Chapter 2

The OSI Model

THE FOLLOWING NETWORK+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ **1.2 Specify the main features of 802.2 (LLC), 802.3 (Ethernet), 802.5 (Token Ring), 802.11b (wireless), and FDDI networking technologies, including:**
  - Speed
  - Access
  - Method
  - Topology
  - Media
- ✓ **2.1 Given an example, identify a MAC address.**
- ✓ **2.2 Identify the seven layers of the OSI model and their functions.**
- ✓ **2.3 Differentiate between the following network protocols in terms of routing, addressing schemes, interoperability, and naming conventions:**
  - TCP/IP
  - IPX/SPX
  - NetBEUI
  - AppleTalk
- ✓ **2.4 Identify the OSI layers at which the following network components operate:**
  - Hubs
  - Switches
  - Bridges
  - Routers
  - Network interface cards

You can't open a book on networking technologies without reading about the Open Systems Interconnect (OSI) model. This book is no exception, and for good reason. The OSI model helps us understand the fundamentals of network data transmission by offering a guideline to sending data from one computer to another. In this chapter, we will discuss the makeup of the various network models and, specifically, the most commonly discussed network model, the OSI model.

Introducing the OSI Model

The OSI model was designed to promote interoperability by creating a guideline for network data transmission between computers that have different hardware vendors, software, operating systems, and protocols. For example, look at the simple process of transferring a file. From a user's perspective, a single operation has been performed to transfer the file. In reality, however, many different procedures had to take place behind the scenes to accomplish this seemingly simple task. Network data transmission (like the file transfer) is performed through the use of a protocol suite, also known as a protocol stack.

A *protocol suite* is most easily defined as a set of rules used to determine how computers communicate with each other. It is similar to language. If I speak English and you speak English, then we can communicate. But if I speak only Spanish and you speak only English, we won't be able to communicate.

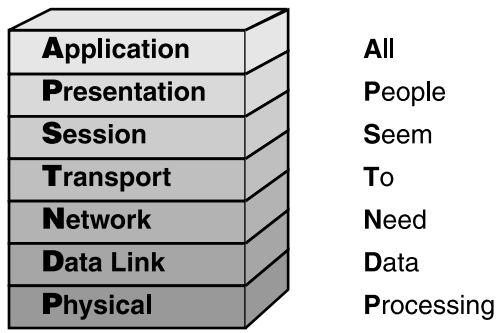
The OSI model is used to describe what tasks a protocol suite performs as you explore how data moves across a network. Keep in mind that not all protocols map directly to the guideline provided for us through the OSI model, but there are enough similarities so that you can use the OSI model to

examine how these protocols function. There are a myriad of protocol suites in use today, including IPX/SPX, NetBIOS, and TCP/IP. Each performs a specific function. Many of these functions that are provided through the use of a protocol stack and its components are standard functions performed by other components in other protocol stacks.

ISO is not an abbreviation for the International Organization for Standardization, but is instead derived from the Greek word *isos*, which means "equal," and was adopted by the organization. For more information, go to www.iso.ch.

The most commonly referenced protocol model, the OSI model, was developed in 1977 by the International Organization for Standardization (ISO) to provide "common ground" when describing any network protocol (see Figure 2.1).

FIGURE 2.1 The Open Systems Interconnect (OSI) model

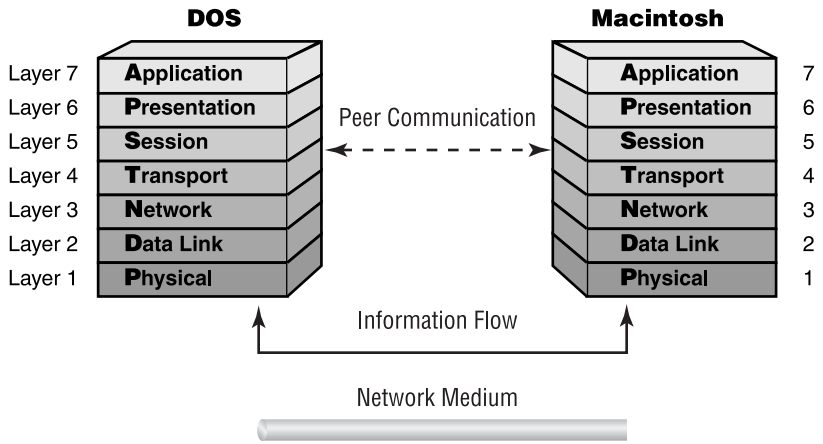


You can use mnemonic devices to help you remember the order of the OSI model layers: APSTNDP (from top to bottom). The most popular mnemonic for this arrangement is All People Seem To Need Data Processing. A reverse mnemonic (from Physical to Application, bottom to top) is Please Do Not Throw Sausage Pizza Away. (Good advice, don't you think?)

As you can see in Figure 2.1, the OSI model consists of seven layers. Each layer performs a specific function and then passes on the result to another layer. When a sending station has data to send, it formats a network

request and then passes that request to the network protocol at the top layer, the Application layer. The protocol that runs at the Application layer performs an operation on the request and then passes it to the next, lower layer. Each protocol at each layer below the Application layer performs its own calculations and appends its own information to the data sent from the layer above it. At the receiving station, the process happens in reverse. Figure 2.2 illustrates this basic process.

FIGURE 2.2 How data travels through the layers of the OSI model



The OSI model is only a model; it is not a protocol. Nobody is running the "OSI protocol" (at least no one has developed one at the time of this writing). Let's take a brief look at the layers of the OSI model and the basic protocol functions they describe. We'll start at the top with the Application layer and work our way down to the Physical layer.

The Application Layer

The Application layer, the top layer of the OSI model, does not refer to applications such as word processors, but rather refers to a set of tools that an application can use to accomplish a task, such as a word processor application requesting a file transfer. This layer is responsible for defining how interactions occur between network services (applications) and the network. Services that function at the Application layer include, but are not limited to, file, print, and messaging services. The Application layer may also support error recovery.

The Presentation Layer

The Presentation layer is responsible for formatting data exchange. In this layer, character sets are converted, and data is encrypted. Data may also be compressed in this layer, and this layer usually handles the redirection of data streams.

The Session Layer

The Session layer defines how two computers establish, synchronize, maintain, and end a session. Practical functions, such as security authentication, connection ID establishment, data transfer, acknowledgments, and connection release, take place here. This list is not all-inclusive. Any communications that require milestones—or, put another way, require an answer to "Have you got that data I sent?"—are performed here. Typically these milestones are called *checkpoints*. Once a checkpoint has been crossed, any data not received needs retransmission only from the last good checkpoint. Adjusting checkpoints to account for very reliable or unreliable connections can greatly improve the actual throughput of data transmission.

The Transport Layer

The Transport layer is responsible for checking that the data was delivered error-free. It is also used to divide a message that is too long into smaller segments and, in the reverse, take a series of short messages and combine them into one longer segment. These smaller or combined segments must later be correctly reassembled. This is accomplished through segment sequencing (usually by appending a number to each of the segments).

This layer also handles logical address/name resolution. Additionally, this layer can send an acknowledgment that it got the data packet. Frequently you will see this referred to as an ACK, which is short for acknowledgment. This layer is responsible for the majority of error and flow control in network communications.

The Network Layer

The Network layer is responsible for logical addressing and translating logical names into physical addresses. A little-known function of the Network layer is prioritizing data. Not all data is of equal importance. Nobody is hurt

if an e-mail message is delayed a fraction of a second. Delaying audio or video data a fraction of a second could be disastrous to the message. This prioritization is known as *Quality of Service (QoS)*.

In addition, the Network layer controls congestion, routes data from source to destination, and builds and tears down packets. Most routing protocols function at this layer.

The Data Link Layer

The Data Link layer takes raw data from the Physical layer and gives it a logical structure. This logic includes information about where the data is meant to go, which computer sent the data, and the overall validity of the bytes sent. In most situations, after a data frame is sent, the Data Link layer then waits for a positive ACK. If one is not received or if the frame is damaged, another frame is sent.

The Data Link layer also controls functions of logical network topologies and physical addressing as well as data transmission synchronization and connection.

The Physical Layer

The Physical layer is responsible for controlling the functional interface, such as transmission technique, pin layout, and connector type.

The OSI Model's Lower Layers

Now that you have a broad overview of the OSI model and its seven layers, you will now learn about the functions of each layer in a little more detail, starting with the lower layers. In addition to the concepts, you'll read about some of the devices that operate at those layers and some of their installation concepts.

The Physical Layer

The easiest way to think about the Physical layer is that it deals with measurable, physical entities. Any protocol or device that operates at the Physical layer deals with the physical concepts of a network.

Physical Layer Concepts

Generally speaking, Physical layer concepts deal with a network component that is tangible or measurable. For example, when a protocol at the Physical layer receives information from the upper layers, it translates all the data into signals that can be transmitted on a transmission medium. This process is known as *signal encoding* (or *encoding*, for short). With cable media (also called *bounded media*), the protocols that operate at the Physical layer translate the ones and zeros of the data into electrical ons and offs.

Additionally, the Physical layer specifies how much of the media will be used (in other words, its *signaling method*) during data transmission. If a network signal uses all available signal frequencies (or, to put it differently, the entire bandwidth), the technology is said to use *baseband* signaling. Most LAN technologies, such as Ethernet, use baseband signaling. On the other hand, if a signal uses only one frequency (or only part of the bandwidth), the technology is said to use *broadband* signaling. This means multiple signals can be transmitted on the media simultaneously. Television signals use broadband signaling.

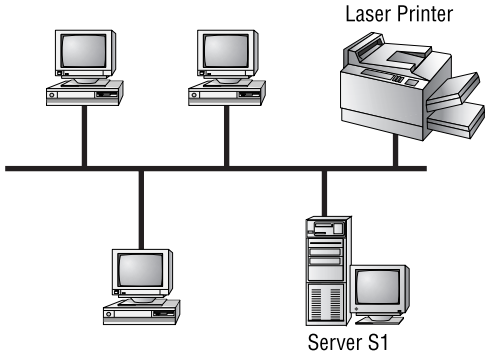
Finally, the Physical layer specifies the layout of the transmission media (its topology, in other words). A physical topology describes the way the cabling is physically laid out (as opposed to a logical topology, discussed later in the section titled "The Data Link Layer"). The physical topologies include the following:

- Bus
- Star
- Ring
- Mesh

The Bus Topology

In a physical bus topology, every computer is directly connected to a common medium. A physical bus network uses one network cable that runs from one end of the network to the other. Workstations connect at various points along this cable. The main advantage to this topology is simplicity: Only one cable is used, and a physical bus topology typically requires less cable than other physical topologies. However, a cable fault can bring down the entire network, thus making a physical bus topology the least fault tolerant of all the physical topologies. Figure 2.3 shows a sample physical bus network.

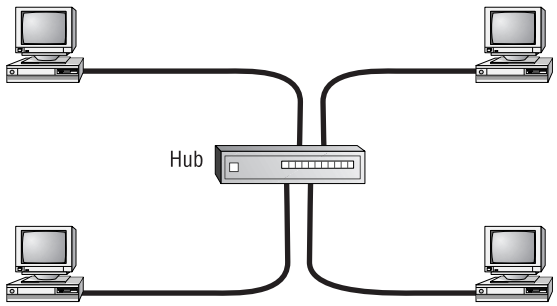
FIGURE 2.3 A sample physical bus topology



The Star Topology

In a physical star topology, a cable runs from each network entity to a central device. This central device (called a *hub*) allows all devices to communicate as if they were all directly connected. The main advantage to a physical star topology is its fault tolerance. If one node or cable malfunctions, the rest of the network is not affected. The hub simply won't be able to communicate with the station attached to that port. An Ethernet 10BaseT network is one example of a network type that requires a physical star topology. Figure 2.4 shows a sample network that uses a physical star topology.

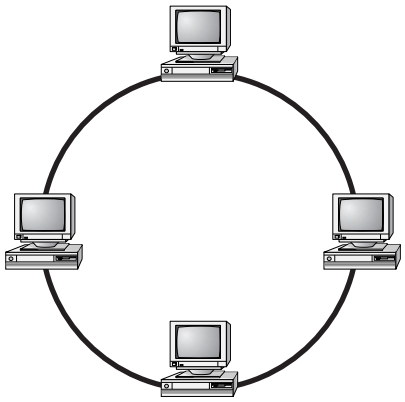
FIGURE 2.4 A physical star topology



The Ring Topology

A physical ring topology isn't seen much in the computer-networking world. If you do see it, it's usually in a wide area network (WAN) environment. In a physical ring topology, every network entity connects directly to only two other network entities (the one immediately preceding it and the one immediately following it). The complexity of the ring topology makes it a poor choice in most network environments. Figure 2.5 shows a physical ring network.

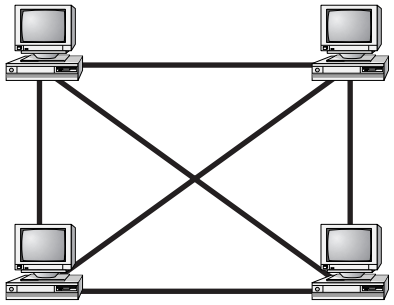
FIGURE 2.5 A physical ring topology



The Mesh Topology

A physical mesh topology is another physical topology that isn't widely used in computer networks (except in special WAN cases). In a physical mesh topology, every computer is directly connected to every other computer in the network. The more computers that are on a mesh network, the more cables that make up the network. If a mesh network has *n* computers, there will be $n(n-1)/2$ cables. With 10 computers, there would be $10(10-1)/2$, or 45 cables. As you can see, this topology quickly becomes unmanageable with only a few computers. Figure 2.6 shows a sample mesh network.

FIGURE 2.6 A physical mesh topology



Physical Layer Devices

Several devices operate primarily at the Physical layer of the OSI model. These devices manipulate mainly the physical aspects of a network data

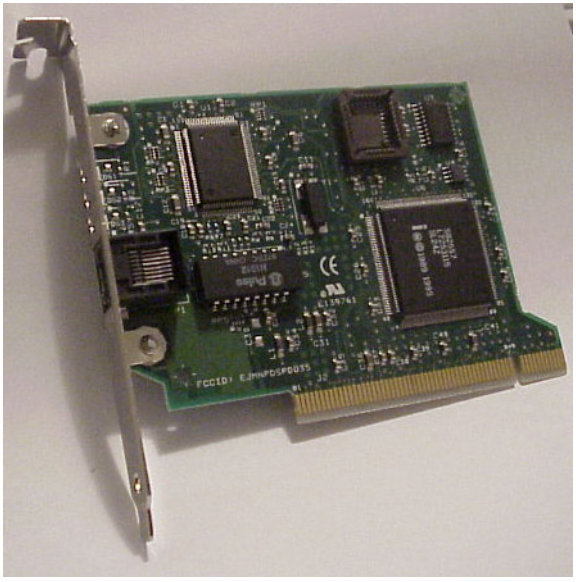
stream (such as the voltages, signal direction, and signal strength). Let's take a quick look at some of the most popular:

- NIC
- Transceivers
- Repeaters
- Hubs
- MAUs

The Network Interface Card (NIC)

Probably the most common component on any network is the network interface card (NIC). A NIC is the component that provides the connection between a computer's internal bus and the network media. NICs come in many shapes and sizes. They vary by the type of bus connection they employ and their network media connection ports. Figure 2.7 shows an example of a network interface card.

FIGURE 2.7 A sample network interface card



The Transceiver

In the strictest definition, a *transceiver* is the part of any network interface that transmits and receives network signals (transmitter/receiver). Every

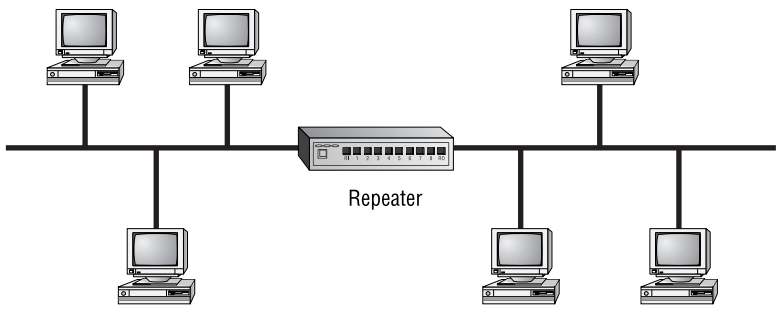
network interface has a transceiver. The appearance and function of the transceiver vary with the type of network cable and topology in use.

Some network interface cards have an Attachment Unit Interface (AUI) port (typically a 15-pin DIN connector) that allows a different, external transceiver type to be used, thus changing the media types to which the NIC can connect. For example, if you are using an Ethernet 10Base2 network interface card with an AUI port, you can connect to an Ethernet 10BaseT network by using an external transceiver attached to the AUI port. A DIN connector meets the specification of the German national standards body, Deutsche Industrie Norm, or DIN.

The Repeater

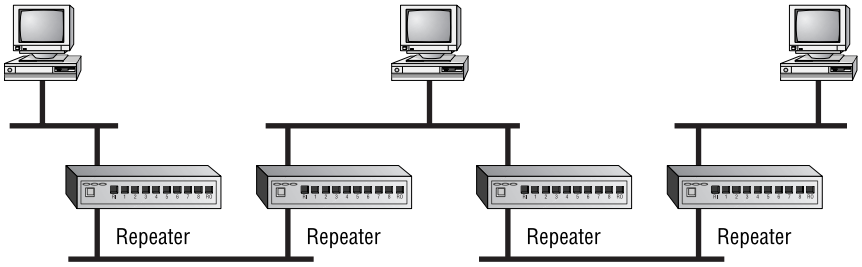
The simplest of all the Physical layer devices is the repeater, which simply amplifies the signals it receives on one port and resends (or "repeats") them on another. Repeaters are used to extend the maximum length of a network segment. They are often used if a few network stations are located far from the rest of the network. Figure 2.8 shows a network that uses a repeater.

FIGURE 2.8 A repeater installed on a network



The main downfall of a repeater is that it repeats *everything* it receives on one port, including noise, to its other ports. This has the ultimate effect of limiting the number of repeaters that can practically be used on a network. The 5-4-3 Rule dictates how many repeaters can be used on a network and where they can be placed. According to this rule, a single network can have five network segments connected by four repeaters, with three of the segments populated. If this rule is violated, one station may not be able to see the rest of the network. Figure 2.9 illustrates the 5-4-3 Rule.

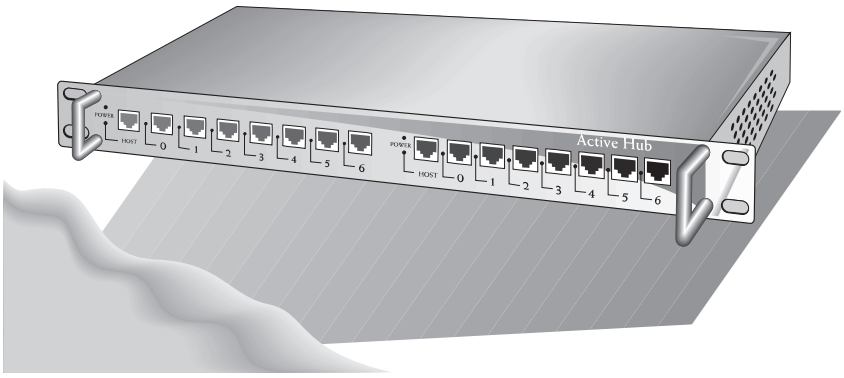
FIGURE 2.9 The 5-4-3 Rule for network repeaters



The Hub

After the NIC, a hub is probably the most common Physical layer device found on networks today. A hub (also called a *concentrator*) serves as a central connection point for several network devices. At its basic level, a hub is nothing more than a multiport repeater. A hub repeats what it receives on one port to all other ports. It is, therefore, also subject to the 5-4-3 Rule. Figure 2.10 shows an example of a hub.

FIGURE 2.10 A standard hub



There are many classifications of hubs, but two of the most important are active and passive:

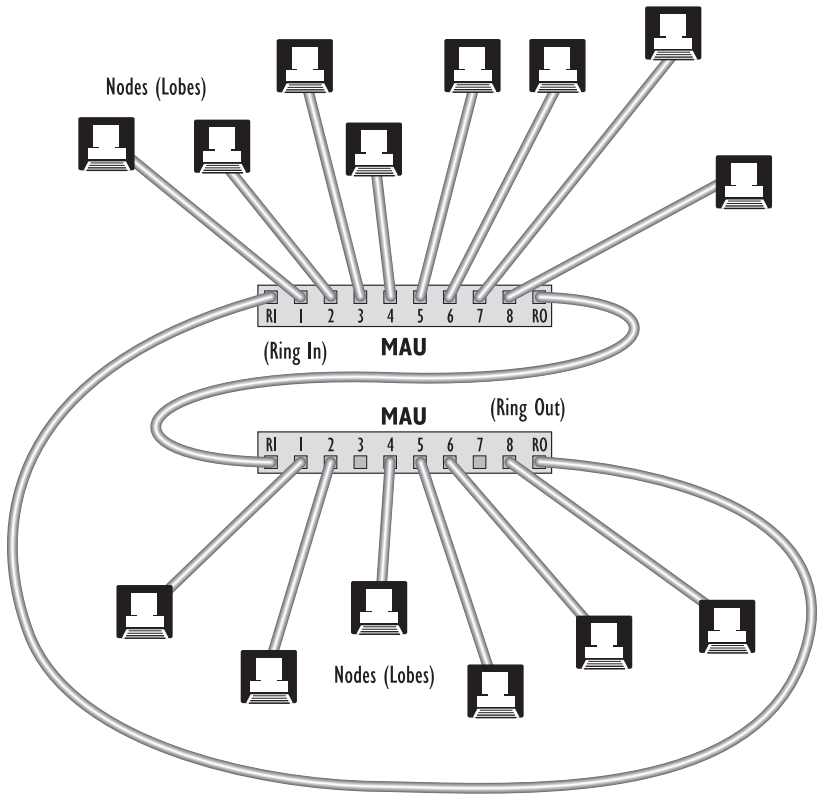
- An active hub is usually powered and it actually amplifies and cleans up the signal it receives, thus doubling the effective segment distance limitation for the specific topology (for example, extending an Ethernet segment another 100 meters).
- A passive hub is typically unpowered and makes only physical, electrical connections. Typically, the maximum segment distance of a

particular topology is shortened because the hub takes some power away from the signal strength in order to do its job.

The Multistation Access Unit (MAU)

This Physical layer device is unique to Token Ring networks. Token Ring networks use a physical star topology, yet they use a logical ring topology (discussed later). The central device on an Ethernet star topology network is a hub, but on a Token Ring network, the central device is a Multistation Access Unit (MAU, sometimes called MSAU). The functionality of the MAU is similar to that of a hub, but the MAU provides the data path that creates the logical "ring" in a Token Ring network. The data can travel in an endless loop between stations. MAUs are chained together by connecting the Ring Out port of one MAU to the Ring In port of another and connecting the last Ring Out port to the Ring In of the first MAU in the chain, thus forming a complete loop. In a Token Ring network, you can have up to 33 MAUs chained together. MAUs are shown in Figure 2.11.

FIGURE 2.11 MAUs in a Token Ring network



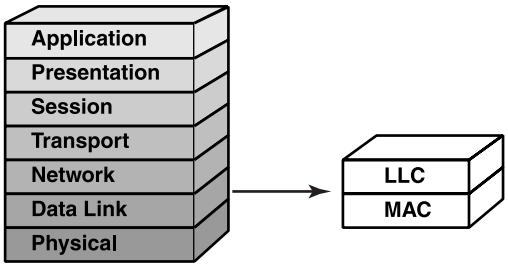
The Data Link Layer

The Data Link layer is actually made up of two sublayers:

- The Media Access Control (MAC)
- The Logical Link Control (LLC)

Figure 2.12 illustrates this arrangement.

FIGURE 2.12 Sublayers of the Data Link layer



Data Link Layer Concepts

Protocols that operate at the Data Link layer have several responsibilities, including creating, transmitting, and receiving packets. Additionally, the Data Link layer is responsible for physical (MAC) addressing and logical link control (LLC) processing, creating logical topologies, and controlling media access.

Packets

At the Data Link layer, data coming from upper-layer protocols are divided into logical chunks called *packets*. A packet is a unit of data transmission. The size and format of these packets depend on the transmission technology.

The Hardware (MAC) Address

Every network interface card has an address, typically assigned at the factory. This address is protocol-independent and is often called the hardware address. It's technically accurate, however, to call it the *MAC address* because it exists at the MAC sublayer of the Data Link layer. This address is also called the *Ethernet address* or the *physical address*.

The MAC address itself is a 12-digit hexadecimal number. As you may remember, a hexadecimal uses all digits from 0 through 9 and A through F. Each two-digit set is separated by colons, like so:

07:57:AC:1F:B2:76

Normally, the MAC address of a network interface card is set at the factory and cannot be changed. For this purpose, all NIC manufacturers keep track of the MAC addresses they use so they don't duplicate addresses between vendors. As of late, however, some manufacturers have started reusing their blocks of MAC addresses. This makes it necessary for administrators to be able to change the MAC addresses of the cards they receive (using a factory-supplied program), so if they discover a duplicated MAC address, they can resolve the conflict.

Logical Topology

In addition to these responsibilities, the Data Link layer can also dictate the logical topology of a network, or the way the packets move through a network. A logical topology differs from a physical topology in that the physical topology dictates the way the cables are laid out; the logical topology dictates the way the information flows. The types of logical topologies are the same as the physical topologies, except that the information flow specifies the type of topology to use.

Finally, the Data Link layer can describe the method of media access. The three main methods of media access are:

- Contention, in which every station "competes" with other stations for the opportunity to transmit, and each has an equal chance at transmitting. If two stations transmit at the same time, an error, referred to as a *collision*, occurs, and the stations try again.
- Polling, in which a central device, called a *controller*, polls each device, in turn, and asks if it has data to transmit. This type of media access virtually eliminates collisions.
- Token passing, which uses a special data packet called a *token*. When a station has the token, it can transmit. If it doesn't have the token, it can't transmit. This media access technology also eliminates collision problems.

Media Access

With many stations on the same piece of network media, there has to be a way of vying for time on the cable. This process is called media access, and there are three main methods: CSMA/CD, token passing, and CSMA/CA.

CARRIER SENSE/MULTIPLE ACCESS WITH COLLISION DETECTION (CSMA/CD)

This media access technology with the extremely long acronym is probably the most common. When a protocol that uses CSMA/CD has data to transmit,

it first senses if a signal is already on the wire (a *carrier*), indicating that someone is transmitting currently. That's the "Carrier Sense" part. If no one else is transmitting, it attempts a transmission and then listens to hear if someone else tried to transmit at the same time. If someone else transmits at the exact same time, a collision occurs. Both senders "back off" and don't transmit until some random period of time has passed. Then they both retry. That's the "Collision Detection" part. The final part ("Multiple Access") just means that more than one station can be on the network at the same time. CSMA/CD is the access method used in Ethernet and wireless Ethernet networks.

TOKEN PASSING

This media access method uses a special packet called a token. The first computer that is turned on creates the token. It then passes on the token to the next computer. The token passes around the network until a computer that has data to send takes the token off the network, modifies it, and puts it back on the network along with the data it has to send. Each station between the sender and the receiver along the network reads the destination address in the token. If the destination address doesn't match its own, the station simply sends the package on its way. When the destination station recognizes its address in the destination address of the token, the NIC copies the data into the station's memory and modifies the token, indicating it has received the data. The token continues around the network until the original sender receives the token again. If the original sender has more data to send, the process repeats itself. If not, the sender modifies the token to indicate that the token is "free" for anyone else to use. With this method, there are no collisions (as in CSMA/CD networks) because everyone has to have "permission" to transmit (via the token).

CARRIER SENSE/MULTIPLE ACCESS WITH COLLISION AVOIDANCE (CSMA/CA)

This technology works almost identically to CSMA/CD, but instead of sending the whole data chunk and then listening to hear if it was transmitted, the sender transmits a request to send (RTS) packet and waits for a clear to send (CTS) before sending. When it receives the CTS, the sender sends the chunk. AppleTalk networks use this method of media access. The difference between CSMA/CD and CSMA/CA has been described like this: Say you want to cross a busy street and you want to use one of these protocols to cross it. If you are using CSMA/CD, you just cross the street. If you get hit, you go back to the curb and try again. If you're using CSMA/CA, you send your little brother across. If he makes it, it's probably OK for you to go.

Project 802

One of the major components of the Data Link layer is the result of the Institute of Electrical and Electronics Engineers' (IEEE) 802 subcommittees and their work on standards for local area and metropolitan area networks (LANs/MANs). The committee met in February 1980, so they used the "80" from 1980 and the "2" from the second month to create the name Project 802. The designation for an 802 standard always includes a dot (.) followed by either a single or a double digit. These numeric digits specify particular categories within the 802 standard. Currently, there are 12 standards. These standards, shown in Figure 2.13, are listed in Table 2.1 and described in more detail in the following sections.

Some standards have a letter to further distinguish the standard (e.g., 802.11b). The letters usually refer to different versions or interpretations of the standard.

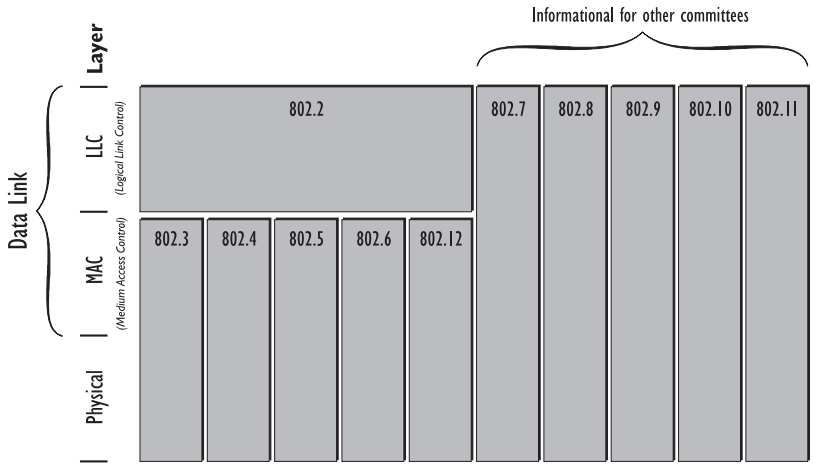
TABLE 2.1 IEEE 802 Networking Standards

Standard	Topic
802.1	LAN/MAN Management (and Media Access Control Bridges)
802.2	Logical Link Control
802.3	CSMA/CD
802.4	Token Bus
802.5	Token Ring
802.6	Distributed Queue Dual Bus (DQDB) Metropolitan Area Network (MAN)
802.7	Broadband Local Area Networks
802.8	Fiber-Optic LANs and MANs
802.9	Integrated Services (IS) LAN Interface

TABLE 2.1 IEEE 802 Networking Standards *(continued)*

Standard	Topic
802.10	LAN/MAN Security
802.11b	Wireless LAN
802.12	Demand Priority Access Method

FIGURE 2.13 The IEEE standards' relationship to the OSI model



The 802.1 LAN/MAN Management (and Media Access Control Bridges)

IEEE 802.1 discusses standards for LAN and MAN management, as well as for MAC bridges. One of the derivatives of 802.1 is the spanning tree algorithm for network bridges (bridges are discussed later in this chapter). The spanning tree algorithm helps to prevent bridge loops in a multibridge network.

The 802.2 Logical Link Control

This standard specifies the operation of the Logical Link Control (LLC) sublayer of the Data Link layer of the OSI model. The LLC sublayer provides an interface between the MAC sublayer and the Network layer. The 802.2 standard is used by the IEEE 802.3 Ethernet specification (discussed next), but

not by the earlier Ethernet 2 specifications (used in early implementations of Ethernet).

The 802.3 CSMA/CD

This standard specifies a network that uses a bus topology, baseband signaling, and a CSMA/CD network access method. This standard was developed to match the Digital, Intel, and Xerox (DIX) Ethernet networking technology. So many people implemented the 802.3 standard, which resembles the DIX Ethernet, that people just started calling it Ethernet. It is the most widely implemented of all the 802 standards because of its simplicity and low cost.

Recently the 802.3u working group updated 802.3 to include Ethernet 100BaseT implementations.

The 802.4 Token Bus

This standard specifies a physical and a logical bus topology that uses coaxial or fiber-optic cable and a token-passing media access method. It is used mainly for factory automation and is seldom used in computer networking. It most closely resembles the Manufacturing Automation Protocol (MAP), developed by General Motors and used by many manufacturing companies. Some people think that the IEEE 802.4 standard is for a technology known as the Attached Resource Computer Network (ARCnet). That is an incorrect assumption. Although the technologies are similar, the IEEE 802.4 standard more closely resembles MAP, not ARCnet.

The 802.5 Token Ring

This standard is one example of a commonly used product becoming a documented standard. Typically, a standard is developed and then products are written to conform to the standard. Token Ring was developed by IBM in 1984, and the 802.5 standard soon followed. The 802.5 standard and Token Ring are almost identical.

Like Ethernet, Token Ring can use several cable types. Most often, it is installed using *twisted-pair* cabling, which can be either *shielded* or *unshielded*. Shielding adds to the cable investment but offers the advantage of resistance to unwanted electrical signals that could impair the network signal.

Possible transmission rates for Token Ring have increased with time; after 4Mbps Token Ring came 16Mbps Token Ring. Token Ring uses a physical

star, logical ring topology with token-passing media access. If you install 4Mbps NICs on a network that otherwise uses 16Mbps NICs, your entire ring speed is reduced to 4Mbps. Unlike Ethernet, a computer cannot talk unless it has a token. This can cause some grief if a token gets "stuck."

Unlike ARCnet, Token Ring is still used in a number of locations for two reasons:

- IBM made sure that Token Ring did a fine job of talking to IBM mainframes, which are still commonly used.
- Token Ring network performance "degrades with grace."

The latter means that as network traffic increases, the network slowly gets slower, because the single token, which can travel in only one direction, gets busy carrying all that traffic. Ethernet, on the other hand, can become so flooded as network traffic increases that the entire network fails. Now, suppose you were wiring a computerized fire alarm system for a large building. Which would you rather use: Ethernet or Token Ring? To increase performance, some Token Ring technologies implement early token release, whereby the sending station doesn't hog the token. It simply grabs the token, sends its data, and frees the token.

In Token Ring, just as in all ARCnet and most Ethernet schemes, there is a central device to which stations connect. It isn't, however, called a hub. IBM calls it a MAU. IBM often has a different name for things. Even their name for Token Ring cabling is different. In telephone and computer networks, twisted cable is rated by *categories*. IBM rates Token Ring cable by *type*.

One final difference between Token Ring and the others is the *regeneration process*. Data signals are read, amplified, and repeated by every device on the network, to reduce degradation. This includes MAUs and NICs and is one reason that Token Ring is fairly expensive. An average Token Ring NIC is upward of $200, whereas a similar Ethernet card can be less than $20.

The 802.6 Distributed Queue Dual Bus (DQDB) Metropolitan Area Network

In some ways, asking what defines a metropolitan area network (MAN) is like asking how long a rope is. We can safely say that a MAN reaches beyond the area of a LAN. The interesting question is "When does a MAN become a WAN?" Sorry to say, there is no easy answer. Like a WAN, a MAN can support many computers. How many miles a MAN can cover has more to do

with regulations than with geography. For example, from a geographical standpoint, Portland, Oregon, and Vancouver, Washington, are separated by nothing more than several hundred feet of water. From a political standpoint, they are in different states, and, therefore, different telecommunication regulations apply to each city. This could mean that no MANs can connect Portland and Vancouver. For our purposes, we need to know only that a MAN generally encompasses a city-sized area and can support many-to-many connections. Transmission speeds vary with the size of an enterprise's bank account. The standard recommends the use of Distributed Queue Dual Bus (DQDB) technologies for MANs.

The 802.7 Broadband Local Area Networks

Don't let the fancy phrasing fool you. You have already used broadband if you have seen cable TV. When one cable carries multiple signals, that is broadband. The most common method for separating signals is to have them on different frequencies, which is called *Frequency Division Multiplexing (FDM)*. For example, each channel on a TV uses a different frequency. It is as simple as that. Maybe you can win a beer from some friends by seeing if they can explain Frequency Division Multiplexing. If they can't, collect your reward and tell them that is how all those TV channels get into their TV from one cable. The alternative to sending a set of signals this way is to use the entire cable for one signal. This is known as baseband and is used by standards such as Ethernet.

The 802.8 Fiber-Optic LANs and MANs

As the name implies, this working group handed down guidelines for fiber-optic usage on networks defined by 802.3 through 802.6, which includes *Fiber Distributed Data Interface (FDDI)* as well as *10BaseFL*. 10BaseFL defines Ethernet over fiber-optic cable. As you can see, some of the 802 definitions have more to do with your day-to-day work than others do.

The 802.9 Integrated Services (IS) LAN Interface

For a while, it seemed that this definition would have a profound effect on daily networking, because it laid out how *Integrated Services Digital Network (ISDN)* behaves. Late in 1998, however, many industry watchers began to call for the slow death of ISDN, because both cable modems and *asymmetrical digital subscriber line (ADSL)* had overtaken ISDN with less-complicated setup, higher performance, and lower cost.

The 802.10 LAN/MAN Security

This standard provides a secure pathway for data across a shared path. An implementation of this standard is using the public Internet as a backbone for a private interconnection between locations. The term for this form of connecting is known as *virtual private networking (VPN)*. Because VPN costs less than direct private connections, VPN is likely to become popular in the near future.

The 802.11 Wireless LAN

Wireless networking usually requires a higher up-front investment than cable-based networking. Still, the cost can be justified if an office is rearranged with any regularity or must be moved from location to location to satisfy business requirements. A famous example of this is the Red Cross. This agency would not be effective if it had to wire computers together before assisting at each disaster area.

Recently, 802.11 was updated to include the 802.11b standard, which specifies higher wireless speeds (11Mbps instead of 1Mbps for the original 802.11 standard). This demonstrates that the 802 standards have not been static for 20 years; instead, they've been a dynamic set of rules that continue to be updated as technology moves forward.

The 802.12 Demand Priority Access Method

First developed by Hewlett-Packard, this standard combines the concepts of Ethernet and ATM. The communication scheme used is called Demand Priority (thus, the name of the standard). It uses "intelligent" hubs that allocate more bandwidth to frames that have been assigned a higher priority by the sending computer. The hub scans its ports and then allocates bandwidth according to each frame's priority. This is extremely valuable for real-time audio and video transmissions.

The 802.12 standard is also known as *100VG (Voice Grade)*, *100VGAnyLAN*, *100BaseVG*, and *AnyLAN*. The 100 is short for 100Mbps, or 10 times faster than the original Ethernet speeds. Other manufacturers didn't buy into the ideas of 100VG, perhaps in part because of the higher overhead of demand priority due to port scanning. Instead, they updated the original Ethernet to *Fast Ethernet*, which also supports 100Mbps while maintaining the 802.3 standards.

Table 2.2 summarizes the main features—including speed, access method, topology, and media—of various network technologies, such as 802 standards and FDDI.

TABLE 2.2 Main Features of Various Network Technologies

Technology	Speed(s)	Access Method	Topologies	Media
IEEE 802.3	10, 100, or 1000 Mbps	CSMA/CD	Logical bus	Coax or UTP
IEEE 802.5	4 or 16Mbps	Token Passing	Physical star, Logical ring	STP
IEEE 802.11b	1 or 11Mbps	CSMA/CA	Cellular	None (Wireless)
FDDI	200Mbps	Token Passing	Physical star, Logical ring	Fiber-optic (UTP implemented as CDDI)

Data Link Layer Devices

Three main devices manipulate data at the Data Link layer:

- Bridges
- Switches
- NIC

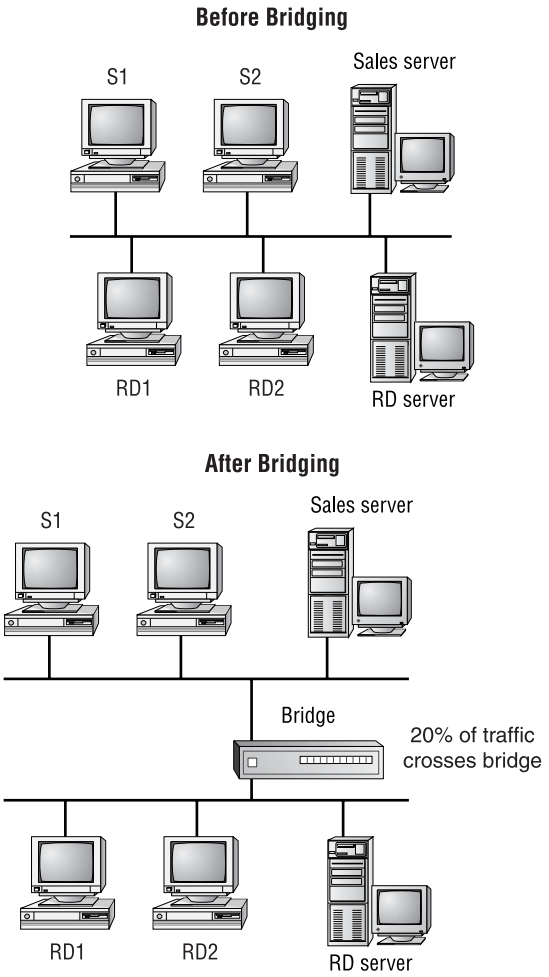
They are more complex than their Physical layer counterparts and thus are more expensive and more difficult to implement. But they each bring unique advantages to the network.

The Bridge

A bridge is a network device, operating at the Data Link layer, that logically separates a single network into two segments, but it lets the two segments appear to be one network to higher layer protocols. The primary use for a bridge is to keep traffic meant for stations on one side of the bridge and not let it pass to the other side. For example, if you have a group of workstations that constantly exchange data on the same network segment as a group of workstations that don't use the network much at all, the busy group will slow down the performance of the network for the other users. If you put in a bridge to separate the two groups, however, only traffic destined for a workstation on the other side of the bridge will pass to the other side.

All other traffic stays local. Figure 2.14 shows a network before and after bridging.

FIGURE 2.14 A sample network before and after bridging



Bridges can connect dissimilar network types (for example, Token Ring and Ethernet) as long as the bridge operates at the LLC sublayer of the Data Link layer. If the bridge operates only at the lower sublayer (the MAC sublayer), the bridge can connect only similar network types (Token Ring to Token Ring and Ethernet to Ethernet).

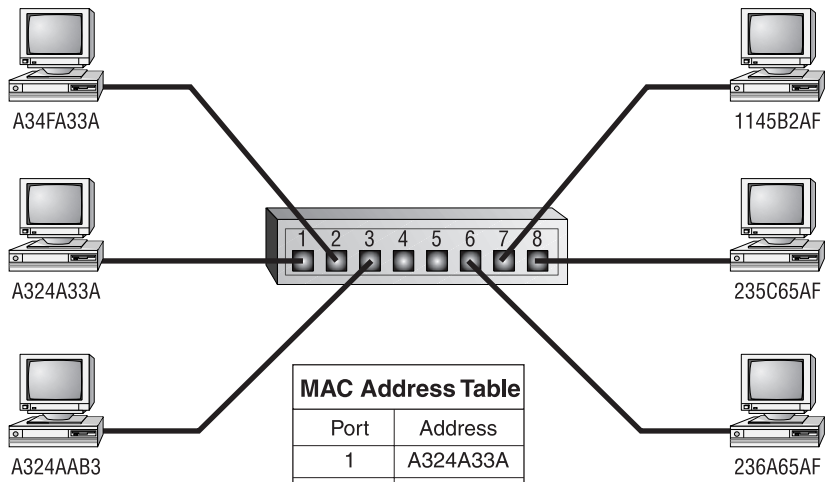
The Switching Hub

In the past few years, the switching hub has received a lot of attention as a replacement for the standard hub. The switching hub is more intelligent than a standard hub in that it can actually understand some of the traffic that passes through it. A switching hub (or switch for short) operates at the Data Link layer and is also known as a Layer 2 Switch. Layer 2 switches build a table of the MAC addresses of all the connected stations (see Figure 2.15).

When two stations attached to the switch want to communicate, the sending station sends its data to the switch. This part of the process is similar to the way a standard hub functions. However, when the switch receives the data, rather than broadcasting it over all its other ports as a hub would, the switch examines the Data Link header for the MAC address of the receiving station and forwards it to the correct port. This opens a virtual pipe between ports that can use the full bandwidth of the topology.

Switches have received a lot of attention because of this ability. If a server and several workstations were connected to the same 100Mbps Ethernet switch, each workstation would need a dedicated 100Mbps channel to the server, and there would never be any collisions.

FIGURE 2.15 A switch builds a table of all MAC addresses of all connected stations



MAC Address Table	
Port	Address
1	A324A33A
2	A34FA33A
3	A324AAB3
4	—
5	—
6	236A65AF
7	1145B2AF
8	235C65AF

The OSI Model's Middle Layers

As you move up the OSI model, the protocols at each successive layer get more complex and have more responsibilities. At the middle are the Network and Transport layers, which perform the bulk of the work for a protocol stack. You'll see why in the sections to follow.

The Network Layer

The Network layer of the OSI model defines protocols that ensure that the data arrive at the correct destination. This is probably the most commonly discussed layer of the OSI model.

Network Layer Concepts

The most important Network layer concepts are:

- Logical network addressing
- Routing

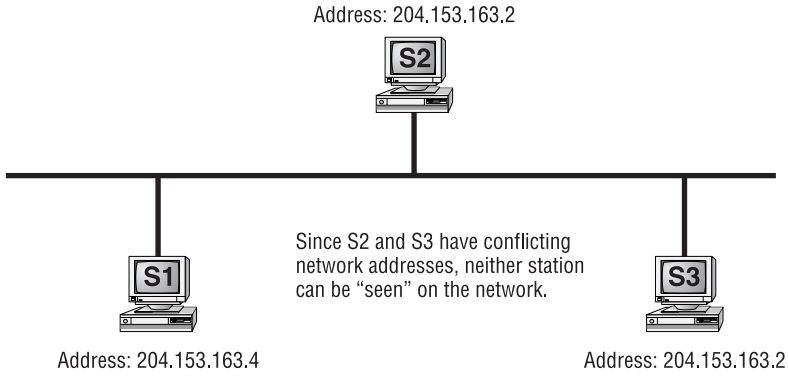
Logical Network Addressing

In the last section, you learned that every network device has an address (the MAC address) assigned at the factory and that this address is protocol-independent. But, as you know, most networks communicate using protocols that must have their own addressing scheme. If the MAC address is the Data Link layer physical address, the protocol-addressing scheme at the Network layer defines the logical address.

If IP addresses are duplicated on Windows 95/98 workstations, the first station that is assigned an address gets to use it. Any other station that has that address receives error messages about duplicated IP addresses. The address is then unassigned. The first station receives error messages as well, but it can continue to function.

Each logical network address is protocol-dependent. For example, a TCP/IP address is not the same as an IPX address. Additionally, the two protocols can coexist on the same computer without conflict. However, two different stations using the same protocol cannot have the same logical network address on the same network. If that happens, neither station can be seen on the network (see Figure 2.16).

FIGURE 2.16 Address conflicts on a network



Address conflicts can be common with TCP/IP because an administrator often needs to assign IP addresses. IPX addresses don't suffer from conflict nearly as often, because they use the MAC address as part of the IPX address. The MAC address is unique and can't be changed. For more information on network addresses, see Chapter 4, "TCP/IP Utilities."

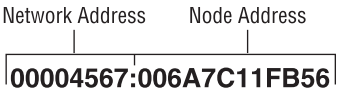
Real World Scenario

Using Network Address Formats

Whenever you have to set up a network or add a station, it is important to have an understanding of how network addresses work. Every network address in either TCP/IP or IPX has both a network portion and a node portion. The network portion is the number that is assigned to the network segment to which the station is connected. The node portion is the unique number that identifies that station on the segment. Together, the network portion and the node portion of an address ensure that a network address will be unique across the entire network.

IPX addresses use an eight-digit hexadecimal number for the network portion. This number, called the *IPX network address*, can be assigned randomly by the installation program or manually by the network administrator. The node portion is the 12-digit hexadecimal MAC address

assigned by the manufacturer. A colon separates the two portions. Here is a sample IPX address:



TCP/IP addresses, on the other hand, use a dotted decimal notation in the format xxx.xxx.xxx.xxx as shown in the following:

199.217.67.34 IP Address

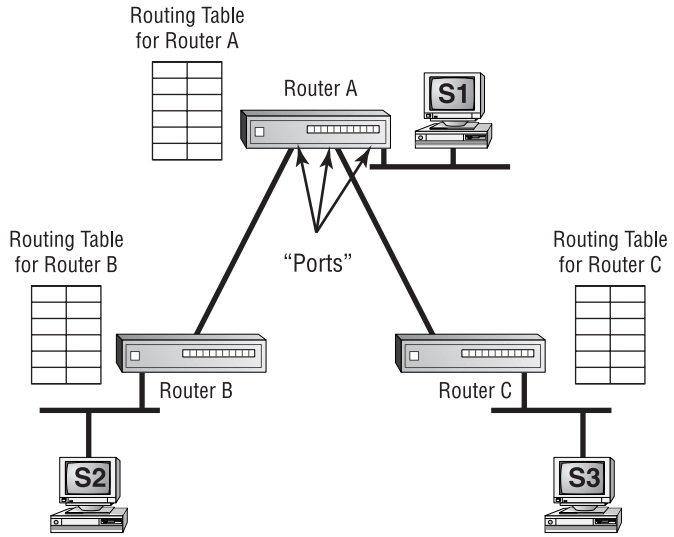
255.255.255.0 Subnet Mask

The address consists of four collections of eight-digit binary numbers (or up to three decimal digits) called octets, separated by periods. Each decimal number in an IP address is typically a number in the range of 1 through 254. Which portion is the network and which portion is the node depends on the class of the address and the *subnet mask* assigned with the address. A subnet mask is also a dotted decimal number with numbers in the range of 0 through 255. If a subnet mask contains 255 in any position (corresponding to a binary number of all ones), the corresponding part of the IP address is the network address. For example, if you have the mask 255.255.255.0, the first three octets are the network portion, and the last portion is the node.

Routing

Routing is the process of moving data throughout a network, passing through several network segments using devices called routers, which select the path the data takes. Placing routers on a network to connect several smaller routers turns a network into an entity known as an *internetwork*. Routers get information about which paths to take from files on the routers called routing tables. These tables contain information about which router network interface (or port) to place information on in order to send it to a particular network segment. Routers will not pass unknown or broadcast packets. A router will route a packet only if it has a specific destination. Figure 2.17 illustrates these components and their participation in the routing process.

FIGURE 2.17 Routing components



Information gets into routing tables in two ways:

- Through static routing
- Through dynamic routing

In *static routing*, the network administrator manually updates the router's routing table. The administrator enters every network into the routing table and selects the port on which the router should place data when the router intercepts data destined for that network. Unfortunately, on networks with more than a few segments, manually updating routing tables is time-intensive and prohibitive.

When using a Windows NT server as a router, use the ROUTE command to add, change, or remove static routes.

Dynamic routing, on the other hand, uses route discovery protocols (or routing protocols for short) to talk to other routers and find out which networks they are attached to. Routers that use dynamic routing send out special packets to request updates of the other routers on the network as well as to send their own updates. Dynamic routing is the most popular routing technology.

With dynamic routing, the two categories of route discovery protocols are distance vector and link state. Older route discovery protocols, such as Routing Information Protocol (RIP) for TCP/IP and RIP for IPX, use the distance vector method. In distance vector routing, a router sends out its routing table when the router is brought online and the contents of its routing tables every 30 seconds thereafter. When another router receives the contents of the other router's table, it adds 1 to the hop count of each route in the list of routes and then rebroadcasts the list. A *hop* is one pass through a router. This process typically takes place every 30 seconds.

The main downside to distance vector route discovery is the overhead required in broadcasting the entire routing table every 30 seconds. Link state route discovery is more efficient. Routers using link state route discovery routers send out their routing table via a multicast, not a broadcast packet, every five minutes or so. If there is an update, only the update is sent. NetWare Link Services Protocol (NLSP) for IPX and Open Shortest Path First (OSPF) for TCP/IP are two link state route discovery protocols.

Several protocols can be routed, but a few protocols can't be routed. It is important to know which protocols are routable and which aren't so that you can choose the appropriate protocol when it comes time to design an internetwork. Table 2.3 shows a few of the most common routable and nonroutable protocols and the routing protocols they use, if any.

TABLE 2.3 Routable and Nonroutable Protocols

Protocol	Route Discovery Protocol	Routable?
IPX	RIP	Yes
IPX	NLSP	Yes
NetBEUI	None	No
TCP/IP	RIP	Yes
TCP/IP	OSPF	Yes
XNS	RIP	Yes

When setting up routing on your network, you may have to configure a default gateway. A *default gateway,* when configured on a workstation, is the router that all packets are sent to when the workstation doesn't know where the station is or can't find it on the local segment. TCP/IP networks sometimes have multiple routers as well and must use this parameter to specify which router is the default. Other protocols don't have very good routing functions at the workstation, so they must use this feature to "find" the router.

Network Layer Devices

Three devices operate at the Network layer:

- Routers
- Brouters
- Layer 3 Switches

The Router

The router is the device that connects multiple networks or segments to form a larger internetwork. It is also the device that facilitates communication within this internetwork. It makes the choices about how best to send packets within the network so that they arrive at their destination.

Several companies manufacture routers, but probably the two biggest names in the business are Bay Networks and Cisco. Bay Networks is a conglomeration of smaller networking companies bought out by networking giant Synoptics. Cisco has always been a built-from-the-ground-up router company. Both companies make other products, to be sure, but their bread and butter is routing technologies.

Routers have many functions other than simply routing packets. Routers can connect many small segments into a network, as well as connect networks to a much larger network, such as a corporate WAN or the Internet. Routers can also connect dissimilar lower-layer topologies. For example, you can connect an Ethernet and a Token Ring network using a router. Additionally, with added software, routers can perform firewall functions and packet filtering.

Routers are probably the most complex devices on a network today. Consequently, they are likely to be the most expensive. But simple low-end routers have been introduced by Bay Networks, Cisco, and other companies

in the sub-$1,000 range that make Internet connectivity more affordable. Hub vendors have begun to introduce basic intranetwork routing functionality into their products as well. You will learn more about that later in this chapter when we discuss switches.

The Brouter

The *brouter* is a unique device that combines the functionality of a bridge and a router. It routes most packets, but if it can't route a particular packet, it will try and bridge it. Unfortunately, if you try to use a brouter as either a bridge or a router, it will fall short in the functionality of either.

The brouter was mainly used to connect different network topologies and to bridge them, but it is not used much anymore.

Layer 3 Switches

A fairly new Network layer device that has received much media attention of late is the Layer 3 Switch. The Layer 3 part of the name corresponds to the Network layer of the OSI model. It performs the multiport, virtual LAN, data-pipelining functions of a standard Layer 2 Switch, but it can also perform basic routing functions between virtual LANs. In some workgroups, a Layer 3 Switch can replace a workgroup router.

The Transport Layer

The Transport layer defines the protocols for structuring messages and checks the validity of transmissions.

Transport Layer Concepts

The Transport layer reminds me of what my old Net Tech instructors used to pound into my head: "Reliable end-to-end error and flow control." (Thanks, Doug and Al!) The Transport layer does other things as well, but the protocols that operate at the Transport layer mainly ensure reliable communications between upper peer layers.

The Connection Type

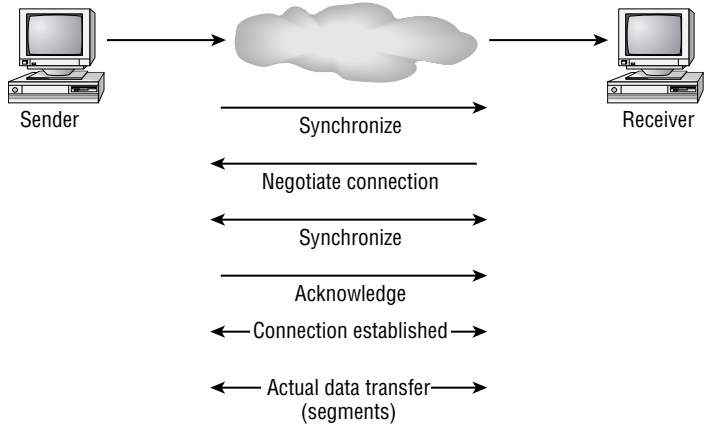
To provide error and flow control services, protocols at the Transport layer use connection services. The two types of connection services are:

- Connection-oriented
- Connectionless

Connection-oriented connection services use acknowledgments and responses to establish a virtual connection between sending and receiving stations. The acknowledgments are also used to ensure that the connection is maintained.

Connection-oriented connections are similar to phone calls. You dial the intended recipient, and the recipient picks up and says hello. You then identify yourself and say that you'd like to talk about something, and the conversation begins. If you hear silence for a while, you might ask "Are you still there?" to make sure the recipient is still on the line. When finished, you both agree to end the connection by hanging up. Connection-oriented services work in the same way, except that instead of mouths, phones, and words, they use computers, NICs, and special packets. Figure 2.18 shows an example of the beginning of communications between two computers using connection-oriented services.

FIGURE 2.18 Initiating communications using a connection-oriented service



Connectionless services, on the other hand, don't have error and flow control. They do have one simple advantage: speed. Because connectionless services don't have the overhead of maintaining the connection, the sacrifice in error control is more than made up for in speed. To make another analogy, connectionless services are similar to a postcard. Each message is considered singular and not related to any other. So, if one part of the message is lost, it can simply be resent.

Name Resolution

The Transport layer also handles logical address–to–logical name resolution. In some protocols, a node address, such as 185.45.2.23, isn't the best way to reference a host. Some protocol stacks (TCP/IP and IPX/SPX, for example) can use Transport layer logical names for hosts in addition to their Network layer logical addresses. These logical names make it easier for you to find hosts on the network.

At the Transport layer, various protocol stacks implement a protocol to translate Network layer addresses into Transport layer logical names.

Transport Layer Implementations

Before we discuss the other layers of the OSI model, let's take a look at the IPX/SPX, TCP/IP, and NetBEUI implementations of the Transport layer.

The IPX/SPX Protocol

As far as the connection services of IPX/SPX are concerned, there are two transport protocols: IPX and SPX. IPX is connectionless and thus enjoys the benefits of connectionless transports, including increased speed. SPX, on the other hand, uses connection-oriented services.

IPX/SPX has no name resolution system by default. That functionality is employed when a NetWare server is running Novell Directory Services (NDS) and the NDS directory requester (which runs at the Session, Presentation, and Application layers) can make requests of an NDS database.

The TCP/IP Protocol

Like the IPX/SPX protocol stack, the TCP/IP protocol stack has two transport protocols:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

TCP is connection-oriented, and UDP is connectionless. Some upper-layer protocols, such as FTP and HTTP, require reliable connection-oriented service and, therefore, use TCP. Other upper-layer protocols, such as Trivial File Transfer Protocol (TFTP) and Network File System (NFS), require increased speed and will trade reliability for that speed. They, therefore, use UDP.

For network address—to–name resolution, TCP/IP uses Domain Name Services (DNS). It is my belief that the name resolution of the OSI model's Transport layer was designed for DNS. Many operating systems use DNS for name resolution, but Unix (whose networking is based on TCP/IP) uses DNS almost exclusively. DNS is probably the most cross-platform name resolution method available. Chapter 4 discusses the function and operation of DNS.

The NetBEUI Implementation

Because it is based on the NetBIOS protocol, NetBEUI (NetBIOS Enhanced User Interface) has datagram support and, thus, has support for connectionless transmission. It doesn't, however, have support for connection-oriented services. NetBIOS does allow hosts to have logical names (using WINS), but the naming service, as with NDS, functions at the upper layers of the OSI model.

The OSI Model's Upper Layers

The upper layers of the OSI model deal with less esoteric concepts. Even though we're still discussing computer networking, the top three layers (Session, Presentation, and Application) seem easier to understand. Because the Network+ exam doesn't cover the upper layers (and many times these top three layers are grouped together), the following sections will give only a brief overview.

The Session Layer

Protocols that operate at the Session layer of the OSI model are responsible for establishing, maintaining, and breaking sessions, or *dialogs*. This is different from the connection services provided at the Transport layer, because the Session layer operates at a higher level and looks at the bigger picture—the entire conversation, not just one sentence. Many gateways operate at the Session layer.

The Presentation Layer

The Presentation layer does what you might think it does: It changes the look, or *presentation*, of the data from the lower layers into a format that the upper-layer processes can work with. Among other services, the Presentation layer deals with encryption, data compression, and network redirectors.

In addition, the Presentation layer deals with character-set translation. Not all computer systems use the same table to convert binary numbers into text. Most standard computer systems use the American Standard Code for Information Interchange (ASCII). Mainframe computers (and some IBM networking systems) use the Extended Binary Coded Decimal Interchange Code (EBCDIC). The two are totally different. Protocols at the Presentation layer can translate between the two.

The Application Layer

Now I know what you might be thinking: "This layer is for my programs, right?" Wrong. The Application layer defines several standard network services that fall into categories such as file transfer, print access, and e-mail relay. The applications that access these network services are located above the Application layer (although some people say that applications are an extension of the Application layer).

Upper-Layer Devices

There are only a few upper-layer devices, none of which operate at any specific layer. Because they perform a range of functions for the network, they fall into the class of devices known as *gateways*. A gateway translates one type of network data into another. Gateways can be either hardware or software, but the most popular way to run a gateway is as a software program on a dedicated computer.

There are many, many types of gateways, but the one most people think of is an e-mail gateway. E-mail gateways translate e-mail messages from one type of e-mail system so that they can be transmitted on another (for example, from GroupWise e-mail to SMTP mail for the Internet).

Networking Protocols

Now that you have a basic understanding of the OSI model and its related concepts, you can use these OSI concepts to understand how the major protocols work and how each of the protocols within each protocol stack maps to the OSI model, thus describing its function.

In this section you will learn about four major protocol stacks and how each one handles the concepts of addressing, routing, interoperability, and naming. These four protocol stacks are:

- TCP/IP
- IPX/SPX
- NetBEUI
- AppleTalk

TCP/IP

The Transmission Control Protocol/Internet Protocol (TCP/IP) is the protocol of choice today. It, like other protocols, is used to allow two computers to communicate over a network. However, TCP/IP is used not only on local area networks, but also over wide area networks and the Internet. Actually, TCP/IP is the only protocol in use on the Internet. You'll learn more about TCP/IP in Chapter 3, "TCP/IP Fundamentals."

Addressing

Addressing the network entities protocol (called *hosts* in TCP/IP parlance) that runs the TCP/IP is fairly straightforward in TCP/IP. Each host is given (either manually or automatically) a dotted decimal IP address in the format xxx.xxx.xxx.xxx where xxx is a number from 0 to 255. There are several addressing rules, which you will learn more about in Chapter 3.

Because addressing is a Network layer concept, the protocols that deal with addressing can be found at this layer. The Address Resolution Protocol (ARP) is responsible for resolving an IP address to the MAC address of the receiving host. The MAC address is a Data Link layer address hard-coded to each network card at the manufacturer. When a TCP/IP packet is sent, at some point a router will need to determine exactly which station the packet

is intended for. On Ethernet networks, the router will use an ARP lookup and ARP broadcasts. Essentially, the router listens for the periodic ARP broadcasts from all hosts and records the information in its ARP cache (basically a table that says which IP address is associated with which MAC address). When a router receives packets and needs to send them to a particular station on one of its own segments, it examines the IP address of the destination, looks up the MAC address of that station using ARP, and forwards the packet via Ethernet to the intended destination.

Routing

On TCP/IP networks, routing is a fairly involved process. In order to send a packet through an internetwork (like the Internet), the router must have three pieces of information: the IP address of the sender, the IP address of the destination, and the IP address of the next router to which the packet should be sent. The first two are part of the IP datagram being sent, but the router must figure out the last item itself. The router uses information it receives from other routers about what IP addresses they have on their local segments in order to build a logical "map" of the network (called a *routing table*). Then, the router can determine the best way to get the datagram to its destination and send on the information to the next router.

Routers build routing tables using either RIP or OSPF. The major difference between these two routing protocols (which operate at the Network layer of the OSI model) is that RIP is a *distance vector routing protocol* and OSPF is a *link state routing protocol*. The difference between them is pretty simple. Distance vector protocols (like RIP) are used by routers to gather information about the hosts connected to them and to build a table of the addresses and the segment they are on (called a routing table). The router then broadcasts this information to all the routers it is connected to. All of the routers that receive this information add the route information to their own routing tables and rebroadcast them. Approximately every 30 seconds, distance vector protocol routers will rebroadcast their entire routing table. Eventually, all routers in the internetwork know about all the other routers and the networks they serve.

Link state routing protocols (like OSPF) work slightly differently. Whereas RIP routers will broadcast their entire routing table every 60 seconds, a link state router will send out to its "neighbors" only the changes to its routing table. Additionally, link state routers have a more directed relationship with their neighbors. Instead of broadcasting all of its information

to everyone on the internetwork, link state protocols (like OSPF) prefer to send only updates and a small amount of information to a specific list of addresses.

Interoperability

Of all the protocols listed in this chapter, no protocol is more flexible or more interoperable than TCP/IP. As the Internet gained popularity, everyone wanted to "get on the Net." As such, almost every computer had to have two things: a web browser and some form of TCP/IP connection. Therefore, every computer that is connected to the Internet is running TCP/IP in one way or another. Many companies have used the TCP/IP protocol suite to communicate with one another over the Internet.

Additionally, because of this phenomenon, every operating system has some form of TCP/IP protocol stack and, as such, can communicate with other operating systems on some fundamental level.

Naming

TCP/IP hosts are named according to the DNS convention. DNS is a service that resolves names to IP addresses so that we can use friendly names like `www.trainsolutions.com` to refer to computers instead of unfriendly IP addresses like 192.168.24.31.

There are two parts to a DNS name: the host name (e.g., `www`) and the domain name (e.g., `trainsolutions.com`). Each of these components is separated by a period. Typically, you would assign a host name that says what the computer's function is (i.e., `www` for a web server). The domain name, on the other hand, is usually the name of the company in which the computer resides, or some related name, followed by `.com`, `.edu`, `.net`, or any other domain suffix. You'll learn more about DNS in Chapter 3.

IPX/SPX

When Novell NetWare was introduced, it was designed to be a server platform for a local area and wide area networks. To that end, they designed a protocol stack that was very efficient over local area networks and that would also work on wide area networks. That protocol stack was the Internetwork Packet eXchange/Sequenced Packet eXchange, or IPX/SPX.

Addressing

IPX is the Network layer protocol that handles addressing and routing for the IPX/SPX protocol stack. IPX addressing is actually very simple. It takes the 12-digit hexadecimal address, as that is the address for the individual node on that network segment. The network segment is referred to by its own unique 8-digit hexadecimal address. For example, the address:

```
0001ABF3:12AB341FF414
```

would correspond to a station with a MAC address of 12AB341FF414 on the network segment labeled 0001ABF3. Every network segment is assigned its own, unique IPX network address. Since the network card has the MAC address burned in at the factory and, for the most part, can't be changed, it doesn't have to be configured. The only configuration that must be done is to assign the IPX network address and configure the server with that address.

In addition to a station address, routers are given an internal IPX address. This address uniquely identifies a router to the rest of a network. NetWare servers always have an internal IPX address because they can function as routers.

Routing

Most routers that route TCP/IP traffic can also route IPX traffic (although they may require additional software or configuration). IPX/SPX is a routable protocol stack because it has routing protocols designed into it. The routing protocols for IPX/SPX are RIP and NLSP.

IPX RIP is very similar to the RIP protocol in TCP/IP in that RIP for IPX is the distance vector routing protocol for IPX. Similarly, NLSP is the link state routing protocol for IPX/SPX. Both work similarly to their TCP/IP counterparts. RIP uses broadcasts of the entire IPX routing tables to keep all IPX routers updated. And, just like OSPF, NLSP sends out only the changes to the routing tables and then only to a select group of network addresses.

Interoperability

IPX/SPX isn't as ubiquitous as TCP/IP (which can even be found running on Coke machines), but it holds its own when it comes to allowing many

different platforms to talk. Windows 9*x*, NT, Me, 2000, NetWare, OS/2, and a few versions of Linux come "out of the box" with support for communicating with other entities via the IPX/SPX protocol stack. Before the popularity explosion of the Internet in the mid-1990s, the IPX/SPX protocol stack was the only protocol stack many companies would run.

The only downside to interoperability using IPX/SPX is that many versions of Unix, or other high-end operating systems like OS/400, don't come with built-in support for the IPX/SPX protocol stack or even with an option for support.

Naming

Really, the only items that have names are the NetWare servers. Generally speaking, you can name a NetWare server anything you want, as long as you follow these rules:

- The name must not include any of the "illegal" characters, including a period (.), a comma (,), a plus sign (+), an equals sign (=), and a backslash (\).
- Names must be less than 64 characters (or 47 characters in older versions of NetWare).
- Names are not case sensitive.

These names are resolved using either Bindery Services or Novell Directory Services. These will be discussed more in Chapter 5, "Major Network Operating Systems."

NetBEUI

NetBEUI is a Network layer protocol designed to provide support for NetBIOS networks. NetBIOS is a protocol that was developed by IBM (and later enhanced by Microsoft and Novell) for use with network-aware operating systems like LAN Manager/LAN Server, Windows 9*x*, Windows NT, and Windows 2000. It is a very fast and efficient protocol with low overhead. Because it is small and efficient, it works well on small LANs with between 10 and 200 nodes. The two protocols are often referred to together as NetBEUI/NetBIOS.

Naming and Addressing

There is very little network addressing with NetBEUI/NetBIOS. Actually, for NetBEUI, naming and addressing are the same thing. Each station is configured with a unique name (called the *NetBIOS name*) that is used for all communications. It's simple and quick. The only item that must be configured on the workstation is the name of the workstation.

Routing

Because the NetBEUI/NetBIOS protocol stack does not have route discovery protocols and was never designed to be routable, it can't be routed. All routers will drop NetBEUI/NetBIOS packets. Some routers, however, are smart enough to try and bridge these packets to all segments when it finds out that the packet is NetBEUI.

Interoperability

Only a few operating systems run NetBEUI/NetBIOS. The operating systems for IBM and Microsoft are the primary supporters of this protocol. Windows 9*x*, NT, 2000, LAN Manager, and OS/2 support NetBEUI/NetBIOS. These operating systems can therefore communicate using NetBEUI/NetBIOS. The Macintosh operating system, however, does not support NetBEUI natively.

AppleTalk

When Apple introduced the Macintosh in 1984, the Mac included networking software. This networking software used a protocol known as AppleTalk and a cabling system known as LocalTalk. It is a very simple and elegant protocol in that the computer takes care of most of the configuration. You simply plug it in and it works. Because of its simplicity and popularity with Mac users, and because the Mac users wanted a faster version, Apple developed AppleTalk version 2 with support for Ethernet (EtherTalk).

Addressing

Each station on an AppleTalk network uses an address that is 24 bits long. Sixteen of those bits are given to the network, and each network can support 254 nodes. Each network segment can be given either a single 16-bit network number or a range of 16-bit network numbers. If a network is assigned a

range of numbers, that network is considered an *Extended AppleTalk network* because it can support more than 254 nodes. The node address is automatically assigned by the computer itself.

In addition to network numbers, AppleTalk networks use areas called zones. Zones allow an administrator to divide a network into logical areas for easier administration and to make it easier for a user to find resources.

Although you can have multiple zones on an AppleTalk network, an AppleTalk node can belong to only one zone.

Routing

AppleTalk wasn't originally designed to be routed over a WAN, but with the release of AppleTalk version 2, Apple included routing functionality with the introduction of the Routing Table Maintenance Protocol (RTMP). RTMP is a distance vector routing protocol, like RIP for both IP and IPX.

Interoperability

The only computer that comes with AppleTalk installed by default is the Macintosh. Most Windows operating systems are able to use the AppleTalk protocol, but require that additional software be installed.

Naming

AppleTalk uses the Name Binding Protocol (NBP) to associate the name of the computer with its network address. It is broadcast based. Every station broadcasts its name when it comes up on a network. The AppleTalk router on a network will cache these names and respond to the NBP request. When a node requests a name resolution, the local router will answer with information it has obtained from this cache.

If an AppleTalk network doesn't have a router, each node will perform both NBP requests and NBP responses.

Summary

In this chapter, you learned about the OSI model and had an introduction to a few of the most popular protocols in use today. You also learned about the seven layers that make up the OSI model, including (from top to bottom) the Application, Presentation, Session, Transport, Network, Data Link, and Physical layers. You also learned what each layer's primary responsibility is. In the later sections, you learned about which devices operate at each layer of the OSI model.

In this chapter, you also learned about some of the major protocols, including TCP/IP, IPX/SPX, NetBEUI/NetBIOS, and AppleTalk, and how the different parts work together. For each protocol, you learned which parts of the protocol stack handle the concepts of addressing, routing, interoperability, and naming.

Exam Essentials

Be able to specify the main features—including speed, access method, topology, and media—of various network technologies, such as 802 standards and FDDI. You should be able to differentiate between the various technologies when studying for the exam. Refer to Table 2.2 for help.

Be able to identify a MAC address. A MAC address on a network is a 12-digit hexadecimal number in the format xx:xx:xx:xx:xx:xx where x is a number from 0 to 9 or a letter from A through F.

Be able to identify the seven layers of the OSI model and describe their functions. The seven layers of the OSI model (from the bottom to top or Layer 1 to Layer 7) and their functions are:

- Physical layer, which is responsible for placing data on the network in the form of electrical signals
- Data Link layer, which is responsible for dividing datagrams into packets as well as physical addressing

- Network layer, which is responsible for network addressing and routing
- Transport layer, which is responsible for reliable end-to-end data delivery and flow control
- Session layer, which is responsible for establishing and maintaining a session, or dialog
- Presentation layer, which is responsible for the "look" of the data, including encryption/decryption and character-set translation
- Application layer, which is responsible for providing network services

Know how to differentiate between the IP, IPX, NetBEUI, and AppleTalk protocols when it comes to routing, addressing schemes, interoperability, and naming conventions. TCP/IP uses RIP or OSPF for routing protocols, uses a dotted decimal notation (four sets of numbers, each from 0 to 255) for the addressing, is completely interoperable, and uses DNS for host naming.

IPX, on the other hand, uses IPX RIP and NLSP for routing information, uses a unique 20-digit address (incorporating the MAC address) for the station address, interoperates with several different operating systems (but not as many as TCP/IP), and uses NDS for host naming.

NetBEUI isn't as flexible or has as many features, but does offer performance on a LAN segment. Addressing and naming are completely automatic (naming does require a user to enter a station name).

Finally, AppleTalk does have routing protocols (RTMP), and uses an automatic addressing scheme. It requires only that the user name the computer when enabling AppleTalk. It is by far the simplest protocol, but has the lowest performance and the least interoperability.

Be able to explain the issues that must be considered when multiple protocols are running at the same time. When running multiple protocols, not only are you using more memory on a computer, but you're adding a level of complexity to the network that is multiplied by the number of stations that you add. It is better to run the fewest protocols possible. Some issues you will see include running out of memory, program confusion, stations unable to communicate (each is running a different protocol), and network congestion.

Identify the OSI layers at which hubs, switches, bridges, routers, and network interface cards operate. Hubs operate at the Physical layer for the most part. Switches can operate at many different layers (up to Layer 5), but the lowest common denominator for all network switches is OSI Layer 2 (Data Link layer). Bridges are relatively simple devices and operate primarily at the Data Link layer. Routers are more complex devices, but because all they do is route packets, they operate at Layer 3 (Network layer). Finally, network interface cards (NICs) operate at the Physical and Data Link layers.

Key Terms

Before you take the exam, be certain that you are familiar with the following terms:

100BaseVG	concentrator
100VG (Voice Grade)	connectionless services
100VGAnyLAN	connection-oriented services
10BaseFL	controller
AnyLAN	default gateway
asymmetrical digital subscriber line (ADSL)	dialogs
baseband	distance vector routing protocol
bounded media	dynamic routing
broadband	encoding
brouter	Ethernet address
carrier	Extended AppleTalk network
categories	Fast Ethernet
checkpoints	Fiber Distributed Data Interface (FDDI)
collision	Frequency Division Multiplexing (FDM)

gateways

hop

hosts

hub

Integrated Services Digital Network (ISDN)

internetwork

IPX network address

link state routing protocol

MAC address

NetBIOS name

packets

physical address

presentation

protocol suite

Quality of Service (QoS)

regeneration process

routing

routing table

shielded

signal encoding

signaling method

static routing

subnet mask

token

transceiver

twisted-pair

type

unshielded

virtual private networking (VPN)

Review Questions

1. Which layer of the OSI model ensures reliable, end-to-end communications?
   - **A.** Network
   - **B.** Transport
   - **C.** Session
   - **D.** Presentation

2. Which layer of the OSI model provides routing functionality?
   - **A.** Transport
   - **B.** Data Link
   - **C.** Physical
   - **D.** Network

3. Which layer of the OSI model translates the data from upper-layer protocols into electrical signals and places them on the network media?
   - **A.** Physical
   - **B.** Transport
   - **C.** Data Link
   - **D.** Network

4. You are a consultant designing a network for a company with more than 1000 users. Which 802 standard would you implement to ensure that bandwidth would be sufficient and equal without bridging or additional segments?
   - **A.** 802.1
   - **B.** 802.2
   - **C.** 802.3
   - **D.** 802.5

5. You have a limited budget and need to design a network for 50 users. Which 802 standard would you implement?

   A. 802.1

   B. 802.3

   C. 802.5

   D. 802.9

6. You are installing a Windows 95/98–based TCP/IP network. You accidentally set workstation B to the same IP address as workstation A. Which workstation(s) will receive an error message?

   A. Workstation A

   B. Workstation B

   C. Neither

   D. Both

7. You are installing a Windows 95/98–based TCP/IP network. You accidentally set workstation B to the same IP address as workstation A. Which workstation(s) will have a valid IP address?

   A. Workstation A

   B. Workstation B

   C. Neither

   D. Both

8. Unix uses which method to resolve Transport layer names into logical network addresses?

   A. WINS

   B. NDS

   C. DNS

   D. TRS

9. Which of the following protocols use a connectionless transport? (Choose all that apply.)

   A. HTTP

   B. TCP

   C. TFTP

   D. IP

   E. NetBIOS

10. Which protocols use a connection-oriented transport?

    A. UDP

    B. NetBIOS

    C. HTTP

    D. NLSP

11. Which name resolution system is implemented with TCP/IP by default?

    A. DNS

    B. NDS

    C. SND

    D. WINS

12. Which OSI model layer has both a MAC sublayer and an LLC 12 sublayer?

    A. Physical

    B. Transport

    C. Network

    D. Data Link

13. Which OSI model layer is responsible for establishing, maintaining, and breaking down dialog?

    A. Application

    B. Gateway

    C. Session

    D. Network

14. Which OSI layer is responsible for network services such as messaging and file transfer?

    A. Transport

    B. Network

    C. Application

    D. Session

15. Which OSI layer is responsible for building and tearing down packets?

    A. Network

    B. Transport

    C. Data Link

    D. Physical

16. On an Ethernet network, every station must have a _____.

    A. Hub

    B. NIC

    C. Switch

    D. Transceiver

17. Which type of hub doesn't require power?

    A. Active

    B. Passive

    C. Intelligent

    D. Switched

18. You are the administrator of a 100-station Ethernet network. Your users are complaining of slow network speeds. What could you replace your hub with to increase your network throughput?

A. Router

B. Bridge

C. Switch

D. NIC

19. At which OSI model layer do routers operate?

A. Physical

B. Data Link

C. Transport

D. Network

20. Which of the following is a MAC address?

A. 199.165.217.45

B. 00076A: 01A5BBA7FF60

C. 01:A5:BB:A7:FF:60

D. 311 S. Park St.

Answers to Review Questions

1. B. Of the layers listed, the only OSI layer that is responsible for reliable, end-to-end communications is the Transport layer. The Network layer is responsible for logical network addresses, the Session layer is responsible for opening and maintaining session information, and the Presentation layer is responsible for how data "looks" to the upper layer(s).
2. D. Of the OSI model layers listed, the Network layer is the only one that is responsible for routing information, because it contains information for logical network addressing.
3. A. The Physical layer, as its name suggests, is the layer responsible for placing electrical transitions on the physical media. The other layers are all upper layers.
4. D. The 802.5 standard is similar to the Token Ring technology developed by IBM. That technology scales well and could handle more than 1000 users without bridging or additional segments. Also, the performance would be better than that of any of the other technologies listed.
5. B. The 802.3 standard (similar to Ethernet) would work best in this situation because it is flexible, simple to implement, and, most importantly, cheaper than the other technologies listed.
6. D. Through broadcasts, both workstations will detect if there is a duplicate IP address on the network and will display error messages to that effect.
7. A. Because workstation A had a valid IP address to begin with, Windows takes a first come, first served approach with the IP addresses and lets Workstation A keep its IP address. Workstation B detects that A already has it and just deactivates that address.
8. C. Domain Name Services (DNS) is the primary method most Unix implementations use to map logical names to network (IP) addresses. Although some versions of Unix can use WINS and NDS, DNS is the preferred method.

9. C, E. Answers C and E, TFTP and NetBIOS, both use a connectionless transport. Answer B is, in fact, a connection-oriented transport protocol. HTTP uses TCP, so it is therefore connection-oriented. And IP is a Network layer protocol.

10. C. Of all the protocols listed, HTTP is the only one that uses a connection-oriented transport protocol (TCP). The others use connectionless transport.

11. A. Although WINS is a name resolution that does use TCP/IP, it works only on Windows-based networks. The only true name resolution system that almost every TCP/IP network uses is DNS.

12. D. The Data Link layer is divided into two sublayers: the MAC sublayer and an LLC sublayer. The other layers aren't normally subdivided.

13. C. The Session layer is responsible for establishing, maintaining, and breaking down dialog.

14. C. The services listed are all network applications, and the only layer that provides network application services is the Application layer.

15. A. The Network layer is responsible for packaging data into packets. The other layers use different terms for data packages, such as frames.

16. B. All of the devices listed, except the NIC, are external devices. Additionally, there is usually only one of each of the other devices on a network, but there has to be at least one NIC per station.

17. B. Passive hubs simply make physical connections, and thus are usually unpowered. All of the other types listed require power.

18. C. A switch would increase performance by making virtual, direct connections between sender and receiver. Bridges and routers actually decrease performance because these devices introduce latency into the communication. Replacing the hub with a NIC just can't be done.

19. D. Because routers deal with logical network addresses, they operate at the Network layer.

20. C. MAC addresses use a 12-digit hexadecimal number that is separated into six pairs of hex numbers. The only one that corresponds to that format is Answer C.