Network Fundamentals

ITINERARY

- **Objective 1.01** Overview of How Networks Work
- **Objective 1.02** The OSI Seven-Layer Model
- **Objective 1.03** The TCP/IP Model

NEWBIE	SOME EXPERIENCE	EXPERT
4 hours	2 hours	1 hour

When you link computers together to share files and communicate and do all the things we like to do, you create a *network.* Networks range in size from the smallest and simplest network—two computers connected together—to the largest and most complex network of all—the Internet.

This chapter begins with an overview of all the pieces that come together to make a computer network, including the hardware needed to make the physical connections. The chapter then dives into two network models techs use to discuss network components and functions.

Objective 1.01 Overview of How Networks Work

Networks come in many sizes and vary widely in the number of computers attached to them. Some people connect two computers in their house so that they can share files and play games together—the smallest network you can have. Compare this to companies that have thousands of employees in dozens of countries and need to network their computers together to get work done. Network folks put most networks into one of two categories: LANs and WANs. You'll find a few other groupings as well.

A *local area network (LAN)* covers a small area and contains a modest number of computers (Figure 1.1). LANs are usually in a single building or group of nearby buildings. Typical LANs include home and school networks.

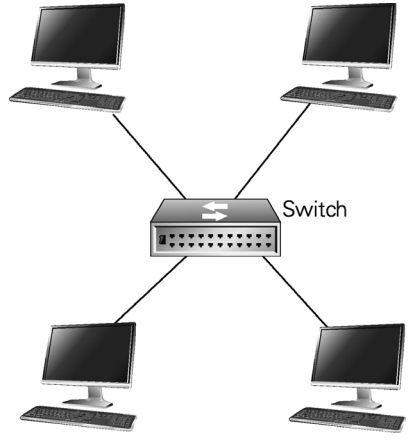


FIGURE 1.1 A local area network (LAN)

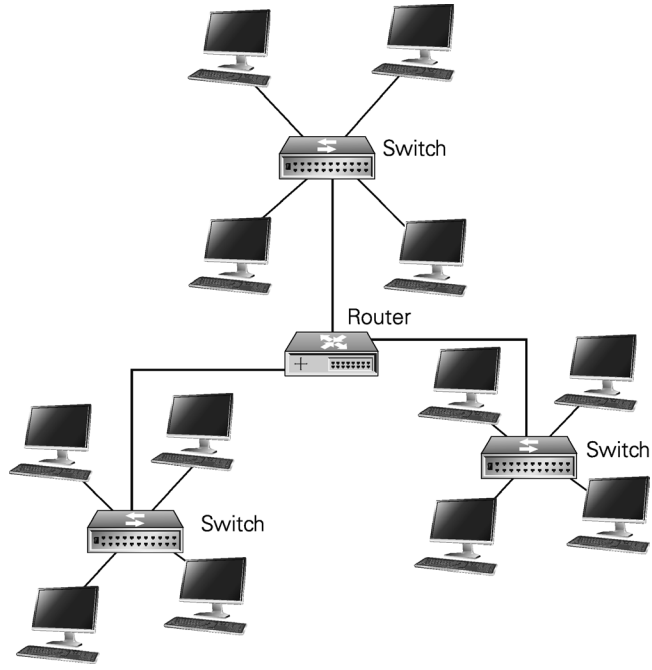


FIGURE 1.2 A wide area network (WAN)

A *wide area network (WAN)* covers a large area and can have a substantial number of computers (Figure 1.2). Usually, a WAN is composed of two or more LANs connected together. All of the LANs in all of the schools in a city school district, for example, link together to form a WAN. Computers in a WAN usually connect through some type of public network, such as a telephone system, leased lines, or satellites. The largest WAN in existence is the *Internet,* which is a worldwide network that connects millions of computers and networks.

An *intranet,* in contrast, is essentially a private TCP/IP network that is a scaled-down version of the Internet for a very specific group of users. Just like the Internet, an intranet will offer various network services, such as websites, FTP access, Voice over IP, and so on. The key difference is that it's private rather than public.

Another similar term, *extranet,* is used to denote a private intranet that is also made accessible to a select group of outsiders using the Internet.

Here are a few other *x*ANs in use in various networks:

- A *campus area network (CAN)* is a group of interconnected LANs within a small geographical area, such as a school campus, university, hospital, or military base.
- A *metropolitan area network (MAN)* is a group of networks with a sociopolitical boundary, such as a network of district authority offices in a town or city. MANs can range in size from a few city blocks to entire cities. Sites on a MAN are usually interconnected using fiber-optic cable or some other high-speed digital circuit, and the MAN itself may carry voice as well as data traffic.
- A *global area network (GAN)* is a single network with connection points spread around the world. GANs are used mostly by large corporate organizations and consist of a series of networked, orbiting satellites. Note the subtle difference between a WAN and a GAN. The latter is a single network, not a number of interconnected networks.

Travel Advisory

The terms CAN and GAN don't exist as official standards, but their use and definitions have become generally accepted over time. A MAN is an official standard of the Institute of Electronics and Electrical Engineers (IEEE) as the IEEE 802.6 standard.

Servers and Clients

People use two types of devices in networks these days: servers and clients. In a nutshell, *servers* share things—such as files, folders, and printers—and *clients* request access to those shared things. Let's get one thing straight: Almost any personal computer can act as a server or a client or both! A lot of it has to do with how you set up the computer.

Computers running Windows, Macintosh, and the many varieties of Linux make up the vast majority of clients. You'll also find other devices that are clients, though, such as the following examples:

- Game consoles, like the Xbox 360
- Smartphones and tablets, such as the iPad
- DVRs, like TiVo and other set-top boxes

Server computers come in all shapes and sizes, but they serve—if you'll pardon the pun—a similar purpose. Servers manage *network resources* (like printers and

FIGURE 1.3 A server sharing network resources

e-mail—all the stuff that makes a network valuable), provide central storage of files, and provide services for users (such as the printer server telling the printer to print, or the e-mail server sending your e-mail). See Figure 1.3.

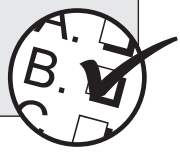
Client computers enable you to access the shared resources, programs, and services on server machines (Figure 1.4). Most users access servers via clients, although there's no law that says you can't access a server from another server machine. The latter machine, in that case, would be *acting* as a client regardless of the firepower of the box!

FIGURE 1.4 A client accessing network resources

Networks are traditionally classified into *client/server* and *peer-to-peer designations,* depending on the role played by each computer in the network. In a client/server network, one or more computer systems act as a server, while the remaining computers are clients that access resources from the server. On some home or small office networks, however, there may not be a separate server. Instead, every computer on the network acts as both a client and a server. Such networks are called peer-to-peer networks.

Exam Tip

The CompTIA Network+ exam uses the terms *client/server topology* and *peer-to-peer topology* to describe these two network arrangements. A *topology* more commonly refers to the way computers connect together rather than the roles they play on a network, but be prepared for the unusual use of the word on the exam. Chapter 3 covers the more commonly described network topologies.



Every operating system (OS) today can operate as a client, a server, or both, and many networks employ a mix. My network, for example, has a set of dedicated servers and each employee has one, two, or more computers in his or her office. Many of the office computers have shared folders, such as music or games, so they function as both clients and servers. This nice mishmash of machine roles creates a *hybrid* network.

Network Components

Whether you want to put together a LAN or connect a couple of LANs into a WAN, you need connectivity between the PCs and a way to handle communication. Computers connect to a network in one of two ways:

- Directly to a LAN via a cable from the computer to a LAN port
- Wirelessly to the LAN (this will be covered in Chapters 2 and 10)

A typical network client has a *network adapter* or *network interface card (NIC)* that connects to a cable that connects to a central network box, called a switch. Figure 1.5 shows a typical NIC.

Every NIC has a unique identifier called a *media access control (MAC) address.* I'll go into more detail on these addresses in Chapter 4. For now, just know that a MAC address acts like a name for a computer on a LAN.

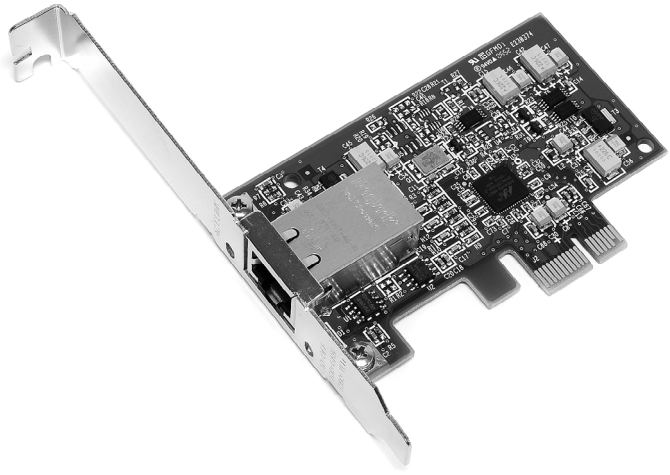


FIGURE 1.5 A network interface card

To make this into a nicely configured network, add another network client. Throw in a server. Don't add water, but turn on network sharing, and voilà! You have a network. Each machine attaches to a network cable that then connects at the other end to the switch. Any device attached to a network—client, server, printer, or whatnot—is called a *node.*

Ethernet

You might be wondering how you can tell what sort of cable to use for this network and how to determine the type of switch required for a network. Networking means communicating; the computers need to be able to speak the same language and follow the same technology.

The *Ethernet* standard defines everything about modern network hardware. Ethernet cables have standard connectors, for example, such as the *RJ-45 connectors* shown in Figure 1.6. Ethernet defines electrical signaling as well. That way, the sending NIC will break data down into little pieces and the receiving NIC will know exactly how to put them back together.

If two machines do not have the same kind of networking technology—a common problem in the early days of computer networks—then they can't network together. I won't bore you with a list of all the networking technologies that have had a brief moment of glory and market share in the past. Suffice it to say that today, Ethernet is king of the LAN.

FIGURE 1.6 RJ-45 connectors

Most modern Ethernet networks employ one of three technologies (and sometimes all three), *10BaseT, 100BaseT,* or *1000BaseT.* As the numbers in the names suggest, 10BaseT networks run at 10 Mbps, 100BaseT networks—called *Fast Ethernet*—run at 100 Mbps, and 1000BaseT networks—called *Gigabit Ethernet*—run at 1000 Mbps, or 1 Gbps.

Each Ethernet technology requires a specific kind of cabling that can handle its top speed. 100BaseT networks use Category 5 (CAT 5) or better Ethernet cables (Figure 1.7), while Gigabit Ethernet runs on Category 6 (CAT 6) or better Ethernet cables.

FIGURE 1.7 Category 5e (CAT 5e) cable

Hubs and Switches

Hubs and switches sit at the very center of networking, handling the tasks of receiving and sending packets of data to the connected computers. Each functions quite differently when it receives an Ethernet frame.

A *hub* repeats the frame down every network cable connected, hoping one of the computers connected is the recipient machine, such as Johan's laptop, for example (Figure 1.8).

A *switch,* in contrast, learns the network address of every machine connected to it, reads the recipient address on the frames, and sends them along only on the appropriate connection (Figure 1.9).

The radically more efficient switches now have completely replaced the earlier hubs in the marketplace.

Software

Of course it takes both hardware and software to make network communication work well. If Johan's computer requests an MP3 file from Michael's computer, Michael's operating system and other software take that MP3 file and break it into small, individually numbered units called *packets.* The NIC then takes the

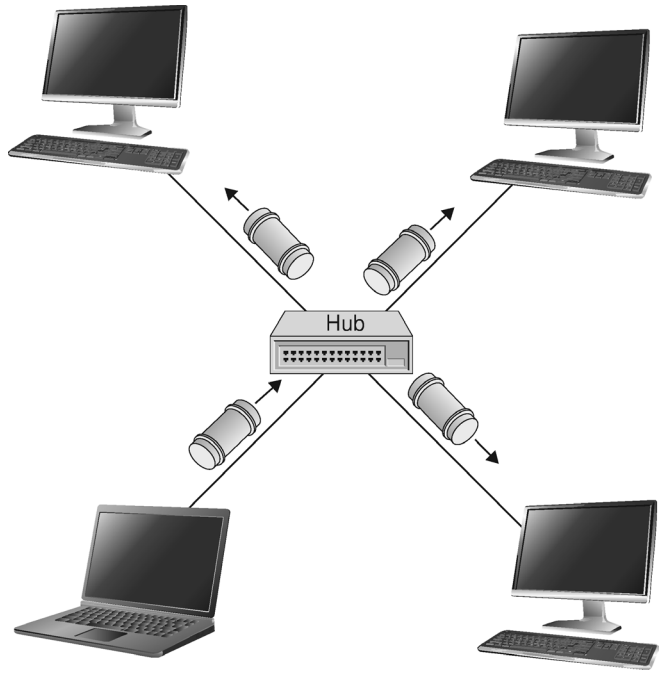


FIGURE 1.8 A hub repeating frames down every network cable

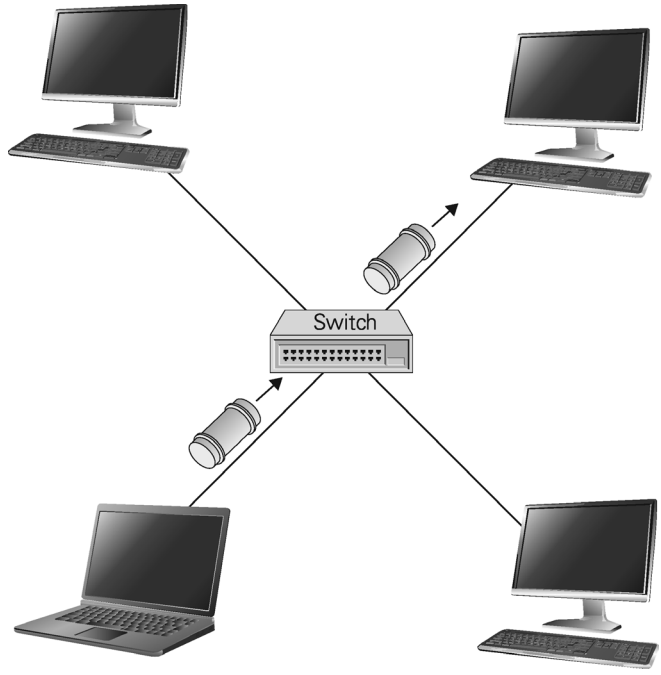


FIGURE 1.9 A switch sending frames only to the recipient

packets and, following the Ethernet standards, wraps up those packets into *network frames* that get sent out along the cable to the central network hub or switch (Figure 1.10).

All the machines on the network must use the same language—or *protocol*—for any sharing to happen. Over the years, various protocols have been developed, and you had to choose the protocol that worked best with a specific type of network or network needs. Today, that choice is easy because everybody uses

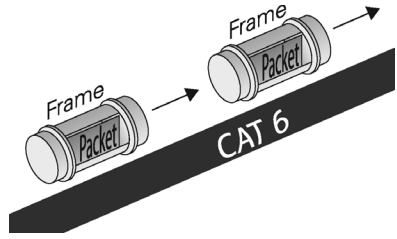


FIGURE 1.10 Packets wrapped in frames sent along an Ethernet CAT 6 cable

Transmission Control Protocol/Internet Protocol (TCP/IP), the language of the Internet. Chapter 5 covers TCP/IP in depth, so I won't go into the details here.

Applications

Finally, you need network-aware applications to accomplish things like accessing a shared file over a network. A commonly used network application is the web browser, such as Google Chrome, my personal favorite (Figure 1.11).

Connecting LANs

Enabling communication between two or more LANs requires several other pieces. First, you need a physical connection through cabling or radio waves. Second, you need special-purpose boxes to provide the intelligent direction so

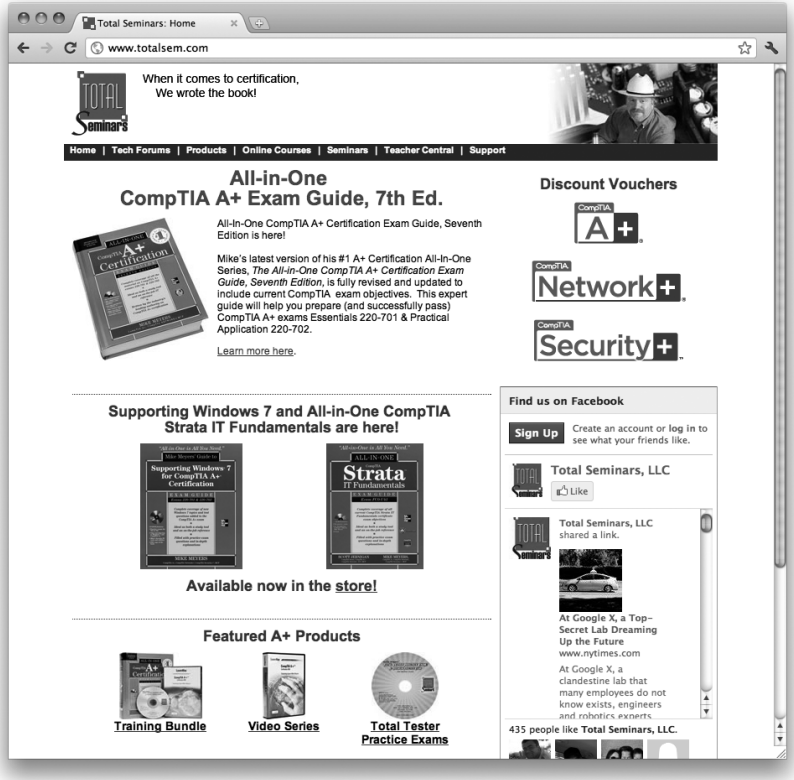


FIGURE 1.11 Chrome web browser

that data can properly flow either within a LAN (switches) or between the LANs (*routers*). Finally, devices need an address that goes beyond the LAN and applies WAN-wide. Today, that address is an *IP address,* because everyone uses TCP/IP to communicate. Chapter 5 covers IP addresses.

Travel Advisory

All nodes on a TCP/IP network have two addresses. The MAC address is the physical address of a computer on a LAN. The IP address enables communication across routers and thus between LANs as well as within a LAN.

Objective 1.02 The OSI Seven-Layer Model

The *International Organization for Standardization (ISO)* created a framework into which the major network hardware and software components and protocols could be placed to give every item a common reference point. This framework, called the *Open Systems Interconnect (OSI) seven-layer model,* provides a means of relating the components and their functions to each other and a way of standardizing some of the components and protocols.

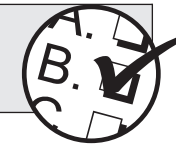
Travel Advisory

The letters used for the International Organization for Standardization—ISO—don't map to the initials in English, French, or Russian, the three official languages used by the body. Rumors abound that the word is derived from a Greek word that means equal, but those are just rumors.

The OSI model provides a critical common language that network hardware and software engineers can use to communicate and ensure that their equipment will function together. Each layer of the model represents a particular aspect of network function.

Exam Tip

The CompTIA Network+ exam expects you to know the layers by name (especially layers 1 through 4), how they function in relation to each other, and what they represent.



As well as helping to standardize the design elements of network components, the OSI model helps describe the relationships between network protocols. As you'll see, more than one protocol or action is needed to get your data onto a network.

The Layers and What They Represent

Let's run through the layers and an overview of their tasks and responsibilities. Figure 1.12 summarizes the layers and their functions.

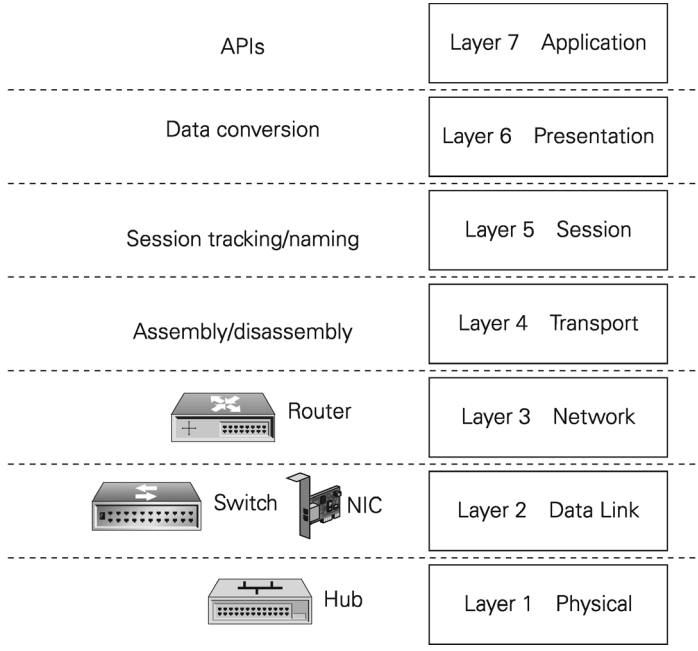


FIGURE 1.12 The seven-layer OSI model

Layer 1: Physical Layer

Layer 1 of the OSI model, the *Physical layer*, defines the network standards relating to the electrical signals that travel the network cables, the connectors, and the media types (cables) themselves. The Physical layer also determines the way that data is placed on the network media.

For the CompTIA Network+ exam, you need to know examples of components that run at each layer of the OSI. Examples of network components that are considered the Physical layer are cabling and hubs (Figure 1.13).

Layer 2: Data Link Layer

Layer 2, the *Data Link layer*, defines the rules for gathering and completing all the elements that make up a data frame and putting the whole thing together so that it can be passed to a Physical-layer device and on to the network. The exact components of the frame will vary depending on the data-link protocol being used, but would typically include the data being sent, an identifier for the sending machine, an identifier for the receiving machine, and an error-correction mechanism such as a frame check sequence (FCS).

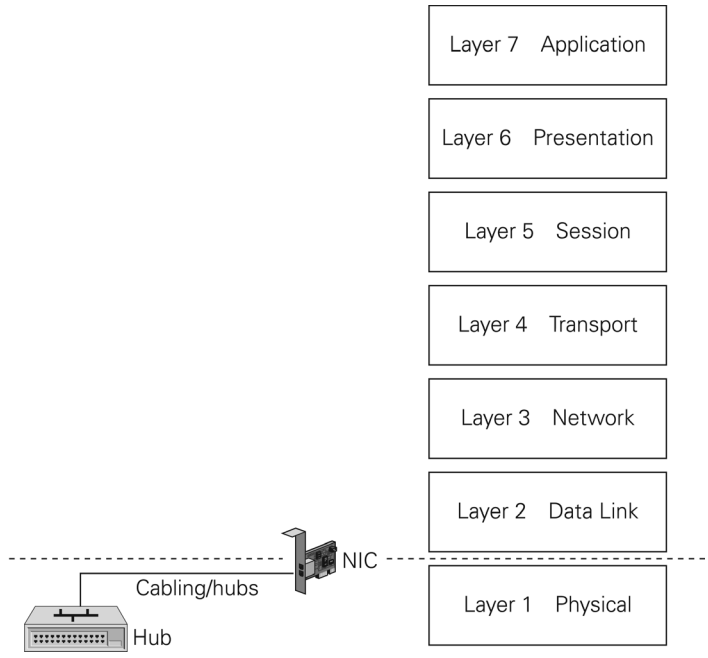


FIGURE 1.13 Layer 1 components

The Data Link layer on the sending machine assembles outgoing frames and calculates the FCS by applying a standard mathematical formula to the contents of the frame. The receiving machine performs the same calculation for incoming frames, enabling the receiving machine to verify the validity of the data by comparing its locally generated FCS value with that sent in the frame. If the values don't match, the frame is discarded and requested again.

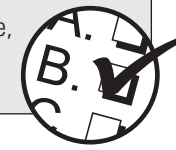
The Data Link layer also determines how data is placed on the wire by using an access method. The wired access method is *carrier sense multiple access/collision detection (CSMA/CD),* used by all wired Ethernet networks.

The Data Link layer is divided into two sublayers:

- **Logical Link Control (LLC)** The LLC is the component layer responsible for error-correction and flow-control functions.
- **Media Access Control (MAC)** The MAC is responsible for addressing network devices by using the physical address—that's the MAC address that is burned into the ROM chip of each network card. This physical address is placed in the layer-2 header for the sending and receiving system.

Exam Tip

For the CompTIA Network+ exam, know that layer 2 is divided into two sublayers and is responsible for physical addressing. Any device, such as a switch, that works with a physical address runs at this layer.

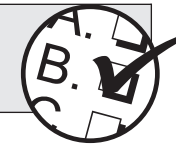


Layer 3: Network Layer

Layer 3, the *Network layer*, is responsible for routing functions and logical addressing. The Network layer addresses identify not only a system, but also the network on which the system resides. The router uses this information to determine how to send data to the destination network. The IP address in a TCP/IP network is a layer-3 address; routers use this address to determine to which network and node to send a packet.

Exam Tip

Examples of layer-3 components are the IP protocol and a router. An IP address is considered a layer-3 address; a MAC address is a layer-2 address.



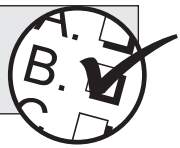
Layer 4: Transport Layer

If the data being sent is bigger than the packet size allowed by the lower-level protocols, layer 4, the *Transport layer,* breaks the data into smaller, manageable chunks that will fit inside two or more packets. Breaking up data into smaller chunks is known as *fragmentation.*

The Transport layer is also responsible for confirming whether transmitted packets have reached their destination intact and retransmitting them if they haven't. For incoming packets, the Transport layer reassembles the fragmented data, ensuring that received packets are processed in the right order.

Exam Tip

Examples of layer-4 protocols are Transmission Control Protocol (TCP) and User Data Protocol (UDP), which are part of the TCP/IP protocol suite.



Layer 5: Session Layer

Layer 5, the *Session layer*, is responsible for the session setup. The Session layer also manages and terminates the data connections (called *sessions*) between programs on networked devices. These sessions enable networked systems to exchange information.

Layer 6: Presentation Layer

Layer 6, the *Presentation layer*, is responsible for managing and translating the information into an understandable format that the Application layer can process further. In fact, many "Application-layer" protocols function at the Presentation layer too, taking datagrams and segments and turning them into formats programs can use.

Layer 7: Application Layer

Layer 7, the *Application layer*, represents the network-related program code and functions running on a computer system that either initiate the request (on the sending system) or service the request (on the receiving system).

Note that the Application layer does not refer to applications such as Microsoft Outlook. Instead, it refers to the protocols on which those programs rely. For example, Post Office Protocol 3 (POP3) and Simple Mail Transfer Protocol (SMTP) are important Application-layer protocols for e-mail, but many different end-user applications use those protocols (such as Outlook and Mozilla Thunderbird).

Using the Seven-Layer Model

The seven-layer model is only a theoretical representation of how networks function. Although knowing it inside-out won't change your life, it should help you pass the CompTIA Network+ exam. The conceptual use of the model assumes that an event on one computer system (for example, a user pressing ENTER on a login screen) creates some data that sets off a chain of events. The data runs down through the layers on the sending machine and then leaves the system, traveling across the network and then up through the layers on the receiving machine, until the data arrives intact at the Application layer and is processed by the receiving system. Later chapters in this book point out where certain key protocols and hardware fit into the model, and this can be useful stuff to know for both the CompTIA Network+ exam and real life.

Objective 1.03 The TCP/IP Model

The OSI model was developed as a reaction to a world of many different protocols made by different manufacturers that needed to play together. ISO created the OSI seven-layer model as the tool for manufacturers of networking equipment to find common ground between multiple protocols, enabling them to create standards for interoperability of networking software and hardware.

The adoption of TCP/IP as the sole protocol suite used in modern networks has rendered the OSI seven-layer model somewhat obsolete at the layers specific to TCP/IP. Many techs use a model specifically tailored to TCP/IP networks called, appropriately, the *TCP/IP model.*

Local Lingo

Internet model A lot of techs and tech sites call the TCP/IP model the *Internet model.*

The TCP/IP model consists of four layers:

- Link/Network Interface
- Internet
- Transport
- Application

It's important to appreciate that the TCP/IP model doesn't have a standards body to define the layers. Because of this, there are a surprising number of variations on the TCP/IP model. Some even have it as five layers rather than four!

A great example of this lack of standardization is the Link layer. Without a standardizing body, we can't even agree on the name. While "Link layer" is extremely common, the term "Network Interface layer" is equally popular. A good tech knows both of these terms and understands that they are interchangeable. Notice also that, unlike the OSI model, the TCP/IP model does not identify each layer with a number.

CompTIA has chosen one popular version of the TCP/IP model for the CompTIA Network+ competencies and exam. That's the version you'll learn right here. It's concise, having only four layers, and many important companies, like Cisco and Microsoft, use it, although with a few variations in names as just described. The TCP/IP model gives each protocol in the TCP/IP protocol suite a clear home in one of the four layers.

The clarity of the TCP/IP model shows the flaws in the OSI model. The OSI model couldn't perfectly describe all the TCP/IP protocols. The TCP/IP model fixes this ambiguity, at least for TCP/IP.

The Link Layer

The TCP/IP model lumps together the OSI model's layer 1 and layer 2 into a single layer called the *Link layer* (or *Network Interface layer*).

A nice way to separate layers in the TCP/IP model is to think about packets and frames. Any part of the network that deals with complete frames is in the Link layer. The moment the frame information is stripped away from an IP packet, we move out of the Link layer and into the Internet layer.

Travel Advisory

At the Link layer, just about every network tech reverts back to the OSI model for troubleshooting. It's important to distinguish between problems happening at the Physical layer, with cabling, for example, and problems that reflect the Data Link layer, with switches and MAC addresses. That's why accomplished techs know both models!

The Internet Layer

The *Internet layer* should really be called the "IP packet" layer. Any device or protocol that deals with pure IP packets—getting an IP packet to its

destination—sits in the Internet layer. IP addressing itself is also part of the Internet layer, as are routers and the magic they perform to get IP packets to the next router. IP packets are created at this layer.

The Transport Layer

The *Transport layer* combines features of the OSI Transport and Session layers with a dash of Application layer just for flavor. While the TCP/IP model is certainly involved with the assembly and disassembly of data, it also defines other functions, such as connection-oriented and connectionless communication.

Connection-oriented vs. Connectionless Communication

Some protocols, like the popular Post Office Protocol (POP) used for sending e-mail messages, require that the e-mail client and server verify that they have a good connection before a message is sent (Figure 1.14). This makes sense because you don't want your e-mail message to be a corrupted mess when it arrives.

Alternatively, a number of TCP/IP protocols simply send data without first waiting to verify that the receiving system is ready (Figure 1.15). When using Voice over IP (VoIP), for example, the call is made without verifying first whether another device is there.

FIGURE 1.14 Connection between e-mail client and server

FIGURE 1.15 Connectionless communication

The connection-oriented protocol is called *Transmission Control Protocol (TCP)*. The connectionless protocol is called *User Datagram Protocol (UDP)*.

Travel Assistance

Chapter 5 covers TCP, UDP, and all sorts of other protocols in detail.

Everything you can do on the Internet, from web browsing to Skype phone calls to playing World of Warcraft, is predetermined to be either connection-oriented or connectionless.

Segments Within Packets and Datagrams Within Packets

To see the Transport layer in action, strip away the IP addresses from an IP packet. What's left is a chunk of data in yet another container called a *TCP segment* or a *UDP datagram*.

FIGURE 1.16 TCP segment

TCP segments have many fields that ensure the data gets to its destination in good order. These fields have names such as Checksum, Flags, and Acknowledgement. Chapter 5 goes into more detail on TCP segments, but for now, just know that TCP segments have fields that ensure the connection-oriented communication works properly. Figure 1.16 shows a typical (although simplified) TCP segment.

Data comes from the Application-layer applications. The Transport layer breaks that data into chunks, adding port numbers and sequence numbers, creating the TCP segment. The Transport layer then hands the TCP segment to the Internet layer that, in turn, creates the IP packet, which encapsulates the segment.

UDP also gets data from the Application-layer programs and adds port and sequencing numbers to create a container called a *UDP datagram.* A UDP datagram lacks most of the extra fields found in TCP segments, simply because UDP doesn't care if the receiving computer gets its data. Figure 1.17 shows a UDP datagram.

Just like with TCP segments, when the Transport layer hands the UDP datagram to the Internet layer, it in turn creates the IP packet, which encapsulates the datagram.

The Application Layer

The TCP/IP *Application layer* combines features of the top three layers of the OSI model (Figure 1.18). Every application, especially connection-oriented applications, must know how to initiate, control, and disconnect from a remote system. No single method exists for doing this. Each TCP/IP application uses its own method.

FIGURE 1.17 UDP datagram

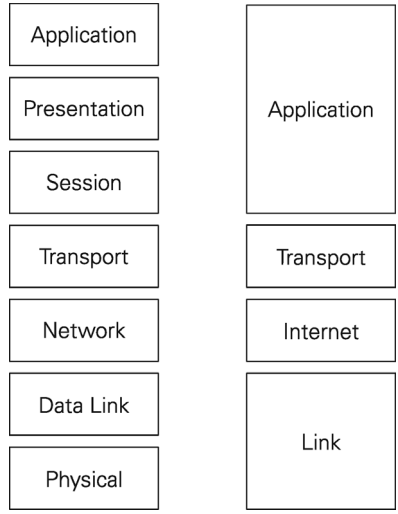


FIGURE 1.18 TCP/IP Application layer compared to OSI layers 5–7

TCP/IP uses a unique port-numbering system that gives each application a unique number between 1 and 65,535. Some of these port numbers are very well known. The protocol that makes webpages work, HTTP, uses port 80, for example.

Although we can say that the OSI model's Presentation layer fits inside the TCP/IP model's Application layer, no application requires any particular form of presentation as seen in the OSI model. Standard formats are part and parcel with TCP/IP protocols. For example, all e-mail messages use an extremely strict format called Multipurpose Internet Mail Extension (MIME). All e-mail servers and clients read MIME without exception.

In the OSI model, we describe the Application Programming Interface (API)—the smarts that make applications network aware—as being part of the Application layer. While this is still true for the TCP/IP model, all applications designed for TCP/IP are, by definition, network aware. There is no such thing as a "TCP/IP word processor" or a "TCP/IP image editor" that requires the added ability to know how to talk to a network—all TCP/IP applications can talk to the network, as long as they are part of a network. That's because they work directly with the APIs at the Application layer to send and receive data.

✔ **Objective 1.01: Overview of How Networks Work** The most obvious pieces of network hardware are the computers on the network. These are divided into client and server systems unless they are desktop systems that are sharing resources, in which case they are known as peer-to-peer systems. Corporate networks generally use dedicated servers because they offer higher performance, greater stability, and better security than peer-to-peer options. Your network won't be complete without some media—such as copper wiring, fiber optics, wireless, or infrared—to interconnect your systems, as well as a network interface card (NIC) to connect your system to the media. Other devices on the network—such as switches and routers—enable you to expand the system locally or to other sites.

✔ **Objective 1.02: The OSI Seven-Layer Model** The OSI seven-layer model describes how data flows from one networked system to another—it's a theoretical model into which many of the standards, components, and functions of a network fit. The model promotes the use of recognized network standards and helps ensure compatibility between network hardware and software from different manufacturers.

✔ **Objective 1.03: The TCP/IP Model** The TCP/IP model describes how data flows from one networked system to another, specifically for TCP/IP networks. Every TCP/IP protocol and application fits into one of the four layers in the model, making the TCP/IP model ideal for troubleshooting modern networks.

REVIEW QUESTIONS

1. What name is given to a network in which computers act as both clients and servers?
   - **A.** A multitasking network
   - **B.** A mainframe network
   - **C.** A peer-to-peer network
   - **D.** A LAN network

2. What standard defines the hardware technology of modern LANs?
   - **A.** ARPANET
   - **B.** Ethernet
   - **C.** OSI
   - **D.** TCP/IP
3. Which device is being used if frames are repeated down every attached Ethernet cable?
   - **A.** Modem
   - **B.** Switch
   - **C.** Frame
   - **D.** Hub
4. What device enables LANs to connect and direct packets to the correct LAN?
   - **A.** Hub
   - **B.** Frame
   - **C.** Router
   - **D.** Switch
5. A protocol operating at which layer of the OSI model is responsible for logical addressing and routing?
   - **A.** Transport
   - **B.** Network
   - **C.** Session
   - **D.** Application
6. A protocol operating at which layer of the OSI model handles the formatting of data so upper or lower layers can work with them further?
   - **A.** Application
   - **B.** Presentation
   - **C.** Session
   - **D.** Transport
7. Layer 3 is the _____ layer of the OSI model.
   - **A.** Session
   - **B.** Application
   - **C.** Data Link
   - **D.** Network

8. At which layer of the TCP/IP model are UDP datagrams created?
   - **A.** Link/Network Interface
   - **B.** Internet
   - **C.** Transport
   - **D.** Application
9. Which type of communication requires the client and server to acknowledge the transmission?
   - **A.** ACK request
   - **B.** Connectionless
   - **C.** Connection-oriented
   - **D.** Session
10. At which layer of the TCP/IP model do cables fit?
   - **A.** Link/Network Interface
   - **B.** Internet
   - **C.** Transport
   - **D.** Application

REVIEW ANSWERS

1. **C** A network with computers acting as both clients and servers is a peer-to-peer network.
2. **B** Ethernet is the standard.
3. **D** A hub repeats frames down every attached network cable.
4. **C** A router connects LANs and directs packets to the correct LAN.
5. **B** A protocol operating at the Network layer provides addressing and routing functions.
6. **B** A protocol operating at the Presentation layer handles the formatting of data (among other functions).
7. **D** Layer 3 of the OSI model is the Network layer.
8. **C** Data is divided into chunks at the Transport layer and then bundled into UDP datagrams or TCP segments, depending on which protocol is used.
9. **C** Connection-oriented communication requires the client and server to acknowledge the transmission.
10. **A** Cabling is in the Link/Network Interface layer of the TCP/IP model.