2

Network Protocols and Standards

CERTIFICATION OBJECTIVES

CERTIFICATION OBJECTIVE 2.01

Network Protocols

Understanding the concepts of networking protocols is critical to being able to troubleshoot communication problems in networking environments. This section will introduce you to four common network protocols found in networking environments and the difference between routable and nonroutable protocols.

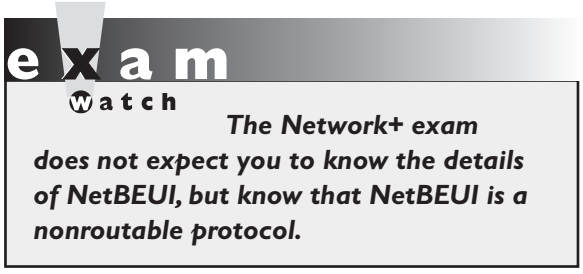
A network protocol is a language that is used by systems that wish to communicate with one another. Let's look at an example of a communication problem that could occur when two persons who want to talk are not speaking the same language. Let's say you are traveling the country on your summer vacation and stopped in a fast food restaurant. When ordering your favorite meal, you would need to ensure that you spoke the same language as the person taking the order. If you speak English and the waiter speaks French, you would be giving your order, but the waiter would not be able to understand you. The same thing will happen on the network when two systems use two totally different protocols—everyone is talking, but no one is communicating. The first step to networking is making sure that the two systems that are trying to talk have the same protocol installed.

Four of the major protocols found in networking environments today are

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

NetBEUI

NetBIOS Extended User Interface (NetBEUI) is a transport protocol developed by IBM but adopted by Microsoft for use in earlier versions of Windows and DOS. NetBEUI commonly was found in smaller networks due to the fact that it is a nonroutable protocol. A *nonroutable protocol* is a protocol that sends data, but the data is unable to cross a router to reach other networks; communication is limited to the local area network (LAN) only. The fact that NetBEUI is a nonroutable protocol has limited its use on networks dramatically.



NetBEUI was first implemented with LAN Manager networks and became popular in smaller Microsoft networks back in the Windows 3.11, Windows 95, and Windows 98 days. It is no longer supported in Windows 7. NetBEUI is an extremely efficient and simple protocol with little overhead because of its inability to route packets. One of the major advantages of NetBEUI is that it is extremely simple to install and configure. Minimal configuration is required to allow the protocol to work—you install it, specify a unique computer name, and it works!

What Is NetBIOS?

NetBEUI has a close friend, NetBIOS (short for Network Basic Input/Output System), with which it works closely when communicating with systems on the network. NetBIOS is an application programming interface (API) that is used to make network calls to remote systems. When you install NetBEUI, it includes the NetBIOS protocol, and NetBEUI relies on NetBIOS for session management functionality. Also, NetBIOS is nonroutable, but may be installed with other routable protocols, such as IPX/SPX or TCP/IP, to allow NetBIOS traffic to travel across networks. NetBIOS has two communication modes:

- **Session mode** This is used for connection-oriented communication in which NetBIOS is responsible for establishing a session with the target system, monitoring the session to detect any errors in transmission, and then recovering from those errors by retransmitting any data that went missing or was corrupt.
- **Datagram mode** This is used for connectionless communication in which a session is not needed. Datagram mode also is used by NetBIOS broadcasts. Datagram mode does not support error detection and correction services, which are the responsibility of the application using NetBIOS.

Now that you understand a little bit about NetBIOS, here are some important things to keep in mind regarding NetBIOS and NetBEUI:

- NetBIOS is a session protocol, whereas NetBEUI is a transport protocol (more on session and transport later in this chapter, when you learn about the OSI model).

- NetBIOS is used by other protocols as well, such as TCP/IP.
- Since NetBIOS is not a transport protocol, it does not directly support routing, but depends on one of two transport protocols—TCP/IP or IPX/SPX—to do this.
- NetBIOS uses NetBIOS names as a method of identifying systems on the network. A NetBIOS name, also known as a computer name, can be a maximum of 16 bytes long—15 bytes for the name and 1 byte for the NetBIOS name suffix (a code at the end of the name representing the running service). The NetBIOS computer name must be unique on the LAN.

IPX/SPX

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) is a protocol suite (which means there are many protocols in one) that was developed by Novell and was popular on older NetWare networks. However, newer versions of NetWare (NetWare 5.*x* and later) have moved away from it and are using TCP/IP as the preferred protocol. Microsoft refers to IPX/SPX as NWLink (NetWare Link).

exam Watch

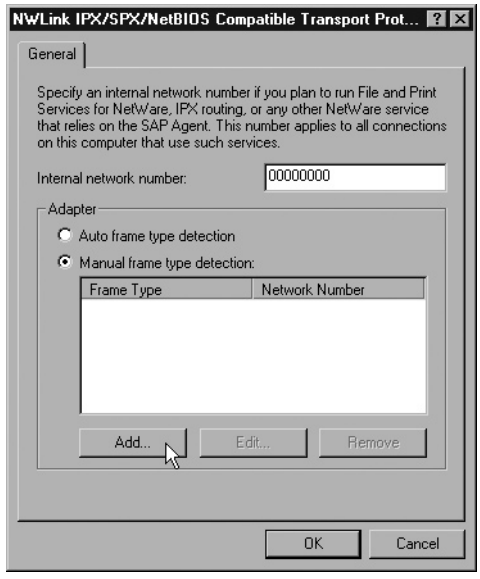
The Network+ exam is focused on TCP/IP as a protocol suite and, therefore, you are not tested on the details of IPX/SPX.

The IPX protocol of the IPX/SPX protocol suite is responsible for the routing of information across the network. IPX/SPX is a routable protocol, so its addressing scheme must be able to identify each system on the network and the network itself using a network ID. The network administrator assigns each network a network ID. An IPX network ID is an eight-character hexadecimal value—for example, 0BADBEEF. A complete IPX address is made up of the network ID, a period (.), and then the six-byte Media Access Control (MAC) address of the network card (a unique address burned into the network card) in the system. For example, the computer I am sitting at right now has a MAC address of 00-90-4B-4C-C1-59. If my system were connected to network ID 0BADBEEF, then my IPX network address would be 0BADBEEF.00904B4CC159. The fact that the MAC address is used means that there is no need to have it resolved when communication occurs—which will make the protocol more efficient than other protocols such as TCP/IP, which does require the IP address to be resolved to a MAC address.

IPX/SPX is not as easy to configure as NetBEUI. When doing an IPX installation, you will need to be familiar with configuration issues such as the network number and frame type (shown in Figure 2-1).

FIGURE 2-1

Configuring the IPX/SPX protocol



- **Network number** This is the number assigned to the Novell network segment. It is a hexadecimal value, with a maximum of eight digits.
- **Frame type** This is the format of the packet that is used by the network. It is important to make sure that all systems on the network are configured for the same frame type. For example, if I want to connect to SERVER1, which uses the frame type 802.2, then I would need to ensure that my frame type was set to 802.2—otherwise, I would not be able to communicate with SERVER1. The four major frame types are 802.2, 802.3, ETHERNET_SNAP, and ETHERNET_II.

The Microsoft operating systems default to an auto-setting on the frame type, which allows the IPX/SPX protocol to "sense" the frame type being used on the network and configure itself accordingly. This has made the configuration of IPX/SPX much easier during the past few years.

on the job

If you happen to work on an older network where there are multiple frame types configured, such as 802.2 and 802.3, the clients that are configured to auto-detect the frame type will configure themselves for 802.2 because it is the default frame type.

While IPX is responsible for the routing of packets, it is also a connectionless, unreliable transport. Unreliable means IPX packets are sent to a destination without requiring the destination to acknowledge receiving those packets. Connectionless means that no session is established between sender and receiver before transmitting data.

SPX is the protocol in the IPX/SPX protocol suite that is responsible for reliable delivery. SPX is a connection-oriented protocol that will ensure packets that are not received at the destination are retransmitted on the wire.

To install IPX/SPX in pre–Windows Vista versions, you will go to your Local Area Connection properties dialog box and then choose the Install button. When shown a list of components to install, you select Protocol and then click Add. When shown the list of protocols, you select the NWLink IPX/SPX entry and click OK. To configure the network number and frame type, go to the properties dialog box for NWLink. NWLink is not supported by Windows Vista and Windows 7.

AppleTalk

AppleTalk is a routable protocol that is used primarily in Macintosh environments to connect multiple systems together in a network environment. AppleTalk was implemented in two phases, known as phase 1 and phase 2, with the second phase being more popular today.

- **Phase 1** This was designed for small workgroup environments and, therefore, supports a much smaller number of nodes on the network. Phase 1 supports nonextended networks; each network segment can be assigned only a single network number, and only one zone is allowed in a nonextended network. A zone is a logical grouping of nodes—the network administrator will assign nodes to a particular zone.
- **Phase 2** This was designed for larger networks and supports more than 200 hosts on the network. Phase 2 supports extended networks, thereby allowing one network segment to be assigned multiple network numbers and allowing for multiple zones on that network segment. Each node is part of a single zone on an extended network.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is the most common network protocol suite used today. A routable protocol, TCP/IP is the protocol on

which the Internet is built. TCP/IP is robust and commonly is associated with UNIX and Linux systems.

TCP/IP originally was designed in the 1970s to be used by the Defense Advanced Research Projects Agency (DARPA) and the U.S. Department of Defense (DOD) to connect dissimilar systems across the country. This design required the capability to cope with unstable network conditions. Therefore, the design of TCP/IP included the capability to reroute packets.

One of the major advantages of TCP/IP was the fact that it could be used to connect heterogeneous (dissimilar) environments together, which is why it has become the protocol of the Internet—but what are its drawbacks? TCP/IP has two major drawbacks:

- **Configuration** TCP/IP requires configuration, and to administer it, you need to be familiar with IP addresses, subnet masks, and default gateways—not complicated topics once you are familiar with them, but there is a bit of a learning curve compared to installing NetBEUI.
- **Security** Because of the open design of TCP/IP, is an unsecure protocol. If security is a concern, you need to make certain that you implement additional technologies to secure the network traffic or systems running TCP/IP. For example, if you want to ensure that other individuals cannot read the data sent to your web server, you would use SSL with the website—which would encrypt traffic between a client and your web server. You will be introduced to more on network security in Chapter 14, but be aware that security could be an issue for TCP/IP if not handled appropriately.

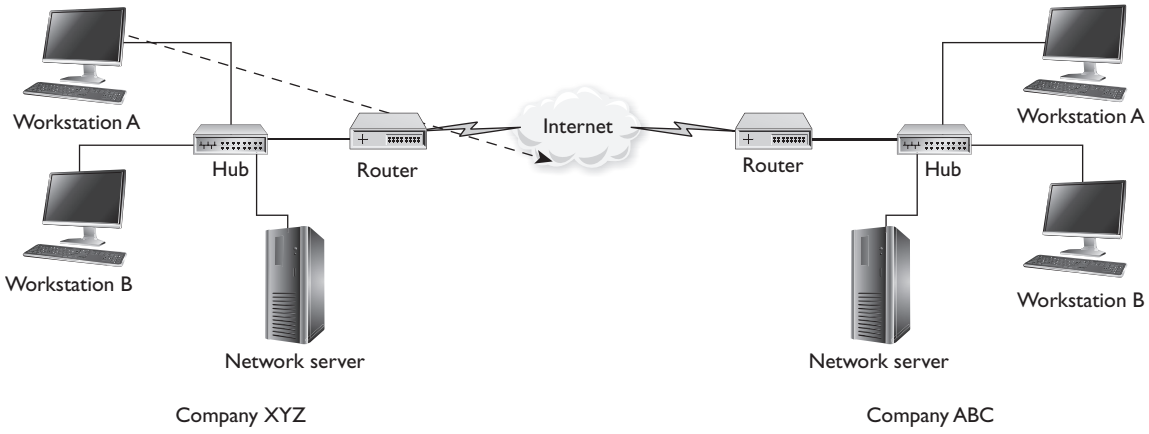
exam Watch

The Network+ exam focuses on TCP/IP as the core protocol suite. Note that Chapters 4, 5, and 7 go into more detail on TCP/IP—please be sure to spend a lot of time with those chapters to prepare for the exam.

Routable vs. Nonroutable Protocols

We have discussed each of the four major protocols, and you have learned that NetBEUI is a nonroutable protocol, whereas IPX/SPX, AppleTalk, and TCP/IP are routable protocols. What exactly is a routable protocol? A routable protocol is a protocol whose packets may leave your network, pass through your router, and be delivered to a remote network, as shown in Figure 2-2.

FIGURE 2-2 A routable protocol sending data through a router



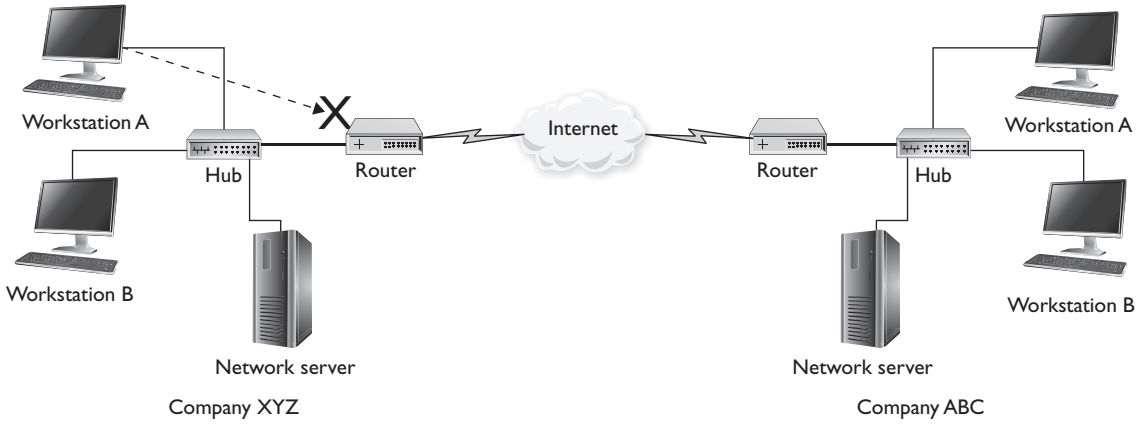
exam Watch

TCP/IP, IPX/SPX, and AppleTalk are all examples of routable protocols, while NetBEUI is a nonroutable protocol.

A nonroutable protocol does not have the capability to send packets across a router from one network to another network. This is due to the fact that this is a simple protocol and does not accommodate addressing patterns in the packets that give knowledge of multiple networks. For example, NetBEUI uses NetBIOS names to send data back and forth, but a NETBIOS name does not identify "what network" the destination system exists on, whereas TCP/IP and IPX/SPX both have a network ID portion to their addressing schemes that identify "what network" the destination system exists on.

When a nonroutable packet reaches the router, the router discards it, as shown in Figure 2-3, because there is no routing information in the packet, such as a layer-3 destination address.

FIGURE 2-3 A nonroutable protocol cannot send data across routers



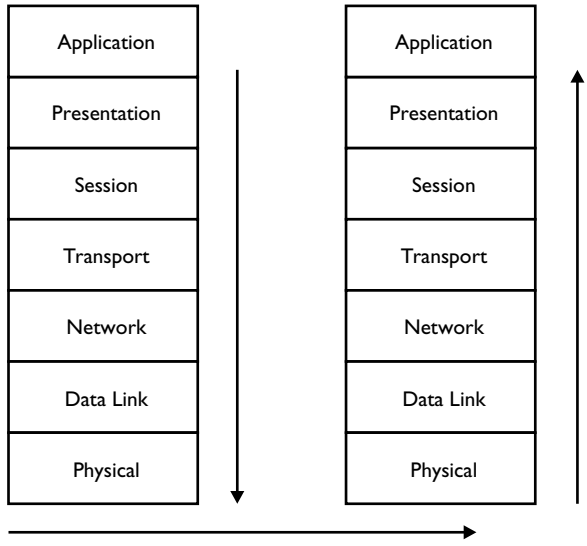
CERTIFICATION OBJECTIVE 2.02

The OSI Model

In the early 1980s, the International Organization for Standardization (ISO) defined a standard, or set of rules, for manufacturers of networking components that would allow these networking components to communicate in dissimilar environments. This standard is known as the Open Systems Interconnect (OSI) model and is made up of seven layers. Each layer of the OSI model is responsible for a specific function or task within the stages of network communication. The seven layers, from highest to lowest, are application, presentation, session, transport, network, data link, and physical. Network communication starts at the application layer of the OSI model (on the sending system) and works its way down through the layers to the physical layer. The information then passes along the communication medium to the receiving computer, which works its way back up the layers starting at the physical layer. Figure 2-4 shows an example of packets being transmitted down through the OSI layers of the sending computer, across the medium, and back up the OSI layers

FIGURE 2-4

Layers of the OSI model



on the receiving computer. Be sure to refer to this figure frequently when going through this section.

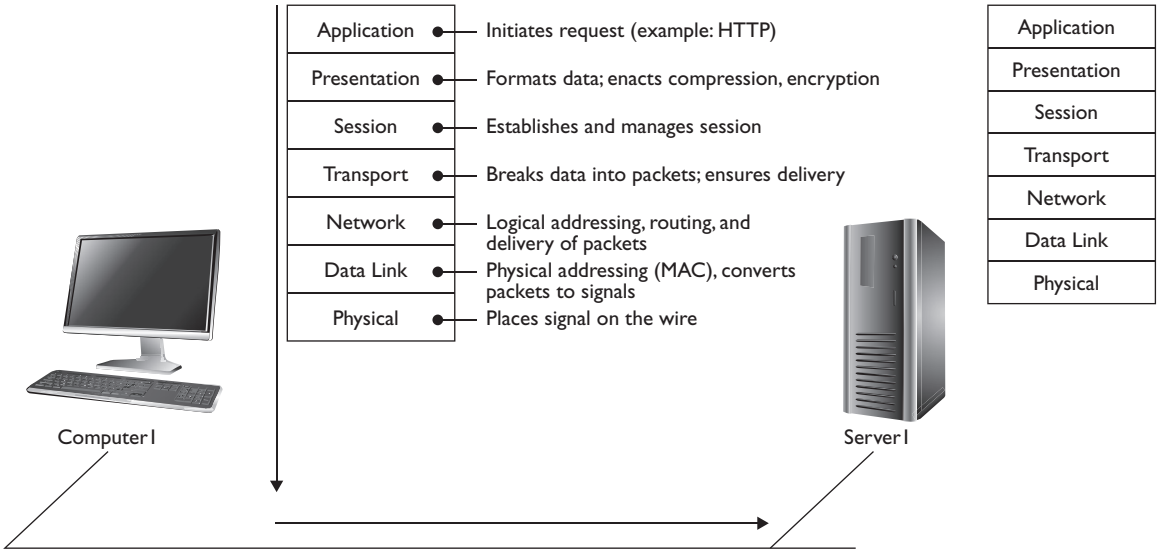
Each layer of the OSI model is responsible for certain functions within the process of sending data from one system to another. Each layer is responsible for communicating with the layers immediately above it and below it. For example, the presentation layer will receive information from the application layer, format it appropriately, and then pass it to the session layer. The presentation layer will never deal directly with the network or data link layers.

Let's look at the layers from the point of view of two computers that will send data between each other: COMPUTER1 and SERVER1 are going to exchange data on the network. COMPUTER1 is the sending computer, and SERVER1 is the receiving computer, as shown in Figure 2-5. The data exchange starts with COMPUTER1 sending a request to SERVER1. It is important to notice as you progress through the layers that whatever function is performed at a layer on the sending system must be undone at the same layer on the receiving system. For example, if the presentation layer compresses the data on the sending system, the presentation layer will decompress the data on the receiving system before passing it up to the application layer.

exam Watch

The Network+ exam is sure to test your knowledge of the OSI model and each of its layers, so be familiar with this for the exam!

FIGURE 2-5 Identifying the function of each layer of the OSI model



Layer 7: The Application Layer

The application layer running on the sending system (COMPUTER1) is responsible for the actual request being made. This could be any type of networking request—a web request using a web browser (HTTP), an e-mail delivery request using SMTP, or a file system request using the network client redirector software. On the receiving system, the application layer would be responsible for passing the request to the appropriate application or service on that system. In our example, we will assume that you are sitting at COMPUTER1 and you have typed the address of SERVER1 into your web browser to create an HTTP request.

Layer 6: The Presentation Layer

After the request is made, the application layer passes the data down to the presentation layer, where it is formatted so that the data (or request) can be interpreted by the receiving system. When the presentation layer receives data from the application layer, it makes sure the data is in the proper format—if it is not, the presentation layer converts the data accordingly. On the receiving system, when the presentation layer receives network data from the session layer, it makes sure the data is in the proper format and once again converts it if it is not.

Formatting functions that could occur at the presentation layer include compression, encryption, and ensuring that the character code set can be interpreted on the other side. For example, if we choose to compress our data from the application that we are using, the application layer will pass that request to the presentation layer, but it will be the presentation layer that does the compression. Now, at some point, this data must be decompressed so that it can be read. When the data reaches the presentation layer of the receiving computer, it will decompress the data and pass it up to the application layer.

Layer 5: The Session Layer

The session layer manages the dialog between computers. It does this by establishing, managing, and terminating communications between two computers. When a session is established, three distinct phases are involved. In the establishment phase, the requestor initiates the service and the rules for communication between the two systems. These rules could include such things as who transmits and when, as well as how much data can be sent at a time. Both systems must agree on the rules; the rules are like the etiquette of the conversation. Once the rules are established, the data transfer phase begins. Both sides know how to talk to each other, what are the most efficient methods to use, and how to detect errors, all because of the rules defined in the first phase. Finally, termination occurs when the session is complete, and communication ends in an orderly fashion.

In our example, COMPUTER1 creates a session with SERVER1 at this point, and they agree on the rules of the conversation.

Layer 4: The Transport Layer

The transport layer handles functions such as reliable and unreliable delivery of the data. For reliable transport protocols, the transport layer works hard to ensure reliable delivery of data to its destinations. On the sending system, the transport layer is responsible for breaking the data into smaller parts, known as segments, so that if retransmission is required, only the missing segments will be sent. Missing segments are detected when the transport layer receives acknowledgments (ACKs) from the remote system upon receiving the packets. At the receiving system, the transport layer is responsible for opening all of the packets and reconstructing the original message.

Another function of the transport layer is segment sequencing. Sequencing is a connection-oriented service that takes segments that are received out of order and resequences them in the right order. For example, if I send you five packets and

exam Watch

TCP is an example of a transport layer protocol responsible for reliable delivery, whereas User Datagram Protocol (UDP) is an example of a transport layer protocol responsible for unreliable delivery.

you receive the packets in this order (by their sequence number): 3, 1, 4, 2, 5, the transport layer will read the sequence numbers and assemble them in the correct order.

The transport layer also enables the option of specifying a "service address," known as a *port address*. The port address allows the services or applications that are running on the systems to specify what application the request came from and what application the request is

INSIDE THE EXAM

Connection-Oriented Communication

Connection-oriented communication ensures reliable delivery of data from the sender to the receiver. When establishing these services, the protocol must perform some sort of handshaking function. Handshaking takes place at the beginning of a communication session. During this process, the two computers determine the rules for communication, such as transmission speed and which ports to use. Handshaking also determines the proper way to terminate the session when finished. This ensures that communication ends in an orderly manner.

A session is a reliable dialog between two computers. Because connection-oriented services can provide reliable communication, they are used when two computers need to communicate in a session. Sessions are maintained until the two computers decide that they are finished communicating. A session is just like a telephone call. You set up a telephone call by dialing (handshaking), speak to the other person (exchange data), say "Goodbye," and hang up when finished.

Connectionless Communication

Connectionless communication is a form of communication in which the sending system does not "introduce" itself—it just fires the data off. Also, the destination computer does not notify the source when the information is received. This type of communication can be unreliable because there is no notification to guarantee delivery. Connectionless communication can be faster than connection-oriented communication because the overhead of managing the session is not there, and after the information is sent, there is no second step to ensure it was received properly.

headed for by having each application use a unique port address on the system. All modern operating systems run many programs at once, and each network program has a unique service address. Service addresses that are well defined (by networking standards, for example) are called well-known addresses. Service addresses also are called sockets or ports by protocols such as TCP/IP.

At this point in our example, the request is broken into segments in preparation for being delivered across the network, and transport layer information (such as the transport protocol being used and any additional transport information) is appended to the request. In this example, because we are dealing with a TCP/IP application, the source port and destination port are added.

Layer 3: The Network Layer

The network layer is responsible for managing logical addressing information in the packets and the delivery, or routing, of those packets by using information stored in a routing table. The routing table is a list of available destinations that are stored in memory on the routers (more on routing in Chapter 7).

The network layer is responsible for working with logical addresses. Logical addresses uniquely identify a system on the network, and at the same time identify the network that the system resides on. This is unlike a MAC address (the physical address burned into the network card), because a MAC address just gives the system a unique address and does not specify or imply what network the system lives on. The logical address is used by network-layer protocols to deliver the packets to the correct network.

exam Watch

Remember that layer 3 of the OSI model handles logical addressing and routing. An example of a logical address is an IP address, which takes the form of 192.168.3.24. An IP address is also known as a layer-3 address.

In our example, the request is coming from a web browser and is destined for a web server, both of which are applications that run on TCP/IP. At this point, the network layer will add the source address (the IP address of the sending system) and the destination address (the IP address of the destination system) to the packet so that the receiving system will know where the packet came from.

Layer 2: The Data Link Layer

The data link layer is responsible for converting the data from a packet to a pattern of electrical bit signals that will be used to send the data across the communication medium. On the receiving system, the electrical signals will be converted to packets

by the data link layer and then passed up to the network layer for further processing. The data link layer is divided into two sublayers:

- **Logical link control (LLC)** This is responsible for error correction and control functions.
- **Media Access Control (MAC)** This determines the physical addressing of the hosts. It also determines how the host places traffic on the medium—for example, CSMA/CD versus token passing.

The MAC sublayer maintains physical device addresses (commonly referred to as MAC addresses) for communicating with other devices on the network. These physical addresses are burned into the network cards and constitute the low-level address used to determine the source and destination of network traffic.

exam Watch

For the Network+ exam, remember that a MAC address is the physical address assigned to the network card and is known as a layer-2 address. An example of a MAC address is 00-02-3F-6B-25-13.

In our example, once the sending system's network layer appends the IP address information, the data link layer will append the MAC address information for the sending and receiving systems. This layer will also prepare the data for the wire by converting the packets to binary signals. On the receiving system, the data link layer will convert the signals passed to it by the physical layer to data and then pass the packets to the network layer for further processing.

Note for the exam that the network access methods and architectures you learned about in the last chapter run at layer 2 of the OSI model. For example, Ethernet and Token Ring network architectures are defined at layer 2 of the OSI model.

Layer 1: The Physical Layer

The bottom layer of the OSI hierarchy is concerned only with moving bits of data on and off the network medium. This includes the physical topology (or structure) of the network, the electrical and physical aspects of the medium used, and encoding and timing of bit transmission and reception.

In our example, once the network layer has appended the logical addresses and passed the data to the data link layer, where the MAC addresses have been appended and the data was converted to electrical signals, the data is then passed to the physical layer so that it can be released on the communication medium. On the receiving system, the physical layer will pick the data up off the wire and pass it to

exam Watch

Remember for the Network+ exam that anything that works with the electrical signal runs at layer 1 of the OSI model. This includes the network cables and connectors you learned about in the last chapter.

the data link layer, where it will ensure that the signal is destined for that system by reading the destination MAC address.

Data Encapsulation

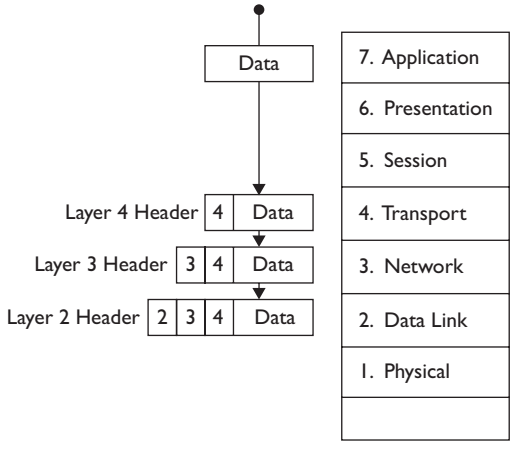
The term *data encapsulation* refers to the fact that as data is passed down the seven layers of the OSI model header information is added to the message. For example, when the information reaches layer 4 of the OSI model, a layer-4 header is added, which contains protocol information for that layer, such as the port number. On the sending system, the layer-4 header is added and then the data is passed down to layer 3, where the layer-3 header is added to the left side of the data and layer-4 header. The layer-3 header contains the layer-3 protocol information, such as the layer-3 source and destination address. Once the layer-3 header is applied, the message is then passed down to layer 2, where the layer-2 header is assigned, and contains the source and destination MAC addresses (layer-2 addresses).

On the receiving system, the message is passed up the OSI model. The receiving system strips the layer-2 header off and reads the destination MAC address to ensure this system is the destination of the message. Once the layer-2 header is read, the message is then passed up to the layer-3 protocol, which reads the layer-3 header (as shown in Figure 2-6). This process continues up the seven layers of the OSI model.

Now that you have been introduced to the seven-layer OSI model, let's try an exercise to put your newfound knowledge to the test.

FIGURE 2-6

Each layer of the OSI model adds a header.



EXERCISE 2-1

Mixing and Matching OSI Model Definitions

In this exercise, you will take a look at some terms and match them with their appropriate definitions. This exercise is designed to give you the opportunity to identify the purpose of each layer of the OSI model.

Definition	Layer
_____ Responsible for the logical addressing and delivery of the packets.	A. Session
_____ Responsible for formatting the message.	B. Physical
_____ Responsible for physical addressing and converting the data packets to electrical signals.	C. Application
_____ Responsible for creating, managing, and ending a dialog.	D. Network
_____ Responsible for reliable delivery, sequencing, and breaking the message into packets.	E. Data link
_____ Responsible for placing or removing the signal on and off the wire.	F. Presentation
_____ Responsible for initiating or receiving the network request.	G. Transport

Once you have matched the previous list of layers with a definition, review the following for the answers:

Definition	Layer
D Responsible for the logical addressing and delivery of the packets.	A. Session
F Responsible for formatting the message.	B. Physical
E Responsible for physical addressing and converting the data packets to electrical signals.	C. Application
A Responsible for creating, managing, and ending a dialog.	D. Network
G Responsible for reliable delivery, sequencing, and breaking the message into segments.	E. Data link
B Responsible for placing or removing the signal on and off the wire.	F. Presentation
C Responsible for initiating or receiving the network request.	G. Transport

Protocols and the OSI Layers

Different protocols work at different levels of the OSI model. Here, we look at a few of the main protocols for this exam, apply them to the OSI model, and see how they fit in the OSI model's seven layers. For more information on protocols and services, check out Chapter 4.

IPX IPX is an extremely fast, streamlined protocol that is not connection oriented. IPX was once fairly common because of its widespread use on Novell NetWare. This is a routable protocol that is located at the network layer of the OSI model. Because it is also an unreliable connectionless transport, IPX also applies to layer 4—the transport layer. Remember, unreliable means data is sent without acknowledgment of receipt, and connectionless means that a session is not established before transmitting. IPX is capable of being run over both Ethernet and Token Ring networks using the appropriate network interface card (NIC). For a number of years, IPX over Ethernet was the default use of NICs.

exam Watch

Although IPX runs at layer 3 (network layer) and layer 4 (transport layer), the Network+ exam places it at layer 3.

SPX Sequenced Packet Exchange (SPX) is a transport protocol used by IPX for connection-oriented communication. It is responsible for breaking the message into manageable packets and ensuring the data reaches the destination. SPX is equivalent to TCP in the TCP/IP protocol suite. Because SPX runs at the transport layer, it is considered a layer-4 protocol.

IP The Internet Protocol (IP) in the TCP/IP protocol suite performs the same routing functions that IPX does for the IPX/SPX protocol suite. IP is responsible for the logical addressing and routing of messages across the network. It does not ensure the delivery of the packets; that is the responsibility of higher-layer protocols, such as TCP.

The logical address that IP uses is known as an IP address and it looks similar to 192.168.3.200—which is different from the physical address (MAC address), which looks like 00-02-3F-6B-25-13. The logical address is responsible for identifying the network the system

exam Watch

IP is a network-layer protocol and is responsible for logical addressing—as a result, an IP address is referred to as a layer-3 address.

resides on, along with an address for the system, whereas a MAC address is flat and identifies only the physical system on the LAN—not "where" the system resides.

IP is fully capable of running over either Token Ring or Ethernet networks, as long as an appropriate NIC is used. IP over Ethernet is the most common implementation in networking today, because Ethernet is much less expensive than Token Ring and because TCP/IP is used widely on the Internet.

TCP The Transmission Control Protocol (TCP) is a transport-layer protocol that is responsible for breaking the data into manageable packets and ensuring that the packets reach their destination. TCP is considered a connection-oriented protocol, which means that it relies on a session being established first. This is different from a connectionless communication, which just sends the data out and if it reaches the destination, great; if not, no big deal. With connection-oriented protocols, a session is established through introductions. ("Hi, I'm Glen Clarke. Nice to meet you, I am going to send you some data.") Connection-oriented protocols will monitor that session to ensure that the packets have reached their destination.

UDP The User Datagram Protocol (UDP) is part of the TCP/IP protocol suite and is similar to TCP. When you send data on a TCP/IP network and you need a connection-oriented conversation, the TCP protocol is used. But what protocol do we use if we want to have a connectionless, unacknowledged conversation? UDP. Both TCP and UDP are layer-4 protocols. IP is used to deliver both types of data, but TCP and UDP determine whether the delivery is connection-oriented or not.

exam Watch

TCP and UDP run at the transport layer of the OSI model and are therefore considered layer-4 protocols.

NFS The Network File System (NFS) is a protocol for file sharing that enables a user to use network disks as though they were connected to the local machine. NFS was created by Sun Microsystems for use on Solaris, Sun's version of UNIX. NFS is still used frequently in the UNIX and Linux worlds (it is used universally by the UNIX community), and is available for use with nearly all operating systems. Vendor and third-party software products enable other operating systems to use NFS. It has gained acceptance with many companies and can be added to nearly any operating system. In addition to file sharing, NFS enables you to share printers. It is located in the application layer of the OSI model and is considered a member of the TCP/IP protocol suite. The primary reason to use the NFS protocol is to access resources located on a UNIX server or to share resources with someone working on a UNIX workstation.

SMB and Novell NCP Microsoft's Server Message Block (SMB) and Novell's NetWare Core Protocol (NCP) are protocols that are implemented in redirectors. A *redirector* is software that intercepts requests, formats them according to the protocol in use, and passes the message to a lower-level protocol for delivery. Redirectors also intercept incoming messages, process the instructions, and pass them to the correct upper-level application for additional processing.

SMB and NCP are used primarily for file and printer sharing in Microsoft and Novell networks, respectively, and are considered application-layer protocols.

exam Watch

SMTP is an application-layer protocol for sending e-mail on the Internet.

SMTP The Simple Mail Transport Protocol (SMTP) is the protocol for sending Internet e-mail messages. SMTP uses a well-defined syntax for transferring messages. An SMTP session includes initializing the connection, sending the destination e-mail address, sending the source e-mail address, sending the subject, and sending the body of the e-mail message.

FTP and TFTP The File Transfer Protocol (FTP) is a standardized method of transferring files between two machines. FTP is a connection-oriented protocol, which means that the protocol verifies that packets successfully reach their destinations.

The Trivial File Transfer Protocol (TFTP) has the same purpose and function as FTP, except that it is not a connection-oriented protocol and does not verify that packets reached their destinations. By not verifying that data has been successfully transferred to its destination and therefore requiring less overhead to establish and maintain a connection, TFTP is able to operate faster than FTP. TFTP has no authentication mechanism, whereas FTP can require a user name and password.

exam Watch

TCP/IP, IPX/SPX, AppleTalk, and DECnet are routable protocols; NetBEUI and DLC are not.

DECnet DECnet is a proprietary protocol developed by the Digital Equipment Corporation for use primarily in wide area networks (WANs). You can run DECnet on an Ethernet network, but it is done infrequently. DECnet is a routable protocol.

DLC Data Link Control (DLC) is not a common protocol. This nonroutable protocol was sometimes used to connect Windows NT servers to printers.

EXERCISE 2-2

Viewing Protocol Information with Network Monitor

In this exercise, you will install a network monitoring tool known as Network Monitor that comes with Windows servers, and you will look at network traffic that was captured previously in a file. In this exercise, a user has provided a credit card number to a website and you have captured the traffic. Your end goal is to find the credit card number in the packet. Figure 2-7 shows the user supplying the credit card number on a webpage.

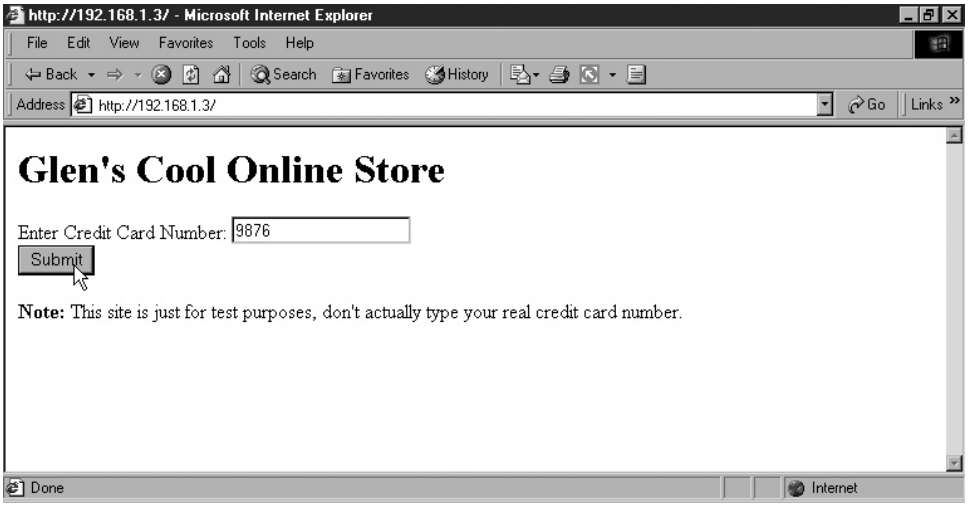
Let's start the exercise by installing the Network Monitor software on your Windows Server 2003 system.

Installing Network Monitor on a Windows Server

1. Ensure you are on the 2003ServerA VM.
2. Choose Start | Control Panel | Add/Remove Programs.

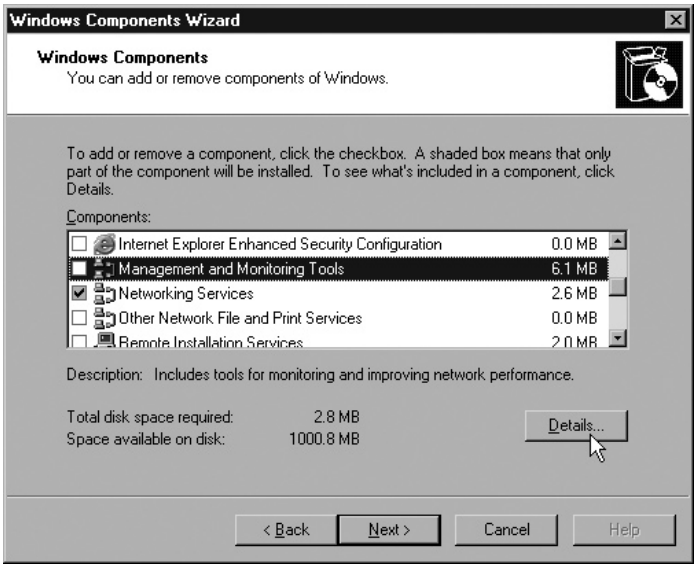
FIGURE 2-7

A user typing a credit card number into an unsecure website

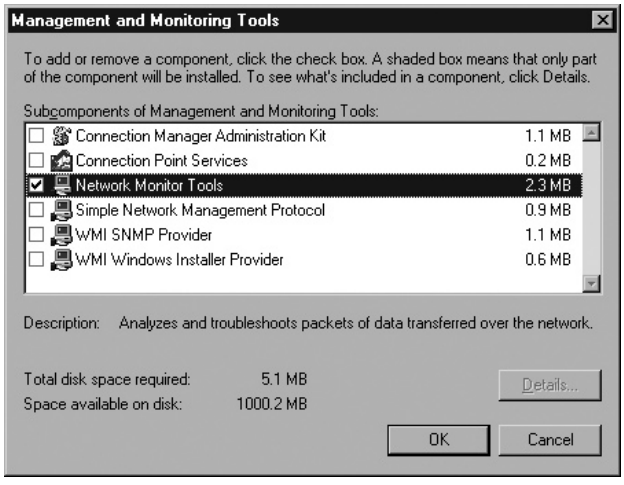


3. In the Add/Remove Programs dialog box, choose Add/Remove Windows Components on the left side.

4. In the Windows Components Wizard, scroll down to find Management And Monitoring Tools. Highlight Management And Monitoring Tools, and click Details.



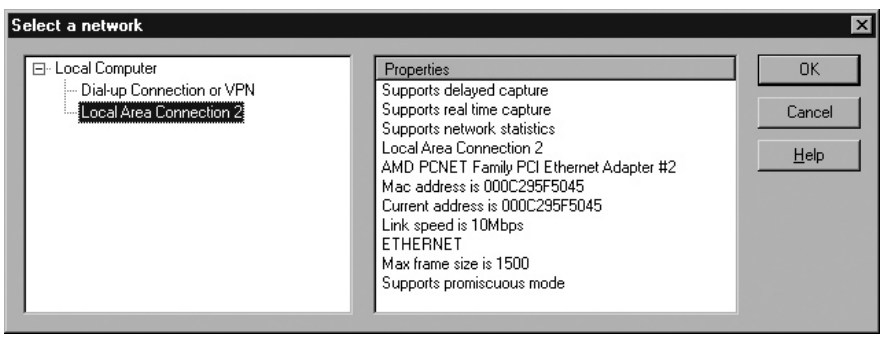
5. In the Management And Monitoring Tools dialog box, select the Network Monitor Tools check box.



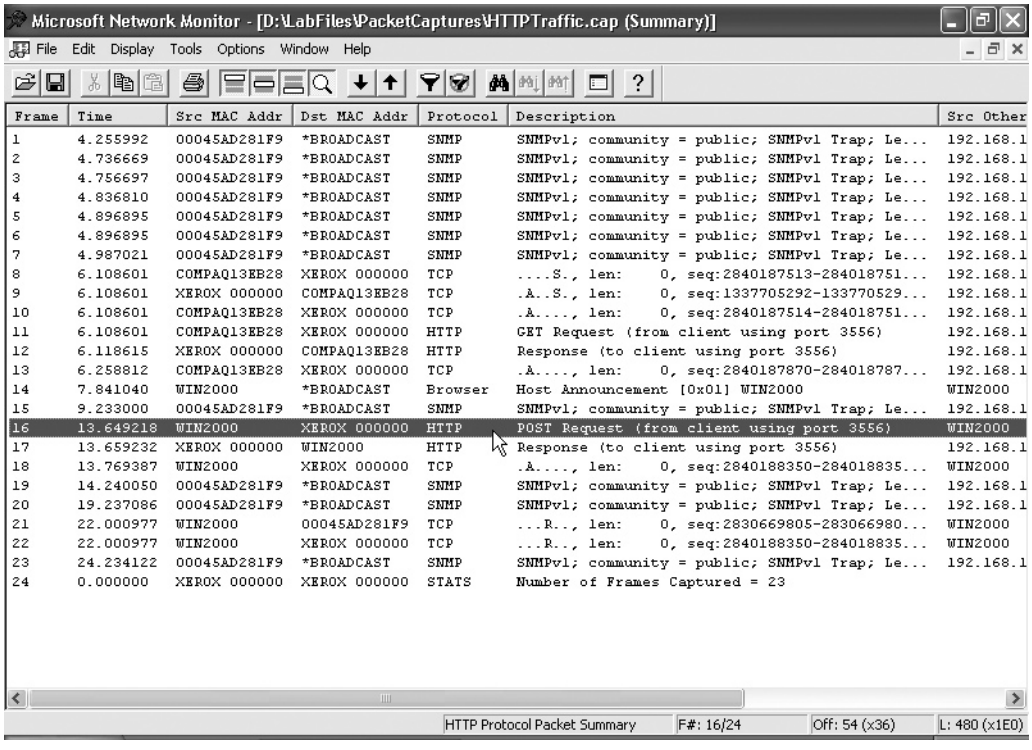
6. Click OK. You may be asked for the Windows Server CD.
7. When the file copy is complete, click Finish.
8. Click Close.
9. Close the Control Panel.

Viewing Packet Data with Network Monitor

1. To start Network Monitor, choose Start | All Programs | Administrative Tools | Network Monitor.
2. When you start Network Monitor, you may be asked to select a network (which means choosing your network card). Expand Local Computer on the left, and then select the local area connection that represents your network card.

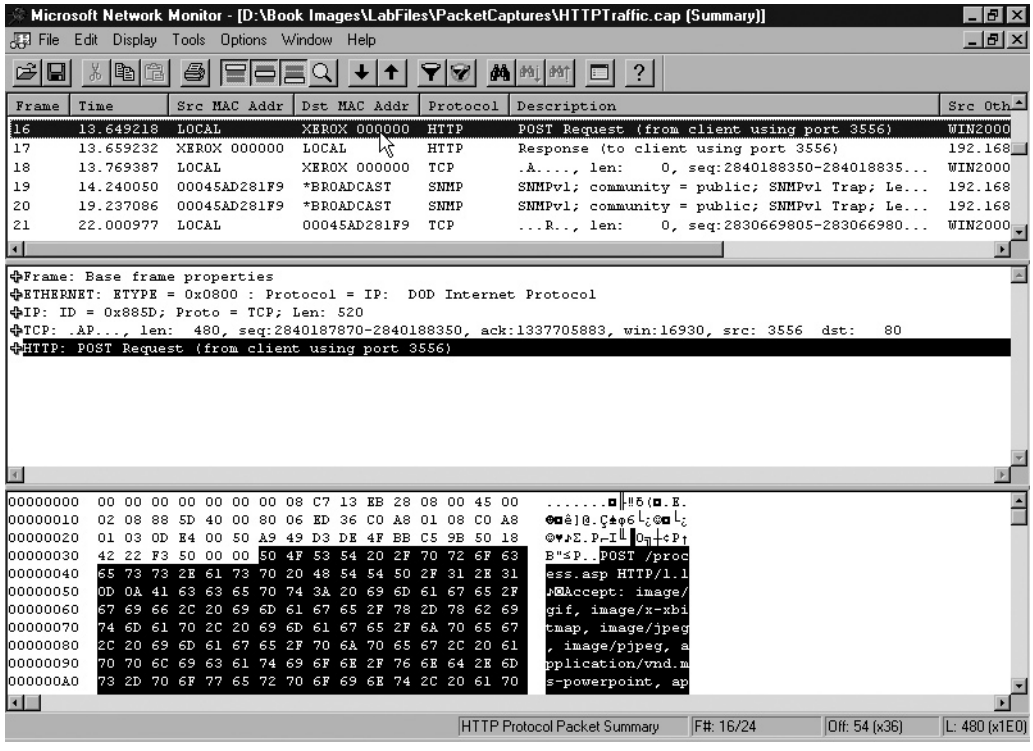


3. Once the network card has been selected, you should have Network Monitor on the screen in front of you. You want to view network traffic that was captured previously, so choose File | Open.
4. In the Open dialog box, open the HTTPTraffic.cap file located in the LabFiles\PacketCaptures folder.
5. The contents of the packet capture are displayed. Notice that there are 24 frames (numbers listed down the left) captured and that frame 16 is the actual HTTP Post Request, which is the form's information posted to the server. This is the phase where the credit card number was submitted. We will use frame 16 as our learning tool to view network traffic.



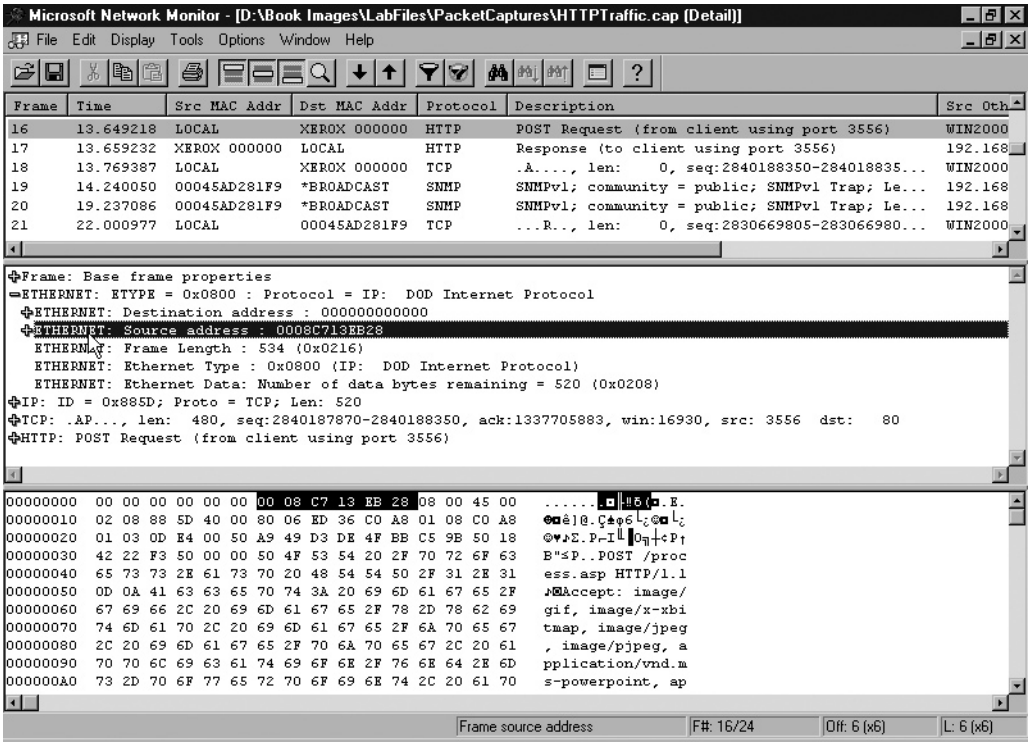
Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other
1	4.255992	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
2	4.736669	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
3	4.756697	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
4	4.836810	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
5	4.896895	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
6	4.896895	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
7	4.987021	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
8	6.108601	COMPAQ13EB28	XEROX 000000	TCP	....S., len: 0, seq:2840187513-284018751...	192.168.1
9	6.108601	XEROX 000000	COMPAQ13EB28	TCP	.A..S., len: 0, seq:1337705292-133770529...	192.168.1
10	6.108601	COMPAQ13EB28	XEROX 000000	TCP	.A...., len: 0, seq:2840187514-284018751...	192.168.1
11	6.108601	COMPAQ13EB28	XEROX 000000	HTTP	GET Request (from client using port 3556)	192.168.1
12	6.118615	XEROX 000000	COMPAQ13EB28	HTTP	Response (to client using port 3556)	192.168.1
13	6.258812	COMPAQ13EB28	XEROX 000000	TCP	.A...., len: 0, seq:2840187870-284018787...	192.168.1
14	7.841040	WIN2000	*BROADCAST	Browser	Host Announcement [0x01] WIN2000	WIN2000
15	9.233000	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
16	13.649218	WIN2000	XEROX 000000	HTTP	POST Request (from client using port 3556)	WIN2000
17	13.659232	XEROX 000000	WIN2000	HTTP	Response (to client using port 3556)	192.168.1
18	13.769387	WIN2000	XEROX 000000	TCP	.A...., len: 0, seq:2840188350-284018835...	WIN2000
19	14.240050	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
20	19.237086	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
21	22.000977	WIN2000	00045AD281F9	TCP	...R.., len: 0, seq:2830669805-283066980...	WIN2000
22	22.000977	WIN2000	XEROX 000000	TCP	...R.., len: 0, seq:2840188350-284018835...	WIN2000
23	24.234122	00045AD281F9	*BROADCAST	SNMP	SNMPv1; community = public; SNMPv1 Trap; Le...	192.168.1
24	0.000000	XEROX 000000	XEROX 000000	STATS	Number of Frames Captured = 23	

6. Double-click frame 16 to view the details of the traffic (shown in the accompanying illustration).



7. The window is divided into three panes; the top pane is the summary pane listing all the frames, the middle pane is the detail pane showing your packet details, and the bottom pane shows the hex data for that frame. Ensure that frame 16 is still selected in the summary pane so that you can investigate your packet.

8. In the detail pane (middle part of the screen), double-click Ethernet, which will expand the Ethernet section showing you the source and destination Ethernet addresses or MAC addresses (shown in the accompanying illustration).



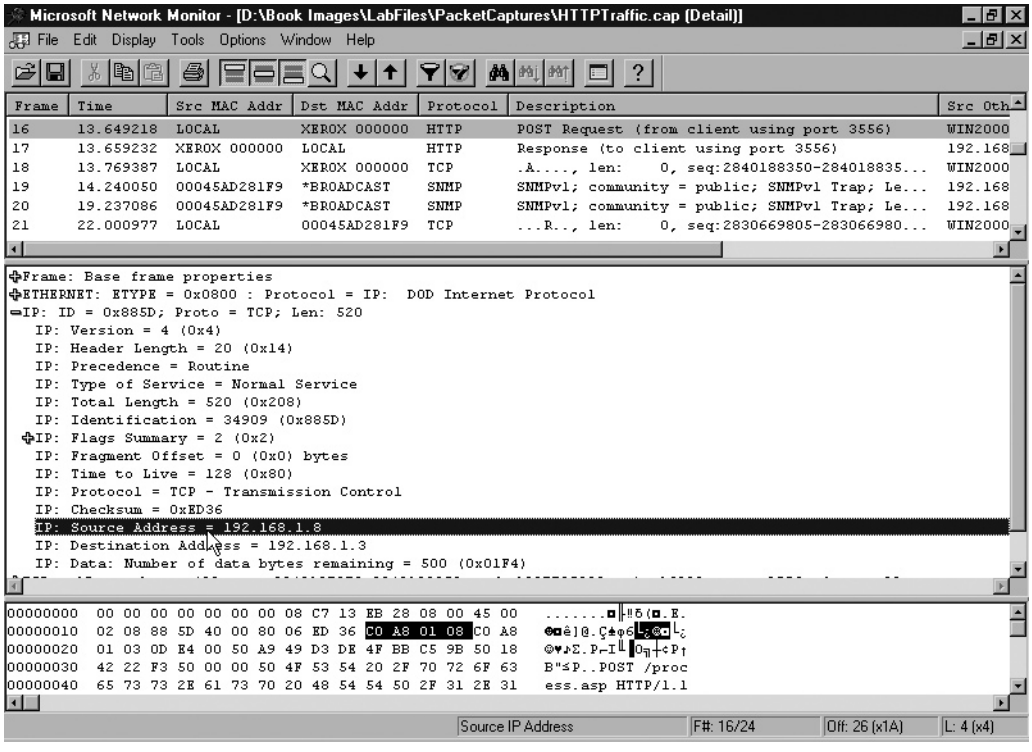
9. Record the source MAC address, which is the system that sent the packet, in the blanks.

   Source MAC address: _____

   What layer of the OSI model does this information pertain to? _____

10. Below the Ethernet section is the protocol information. What layer-3 protocol is this network traffic using? _____

11. If you answered IP in the preceding question, you are correct! If you double-click the IP section, you will see what layer-3 addresses (IP address) are the source of the packet and the destination of the packet.



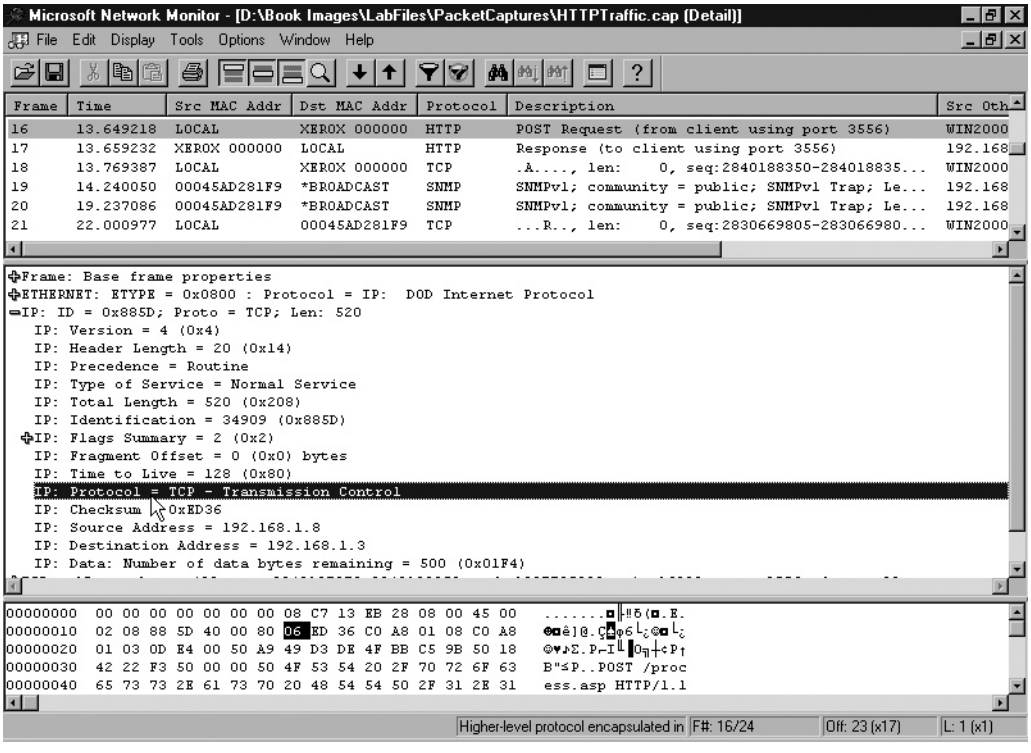
12. Fill in the following information:

Where is the packet headed? _____

Where did the packet come from? _____

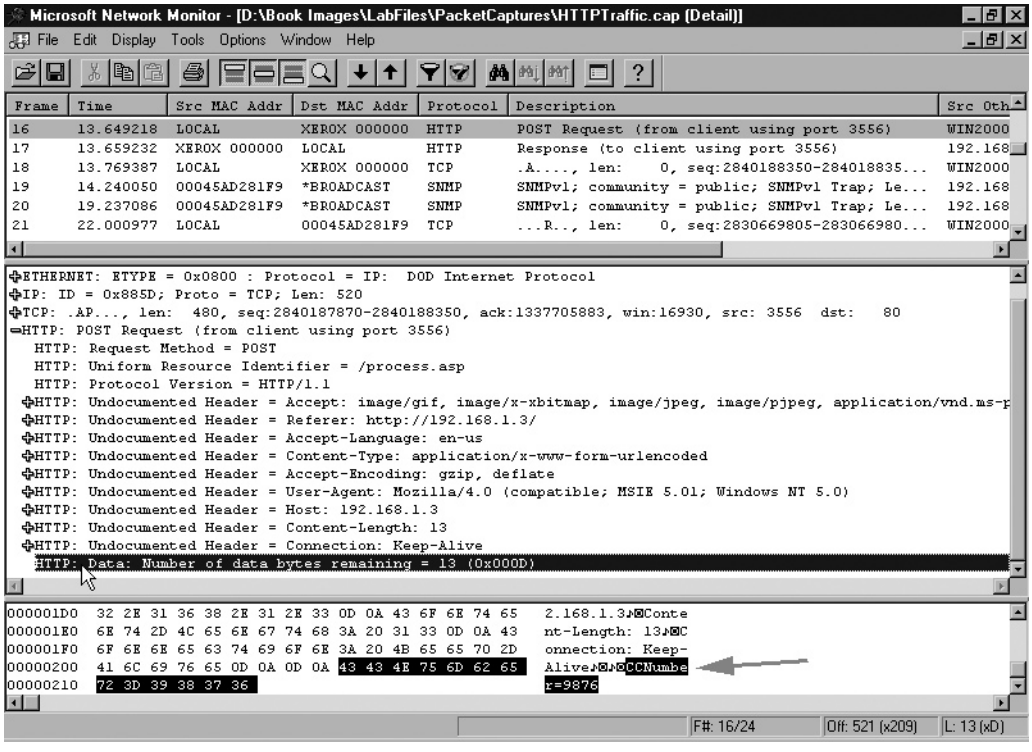
Hint: View the source and destination addresses.

13. You also can see what transport protocol was used by IP to deliver this packet. Two lines above the source IP address, you can see that IP is using TCP, a connection-oriented layer-4 protocol, to ensure that the packet reaches the destination (shown in the accompanying illustration).



14. If you double-click the IP heading, you will collapse the IP details. Let's look at the application protocol information for this packet. You want to see the credit card number that was typed into the webpage. In the details pane, double-click HTTP to expand the detailed application information.

15. Select the last piece of information for HTTP, which is the HTTP: Data: line. To view the data that was typed into the browser, look in the bottom-right area of the screen.



16. What was the credit card number? _____

17. Close Network Monitor.

This exercise has shown you how to view layer-2 information in a packet, such as the source and destination MAC addresses. It has also shown you how to view logical address information, such as the source and destination IP addresses, which were found with layer-3 information. You also saw how the layer-3 protocol (IP) relies on TCP to ensure delivery of the information. Finally, you viewed the application information that was submitted with the request. This will hopefully show you why it is important to ensure that you are using an encryption protocol to encrypt the data typed into an application.

TABLE 2-1

OSI Layers for Popular Protocols and Services

OSI Layer	Protocols, Services, Methods, and Layers
Application	FTP, SMTP, Telnet
Presentation	JPEG, GIF, MPEG
Session	NFS, RPC
Transport	TCP, UDP, SPX, IPX
Network	IPX, IP
Data Link	Ethernet, Token Ring
Physical	Twisted-pair, thinnet coax, AUI, network interface card

It is important to understand the protocols, services, and applications that we deal with every day and what layer of the OSI model those products may be working with. Table 2-1 summarizes some of the popular protocols, services, and applications that are found in networking environments and specifies what layer of the OSI model they run at.

EXERCISE 2-3

Analyzing Network Traffic

Your manager has been recording network traffic to your web server and has noticed that someone has been submitting fake data into the online store. She wants you to open one of the packet captures stored in Lab2.cap (located in your LabFiles\PacketCaptures folder) and analyze one of the packets. She would like you to report back to her the following information:

Source MAC Address: _____

Source IP Address: _____

Destination IP Address: _____

Fake Credit Card Number Used: _____

If you have trouble with this lab, look back to the exercise walk-through you did to learn where to find information about layer-2 and layer-3 addresses and also where to find the specific application data.

Exercise Answer:

After you have opened the packet capture file of lab2.cap, you would focus on the Ethernet section to find the MAC address, the IP section to find the source and destination IP addresses, and the HTTP section to find out the fake credit card number that was submitted. You should have come up with the following answers:

Source MAC Address: **00119520028C**

Source IP Address: **192.168.1.6**

Destination IP Address: **192.168.1.3**

Fake Credit Card Number Used: **5678**

CERTIFICATION OBJECTIVE 2.03

802 Project Standards

The Institute of Electrical and Electronics Engineers (IEEE) is a large and respected professional organization that is also active in defining standards. The 802 committee of the IEEE defines one set of standards dear to the hearts of most network professionals. Twelve subcommittees of the 802 committee define low-level LAN and WAN access protocols. Most of the protocols defined by the 802 committee reside in the physical and data link layers of the OSI model.

IEEE 802 Categories

As the use of LANs increased, standards were needed to define consistency and compatibility among vendors. The IEEE began a project in February 1980, known as Project 802 for the year and month it began. IEEE 802 is a set of standards given to the various LAN architectures, such as Ethernet, Token Ring, and ArcNet, by the LAN standards committee. The goal of the committee was to define more of the OSI's data link layer, which already contained the LLC and MAC sublayers. Several 802 subcommittee protocols are at the heart of PC networking. Although there are a number of 802 project categories, the exam focuses on only a few of them, which are discussed in this section.

802.3 Based on the original Ethernet network from DIX (Digital-Intel-Xerox), 802.3 is the standard for Ethernet networks today. The only difference between 802.3 Ethernet and DIX Ethernet V.2 is the frame type. The two Ethernet networks can use the same physical network, but devices on one standard cannot communicate with devices on the other standard.

exam Watch

Remember that Ethernet is defined by the IEEE 802.3 standard.

The MAC sublayer uses carrier sense multiple access with collision detection (CSMA/CD) for access to the physical medium. CSMA/CD keeps devices on the network from interfering with one another when trying to transmit. To reduce collisions, CSMA/CD devices listen to the network before transmitting. If the network is "quiet" (no other devices are transmitting), the device can send its data. Because two devices can think the network is clear and start transmitting at the same time (which would result in a collision), all devices listen as they transmit. If a device detects another device transmitting at the same time, a collision occurs. The device stops transmitting and sends a signal to alert other nodes about the collision. Then, all the nodes stop transmitting and wait a random amount of time before they begin the process again.

CSMA/CD doesn't stop collisions from happening, but it helps manage the situations when they do occur. In fact, collisions are a normal part of Ethernet operation. You need to become concerned only when collisions begin to occur frequently.

exam Watch

Make sure that you are familiar with all of the Ethernet project categories in Table 2-2 for the exam.

Ethernet has evolved over the years to include a number of popular specifications. These specifications are based, in part, on the media variety they employ, such as coaxial, twisted-pair, and fiber-optic cabling.

- The 10Base5 specification, commonly referred to as thicknet, was the original Ethernet specification. It has a maximum distance of 500 meters (approximately 1640 feet) with a maximum speed of 10 Mbps.
- The 10Base2 specification, commonly referred to as thinnet, uses a thinner coaxial cable than 10Base5. It has a maximum distance of 185 meters (approximately 607 feet) with a maximum speed of 10 Mbps.
- The 10BaseT specification uses twisted-pair cabling with a maximum distance of 100 meters (approximately 328 feet) with a speed of 10 to 100 Mbps.

A number of Ethernet standards have been developed in the 802.3 category, as shown in Table 2-2.

TABLE 2-2 Popular Ethernet IEEE 802.3 Project Standards

IEEE Project Standard	Description
802.3	Ethernet (CSMA/CD)
802.3u	Fast Ethernet (100 Mbps)
802.3z	Gigabit Ethernet over fiber-optic cabling or coaxial cabling
802.3ab	Gigabit Ethernet over twisted-pair cabling
802.3ae	10-Gigabit Ethernet

802.5 Although Token Ring was first designed in the late 1960s, IBM's token-passing implementation did not become IEEE standard 802.5 until 1985.

The Token Ring IEEE 802.5 standard passes a special frame known as a token around the network. This token is generated by the first computer that comes online on the Token Ring network. When another workstation wants to transmit data, it grabs the token and then begins transmitting. This computer will send a data frame on the network with the address of the destination computer. The destination computer receives the data frame, modifies it, and sends it on the network back to the destination computer, indicating successful transmission of data. When the workstation has finished transmitting, the token is released back to the network. This ensures that workstations will not communicate on the network simultaneously, as in the CSMA/CD access method.

exam Watch

Remember that Token Ring is defined in the IEEE 802.5 project.

802.11 The IEEE 802.11 standard addresses wireless networking (discussed in Chapter 9). This includes the wireless access point (WAP) devices and the wireless network interface cards (NICs) that are used to send and receive broadcasts from the cell or WAP device.

The WAPs and wireless NICs can be set to use different frequencies to allow for cell overlap. This is not the same technology used by cell phones to manage movement of PCs or mobile devices. The wireless NIC is set to a specific frequency and must be changed manually in order to communicate with another cell. This means that a PC cannot be moved from one cell area to another without changing the frequency, unless, for some reason, the cells operate on the same frequency and have no overlap of coverage area.

Important wireless standards in the IEEE 802.11 category include the following:

- **802.11a** Supports speeds of 54 Mbps at frequencies ranging from 5.725 GHz to 5.850 GHz. 802.11a wireless components are not compatible with 802.11b devices.
- **802.11b** Supports speeds of 11 Mbps at frequency ranges of 2.400 GHz to 2.4835 GHz. 802.11b wireless components are compatible with 802.11g devices, which use an enhancement of the 802.11b standard.

exam Watch

There are other wireless standards in the IEEE 802.11 project category, but these four are the most popular, and you should be familiar with them for the exam.

- **802.11g** Supports speeds of 54 Mbps at the same frequency range as 802.11b, which allows devices from the two standards to coexist. For example, I have an 802.11b wireless access point, but I am connected to it with my 802.11g wireless network card. I am getting only the 11 Mbps transfer rate because it is the lowest common denominator between the two standards.
- **802.11n** A new wireless project that runs at 5 GHz or 2.4 GHz and is backward compatible with 802.11a/b/g standards. The goal of 802.11n is to increase the bandwidth and the range. 802.11n has data transfer rates of over 100 Mbps!

exam Watch

Expect to be asked about the IEEE standards on the exam, especially the ones that pertain to Ethernet, Token Ring, and wireless.

You will need to be familiar with the IEEE 802 projects that have been mentioned, as the exam will focus on those, but you should be familiar with the other 802 standards as well. Table 2-3 lists most of the 802 project standards.

TABLE 2-3

IEEE 802 Project Standards

Project	Description
802.1	Internetworking
802.2	Logical link control
802.3	Ethernet
802.4	Token bus
802.5	Token Ring
802.6	Metropolitan area network (MAN)
802.7	Broadband technology
802.8	Fiber-optic technology
802.9	Voice and data integration
802.10	Network security
802.11	Wireless networking
802.12	Demand priority networking

CERTIFICATION SUMMARY

In this chapter, you have learned about some of the more popular network protocols, such as NetBEUI, IPX/SPX, and TCP/IP. You have learned about the advantages and disadvantages of these protocols, which ones are routable, and which ones are nonroutable.

You have also learned that in order for all of the different manufacturers of networking components to build technologies that will work together, some standards had to be defined. There are two major standards that manufacturers follow: the 802 project models and the OSI model. In this chapter, you looked at each layer of the OSI model and what functions they perform. An easy way to remember the layers (application, presentation, session, transport, network, data link, and physical) is with the sentence, "All People Seem To Need Data Processing."

TWO-MINUTE DRILL

Network Protocols

- ❑ Packets and protocols are the fundamental building blocks of data transmission over the network.
- ❑ Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) is the protocol most commonly used with older versions of Novell NetWare.
- ❑ IPX/SPX is the fastest routable network protocol suite available.
- ❑ The Transmission Control Protocol/Internet Protocol (TCP/IP) is the most common protocol used today. TCP/IP, a routable protocol, is the protocol on which the Internet is built.
- ❑ The NetBIOS Extended User Interface (NetBEUI) is a transport protocol commonly found in smaller peer-to-peer networks.
- ❑ NetBEUI is a nonroutable protocol.
- ❑ AppleTalk is a routable protocol used in Macintosh environments.

The OSI Model

- ❑ The Open Systems Interconnect (OSI) model is a seven-layer model that defines the function of network protocols and devices.
- ❑ The seven layers of the OSI model, from highest to lowest, are application, presentation, session, transport, network, data link, and physical.
- ❑ SMTP, HTTP, Telnet, and FTP are all examples of application-layer (layer 7) protocols.
- ❑ Compression and encryption are examples of functions that can be performed at the presentation layer (layer 6).
- ❑ The session layer (layer 5) is responsible for the creation of sessions and the management of those sessions.
- ❑ The transport layer (layer 4) is responsible for the reliability of the transmission, including breaking the data down into manageable sizes using acknowledgments and packet sequence numbers to ensure that data arrives at the destination and is pieced together in the correct order. Examples of layer-4 protocols are TCP, UDP, and SPX.

- ❑ Layer 3, known as the network layer, performs logical addressing and delivery functions. Examples of layer-3 protocols are IP and IPX.
- ❑ The data link layer, layer 2, is responsible for physical addressing and converting the packets to electrical signals. Any device that works with MAC addresses runs at this layer.
- ❑ The first layer of the OSI model, located at the bottom, is known as the physical layer and is responsible for carrying the signal. Your network media and architectures are defined at this level.
- ❑ An IP address is known as a layer-3 address and looks similar to 192.168.45.6.
- ❑ A MAC address is known as a layer-2 address and looks similar to 00-02-3F-6B-25-13.
- ❑ A port address is known as a layer-4 address and looks similar to 80 (web server port).

802 Project Standards

- ❑ The Institute of Electrical and Electronics Engineers (IEEE) has created project groups that define networking standards.
- ❑ 802.3 is the Ethernet (CSMA/CD) standard.
- ❑ 802.5 defines the Token Ring standard.
- ❑ 802.11 defines the wireless standard.

SELF TEST

The following questions will help you measure your understanding of the material presented in this chapter. Read all the choices carefully because there may appear to be more than one correct answer and you need to choose the best answer.

Network Protocols

1. What is the name given to languages that are used for network communication?
   - A. NIC
   - B. Segment
   - C. Protocol
   - D. Cable
2. Which network protocol did Novell develop for use in its networking environment?
   - A. IPX/SPX
   - B. TCP/IP
   - C. NetBEUI
   - D. DLC
3. Which protocol used on the Internet gives each computer a unique address?
   - A. IPX/SPX
   - B. TCP/IP
   - C. NetBEUI
   - D. DLC
4. Which of the following protocols is a nonroutable protocol?
   - A. IPX/SPX
   - B. TCP/IP
   - C. NetBEUI
   - D. AppleTalk
5. Which protocol was developed by IBM and used primarily in Microsoft workgroup environments?
   - A. NetBEUI
   - B. TCP/IP
   - C. IPX/SPX
   - D. AppleTalk

6. Which protocol configures hosts in zones on the network?
   A. IPX/SPX
   B. TCP/IP
   C. NetBEUI
   D. AppleTalk
7. You are troubleshooting to find out why a client on your NetWare 4.*x* network can communicate only with some of the Novell servers on the network. You have verified that the IPX/SPX protocol is installed; what else would you check?
   A. Ensure that the IP address is configured correctly.
   B. Ensure that all servers and clients are configured for the same frame type.
   C. Ensure that the client has a network card driver loaded.
   D. Ensure that the client software is loaded.

The OSI Model

8. Which of the following is not a layer in the OSI model?
   A. Physical
   B. Transport
   C. Network
   D. Data transmission
9. Which of the following protocols are layer-3 protocols? (Choose two.)
   A. IPX
   B. TCP
   C. IP
   D. SPX
10. Which of the following represents a layer-2 address?
   A. COMPUTER1
   B. 00-02-3F-6B-25-13
   C. 192.168.3.200
   D. www.gleneclarke.com

11. Which of the following functions can be performed at layer 6 of the OSI model? (Select all that apply.)

A. Routing of the message
B. Compression
C. Encryption
D. Converting the message to a format that is understood by the destination

12. Which of the following protocols are transport-layer protocols? (Choose two.)

A. IPX
B. TCP
A. IP
B. SPX

13. Which of the following represents a layer-3 address?

A. COMPUTER1
B. 00-02-3F-6B-25-13
C. 192.168.3.200
D. www.gleneclarke.com

14. Which of the following represents an application-layer protocol?

A. SMTP
B. IP
C. SPX
D. TCP

15. Which layer of the OSI model is responsible for converting the packet to an electrical signal that will be placed on the wire?

A. Layer 1
B. Layer 4
C. Layer 3
D. Layer 2

16. Which protocol in the IPX/SPX protocol suite is responsible for logical addressing and delivery?

A. IP
B. SPX
C. ARP
A. IPX

802 Project Standards

17. Which 802 project standard defines Gigabit Ethernet using fiber-optic cabling?

A. 802.5
B. 802.3z
C. 802.3ab
D. 802.11g

18. Which 802 project standard defines Token Ring?

A. 802.5
B. 802.3z
C. 802.3ab
D. 802.11g

19. Which 802 project standard defines 10-Gigabit Ethernet?

A. 802.3z
B. 802.3ae
C. 802.3ab
D. 802.11g

20. Which 802 project standard defines wireless at speeds of 54 Mbps and a frequency range of 2.4 GHz?

A. 802.11a
B. 802.11b
C. 802.11c
D. 802.11g

SELF TEST ANSWERS

Network Protocols

1. ☑ **C.** A protocol is the network language used by two systems to communicate across the network.
   ☒ **A, B,** and **D** are incorrect because a NIC is a network card, which is not a language—it is a network device. The segment is the term for a part of network cabling on one side of a router or bridge. The cable is not a language; it is the network medium used to carry the signals.
2. ☑ **A.** IPX/SPX is the protocol developed by Novell for use in NetWare environments.
   ☒ **B, C,** and **D** are incorrect—none of them were developed by Novell. TCP/IP is the protocol of the Internet; NetBEUI was developed by IBM and used in Microsoft workgroup environments. DLC is a protocol used to connect to printers.
3. ☑ **B.** TCP/IP is the protocol of the Internet, and each system is assigned a unique IP address.
   ☒ **A, C,** and **D** are incorrect. IPX/SPX is the protocol developed by Novell for use in NetWare environments, NetBEUI was developed by IBM and used in Microsoft workgroup environments, and DLC is a protocol used to connect to printers.
4. ☑ **C.** NetBEUI is a nonroutable protocol.
   ☒ **A, B,** and **D** are incorrect because IPX/SPX, TCP/IP, and AppleTalk are all routable protocols.
5. ☑ **A.** NetBEUI was developed by IBM and used primarily in Microsoft workgroup environments.
   ☒ **B, C,** and **D** are incorrect. TCP/IP is the protocol of the Internet, IPX/SPX was developed by Novell, and AppleTalk was developed by Apple.
6. ☑ **D.** The AppleTalk protocol configures hosts into zones.
   ☒ **A, B,** and **C** are incorrect. IPX/SPX, TCP/IP, and NetBEUI do not use zones to organize nodes on the network.
7. ☑ **B.** Using IPX/SPX and having trouble connecting to some of the servers on the network but not others is a classic description of a communication problem, indicating that the client has the frame type set to something different than that used by the servers. You will need to verify the frame type on all systems and ensure that systems that wish to talk to one another are configured with the same frame type.
   ☒ **A, C,** and **D** are incorrect. A is incorrect because IP addresses have nothing to do with the IPX/SPX protocol. C and D are incorrect because both are describing issues that would arise when connecting to "any" server. In our example, the client can connect to some servers, so the client software and the network card driver must already be loaded.

The OSI Model

8. ☑ **D.** Data transmission is not a layer of the OSI model.
☒ **A, B,** and **C** are incorrect because physical, transport, and network are all layers of the OSI model.

9. ☑ **A** and **C.** IP is the network-layer protocol in the TCP/IP protocol suite, and IPX is the network-layer protocol in the IPX/SPX protocol suite.
☒ **B** and **D** are incorrect because TCP and SPX are transport-layer protocols.

10. ☑ **B.** 00-02-3F-6B-25-13 is an example of a MAC address, which is a layer-2 address.
☒ **A**, **C**, and **D** are incorrect. COMPUTER1 is an example of a NetBIOS name (computer name); 192.168.3.200 is an example of an IP address, which is a layer-3 address; and www.gleneclarke.com is an example of a DNS name.

11. ☑ **B, C,** and **D.** They are all examples of data formatting that is performed at the presentation layer.
☒ **A** is incorrect because the routing of the message is handled by the network layer, which is layer 3.

12. ☑ **B** and **D.** TCP is the transport protocol responsible for reliable delivery in the TCP/IP protocol suite, whereas SPX performs the same function in the IPX/SPX protocol suite.
☒ **A** and **C** are incorrect. IPX and IP are network-layer protocols responsible for the addressing and delivery of data.

13. ☑ **C.** 192.168.3.200 is an example of an IP address that is a layer-3 protocol; thus, this is a layer-3 address.
☒ **A, B,** and **D** are incorrect. COMPUTER1 is a computer name, 00-02-3F-6B-25-13 is an example of a Mac address (layer-2 address), and www.gleneclarke.com is an example of a DNS-style name.

14. ☑ **A.** An application-layer protocol is responsible for initiating some form of request. SMTP is used to send e-mail from server to server.
☒ **B, C,** and **D** are incorrect. IP is a layer-3 address (network layer); SPX and TCP are transport-layer protocols.

15. ☑ **D.** Layer 2 (the data link layer) is responsible for converting the packet to an electrical signal.
☒ **A, B,** and **C** are incorrect. Layer 1 (physical layer) is responsible for placing the signal on the wire, layer 4 (transport layer) is responsible for reliable delivery, and layer 3 (network layer) is responsible for logical addressing, routing, and delivery.

16. ☑ **D.** IPX is responsible for logical addressing and delivery of the message. IPX is similar in function to the IP and UDP protocols found in the TCP/IP protocol suite.
☒ **A, B,** and **C** are incorrect. IP is responsible for logical addressing and delivery, but is not found in the IPX/SPX protocol—it is found in the TCP/IP suite. SPX is a transport protocol responsible for reliable delivery, and ARP is an address resolution protocol found in the TCP/IP protocol suite.

802 Project Standards

17. ☑ **B.** Gigabit Ethernet over fiber is defined in the IEEE 802.3z project standard.
☒ **A, C,** and **D** are incorrect. The 802.5 standard defines Token Ring, 802.3ab defines Gigabit Ethernet over twisted-pair, and 802.11g defines wireless at 54 Mbps.

18. ☑ **A.** The IEEE 802.5 project standard defines Token Ring.
☒ **B, C,** and **D** are incorrect. 802.3z defines Gigabit Ethernet over fiber, 802.3ab defines Gigabit Ethernet over twisted-pair, and 802.11g defines wireless at 54 Mbps.

19. ☑ **B.** The IEEE 802.3ae standard defines 10-Gigabit Ethernet.
☒ **A, C,** and **D** are incorrect. 802.3z defines Gigabit Ethernet over fiber, 802.3ab defines Gigabit Ethernet over twisted-pair, and 802.11g defines wireless at 54 Mbps.

20. ☑ **D.** 802.11g defines a wireless standard at 54 Mbps while maintaining compatibility with 802.11b by being on the same frequency.
☒ **A, B,** and **C** are incorrect. 802.11a is at 54 Mbps but is not at a frequency of 2.4 GHz, 802.11b is at 11 Mbps but compatible with 802.11g, because it runs at the same frequency, and both are Wi-Fi compatible. 802.11c is not a wireless standard.