Network Protocols

Terms you'll need to understand:

- √ OSI Reference Model
- √ Application layer
- √ Presentation layer
- √ Session layer
- √ Transport layer
- √ Network layer
- √ Data Link layer
- √ Physical layer
- √ Media Access Control sublayer
- √ Logical Link Control sublayer
- √ IEEE 802 specifications
- √ Redirectors
- √ Protocols: NetBEUI, TCP/IP, XNS, AppleTalk, APPC, X.25, and HDLC

Techniques you'll need to master:

- √ Interpreting the OSI Reference Model and how it relates to protocol suites
- √ Exploring the IEEE's 802 network specifications
- √ Understanding and using redirectors
- √ Comprehending and implementing protocols

To enable networked communications, computers must be able to transmit data among one another. Protocols, agreed-upon methods of communication, make this possible. In this chapter, we discuss the various network protocols and how they make networked communications possible.

In addition, we introduce you to the standards upon which network protocols are based: the Open Systems Interconnection (OSI) Reference Model and the IEEE 802 standards. The OSI Reference Model was developed by the International Standards Organization (ISO) to provide a standardized method for computers to communicate; the Institute of Electrical and Electronic Engineers (IEEE) 802 standards further expanded this model. As always, we provide pointers along the way that will assist you in preparing for the Networking Essentials exam and give you additional resources should you need more details on the topics we discuss in this chapter.

The OSI Reference Model

As the concept of networking became more widespread in the business world, the idea of being able to connect networks and disparate systems became a necessity. For this type of communication to take place, however, there needed to be a standard design. The solution came in 1978 when the ISO released an architecture that would achieve this goal. These specifications were revised in 1984 and became international standards for networked communication. It is important for network administrators to know the history and understand the function of this specification, which is called the OSI Reference Model.

The OSI model presents a layered approach to networking. Each layer of the model handles a different portion of the communications process. By separating such communications into layers, the OSI model simplified how network hardware and software work together. It also eased troubleshooting woes by providing a specific method for how components should function. Now that we know why the model was implemented, let's move on to explore just how it works.

Keep in mind that the OSI model is a completely conceptual reference. Later in the chapter, we'll discuss how protocol suites map to the model to provide network communications.

Learning The Layers

The OSI Reference Model divides networking into seven layers, as shown in Figure 3.1. These layers are described as follows:

- Application layer Provides a set of interfaces for applications to use to gain access to networked services.
- Presentation layer Converts data into a generic format for network transmission; for incoming messages, it converts data from this format into a format that the receiving application can understand.
- Session layer Enables two parties to hold ongoing communications—called sessions—across a network.
- Transport layer Manages the transmission of data across a network.
- Network layer Handles addressing messages for delivery, as well as translates logical network addresses and names into their physical counterparts.

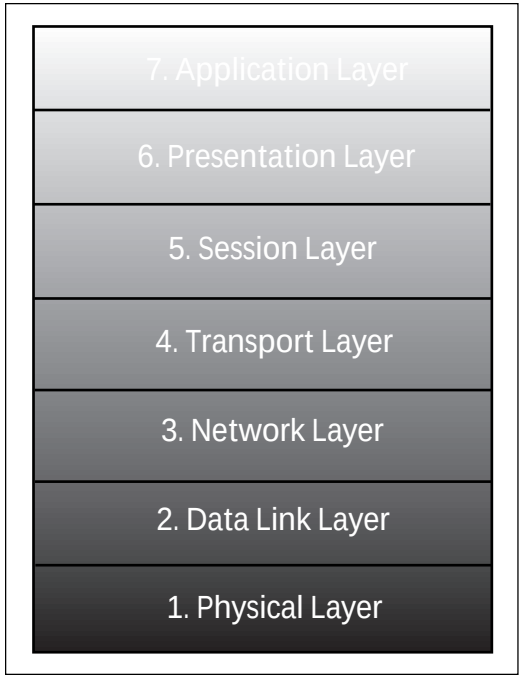

Figure 3.1 The OSI model separates networking functions into seven layers.

- Data Link layer Handles special data frames between the Network layer and the Physical layer.
- Physical layer Converts bits into signals for outgoing messages and converts signals into bits for incoming messages.

It is essential that you know the layers of the OSI model. A great instructor once provided the following mnemonic, which helps you remember the order of these layers: From the bottom up, take the first letter of each layer (PDNTSPA) and assign a more approachable phrase such as "Please Do Not Throw Sausage Pizza Away."

In the following sections, we'll examine each layer of the OSI Reference Model in more detail.

Layer 7: The Application Layer

The Application layer is referred to as the top layer of the OSI Reference Model. This layer allows access to network services—such as networked file transfer, message handling, and database query processing—that support applications directly. This layer also controls general network access, transmission of data from sending applications to receiving applications, and provides error and status information for applications when network errors interfere with service access or delivery.

Layer 6: The Presentation Layer

The Presentation layer manages data-format information for networked communications. Also called the network's translator, it converts outgoing messages into a generic format that can be transmitted across a network. Then, it converts incoming messages from that generic format into one that makes sense to the receiving application. This layer is also responsible for protocol conversion, data encryption and decryption, and graphics commands.

Information sent by the Presentation layer may sometimes be compressed to reduce the amount of data to be transferred (this also requires decompression on the receiving end). It is at this layer that a special software facility known as a redirector operates. The redirector intercepts requests for service and redirects requests that cannot be resolved locally to the networked resource that can handle them.

Layer 5: The Session Layer

The Session layer allows two networked resources to hold ongoing communications, called a session, across a network. In other words, applications on each end of the session are able to exchange data for the duration of the session. This layer manages session setup, information or message exchanges, and tear-down when the session ends. It is also responsible for identification that allows only designated parties to participate in the session, and handles security services to control access to session information.

The Session layer provides synchronization services between tasks at each end of the session. This layer places checkpoints in the data stream, so if communications fail, only data after the most recent checkpoint will need to be retransmitted. The Session layer also manages issues such as who may transmit data at a certain time and for how long, and maintains a connection through transmission of messages that keep the connection active. These messages are designed to keep the connection from being closed down due to inactivity.

Layer 4: The Transport Layer

The Transport layer manages the flow control of data between parties across a network. It does this by segmenting long streams of data into chunks that adhere to the maximum packet size for the networking medium in use. The layer also provides error checks to guarantee error-free data delivery and resequences chunks back into the original data when it is received. In addition, the Transport layer provides acknowledgment of successful transmissions and is responsible for requesting retransmission if some packets arrive with errors.

Layer 3: The Network Layer

The Network layer addresses messages for delivery and translates logical network addresses and names into their physical equivalents. This layer also decides how to route transmissions between computers. To decide how to get data from one point to the next, the Network layer considers other factors, such as quality of service information, alternative routes, and delivery priorities. This layer also handles packet switching, data routing, and network congestion control.

Layer 2: The Data Link Layer

The Data Link layer handles special data frames between the Network and Physical layers. At the receiving end, this layer packages raw data from the

Physical layer into data frames for delivery to the Network layer. A data frame is the basic unit for network traffic as data is sent across the network medium. It is a highly structured format in which data from the upper layers is placed for transmission and from which data is extracted upon receipt and passed on to the upper layers.

Layer 1: The Physical Layer

The Physical layer converts bits into signals for outgoing messages and converts signals into bits for incoming ones. This layer arranges the transmission of a data frame's bits when they are dispatched across the network. The Physical layer manages the interface between a computer and the network medium and tells the driver software and the network interface what needs to be sent across the medium.

That concludes the layer-by-layer discussion of the OSI Reference Model. Now, let's take a look at how the IEEE 802 specifications further standardized network communication.

IEEE 802 Specifications

At roughly the same time the OSI model was developed, the IEEE published the 802 specifications, which defined standards for the physical components of a network. These components, namely network interface cards (NICs) and network media, are also accounted for in the Physical and Data Link layers of the OSI model. The 802 specs defined how network adapters access and transmit information over the network cable.

The 802 specifications fall into 12 distinct categories, each of which has its own number, as described in the following:

- **802.1** Internetworking
- **802.2** Logical Link Control (LLC)
- **802.3** Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) LANs (Ethernet)
- **802.4** Token Bus LAN
- **802.5** Token Ring LAN
- **802.6** Metropolitan Area Network (MAN)
- **802.7** Broadband Technical Advisory Group
- **802.8** Fiber Optic Technical Advisory Group

- **802.9** Integrated Voice and Data Networks
- **802.10** Network Security Technical Advisory Group
- **802.11** Wireless Networks
- **802.12** Demand Priority Access LAN, 100VG-AnyLAN

As previously mentioned, the 802 specification actually expanded the OSI Reference Model. This expansion is at the Physical and Data Link layers, which define how more than one computer can access the network without causing interference with other computers on the network. The 802 standards provide more detail at these layers by breaking the Data Link layer into the following sublayers (see Figure 3.2):

- Logical Link Control (LLC) For error correction and flow control
- Media Access Control (MAC) For access control

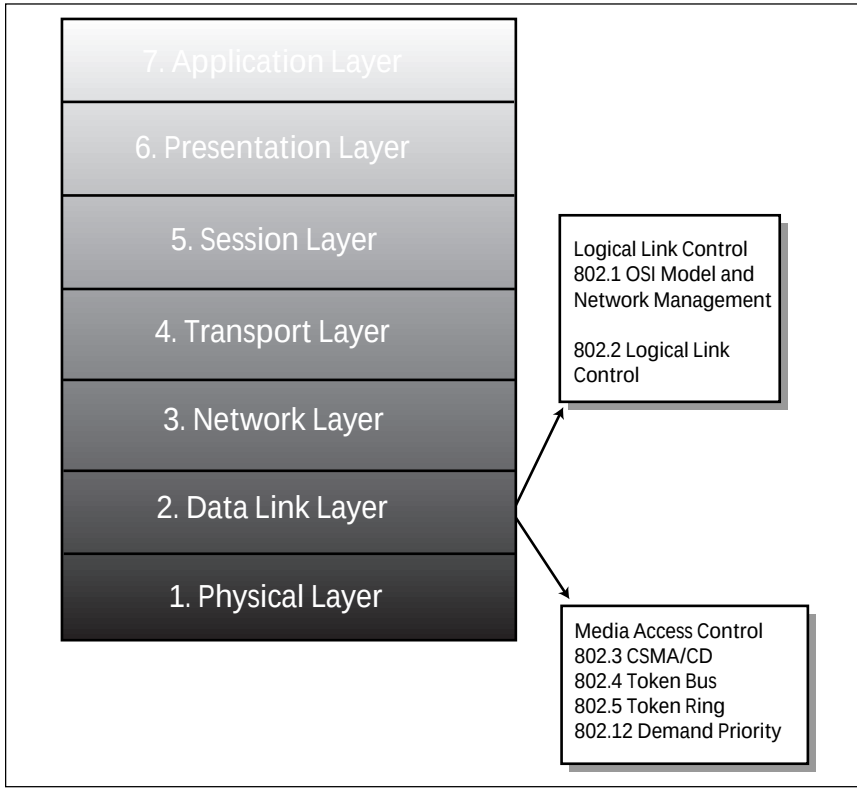

Figure 3.2 The 802 specs within the OSI model.

The Logical Link sublayer (as defined by 802.2) controls data-link communication, and defines the use of logical interface points, called Service Access Points (SAPs), that other computers can use to transfer information from the LLC sublayer to the upper OSI layers.

The Media Access Control sublayer provides shared access for multiple NICs with the Physical layer. The MAC has direct communication with a computer's NIC and is responsible for ensuring error-free data transmission between computers on a network.

This concludes the theoretical discussion of network models. In the following section, we'll discuss how protocol suites are mapped to this model to provide networked communications.

Up And Down The Protocol Stack

In general, most protocols follow the guidelines established by the OSI model. A protocol suite, also called a stack, is a combination of protocols that work together to achieve network communication. These protocol suites are generally broken up into three sections that map to the OSI model: network, transport, and application. Because each layer performs a specific function and has its own rules, a protocol stack often has a different protocol for each of these layers.

Network Protocols

Network protocols provide the following services: addressing and routing information, error checking, requesting retransmissions, and establishing rules for communicating in a particular networking environment. These services are also called link services. Some popular network protocols are:

- DDP (Delivery Datagram Protocol) Apple's data transport protocol that is used in AppleTalk
- IP (Internet Protocol) Part of the TCP/IP protocol suite that provides addressing and routing information
- IPX (Internetwork Packet Exchange) and NWLink Novell's NetWare protocol (and Microsoft's implementation of this protocol, respectively) used for packet routing and forwarding
- NetBEUI Developed by IBM and Microsoft, it provides transport services for NetBIOS

Transport Protocols

In addition, protocol suites also contain transport protocols, which are responsible for ensuring reliable data delivery between computers. Some popular transport protocols are:

- ATP (AppleTalk Transaction Protocol) and NBP (Name Binding Protocol) AppleTalk's session and data transport protocols
- NetBIOS/NetBEUI NetBIOS establishes and manages communications between computers; NetBEUI provides data transport services for that communication
- SPX (Sequenced Packet Exchange) and NWLink Novell's connection-oriented protocol that is used to guarantee data delivery (and Microsoft's implementation of this protocol)
- TCP (Transmission Control Protocol) The portion of the TCP/IP protocol suite that is responsible for reliable delivery of data

Application Protocols

Finally, there are application protocols, which are responsible for application-to-application services. Some popular application protocols are:

- AFP (AppleTalk File Protocol) Apple's remote file management protocol
- FTP (File Transfer Protocol) Another member of the TCP/IP protocol suite that is used to provide file transfer services
- NCP (NetWare Core Protocol) Novell's client shells and redirectors
- NFS (Network File System) A client/server file system protocol primarily used to share directories with Unix systems
- SMB (Server Message Block) A protocol that sits above NetBEUI and NetBIOS that defines and formats commands for information passing between networked computers
- SMTP (Simple Mail Transport Protocol) A member of the TCP/IP protocol suite that is responsible for transferring email
- SNMP (Simple Network Management Protocol) A TCP/IP protocol that is used to manage and monitor network devices

That's it for our discussion of how protocol suites map to the established network standards. We now provide a more detailed look at the protocol suites.

Protocols

As already mentioned, computers must agree on a protocol to be used for any type of communication to take place. The following sections provide more detail on the more common protocols in use today.

NetBEUI

NetBEUI is a simple Network layer transport protocol that was developed to support NetBIOS networks. Like NetBIOS, NetBEUI is not routable, so it really has no place on an enterprise network. NetBEUI is the fastest transport protocol available to Windows NT. It's great for fast transmission, but is not usable across routed networks. Benefits of NetBEUI include: speed, good error protection, ease of implementation, and low memory overhead. Some disadvantages are: It's not routable, it has very little support for cross-platform applications, and it has very few troubleshooting tools available.

TCP/IP

TCP/IP is the most widely used protocol suite in networking today. This is due in part to the vast growth of the global Internet. TCP/IP is able to span wide areas and is very flexible. In addition, it provides cross-platform support, routing capabilities, as well as support for the Simple Network Management Protocol (SNMP), the Dynamic Host Configuration Protocol (DHCP), the Windows Internet Name Service (WINS), the Domain Name Service (DNS), and a host of other useful protocols. However, TCP/IP's rich set of features are provided at the expense of additional overhead, which may make it too cumbersome for some networks or applications.

AppleTalk

It should come as no surprise that the AppleTalk protocol is used for communication with Macintosh computers. By enabling AppleTalk, you allow Mac clients to store and access files located on a Windows NT Server, print to Windows NT printers, and vice versa. An item of note: You must first install the Windows NT Services For Macintosh before you can install AppleTalk. Also, Mac support is only available from an NTFS partition.

APPC

The Advanced Program-to-Program Communication (APPC) protocol, developed by IBM, is a peer-to-peer protocol used in IBM's Systems Network Architecture (SNA) for use on AS/400-series computers.

X.25

X.25 is a set of wide-area protocols that are used in packet-switching networks. It was created to connect remote terminals to mainframes. Although many other wide-area communications types are available in the United States, X.25 is still widely used in Europe.

HDLC

High-level Data Link Control (HDLC) is a flexible, bit-oriented data link protocol that is based on IBM's Synchronous Data Link Control (SDLC). It has been standardized by the ISO. HDLC can support half- or full-duplex transmission, circuit- or packet-switched networks, peer-to-peer or client/server networks, and transmission over cable or wireless media.

XNS

The Xerox Network System (XNS) was created by Xerox for use in Ethernet networks. XNS is the basis for Novell's IPX/SPX, but it is seldom found in today's networks.

Practice Questions

Question 1

Which of the following IEEE 802 specifications provides details on network security?

- ❍ a. 802.8
- ❍ b. 802.9
- ❍ c. 802.10
- ❍ d. 802.11

Answer c is correct because the 802.10 provides information on network security. The 802.8 spec details fiber optic networks. Therefore, answer a is incorrect. Answer b is incorrect because 802.9 details integrated voice and data networks. The 802.11 specification details wireless networks. Therefore, answer d is incorrect.

Question 2

Which layer of the OSI model converts data into a generic format for network transmission?

- ❍ a. Transport layer
- ❍ b. Session layer
- ❍ c. Presentation layer
- ❍ d. Application layer

Answer c is the correct choice; the Presentation layer is responsible for data conversion. Answer a is incorrect because the Transport layer manages the transmission of data across a network. The Session layer maintains a session between computers. Therefore, answer b is also incorrect. The Application layer provides an interface for applications to use to gain access to networked services, so answer d is incorrect.

Question 3

Which layer of the OSI model manages flow control and error correction?

- ❍ a. Transport layer
- ❍ b. Session layer
- ❍ c. Network layer
- ❍ d. Physical layer

Answer a is the correct choice. The Transport layer is responsible for error-handling information and flow control. The Session layer maintains a session between computers. Therefore, answer b is incorrect. The Network layer handles packet addressing and sequencing. Therefore, answer c is incorrect. The Physical layer is responsible for communication with the network media. Therefore, answer d is incorrect.

Question 4

Which layer of the OSI model establishes the route between the sending and receiving computer?

- ❍ a. Transport layer
- ❍ b. Session layer
- ❍ c. Network layer
- ❍ d. Physical layer

Answer c is the correct choice. The Network layer is responsible for determining the route from the source to destination computer. The Transport layer is responsible for error-handling information and flow control. Therefore, answer a is incorrect. The Session layer maintains a session between computers. Therefore, answer b is also incorrect. The Physical layer is responsible for communication with the network media. Therefore, answer d is incorrect.

Question 5

In which OSI model layer does the Media Access Control sublayer reside?

- ❍ a. Transport layer
- ❍ b. Network layer
- ❍ c. Data Link layer
- ❍ d. Physical layer

The only correct answer to this question is answer c. Only the Data Link layer was given sublayers by the IEEE 802 specifications, which defined the Media Access Control and Logical Link Control sublayers. None of the other choices was given sublayers. Therefore, a, b, and d are incorrect.

Question 6

Which of the following protocols is considered a network protocol?

- ❍ a. IPX
- ❍ b. Telnet
- ❍ c. FTP
- ❍ d. SPX

Answer a is the correct choice; IPX is a network protocol. Telnet and FTP are both application protocols. Therefore answers b and c are incorrect. SPX is a transport protocol. Therefore, answer d is also incorrect.

Question 7

Which of the following protocols is considered a transport protocol?

- ❍ a. SNMP
- ❍ b. SMTP
- ❍ c. FTP
- ❍ d. IPX
- ❍ e. TCP

Answer e is correct; TCP is a transport protocol. SNMP, SMTP, and FTP are application protocols. Therefore, answers a, b, and c are incorrect. IPX is a network protocol. Therefore, answer d is also incorrect.

Question 8

Which of the following protocols are considered application protocols? [Check all correct answers]

- ❑ a. TCP
- ❑ b. SNMP
- ❑ c. FTP
- ❑ d. SPX
- ❑ e. NetBEUI

Answers b and c are both correct because SNMP and FTP are both application protocols. TCP and SPX are transport protocols. Therefore answers a and d are incorrect. NetBEUI is a transport protocol. Therefore, answer e is incorrect.

Question 9

Which of the following 802 specifications provide details on how an Ethernet network operates?

- ❍ a. 802.2
- ❍ b. 802.3
- ❍ c. 802.4
- ❍ d. 802.5

Answer b is correct because the 802.3 specification defines standards for Ethernet networks. 802.2 defines Logical Link Control. Therefore, answer a is incorrect. 802.4 defines Token Bus LANs. Therefore, answer c is incorrect. 802.5 defines Token Ring LANs; therefore, answer d is also incorrect.

Need To Know More?

Chellis, James, Charles Perkins, and Matthew Strebe: *MCSE: Networking Essentials Study Guide, 2nd Edition*. Sybex Network Press, San Francisco, CA, 1998. ISBN 0-7821-2220-5. Chapter 3, "The Theoretical Network," discusses the OSI Reference Model at length.

Microsoft Press: *Networking Essentials, 2nd Edition*. Redmond, WA, 1997. ISBN 1-57231-527-X. Unit 3, Lesson 7, "The OSI and 802 Networking Models," and Unit 3, Lesson 10, "Protocols," both discuss the topics covered in this chapter in great detail.