3

Networking Devices

Objectives

1.6 Identify the purposes, features, and functions of the following network components:

- Hubs
- Switches
- Bridges
- Routers
- Gateways
- CSU/DSU (Channel Service Unit/Data Service Unit)
- NICs (Network Interface Card)
- ISDN (Integrated Services Digital Network) adapters
- WAPs (Wireless Access Point)
- Modems
- Transceivers (media converters)
- Firewalls

2.1 Identify a MAC (Media Access Control) address and its parts

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/Digital Service Unit (CSU/DSU) and gateways
- Describe the purpose and function of network cards
- Describe how to identify a MAC address
- Understand the function of a transceiver
- 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 requirements for a Network+ candidate.

This chapter introduces commonly used networking devices, and, although it is true that you are not likely to encounter all of 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 can also be joined together 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 of the connected devices. A hub does not perform any processing on the data that 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 referred to as *workgroup hubs*. Others can accommodate larger numbers of devices (normally up to 32). These are referred to as *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. 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 however, it is commonly referred to as an MAU. Both are acceptable acronyms.

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 that they receive. Whereas a hub forwards the data it receives to all of the ports on the device, a switch forwards it only to 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.

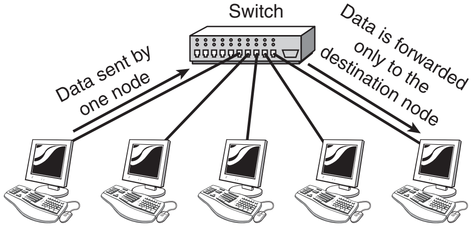

Figure 3.1 How a switch works.

By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways. First, by creating a direct path between two devices and controlling their communication, it can greatly reduce the number of collisions on the network. 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 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 creates the possibility of errors being propagated through the network, as there is no error checking.
- **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 also 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 serves to uncross the internal crossing. You can see diagrams of the cable pinouts for both a straight-through and crossover cable in Figures 3.2 and 3.3, respectively.

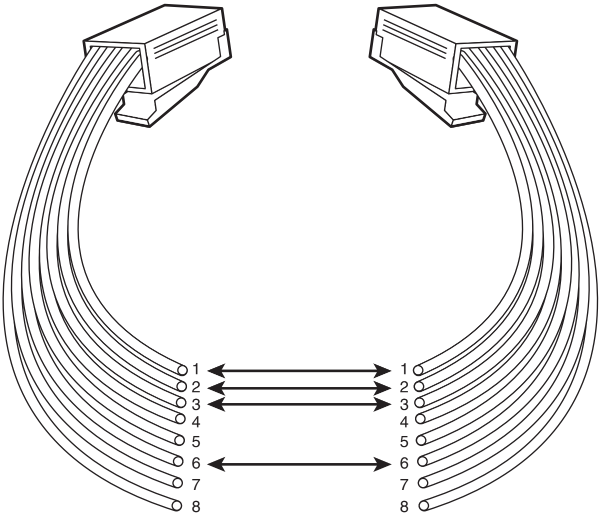

Figure 3.2 The pinouts for a straight-through cable.

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

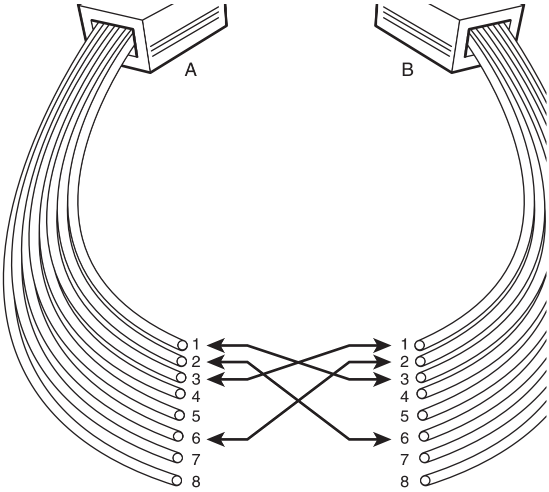

Figure 3.3 The pinouts for a crossover cable.

Bridges

Bridges are used to divide larger networks into smaller sections. They do 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 3.4 shows how a bridge can be 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, 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.

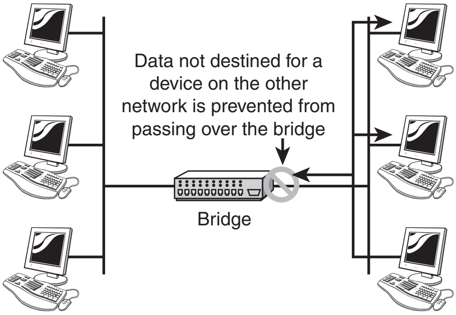
Data not destined for a device on the other network is prevented from passing over the bridge
Bridge

Figure 3.4 How a bridge is used to segregate networks.

Bridge Placement and Bridging Loops

There are two issues that you must consider when using bridges. The first is the bridge placement, and the other is the elimination of bridging loops:

- **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 that the other 20% should be destined for devices on the other side of the bridge.
- **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 within the packet.
- **Translational bridge**—Used to convert one networking data format to another; for example, 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 referred to as multiport bridges because of the way they operate.

Routers

In a common configuration, routers are used to create larger networks by joining two network segments. Such as a SOHO router used to connect a user to the Internet. 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 will normally create, add, or divide on the Network Layer as they are normally IP-based devices.

A router derives its name from the fact that it can route data it receives from one network onto another. When a router receives a packet of data, it reads the header of the packet to determine the destination address. Once it has determined the address, it looks in its routing table to determine whether it knows how to reach the destination and, 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 3.5 shows, in basic terms, how a router works.

As you can see from this example, routing tables play a very important role in the routing process. They are the means by which the router makes its decisions. For this reason, a routing table needs to be two things. It must be up-to-date, and it must be complete. There are two ways that the router can get the information for the routing table—through static routing or dynamic routing.

Static Routing

In environments that use *static routing*, routes and route information are entered into the routing tables manually. Not only can this be a time-consuming task, but also errors are more common. Additionally, when there is a change in the layout, or topology, of the network, statically configured routers must be manually updated with the changes. Again, this is a time-consuming and potentially error-laden task. For these reasons, static routing is suited to only the smallest environments with perhaps just one or two routers. A far more practical solution, particularly in larger environments, is to use dynamic routing.

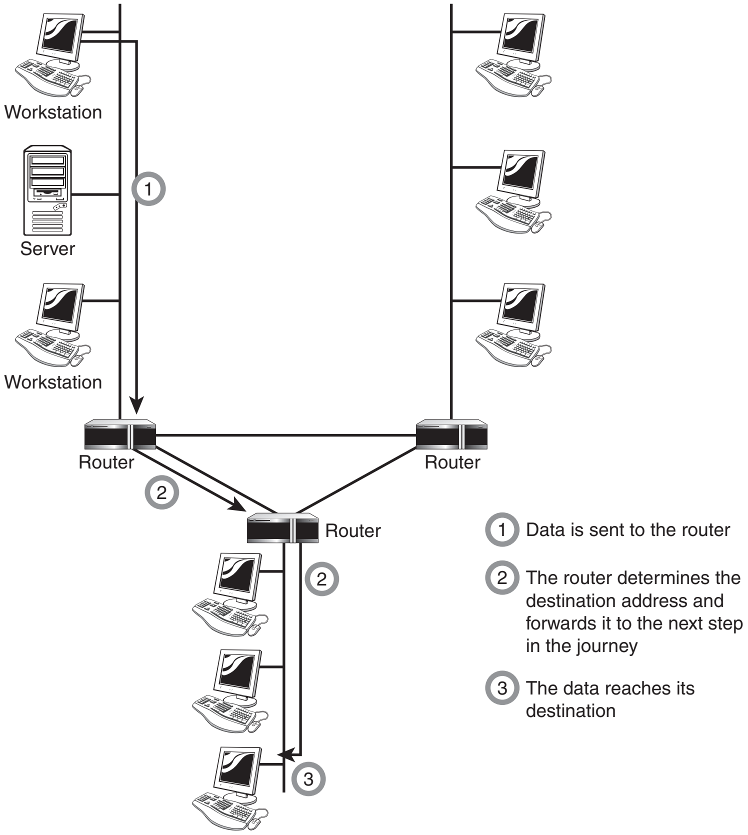
Workstation
Server
Workstation
1
Router
Router
2
Router
2
3
1 Data is sent to the router
2 The router determines the destination address and forwards it to the next step in the journey
3 The data reaches its destination

Figure 3.5 How a router works.

Dynamic Routing

In a *dynamic routing* environment, routers use special routing protocols to communicate. The purpose of these protocols is simple; they enable routers to pass on information about themselves to other routers so that other routers can build routing tables. There are two types of routing protocols used—the older distance vector protocols and the newer link state protocols.

Distance Vector Routing

The two most commonly used distance vector routing protocols are both called Routing Information Protocol (RIP). One version is used on networks running TCP/IP. The other, sometimes referred to as IPX RIP, is designed for use on networks running the IPX/SPX protocol.

RIP works on the basis of *hop counts*. A hop is defined as one step on the journey to the data's destination. Each router that the data has to cross to reach its destination constitutes a hop. The maximum number of hops that RIP can accommodate is 15. That is to say that in a network that uses RIP, all routers must be within 15 hops of each other to communicate. Any hop count that is in excess of 15 is considered unreachable.

Distance vector routing protocols operate by having each router send updates about all the other routers it knows about to the routers directly connected to it. These updates are used by the routers to compile their routing tables. The updates are sent out automatically every 30 or 60 seconds. The actual interval depends on the routing protocol being used. Apart from the periodic updates, routers can also be configured to send a *triggered update* if a change in the network topology is detected. The process by which routers learn of a change in the network topology is known as *convergence*.

Although distance vector protocols are capable of maintaining routing tables, they have three problems. The first is that the periodic update system can make the update process very slow. The second problem is that the periodic updates can create large amounts of network traffic—much of the time unnecessarily as the topology of the network should rarely change. The last, and perhaps more significant, problem is that because the routers only know about the next hop in the journey, incorrect information can be propagated between routers, creating routing loops.

Two strategies are used to combat this last problem. One, *split horizon*, works by preventing the router from advertising a route back to the other router from which it was learned. The other, *poison reverse* (also called split horizon with poison reverse), dictates that the route *is* advertised back on the interface from which it was learned, but that it has a metric of 16. Recall that a metric of 16 is considered an unreachable destination.

Link State Routing

Link state routing works quite differently from distance vector-based routing. Rather than each router telling each other connected router about the routes it is aware of, routers in a link state environment send out special packets, called *link state advertisements (LSA)*, which contain information only about that router. These LSAs are forwarded to all the routers on the network, which enables them to build a map of the entire network. The advertisements are sent when the router is first brought onto the network and when a change in the topology is detected.

Of the two (distance vector and link state), distance vector routing is better suited to small networks and link state routing to larger ones. Link state protocols do not suffer from the constant updates and limited hop count, and they are also quicker to correct themselves (to converge) when the network topology changes.

On TCP/IP networks, the most commonly used link state routing protocol is the Open Shortest Path First (OSPF). On IPX networks, the NetWare Link State Protocol (NLSP) is used. Table 3.1 summarizes the distance vector and link state protocols used with each network protocol.

EXAM ALERT

It is necessary to know which distance vector and link state routing protocols are associated with which network protocols.

Table 3.1 Routing Protocols

Network Protocol	Distance Vector	Link State
TCP/IP	RIP	OSPF
IPX/SPX	RIP*	NLSP

IPX RIP

Sometimes, to distinguish between the versions of RIP for IP and IPX, the version for IPX is referred to as IPX RIP.

Gateways

Any device that translates one data format to another is called a *gateway*. Some examples of gateways include a router that translates data from one network protocol to 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.

Gateways and Default Gateways

Don't confuse a gateway with the term *default gateway*, which is discussed in Chapter 6, "WAN Technologies, Remote Access, and Security Protocols." The term default gateway refers to a router to which all network transmissions not destined for the local network are sent.

CSU/DSU

A Channel Service Unit/Digital Service Unit (CSU/DSU), sometimes called Data Service Unit, is a device that converts the digital signal format used on LANs into one used on WANs. Such translation is necessary because the networking technologies used on WANs are different from those used on LANs.

The CSU/DSU sits between the LAN and the access point provided by the telecommunications company. Many router manufacturers are now incorporating CSU/DSU functionality into their products.

Network Cards

Network cards, also called Network Interface Cards, are devices that enable computers 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 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.

Even more than the assumption you are using twisted-pair cabling is that the networking system being used is Ethernet. If you require a card for another networking system such as Token Ring, this must be specified when you order.

When working on a Token Ring network, you have to ensure that all network cards are set to transmit at the same speeds. NICs on an Ethernet network can operate at different speeds.

To install or configure a network interface, you will need drivers of the device, and might need to configure it, although many devices are now plug and play. Most network cards are now software configured. Many of these software configuration utilities also include testing capabilities. The drivers and software configuration utilities supplied with the cards are often not the latest available, so it is best practice to log on to the Internet and download the latest drivers and associated software.

ISDN Adapters

Integrated Services Digital Network (ISDN) is a remote access and WAN technology that can be used in place of a Plain Old Telephone Service (POTS) dial-up link if it is available. The availability of ISDN depends on whether your local telecommunications service provider offers the service, the quality of the line to your premises, and your proximity to the provider's location. ISDN offers greater speeds than a modem and can also pick up and drop the line considerably faster.

If ISDN is available and you do elect to use it, a special device called an *ISDN terminal adapter* is needed to connect to the line. ISDN terminal adapters can be add-in expansion cards, external devices that connect to the serial port of the system, or specialized interfaces built in to routers or other networking equipment. The ISDN terminal adapter is necessary because, although it uses digital signals, the signals are formatted differently from those used on a LAN. In addition, ISDN can create multiple communication channels on a single line. Today, ISDN is not widely deployed and has been replaced by faster and often cheaper technologies.

Wireless Access Points

Wireless access points (APs) are a transmitter and receiver (transceiver) device used to create a wireless LAN (WLAN). APs are typically 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 allowing 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 transmissions range—the distance a client can be from a AP and still get a useable signal. The actual distance depends on the wireless standard being used and the obstructions and environmental conditions between the client and the AP.

> NOTE
>
> A WAP 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 size of the network. Systems can be added and removed from the network with no affect on other systems on the network. Also, many APs provide firewall capabilities and DHCP service. When they are hooked up, they will provide client systems with a private IP address and then prevent Internet traffic from accessing client systems. So in effect, the AP is a switch, a DHCP Server, router, and a 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 the range that 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.

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 the computer can understand. Modems can be used as a means to connect to an ISP or as a mechanism for dialing up to a LAN.

Modems can be internal add-in expansion cards, external devices that connect to the serial or USB port of a system, 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 those (typically COM2). Table 3.2 shows the resources associated with serial (COM) port assignments.

Table 3.2 Common Serial (COM) Port Resource Assignments

Port ID	IRQ	I/O Address	Associated Serial I/F 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, as 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. Once 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 the serial communication of a computer, and 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. The UART chip installed in the system can normally be determined by looking at the documentation that comes with the system. Table 3.3 shows the maximum speed of the commonly used UART chip types.

Table 3.3 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.

ALERT

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.

Transceivers (Media Converters)

The term transceiver does describe a separate network device, but it can also be technology built and embedded in devices such as network cards and modems. In a network environment, a transceiver gets its name from being both a transmitter and a receiver of signals—thus the name transceivers. Technically, on a LAN, the transceiver is responsible for placing signals onto the network media and also detecting incoming signals traveling through the same wire. Given the description of the function of a transceiver, it makes sense that that technology would be found with network cards.

Although transceivers are found in network cards, they can be external devices as well. As far as networking is concerned, transceivers can ship as a module or chip type. Chip transceivers are small and are inserted into a system board or wired directly on a circuit board. Module transceivers are external to the network and are installed and function similarly to other computer peripherals, or they can function as standalone devices.

There are many types of transceivers—RF transceivers, fiber optic transceivers, Ethernet transceivers, wireless (WAP) transceivers, and more. Though each of these media types are different, the function of the transceiver remains the same. Each type of the transceiver used has different characteristics, such as the number of ports available to connect to the network and whether full-duplex communication is supported.

Listed with transceivers in the CompTIA objectives are media converters. Media converters are a technology that allows administrators to interconnect different media types—for example, twisted pair, fiber, and Thin or thick coax—within an existing network. Using a media converter, it is possible to connect newer 100Mbps, Gigabit Ethernet, or ATM equipment to existing networks such as 10BASE-T or 100BASE-T. They can also be used in pairs to insert a fiber segment into copper networks to increase cabling distances and enhance immunity to electromagnetic interference (EMI).

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 are typically placed at entry/exit points of a network—for example, placing a firewall between an internal network and the Internet. Once there, it can control access in 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—for example, placing a firewall between the Accounts and the Sales departments.

As mentioned, firewalls can be implemented through software or through a dedicated hardware device. Organizations implement software firewalls through network operating systems (NOS) such as Linux/UNIX, Windows servers, and Mac OS servers. The firewall is configured on the server to allow or permit certain types of network traffic. In small offices and for regular home use, a firewall is commonly installed on the local system and 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 and protect all systems behind the firewall from outside sources. Hardware firewalls are readily available and often combined with other devices today. For example, many broadband routers and wireless access points have firewall functionality built in. In such case, the router or WAP might have a number of ports available to plug systems in to.

NOTE

Firewalls are discussed in greater detail in Chapter 8, “Configuring Network Security.”

Table 3.4 provides a summary of the networking devices identified in this chapter.

Table 3.4 Network Devices Summary

Device	Function/Purpose	Key Points
Hub	Connects devices on a 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.
Bridge	Divides networks to reduce overall network traffic.	A bridge allows or prevents data from passing through it by reading the MAC address.
Router	Connects networks together.	A router uses the software-configured network address to make forwarding decisions.
Gateway	Translates from one data format to another.	Gateways can be hardware or software based. Any device that translates data formats is called agateway.
CSU/DSU	Translates digital signals used on a LAN to those used on a WAN.	CSU/DSU functionality is sometimes incorporated into other devices, such as a router with a WAN connection.
Network card	Enables systems to connect to the network.	Network interfaces can be add-in expansion cards, PCMCIA cards, or built-in interfaces.
ISDN terminal adapter	Connects devices to ISDN lines.	ISDN is a digital WAN technology often used in place of slower modem links. ISDN terminal adapters are required to reformat the data format for transmission on ISDN links.
WAP	Provides network capabilities to wireless network devices.	A WAP is often used to connect to a wired network, thereby acting as a link between wired and wireless portions of the network.

(continued)

Table 3.4 Network Devices Summary *(continued)*

Device	Function/Purpose	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.
Transceiver	Coverts one media type to another, such as UTP to fiber.	A device that functions as a transmitter and a receiver of signals such as analog or digital.
Firewall	Provides controlled data access between networks.	Firewalls can be hardware or software based and are an essential part of a networks security strategy.

MAC Addresses

A *MAC address* is a unique 6-byte address that is burned into each network interface or more specifically, directly into the PROM chip on the NIC. The number must be unique, as the MAC address is the basis by which almost all network communication takes place. No matter which networking protocol is being used, the MAC address is still the means by which the network interface is identified on the network. Notice that I say network interface. That's very important, as a system that has more than one network card in it will have more than one MAC address.

MAC addresses are expressed in six hexadecimal values. In some instances, the six values are separated by colons (:); in others, hyphens (-) are used; and in still others, a space is simply inserted between the values. In any case, because the six values are hexadecimal, they can only be numbers 0–9 and the letters A–F. So, a valid MAC address might be `00-D0-56-F2-B5-12` or `00-26-DD-14-C4-EE`. There is a way of finding out whether a MAC address exists through the IEEE, which is responsible for managing MAC address assignment. The IEEE has a system in place that lets you identify the manufacturer of the network interface by looking at the MAC address.

For example, in the MAC address `00-80-C8-E3-4C-BD`, the `00-80-C8` portion identifies the manufacturer and the `E3-4C-BD` portion is assigned by the manufacturer to make the address unique. The IEEE is the body that assigns manufacturers their IDs, called Organizationally Unique Identifiers, and the manufacturer then assigns the second half, called the Universal LAN MAC address. From the IEEE's perspective, leaving the actual assignment of addresses to the manufacturers significantly reduces the administrative overhead for the IEEE.

As discussed, MAC addresses are expressed in hexadecimal format. For that reason, they can only use the numbers 0–9 and the letters A–F. There are only six bytes, so a MAC address should be six groups of two characters. Any other number of characters or any answer that contains a letter other than those described can be immediately discounted as an answer.

The method by which you can discover the MAC address of the network interfaces in your equipment depends on which operating system is being used. Table 3.5 shows you how to obtain the MAC address on some of the more common platforms.

Be prepared to identify the commands used to view a MAC address as shown in Table 3.5. You might be asked to identify these commands on the Network+ exam.

Table 3.5 Commands to Obtain MAC Addresses

Platform	Method
Windows 95/98/Me	Run the **winipcfg** utility.
Windows NT/2000	Run **ipconfig /all** from a command prompt.
Linux/Some UNIX	Run the **ifconfig -a** command.
Novell NetWare	Run the **config** command.
Cisco Router	Run the **sh int <*interface name*>** command.

As you work with network interfaces more, you might start to become familiar with which ID is associated with which manufacturer. Although this is a skill that might astound your friends and impress your colleagues, it won't help you with the Network+ exam. Just knowing what does, and doesn't, represent a valid MAC address will be sufficient on the exam.

Review and Test Yourself

The following sections provide you with the opportunity to review what you 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) 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.
- Most hubs are considered *active* because they regenerate a signal before forwarding it to all the ports on the device. In order 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.
- 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 up 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 destination of the data, 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.
- RIP is a distance routing protocol for both TCP and IPX.
- 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.
- Open Shortest Path First (OSPF) and NetWare Link State Protocol (NLSP) are the most commonly used link state routing protocols used on IP and IPX networks respectively.
- The term *gateway* is applied to any device, system, or software application that can perform the function of translating data from one format to another.
- A CSU/DSU acts as a translator between the LAN and the 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.
- Transceivers are devices on the network that both transmit and receive data signals.
- Media converters are used to convert between one media type and another.

Key Terms

- Hub
- Bridge
- Gateway
- Network Interface Cards
- ISDN adapters
- Switch
- Router
- CSU/DSU
- System area network cards
- Wireless Access Points (WAPs)
- Modems
- MAC addresses
- Distance vector
- Link state
- Dynamic routing
- Static routing
- NLSP
- OSPF
- RIP
- Convergence
- Bridging loops
- Transceivers
- Media converters

Exam Prep Questions

1. Users are complaining that the performance of the network is not satisfactory. It takes a long time to pull files from the server, and, under heavy loads, workstations can become disconnected from the server. The network is heavily used, and a new video conferencing application is about to be installed. The network is a 100BaseT system created with Ethernet hubs. Which of the following devices are you most likely to install to alleviate the performance problems?

❑ A. Switch

❑ B. Router

❑ C. Bridge

❑ D. Gateway

2. Which of the following devices forwards data packets to all connected ports?

❑ A. Router

❑ B. Switch

❑ C. Bridge

❑ D. Hub

3. Of the following routing methods, which is likely to take the most amount of administration time in the long term?

❑ A. Static

❑ B. Link state

❑ C. Distance vector

❑ D. Dynamic

4. Your manager asks you to look into some upgrades for your network. The current network is a 10Base2 system, and you have been experiencing numerous hard-to-track-down cable problems. As a result, you have decided to upgrade to a 10BaseT system. On the networking vendor's price list are both active and passive hubs. The passive hubs are considerably cheaper than the active ones, and you are tempted to opt for them so that you come in under budget. A colleague advises you against the purchase of passive hubs. What is the primary difference between an active and a passive hub?

❑ A. Passive hubs do not offer any management capabilities.

❑ B. Passive hubs cannot be used in full-duplex mode.

❑ C. Passive hubs do not regenerate the data signal.

❑ D. Passive hubs forward data to all ports on the hub, not just the one for which they are intended.

5. Which of the following statements best describes a gateway?
   - ❑ A. It is a device that enables data to be routed from one network to another.
   - ❑ B. It is a term used to refer to any device that resides at the entrance of a network.
   - ❑ C. It is a device, system, or application that translates data from one format to another.
   - ❑ D. It is a network device that can forward or block data based on the MAC address embedded within the packet.

6. You have a thin coaxial-based Ethernet network and are experiencing performance problems on the network. By using a network performance-monitoring tool, you determine that there are a large number of collisions on the network. In an effort to reduce the collisions, you decide to install a network bridge. What kind of bridge are you most likely to implement?
   - ❑ A. Collision bridge
   - ❑ B. Transparent bridge
   - ❑ C. Visible bridge
   - ❑ D. Translational bridge

7. Which of the following represents a valid MAC address?
   - ❑ A. **00-D0-56-F2-B5-12**
   - ❑ B. **00-63-T6-4H-7U-78**
   - ❑ C. **00-62-DE-6F-D2**
   - ❑ D. **000-622-DE5-75E-EA6**

8. Which of the following devices passes data based on the MAC address?
   - ❑ A. Hub
   - ❑ B. Switch
   - ❑ C. MSAU
   - ❑ D. Router

9. What is the speed of the 16550 UART chip?
   - ❑ A. 921,600
   - ❑ B. 430,800
   - ❑ C. 115,200
   - ❑ D. 9,600

10. Which of the following devices would you find only on a Token Ring network?
    - ❑ A. Hub
    - ❑ B. Switch
    - ❑ C. MSAU
    - ❑ D. Router

Answers to Exam Prep Questions

1. The correct answer is A. Replacing Ethernet hubs with switches can yield significant performance improvements. Of the devices listed, they are also the only one that can be substituted for hubs. Answer B, router, is incorrect as a router is used to separate networks, not as a connectivity point for workstations. A bridge could be used to segregate the network and so improve performance, but a switch is a more obvious choice in this example. Therefore, answer C is incorrect. Answer D, gateway, is incorrect. A gateway is a device, system, or application that translates data from one format to another.

2. The correct answer is D. Hubs are inefficient devices that send data packets to all connected devices. Many of today's networks are upgrading to switches that pass data packets to the specific destination device. This method significantly increases network performance.

3. The correct answer is A. Static routing will take more time to administer in the long term, as any changes to the network routing table must be entered manually. Answers B and C are incorrect. Distance vector and link state are both dynamic routing methods. Answer D is also incorrect. Dynamic routing might take more time to configure initially; but in the long term, it will require less administration time. It can adapt to changes in the network layout automatically.

4. The correct answer is C. An active hub regenerates the data signal before forwarding, it a passive hub does not. Answer A is incorrect. The management capabilities of a hub have nothing to do with the active/passive aspect of the device. Answer B is incorrect. Hubs are not capable of operating in full-duplex mode. Only network switches are capable of performing this function in this context. Answer D describes the function of a switch, not a hub.

5. The correct answer is C. A gateway can be a device, system, or application that translates data from one format to another. Answers B and D are more likely to describe a router than a gateway. Answer D describes a bridge. A bridge is a device that is used to segregate a network. It makes forwarding or blocking decisions based on the MAC address embedded within the packet.

6. The correct answer is B. A transparent bridge can be used to segment a network, which reduces the amount of collisions and the overall network traffic. It is called transparent because the other devices on the network do not need to be aware of the device and will, in fact, operate as if it wasn't there. Answer D is incorrect as a translational bridge is

used in environments where it is necessary to translate from one data format to another. Such a conversion is not necessary in this scenario. Answers A and C are invalid. There is no such thing as a collision bridge or a visible bridge.

7. The correct answer is A. A MAC address is a 6-byte address that is expressed in hexadecimal format. Answer B contains the letters T and U, which are not valid. Hexadecimal format uses only numbers and the letters A through F. For this reason, answer B is incorrect. Answer C is only five bytes, so it is incorrect. Answer D is incorrect because a byte in hexadecimal is expressed in two characters and the answer uses three.

8. The correct answer is B. When determining the destination for a data packet, the switch learns the MAC address of all devices attached to it and then matches the destination MAC address in the data it receives. None of the other devices pass data based solely on the MAC address.

9. The correct answer is C. 115,200 is the speed of the 16550 UART chip. Answer A is incorrect as 921,600 is the speed of the 16750 and 16950 UART chips. Answer B is incorrect as 430,800 is the speed of the 16650 UART chip and 9600 is the speed of the 8250 UART chip.

10. The correct answer is C. A Multistation Access Unit (MSAU) is used as the connectivity point on a Token Ring network. Answers A and B are incorrect. Switches and hubs are associated with Ethernet networks. Answer D is incorrect. Routers can be found on both Token Ring and Ethernet networks.

Need to Know More?

Olexa, Ron. *Implementing 802.11, 802.16, and 802.20 Wireless Networks: Planning, Troubleshooting, and Operations*. Communications Engineering. Newnes Publishing, 2004.

Computer networking products and information—www.alliedtelesyn.com.

Computer networking device information—www.3com.com.

“Computer Networking Tutorials and Advice”—compnetworking.about.com.