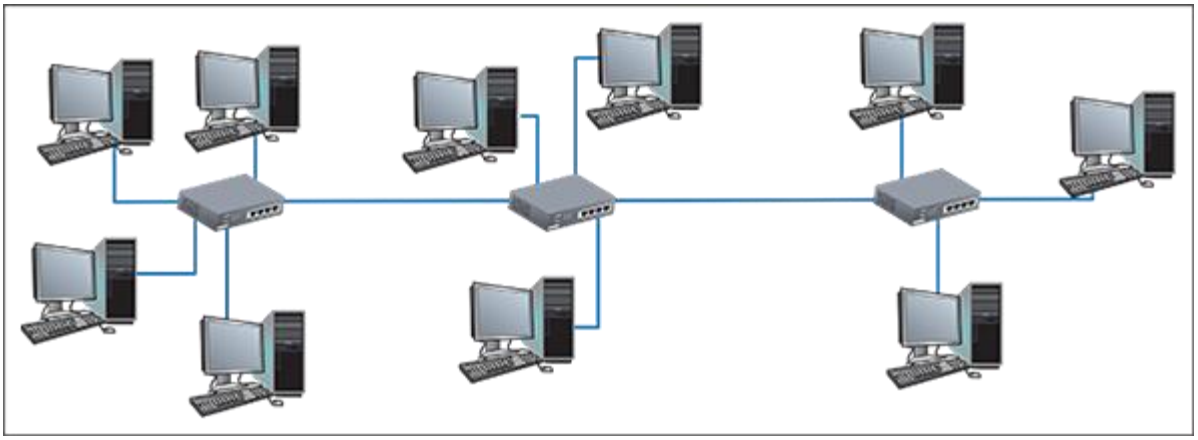
- 2.2

  Compare and contrast common networking hardware.

  Today's Ethernet networks use a design called a star bus topology, which means that nodes are connected to one or more centralized devices, which are connected to each other (see Figure 7-27). The three centralized devices shown in the figure are called switches.

Figure 7-27

A star bus network is formed by nodes connected to multiple switches



Here are the differences between a hub and a switch:

- An Ethernet **hub** sends a message to every device except the device that sent the message, as shown in Figure 7-28A. A hub is just a passthrough and distribution point for every device connected to it, without regard for what kind of data is passing through and where the data might be going. Hubs are outdated technology, having been replaced by switches. Figure 7-29 shows a hub that supports 10 Mbps and 100 Mbps Ethernet speeds. (You can't find hubs these days to support faster networks.)

Figure 7-28

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

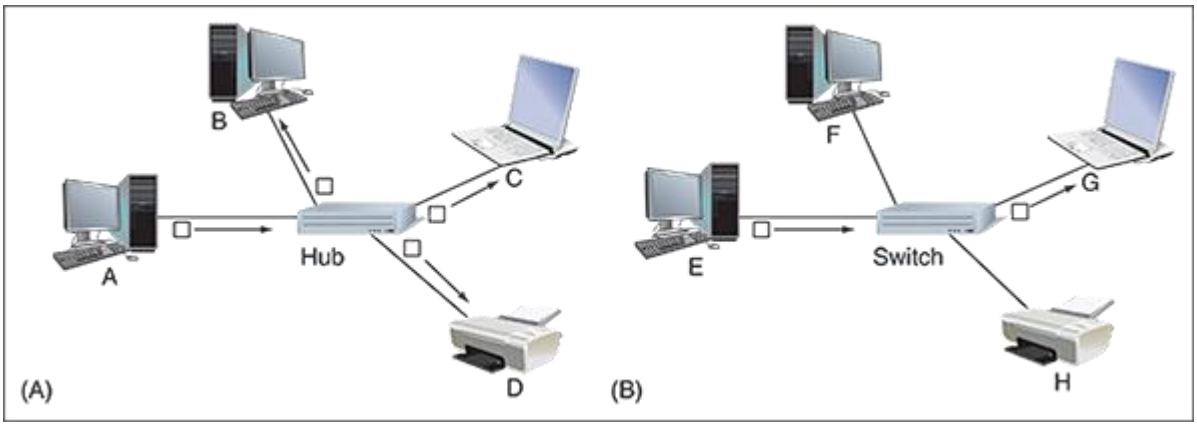
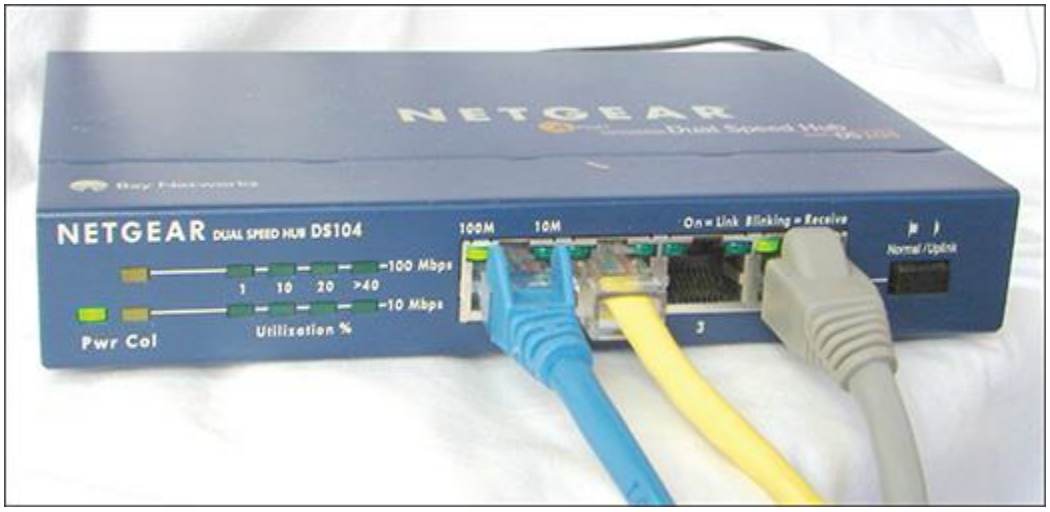


Figure 7-29

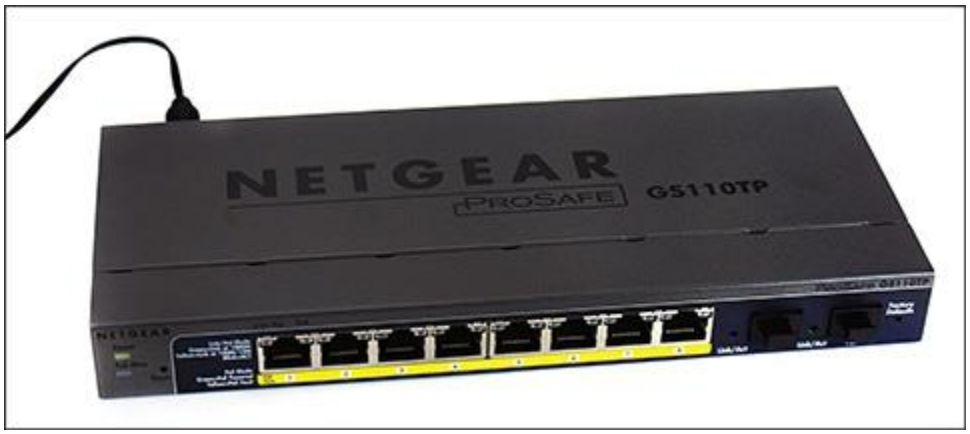
This hub supports 10 Mbps and 100 Mbps Ethernet speeds



- A **switch** (see Figure 7-30) is smarter and more efficient than a hub because it keeps a table of all the MAC addresses for devices connected to it. When the switch receives a message, it searches its MAC address table for the destination MAC address of the message and sends the message only to the interface for the device using this MAC address (see Figure 7-28B). At first, a switch does not know the MAC addresses of every device connected to it. It learns this information as it receives messages and records each source MAC address in its MAC address table. When it receives a message destined to a MAC address not in its table, the switch acts like a hub and sends the message to all devices except the one that sent it. In the module "Network Infrastructure and Cloud Computing," you learn more about how switches manage network traffic.

Figure 7-30

This Gigabit Ethernet switch by NETGEAR has eight Ethernet ports



7-2c Cable Modem

Core 1 Objective

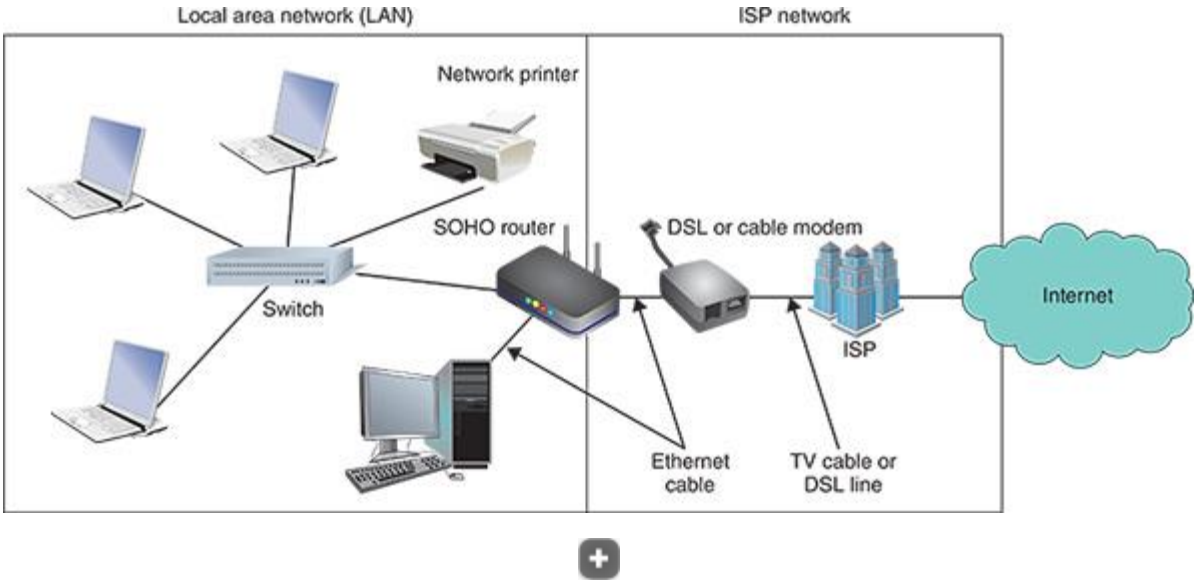
- 2.2

Compare and contrast common networking hardware.

To connect to the Internet, a device or a network first connects to an **Internet service provider (ISP)**, such as Xfinity or Spectrum. The most common types of connections for SOHO networks are cable, fiber optic, and DSL. See Figure 7-31.

Figure 7-31

A modem stands between the ISP and the local network to convert signals to Ethernet used on the LAN



A device is needed to convert cable, DSL, or fiber optic transmissions to Ethernet transmissions used on a local network. For cable, this device is called a **cable modem** (see Figure 7-32). DSL uses a DSL modem, and fiber optic uses an optical network terminal (ONT). Cable modems and DSL modems usually sit beside the SOHO router inside an office or data closet. An ONT is usually mounted on the outside of the building where fiber optic cable terminates, and the ONT connects to an Ethernet cable that enters the building. Regardless of the transmission technology or converting device used, each provides an RJ-45 Ethernet port for a SOHO router or computer to connect to. Looking back at Figure 7-31, note that the LAN begins with the router, which is also considered part of the ISP network. (A router stands between and is part of two or more networks.) The ISP is normally responsible only for its system up to and including the modem or ONT.

Figure 7-32

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

To set up a modem, plug in the TV coax cable and the Ethernet cable, and turn on the modem. Notice in Figure 7-32, the red Reset button, which you can use to reset a modem to its factory default settings. When troubleshooting a modem, try rebooting it first, and only use the reset button as a last resort.

7-2d Multifunction SOHO Router

Core 1 Objective

- 2.2

Compare and contrast common networking hardware.

Routers can range from small ones designed to manage a SOHO network that connects to an ISP (costing around $50 to $300) to those that manage multiple networks and extensive traffic (costing several thousand dollars). On a small office or home network, a router stands between the ISP network and the local network (refer back to Figure 7-31), and the router is the local network's gateway to the Internet.

An example of a multifunction router is the Nighthawk AC1900 by NETGEAR, shown in Figures 7-33 and 7-34. It has one Internet port (also called the WAN or wide-area-network port) to connect to the ISP by way of a modem or ONT and four ports for devices on the network. The USB port can be used to plug in a USB external hard drive for file sharing on the network.

The router is also a wireless access point with multiple antennas to increase speed and range.

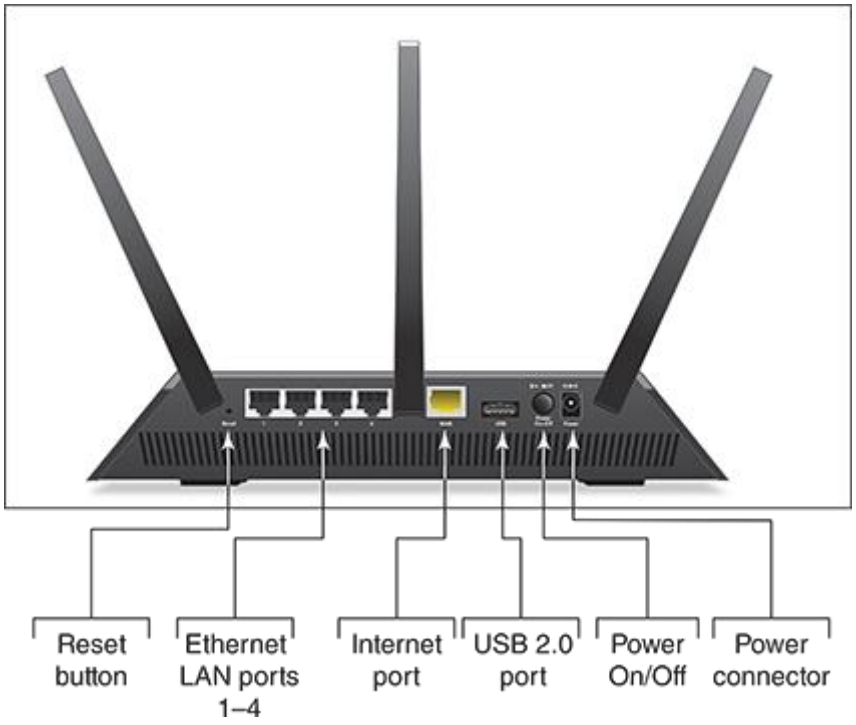
Figure 7-33

The NETGEAR Nighthawk AC1900 dual band Wi-Fi Gigabit router

Source: Amazon.com, Inc.

Figure 7-34

Connections and ports at the back of the NETGEAR router



Source: NETGEAR

Computer, printers, smartphones and other devices can connect to this router using wired or wireless connections. This is because a SOHO router often serves different functions in a single device. A typical SOHO router usually combines these functions:

- As a router, it stands between two networks—the ISP network and the local network—and routes traffic between the two networks.
- As a switch, it manages several network ports that can be connected to wired devices on the local network or to a dedicated switch that provides even more ports for locally networked computers. Looking back at Figure 7-31, one LAN port connects to a switch, and another LAN port connects to a desktop computer.
- As a DHCP server, it can provide IP addresses to computers and other devices on the local network.
- As a **wireless access point (WAP)**, it enables wireless devices to connect to the network. These wireless connections can be secured using wireless security features, which you learn about in the Core 2 module "Network Security and Troubleshooting."
- As a **firewall**, it blocks unwanted traffic from the Internet and can restrict Internet access for local devices behind the firewall. Restrictions on local devices can apply to days of the week, time of day, keywords used, certain websites, and specific applications.
- If an external storage device, such as a USB flash drive or external hard drive, connects to the router via the USB port, the router can be used to share files with network users.

Exam Tip

The A+ Core 1 and + Core 2 exams may require you to evaluate the needs of a business or residence in a given scenario and to install, configure, and secure a SOHO wired and wireless router based on those needs. You learn more about configuring routers in the Core 2 module "Network Security and Troubleshooting," including how to secure the local wired and wireless network using features on the router.

Now that you know about TCP/IP, Windows networking and networking hardware, let's see how to set up and configure a new network from scratch.

7-3 Local Network Setup and Configuration

Core 1 Objectives

- 2.5

  Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

- 2.6

  Compare and contrast common network configuration concepts.

  Suppose you are called on to help a small bookkeeping company with three employees set up its network in a single office space. You have purchased a SOHO router, switch, several patch cables, three laptops, a desktop computer, and network printer. The local telecommunications company has already installed the fiber optic cable to the office along with Ethernet cabling from the ONT unit outside the building to a wall jack in the office. Let's step through the process of setting up and configuring the local network.

Note 8

The process of building and maintaining a large, corporate network is outside the scope of this text. However, working with smaller networks, such as those used in homes and small businesses, helps prepare you to work in larger network environments.

We begin our setup with configuring the router.

7-3a Installing and Configuring a SOHO Router

Core 1 Objectives

- 2.5

  Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

- 2.6

  Compare and contrast common network configuration concepts.

For routers that have external antennas, raise the antennas to vertical positions. Connect the network cable from the ISP modem or other device or wall jack to the WAN port on the router. Plug in and turn on the router. Indicator lights should indicate network activity on the WAN.

To configure a router for the first time, always follow the directions of the manufacturer. For most SOHO routers, you have some options:

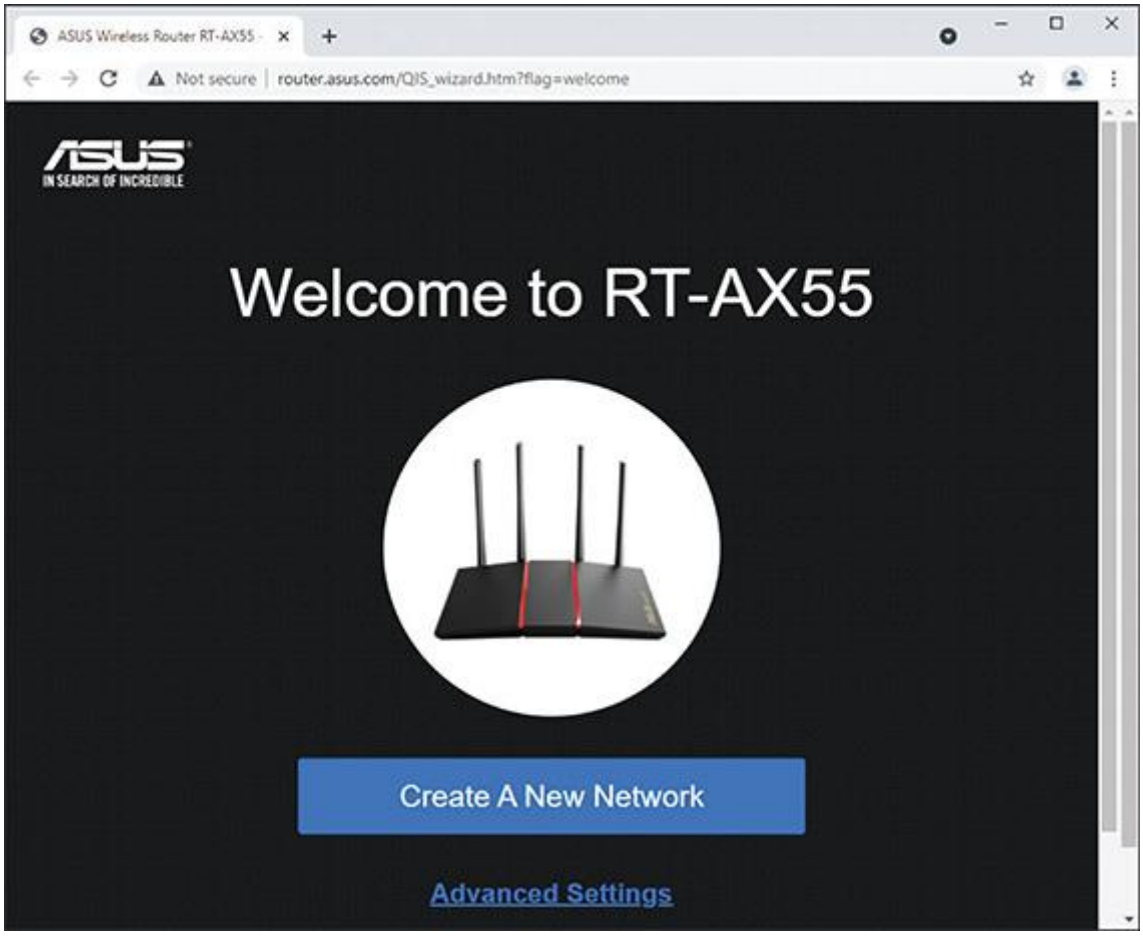
- **For wireless connections.** Download the router manufacturer's app to your smartphone or laptop. Then to connect to the router's wireless network, for a smartphone, open the Settings app, go the Wi-Fi setup and select the name of the router's wireless network, which is called the **Service Set Identifier (SSID)**. It should be printed on the bottom

of the router. Open the router app, which should step you through the router setup.

- **For wired connections.** Use a network cable to connect a laptop or desktop computer to a LAN port on the router. Open a browser window. The browser should automatically connect to the webpage of the router (see Figure 7-35). If it does not connect, look in the router documentation for the URL of the router's webpage (for example, router.asus.com) or the IP address of the router (for example, 192.168.1.1.).

Figure 7-35

Starting page for the router's quick Internet setup routine



Regardless of how you connect to the router, the initial setup should:

- Provide a username and password if needed to connect to your ISP
- Assign a new SSID and password (security key) to the wireless network
- Update the router firmware
- Change the password for the router firmware
- Configure the DHCP server embedded in the router firmware

Core to Core

There's more you can do to configure a router to secure a local wired or wireless network, which you learn about in the Core 2 module "Network Security and Troubleshooting."

The setup screens for each router might be different. For the ASUS RT-AX55, on the router home page shown in Figure 7-35, click **Create A New Network**. On the screens that follow, you are given the chance to enter the optional username and password to the ISP, assign a new SSID and password to the wireless network (see Figure 7-36), update the router firmware, and assign a username and password to sign in to the router firmware (see Figure 7-37).

Figure 7-36

Set the SSID and password to the wireless network

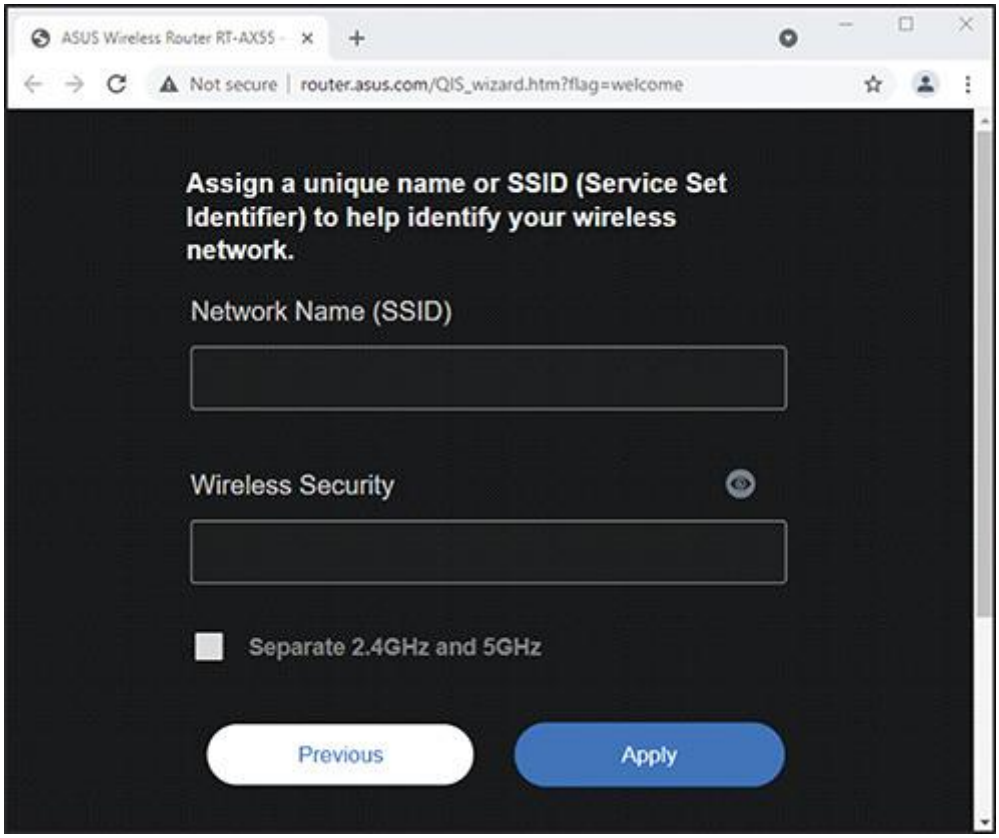
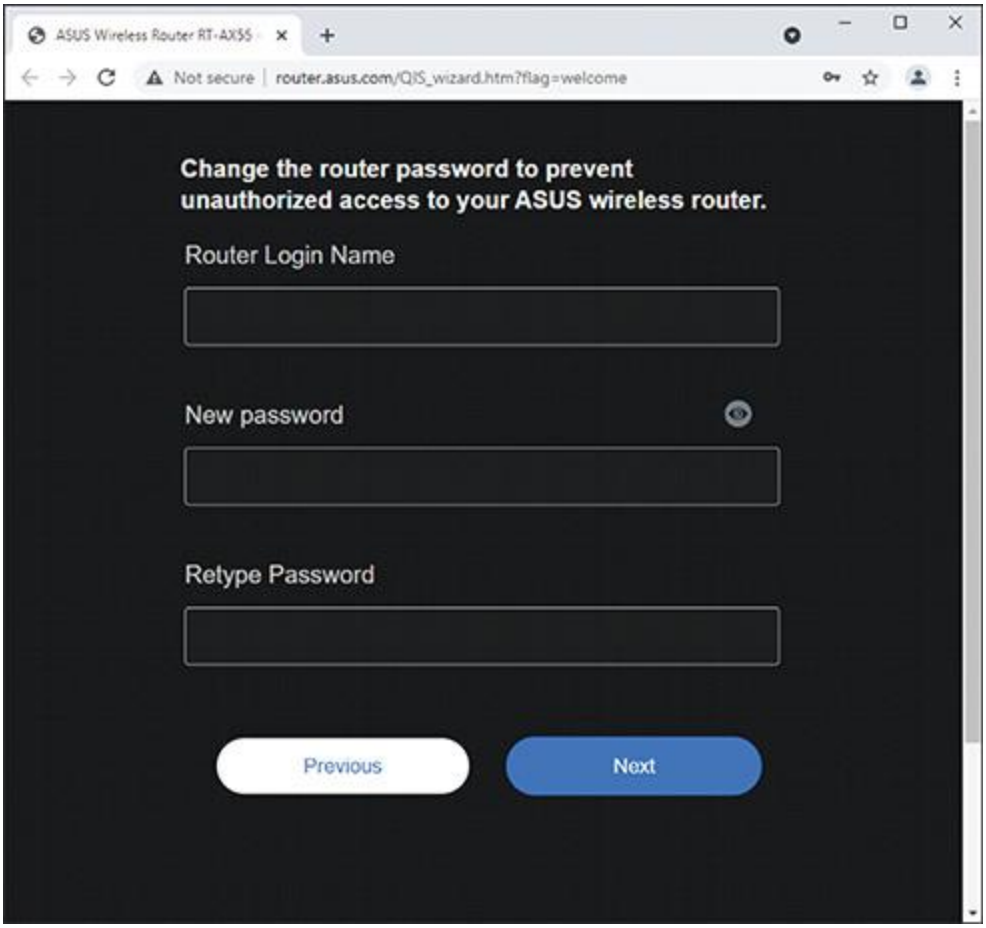


Figure 7-37

Change the router login name and password to the router firmware



Caution

Changing the router firmware login name and password is especially important if the router is a wireless router. Unless you have disabled or secured the wireless network, anyone within its range—even outside your building—can use your wireless network. If someone guesses the default login in name and password to the router, they can change the password to hijack your router and access your wireless network, potentially using it for criminal activity.

After the initial setup, you should be able to browse the web. If you ever need to further configure the router, using any computer on your local network, open a browser and point to your router's URL, such as router.asus.com, or its IP address.

Configure the DHCP Server

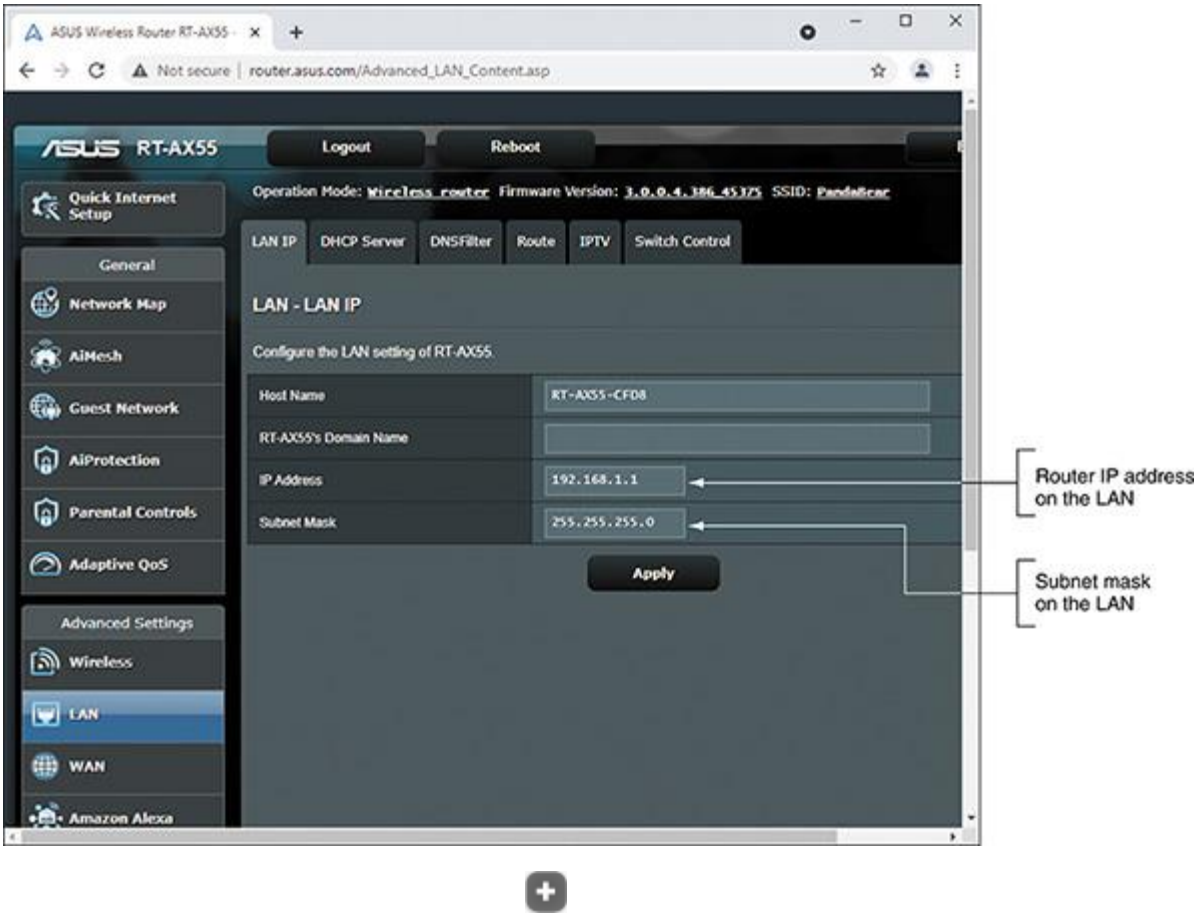
A DHCP server on a SOHO router is usually configured for dynamic IP addressing by default. To verify and change the DHCP settings, do the following:

1. Go to the router firmware home page (router.asus.com, for example) and sign in with your router account username and password that you set up earlier. The main menu for the router appears. Figure 7-38 shows the main menu for the ASUS RT-AX55, but yours might look

different. To configure the DHCP server, click **LAN** in the left pane. The LAN submenu tabs appear.

Figure 7-38

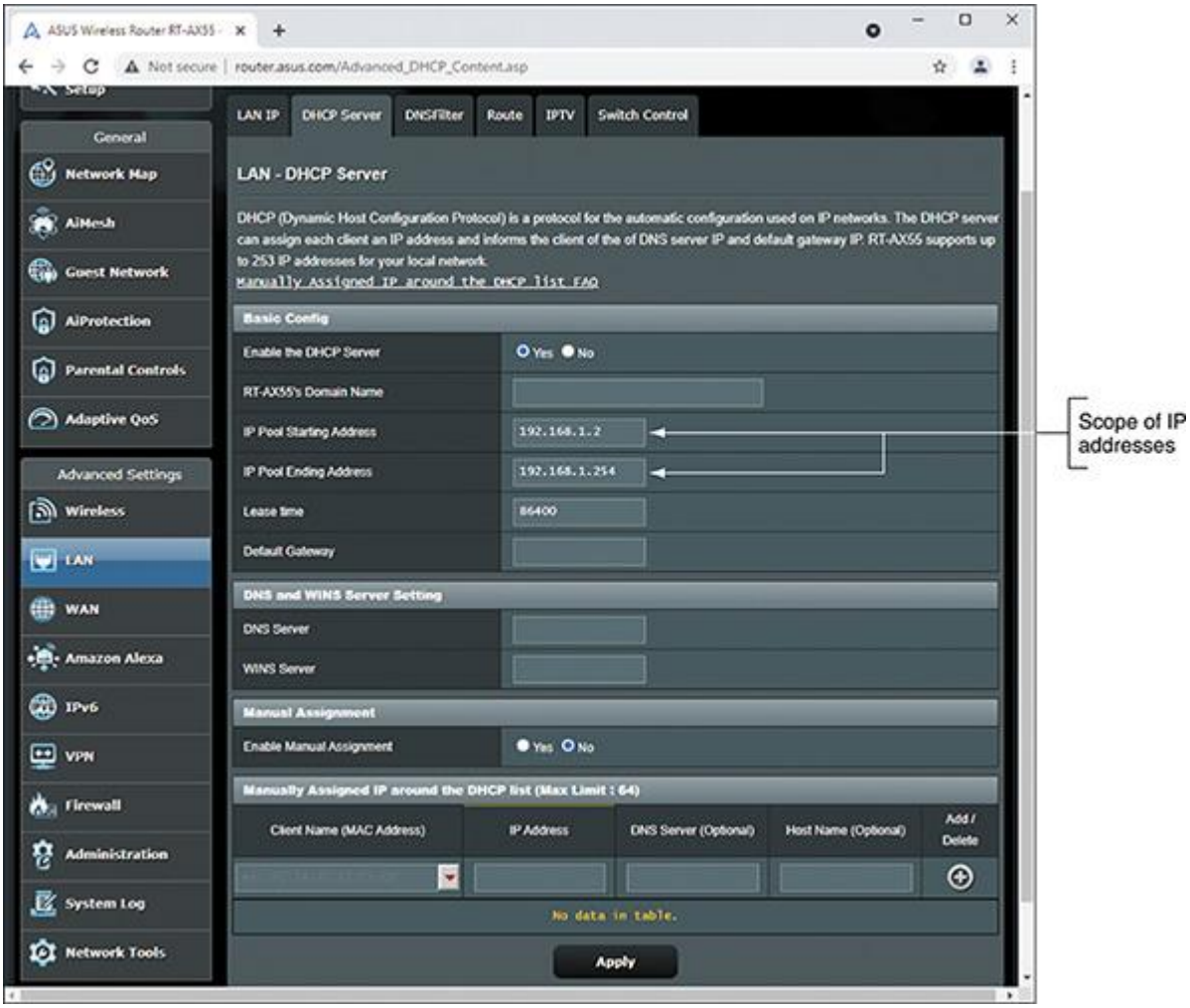
Main menu for a router with LAN submenus shown



2. Notice in Figure 7-38 the IP address of the router on the LAN is 192.168.1.1 and the subnet mask for the LAN is 255.255.255.0. Click the **DHCP Server** tab to see options for configuring the DHCP server (see Figure 7-39).

Figure 7-39

Configure the DHCP server



3. By default, DHCP is enabled and the scope of IP addresses that DHCP can lease to DHCP client devices is 192.168.1.2 through 192.168.1.254. Because the default gateway does not have a value, it is assumed the router itself is the gateway. After making changes on this page, click **Apply** to save your changes.

Note 9

As you advance in your networking skills, you'll learn how to choose subnet masks and ranges of IP addresses to divide a large network into more manageable subnets. For now, know that if your range of IP addresses varies only in the last octet, the subnet mask is 255.255.255.0. If the range of IP addresses varies in the last two octets, the subnet mask is 255.255.0.0. You'll learn more about subnets in the module "Network Infrastructure and Cloud Computing."

Reserve IP Addresses

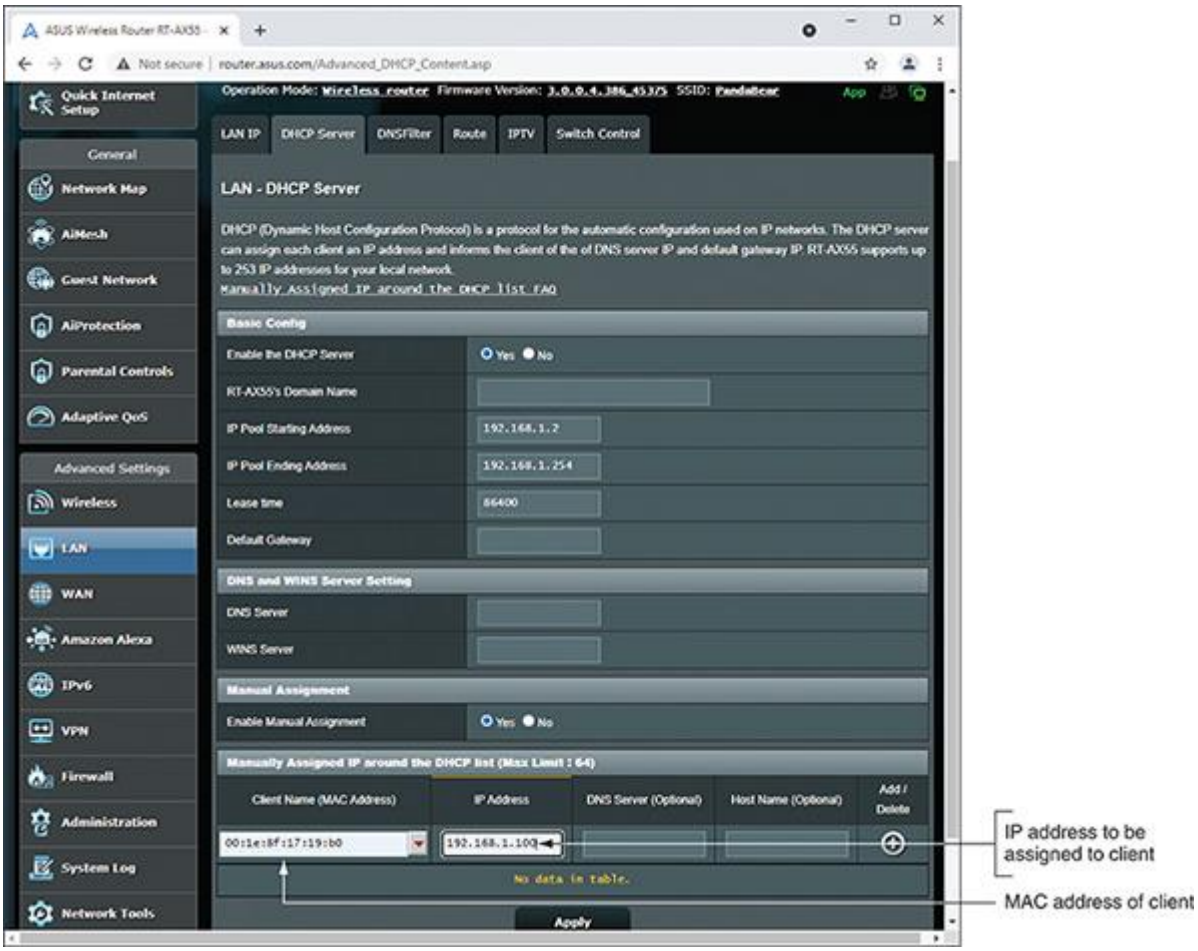
A network device such as a printer needs a consistent IP address at all times, so computers that access the printer don't need to be told its new IP address each time it reconnects to the network. In addition, a computer that is running a service, such as a web server, needs a consistent IP address so

other computers can consistently find the web server. You could assign the printer and web server IP addresses by configuring the device or computer for static IP addressing. Alternately, you can assign the same IP address to a device or computer by creating an **address reservation** on the DHCP server so the DHCP client receives or leases the same IP address each time it connects to the network. Do the following to reserve an IP address:

1. To identify the computer or printer, you'll need its MAC address. When the client is connected to the network, the router can report its MAC address. Look for a Network Map page. If the router doesn't report the MAC address, look for a label near the network port of the printer or in its documentation.
2. To assign a reserved IP address to the client, go to the LAN-DHCP Server page shown earlier in Figure 7-39. For Enable Manual Assignment, select **Yes**. Enter the MAC address and reserved IP address for the client (see Figure 7-40). Be sure to use an IP address in the range of IP addresses assigned by the DHCP server. Click the **+** sign to the left of the entries, and then click **Apply**. In Figure 7-40, a Canon network printer is set to receive the IP address 192.168.1.100 each time it connects to the network. It's helpful to network users to write this IP address on a label taped in plain sight on the printer or web server.

Figure 7-40

Manually assign a reserved IP address to a printer or other device that needs a static IP address



Now that you have set up and configured the router and verified the Internet connection, you can connect other computers to the network.

7-3bConnecting a Computer to a Local Network

Core 1 Objectives

- 2.5

  Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

- 2.6

  Compare and contrast common network configuration concepts.

Connecting a laptop or desktop computer to a network is quick and easy in most situations. To connect a computer to a network using an Ethernet wired or Wi-Fi wireless connection, follow these steps:

1. 1

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

2. 2
   Do one of the following to connect to the network:

   - For a wired network, plug in the network cable to a wall jack or switch, or directly to a SOHO router. Plug the other end into the computer's Ethernet port. Indicator lights near the network port should light up to indicate connectivity and activity. For Ethernet, Windows should automatically configure the connection.
   - For a wireless network, click the **Network** icon in the taskbar on the desktop, and select a wireless network. Click **Connect**. If the network is secured, you must enter the security key to the wireless network to connect.

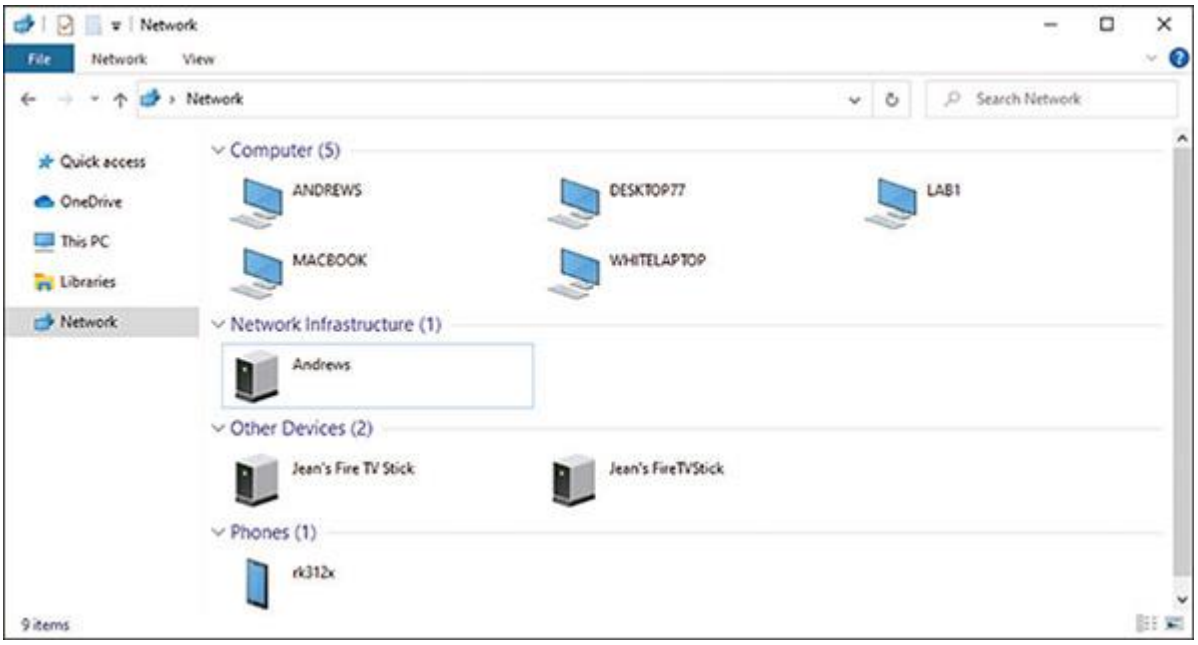
3. 3
   If this is the first time you've connected to a local network, you'll be asked if you want to make the PC discoverable. For private networks (such as your home or business), click **Yes**, and for public networks (such as a coffee shop hotspot), click **No**.

   Note 10
   For a private corporate or enterprise network, Windows Server or Microsoft Azure is likely used to manage access to the network using a Windows domain. You must sign in to the Windows domain with a user name and password. Press Ctrl+Alt+Del to access the sign-on screen. The username might be text such as Jane Smith or an email address such as JSmith@mycompany.com. You learn more about private networks, public networks, and Windows domains in the Core 2 module "The Complex World of IT Professionals."

4. 4
   Open your browser and make sure you can access the web. For wireless connections, some hotspots provide an initial page called a captive portal, where you must enter a code or agree to the terms of use before you can use the network. On a private network, open **Explorer** and drill down into the Network group to verify that network resources are available (see Figure 7-41).

Figure 7-41

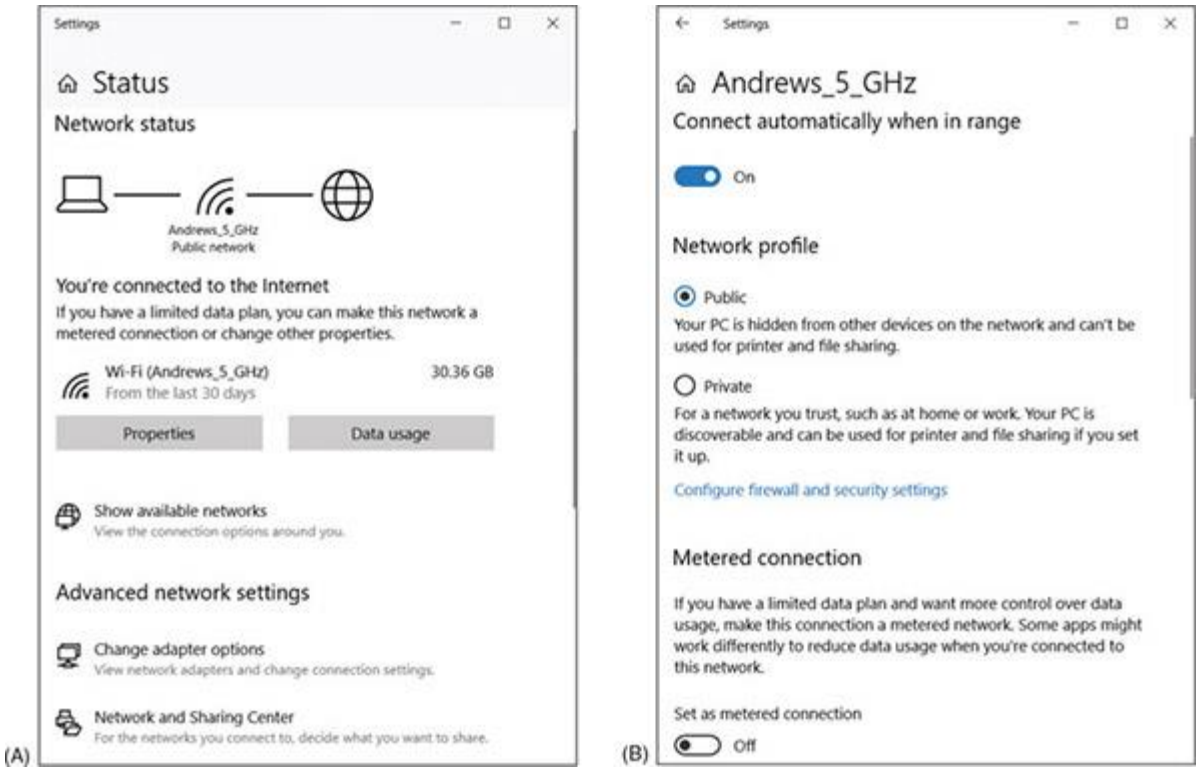
File Explorer shows resources on the network



To view and change network security settings, in the Settings app, click **Network & Internet**. In the Status window (see Figure 7-42A), under *Network status*, click **Properties**. Under *Network profile*, select either **Public** or **Private**. See Figure 7-42B.

Figure 7-42

Configure the network connection for a public or private network

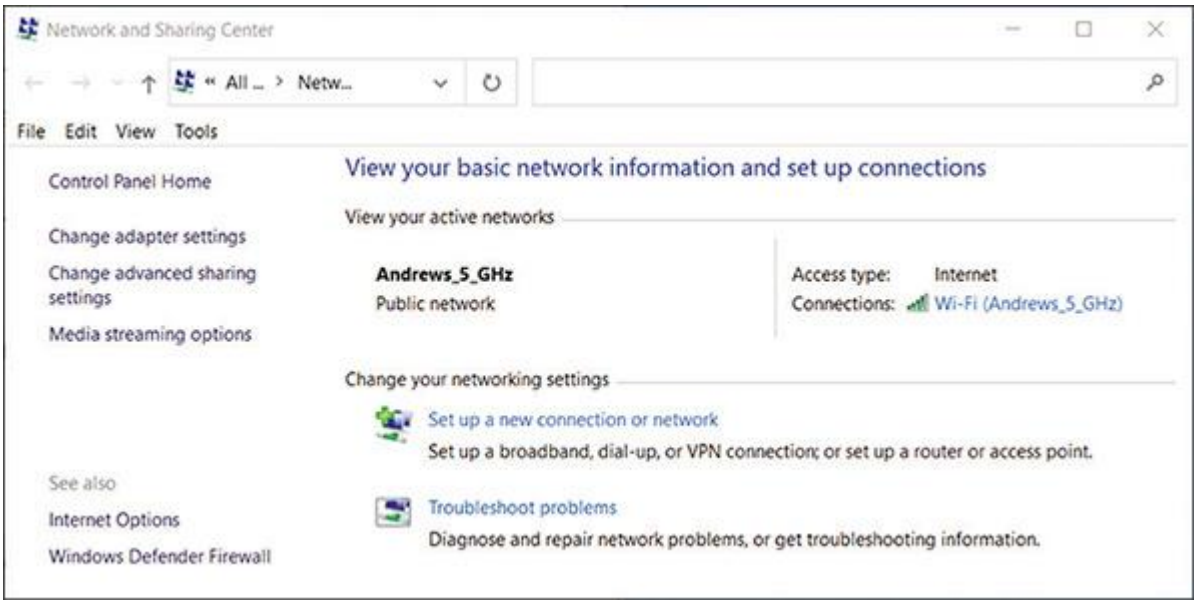


Although the Settings app provides several tools to manage network connections, you have more detailed control when using the Network and Sharing Center. For example, to view the security key used for a wireless connection, do the following:

1. Open **Control Panel** and open the **Network and Sharing Center**. Alternately, right-click **Start**, click **Network Connections**, and click **Network and Sharing Center**. In the Network and Sharing Center (see Figure 7-43), click **Change adapter settings**, or in the Network & Internet window, click **Change adapter options**.

Figure 7-43

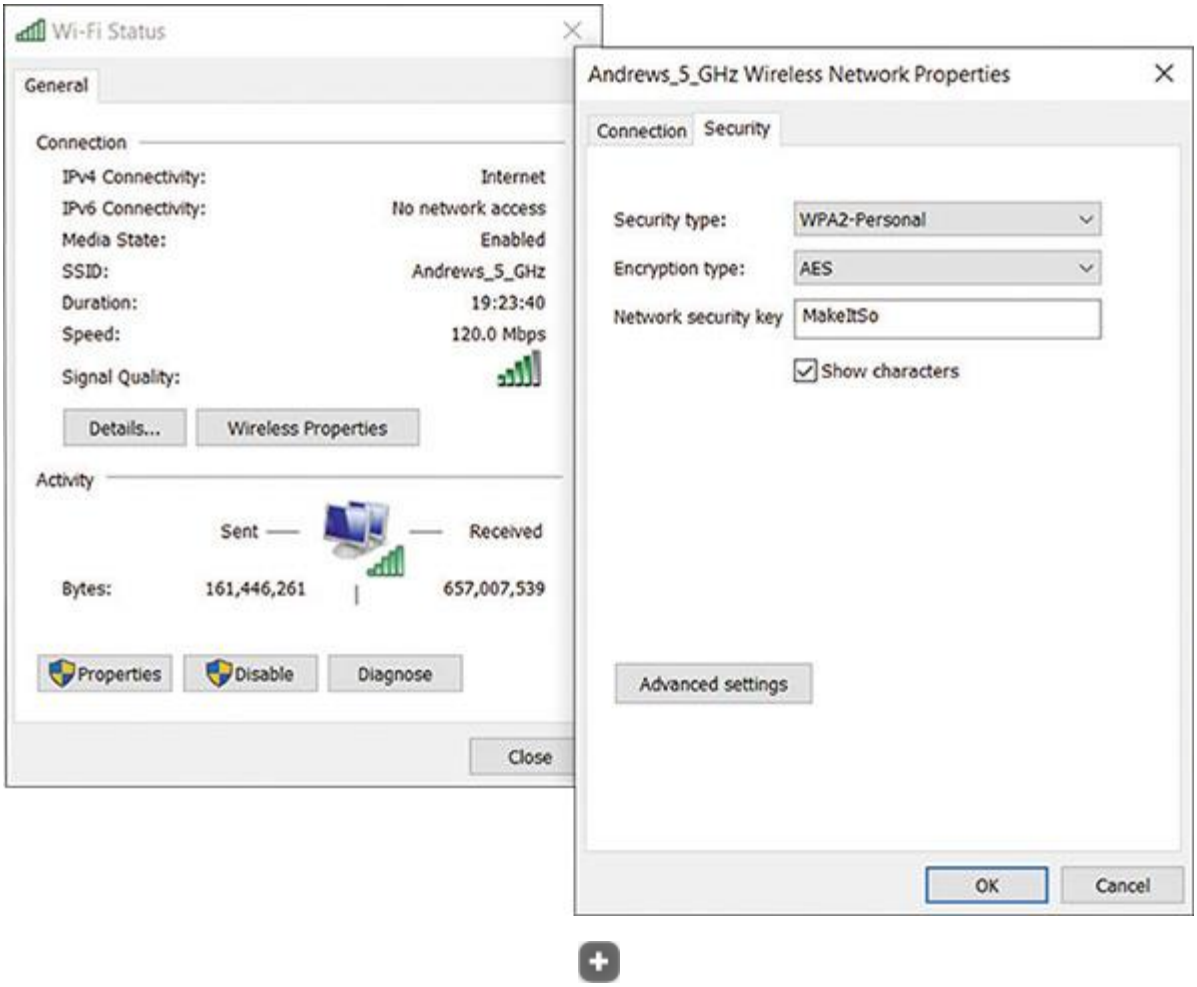
The Network and Sharing Center reports a healthy wireless network connection



2. In the Network Connections window, right-click the **Wi-Fi** connection (refer back to Figure 7-12), and click **Status**. In the Wi-Fi Status dialog box (see Figure 7-44), click **Wireless Properties**. In the Wireless Network Properties dialog box, select the **Security** tab. To view the security key, check **Show characters**. You can also see the security and encryption types that Windows automatically detected and applied when it made the connection.

Figure 7-44

View the network security key for the wireless network



Core to Core

You learn more about wireless network security in the Core 2 module "Network Security and Troubleshooting."

If you have a problem making a network connection, you can reset the connection. Open the **Network Connections** window and right-click the network connection. Select **Disable** from the shortcut menu, as shown earlier in Figure 7-12. Right-click the connection again, and select **Enable**. The connection is reset. Try again to browse the web or access resources on the network. If you still don't have local or Internet access, it's time to dig a little deeper into the source of the problem. More network troubleshooting tools and solutions are covered in the module "Network Security and Troubleshooting."

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

7-3c Configure TCP/IP Settings

Core 1 Objectives

- 2.5

  Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

- 2.6

  Compare and contrast common network configuration concepts.

Most networks use dynamic IP addressing. By default, Windows requests dynamic IP configuration from the DHCP server, and there is nothing for you to configure. (As you know, the DHCP server might serve up a dynamic or reserved IP address to a client.) In some situations, however, the network does not have a DHCP server, so as an IT support technician, you need to know how to configure static IP addressing.

Exam Tip

The A+ Core 1 exam expects you to know how to configure dynamic, reserved, and static IP addresses on a router or computer. You also need to recognize whether an IP address is an automatic private IP address.

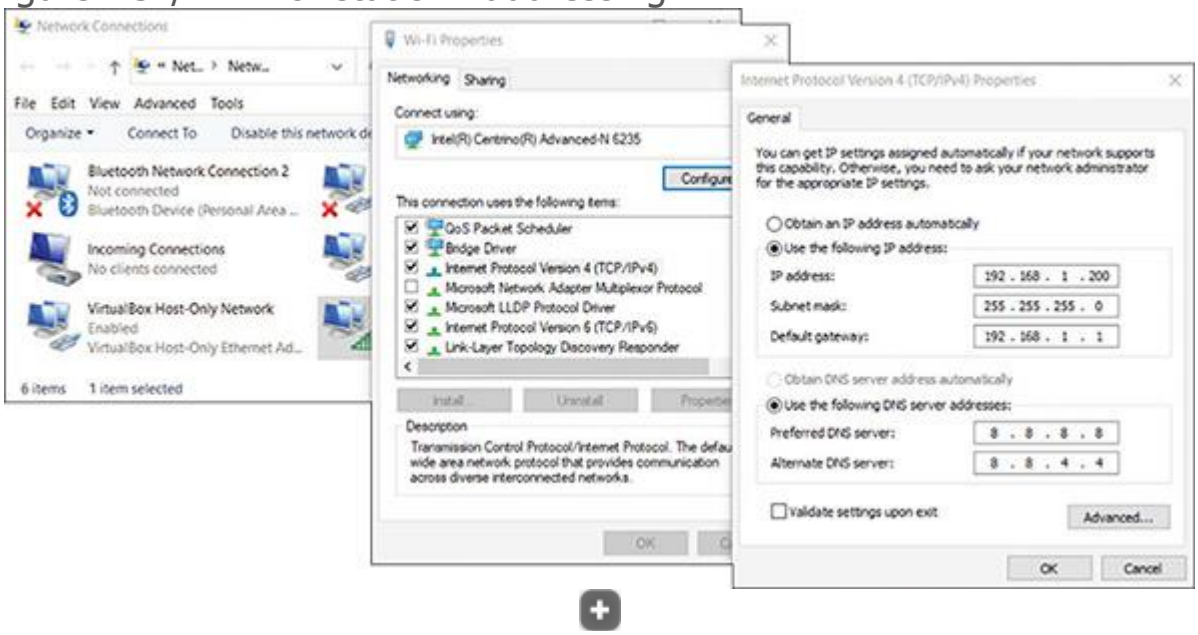
Follow these steps to configure static IP addressing:

1. 1

   Open the **Network Connections** window. Right-click the network connection, and click **Properties**. In the Properties dialog box on the **Networking** tab (as shown in the middle box of Figure 7-45), select **Internet Protocol Version 4 (TCP/IPv4)**, and click **Properties**. The TCP/IPv4 Properties dialog box appears (see the right side of Figure 7-45).

Figure 7-45

Configure TCP/IPv4 for static IP addressing



2. 2

As you saw in Figure 7-13, the default is dynamic IP addressing, which uses the *Obtain an IP address automatically* and *Obtain DNS server address automatically* settings. In Figure 7-45, static IP addressing is used. To change the settings to static IP addressing, select **Use the following IP address**. Then enter the IP address, subnet mask, and default gateway.

3. 3
   If your network administrator has given you the IP addresses of DNS servers, select **Use the following DNS server addresses**, and enter up to two IP addresses. If you have additional DNS IP addresses, click **Advanced** and enter them on the **DNS** tab of the Advanced TCP/IP Settings box.

Note 11

As an IT support technician, it's unlikely you'll ever be called on to configure static IPv6 addressing. However, to do so, use the Properties dialog box shown in the middle of Figure 7-45. Select Internet Protocol Version 6 (TCP/IPv6), and click Properties.

You can also uncheck Internet Protocol Version 6 (TCP/IPv6) to disable it. For most situations, you need to leave it enabled.

7-3dAlternate IP Address Configuration

Core 1 Objective

- 2.5

  Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

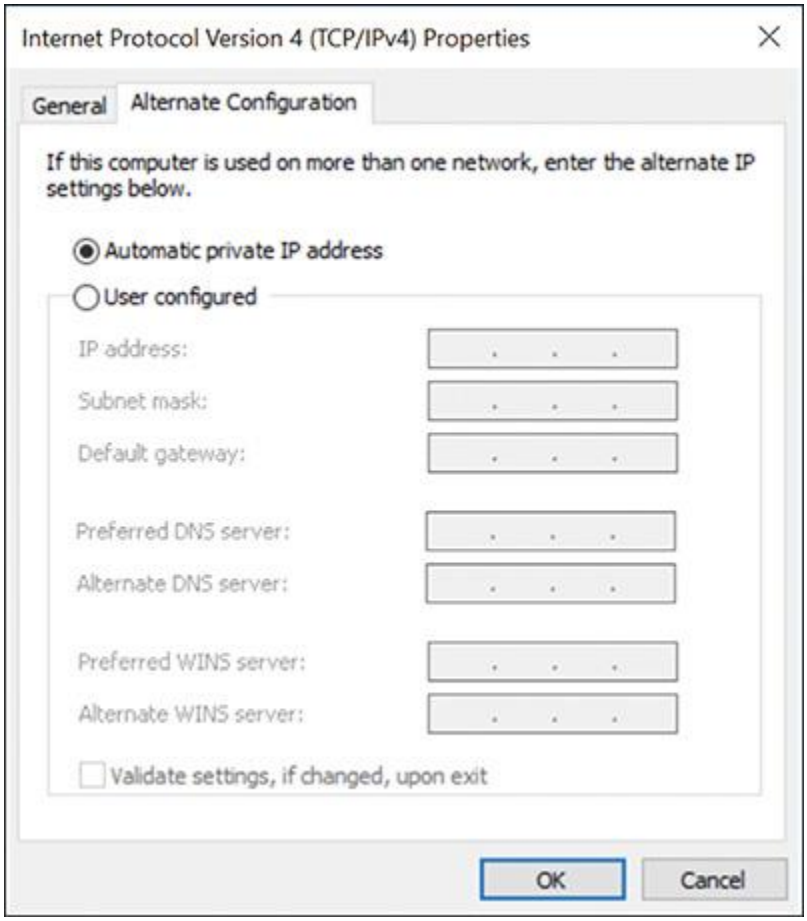
  Suppose an employee with a laptop often travels, and the work network uses static IP addressing, even though most public networks use dynamic IP addressing. How do you configure the employee's computer's network connection settings? For travel, you would configure the computer to use dynamic IP addressing in order to connect to public networks. However, using that configuration means that when the computer attempts to connect to the corporate network, it won't be able to find a DHCP server. Recall that, in this situation, the computer generates an Automatic private IP address (APIPA) in the address range 169.254.x.y. However, you can assign a static IP address by using an alternate configuration.

  To create an alternate configuration, first use the General tab of the TCP/IPv4 Properties dialog box shown earlier in Figure 7-13 to set the configuration for dynamic IP addressing. Then click the **Alternate Configuration** tab. See Figure 7-46. Select **User configured**. Then enter a

static IP address, subnet mask, default gateway, and DNS server addresses for the alternate configuration to be used on the company network.
Click **OK** and close all dialog boxes. Now the computer will first attempt to gather network connection settings from a DHCP server. If a DHCP server is not available on the network, the computer will instead use the static IP settings you just entered.

Figure 7-46

Create an alternate static IP address configuration



Next, let's learn a little about configuring DNS, which might also be expected of IT technicians when configuring networks.

7-3e DNS Configuration Basics

Core 1 Objective

- 2.6

Compare and contrast common network configuration concepts.

Suppose your company decides to publish a website or run its own email server. In this situation, you might be called on to make entries in the DNS

namespace so that the world will know how to reach your website or email server. The DNS **namespace** is the entire collection of DNS databases stored on DNS servers (also called name servers) around the globe. In these databases, an individual entry, such as one that associates a host name with a given IP address, is called a **resource record (RR)**. Resource records are collected into zone files. Often, one **zone file** holds all the records for a single domain, such as *cengage.com*. Each resource record can have up to six parts:

- Name of the resource (host name)
- Record type
- Class code (always IN, which means the record is allowed on the Internet)
- TTL (time-to-live)—the time a server can hold the record in its cache; the default is one hour
- Length of data
- Data

There are about 30 types of DNS records. Here are the most common types of records you might be called on to edit:

- **A record.** An **A record (address record)** points a host name to its IP address. A website requires an A record such as this one:

  ```
  www.mycompany.com A IN 14400 89.210.18.45
  ```

  Explanation:

  - The resource name is the host www.mycompany.com.
  - The record type is A.
  - The class is IN.
  - TTL is 14,400 seconds.
  - Data is the IP address mapped to the host.
- **AAAA record.** A **AAAA record** (pronounced "quad-A record") is an address record for IPv6 addresses. Here is an example:

  ```
  www.mycompany.com AAAA IN
  2001:07b8:8ba3:0000:0000:6a22:0323:7223
  ```

- **CNAME record.** A **CNAME (Canonical Name) record** redirects from one host name to another, for example:

  ```
  www.mycompany.com CNAME IN newcompany.com
  ```

- **MX record.** The **MX (Mail Exchanger) record** points an email server domain name to an IP address:

  ```
  email.mycompany.com MX IN 95.165.13.45
  ```

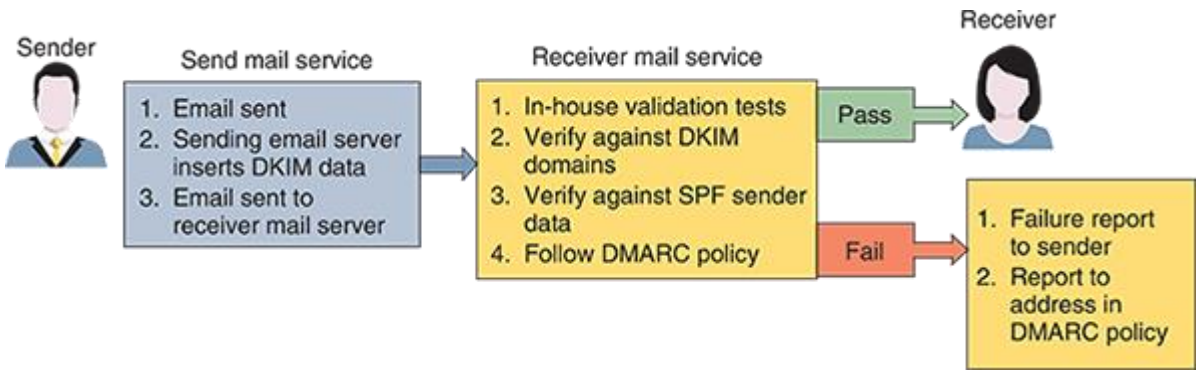
- **TXT record.** A **TXT (Text) record** is a general-purpose record used to insert text into the DNS namespace. One clever way TXT records are

used is when a company, such as PayPal, sends TXT records to an email provider, such as Yahoo!, to alert the email provider of potential fraudulent email, thereby preventing spoofing (email pretending to be from PayPal). Here are three ways TXT records are used for this purpose:

- **DKIM (DomainKeys Identified Mail) records** authenticate that an email message came from a trusted source by attaching a domain name identifier to the message. For more info, see dkim.org.
- **SPF (Sender Policy Framework) records** combat email spoofing by informing a recipient's mail server which email servers can send email from your domain.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance) records** tell a recipient's mail server what to do when it receives a fraudulent email message and is designed to work with DKIM and SPF. Figure 7-47 shows how the process works. For more info, see dmarc.org/overview.

Figure 7-47

DKIM, SPF, and DMARC work together to reduce fraudulent email



Exam Tip

The A+ Core 1 exam expects you to understand the purposes of DNS servers and be familiar with A, AAAA, MX, and TXT records, including how DKIM, SPF, and DMARC use TXT records for spam management.

Applying Concepts

Viewing and Clearing the DNS Cache

- **Est. Time:** 15 minutes
- **Core 1 Objective:** 2.6

When Windows is trying to resolve a computer name to an IP address, it first looks in the DNS cache it holds in memory. If the computer name is not found in the cache, Windows then turns to a DNS server if it has the IP address of the server.

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

Note 12

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

7-4a Module Summary

Understanding TCP/IP and Windows Networking

- In networking, an application is identified by a port address. A device on the network—and its network connection—are identified by an IP address. A network adapter is identified by a MAC address.
- A computer can be assigned a computer name, and a network can be assigned a domain name. A fully qualified domain name (FQDN) includes the computer name and the domain name. An FQDN can be used to find a computer on the Internet if this name is associated with an IP address kept by DNS servers in the DNS namespace.
- According to the TCP/IP model, networking communication must happen at four layers: Link, Internet, Transport, and Application.
- The Internet primarily uses client/server applications for communication. Common server applications include a web server, mail server, file server, print server, DHCP server, DNS server, proxy server, AAA server, syslog server, FTP server, Telnet server, SSH server, RDP server, and SNMP server.
- TCP/IP uses several protocols at the Application layer (such as FTP, HTTP, and Telnet) and at the Transport layer (such as TCP and UDP). The Internet layer primarily relies on IP, and the Link layer mostly uses Ethernet and Wi-Fi protocols.
- At the Transport layer, TCP is a connection-oriented protocol, and UDP is a connectionless protocol.
- At the Internet layer, the OS identifies a network connection by an IP address. At the Transport layer, a port address identifies an application.
- At the Link layer, a network adapter has a MAC address that uniquely identifies it on the network.

- 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.
- A host needs an IP address, a subnet mask, a default gateway, and IP addresses for DNS servers to communicate with other hosts on the local or remote networks.
- An IPv4 address has 32 bits, and an IPv6 address has 128 bits. Some IP addresses are private and can only be used on a local network.
- Using IPv4, the string of 1s in a subnet mask determines the number of leftmost bits in an IP address that identify the local network. The string of 0s determines the number of rightmost bits in the IP address that identify the host.
- Using IPv6, three types of IP addresses are a multicast address (used for one-to-many transmissions), anycast address (used by routers), and unicast address (used to address a single node on a network).

Network Hardware

- Network adapters, commonly called NICs, are rated by speed, and each has a MAC address. Some NICs have status indicator lights and wake-on-LAN and QoS features.
- A hub is an outdated networking distribution device that broadcasts messages. A switch is more efficient because it works to send a message only to the device to which the message is addressed.
- A cable modem stands between an ISP and a local network to convert signals from each network so the other network can understand it.
- A multifunction router for a small office/home office network might serve several functions, including router, switch, DHCP server, wireless access point, firewall, and FTP server.

Local Network Setup and Configuration

- It's extremely important to change the administrative password on a router as soon as you install it, especially if the router also serves as a wireless access point.
- A DHCP server is configured to lease a scope or range of IP addresses to DHCP clients on the network and can reserve certain IP addresses to be used as static IP addresses on the network.
- When connecting a computer to the local network, static or dynamic IP addressing can be used, and the computer recognizes the network as a public or private network.
- Four common types of DNS records include address records (A and AAAA), CNAME, MX records, and TXT records.

7-4c Thinking Critically

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

1. You just finished installing a network adapter, and after booting up the system, you installed the drivers. You open Explorer on a remote computer and don't see the computer on which you installed the new NIC. What is the first thing you check? What is the second thing?

    1. Has IPv6 addressing been enabled?
    2. Can the computer on which you installed the NIC access the network?
    3. Do the lights on the adapter indicate it's functioning correctly?
    4. Has the computer been assigned a computer name?

2. Your manager has asked you to configure a DHCP reservation on the network for a Windows computer that is used to configure other devices on a network. To do this, you need the computer's MAC address. What command can you enter at the command line to access this information?

3. The DHCP server in a SOHO router is using the IP scope of 192.168.50.2 to 192.168.50.254. The subnet mask is 255.255.255.0. The technician has configured one computer with the static IP address of 192.168.1.100 and subnet mask of 255.255.255.0. This computer cannot communicate with other computers on the local network. What is the problem and a workable solution?

    1. The computer is not in the same subnet as others on the network. Change the static IP address to 192.168.100.1.
    2. The subnet mask on the router is not correct. Change it to 255.255.255.255.
    3. The computer is not in the same subnet as others on the network. Change the static IP address to 192.168.50.100.
    4. The subnet needs to be enlarged to include more IP addresses. Change the subnet mask on the router to 255.255.0.0.

4. A computer on a LAN is not able to connect to the Internet even though other computers on the LAN are able to connect. You use the ipconfig command to discover the IP address of the computer is 169.254.18.45. What can you conclude from this information?

    1. The ISP connection is down, and you need to reboot the router.
    2. The computer did not connect to the router to receive a dynamic IP address.
    3. The computer's NIC is not functioning correctly, or a port on the router is bad.
    4. The router's DHCP server is not configured correctly.

5. Why does a DHCP server and client use UDP rather than TCP for transmissions? (Choose all that apply.)

    1. UDP is required for all client/server applications.
    2. A DHCP client broadcasts over the local network looking for a DHCP server when it first connects to the network.
    3. UDP relies on MAC addresses for communication and TCP does not.
    4. TCP works only on the Internet and not on the local network.

6. Your new company is setting up its first website with a public IP address it has leased from its ISP. Your manager has asked you to set up the necessary DNS records so the website can be found on the web. Which type of DNS record will you create?

1. A record
2. AAAA record
3. MX record
4. CNAME record

7. Which statements are true about TCP and UDP? (Choose all that apply.)

1. TCP is generally faster than UPD.
2. TCP guarantees delivery and UDP does not.
3. UDP is used on the local network but not on the Internet; TCP works on both the local network and the Internet.
4. TCP establishes a session between source and destination before it sends data, and UDP sends data without first establishing a session.

8. Which ports might you use when configuring email client/server applications? (Choose all that apply.)

1. Ports 25, 110, and 143
2. Ports 21, 22, and 23
3. Ports 22, 110, and 143
4. Ports 67, 68, 80, and 110

9. What does a web server use port 80 for, and what does it use port 443 for?

1. For secured transmissions; for unsecured transmissions
2. For sending data; for receiving data
3. For unsecured transmissions; for secured transmissions
4. For communication with browsers; for communication with smartphones

10. Which port is used by either TCP or UDP when Windows shares files across a local network?

1. Port 443
2. Port 445
3. Port 3389
4. Port 53

11. Computer A has an IP address of 10.200.45.60 and a subnet mask of 255.255.0.0. Which of the following statements are true? (Choose all that apply.)

1. Computer B, with IP address of 10.200.200.200, is on the same local network as Computer A.
2. Computer B, with IP address of 10.250.10.12, is on the same local network as Computer A.
3. Computer B, with IP address of 10.200.45.200, is on the same local network as Computer A.
4. Computer B, with IP address of 192.168.1.1, is on the same local network as Computer A.

12. Which of the following IP addresses are recommended for private networks? (Choose all that apply.)

1. IP addresses that begin with 10 as their first octet

2. IP addresses that begin with 172 as their first octet
3. IP addresses that begin with 192.168 as their first two octets
4. IP addresses that begin with 192 as their first octet

13. Which of the following IPv6 addresses are global addresses allowed on the Internet? (Choose all that apply.)

1. 128-bit IP addresses that begin with 2001
2. 128-bit IP addresses that begin with 2000
3. 32-bit IP addresses that begin with 9 in the first octet
4. 128-bit IP addresses that begin with 8888

14. When connecting a wireless device to a Wi-Fi network, the network is identified by which of the following?

1. Service Set Identifier
2. IP address
3. Domain name
4. MAC address

15. Which DNS record type is used to provide information intended to help filter email to allow only trusted sources?

1. A records
2. CNAME records
3. AAAA records
4. TXT records