3

CHAPTER THREE

Networking Components and Devices

Objectives

3.1 Install, configure and differentiate between common network devices

- Hub
- Repeater
- Modem
- NIC
- Media converters
- Basic switch
- Bridge
- Wireless access point
- Basic router
- Basic firewall
- Basic DHCP server

3.2 Identify the functions of specialized network devices

- Multilayer switch
- Content switch
- IDS/IPS
- Load balancer
- Multifunction network devices
- DNS server
- Bandwidth shaper
- Proxy server
- CSU/DSU

3.3 Explain the advanced features of a switch

- PoE
- Spanning tree
- VLAN
- Trunking
- Port mirroring
- Port authentication

What You Need To Know

- Describe how hubs and switches work.
- Explain how hubs and switches can be connected to create larger networks.
- Describe how bridges, routers, and gateways work.
- Describe how routing protocols are used for dynamic routing.
- Explain the purpose of other networking components, such as Channel Service Unit/Data Service Unit (CSU/DSU) and gateways.
- Describe the purpose and function of network cards.
- Describe the purpose of a firewall.

Introduction

All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and are requirements for a Network+ candidate.

This chapter introduces commonly used networking devices. Although it is true that you are not likely to encounter all the devices mentioned in this chapter on the exam, you can be assured of working with at least some of them.

Hubs

At the bottom of the networking food chain, so to speak, are hubs. Hubs are used in networks that use twisted-pair cabling to connect devices. Hubs also can be joined to create larger networks. *Hubs* are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data package is destined for the device. This makes them inefficient devices and can create a performance bottleneck on busy networks.

In its most basic form, a hub does nothing except provide a pathway for the electrical signals to travel along. Such a device is called a *passive* hub. Far more common nowadays is an *active* hub, which, as well as providing a path for the data signals, regenerates the signal before it forwards it to all the connected devices. In addition, an active hub can buffer data before forwarding it. However, a hub does not perform any processing on the data it forwards, nor does it perform any error checking.

Hubs come in a variety of shapes and sizes. Small hubs with five or eight connection ports are commonly called *workgroup hubs*. Others can accommodate larger numbers of devices (normally up to 32). These are called *high-density devices*. Because hubs don't perform any processing, they do little except enable communication between connected devices. For today's high-demand network applications, something with a little more intelligence is required. That's where switches come in.

MSAU

In a token ring network, a multistation access unit (MSAU) is used in place of the hub that is used on an Ethernet network. The MSAU performs the token circulation inside the device, giving the network a physical star appearance. It functions as a logical ring. The logical ring function is performed from within the MSAU. Each MSAU has a ring in (RI) port on the device, which is connected to the ring out (RO) port on another MSAU. The last MSAU in the ring is then connected to the first to complete the ring. Because token ring networks are few and far between nowadays, it is far more likely that you will find yourself working with Ethernet hubs and switches.

NOTE

Multistation access unit is sometimes written as MSAU, but it is commonly called MAU. Both acronyms are acceptable.

EXAM ALERT

Even though MSAU and token ring networks are not common, you can expect a few questions on them on the exam.

Switches

Like hubs, *switches* are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data they receive. Whereas a hub forwards the data it receives to all the ports on the device, a switch forwards it to only the port that connects to the destination device. It does this by *learning* the MAC address of the devices attached to it and then by matching the destination MAC address in the data it receives. Figure 3.1 shows how a switch works.

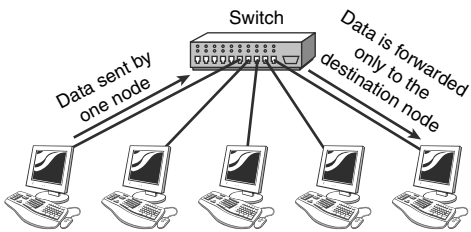

FIGURE 3.1 How a switch works.

By forwarding data to only the connection that should receive it, the switch can greatly improve network performance. By creating a direct path between two devices and controlling their communication, the switch can greatly reduce the traffic on the network and therefore the number of collisions. As you might recall, collisions occur on Ethernet networks when two devices attempt to transmit at exactly the same time. In addition, the lack of collisions enables switches to communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send data to and receive data from the switch at the same time. Contrast this with half-duplex communication, in which communication can occur in only one direction at a time. Full-duplex transmission speeds are double that of a standard half-duplex connection. So, a 10Mbps connection becomes 20Mbps, and a 100Mbps connection becomes 200Mbps.

The net result of these measures is that switches can offer significant performance improvements over hub-based networks, particularly when network use is high.

Irrespective of whether a connection is at full or half duplex, the method of switching dictates how the switch deals with the data it receives. The following is a brief explanation of each method:

- **Cut-through**: In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is very fast,

but it creates the possibility of errors being propagated through the network, because no error checking occurs.

- **Store-and-forward**: Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error-checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error-checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.
- **FragmentFree**: To take advantage of the error checking of store-and-forward switching, but still offer performance levels nearing that of cut-through switching, FragmentFree switching can be used. In a FragmentFree-switching environment, enough of the packet is read so that the switch can determine whether the packet has been involved in a collision. As soon as the collision status has been determined, the packet is forwarded.

Hub and Switch Cabling

In addition to acting as a connection point for network devices, hubs and switches can be connected to create larger networks. This connection can be achieved through standard ports with a special cable or by using special ports with a standard cable.

The ports on a hub to which computer systems are attached are called *Medium-Dependent Interface Crossed (MDI-X)*. The crossed designation is derived from the fact that two of the wires within the connection are crossed so that the send signal wire on one device becomes the receive signal of the other. Because the ports are crossed internally, a standard or *straight-through* cable can be used to connect devices.

Another type of port, called a *Medium-Dependent Interface (MDI)* port, is often included on a hub or switch to facilitate the connection of two switches or hubs. Because the hubs or switches are designed to see each other as simply an extension of the network, there is no need for the signal to be crossed. If a hub or switch does not have an MDI port, hubs or switches can be connected by using a *crossover* cable between two MDI-X ports. The crossover cable uncrosses the internal crossing. Crossover cables are discussed in Chapter 2, "Cabling, Connectors, and Ethernet Standards."

NOTE

In a crossover cable, wires 1 and 3 and wires 2 and 6 are crossed.

Bridges

Bridges are used to divide larger networks into smaller sections. Bridges accomplish this by sitting between two physical network segments and managing the flow of data between the two. By looking at the MAC address of the devices connected to each segment, bridges can elect to forward the data (if they believe that the destination address is on another interface) or block it from crossing (if they can verify that it is on the interface from which it came). Figure 3.2 shows how a bridge can be used to segregate a network.

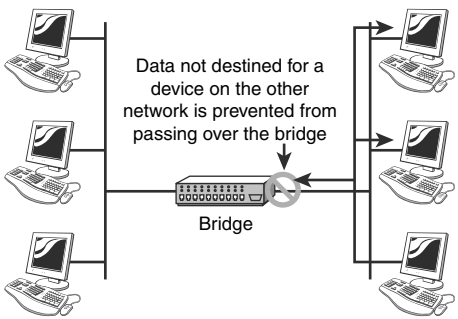

FIGURE 3.2 How a bridge is used to segregate a network.

NOTE

Bridges can also be used to connect two physical LANs into a larger logical LAN.

When bridges were introduced, the MAC addresses of the devices on the connected networks had to be entered manually. This was a time-consuming process that had plenty of opportunity for error. Today, almost all bridges can build a list of the MAC addresses on an interface by watching the traffic on the network. Such devices are called *learning bridges* because of this functionality.

Bridge Placement and Bridging Loops

You must consider two issues when using bridges:

- **Bridge placement**: Bridges should be positioned in the network using the 80/20 rule. This rule dictates that 80% of the data should be local and the other 20% should be destined for devices on the other side of the bridge.
- **Eliminating bridging loops**: Bridging loops can occur when more than one bridge is implemented on the network. In this scenario, the bridges can confuse each other by leading one another to believe that a device is located on a certain segment when it is not. To combat the bridging loop problem, the IEEE 802.1d Spanning Tree Protocol enables bridge interfaces to be assigned a value that is then used to control the bridge-learning process.

Types of Bridges

Three types of bridges are used in networks:

- **Transparent bridge**: Derives its name from the fact that the devices on the network are unaware of its existence. A transparent bridge does nothing except block or forward data based on the MAC address.
- **Source route bridge**: Used in token ring networks. The source route bridge derives its name from the fact that the entire path that the packet is to take through the network is embedded in the packet.
- **Translational bridge**: Used to convert one networking data format to another, such as from token ring to Ethernet and vice versa.

Today, bridges are slowly but surely falling out of favor. Ethernet switches offer similar functionality; they can provide logical divisions, or segments, in the network. In fact, switches are sometimes called *multiport bridges* because of how they operate.

Routers

In a common configuration, routers are used to create larger networks by joining two network segments. A small office, home office (SOHO) router is used to connect a user to the Internet. A SOHO router typically serves 1 to 10 users on the system. A router can be a dedicated hardware device or a computer system with more than one network interface and the appropriate routing software. All modern network operating systems include the functionality to act as a router.

NOTE

Routers normally create, add, or divide networks or network segments at the network layer of the OSI reference model because they normally are IP-based devices. Chapter 4, "OSI Model and Network Protocols," covers the OSI reference model in greater detail.

A router derives its name from the fact that it can route data it receives from one network to another. When a router receives a packet of data, it reads the packet's header to determine the destination address. After the router has determined the address, it looks in its routing table to determine whether it knows how to reach the destination; if it does, it forwards the packet to the next hop on the route. The next hop might be the final destination, or it might be another router. Figure 3.3 shows, in basic terms, how a router works.

NOTE

You can find more information on network routing in Chapter 5, "TCP/IP Routing and Addressing."

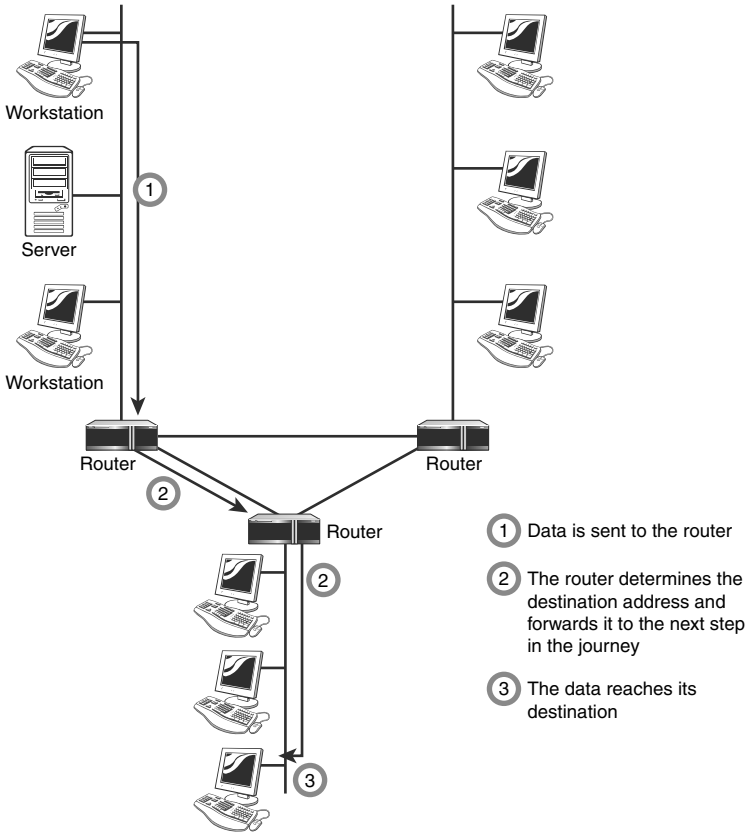

FIGURE 3.3 How a router works.

Gateways

Any device that translates one data format into another is called a *gateway*. Some examples of gateways include a router that translates data from one network protocol into another, a bridge that converts between two networking systems, and a software application that converts between two dissimilar formats. The key point about a gateway is that only the data format is translated, not the data itself. In many cases, the gateway functionality is incorporated into another device.

Don't confuse a gateway with the term *default gateway*. The term default gateway refers to a router to which all network transmissions not destined for the local network are sent. Chapter 5 covers default gateways in greater detail.

Network Cards

A network card, also called a network interface card (NIC), is a device that enables a computer to connect to the network.

When specifying or installing a NIC, you must consider the following issues:

- **System bus compatibility**: If the network interface you are installing is an internal device, bus compatibility must be verified. The most common bus system in use is the Peripheral Component Interconnect (PCI) bus, but some older systems might still use Industry Standard Architecture (ISA) expansion cards.
- **System resources**: Network cards, like other devices, need Interrupt Request (IRQ) and memory I/O addresses. If the network card does not operate correctly after installation, there might be a device conflict.
- **Media compatibility**: Today, the assumption is that networks use twisted-pair cabling, so if you need a card for coaxial or fiber-optic connections, you must specify this. Wireless network cards are also available.

Types of Network Interfaces

Network interfaces come as add-in expansion cards or as PCMCIA cards used in laptop systems. In some cases, rather than having an add-in NIC, the network interface is embedded into the motherboard.

A network interface typically has at least two LEDs that indicate certain conditions:

- **Link light**: This LED indicates whether a network connection exists between the card and the network. An unlit link light indicates that something is awry with the network cable or connection.
- **Activity light**: This LED indicates network activity. Under normal conditions, the light should flicker sporadically and often. Constant flickering might indicate a very busy network or a problem somewhere on the network that is worth investigating.
- **Speed light**: This LED indicates that the interface is connected at a certain speed. This feature normally is found on Ethernet NICs that operate at 10Mbps/100Mbps—and then only on certain cards.

Some network cards combine the functions of certain lights by using dual-color LEDs. PCMCIA cards sometimes have no lights, or the lights are incorporated into the media adapter that comes with the card.

Installing Network Cards

At some point in your networking career, it is likely that you will have to install a NIC into a system. For that reason, an understanding of the procedures and considerations related to NIC installations is useful. The following are some of the main things to consider.

CAUTION

Avoid ESD When installing any component in a system, you need to observe proper and correct procedures to guard against electrostatic discharge (ESD). ESD can cause components to fail immediately or degrade and fail at some point in the future. Proper ESD precautions include wearing an antistatic wrist strap and properly grounding yourself.

- **Drivers**: Almost every NIC is supplied with a driver disk, but the likelihood of the drivers on the disk being the latest drivers is slim. A device driver is software that allows communication between the hardware and the operating system. All hardware devices require device drivers to function. Always make sure that you have the latest drivers by visiting the website of the NIC manufacturer. The drivers play an important role in the correct functioning of the NIC, so spend a few extra minutes to make sure that the drivers are installed and configured correctly.
- **NIC configuration utilities**: In days gone by, NICs were configured with small groups of pins known as *jumpers*, or with small plastic blocks of switches known as *dip switches*. Unless you are working with very old equipment, you are unlikely to encounter dip switches.

  Although these methods were efficient and easy to use, they have largely been abandoned in favor of software configuration utilities. These allow you to configure the card's settings (if any) and to test whether the card is working properly. Other utilities can be used through the operating system to obtain statistical information, help, and a range of other features.
- **System resources**: To function correctly, NICs must have certain system resources allocated to them: the interrupt request (IRQ) and memory addresses. In some cases, you might need to assign the values for these manually. In most cases, you can rely on plug-and-play, which assigns resources for devices automatically.

- **Physical slot availability**: Most modern PCs have at least three or four usable expansion slots. Not only that, but the increasing trend toward component integration on the motherboard means that devices such as serial and parallel ports and sound cards are now built in to the system board and therefore don't use up valuable slots. If you're working on older systems or systems that have a lot of add-in hardware, you might be short of slots. Check to make sure that a slot is available before you begin.
- **Built-in network interfaces**: A built-in network interface is a double-edged sword. The upsides are that it doesn't occupy an expansion slot, and hardware compatibility with the rest of the system is almost guaranteed. The downside is that a built-in component cannot be upgraded. For this reason, you might find yourself installing an add-in NIC and at the same time disabling the onboard network interface. Disabling the onboard interface normally is a straightforward process; you go into the BIOS setup screen or, on some systems, use a system configuration utility. In either case, consult the documentation that came with the system, or look for information on the manufacturer's website.

As time goes on, NIC and operating system manufacturers are making it increasingly easy to install NICs in systems of all sorts and sizes. By understanding the card's requirements and the correct installation procedure, you should be able to install cards simply and efficiently.

Media Converters

Network technologies change rapidly, and administrators are always on the lookout for cost-effective ways to increase network performance. The demand for higher speeds and greater distances keeps administrators on their toes. The process of incorporating new technology with older infrastructure is made easier with media converters.

Network media converters are used to interconnect different types of cables within an existing network. For example, the media converter can be used to connect newer Gigabit Ethernet technologies with older 100BaseT networks.

The ability to combine networks and increase networking flexibility while decreasing the cost of having to retrofit the network to accommodate new technology is very important. Converters come in many shapes and sizes to connect to a variety of networks. This includes coax, twisted pair, single mode, and multimode fiber. Converters can be designed to work with any network type,

including Ethernet, Fast Ethernet, Gigabit Ethernet, Asynchronous Transfer Mode (ATM), Fiber Distributed Data Interface (FDDI), and token ring.

EXAM ALERT

Using media converters, companies do not need to dismantle the current wiring infrastructures. Media converters allow us to use existing infrastructure while keeping pace with changing technologies.

Wireless Access Points

Wireless access points (APs) are a transmitter and receiver (transceiver) device used to create a wireless LAN (WLAN). APs typically are a separate network device with a built-in antenna, transmitter, and adapter. APs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. APs also typically have several ports, giving you a way to expand the network to support additional clients.

Depending on the size of the network, one or more APs might be required. Additional APs are used to allow access to more wireless clients and to expand the range of the wireless network. Each AP is limited by a transmission range—the distance a client can be from an AP and still get a usable signal. The actual distance depends on the wireless standard being used and the obstructions and environmental conditions between the client and the AP.

EXAM ALERT

An AP can operate as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

Saying that an AP is used to extend a wired LAN to wireless clients doesn't give you the complete picture. A wireless AP today can provide different services in addition to just an access point. Today, the APs might provide many ports that can be used to easily increase the network's size. Systems can be added to and removed from the network with no effect on other systems on the network. Also, many APs provide firewall capabilities and DHCP service. When they are hooked up, they give client systems a private IP address and then prevent Internet traffic from accessing those systems. So, in effect, the AP is a switch, DHCP server, router, and firewall.

APs come in all different shapes and sizes. Many are cheaper and designed strictly for home or small-office use. Such APs have low-powered antennas and limited expansion ports. Higher-end APs used for commercial purposes have very high-powered antennas, enabling them to extend how far the wireless signal can travel.

NOTE

APs are used to create a wireless LAN and to extend a wired network. APs are used in the infrastructure wireless topology. Chapter 1, "Introduction to Networking," discusses wireless topologies.

Modems

A *modem*, short for modulator/demodulator, is a device that converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines. The modem at the receiving end converts the signal back into a format that the computer can understand. Modems can be used as a means to connect to an ISP or as a mechanism for dialing up a LAN.

Modems can be internal add-in expansion cards or integrated with the motherboard, external devices that connect to a system's serial or USB port, PCMCIA cards designed for use in laptops, or proprietary devices designed for use on other devices, such as portables and handhelds.

The configuration of a modem depends on whether it is an internal or external device. For internal devices, the modem must be configured with an interrupt request (IRQ) and a memory I/O address. It is common practice, when installing an internal modem, to disable the built-in serial interfaces and assign the modem the resources of one of them (typically COM2). Table 3.1 shows the resources associated with serial (COM) port assignments.

Table 3.1 Common Serial (COM) Port Resource Assignments

Port ID	IRQ	I/O Address	Associated Serial Interface Number
COM1	4	03F8	1
COM2	3	02F8	2
COM3	4	03E8	1
COM4	3	02E8	2

For external modems, you need not concern yourself directly with these port assignments, because the modem connects to the serial port and uses the resources assigned to it. This is a much more straightforward approach and one favored by those who work with modems on a regular basis. For PCMCIA and USB modems, the plug-and-play nature of these devices makes them simple to configure, and no manual resource assignment is required. After the modem is installed and recognized by the system, drivers must be configured to enable use of the device.

Two factors directly affect the speed of the modem connection—the speed of the modem itself and the speed of the Universal Asynchronous Receiver/Transmitter (UART) chip in the computer that is connected to the modem. The UART chip controls a computer's serial communication. Although modern systems have UART chips that can accommodate far greater speeds than the modem is capable of, older systems should be checked to make sure that the UART chip is of sufficient speed to support the modem speed. Normally you can determine which UART chip is installed in the system by looking at the documentation that comes with the system. Table 3.2 shows the maximum speed of the commonly used UART chip types.

EXAM ALERT

Be prepared to identify the information from Table 3.2 for the Network+ exam.

Table 3.2 UART Chip Speeds

UART Chip	Speed (Kbps)
8250	9600
16450	9600
16550	115,200
16650	430,800
16750	921,600
16950	921,600

NOTE

Keep in mind that internal modems have their own UARTs, but external modems use the UART that works with the COM port.

CAUTION

If you have installed an internal modem and are experiencing problems with other devices such as a mouse, there might be a resource conflict between the mouse and the modem. Also, legacy ISA NICs often use IRQ3 and might conflict with the modems.

Firewalls

A *firewall* is a networking device, either hardware- or software-based, that controls access to your organization's network. This controlled access is designed to protect data and resources from an outside threat. To do this, firewalls typically are placed at a network's entry/exit points—for example, between an internal network and the Internet. After it is in place, a firewall can control access into and out of that point.

Although firewalls typically protect internal networks from public networks, they are also used to control access between specific network segments within a network. An example is placing a firewall between the Accounts and Sales departments.

As mentioned, firewalls can be implemented through software or through a dedicated hardware device. Organizations implement software firewalls through network operating systems (NOSs) such as Linux/UNIX, Windows servers, and Mac OS servers. The firewall is configured on the server to allow or block certain types of network traffic. In small offices and for regular home use, a firewall is commonly installed on the local system and is configured to control traffic. Many third-party firewalls are available.

Hardware firewalls are used in networks of all sizes today. Hardware firewalls are often dedicated network devices that can be implemented with very little configuration. They protect all systems behind the firewall from outside sources. Hardware firewalls are readily available and often are combined with other devices today. For example, many broadband routers and wireless access points have firewall functionality built in. In such a case, the router or AP might have a number of ports available to plug systems into.

EXAM ALERT

For the Network+ exam, remember that a firewall can protect internal networks from public networks and control access between specific network segments.

NOTE

Firewalls are discussed in greater detail in Chapter 9, "Network Security."

DHCP Server

Without question, the easiest way to assign TCP/IP information to client systems is to use a Dynamic Host Configuration Protocol (DHCP) server. On a network running TCP/IP, each computer must have a unique IP address in order to be recognized and be part of the network. Briefly, a *protocol* is a method of communicating between computers.

Computers on a network using TCP/IP require specific network settings to be able to connect to the network. First among these settings is the IP address. An IP address consists of four *octets*, or four sets of 8 bits—for example, 192.168.2.1. Each computer on the network must have one of these numbers in order to perform network functions through TCP/IP. The number must be unique to the PC and must be within a certain range to allow the PC to connect to other systems.

There was a time when these IP addresses were entered manually into the network settings of each client workstation. Manually set, or static, IP addresses were very difficult to maintain in large networks. Adding to the time it takes to individually set the IP addresses is the fact that each address must be unique. Duplicate IP addresses will prevent a successful connection to the network, meaning that all network services will be unavailable to the workstations with the duplicate addresses. When you're setting static IP addresses, it is essential to track assigned IP addresses carefully to prevent duplicating addresses and to make future expansion and troubleshooting easier.

In larger networks, the assignment of manual addresses can be a nightmare, especially when IP addressing schemes can be changed and computers can be moved, retired, or replaced. That's where DHCP comes in. DHCP assigns IP addresses, eliminating the need to assign IP addresses individually and making the job of network administrators considerably easier. When a DHCP server is running on a network, the workstation boots up and requests an IP address from the server. The server responds to the request and automatically assigns an IP address to the computer for a given period of time, known as a *lease*. The workstation acknowledges the receipt of the IP address, and the workstation has all the information it needs to become part of the network. This communication between the server and the workstation happens completely automatically and is invisible to the computer user.

Because of their capability to efficiently distribute IP addresses to network workstations, DHCP servers are widely used in client/server environments. People working with networks will most certainly encounter DHCP servers. The critical nature of DHCP services means that companies often choose to run more than one DHCP server. Mechanisms built in to DHCP allow this to happen.

EXAM ALERT

Be prepared to identify the role of a DHCP server for the Network+ exam.

NOTE

More on DHCP The DHCP protocol is discussed in more detail in Chapter 4.

Repeaters

As mentioned in Chapter 2, data signals weaken as they travel down a particular medium. This is known as *attenuation*. To increase the distance a signal can travel, you can use repeaters. Repeaters increase the cable's usable length and are commonly used with coaxial network configurations. Because coaxial networks have fallen out of favor, and because the functionality of repeaters has been built in to other devices, such as hubs and switches, repeaters are rarely used as an independent device.

NOTE

The function of the repeater is to regenerate data signals so that they can travel greater distances.

Specialized Network Devices

Any network is composed of many different pieces of hardware. Some, like firewalls and DHCP servers, are in most networks. Other devices are more specialized and are not found in every network environment. CompTIA lists the following as specialized networking devices:

- Multilayer and content switch
- IDS and IPS

- Load balancer
- Multifunction network devices
- DNS server
- Bandwidth shaper
- Proxy server
- CSU/DSU

The following sections take a quick look at what these devices are designed to do.

Multilayer and Content Switches

It used to be that networking devices and the functions they performed were pretty much separate. We had bridges, routers, hubs, and more, but they were separate devices. Over time, the functions of some individual network devices became integrated into a single device. This is true of multilayer switches.

A multilayer switch is one that can operate at both Layer 2 and Layer 3 of the OSI model, which means that the multilayer device can operate as both a switch and a router. Also called a Layer 3 switch, the multilayer switch is a high-performance device that actually supports the same routing protocols that routers do. It is a regular switch directing traffic within the LAN; in addition, it can forward packets between subnets.

NOTE

A multilayer switch operates as both a router and a switch.

A content switch is another specialized device. A content switch is not as common on today's networks, mostly due to cost. A content switch examines the network data it receives, decides where the content is intended to go, and forwards it. The content switch can identify the application that data is targeted for by associating it with a port. For example, if data is using the SMTP port, it could be forwarded to an SMTP server.

Content servers can help with load balancing because they can distribute requests across servers and target data to only the servers that need it, or distribute data between application servers. For example, if multiple mail servers are

used, the content switch can distribute requests between the servers, thereby sharing the load evenly. This is why the content switch is sometimes called a load-balancing switch.

NOTE

Content switching A content switch can distribute incoming data to specific application servers and help distribute the load.

Intrusion Detection and Prevention Systems

Administrators can use several methods to help secure the network. In addition to a firewall, an intrusion detection system (IDS) and intrusion prevention system (IPS) can be used. Both are designed to help identify unwanted network access and traffic; however, they work in slightly different ways.

An IDS is either a hardware- or software-based device that constantly monitors inbound and outbound network traffic. The IDS uses built-in parameters to flag and document any traffic it determines to be suspicious or potentially dangerous. But that is where the IDS stops. It does not actively try to manage the threat. Instead, it identifies the threat, and then the administrator must monitor the IDS to see what the problem might be. Although it doesn't try to fix the potential threat, the IDS can be configured to send an alert to the administrator, notifying him or her of a potential threat and security breach.

In operation, an IDS compares the inbound and outbound traffic to a large database of attack signatures. Attack signatures are known elements of a particular attack. Just as people can be identified through their fingerprints, certain attacks can be identified by their features. So in this way, the IDS can identify attacks that have already been identified elsewhere and can pinpoint them entering or leaving the network. An IDS is only as good as the database it uses to identify attacks. This is why it is important to keep the database up to date.

An IDS can be deployed as a host-based (resident to a single system) or network-based (watches all network traffic) device. In either case, an IDS cannot replace a firewall, because they have different functions. The firewall monitors secured access between two networks such as a business and the Internet and prevents unwanted traffic from entering the network. The IDS inspects an intrusion after it has taken place—that is, after it has passed the firewall. An IDS also watches for threats from within the network while the firewall operates on the network perimeter.

Whereas an IDS looks to flag potential threats, the IPS is a bit more proactive and tries to manage them on its own. Similar to an IDS, the IPS monitors both inbound and outbound traffic, looking for potential threats. But where an IDS flags and documents the threat, the IPS takes immediate action, trying to remove the threat. Whereas an IDS might flag a network intruder, the IPS tries to immediately shut out the intruder. The actions an IPS takes are established by the network administrator.

EXAM ALERT

For the Network+ exam, you will be expected to identify the function of both an IDS and IPS.

Load Balancer

Network servers are the workhorses of the network. They are relied on to hold and distribute data, maintain backups, secure network communications, and more. The load of servers is often a lot for a single server to maintain. This is where load balancing comes into play. Load balancing is a technique in which the workload is distributed between several servers. This feature can take networks to the next level; it increases network performance, reliability, and availability.

EXAM ALERT

Share the load **Remember for the exam that load balancing increases redundancy and therefore data availability. Also, load balancing increases performance by distributing the workload.**

A load balancer can be either a hardware device or software that is specially configured to balance the load.

Multifunction Network Devices

It used to be that each device on a network (firewall, router, repeater, hub, to name a few) had its own purpose. It wasn't long before the functions of these individual devices were combined into single units, creating multifunction network devices. Consider a high-speed cable modem used by home users or small companies to access the Internet. These are multifunction network devices that have combined functionality, including firewall, DHCP server, wireless access

point, switch, and router. Networks are full of multifunction devices, including switches, routers, servers, and more.

Multifunction devices offer some advantages over multiple independent devices or software packages. Suppose an organization maintains antivirus, firewall, content filtering, and IDS/IPS software on a single server or even several servers. This organization must pay for the software on each of the servers, the operating system, and the personnel to maintain the systems. All of this can be simply replaced with a single multifunction network device.

DNS Server

A Domain Name System (DNS) server performs a relatively basic, but vital, role for many organizations. The function of a DNS server is relatively simple in that it provides name resolution from hostnames to IP addresses. The measures to which the server goes to provide a successful resolution, however, are not so simple. As well as consulting its own databases for the requested information, a DNS server contacts other DNS servers as needed to get the necessary information. This process might involve a large number of queries.

As you may know, each device on a network requires a unique IP address so that it can provide services to clients. Rather than rely on flawed human memory to remember these addresses, DNS allows us to use easy-to-remember hostnames, such as comptia.org, to access these hosts. When we type www.comptia.org into a web browser, our configured DNS server takes the request and searches through a system of servers to find the correct TCP/IP address that relates to www.comptia.org. After the DNS server has ascertained the correct TCP/IP address, that address is returned to the client, which then contacts the IP address directly. To speed up subsequent requests for the same address, the DNS server adds the address to its cache. For a workstation to send requests to the DNS server, the TCP/IP address of the DNS server must be provided to the workstations. This can be done manually, or the address can be included in the information supplied by a DHCP (Dynamic Host Configuration Protocol) server.

Before DNS was used, resolution of hostnames to IP addresses was (and still is in some cases) performed through static text files called HOSTS files. These text files quickly became too large to manage easily and therefore were replaced by DNS.

The function of DNS remains largely hidden from most users, but our reliance on the system is amazingly high. In January 2001, a Microsoft employee made a configuration change to one of Microsoft's DNS servers. The change caused an error that rendered some Microsoft-hosted websites, including the popular

Hotmail system, inaccessible for a number of hours. The servers were up and running, but they simply could not be reached.

Most common operating systems provide the capability to act as a DNS server. Some implementations are more sophisticated than others, but the basic principle of hostname-to-TCP/IP address resolution remains the same.

The amount of computing power required by a DNS server is proportional to the number of DNS requests that it will handle. Within an organization, records might be configured for only a relatively small number of hosts, and there might be only a small number of client requests. In such an environment, it would be unlikely to have a server dedicated to DNS functions. In contrast, a DNS server for an Internet service provider would need to be powerful enough to accommodate perhaps millions of requests per hour.

EXAM ALERT

DNS server A DNS server answers clients' requests to translate hostnames into IP addresses.

Bandwidth Shaper

The demand for bandwidth on networks has never been higher. Internet and intranet applications demand a large amount of bandwidth. Administrators have to ensure that despite all these demands, adequate bandwidth is available for mission-critical applications while few resources are dedicated to spam or peer-to-peer downloads. To do this, you need to monitor network traffic to ensure that data is flowing as you need it to.

The term *bandwidth shaping* describes the mechanisms used to control bandwidth usage on the network. With this, administrators can control who uses bandwidth, for what purpose, and what time of day bandwidth can be used. Bandwidth shaping establishes priorities for data traveling to and from the Internet and within the network.

A bandwidth shaper, shown in Figure 3.4, essentially performs two key functions—monitoring and shaping. Monitoring includes identifying where bandwidth usage is high and the time of day. After that information is obtained, administrators can customize or shape bandwidth usage for the best needs of the network.

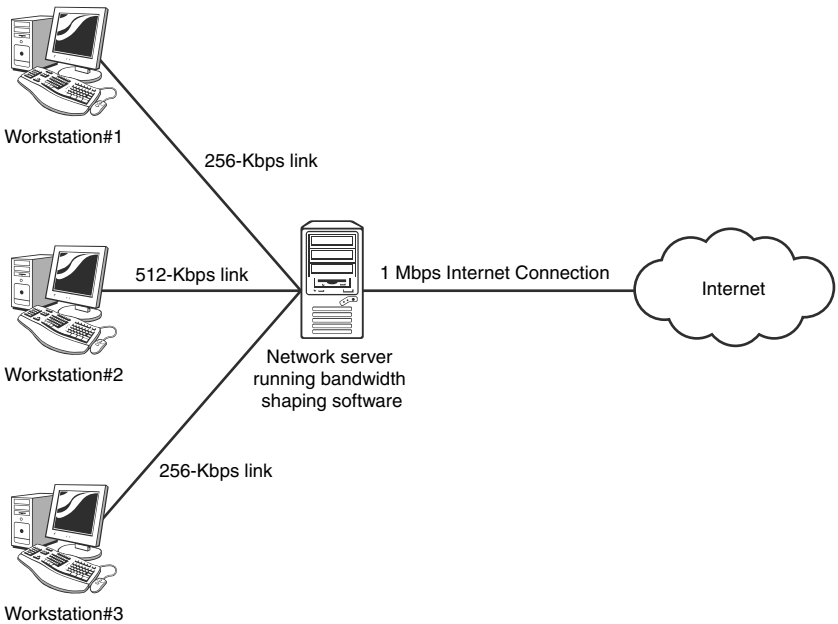

FIGURE 3.4 A bandwidth shaper.

Proxy Server

Proxy servers typically are part of a firewall system. In fact, they have become so integrated with firewalls that the distinction between the two can sometimes be lost.

However, proxy servers perform a unique role in the network environment—a role that is very separate from that of a firewall. For the purposes of this book, a proxy server is defined as a server that sits between a client computer and the Internet, looking at the web page requests the client sends. For example, if a client computer wants to access a web page, the request is sent to the proxy server rather than directly to the Internet. The proxy server first determines whether the request is intended for the Internet or for a web server locally. If the request is intended for the Internet, the proxy server sends the request *as if it originated the request*. When the Internet web server returns the information, the proxy server returns the information to the client. Although a delay might be induced by the extra step of going through the proxy server, the process is largely transparent to the client that originated the request. Because each request a client sends to the Internet is channeled through the proxy server, the proxy server can provide certain functionality over and above just forwarding requests.

One of the biggest of these extra features is that proxy servers can greatly improve network performance through a process called *caching*, shown in Figure 3.5. When a caching proxy server answers a request for a web page, the server makes a copy of all or part of that page in its cache. Then, when the page is requested again, the proxy server answers the request from the cache rather than going back to the Internet. For example, if a client on a network requests the web page www.comptia.org, the proxy server can cache the contents of that web page. When a second client computer on the network attempts to access the same site, that client can grab it from the proxy server cache, and accessing the Internet is unnecessary. This greatly increases the response time to the client and can significantly reduce the bandwidth needed to fulfill client requests.

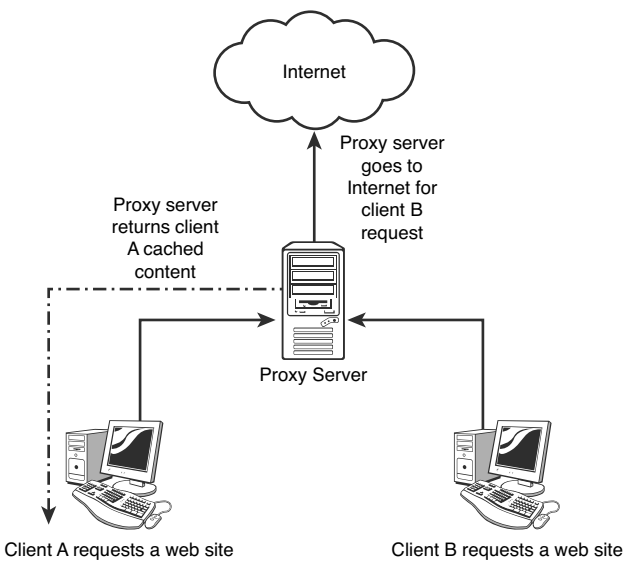

FIGURE 3.5 Proxy caching.

Nowadays, speed is everything, and the ability to quickly access information from the Internet is a crucial concern for some organizations. Proxy servers and their ability to cache web content accommodate this need for speed.

An example of this speed might be found in a classroom. If a teacher asks 30 students to access a specific Uniform Resource Locator (URL), without a proxy server, all 30 requests would be sent into cyberspace and subjected to delays or other issues that might arise. The classroom scene with a proxy server is quite different. Only one request of the 30 finds its way to the Internet; the other 29 are filled by the proxy server's cache. Web page retrieval can be almost instantaneous.

However, this caching has a potential drawback. When you log on to the Internet, you are getting the latest information, but this is not always so when information is retrieved from a cache. For some web pages, it is necessary to go directly to the Internet to ensure that the information is up-to-date. Some proxy servers can update and renew web pages, but they are always one step behind.

The second key feature of proxy servers is allowing network administrators to filter client requests. If a server administrator wants to block access to certain websites, a proxy server allows this control, making it easy to completely disallow access to some websites. This is okay, but what if it were necessary to block numerous websites? This is when maintaining proxy servers gets a bit more complicated.

Determining which websites users can or cannot access typically is done through something called an access control list (ACL). The ACL is a list of allowed or nonallowed websites; as you might imagine, compiling such a list can be a monumental task. Given that millions of websites exist, and new ones are created daily, how can you target and disallow access to the "questionable" ones? One approach is to reverse the situation and deny access to all pages except those that appear in an "allowed" list. This approach has high administrative overhead and can greatly limit the productive benefits available from Internet access.

Understandably, it is impossible to maintain a list that contains the locations of all sites that contain questionable content. In fairness, that is not what proxy servers were designed to do. However, by maintaining a list, proxy servers can better provide a greater level of control than an open system. Along the way, they can make the retrieval of web pages far more efficient.

CSUs/DSUs

A Channel Service Unit/Data Service Unit (CSU/DSU) acts as a translator between the LAN data format and the WAN data format. Such a conversion is necessary because the technologies used on WAN links are different from those used on LANs. Some consider a CSU/DSU a type of digital modem. But unlike a normal modem, which changes the signal from digital to analog, a CSU/DSU changes the signal from one digital format to another.

A CSU/DSU has physical connections for the LAN equipment, normally via a serial interface, and another connection for a WAN. Traditionally, the CSU/DSU has been in a box separate from other networking equipment. However, the increasing use of WAN links means that some router manufacturers are now including CSU/DSU functionality in routers or are providing the expansion capability to do so.

Network Devices Summary

The information in this chapter is important for the Network+ exam. To summarize the coverage of network devices, Table 3.3 lists some of the key points about each device. You should learn this information well.

Table 3.3 Network Devices Summary

Device	Description	Key Points
Hub	Connects devices on an Ethernet twisted-pair network.	A hub does not perform any tasks besides signal regeneration.
Switch	Connects devices on a twisted-pair network.	A switch forwards data to its destination by using the MAC address embedded in each packet.
Repeater	Regenerates data signals.	The function a repeater provides typically is built in to other devices such as switches.
Bridge	Connects LANs to reduce overall network traffic.	A bridge allows data to pass through it or prevents data from passing through it by reading the MAC address.
Router	Connects networks.	A router uses the software-configured network address to make forwarding decisions.
Gateway	Translates from one data format into another.	Gateways can be hardware- or software-based. Any device that translates data formats is called a gateway.
CSU/DSU	Translates digital signals used on a LAN into those used on a WAN.	CSU/DSU functionality is sometimes incorporated into other devices, such as a router with a WAN connection.

Table 3.3 Network Devices Summary *Continued*

Device	Description	Key Points
Modem	Provides serial communication capabilities across phone lines.	Modems modulate the digital signal into analog at the sending end and perform the reverse function at the receiving end.
Network card	Enables systems to connect to the network.	Network interfaces can be add-in expansion cards, PCMCIA cards, or built-in interfaces.
Media converter	Interconnects older technology with new.	A media converter is a hardware device that connects newer Gigabit Ethernet technologies with older 100BaseT networks or older copper standards with fiber.
Firewall	Provides controlled data access between networks.	Firewalls can be hardware- or software-based. They are an essential part of a network's security strategy.
DHCP server	Automatically distributes IP information.	DHCP assigns all IP information, including IP address, subnet mask, DNS, gateway, and more.
Multilayer switch	Functions as a switch or router.	Operates on Layers 2 and 3 of the OSI model as a switch and can perform router functionality.
Content switch	Forwards data by application.	Content switches can identify and forward data by its port and application.
Load balancer	Distributes network load.	Load balancing increases redundancy by distributing the load to multiple servers.

Table 3.3 Network Devices Summary *Continued*

Device	Description	Key Points
Multifunction devices	Combines network services.	These are hardware devices that combine multiple network services into a single device, reducing cost and easing administrative difficulty.
DNS server	Provides name resolution from hostnames to IP addresses.	A DNS server answers clients' requests to translate hostnames into IP addresses.
Bandwidth shaper	Manages network bandwidth.	The bandwidth shaper monitors and controls bandwidth usage.
Proxy server	Manages client Internet requests.	Serves two key network functions: increases network performance by caching, and filters outgoing client requests.

EXAM ALERT

For the Network+ exam, you will be expected to know the function of the devices mentioned in this chapter. Review Table 3.3. Make sure you understand each device and how and why it is used on the network.

Advanced Features of a Switch

As mentioned previously, switches are more complex than hubs. In fact, today's switches do far more than switches from just a few years ago. This section looks at a few of the more advanced features that switches perform.

Power over Ethernet (PoE)

The purpose of Power over Ethernet (PoE) is pretty much described in its name. Essentially, PoE is a technology that allows electrical power to be transmitted over twisted-pair Ethernet cable. The power is transferred, along with data, to provide power to remote devices. These devices may include remote switches, wireless access points, voice over IP (VoIP) equipment, and more.

One of the key advantages of PoE is the centralized management of power. For instance, without PoE, all remote devices need to be powered independently. In the case of a power outage, each of these devices requires an uninterruptible power supply (UPS) to continue operating. A UPS is a battery pack that allows devices to operate for a period of time. With PoE supplying power, a UPS is required only in the main facility. In addition, centralized power management allows administrators to power up or down remote equipment.

NOTE

VLAN and spanning tree VLAN and spanning tree were outlined in the CompTIA objectives for this chapter. Spanning tree is covered next. VLANs are discussed in Chapter 1.

Spanning Tree

An Ethernet network can have only a single active path between devices on a network. When multiple active paths are available, switching loops can occur. Switching loops are simply the result of having more than one path between two switches in a network. Spanning Tree Protocol (STP) is designed to prevent these loops from occurring.

STP is used with network bridges and switches. With the help of Spanning Tree Algorithm (STA), STP avoids or eliminates loops on a Layer 2 network.

NOTE

Layer 2? As a heads-up, when we talk about STP, we are talking about Layer 2 of the OSI model. Both bridges and switches work at Layer 2. Routers work at Layer 3. Chapter 4 covers the OSI model and how it relates to network hardware.

STA enables a bridge or switch to dynamically work around loops in a network's topology. Both STA and STP were developed to prevent loops in the network and provide a way to route around any failed network bridge or ports. If the network topology changes, or if a switch port or bridge fails, STA creates a new spanning tree, notifies the other bridges of the problem, and routes around it. STP is the protocol, and STA is the algorithm STP uses to correct loops.

If a particular port has a problem, STP can perform a number of actions, including blocking the port, disabling the port, or forwarding data destined for that port to another port. It does this to ensure that no redundant links or paths are found in the spanning tree and that only a single active path exists between any two network nodes.

STP uses bridge protocol data units (BPDUs) to identify the status of ports and bridges across the network. BPDUs are simple data messages that are exchanged between switches. BPDUs contain information on ports and provide the status of those ports to other switches. If a BPDU message finds a loop in the network, it is managed by shutting down a particular port or bridge interface.

Redundant paths and potential loops can be avoided within ports in several ways:

- **Blocking**: A blocked port accepts BPDU messages but does not forward them.
- **Disabled**: The port is offline and does not accept BPDU messages.
- **Forwarding**: The port is part of the active spanning tree topology and forwards BPDU messages to other switches.
- **Learning**: In a learning state, the port is not part of the active spanning tree topology but can take over if another port fails. Learning ports receive BPDUs and identify changes to the topology when made.
- **Listening**: A listening port receives BPDU messages and monitors for changes to the network topology.

Most of the time, ports are in either a forwarding or blocked state. When a disruption to the topology occurs or a bridge or switch fails for some reason, listening and learning states are used.

EXAM ALERT

STP actively monitors the network, searching for redundant links. When it finds some, it shuts them down to prevent switching loops. STP uses STA to create a topology database to find and then remove the redundant links. With STP operating from the switch, data is forwarded on approved paths, which limits the potential for loops.

Trunking

In computer networking, the term *trunking* refers to the use of multiple network cables or ports in parallel to increase the link speed beyond the limits of any one cable or port. Sound confusing? If you have network experience, you might have heard the term *link aggregation*, which is essentially the same thing. It is just using multiple cables to increase the throughput. The higher-capacity trunking link is used to connect switches to form larger networks.

Port Mirroring

You need some way to monitor network traffic and monitor how well a switch is working. This is the function of port mirroring. To use port mirroring, administrators configure a copy of all inbound and outbound traffic to go to a certain port. A protocol analyzer is used to examine the data sent to the port and therefore does not interrupt the flow of regular traffic.

EXAM ALERT

Port mirroring Remember for the exam that port mirroring allows administrators to monitor the traffic outbound and inbound to the switch.

Port Authentication

Port authentication is pretty much what it sounds like—authenticating users on a port-by-port basis. One standard that specifies port authentication is the 802.1X standard, often associated with wireless security. Systems that attempt to connect to a LAN port must be authenticated. Those who are authenticated can access the LAN; those who are not authenticated get no further. Chapter 9 provides more information on the 802.1X standard and port authentication.

Review and Test Yourself

The following sections provide you with the opportunity to review what you've learned in this chapter and to test yourself.

The Facts

- Both hubs and switches are used in Ethernet networks. Token ring networks, which are few and far between, use special devices called multistation access units (MSAUs or MAUs) to create the network.
- The function of a hub is to take data from one of the connected devices and forward it to all the other ports on the hub.
- Hubs can be either active or passive. Hubs are considered active when they regenerate a signal before forwarding it to all the ports on the device. To do this, the hub needs a power supply.
- Rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected.

- Switches make forwarding decisions based on the Media Access Control (MAC) addresses of the devices connected to them to determine the correct port.
- In cut-through switching, the switch begins to forward the packet as soon as it is received.
- In a store-and-forward configuration, the switch waits to receive the entire packet before beginning to forward it.
- FragmentFree switching works by reading only the part of the packet that enables it to identify fragments of a transmission.
- Hubs and switches have two types of ports: Medium-Dependent Interface (MDI) and Medium-Dependent Interface Crossed (MDI-X).
- A straight-through cable is used to connect systems to the switch or hub using the MDI-X ports.
- In a crossover cable, wires 1 and 3 and wires 2 and 6 are crossed within twisted-pair cable.
- Both hubs and switches come in managed and unmanaged versions. A managed device has an interface through which it can be configured to perform certain special functions.
- Bridges are used to divide networks and thus reduce the amount of traffic on each network.
- Unlike bridges and switches, which use the hardware-configured MAC address to determine the data's destination, routers use the software-configured network address to make decisions.
- With distance-vector routing protocols, each router communicates all the routes it knows about to all other routers to which it is directly attached.
- Link-state protocols communicate with all other devices on the network to build complete maps of the network. They generate less network traffic than distance vector routing protocols but require more powerful network hardware.
- The term *gateway* is applied to any device, system, or software application that can translate data from one format into another.
- A CSU/DSU acts as a translator between the LAN and WAN data formats.

- Wireless network devices gain access to the network via wireless access points.
- Wireless access points provide additional functionality such as DHCP, router, firewall, and hub/switch.
- Modems translate digital signals from a computer into analog signals that can travel across conventional phone lines.
- Media converters are used to convert between one media type and another.

Key Terms

- Hub
- Bridge
- Gateway
- Network interface card
- Switch
- Router
- CSU/DSU
- Wireless access point (AP)
- Modem
- MAC address
- Distance vector
- Link state
- Dynamic routing
- Static routing
- OSPF
- RIP
- Convergence
- Bridging loop
- Transceiver
- Media converter