1

Networking Infrastructure and Design

CERTIFICATION OBJECTIVES

Converged networks transmit computer data as well as voice and video data. As a student of convergence engineering and administration, you must start by understanding data networking. Data networking comprises the largest single knowledge domain on the CTP+ exam, and this chapter begins the coverage of this domain. In this chapter, you will learn about industry standards organizations and the data networking technologies they manage and develop. You will also learn about the Open System Interconnection (OSI) model of networking and how it applies to modern networks.

After mastering the OSI model, you will learn about the TCP/IP model and how it can be compared and contrasted with the OSI model. While more exhaustive treatment of the TCP/IP protocol suite will be presented in Chapter 2, this chapter will introduce you to several common protocols and where they operate in the TCP/IP and OSI models. To help you understand how data is passed down through these networking models and across the network, you will explore the topic of data encapsulation.

Networks are organized into logical structures, and you will explore these structures in the "Network Topologies and Cable Distribution Schemes" section of this chapter. You will also review data networking hardware to understand the basic building blocks of a modern data network. As you can see, this chapter covers a lot of information to provide a solid foundation for the rest of the book. Make sure you understand the concepts presented here so that you can better understand the remaining topics in ensuing chapters.

To provide you with context, you will first gain a clear understanding of the concept of a network and how it applies to modern computer and information networks.

Networks Defined

A *network* is a "group of connected or interconnected people or things." When those of us working as technology professionals hear the term network, we tend to immediately think of a computer network, but the reality is that this definition is only one type of network. The currently popular website known as LinkedIn (www.linkedin.com) is a networking site that allows people to form connections with one another based on shared likes, dislikes, experiences, or simply the desire to connect. Network marketing is a phrase that has been used for years to reference a form of marketing that takes advantage of an individual's network of connections with other people that is similar to the networks built on the LinkedIn website. The point is that networks are groups of connected entities and are not limited to modern computer networks.

In fact, the telephone system is a perfect example of a network different from the typical computer networks we implement as local area networks in our organizations. Sometimes called the *public switched telephone network (PSTN)*, it is a network that consists of the telephony endpoints and the cables and devices used between these endpoints. This network allows customers to use a traditional landline telephone to place a call to their friends across town or their extended families several states away. Today, cell phone networks also integrate with the PSTN.

When two networks combine or connect in some way, these networks are said to converge. Many years ago users modulated TCP/IP communications (data communications) over an analog phone line using the PSTN that was designed to carry the human voice and not data. The purpose of this modulation was to implement a connection that allowed communications on the Internet or some other network using a standard phone line. Today, systems digitize the human voice over an Internet Protocol (IP) network that was designed to carry computer data and not the human voice. Ultimately, when implementing Voice over IP (VoIP), the IP network eventually connects to the PSTN (in many cases) to route calls outside of the IP network and connect to other telephones that are simply connected to a standard landline. This connection point between the IP network and the traditional telephone network is one way in which we say the networks are converged.

In addition, the fact that voice data is now traveling on a network that was designed for computer data also suggests convergence. We could say that the two data types have converged. The computer data may consist of a word processor document or an e-mail; voice data is a digitized version of the human-generated sound waves. In the end, both data types become IP packets, which are zeros and ones on the communications medium that is utilized.

At least two points of convergence exist in the areas of voice and data. The first point is where our IP networks connect to traditional telephone networks. The second point is the unification of upper-level data, such as voice and computer data, into shared lower-level communications, such as IP packets. These convergence points will all become very clear as you read through this book. For now, let's explore the historical development of information networks. A brief overview of the major developments along the way will help you understand why things work the way they do today and how to best take advantage of the available technologies.

The Evolution of Information Networks

The electric telegraph was the precursor to modern electronic and digital information networks. While other networks, like the Pony Express or Claude Chappe's nonelectric telegraph, existed before the electric telegraph, they required complete and continual involvement of humans either from end to end or at each

end. The electric telegraph was a revolutionary leap forward in technology in that it eventually allowed messages to be sent to a remote location and recorded onto paper tape as raised dots and dashes matching up with Morse code.

It is interesting to note that tests were performed over many years in order to validate the potential of electricity in communications. In 1746 Jean-Antoine Nollet asked about 200 monks to form a long snaking line. He had each one hold the end of a 25-foot iron wire connecting him to the next monk in the line. Then, without warning, he injected an electrical current into the line. The fact that monks in a line nearly one mile long all exclaimed their literal shock at the same time showed that electricity travels long distances very rapidly. Of course, we have much more humane methods of testing today, but these early tests did indeed reveal the knowledge that eventually led to the implementation of high-speed electric telegraphs.

By 1861, the United States was implementing the transcontinental telegraph, which allowed nearly instant communications across the country. Reminiscent of how we are implementing IPv6 alongside our IPv4 networks, the transcontinental telegraph wire was placed alongside the existing Pony Express route. Once the telegraph network was in place, the Pony Express became obsolete and was dissolved. Some of us look forward to the day when IPv6 does the same to IPv4.

In a quick jump to the peak of the era of the telegraph, within 30 years of its beginning, over 650,000 miles of wire was in place and some 20,000 towns were connected to the network. You could send messages from London to Bombay or from New York to Sacramento in just a few minutes. Previously, such communications would have taken weeks or months. The telegraph showed that electronic communications were indeed the way to send information over long distances.

Believe it or not, the use of electricity in sending telegraph messages eventually led to the use of electronic voice communications. The telephone, invented in the late 1800s, converted sound waves into electronic signals on the sending end and then converted electronic signals into sound waves on the receiving end. Sound travels at an average speed of about 1,130 feet (344 meters) per second at sea level. As a comparison, electromagnetic waves travel at about 186,400 miles (300,000 kilometers) per second. This speed means that a message sent electronically could travel around the Earth more than seven times in a second. By converting sound waves to electromagnetic waves and back, we can transmit the human voice very rapidly, which is why you can have a conversation with someone on the other side of the globe with little delay.

The telephone system continued to evolve into the PSTN that we utilize today. In the same way, new forms of information delivery were also being developed, and nearing the end of the twentieth century two distinct networks had evolved: voice networks and data networks. Voice networks allowed the transfer of

human conversations, and data networks allowed the transfer of all other kinds of information. At times, our data networks connected to one another using the voice networks as the infrastructure, and at times, our voice networks crossed over our data networks in the form of packet delivery; however, with the new millennium also came much greater interest in the convergence of voice and data networks.

on the Job

If you would like to learn more about the history of the telegraph and telephone, I suggest the book* The Victorian Internet *by Tom Standage (Walker & Company, 2007) as a starting point. Studying these historical developments can help you better understand the technologies we use today and why convergence is important and beneficial to the future of data networks.

CERTIFICATION OBJECTIVE

1.1.1 Industry Bodies and Standards

To provide consistency across devices and software from different vendors, the data networking and voice communications industries have developed standards. These standards define the way a device should communicate with another device and the way an application should communicate on a network. With such standards in place, we are able to purchase hardware and software from different vendors and trust that they will be able to interoperate.

In addition, governing bodies control communications and use of certain media. For example, you can only communicate with wireless devices in the United States if you comply with Federal Communications Commission (FCC) regulations. In other countries, different governing bodies provide similar oversight. In this section, you will learn about both the industry standards organizations and the governing bodies.

Industry Standards Organizations

Dozens of industry standards organizations exist. Industry standards typically fall into one of two categories. The first is the open standard. Open standards are those standards created by a private or public standards organization. They include such standards as the 802.3 Ethernet standard and the H.323 media communications standard. The second is the de facto standard. De facto standards are those standards that are typically developed by a private organization or group and become so popular they are considered to be the "standard way" to do something.

Standards provide for consistency in communications and for simplicity in implementation. Consistency in communications is provided because all devices based on the same standard communicate in the same way. Simplicity in implementation is provided because you can purchase devices based on a standard and trust they will work well together.

on the Job

While devices that specify they support a given standard will certainly work with other devices implementing the same standard, it is important to remember that many vendors add proprietary features on top of the standard. The result is that a device supporting a specific standard but with a proprietary feature enabled may not communicate properly with another standard-based device that lacks support for the proprietary feature.

Table 1-1 lists the industry standards organizations that you should be aware of as a convergence technology professional. While you will not be required to know every detail of these organizations for the CTP+ exam, you should remember their primary purpose for exam day.

TABLE 1-1 Industry Standards Organizations

Industry Standard Organization	Primary Purpose
American National Standards Institute (ANSI)	Defines coding standards and signaling schemes in the United States. Represents the United States to the ISO and the ITU. Promotes the use of United States standards internationally. For more information, see www.ansi.org.
Communications Information Technology Association (CITA)	Coordinates standards and best practices in the United Kingdom. An affiliate of the TIA. For more information, see www.cita.org.uk.
Electronic Industries Alliance/ Telecommunications Industry Association (EIA/TIA)	Composed of multiple organizations including the TIA. Develops wiring and cabling standards. Defines category 5 (CAT 5) cabling in the document EIA/TIA 568. For more information, see www.eia.org or www.tiaonline.org.
European Telecommunications Standards Institute (ETSI)	Provides standards in the European nations of nearly 60 countries for telecommunications and cabling. Defines cabling standards in the EN 50173 document that are similar to the EIA/TIA 568 document. For more information see www.etsi.org.

TABLE 1-1 Industry Standards Organizations *(continued)*

Industry Standard Organization	Primary Purpose
Institute of Electrical and Electronics Engineers (IEEE)	Defines standards for electronics and electrical communications. Defines wired networking in common use today in the Ethernet 802.3 standard. Defines wireless networking in common use today in the Wi-Fi 802.11 standard. For more information, see www.ieee.org.
International Organization for Standardization (ISO)	Defines international standards and involved participants from national standards bodies in many countries. Defines the Open System Interconnection (OSI) reference model for network communications. For more information, see www.iso.org.
International Telecommunications Union (ITU)	Based in the United States, defines international or global telecommunications networks and services. Government and private sector organizations participate in the ITU. Defines and manages standards for telecommunications. For more information, see www.itu.int.
Internet Architecture Board (IAB)	Responsible for the editorial management and publication of Request for Comments (RFC) standards, which define the majority of Internet standards. Oversees the general technical development of the Internet. For more information, see www.iab.org.
Internet Engineering Task Force (IETF)	Composed of a global community of engineers, researchers, and hardware and software vendors that create working groups to develop and enhance Internet standards. Works under the IAB. For more information, see www.ietf.org. To view RFCs, consider using the site www rfc-editor.org.
Internet Research Task Force (IRTF)	A group that works alongside the IETF. Researches long-term projects for Internet growth and evolution. For more information, see www.irtf.org.
Internet Society (ISOC)	Provides a form of organizational structure to the Internet standards development process. An international organization, the standards it monitors are directed through the IETF and IAB. For more information, see www.isoc.org.

Governing Bodies

Governing bodies or organizations control the telecommunications industry. Some such organizations are government-based, and others are independent of governments and are driven by the industry. Table 1-2 lists the governing bodies you should be aware of as a convergence technology professional.

TABLE 1-2 Governing Bodies

Governing Body	Description
Australian Communications and Media Authority (ACMA)	A government body responsible for the regulation of radio communications within Australia. Manages the electromagnetic spectrum with the intent of minimizing interference. For more information, see www.acma.gov.au.
Federal Communications Commission (FCC)	A government body responsible for communications by radio, television, cable, satellite, and wire within the United States. Manages the electromagnetic spectrum with the intent of minimizing interference. For more information, see www.fcc.gov.
Independent Committee for the Supervision of Standards of Telephone Information Services (ICSTIS)	A nongovernment, industry-funded governing body that ensures telephony companies charge only for proper billing charges. ICSTIS allows customers to lodge complaints against telephone companies. For more information, see www.icstis.org.
Office of Communications (OfCom)	A government body responsible for the regulation of radio communications within the United Kingdom. Manages the electromagnetic spectrum with the intent of minimizing interference. For more information, see www.ofcom.org.uk.

CERTIFICATION OBJECTIVE

1.1.2 OSI/RM Layers

In order to help you understand how the various networking components work together to form a converged network, I will first explain the OSI relational model (RM). While this model is not directly implemented in the TCP/IP networks that are most common today, it is a valuable conceptual model that helps you to relate different technologies to one another and implement the right technology in the right way.

According to document ISO/IEC 7498-1, which is the OSI Basic Reference Model standard document, the OSI model provides a "common basis for the coordination of standards development for the purpose of systems interconnection, while allowing existing standards to be placed into perspective within the overall reference model." In other words, the model is useful for new standards as they are developed and for thinking about existing standards. In Chapter 2, I will show you this reality when I relate the TCP/IP protocol suite to the OSI model. Even though TCP/IP was developed before the OSI model, it can be *placed in perspective* in relation to the model.

The OSI model allows us to think about our network in chunks or layers. You can focus on securing each layer, optimizing each layer, and troubleshooting each layer. This allows you to take a complex communications process apart and evaluate its components. In order to understand this, you'll need to know that the OSI model is broken into seven layers. The seven layers are (from top to bottom):

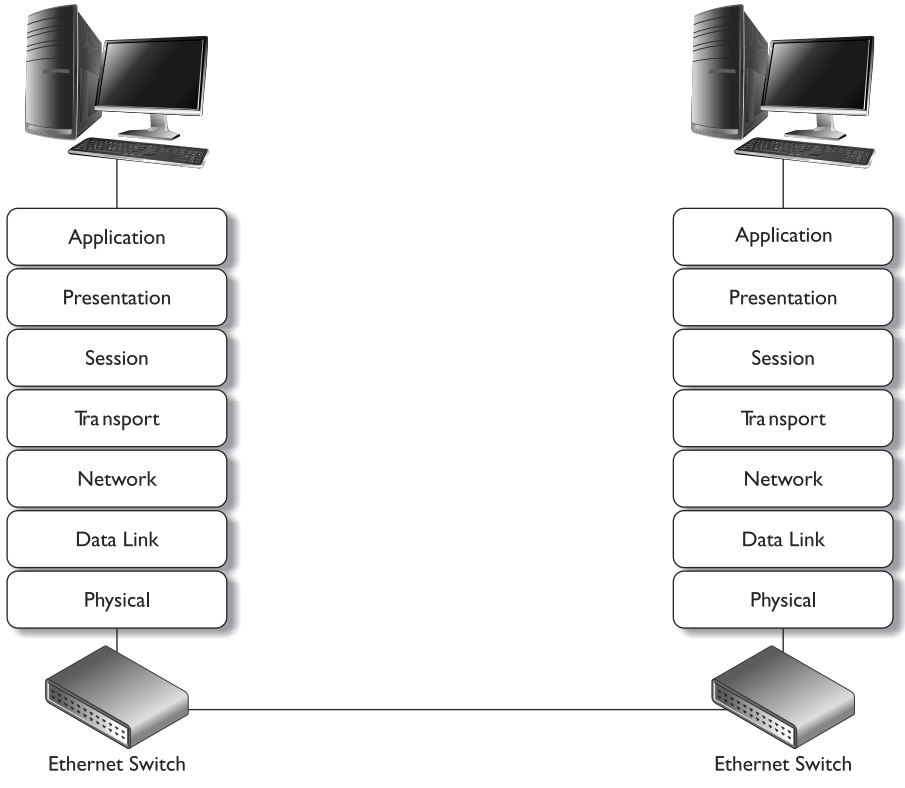
- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Each layer is defined as providing services and receiving services. For example, the Data Link layer provides a service to the Physical layer and receives a service from the Physical layer. How is this? In a simplified explanation, the Data Link layer converts packets into frames for the Physical layer, and the Physical layer transmits these frames as bits on the chosen medium. The Physical layer reads bits off the chosen medium and converts these into frames for the Data Link layer.

The layered model allows for abstraction. In other words, the higher layers do not necessarily have to know how the lower layers are doing their jobs. In addition, the lower layers do not necessarily have to know what the upper layers are actually doing with the results of the lower layers' labors. This abstraction means that you have the ability to use the same web browser and Hypertext Transfer Protocol (HTTP) protocol to communicate on the Internet whether the lower-layer connection is a dial-up modem, a high-speed Internet connection, or somewhere in between. The resulting speed or performance will certainly vary, but the functionality will remain the same.

Figure 1-1 illustrates the concept of the OSI model. As you can see, data moves down through the layers, across the medium, and then back up through the layers on the receiving machine. Remember, most networking standards allow for the substitution of nearly any Data Link and Physical layer. While this example shows a wired Ethernet connection between the two machines, it could have just as easily been a wireless connection using the IEEE 802.11 and IEEE 802.2 standards for the descriptions of the Data Link and Physical layers. This example uses the IEEE 802.3 Ethernet standard and the IEEE 802.2 LLC standard (a layer within the Data Link layer) for the lower layers. The point is that the most popular upper-layer protocol suite, TCP/IP, can work across most lower-layer standards, such as IEEE 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (Wireless LANs), and 802.16 (WiMAX).

FIGURE 1-1 OSI model depiction



In order to fully understand the OSI model and be able to relate to it throughout the rest of this book, it is important that we evaluate each layer. You will need to understand the basic description of each layer and the services it provides to the networking process. I will define each layer and then give examples of its use, starting with the topmost layer, which is the Application layer, since this is the order in which they are documented in the standard.

exam Watch

It is important that you understand the basic operations that take place at each layer of the OSI model.

It's also useful to know the primary components, such as switches, routers, and hubs, that function at each level.

Application Layer

The seven layers of the OSI model are defined in Clause 7 of the document ISO/IEC 7498-1. The Application layer is defined in Subclause 7.1 as the highest layer in the reference model and as the sole means of access to the Open System Interconnection Environment (OSIE). In other words, the Application layer is the layer that provides access to the other OSI layers for applications and to applications for the other OSI layers. Do not confuse the Application layer with the general word "applications," which is used to reference programs like Microsoft Excel, Corel WordPerfect, and so on. The Application layer is the OSI layer that these applications communicate with when they need to send or receive data across the network. You could say that the Application layer contains the higher-level protocols that an application needs to talk to. For example, Microsoft Outlook may need to talk to the Simple Mail Transfer Protocol (SMTP) in order to transfer e-mail messages.

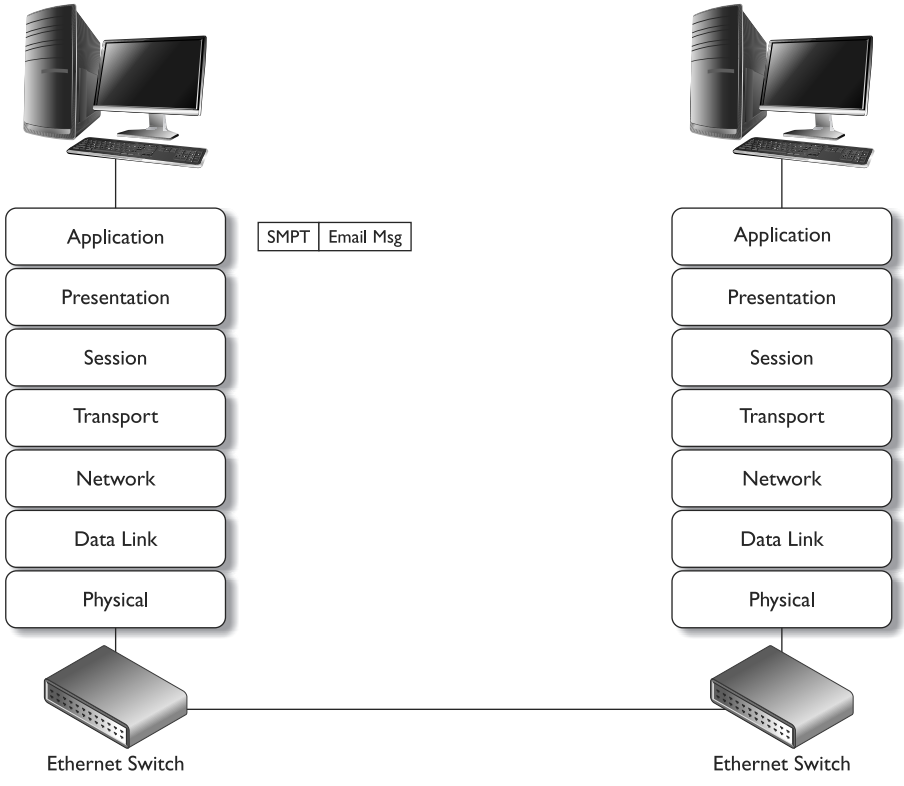
Examples of Application layer protocols and functions include HTTP, File Transfer Protocol (FTP), and SMTP. HTTP is used to transfer Hypertext Markup Language (HTML), Active Server Pages (ASP), PHP Hypertext Processor (PHP), and other types of documents from one machine to another. HTTP is the most heavily used Application layer protocol on the Internet and, possibly, in the world. FTP is used to transfer binary and ASCII files between a server and a client. Both the HTTP and FTP protocols can transfer any file type. SMTP is used to move e-mail messages from one server to another, and usually works in conjunction with other protocols for mail storage.

Application layer processes fall into two general categories: user applications and system applications. E-mail (SMTP), file transfer (FTP), and web browsing (HTTP) functions fall into the user application category, as they provide direct results to applications used by users such as Outlook Express (e-mail), WS_FTP (file transfer), and Firefox (web browsing). Notice that the applications or programs used by the user actually take advantage of the application services in the Application layer, or Layer 7. In other words, Outlook Express takes advantage of SMTP. Outlook Express does not reside in Layer 7, but SMTP does. For examples of system applications, consider DHCP and DNS. The Dynamic Host Configuration Protocol (DHCP) provides for dynamic TCP/IP configuration, and the Domain Name Service (DNS) protocol provides for name-to-IP address resolution. Both of these are considered system-level applications because they are not usually directly accessed by the user (this is open for debate, since administrators are users too and they use command-line tools or programs to directly access these services quite frequently).

The processes operating in the Application layer are known as *application-entities*. An application-entity is defined in the standard as "an active element embodying a set of capabilities which is pertinent to OSI and which is defined for the Application Layer." In other words, application-entities are the services that run in Layer 7 and communicate with lower layers while exposing entry points to the OSI model for applications running on the local computing device. SMTP is an application-entity, as are HTTP and other Layer 7 protocols.

Imagine that you are sending an e-mail using SMTP, which is the most popular method of sending an e-mail message. Your e-mail application will connect to an SMTP server in order to send the e-mail message. Interestingly, from the e-mail application's perspective, it is connecting directly to the SMTP server and is completely unaware of all the other layers of operation that allow this connection to occur. Figure 1-2 shows the e-mail as it exists at Layer 7.

FIGURE 1-2 SMTP e-mail being sent through Layer 7



Presentation Layer

The Presentation layer is defined in Subclause 7.2 of the standard as the sixth layer of the OSI model, and it provides services to the Application layer above it and the Session layer below it. The Presentation layer, or Layer 6, provides for the representation of the information communicated by or referenced by application-entities. The Presentation layer is not used in all network communications, and it, as well as the Application and Session layers, is similar to the single Application layer of the TCP/IP model. The Presentation layer provides for syntax management and conversion as well as encryption services. Syntax management refers to the process of ensuring that the sending and receiving hosts communicate using a shared syntax or language. When you understand this concept, you will realize why encryption is often handled at this layer. After all, encryption is really a modification of the data in such a way that it must be reversed on the receiving end. Therefore, both the sender and receiver must understand the encryption algorithm in order to provide the proper data to the program that is sending or receiving on the network.

on the job

Don't be alarmed to discover that the TCP/IP model has its own Application layer that differs from the OSI model's Application layer. The TCP/IP protocol existed before the OSI model was released. For this reason, we relate the TCP/IP protocol suite to the OSI model, but we cannot say that it complies with the model directly. It's also useful to keep in mind the reality that the TCP/IP protocol is an implemented model and the OSI model is a "reference" model. This definition simply means that we use it as a reference to understand our networks and network communications.

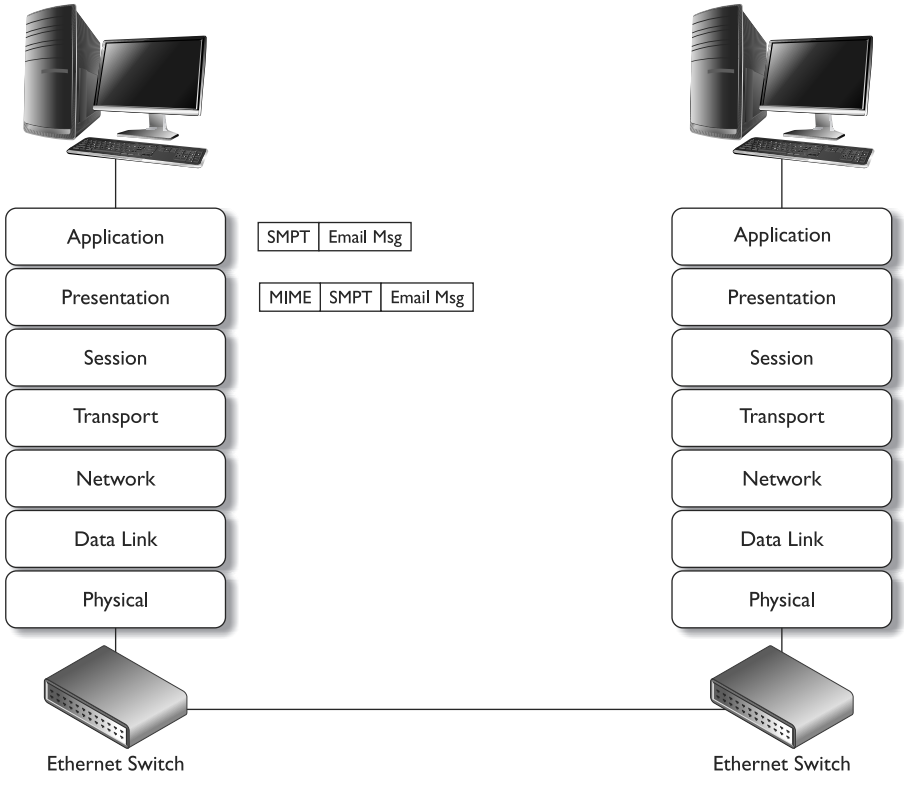
Examples of Presentation layer protocols and functions include any number of data representation and encryption protocols. For example, if you choose to use HTTPS instead of HTTP, you are indicating that you want to use Secure Sockets Layer (SSL) encryption. SSL encryption is related to the Presentation layer, or Layer 6 of the OSI model.

Ultimately Layer 6 is responsible, at least in part, for three major processes: data representation, data security, and data compression. *Data representation* is the process of ensuring that data is presented to Layer 7 in a useful way and that it is passed to Layer 5 in a way that it can be processed by the lower layers. *Data security* usually includes authentication, authorization, and encryption. Authentication is used to verify the identity of the sender and the receiver. With solid authentication, we gain a benefit known as nonrepudiation. *Nonrepudiation* simply means that the sender cannot deny the sending of data. This differentiation is often used for auditing and incident handling purposes. *Authorization* ensures that only valid users can access the data being accessed, and *encryption* ensures the privacy and integrity of the data as it is being transferred.

The processes running at Layer 6 are known as presentation-entities in the OSI model documentation. Therefore, an application-entity is said to depend on the services of a presentation-entity, and the presentation-entity is said to serve the application-entity.

As your e-mail message moves down to the Presentation layer, and since it uses SMTP, it is sent as clear text by default. This transfer is accomplished today using the Layer 6 Multipurpose Internet Mail Extensions (MIME) representation protocol that allows for binary attachments to SMTP messages. This means that the Presentation layer is converting your e-mail message, whatever its origination, into the standard MIME format or syntax. If you wanted to secure the message, the Secure/MIME (S/MIME) protocol could be used instead. The S/MIME protocol, still operating at Layer 6, uses encryption to secure the data as it traverses the network. This encrypted data is sometimes said to be enveloped data. You can see the e-mail now as it exists at Layer 6 in Figure 1-3.

FIGURE 1-3 SMTP e-mail after reaching Layer 6



Session Layer

The Session layer is defined in Subclause 7.3 of the standard as "providing the means necessary for cooperating presentation-entities to organize and to synchronize their dialog and to manage their data exchange." This exchange is accomplished by establishing a connection between two communicating presentation-entities. The result is simple mechanisms for orderly data exchange and session termination.

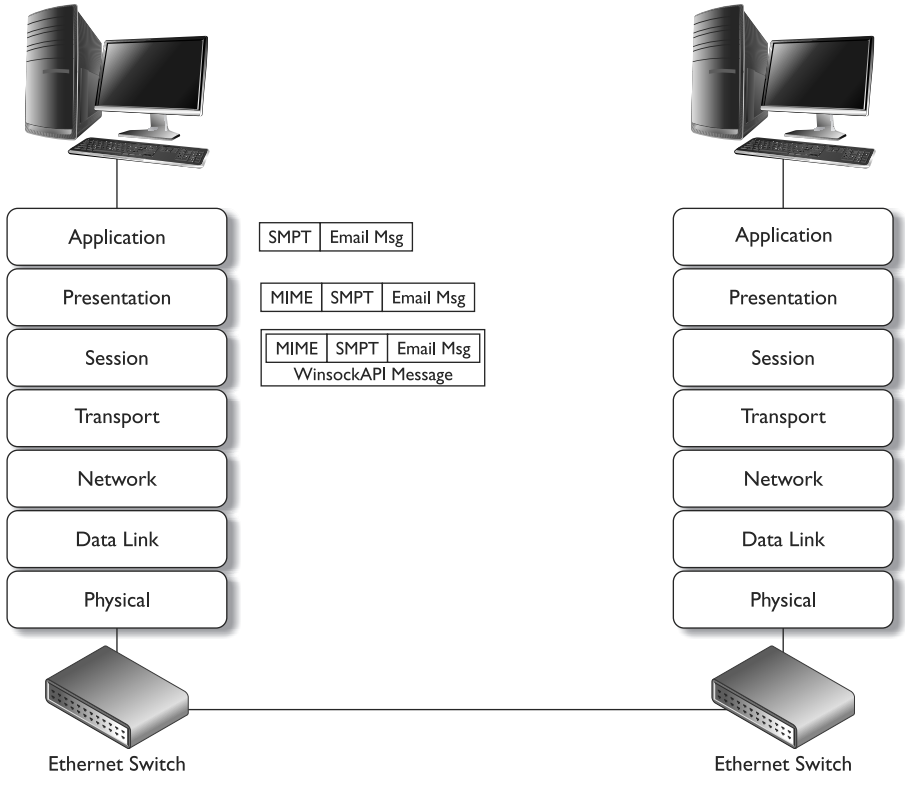
A session includes the agreement to communicate and the rules by which the communications will transpire. Sessions are created, communications occur, and sessions are destroyed or ended. Layer 5 is responsible for establishing the session, managing the dialogs between the endpoints, and conducting the proper closing of the session.

Examples of Session layer protocols and functions include the iSCSI protocol, RPC, and NFS. The Internet Small Computer System Interface (iSCSI) protocol provides access to SCSI devices on remote computers or servers. The protocol allows a SCSI command to be sent to the remote device. The Remote Procedure Call (RPC) protocol allows subroutines to be executed on remote computers. A programmer can develop an application that calls the subroutine in the same way as a local subroutine. RPC abstracts the Network layer and allows the application running above Layer 7 to execute the subroutine without knowledge of the fact that it is running on a remote computer. The Network File System (NFS) protocol is used to provide access to files on remote computers as if they were on the local computer. NFS actually functions using an implementation of RPC known as Open Network Computing RPC (ONC RPC) that was developed by Sun Microsystems for use with NFS; however, ONC RPC has also been used by other systems since that time. Remember that these protocols are provided only as examples of the protocols available at Layer 5 (as were the other protocols mentioned for Layers 6 and 7). By learning the functionality of protocols that operate at each layer, you can better understand the intention of each layer.

The services and processes running in Layer 5 are known as session-entities. Therefore, RPC and NFS would be session-entities. These session-entities will be served by the Transport layer.

At the Session layer, your e-mail message can begin to be transmitted to the receiving mail server. The reality is that SMTP e-mail uses the TCP protocol from the TCP/IP suite to send e-mails, and the analogy is not perfect at this point. This imperfection in the comparison of models is because the TCP/IP protocol does not map directly to the OSI model, as you will learn in the next chapter. For now, know that Layer 5 is used to establish sessions between these presentation-entities. In Windows, the Winsock application programming interface (API) provides access to the TCP/IP protocol suite. We could, therefore, say that your e-mail is passed

FIGURE 1-4 SMTP e-mail at Layer 5



through to the TCP/IP suite using Winsock here at Layer 5. Figure 1-4 shows the e-mail as it is passed through the Winsock API at Layer 5.

Transport Layer

Layer 4, the Transport layer, is defined as providing "transparent transfer of data between session entities and relieving them from any concern with the detailed way in which reliable and cost effective transfer of data is achieved." This definition simply means that the Transport layer, as its name implies, is the layer where the data is segmented for effective transport in compliance with Quality of Service (QoS) requirements and shared medium access.

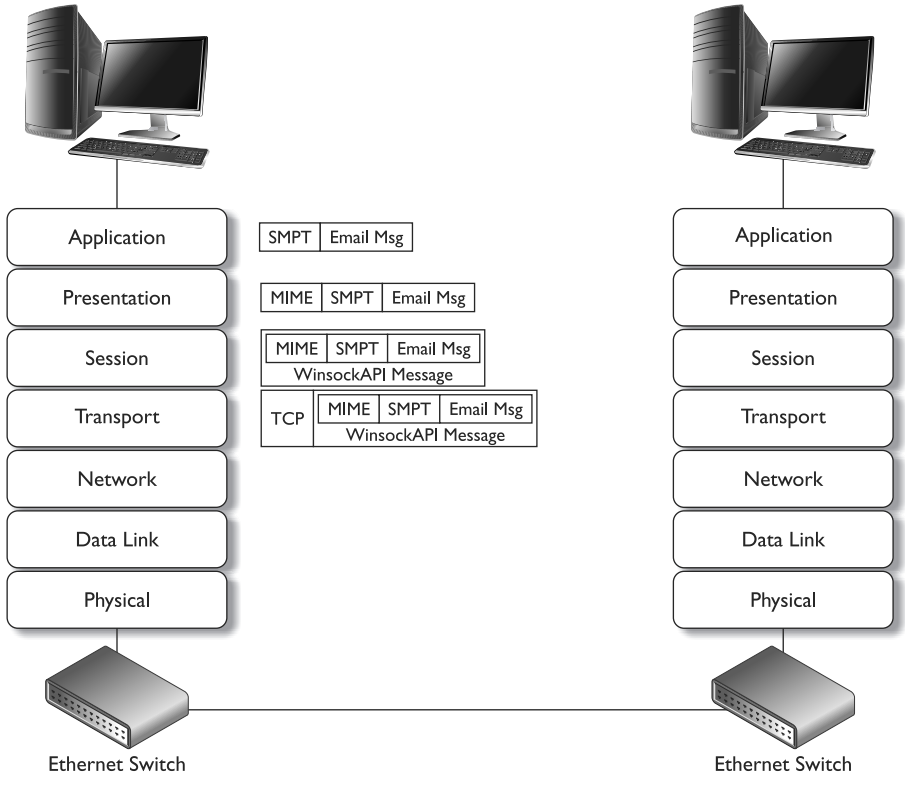
Examples of Transport layer protocols and functions include TCP and UDP. The Transmission Control Protocol (TCP) is the primary protocol used for the transmission of connection-oriented data in the TCP/IP suite. HTTP, SMTP, FTP, and other important Layer 7 protocols depend on TCP for reliable delivery and

receipt of data. The User Datagram Protocol (UDP) is used for connectionless data communications. For example, when speed of communications is more important than reliability, UDP is frequently used. Because voice data has to either arrive or not arrive (as opposed to arriving late), UDP is frequently used for the transfer of voice and video data.

TCP and UDP are examples of transport-entities at Layer 4. These transport-entities will be served by the Network layer. At the Transport layer, the data is broken into segments if necessary. If the data will fit in one segment, then the data becomes a single segment. Otherwise, the data is divided into multiple segments for transmission.

The Transport layer takes the information about your e-mail message from the Session layer and begins dividing (segmenting) it into manageable chunks (packets) for transmission by the lower layers. Figure 1-5 shows the e-mail after processing at the Transport layer.

FIGURE 1-5 E-mail after Layer 4 processing



Network Layer

The Network layer is defined as providing "the functional and procedural means for connectionless-mode (UDP) or connection-mode (TCP) transmission among transport-entities and, therefore, provides to the transport-entities independence of routing and relay considerations." In other words, the Network layer says to the Transport layer, "You just give me the segments you want to be transferred and tell me where you want them to go. I'll take care of the rest." This segregation of communication is why routers do not have to expand data beyond Layer 3 to route the data properly. For example, an IP router does not care if it's routing an e-mail message or voice conversation. It only needs to know the IP address for which the packet is destined and any relevant QoS parameters in order to move the packet along.

Examples of Network layer protocols and functions include IP, ICMP, and IPsec. The Internet Protocol (IP) is used for addressing and routing of data packets in order to allow them to reach their destination. That destination can be on the local network or a remote network. The local machine is never concerned with this destination, with the exception of the required knowledge of an exit point, or default gateway, from the local machine's network. The Internet Control Message Protocol (ICMP) is used for testing the TCP/IP communications and for error message handling within Layer 3. Finally, IP Security (IPsec) is a solution for securing IP communications using authentication and/or encryption for each IP packet. While security protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Secure Shell (SSH) operate at Layers 4 through 7 of the OSI model, IPsec sits solidly at Layer 3. The benefit is that since IPsec sits below Layer 4, any protocols running at or above Layer 4 can take advantage of this secure foundation. For this reason, IPsec has become more and more popular since it was first defined in 1995.

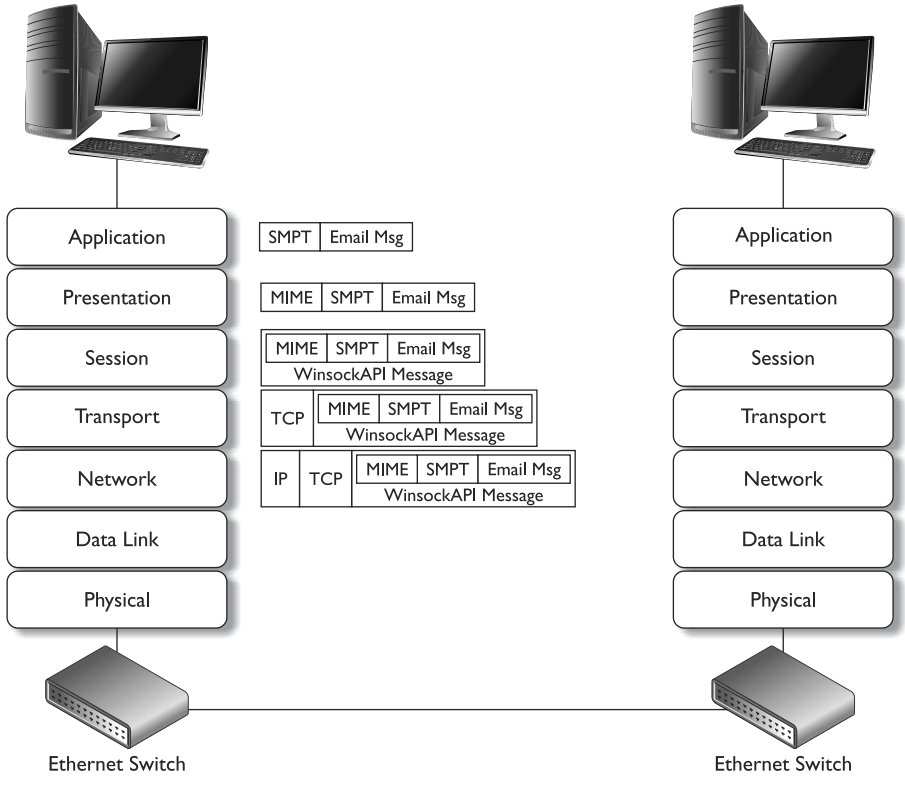
The services and procedures operating in the Network layer are known as network-entities. These network-entities depend on the services provided by the Data Link layer. At the Network layer, Transport layer segments become packets. These packets will be processed by the Data Link layer.

At the Network layer, your e-mail message that was broken into segments at Layer 4 is now appended with appropriate destination and source addressing information in order to ensure that it arrives at the destination. The results of Layer 3 processing are shown in Figure 1-6.

Data Link Layer

The Data Link layer is defined as providing communications between connectionless-mode or connection-mode network entities. This method may include the establishment, maintenance, and release of connections for connection-

FIGURE 1-6 Layer 6 SMTP e-mail



mode network entities. The Data Link layer is also responsible for detecting errors that may occur in the Physical layer. Therefore, the Data Link layer provides services to Layer 3 and Layer 1. The Data Link layer, or Layer 2, may also correct errors detected in the Physical layer automatically.

Examples of Data Link layer protocols and functions include Ethernet, PPP, and HDLC. Ethernet is the most widely used protocol for local area networks (LANs) and will be the type of LAN you deal with when using most modern LAN technologies. Ethernet comes in many different implementations from 10 Mbps (megabits per second or million bits per second) to 1000 Mbps in common implementations. Faster Ethernet technologies are being developed and implemented on a small scale today. The Point to Point Protocol (PPP) is commonly used for wide area network (WAN) links across analog lines and other tunneling purposes across digital lines. The High-Level Data Link Control (HDLC) protocol is a solution created by the ISO for bit-oriented synchronous communications. It is a popular protocol used for WAN links, and is the default WAN link protocol for many Cisco routers.

The IEEE has divided the Data Link layer into two sublayers: the Logical Link Control (LLC) sublayer and the Medium Access Control (MAC) sublayer. The LLC sublayer is not actually used by many transport protocols, such as TCP. The varied IEEE standards identify the behavior of the MAC sublayer within the Data Link layer and the Physical layer as well.

The results of the processing in Layer 2 are that the packet becomes a frame that is ready to be transmitted by the Physical layer, or Layer 1. So the segments became packets in Layer 3 and now the packets have become frames. Remember, this is just the collection of terms that we use; the data is a collection of ones and zeros all the way down through the OSI layers. Each layer is simply manipulating or adding to these ones and zeros in order to perform that layer's service. As in the other layers before it, the services and processes within the Data Link layer are named after the layer and are called data-link-entities.

The Data Link layer adds the necessary header to the e-mail packets received from Layer 3, and your e-mail message, in its one or many parts, is now a frame or set of frames. The frames are ready to be transmitted by the Physical layer. In Figure 1-7 we see the e-mail message after the Data Link layer processing is complete.

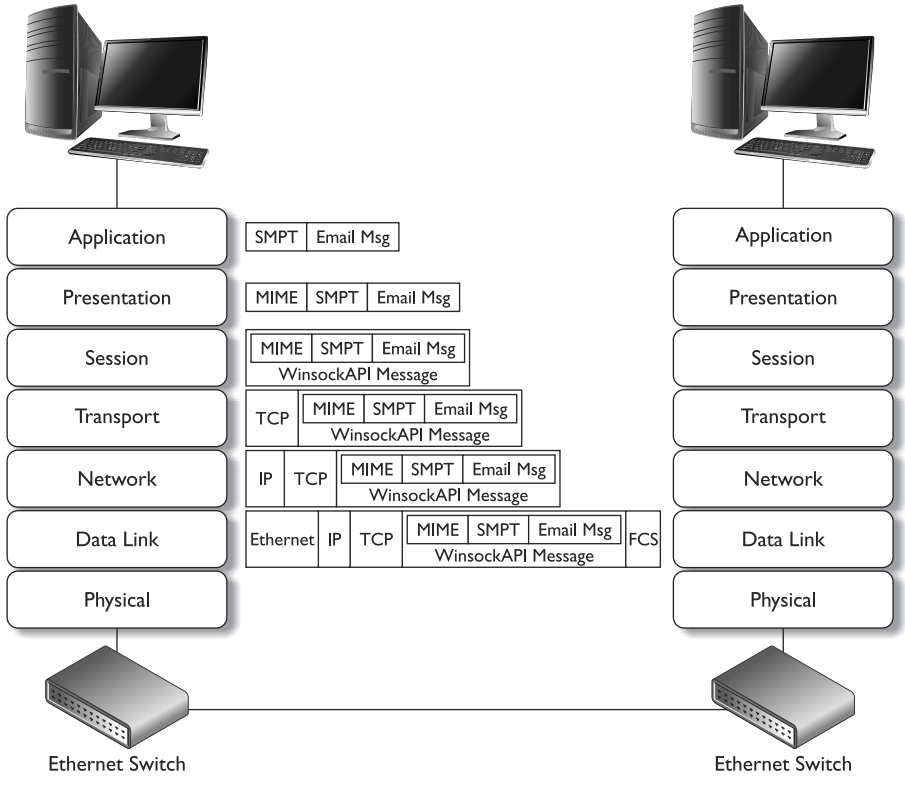
Physical Layer

The Physical layer, sometimes called the PHY, is responsible for providing the mechanical, electrical, functional, or procedural means for establishing physical connections between data-link-entities. The connections between all other layers are really logical connections, as the only real physical connection that results in true transfer of data is at Layer 1—the Physical layer. For example, we say that the Layer 7 HTTP protocol on a client creates a connection with the Layer 7 HTTP protocol on a web server when a user browses an Internet website; however, the reality is that this connection is logical and the real connections happen at the Physical layer.

It is really amazing to think that my computer—the one I'm using to type these words—is connected to a wireless access point (AP) in my office, which is connected to my local network that is in turn connected to the Internet. Through connections—possibly both wired and wireless—I can send signals (that's what happens at Layer 1) to a device on the other side of the globe. To think that there is a potential electrical connection path between these devices and millions of others is really quite amazing.

It is Layer 1 that is responsible for taking the data frames from Layer 2 and transmitting them on the communications medium as binary bits (ones and zeros). This medium may be wired or wireless. It may use electrical signals or light pulses

FIGURE 1-7 Layer 2 e-mail results



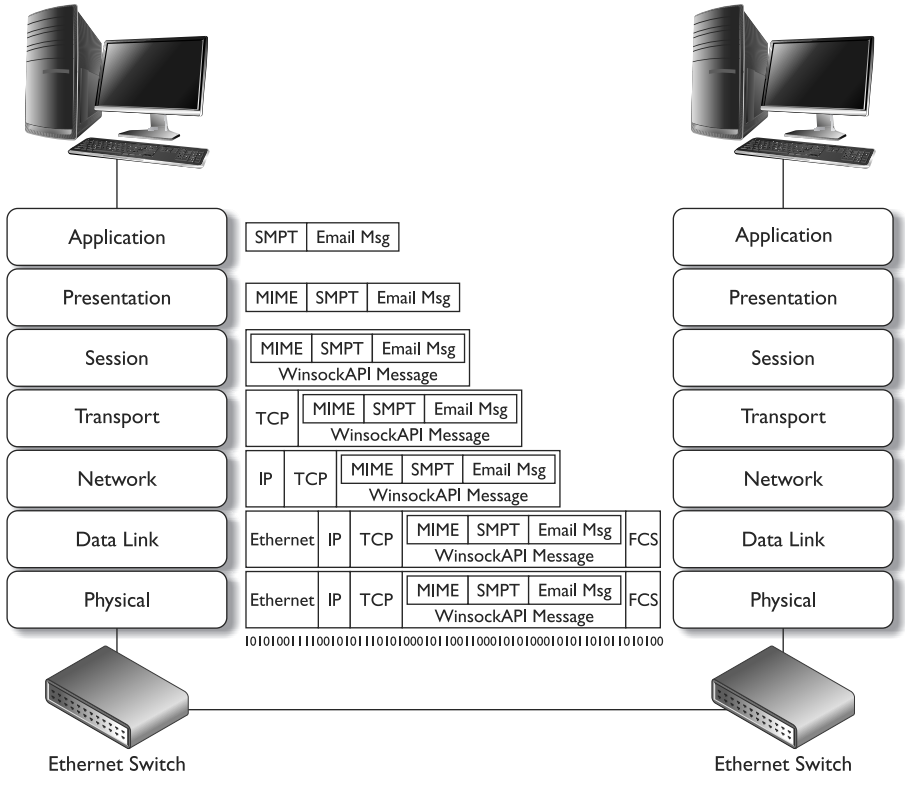
(both actually being electromagnetic in nature). Whatever transmission method you've chosen to use at Layer 1, the upper layers can communicate across it as long as the hardware and drivers abstract that layer so that it provides the services demanded of the upper-layer protocols.

Examples of Physical layer protocols and functions include Ethernet, Wi-Fi, and Digital Subscriber Line (DSL.) You probably noticed that Ethernet was mentioned as an example of a Data Link layer protocol. This categorization is because Ethernet defines both the MAC sublayer functionality within Layer 2 and the PHY for Layer 1. Wi-Fi technologies (IEEE 802.11) are similar in that both the MAC and PHY are specified in the standard. Therefore the Data Link and Physical layers are often defined in standards together. You could say that Layer 2 acts as an intermediary between Layers 3 through 7 so that you can run Internetworked Packet Exchange/Sequenced Packet Exchange (IPX/SPX) (though hardly anyone uses this protocol today) or TCP/IP across a multitude of network types (network types being understood as different MAC and PHY specifications).

Your e-mail is finally being transmitted across the network. First a one and then a zero, then maybe another one or zero, and on and on until the entire e-mail message is transmitted. Figure 1-8 shows the final results with the e-mail, now broken into frames, being transmitted on the medium.

The example of the e-mail transmission has been simplified in comparison to what really takes place. For example, each packet (from Layer 3) will be transmitted by Layer 1 (after being converted to frames by Layer 2), and then the next packet may be sent or the network interface card (NIC) may need to process incoming data.

FIGURE 1-8 Layer 1 e-mail transmission



SCENARIO & SOLUTION	
You are sending a file to an FTP server. The data that is to be transmitted needs to be encrypted. Which layer of the OSI model is the likely area where this will happen?	The Presentation layer because encryption, compression, and syntax are frequently applied at this layer. It is important to keep in mind the possibility that encryption may also occur at other layers. For example, IPsec encrypts data at Layer 3.
Information about the source and destination MAC addresses is being added to a packet. Which layer of the OSI model is performing this operation?	The Data Link layer. Packets are created at the Network layer and are sent down to the Data Link layer, where MAC addresses are added in the frame's header for both the source and the destination.

That incoming data may be a confirmation of a past outgoing packet that was part of the e-mail message, it may be a retry request, or it may be completely unrelated data. Due to the nature of varying underlying Layer 1 technologies, the actual transfer may differ from network to network. However, this example simply illustrates how the data is modified as it passes down through the OSI model.

Now, on the receiving machine, exactly the opposite would transpire. In other words, frames become packets, which become segments, which become the data that may need to be represented, decompressed, or decrypted before being forwarded upstream to the user's program. When the data is sent, it is formatted, chunked, and transmitted. On the receiving end it is received, aggregated, and possibly reformatted. This sequence is what the OSI layers do for us. It is also what many actual network protocols do for us, such as TCP/IP.

OSI Model Communications Process

Now that you understand the layers of the OSI model, it is important for you to understand the communications process utilized within the model. Each layer is said to communicate with a peer layer on another device. This process means that the Application layer on one device is communicating with the Application layer on the other device. In the same way, each layer communicates with its peer layer. This virtual communication is accomplished through segmentation and encapsulation.

INSIDE THE EXAM

Why Is the OSI Model Important?

The OSI model is more than a set of facts that you memorize for certification exams. It has become the most common method for referencing all things networking. Many resources assume that you understand this model and reference it without explanation. You may read statements like the following:

"Web authentication is a *Layer 3* security feature that causes the controller to not allow IP traffic (except DHCP-related packets) from a particular client until that client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define a username and password for each client. When the clients attempt to join the wireless LAN (WLAN), their users must enter the username and password when prompted by a login window."

This statement is quoted from an article at Cisco's website. Within the article there is no explanation of what is meant by *Layer 3*. It is simply assumed that you know what this name means. The OSI model, therefore, has become required foundational knowledge for anyone seeking to work in the computer or data networking industry. Many certification exams will not test you on the OSI model directly, but will phrase questions in such a way so that you will have to understand the OSI model—as well as some other set of facts—in order to answer the question correctly.

For example, it is not uncommon to see questions like this: You are a network administrator working for a manufacturing company. You want to enable secure VoIP communications at Layer 3. What technologies can you use to implement this security?

The possible answers will, of course, be a list of protocols. You'll have to know which of these protocols both provides security and operates at Layer 3 of the OSI model. While you will not see this exact question on the CTP+ examination, you will be greatly benefited by learning the OSI model for both your certification examination and everyday workload. Not to mention the fact that you'll actually be able to understand all those articles, whitepapers, and books that refer to various layers of the OSI model.

The most important thing to remember about all of this is that in actuality the Application layer on one device never talks directly to the Application layer on another device even though they are said to be peers. Instead, the communications travel through many intermediaries (OSI layers) on the way to the final destination. This layered effect is really no different from human communications. Layering is seen in human interactions as well.

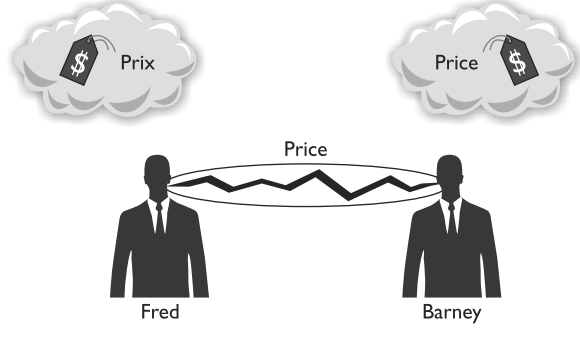
Notice in Figure 1-9 that we have two humans communicating. Behind the communications is an initial thought that needs to be transferred from Fred to Barney. This thought may or may not already be in a language that Fred and Barney know. In this case, we assume that Fred's native speaking language is French and Barney's is English. The result is that Fred's thought is in French and he must translate it into English before he speaks it. After the thought is translated into English, his brain must send signals to the vocal chords and mouth to transmit the signals of sound that result in English enunciation. Now the signals (sound waves) travel through the environment in which they are spoken until they reach Barney's ears. The eardrums receive these signals and send the received information to the brain. Here the information is interpreted and may or may not have been received correctly. Barney can send back a signal (verbal, visual, or kinesthetic) to let Fred know his understanding so that Fred can be sure Barney received the communication properly.

Do you see the similarities? Much as the Session layer represents data in a way that the remote machine can understand it, Fred's brain had to translate the original French thought into a shared language. Much as the Physical layer has to transmit electrical signals on a wired network, the vocal cords and mouth had to transmit signals as sound waves to Barney's ears. The point is that we could break human communications into layers that are similar to that which is defined in the OSI model. Also, the goal here is to provide peer communications from the "thought area" of the brain to another person's "thought area."

Always remember that the OSI model is a reference and not an actual implementation. It is also useful to remember that data travels down through the OSI model on the sending machine and up through the OSI model on the receiving machine. Finally, remember that every device on a network will not need to extract everything within the encapsulated data in order to do its job. For example, a Layer 3 router can extract only to the point of the Layer 3 data and still route the data packets just fine.

FIGURE 1-9

Layering in human communications



exam Watch

You will hear of many different techniques for memorizing the layers of the OSI model. While I can sympathize with these techniques for exam preparation, I encourage you to fully understand the communications process that occurs within the OSI reference model. When you remember what each layer does, it is almost automatic that you'll remember the layers in the proper order. This correlation is because communications should occur in the order in which the layers define them. It's really easy to remember a story, so think of the story of an e-mail message traveling down the stack and across the network to its destination.

CERTIFICATION OBJECTIVE

1.1.3 OSI/RM Protocols, Services, and Equipment

In addition to an understanding of the OSI model and the actions that occur at each layer of the model, you should understand the different protocols and equipment that operate at each layer. In this section, you will discover the many protocols that can function at each layer of the OSI model. Many of the protocols listed in this section are further explored in later chapters. At this point, you need not concern yourself with a mastery of each protocol. For now, be sure you know what protocols work at each layer of the OSI model.

exam Watch

As you study for the CTP+ exam, remember that protocols allow for services. For example, the DNS protocol allows for the service of hostname resolution. The specific services for each protocol will be explained more fully throughout the pages of this book.

Application Layer Protocols and Equipment

The Application layer is the interface to the user in a networked environment. This is the first layer of packet creation in a network. The following protocols operate at the Application layer:

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- H.323
- Hypertext Transfer Protocol (HTTP)
- Lightweight Directory Access Protocol (LDAP)
- Media Gateway Control Protocol (MGCP)
- Post Office Protocol 3 (POP3)
- Session Initiation Protocol (SIP)
- Simple Mail Transfer Protocol (SMTP)
- Telnet
- Trivial File Transfer Protocol (TFTP)

In addition to the knowledge that these protocols operate at Layer 7, you should understand that the following equipment also operates here (many devices operate at several layers of the OSI model):

- Gateways
- Gatekeepers
- Application-level gateways (firewalls)
- Load balancing devices

Presentation Layer Protocols and Equipment

The Presentation layer provides transformations of data so that it is in compliance with standards such as ASCII or EBCDIC. The following protocols operate at Layer 6:

- Abstract Syntax Notation 1 (ASN.1)
- Audio codecs:
  - G.711
  - G.722

- G.723
- G.728
- G.729

- Media codecs:
  - MPEG-1
  - MPEG-2
  - MPEG-4
  - JPG
  - GIF
  - PNG
  - TIFF

In addition, the following equipment operates at the Presentation layer:

- Gateways
- Gatekeepers

Session Layer Protocols and Equipment

Layer 5, the Session layer, defines how protocols make and break connections. The following protocols operate at this layer:

- AppleTalk Session Protocol (ASP)
- NetBIOS
- Real-time Transport Control Protocol (RTCP)
- Structured Query Language (SQL)

In addition, the following equipment operates at Layer 5:

- Gateways
- Gatekeepers

Transport Layer Protocols and Equipment

The Transport layer provides transport between two applications with Session layer connections. The following protocols operate at Layer 4:

- AppleTalk Transaction Protocol (ATP)
- Real-time Transport Protocol (RTP)

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

The following equipment operates at Layer 4 of the OSI model:

- Circuit-level gateway (firewall)
- Gateways
- Multilayer switches (also called Layer 4 switches)

Network Layer Protocols and Equipment

Logical addressing takes places at the Network layer, allowing for scalable networks. The following protocols operate at the Network layer:

- Address Resolution Protocol (ARP)
- Border Gateway Protocol (BGP)
- Datagram Delivery Protocol (DDP)
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)
- Internet Protocol (IP)
- Open Shortest Path First (OSPF)
- Reverse Address Resolution Protocol (RARP)
- Routing Information Protocol (RIP)

The following equipment operates at Layer 3:

- Multilayer switches (also called Layer 3 switches)
- Packet filter (firewall)
- Router

Data Link Layer Protocols and Equipment

Physical data formats take place at the Data Link layer so that information can be transmitted as bits on the medium. In addition, this layer is responsible for physical addressing. The following protocols operate at Layer 2:

- Ethernet (802.3)
- Logical Link Control Protocol (LLC – 802.2)
- Wireless LAN (802.11)

The following equipment operates at Layer 2:

- Bridges
- Network interface card
- Switches

Physical Layer Protocols and Equipment

The Physical layer is responsible for the actual transmission of data. No actual protocols work here because everything has been defined before this layer. You could say that the standards for Ethernet cabling work here. Certainly the standards for Wi-Fi modulation work here. While not commonly thought of as protocols, they do fit the description of a protocol as a standard way to communicate. The following equipment types also operate here at Layer 1:

- Channel Service Unit/Data Service Unit (CSU/DSU)
- Hub
- Modem
- Network interface card
- Repeater

CERTIFICATION OBJECTIVE

1.1.4 TCP/IP Model Protocols, Services, and Equipment

The OSI model is a logical model of communications for networked devices and software. The OSI model does not specify the protocols that should be used at each of the seven layers, but it specifies the functionality that should be provided by those protocols. For this reason, you will read and hear statements like "FTP is a Layer 7 protocol" and "TCP is a Transport layer protocol." These phrases are used to indicate the layers within the OSI model where the protocols operate. The reality, however, is that many protocols and network communications in general do not occur in line with the OSI model. TCP/IP is a perfect example. While we can relate the TCP/IP communications model to the OSI model, it cannot be said to meet the OSI specifications or operate in the way the OSI model indicates to exactness.

This concept is important to keep in mind. It is also why some documents will indicate that a certain protocol operates as Layer 6 and another document may indicate that the exact same protocol operates at Layer 7. Since TCP/IP implements only four layers, the Application layer of the TCP/IP model may be said to encompass Layers 5 through 7 of the OSI model. Even though the TCP/IP model has a layer called the Application layer, this layer is not equivalent to the OSI model's Layer 7, which is also known as the Application layer. Instead, you could say that the OSI model Layer 7 functionality is included in the TCP/IP Application layer. In the end, protocols may be said to function according to the OSI model only theoretically, and they may indeed have their own actual communication model that is very different or somewhat different from the OSI model of communications.

Once you have the physical network connections in place using Ethernet or Wi-Fi or some other protocol, you will need to implement a protocol suite that can provide the functionality for Layers 3 through 7 of the theoretical OSI model. There is no question about the most popular protocol suite in use today, and it is the only suite that I will cover in this chapter. That suite is the TCP/IP protocol suite.

It's important to remember that there is really no such thing as the TCP/IP protocol. TCP is a protocol, and IP is a protocol (though they were the same Transmission Control Protocol from 1974 to 1978, when the single TCP solution was split into TCP for host-to-host communications and IP for network routing). The name TCP/IP indicates that the TCP segments travel as IP packets over the network. In other words, TCP travels over IP just as FTP travels over TCP and SNMP travels over UDP. We're back to the layering concepts again. For this reason, it's important to understand the TCP/IP model as opposed to the OSI model.

TCP/IP Model

Unlike the OSI model's seven layers, the TCP/IP model contains only four layers. The four layers of the TCP/IP model are

- Application layer
- Transport layer
- Internet layer
- Link layer

The *TCP/IP Application layer* can be said to encompass the OSI model's Application and Presentation layers. In other words, Layer 4 of the TCP/IP model performs the services required of Layer 6 and Layer 7 of the OSI model. RFC 1122 specifies two categories of Application layer protocols: user protocols and support protocols. User protocols include common protocols like FTP, SMTP, and HTTP.

These protocols are all used to provide a direct service to the user. FTP allows the user to transfer a file between two machines. SMTP allows the user to send an e-mail message. HTTP allows the user to view webpages from a website. Support protocols include common protocols like DNS, DHCP, and bootstrap protocol (BOOTP). DNS provides name resolution for user requests. For example, if a user requests to browse the home page at www.SysEdCo.com, the DNS support service resolves the website's domain name to an IP address for actual communications. Because this protocol is an indirect service for the user, it is considered a support service as opposed to a user service. DHCP and BOOTP are both used to configure the IP protocol—and possibly other TCP/IP parameters—without user intervention.

The *TCP/IP Transport layer* provides host-to-host or end-to-end communications. Transport layer protocols may provide reliable or nonguaranteed data delivery. TCP is an example of a Transport layer protocol that provides reliable delivery of data (usually called segments), and UDP is an example of a protocol that provides nonguaranteed delivery of data (usually called datagrams). Notice that I did not say that TCP provides guaranteed delivery of data. This is because no network protocol can provide guaranteed delivery of data; however, reliable protocols do provide notice of undelivered data, and UDP does not provide such a notice. Later in this chapter I'll explain why a nonguaranteed data delivery model is useful and how it plays an important role in VoIP networks.

The next layer is the *TCP/IP Internet layer.* The Internet layer is where host identification is utilized to route TCP segments and UDP datagrams to the appropriate end device. The protocol that all Application and Transport layer protocols use within the TCP/IP model is the Internet Protocol (IP). The IP provides the routing functionality that enables the implementation of very large LANs and communications across the Internet. In addition to IP, the Internet Control Message Protocol (ICMP) is considered an integral part of IP, even though it actually uses IP for communications just like TCP and UDP. So ICMP is considered an Internet layer protocol because of its integral use in IP-based communications.

The final or bottom layer of the TCP/IP model is the *Link layer.* This layer is where the upper-layer TCP/IP suite interfaces with the lower-layer physical transmission medium. Some have said that the Link layer is equivalent to the Data Link layer of the OSI model, and of the TCP/IP layers, this description is probably the most accurate linkage of all. In fact, when TCP/IP runs over Ethernet, there is no real Link layer provided by TCP/IP; instead, the MAC and PHY of the IEEE 802.3 protocol provide the functionality of the TCP/IP Link layer to the TCP/IP suite. It is also interesting to note that protocols such as ARP and RARP that actually service the

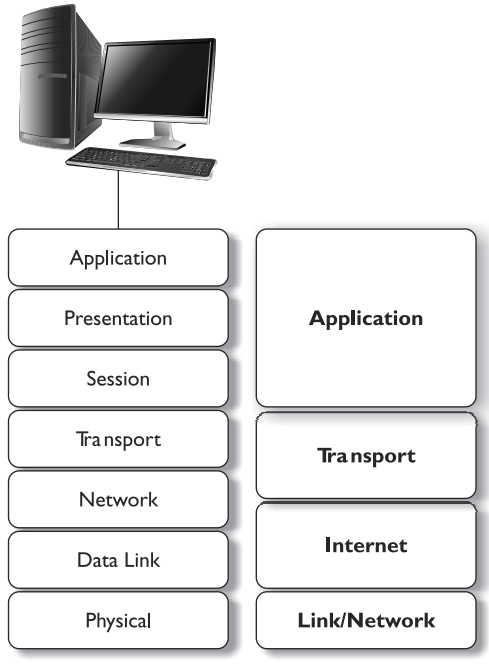
IP protocol are not actually Link layer protocols themselves. Instead, they seem to exist in some ambiguous land between the Link layer and the Internet layer. I would suggest that they are simply part of the Internet layer and that you could represent the Internet layer as having an upper management layer (ICMP, IGMP, etc.), a routing layer (IP), and a routing service layer (ARP and RARP); however, this idea is only my thinking and not really part of the standard TCP/IP model.

It has been much debated over the years whether ARP exists at Layer 2 or Layer 3 of the OSI model or at the Link layer or Internet layer of the TCP/IP model. I suggest that this debate exists because ARP really works between these layers. In fact, ARP is used to resolve the MAC address (a Layer 2 address) when the IP address (a Layer 3 address) is known. It could be said that ARP provides a service *between* these two layers, and this placement may be the point of argumentation and debate. Wherever you decide to place the protocol, know that you will likely meet opposition to your view.

Figure 1-10 shows a common mapping of the TCP/IP model to the OSI model. Again, keep in mind that this diagram is a mapping for understanding purposes only and that the TCP/IP suite of protocols makes no attempt or claim to mapping in this way. It is simply a helpful way of thinking about the functionality of the suite.

FIGURE 1-10

TCP/IP model mapped to the OSI model



exam Watch

Now that you understand how the TCP/IP model maps to the OSI model, you can determine the protocols, services, and equipment that work at each layer of the TCP/IP model by referring back to the section "OSI/RM Protocols, Services, and Equipment."

CERTIFICATION OBJECTIVE

1.1.5 Data Encapsulation

Segmentation is the process of segmenting or separating the data into manageable or allowable sizes for transfer. As an example, the standard Ethernet frame can include a payload (the actual data to be transferred) of no more than 1,500 octets. An *octet* is eight bits and is usually called a *byte*. Therefore, data that is larger than 1,500 bytes will need to be segmented into chunks that are 1,500 bytes or smaller before they can be transmitted. This segmentation begins at Layer 4, where TCP segments are created, and may continue at Layer 3, where IP fragmentation can occur in order to reduce packet sizes so that they can be processed by Layer 2 as Ethernet frames.

Encapsulation is the process of enveloping information within headers so that the information can be passed across varied networks. For example, IP packets (also called *datagrams*) are encapsulated inside of Ethernet frames to be passed on an Ethernet network. This encapsulation means that the IP packet is surrounded by header and possibly footer information that allows the data to be transmitted. Ethernet frames consist of a header that includes the destination and source MAC addresses and the type of frame in the header. The frames also have a footer that consists of a frame check sequence (FCS) used for error correction. Figures 1-2 through 1-8 depict the way the data changes as it travels down through the OSI model; notice how encapsulation begins to occur at Layers 5–7 in an almost vague way (because there is no direct mapping of TCP/IP to the OSI model) and then becomes very clear as we approach Layers 1 through 4.

Table 1-3 provides the term used for the information at the different layers of the OSI model. Notice that the first three layers reference the information simply as data. The bottom three layers use distinct terminology in most literature, such as segments, packets, frames, and bits.

TABLE 1-3 Data Encapsulation Terminology

OSI Model Layer	Information Terminology
Application	Data: At this layer, the application data is accompanied by the Application layer header.
Presentation	Data: At this layer, the data includes the information from the Application layer and the Presentation layer header.
Session	Data: At this layer, the data includes the information from the Presentation layer and the Session layer header.
Transport	Segment: At this layer, the data includes the information from the Session layer and the Transport layer header.
Network	Packet: At this layer, the data includes the information from the Transport layer and the Network layer header.
Data Link	Frame: At this layer, the data includes the information from the Network layer and the Data Link layer header.
Physical	Bits: At this layer the frames are transmitted as a series of ones and zeros on the medium. Depending on the standard, the frame may be preceded by a preamble, which is a series of bits used to indicate that a frame is about to be transmitted.

CERTIFICATION OBJECTIVE

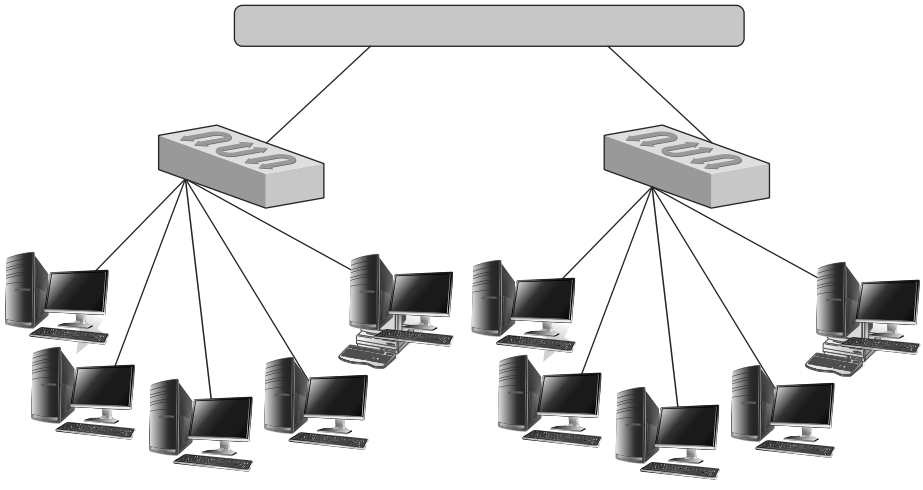
1.2.1 Network Topologies and Cable Distribution Schemes

Networks can be physically and logically designed in many different ways. As an example, Figure 1-11 shows a diagram of a network that effectively uses a bus topology, which you will learn more about later in this section, at the core and then implements a number of interconnected star topologies for end-node connectivity. The point is that you can design your physical network in many different ways, and it is up to you to implement the structure that best serves your organization's needs.

In addition to these physical implementation models, we have many different logical ways to think about the network. When considering logical network design, a layered approach is usually used. A single device can operate at one layer or in multiple layers at the same time. It is only for the sake of thought processes

FIGURE 1-11

A combination topology



and administrative boundaries that we conceptually place the logical model over the physical model. In this section, you will learn about both physical design considerations and logical design philosophies that have become very important in converged networks. Then you will explore various network topologies and cable distribution schemes.

Network Design Models

When it comes to the actual physical implementation of your network, you have two primary options. The centralized network has been used for more than 30 years, and the decentralized network has evolved over the past 20 to become the most common network implementation types.

Centralized Versus Decentralized

The common example of a centralized network model is the traditional mainframe implementation. In this model, all the network resources and processing power are in a centrally located, powerful computer. The access nodes were usually dumb terminals, and they were given this name because they had no local intelligence for any processing other than the display of the information sent back from the mainframe or IBM AS/400. Eventually, some companies began installing desktop PCs with terminal emulation software installed that allowed users to run powerful programs on the local PC while also accessing the centralized information on the mainframe.

Today, computing systems are often built using a technology known as virtualization. With this technology, a single physical server is configured to run multiple virtual servers. Vendors like Microsoft and VMware provide virtualization solutions. Both vendors offer solutions that allow users to access either a virtual desktop or virtual applications that are actually running on the server while they control the screens locally. This model is similar to the mainframe days, but it uses a rich graphical interface.

Modern centralized networks often employ multiple servers at the center of the network, but all communications come into the center from a surrounding "ring" of networked devices. This design is also sometimes called centralized computing today. Often the ring is only a virtual ring, but all of the network resources sit behind one entry point, usually a router. An example of this is depicted in Figure 1-12. This model may be better called centralized resource networking, as all the resources are on a single segment, but it is often referenced as centralized networking. In the strictest sense, centralized networking refers to the data and processing existing at the center and access provided through a distributed model.

Decentralized networking indicates that the network resources are close to the point of need. For example, the file server used by the accounting department may be on the same network segment as the accounting department. The database server used by the engineering department may be on the same segment as the engineering department. This concept is depicted in Figure 1-13. This design is probably the

FIGURE 1-12 Centralized resource networking

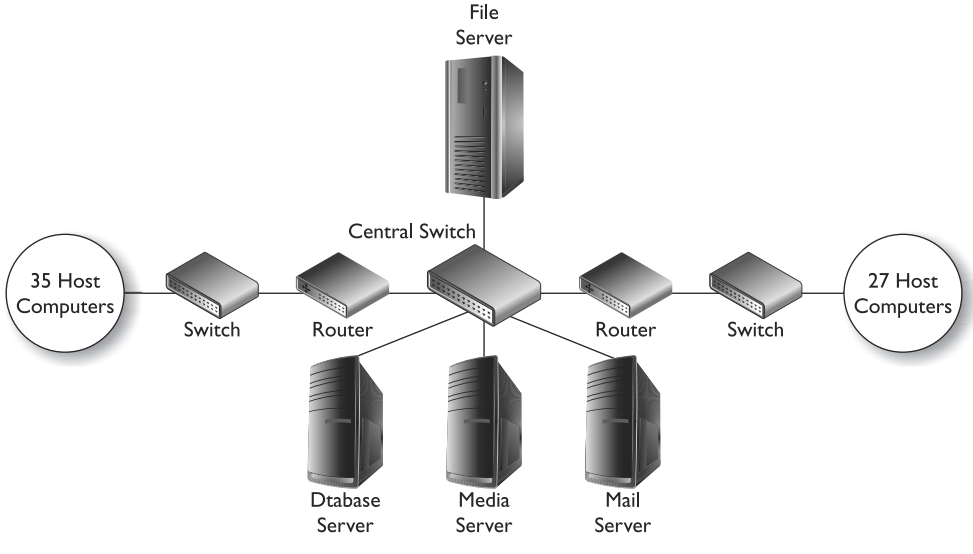
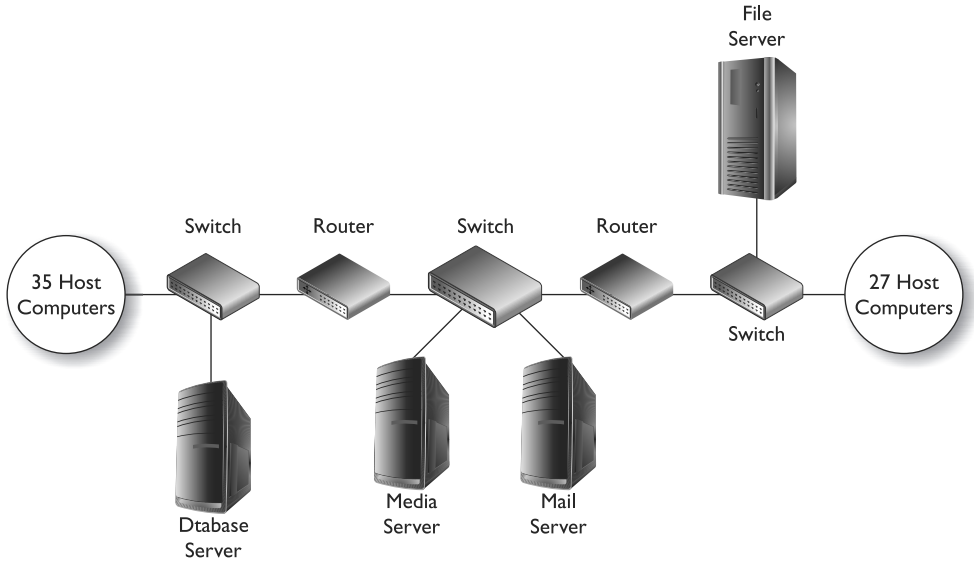


FIGURE 1-13 Decentralized networking



more common model being implemented today. No unnecessary data must traverse across the entire network. Users in one segment can certainly access resources in another segment, but the resources they need the most are closest to them—on either their segment or a close neighbor.

Configuring Converged Resources The concept of centralized versus decentralized networking becomes very important in a converged network. Voice data must travel as rapidly as possible from the sender to the receiver. Delays in data transfer can cause problems with voice communication, such as poor quality or dropped calls. Multimedia communications, such as streaming video, can also be impacted by your decisions here. The best practice is to keep communications as close to the network segment where they originate as possible when it comes to your nonconverged or traditional data (e-mail, file transfer, printing, etc.). This design keeps the backbone or Distribution layer "pipelines" open so that the voice or video data can move across it as quickly as possible. The reality is that voice data packets are very small, so they will move across the local segment very quickly once they reach it, even if they are in contention with other data packets. This concept is particularly true if QoS mechanisms are implemented, as discussed in Chapter 10.

However, dozens or even hundreds of calls may need to be routed across the backbone or Distribution layer of your network as quickly as possible. Keeping

unneeded traditional data off those layers can be helpful. This segregation will be most easily accomplished if you implement a decentralized model where the most needed resources are on the same segment, or at least within the same distribution group or workgroup.

Flat Versus Tiered Networking

When implementing a decentralized network, you can choose between a flat and a tiered networking model. In some ways, these two models are logical in nature in that a device in a tiered or layered model can exist in two tiers at the same time. This method results in the tier being more conceptual or functional than physical. The same physical device may perform functions in two tiers. Therefore, the actual physical implementation may not mirror the logical behavior of the network.

The flat network model is represented in Figure 1-14. Here we see that all of the switches and routers function in a similar way. They all implement access control lists and policies, and most of the switches have both routers and end nodes and other switches connected to them. In this model, there is no "fast" backbone because all of the devices perform security verifications and similar functions.

Now notice the difference in the model in Figure 1-15. Certain functions only take place within certain tiers or layers. In fact, the most common model has three layers: the Core layer, the Distribution layer, and the Access layer. Because each layer performs different functions and the Core layer does little more than move data, the overall performance of the network is improved. Let's look at each of these layers individually.

Core Layer As shown in Figure 1-15, the Core layer (sometimes called the network backbone) is responsible for moving a lot of data as fast as possible. This name is used because all global data access moves across this layer. In other words,

FIGURE 1-14 Flat network

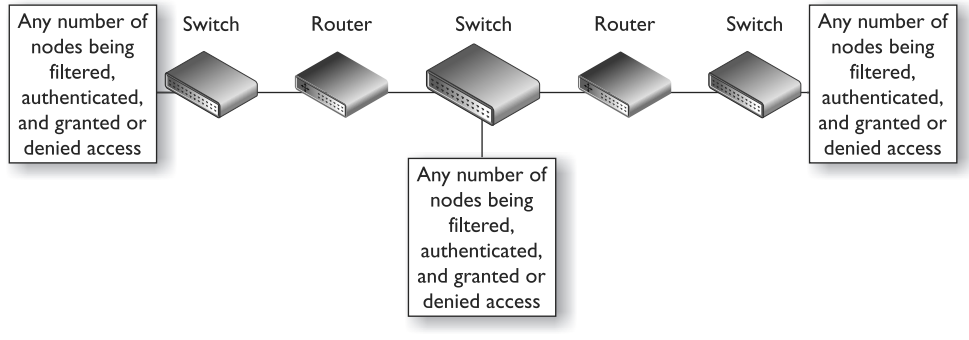
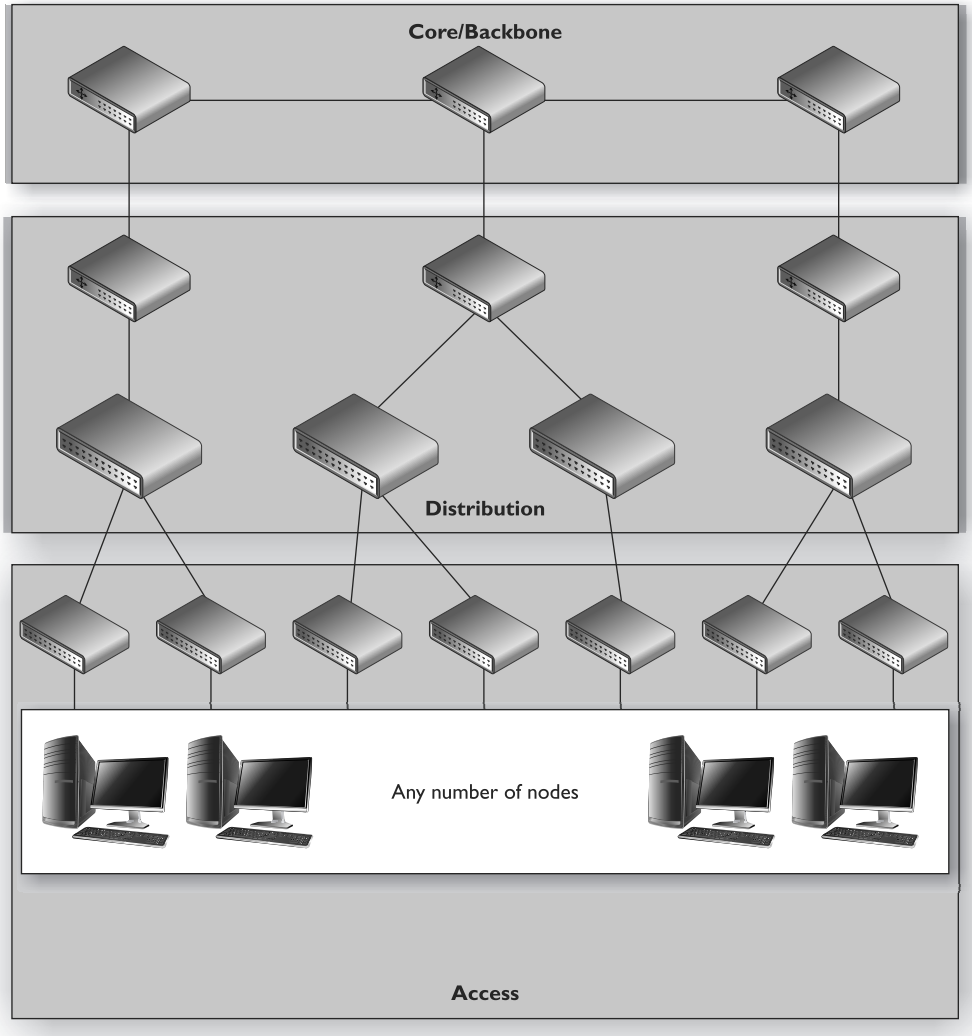


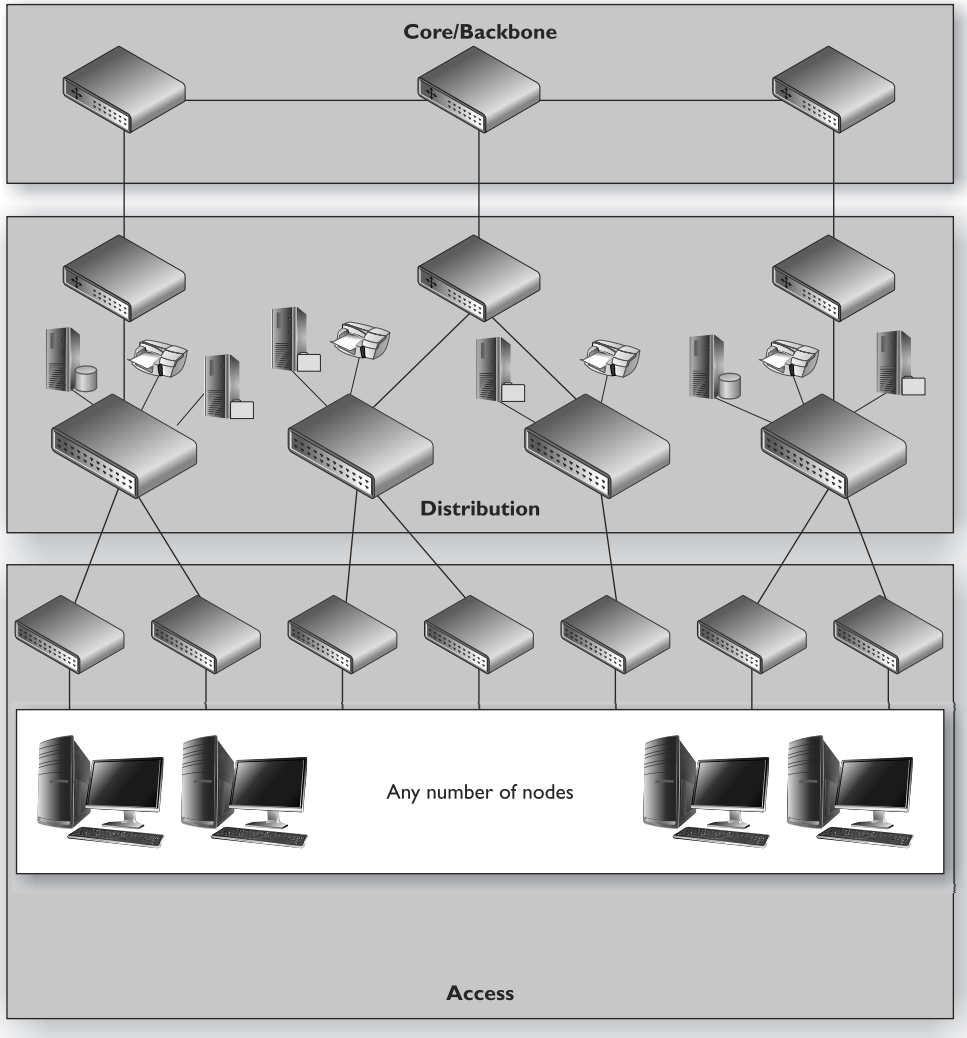
FIGURE 1-15 Tiered or layered network



when users in one office want to access resources in another office, that data will most likely pass across the Core layer. The Core layer may or may not include links to the WAN, and a network core can exist even in a single building implementation. For example, you may choose to implement a series of Gigabit Ethernet routers that route between three or four major sections of your network at the Core layer. Figure 1-16 illustrates a configuration like this one. Notice that there is a Gigabit Ethernet connection from the Distribution layer routers to the Core layer routers and there is a Gigabit Ethernet connection between each of the three Core layer routers.

Here at the Core layer, there is no intensive packet analysis for security purposes. The data is simply moved along as quickly as possible. Notice in Figure 1-16 how each major section of the network has its own printers and file storage, as well as database servers. This placement keeps traditional data off the Core layer as much as possible and allows converged data to move across this backbone very quickly. You can never prevent traditional data from moving across the Core layer completely, but this design will greatly improve your overall converged data performance.

FIGURE 1-16 Fast Core layer implemented



Distribution Layer The Distribution layer is where access control lists (role-based access control, network-based access control, etc.) would be implemented as well as other policies. This layer acts as the intermediary between the Access and Core layers. It is at this layer that the decision is made as to whether data should pass across the Core layer or not, and it is this layer that directs data from the Core layer to the appropriate end devices. You will usually find firewalls, packet filters, queuing devices, multiple routers, and switches at this layer. You may choose to implement WAN links at this layer, though they may also be implemented at the Core layer. The Distribution layer is where the majority of network activity takes place, but it takes place in multiple separated networks all residing at the Distribution layer and interconnected by the Core layer.

Access Layer The Access layer will contain direct access devices such as hubs, switches, and wireless access points. This layer is where your desktop computers are connected to the network and your laptop computers as well. This layer is also where your VoIP phones are connected and associated with the network at large. You may also further segment your network at this point. For example, you may have multiple segments within the Distribution layer, as indicated in Figure 1-16, but you may create additional segments within each Distribution layer segment at the Access layer.

You may also have additional network access policies managed at the Access layer or in a shared management model with the Distribution layer. For example, you may have wireless access points at the Access layer configured to authenticate wireless clients using an authentication server that resides in the Distribution layer. With an implementation like this one, authentication is shared between the Access and Distribution layers.

Branch or Edge Network Solutions

Some network solutions are referred to as branch or edge devices in vendor literature and common vernacular among network engineers. This terminology arises from thinking about network solutions in terms of a tree analogy. The core of the network is often considered the *trunk*, while the distribution devices are considered the *branches* and the end nodes are considered the *edge* of the network.

Some devices are considered edge devices by default. For example, a firewall is usually referred to as an edge or perimeter device. This name is used because it is installed at the edge of a network and allows controlled communications with the outside world or the remote networks. Other devices like spam filters, e-mail gateways, and certain VoIP gateways may also be considered edge devices.

Network Topologies

At this point, you have a foundational understanding of the fact that computers can be connected together to form networks using various connection media and devices such as switches and routers. In addition to this knowledge, it is important that you understand the different types of networks that you can build and the topologies that you can implement within those networks. Of the network types, you will need to be familiar with LANs, MANs, WANs, and GANs for the CTP+ examination.

LAN

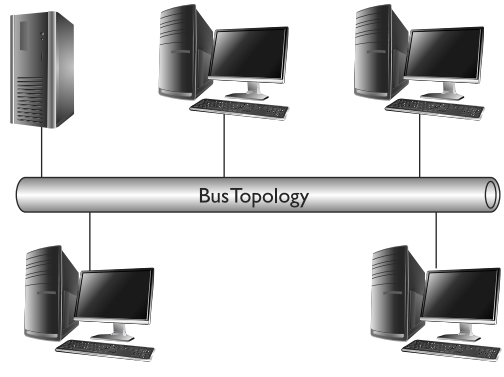
A LAN, or local area network, is usually defined as a group of computing devices connected by a high-speed communications channel that is localized to a campus or single property. A LAN would not be inclusive of the Internet, though it may be connected to the Internet. LANs may be connected together over distances measured in miles or kilometers, but these connected LANs would still be separate LANs, though together they may form a WAN or a metropolitan area network (MAN). A MAN is a network that covers an entire city or region.

LANs can be implemented using many different topologies, including bus, star, mesh, and hybrids. The following sections describe each of these.

Bus The *bus topology*, as depicted in Figure 1-17, requires that all communicating devices share a single bus or communication medium. This bus is usually a coax copper wire that is connected with Bayonet Neill–Concelman (BNC) connectors and BNC Ts and terminators using 50-ohm cables and connectors. The biggest problems with the bus topology are in the maximum device threshold and the single point of failure problem.

FIGURE 1-17

Bus topology



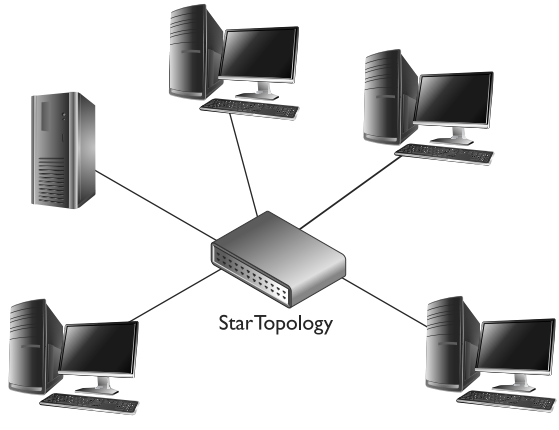
Because all devices share the same bus, you can quickly overwhelm a bus topology. This limitation is because communications occur when a device transmits a signal (frame) on the bus. Only one device can transmit at a time, and this can result in greatly diminished overall bandwidth. For example, there is just 10 Mbps available in common bus topology implementations that use coax cabling. If ten computers were on the bus—even ignoring network management overhead—each computer would only have an average of 1 Mbps available to it when all devices need to communicate. If 100 devices were on the bus, well, you get the picture. The bus becomes saturated very quickly.

In addition, due to the way the frames are passed up and down the bus and the large number of connectors along the way (each computer introduces a new T-connector), there are many potential points of failure. If one T-connector goes bad, the whole bus shuts down. If one computer is disconnected and the technician fails to couple the bus cable after disconnecting the computer, the circuit is broken and the bus shuts down. As you can see, the bus topology is not the ideal topology for modern networks—at least not by itself.

Star Figure 1-18 shows a star topology. The *star topology* is a hub-and-spoke type of network. All the devices communicate back to the central "hub," and the "hub" passes the information out to the proper "spoke." We rarely use real hubs anymore because they are not as efficient as switches in their utilization of the medium. Hubs receive information from one port and flood it out to all other ports whether they all need it or not. Switches, on the other hand, learn about the devices connected to each port and then only forward information to needed ports as much as possible. Switches or hubs can be used to form a star topology.

FIGURE 1-18

Star topology



Of course, you still have a single point of failure. If the switch itself should crash, the star goes down. However, it's much easier to troubleshoot a failed switch than it is to locate the point on the bus where a failure has occurred. For this reason—and the more efficient use of bandwidth—star topologies are much more common in modern LANs.

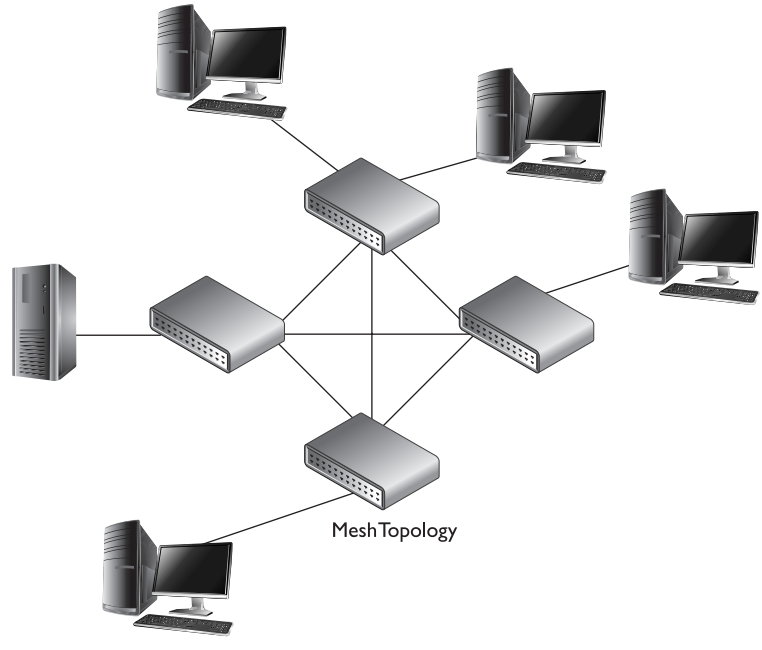
exam Watch

A mesh topology may be a full mesh or a partial mesh. A full mesh topology requires that each infrastructure device be connected to every other device. A partial mesh allows for some devices to be connected to all other devices, while other devices are connected only to a subset of the infrastructure nodes.

Mesh A *mesh topology* is a network structure that includes redundancies for fault tolerance and/or increased bandwidth. Figure 1-19 shows an example of a mesh topology. With this structure, there are multiple routes from and to any endpoint. For example, if router C should fail, the nodes from segment 1 could reach segment 2 through router B. The same is true in reverse: should router B fail, the nodes could reach each other through router C.

FIGURE 1-19

Mesh topology



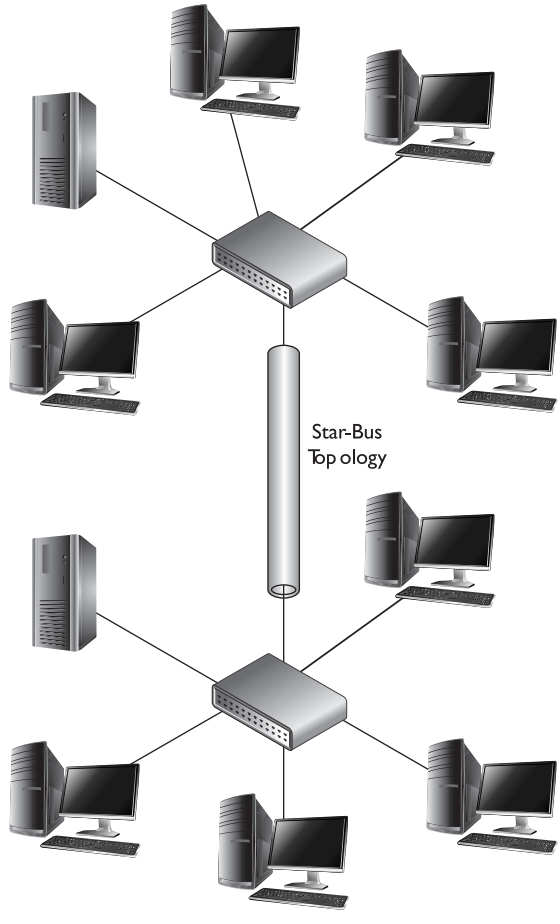
Hybrids A *hybrid topology* is any topology that blends bus, star, or mesh. For example, the star-bus (also called bus-star) topology often uses a bus topology to connect the infrastructure and a star topology for connecting nodes to that infrastructure. Figure 1-20 shows an example of a star-bus topology.

WAN

When you need to connect two LANs together that are separated by miles geographically, you will need to create a *wide area network (WAN)*. WANs are created using lower bandwidth connections than those used within the LAN. For example, it is not uncommon to have gigabit core speeds and 100 megabit speeds down to the individual nodes on LANs today. Very few WANs would support even

FIGURE 1-20

Star-bus topology



100 megabit speeds. Most WAN links will be less than 50 Mbps. This lower speed is simply a factor of cost. A full T3 connection can cost anywhere from $7,500 to $12,000 per month and would provide speeds up to 45 Mbps.

However, this speed variance can be overstated. The reality is that most users need to communicate more with users in the same building or location as they are. That's why they're in the same buildings. Years ago, before networks were even considered, the Industrial Revolution led to large offices for people who managed and administered the workers and products that were being developed in the factories. The optimization movements of that era led to the collocation of employees who needed to work with each other frequently. This model has not changed much today. Even with all of the talk of telecommuting, most people work within a three- to five-minute walk of mostly everyone they need to communicate with.

There are, of course, exceptions, like salespeople and others who spend more time communicating with those outside the company, but these are the exceptions and not the rule. This real-world example is why I say that too much emphasis can be placed on "slow" WAN links as opposed to LAN speeds. We don't need as much bandwidth on most WAN links.

With that said, VoIP and multimedia over IP can potentially impact this model; however, my experience working in companies with 25,000 people and more tells me that it will still be a percentage factor. WAN links are usually fine as long as they are between 20 percent and 35 percent as fast as the local network.

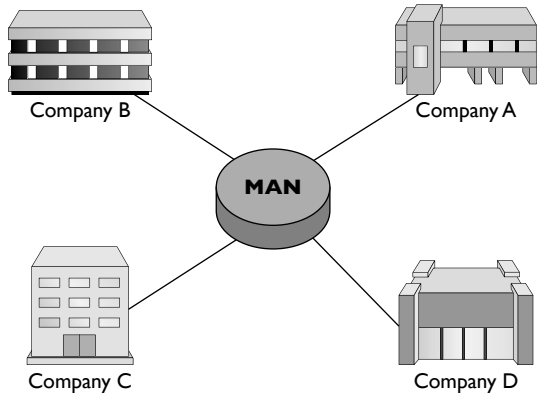
Many technologies can be used to implement WAN links, including DSL, ISDN, ATM, and Frame Relay. It is beyond the scope of this book to cover these WAN technologies in any greater detail, but you should know that they exist and the general concept of a WAN as opposed to a LAN.

MAN

A *metropolitan area network (MAN)* is a network that is usually established by the local municipality or another service provider. The network will span either an entire city or portions thereof and can act as the carrier for traffic between locations in the city for multiple organizations. Figure 1-21 represents this concept. Notice that the network is used by multiple companies that lease bandwidth or time on the network. This way the companies can simply subscribe to the MAN and do not need to worry about purchasing the components needed to form connections across the city themselves. MANs may be developed using wired or wireless technologies. If a MAN is implemented by the local telecommunications company (TelCo), it may be wired; however, most MANs that I've worked with have been wireless when implemented by municipalities or private organizations other than the local telecommunications company.

FIGURE 1-21

Metropolitan area network



GAN

Currently, the Internet is the primary example of a global area network (GAN). However, many refer to the connection between two to LANs as a WAN link or a WAN connection and they refer to the entire corporate network as the GAN, regardless of whether it spans the globe or just the eastern United States. Therefore, the simplest definition of a GAN is a group of interconnected LANs or WANs that cover an unrestricted geographic area.

CERTIFICATION OBJECTIVE

1.2.2 Data Networking Hardware and Connections

In Chapters 4 and 5, you will learn about infrastructure and client hardware in detail. At this point, you should gain a fundamental understanding of the hardware so that you can fully understand the topics in Chapters 2 and 3. This section addresses switches and routers as well as remote network connections.

Switches and Routers

Switches and routers are the building blocks of modern networks. The switches provide access to the network, and the routers build the network links between groups of switches. The following sections briefly explain each of these two important devices.

Switches

Telecommunications networks can implement two primary kinds of switching: circuit switching and packet switching. *Circuit switching* is used to reserve a route or path between the two endpoints that need to communicate. Because a circuit is reserved, the entire communication is sent in sequence and there is no rebuilding of the data at the receiver, as it is certain to arrive in order. Of course, this reservation means the bandwidth cannot be utilized by any other devices that may need it and can make circuit switching rather costly in today's packet-switched world. The benefit of circuit switching is that the connection is always there and the bandwidth is guaranteed as long as the connection exists.

Packet switching (also called *datagram switching*) is used to segment a message into small parts and then send those parts across a shared network. The first part may actually travel a different route than the second part and could in fact arrive at the destination after the second part. VoIP implementations, which are a large focus of the later chapters in this book, rely on packet switching as opposed to circuit switching. This design does introduce concerns, because the voice data must arrive quickly at the destination or calls can be dropped and sound quality can suffer. You will learn how to deal with those issues in Chapter 9, which focuses on QoS technologies.

The term *switching* can also represent the actions carried out by a network switch. In fact, a network switch is a device that performs packet forwarding for packet-switched networks. A switch can forward packets from an incoming port to the necessary outgoing port or ports in order to enable the packet to reach its destination. It is inside of these switches—as well as the routers I'll talk about next—that much of the QoS processing is performed. The switch can extract a frame and determine if it has QoS parameters and, if it does, treat it accordingly. You'll learn much more about switches in Chapter 3.

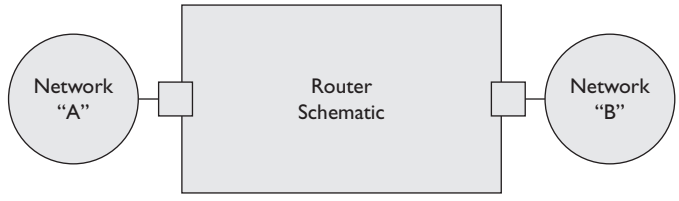
Routers

Routing is the process of moving data packets from one network to another. A data packet that is transmitted from a computing device may be able to move directly to another device on the same network, or it may need to be forwarded to another network by a router. This is the primary job of a router: to connect otherwise disconnected networks.

Here's a good way to remember the difference between a switch and a router: if you connect multiple switches together, you're just creating a bigger physical network segment. The same is not true with routers. In fact, you should really think of routers as being connected together. Instead, routers have two or more interfaces. As seen in Figure 1-22, one interface will be connected to one network and the

FIGURE 1-22

Routers routing packets



other interface will be connected to another. This demarcation allows the router to be used as a packet-routing device when a device in Network A wants to send a packet to a device in Network B. You'll learn more about routers in Chapter 3 as well as switches and other infrastructure devices.

Remote Network Connections

Remote network connections are very important. They can be used to create WAN links or links over long distances within a campus or a MAN. They can be used to connect branch offices back into corporate headquarters or to allow teleworkers to connect to the organization's network. The following remote network connection types should be considered.

Modems

Modems are devices that modulate and demodulate to allow for communications across different network types. The word modem has been used to describe wireless adapters, DSL connection devices, and even cable network connection devices. Modems can provide dial-up connections or high-speed connections. As a convergence technology professional, it is up to you to choose the right technology for a given scenario.

Dial-Up Versus High-Speed In today's networks, Internet connectivity has become essential. Very few organizations have no need for the Internet. At the very least, e-mail is utilized. When connecting your network to the Internet, you have two fundamental choices: very slow or faster. This choice may seem like an oversimplification, but with the current technology, it is also the reality. In the 1990s, I remember dialing up to the Internet and then downloading one- to ten-megabyte files and not feeling frustrated by the fact that it took between ten minutes and ten hours, depending on my connection quality. When the 56k modems came along, I thought I was in heaven and had reached the pinnacle.

Of course, these faster modems were quickly followed by ISDN and then DSL and even cable and satellite technologies that were much faster. The reality is that a dial-up line to the Internet is not likely to provide a fast enough connection for shared Internet in any installation. Even if only two or three users are browsing webpages, it will be unacceptably slow. Today, you will need DSL or business-class cable at a minimum. Larger companies will need dedicated or partial T1s and faster connections.

For this reason, your decision is not really between dial-up and high-speed Internet connections. The decision is to be made among the various high-speed technologies. If your organization has a few dozen people or more that will need access to the Internet (e-mail, web browsing, etc.) concurrently, you will likely need to acquire a high-speed T1 or fractional T1 line from a local provider. If your organization requires that only a few individuals access the Internet concurrently, you may be able to make your decision between the less expensive cable or DSL options.

DSL Versus Cable The DSL service has been a phenomenal option for small businesses and home users for a few years now. It provides speeds up to 52 Mbps on Very High Bit Rate DSL (VDSL), though this standard greatly limits the distance between the service provider and the subscriber unless fiber cabling is used. Asymmetrical DSL (ADSL) is the more common implementation in consumer and small business installations. ADSL provides up to 6 Mbps (6,000 Kbps) down-speeds and up to 640 Kbps up-speeds. This means that you can download faster than you can upload. This difference is an important point of decision if you are implementing any locally hosted services that must be accessed from the Internet side across the DSL connection. Table 1-4 provides a breakdown of the common DSL types and their features. It is important to remember that the actual speed of your DSL connections will depend on line quality, distance from the provider, and the speed of the provider's core network.

Cable Internet service has been in existence for more than seven years now and is very popular in many countries in larger metropolitan areas. This service is sometimes called *broadband cable* or *high-speed cable Internet*. Business-class cable Internet service can provide data rates of greater than 50 Mbps, while consumer-grade service is usually less than or equal to 10 Mbps.

DSL is a dedicated technology. This means that your connections should be very stable. What you get one day is very likely to be what you'll get the next. Cable Internet is a shared technology comparable to Ethernet. Your bandwidth will vary depending on the utilization of the network by other subscribers. Business-class cable

TABLE 1-4 DSL Types and Speeds

DSL Type	Speeds	Distance from Provider
ADSL	6 Mbps down and 640 Kbps up	Usually less than 3 km
ADSL Lite (also called G.lite ADSL or Universal DSL)	1.5 Mbps down and 512 Kbps up	Usually less than 3 km
Rate Adaptive DSL (RADSL)	Variable line speeds adjusted based on current conditions with maximums equal to ADSL	Usually less than 3 km
VDSL	52 Mbps down and 16 Mbps up	About 300 meters for maximum bit rate; bit rate degrades as the signal attenuates (or the bit rate decreases over longer distances)
Symmetric or Single Line DSL (SDSL)	2 Mbps down and up	Usually less than 3 km

subscriptions can provide guaranteed bandwidth, but consumer-class connections usually provide up to a certain bandwidth with either minimum bandwidth guarantees or no guarantees. Pay close attention to the contract when signing up for cable or DSL connections. You want to make sure you have the bandwidth you need for your intended use.

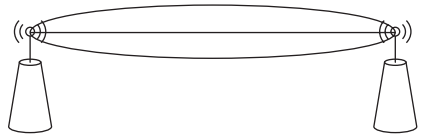
Wireless Media

Wired networking is not the only game in town. Wireless networking has become extremely popular in the last decade. There are many different wireless networking standards and technologies, and they vary in their implementation, but one thing is consistent: electromagnetic waves. They all use electromagnetic waves in order to transmit and receive data. In this section, I will briefly introduce the wireless media that are available. Some are used in WLANs, and others are used in wireless MANs or even wireless WANs.

Line of Sight Technically, any wireless technology can be made a line-of-sight technology by using highly directional antennas; however, some technologies are implemented with the intention of utilizing line of sight for communications. When two wireless endpoints communicate with each other in a highly directional, point-to-point fashion, they are said to be *line-of-sight* connections. Line-of-sight connections are used for bridge connections that connect two otherwise disconnected networks and for high-speed connections to data centers for distant areas in a facility. Figure 1-23 depicts a line-of-sight wireless link.

FIGURE 1-23

Line-of-sight wireless

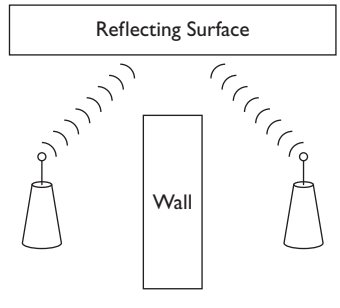


Non–Line of Sight The technologies used in WLANs are non–line-of-sight technologies. This is possible because they use semidirectional or omnidirectional antennas. Semidirectional antennas transmit the radio frequency (electromagnetic waves) signals in a wide path in one direction from the antenna, whereas omnidirectional antennas transmit the signal in all directions fairly evenly around the antenna. The result is that semidirectional antennas provide coverage over a greater distance in a specified direction, and omnidirectional antennas provide coverage over a lesser distance from the antenna in all directions. Figure 1-24 depicts a non–line-of-sight wireless configuration.

Satellite Satellite technology has come into common use for both television service and high-speed Internet service, particularly in rural areas where DSL runs would be too long or cable service is not provided. In addition, satellite is an excellent technology—assuming the bandwidth is sufficient—for both land and sea mobile stations. Satellite Internet connections have traditionally used *one-way with terrestrial return*. In other words, the data received from the Internet is transmitted from the satellite to the receiver and the data transmitted to the Internet is sent through a terrestrial connection (either a landline or a mobile phone). *Two-way* satellite Internet is much more expensive and requires line of sight. Therefore, two-way satellite installations require a well-trained engineer to install and align the equipment. One-way with terrestrial return is great for mobile and stationary connections requiring mostly downloads and little in the way of uploads, and two-way is suitable for stationary applications such as rural areas without other service provision.

FIGURE 1-24

Non–line-of-sight wireless



Wi-Fi The most popular wireless LAN technology is Wi-Fi, which is based on the IEEE 802.11 standards. The last five or six years have seen an explosion of interest and implementations in the Wi-Fi marketplace. I'll discuss Wi-Fi in more detail in Chapters 3 and 4 as we investigate infrastructure and client devices.

EVDO *Evolution Data Optimized*, or *EVDO*, is a broadband mobile wireless standard that has been implemented by several carriers around the world. In the United States, both Verizon Wireless and Sprint Nextel provide EVDO service. EVDO service typically provides down-speeds of between 512 Kbps and 1.4 Mbps. At my home in Ohio I can download at close to 1 Mbps in the right area (I have to be in the corner of the laundry room for best reception—it might not be ideal, but it works). Thankfully, I have 6 Mbps DSL that really works at 6 Mbps piped into my house.

EVDO is not the only game in town when it comes to cell-phone company high-speed Internet provision. Cingular (now AT&T), for example, provides its High-Speed Downlink Packet Access (HSDPA) broadband service. The HSDPA averages between 400 and 700 Kbps down-speeds and acceptable latency (the minimum time required to move data from one point to another).

CERTIFICATION SUMMARY

Understanding the OSI model is an important part of preparing for the CTP+ exam, and it's also an important part of preparing for a career as a network engineer. The reality is that it is a rare piece of vendor literature that does not reference the OSI model in some direct or indirect way. Normally, this documentation will simply state that a certain service is provided at Layer 2 or Layer 3 and will not even mention that it is referencing the OSI model. That's how ubiquitous the model is in network administration and engineering. This chapter introduced you to the OSI model, and you may want to read the actual standard—though you will not need to know any more about the OSI model for the CTP+ exam—in order to familiarize yourself with it even more.

You learned the basic differences between LANs, WANs, MANs, and GANs. The LAN is localized to a property or small area, and the others cover greater areas from metropolitan cities to unlimited global coverage.

You also had a brief introduction to some of the hardware used in networks, including switches and routers. You'll learn more about all of these devices in Chapters 3 and 4. In the next chapter, you'll take the information presented here about the OSI model and apply it specifically to various network protocols that actually make communications happen on your network.

TWO-MINUTE DRILL

Industry Bodies and Standards

- ❑ The industry standards organizations help define standards for the telecommunications and data networking industries.
- ❑ The IETF, ITU, and IEEE are examples of industry standards organizations.
- ❑ The governing bodies ensure that standards are developed in compliance with regulations by defining these regulations for electronic communications.
- ❑ The FCC and OfCom are examples of governing bodies.

OSI/RM Layers

- ❑ The OSI/RM was developed by the ISO and is used to describe network communications.
- ❑ The OSI model defines seven layers for network communications.
- ❑ The OSI model layers from top to bottom are Application, Presentation, Session, Transport, Network, Data Link, and Physical.

OSI/RM Protocols, Services, and Equipment

- ❑ Many devices operate at multiple layers of the OSI model, such as multilayer switches, gateways, and gatekeepers.
- ❑ The most popular protocols at the Transport layer are TCP and UDP.
- ❑ The most popular protocol at the Network layer is IP.
- ❑ For LANs, the most popular protocols at the Data Link and Physical layers are Ethernet (802.3) and Wireless LAN (802.11).

TCP/IP Model Protocols, Services, and Equipment

- ❑ The TCP/IP model does not map directly to the OSI model, as it has fewer layers; however, you can define a relatively close mapping to the OSI model.
- ❑ It is important to remember that the TCP/IP model is an actual protocol that has been implemented on networks, but the OSI model is more of a theoretical model.

Data Encapsulation

- As data passes down through the OSI model or TCP/IP model, it is encapsulated.
- When data is encapsulated, it is prepended, appended, or encased on headers and footers.
- Each layer of the network adds its own headers and possibly footers.
- Each layer treats the data from above it as the payload.

Network Topologies and Cable Distribution Schemes

- The network topology defines the architecture of the network.
- The star topology is defined by nodes connecting through a central device.
- The bus topology provides communications through a chained link of devices.
- The hybrid topology is a combination of other topologies.
- A full mesh topology is very expensive, as it requires every node to connect to every other node within the infrastructure.

Data Networking Hardware and Connections

- Switches are the primary Access layer devices in modern networks.
- Routers provide the interconnections between segments.
- Modems allow for communications on various media through modulation schemes.

SELF TEST

Industry Bodies and Standards

1. What industry standard organization is responsible for the actual development of RFCs for Internet standards?
   A. IETF
   B. IRTF
   C. IEEE
   D. FCC
2. What governing body controls the use of the electromagnetic spectrum in the United States in order to reduce interference and better use the bandwidth?
   A. IETF
   B. ISO
   C. FCC
   D. IEEE

OSI/RM Layers

3. Which layer of the OSI model is responsible for actually transmitting bits onto the communication medium?
   A. Physical layer
   B. Layer 3
   C. Transport layer
   D. Layer 5
4. At which layer of the OSI model does IP address management occur?
   A. Layer 3
   B. Application layer
   C. Layer 1
   D. Layer 5

OSI/RM Protocols, Services, and Equipment

5. You are implementing a new Voice over IP solution. The client has asked you to provide both wireless and wired access to the voice system. Which of the following are Layer 1 and 2 protocols that can be used to implement this solution?

A. Ethernet
B. Wi-Fi
C. TCP
D. UDP

TCP/IP Model Protocols, Services, and Equipment

6. You are implementing a Voice over IP solution. You want to make sure that your data is delivered in a timely fashion to the receiving device, and delivery confirmation is not required. Which of the following two protocols is the right choice?

A. TCP
B. UDP

Data Encapsulation

7. What is the difference between a frame and a packet?

A. The term frame usually refers to the data at Layer 2 that is ready to be transmitted.
B. The term packet usually refers to the data at Layer 2 that is ready to be transmitted.
C. Frames are encrypted and packets are not.
D. Packets are encrypted and frames are not.

Network Topologies and Cable Distribution Schemes

8. You want data packets that are transmitted from client computers on your network to be sent to computers they are intended for but not to other computers. Which combination of topology and device should you implement from those listed?

A. Bus topology with a switch
B. Bus topology with a hub
C. Star topology with a switch
D. Star topology with a hub

9. You have implemented a network solution that includes a single server that is accessed by 40 client devices. The client devices simply display the information sent back from the server, and all processing happens at the server. What kind of networking model have you implemented?

A. Tiered
B. Flat
C. Decentralized
D. Centralized

10. Which of the following are layers in a common tiered network model?
A. Core
B. Access
C. Presentation
D. Distribution

Data Networking Hardware and Connections

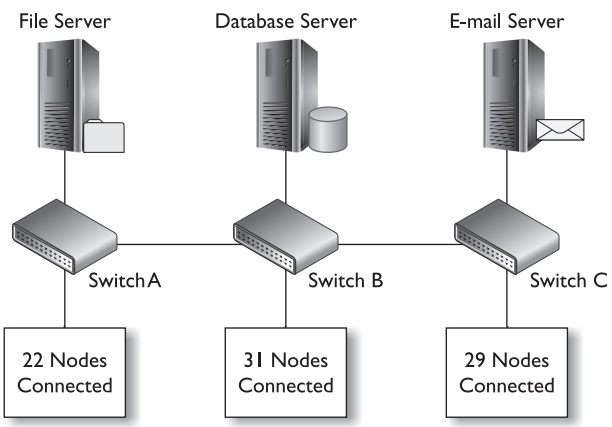
11. You need a device that will allow you to move data throughout your network based on IP address information. Which of the following devices are you most likely to implement?
A. Switch
B. Router
C. Access point
D. CSU/DSU

LAB QUESTION

You are implementing the network represented in Figure 1-25. This network has been designed by an individual who is not aware of a tiered network model. How could you redesign this network—while still providing the services needed by the end nodes—so that a tiered model is in place?

FIGURE 1-25

Flat network design needing to be rebuilt



SELF TEST ANSWERS

Industry Bodies and Standards

1. ☑ **A** is correct. The Internet Engineering Task Force (IETF) is the industry standards organization that develops the RFCs for Internet standards.
   ☒ **B**, **C**, and **D** are incorrect. These organizations do not develop RFCs, but serve other purposes within the industry.

2. ☑ **C** is correct. The Federal Communications Commission (FCC) is responsible for both wired and wireless communications regulation in the United States. This includes the electromagnetic spectrum (wireless).
   ☒ **A**, **B**, and **D** are incorrect. These organizations do not govern the electromagnetic spectrum, though they are involved in standards development for the industry.

OSI/RM Layers

3. ☑ **A** is correct. The Physical layer, also known as Layer 1, is responsible for transmitting bits onto the medium.
   ☒ **B**, **C**, and **D** are incorrect. While these are valid layers of the OSI model, they are not used to transmit bits onto the carrier medium.

4. ☑ **A** is correct. The Network layer or Layer 3 is responsible for IP address management.
   ☒ **B**, **C**, and **D** are incorrect. Layers 1, 5 and 7 (the Application Layer) are not responsible for IP address management.

OSI/RM Protocols, Services, and Equipment

5. ☑ **A** and **B** are correct. Both Ethernet and Wi-Fi are Layer 1 and 2 protocol solutions. They define a Layer 2 solution that is usually called a MAC layer and a Layer 1 solution that is usually called a PHY layer.
   ☒ **C** and **D** are incorrect. Both TCP and UDP are Layer 4 protocols in the OSI model and they are Transport layer protocols in the TCP/IP model.

TCP/IP Model Protocols, Services, and Equipment

6. ☑ **B** is correct. The User Datagram Protocol (UDP) provides connectionless communications and does not offer reliability; however, it is very timely, as it sends data faster and has less overhead than does TCP.

☒ **A** is incorrect. The Transmission Control Protocol (TCP) provides reliable delivery, but it does not provide timely delivery. Therefore, it should not be the foundation of Voice over IP implementations.

Data Encapsulation

7. ☑ **A** is correct. The term frame is usually used to reference the data that has been serviced by the Data Link layer and is ready to be transmitted on the wire. The term packet refers to the Network layer data (the TCP/IP model called this the Internet layer) that is managed by the IP protocol in most networks today.
☒ **B**, **C**, and **D** are incorrect. Layer two data is referenced as a frame and both frames and packets may be encrypted.

Network Topologies and Cable Distribution Schemes

8. ☑ C is correct. The star topology indicates that data be sent to the central device (the switch) and then the central device forwards the data to the intended machine only if that central device is a switch.
☒ **A**, **B**, and **D** are incorrect. The star topology with a hub would not meet our demands, as the data would be sent to all nodes on the star. The bus topology simply will not work since it does not traditionally use a switch.

9. ☑ **D** is correct. This scenario describes a centralized networking model.
☒ **A**, **B**, and **C** are incorrect. A tiered or flat network model has to do with how the data gets from node to node, and either could technically support either centralized or decentralized models.

10. ☑ **A**, **B**, and **D** are correct. The most common layered network design model is the three-layer model consisting of Core, Distribution, and Access layers. Do not confuse this with the OSI model, which is a network communications model. The OSI model of communications may operate over a flat or tiered network design model.
☒ **C** is incorrect. The Presentation layer is a layer of the OSI model and not a layer in the network design model.

Data Networking Hardware and Connections

11. ☑ **B** is correct. A router is a Layer 3 device and will move data based on IP addresses.
☒ **A**, **C**, and **D** are incorrect. Switches work at Layer 2 based on MAC addresses, and access points also work at Layer 2. The CSU/DSU is a WAN solution.

LAB ANSWER

Figure 1.26 shows a possible solution. Notice how the network now uses core routers at the Core layer and distribution switches that are connected to Access layer switches for end-node access. Notice that the servers are in the Distribution layer and are positioned closest to the users who need access to them.

FIGURE 1-26

Tiered model after redesign