

Understanding the OSI Model

The Open Systems Interconnection (OSI) Model is one of the most referenced models in networking. It includes seven layers with specific activities, protocols, and devices working on each. Many network exams test your knowledge of the different elements of the OSI Model, and even some hiring managers quiz potential network employees on their knowledge. The TCP/IP Model is similar but includes only four layers instead of seven. This chapter introduces both models.

- ▶ **Understanding the OSI Model**
- ▶ **Understanding the TCP/IP Model**
- ▶ **Mapping devices on the OSI and TCP/IP models**
- ▶ **Mapping protocols on the OSI and TCP/IP models**

Understanding the OSI Model

The OSI Model is a framework for network communication. The ISO created it, and it includes seven layers.

The seven-layer *Open Systems Interconnection* (OSI) model is a general framework, or set of guidelines, for network communication. It defines how data is handled at several different layers. It also identifies the framework of TCP/IP protocols and hardware used on networks. There is no single standard or compliance test for the OSI Model itself. Instead, many standards have been created based on the different elements of the model.

Figure 3.1 shows the seven layers of the OSI Model. One of the primary goals of the OSI Model is operating system independence. In other words, the OSI Model allows computers running any operating system to communicate with other computers.

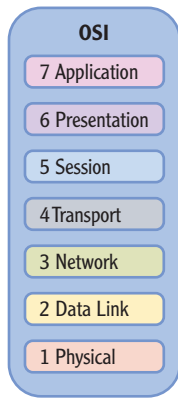


FIGURE 3.1 The OSI Model

The ISO may look like a typo. However, it's not an acronym for the International Organization for Standardization. Instead, ISO is derived from *isos*, which is Greek for equal.

The OSI Model was created by the International Organization for Standardization (ISO). The following are many advantages to the OSI Model:

Layers Interact Only with Adjoining Layers For example, the Transport layer interacts with the Session and Network layers only. It doesn't matter to the Session layer what applications are used on the Application layer. Similarly, it doesn't matter to the Session layer what type of cable media is used to transmit the data on the Physical layer.

It Has Encouraged Creation of Industry Standards Functions at each layer are standardized. Development of network components by different vendors is simplified, and different operating systems are able to communicate with other.

Network Communication Processes Are Segmented Instead of a single protocol that does everything, multiple protocols are used. Troubleshooting is easier once the OSI Model is understood.

You should know the names and number of each layer. Figure 3.2 shows two commonly used memory techniques.

Notice that one method (All People Seem To Need Data Processing) starts at layer 7 and goes to layer 1. The other method (Please Do Not Throw Sausage Pizza Away) starts on layer 1 and goes to layer 7. There are many other sayings used by technicians to memorize these layers. The technique you use isn't as important as using some method to memorize it.

Of course, just knowing the names and numbers of the layers isn't all you need to know. You should also have a basic understanding of what happens at each layer.

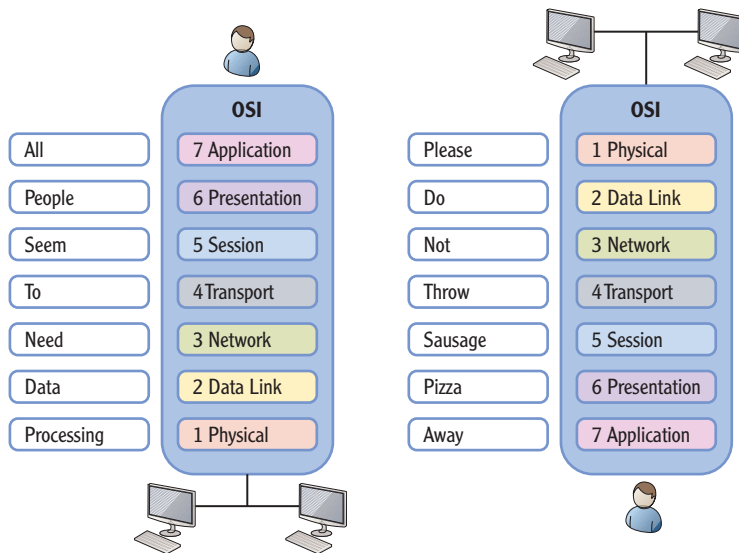


FIGURE 3.2 Mnemonics and the OSI Model

Application Layer

Layer 7 is the *Application layer*. It interacts with the Presentation layer and the end user. Several protocols operate on the Application layer:

Domain Name System (DNS) DNS is the primary name resolution service used on the Internet and in Microsoft networks. DNS resolves host names to IP addresses. In other words, you can pass the name of a server (such as DC1) to DNS, and DNS will return the IP address. DNS is also used to locate servers running specific services within a Microsoft network.

Hypertext Transfer Protocol (HTTP) HTTP is the primary protocol used to transmit data across the Internet for web pages. Similarly, HTTPS is a secure version of HTTP used to transmit data in an encrypted format.

File Transfer Protocol (FTP) FTP is the protocol used to transfer files to and from an FTP server. FTP servers are commonly hosted on the Internet. In contrast, file servers are used on internal networks to host files needed by users.

Trivial FTP (TFTP) TFTP is a lightweight FTP protocol used to transfer smaller files. TFTP is often used to transfer files to network devices such as routers.

Dynamic Host Configuration Protocol (DHCP) DHCP is a method of dynamically assigning TCP/IP configuration information to clients. A DHCP server assigns IP

◀ DNS is a required service in Microsoft domains and is heavily used on the Internet. Chapter 10 presents name resolution and DNS in greater depth.

◀ DHCP saves a lot of labor and is found in most networks. Chapter 5 covers DHCP in more depth.

addresses to systems. It also assigns the subnet mask, the address of the default gateway (a router), the address of a DNS server, the domain name, and much more.

Lightweight Directory Access Protocol (LDAP) LDAP is a protocol used to query a directory service, such as Microsoft's Active Directory Domain Services (AD DS). AD DS is hosted on domain controllers.

Post Office Protocol (POP3) POP3 is an email protocol used to retrieve email from POP3 email servers. POP3 servers are commonly hosted by Internet service providers (ISPs).

Simple Mail Transfer Protocol (SMTP) SMTP is an email protocol used to send email. Clients can send email from an email server. When a POP3 email server is used, users receive email with POP3 and send email with SMTP.

Internet Message Access Protocol (IMAP) IMAP is a protocol used to receive email messages. An IMAP server allows clients to store and manage their email on the server. Users can download the email onto their computer or organize the email in different folders on the server.

Simple Network Management Protocol (SNMP) SNMP is a protocol used to manage network devices such as routers and managed switches. It can detect and report problems before they become significant.

Server Message Block (SMB) SMB is a file transfer protocol used on Microsoft networks. It's primarily used for file and printer sharing.

The Application layer determines whether sufficient network resources are available for network access. For example, if you want to use Internet Explorer to access a web page on the Internet, the Application layer determines whether access to the Internet is available using HTTP.

It's worth pointing out that the Application layer doesn't refer to end user applications. For example, applications such as Internet Explorer are not part of this layer and aren't actually part of the OSI Model at all. However, when the user launches an application that needs network access, protocols on the Application layer ensure that the resources are available to support it.

Presentation Layer

The *Presentation layer* interacts with the Session and Application layers. In essence, it acts as a translator and determines how to format and present the data.

A common method of formatting data is with the American Standard Code for Information Interchange (ASCII) table. This table includes 128 codes to display

characters such as numbers, letters, and symbols. Table 3.1 shows a partial listing of the ASCII table.

TABLE 3.1 Partial ASCII table

Character	Decimal	Hexadecimal	Octal	HTML
A	65	41	101	A
B	66	42	102	B
C	67	43	103	C
a	97	61	141	a
b	98	62	142	b
c	99	63	143	c
1	49	31	061	1
2	50	32	062	2
3	51	33	063	3

Many other codes beyond ASCII are defined at the Presentation layer. For example, the Extended Binary Coded Decimal Interchange Code (EBCDIC) extended the ASCII table from 128 characters to 256 characters. File types such as MP3, JPG, and GIF also have their own codes defined on this layer.

The Presentation layer is also responsible for data compression and decompression and data encryption and decryption. For example, multimedia transferred over the Internet is often compressed to conserve bandwidth. If it wasn't, the World Wide Web might be known as the World Wide Wait.

Session Layer

The *Session layer* has the responsibility of establishing, maintaining, and terminating sessions. A session is simply a lasting connection between two networking devices. For example, if you use a chat program on your computer, it will establish a session with another computer to exchange the data.

Another way of saying this is that the Session layer manages the connections. It starts the session, manages the traffic during the session, and terminates the session when appropriate.

The Session layer also ensures that data from different applications are kept separate for each application at the Application layer. This becomes critical when multiple applications are running or when applications require more than one resource.

For example, you may be having a chat session in one window, downloading music in another, and reading email in a third. Three sessions are established and maintained for three different applications. The Session layer ensures that resources are available for each session and kept separate from each other.

The Session layer also tracks the mode of transmission used by the computers. Computers can transmit data using simplex, half-duplex, or full-duplex modes:

Networking professionals sometimes use the terms *simplex* and *half-duplex* interchangeably. However, they are different.

Simplex Data can be sent only one way. This isn't commonly used today in networking applications.

Half-Duplex Data can be sent both ways but only one way at a time. This is similar to a walkie-talkie where one user can press a button to talk but cannot receive any transmissions while the button is pressed.

Full-Duplex Data can be sent and received at the same time. Separate methods are used to send and receive.

The Session layer coordinates the communication and determines which mode to use. Two network protocols that operate on this layer are the Network Basic Input/Output System (NetBIOS) and Remote Procedure Call (RPC).

Transport Layer

The *Transport layer* is responsible for transporting data. It handles flow control, reliability, and error checking. The Transport layer divides data into smaller chunks, or *segments*, and then reassembles the received data.

For example, imagine you wanted to mail all volumes of Harry Potter to a friend in another state, but you could only use envelopes. You'd have to tear the pages from the books and mail them all separately. Your friend would then have to reassemble the books from all the envelopes.

This is similar to how data is managed on the Transport layer. Huge megabyte-sized files can't travel over the network. Instead, the Transport layer segments, or divides, these large files into smaller-sized segments. These smaller segments are transmitted over the network and then reassembled when they're received. The Transport layer also manages the ordering of the segments so that when the packets arrive, they can be returned to the same order.

Two primary protocols operate on the Transport layer:

Transmission Control Protocol (TCP) TCP provides guaranteed delivery of data. It starts by establishing a session and will not transmit data until a session is

Data traveling on the Transport layer is referred to as *segments*.

Chapter 4 covers TCP and UDP in more depth.

established. TCP is commonly referred to as *connection-oriented*. This means that it establishes a session before transmitting data.

User Datagram Protocol (UDP) UDP provides a best-effort method of delivering data. It does not provide guaranteed delivery of data like TCP. UDP is referred to as *connection-less*. Again, this doesn't refer to the physical connections but instead indicates that data is sent without first verifying a connection with the other system. UDP is commonly used for media streaming and diagnostic messages. Instead of using the additional overhead to establish the connection or session, UDP accepts that there may be some data loss and simply transmits the data.

Port numbers identify details about data on the Transport layer. There are 65,536 possible TCP *ports* and another 65,536 possible UDP ports. Some protocols use both TCP and UDP ports, while others use only one or the other. In this context, a port is simply a number from 0 to 65,535 that is utilized by a protocol for connection purposes. It does not represent a physical port.

For example, the HTTP protocol uses the well-known port of 80 by default. When you visit a website, you could use the HTTP address by itself as `http://www.bing.com/`. However, you could also include the port number as `http://www.bing.com:80`. Bing.com is the website, and once your request reaches the server hosting it, the TCP port of 80 identifies the data as HTTP traffic. The web server passes the data to the service handling the HTTP protocol.

In short, the IP address is used to get traffic from one computer to another. Once the traffic arrives, the port number is used to identify what application, service, or protocol should process the data.

Although port 0 is a valid port, it is reserved for both TCP and UDP.

LOGICAL AND PHYSICAL PORTS

The term *ports* means different things depending on the context. Ports can be either logical (numbers) or physical (connections on devices).

TCP and UDP ports are logical ports. They are simply numbers used to indicate how data is handled when it reaches its destination. Many ports represent specific protocols such as port 80 representing the well-known port of HTTP. Chapter 4 explores ports in greater depth.

Switches and routers have physical ports. Cables plug into these ports. A switch learns what computers are connected to each port, and a router learns what networks are connected to each port.

Network Layer

Data traveling on the Network layer is referred to as packets.

The *Network layer* is responsible for determining the best route to a destination. It uses routing protocols to build routing tables and uses Internet Protocol (IP) as the routed protocol. IP addresses are used at this layer to ensure the data can get to its destination.

Several protocols operate at this layer:

Internet Protocol v4 (IPv4) IPv4 is an addressing protocol using 32-bit addresses. The TCP/IP suite uses IP addressing to get traffic from one computer to another. IPv4 addresses are commonly expressed in dotted decimal format such as 192.168.1.1.

Internet Protocol v6 (IPv6) IPv6 is an addressing protocol using 128-bit addresses. IPv6 is intended to replace IPv4 and is currently being used concurrently with IPv4 on networks throughout the world. IPv6 addresses are commonly expressed in hexadecimal format such as 2001:0000:4137:9E76:3C2B:05AD:3F57:FE98.

Address Resolution Protocol (ARP) This protocol resolves IP addresses to the physical address or the Media Access Control (MAC) address. The IP address is used to route packets to the next hop's network interface card. Switches use MAC addresses to track computers connected to different physical ports. While ARP resolves the IP address to a MAC address, the Reverse Address Resolution Protocol (RARP) does the opposite. RARP can be used to resolve a MAC address to an IP address.

Internet Group Multicast Protocol (IGMP) IGMP is used for multicasting traffic. Multicast traffic goes from one computer to multiple computers. As a reminder, unicast is one-to-one traffic, and broadcast is one-to-all traffic on the same subnet.

Internet Control Message Protocol (ICMP) ICMP is used for error messages and diagnostic reporting. Several diagnostic tools such as Ping, PathPing, TraceRt, and others use ICMP.

Internet Protocol Security (IPSec) IPSec is a security protocol used to secure IP traffic. IPSec can encrypt traffic to protect it when it's transmitted. It also includes authentication mechanisms. IPSec authentication allows computers to ensure they communicate only with known entities.

Routing Information Protocol (RIP) This is a basic routing protocol used by routers in internal networks. Routers use RIP to communicate with each other and share information on the network. The current version is RIPv2, though OSPF has replaced it on most networks.

Open Shortest Path First (OSPF) OSPF is another routing protocol used by routers to communicate with each other on internal networks. OSPF is more advanced than RIP and is used in more networks.

Valid hexadecimal characters are 0 through 9 and A through F.

The MAC address is a 48-bit address assigned to network interface cards. The MAC address is explained more in the "Data Link Layer" section of this chapter.

Chapter 14 covers troubleshooting techniques using Ping, PathPing, and TraceRt.

The Network layer includes two key physical devices. The primary device working on this layer is a router. Routers are the devices that perform IP based routing functions. The router looks at the IP address and determines the best path to the destination network. Data packets are then sent to the destination using this path.

RIP and OSPF are common routing protocols used in internal networks. These two protocols determine the best route to a destination based on a metric (cost). The route with the best metric will have a lower cost and will be the selected route for IP.

This is similar to using a map for highways. You look at a map to determine the best route when traveling from point A to point B. The map provides the routing information, and you can identify the best path to get to your destination. Of course, maps are static and show only paths. They don't show construction, accidents, or other events that can slow traffic down. You may use other online tools to identify traffic congestion or areas of construction.

Routing protocols such as RIP and OSPF are dynamic protocols that can adjust to changing conditions on a network. Routers use these protocols to communicate with each other regularly. If network events occur that impact known routes or if new routes get added, the routing protocols are used to ensure that all the routers quickly learn about the impact.

Data Link Layer

The *Data Link layer* is concerned with data delivery on a local area network. This is where local area network (LAN) technologies such as Ethernet are defined. The Data Link layer is comprised of two sublayers.

Logical Link Control (LLC) IEEE 802.2 LLC interacts directly with the network layer. It is defined by the IEEE 802.2 standard. LLC provides flow control and error control and allows multiple protocols to work simultaneously.

Media Access Control (MAC) IEEE 802.3 MAC defines how packets are placed onto the physical media at the Physical layer. IEEE 802.3 defines Carrier Sense Multiple Access/Collision Detection (CSMA/CD), which is used to handle data collisions.

MAC addresses are also defined at the Data Link layer. The MAC address is also called a *physical address*, *hardware address*, *burned-in address*, or *Ethernet address*. It used to be a permanent address that was written into, or burned into, the read-only-memory (ROM) chip on the network interface card (NIC), but it is usually stored on the NIC's firmware today.

Layer 3 switches also operate on the Network layer (layer 3). Layer 3 switches combine the capabilities of layer 2 switches and routers. Chapter 8 covers switches in more depth.

Data traveling on the Data Link layer is referred to as frames.

Listing 3.1 shows the results of entering the command `ipconfig /all` at the command prompt of a server named DC1. This provides a lot of information including the physical address (or MAC address) of the NIC. Notice that it has an address of A4-BA-DB-FA-60-AD.

Listing 3.1 Output of `ipconfig /all`

```
C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DC1
Primary Dns Suffix . . . . . : Sybex.pub
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : Sybex.pub

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Realtek RTL8168C(P)/8111C(P)
    Family PCI-E
    Gigabit Ethernet NIC (NDIS 6.20)
    Physical Address. . . . . : A4-BA-DB-FA-60-AD
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.1.205(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DNS Servers . . . . . : 127.0.0.1
    NetBIOS over Tcpip. . . . . : Disabled
```

OTHER DEVICES HAVE MAC ADDRESSES

Although the code snippet shows the physical address of a NIC on a server, other devices also have MAC addresses. For example, each interface on a router has a separate MAC address. These MAC addresses at the Data Link layer are then mapped to an IP address assigned at the Network layer.

The MAC is represented with 12 hexadecimal characters (or 6 pairs of hexadecimal characters). Four bits represent each hexadecimal character. Four bits times 12 characters shows that the MAC address is 48 bits long.

Every device on a network has a different MAC address. If MAC addresses on the network aren't unique, the computers with the same MAC address can't communicate on the network.

Organizations that manufacture NICs are assigned an organizationally unique identifier (OUI) that they use in the MAC. They then use serial numbers added to this OUI to create the MAC. Table 3.2 shows how these numbers are combined to create the MAC address of A4-BA-DB-FA-60-AD.

TABLE 3.2 MAC address

Organizationally unique identifier	Manufacturer serial number
A4-BA-DB	FA-60-AD
Six hexadecimal characters (24 bits)	Six hexadecimal characters (24 bits)

These are some of the protocols that operate on the Data Link layer:

Point-to-Point Tunneling Protocol v4 (PPTP) PPTP is commonly used with virtual private networks (VPNs). VPNs provide remote users with access to a private network over a public connection such as the Internet.

Layer 2 Tunneling Protocol (L2TP) L2TP is another protocol used with VPNs. It often uses IPsec (as L2TP/IPsec) to encrypt the traffic.

Token ring IEEE 802.5 defines a token ring technology. A logical token is passed between the computers, and a computer can communicate on the network only when it has the token. Using the token for communication prevents collisions.

Asynchronous Transfer Mode (ATM) ATM is a cell-based method of transferring data. Data is converted into small fixed-sized cells and transferred over the network. ATM is used in WANs.

Frame relay Frame relay is another WAN technology. Data is converted to variable-sized frames and transferred over permanent virtual circuits.

Physical devices operating on the Data Link layer include bridges, switches, and NICs.

Chapter 13 covers
VPNs in more depth.

NICs also operate on
the Physical layer.

Physical Layer

▶
Data traveling on the Physical layer is converted to bits, or ones and zeros (such as 110011010101).

The *Physical layer* defines the physical specifications of the network. This includes physical media such as cables and connectors. It also includes basic devices such as repeaters and hubs. The Physical layer converts the data stream into zeros and ones (bits) and places them onto the physical media in the form of either electrical pulses for copper cable such as twisted-pair cable or light pulses for fiber-optic cable.

The Physical layer has some simple yet unique functions. It defines the physical characteristics of cables and connectors. It is also responsible for encoding signaling types, such as converting digital signals to analog signals.

Ethernet operates on the Physical layer. IEEE 802.3 defines the different technologies used for wired local area networks. Twisted-pair or fiber-optic cables are used for connectivity. It uses CSMA/CD for collision detection.

Putting It Together

Figure 3.3 shows how the OSI Model works when two different computers are interacting. The overall process is referred to as *encapsulation* where data from higher layers is encapsulated in lower layers.

Imagine a user launching Internet Explorer to access a web search engine such as Bing. The Application layer accepts the data, and the Session, Presentation, and Application layers work together to send the request to the Transport layer.

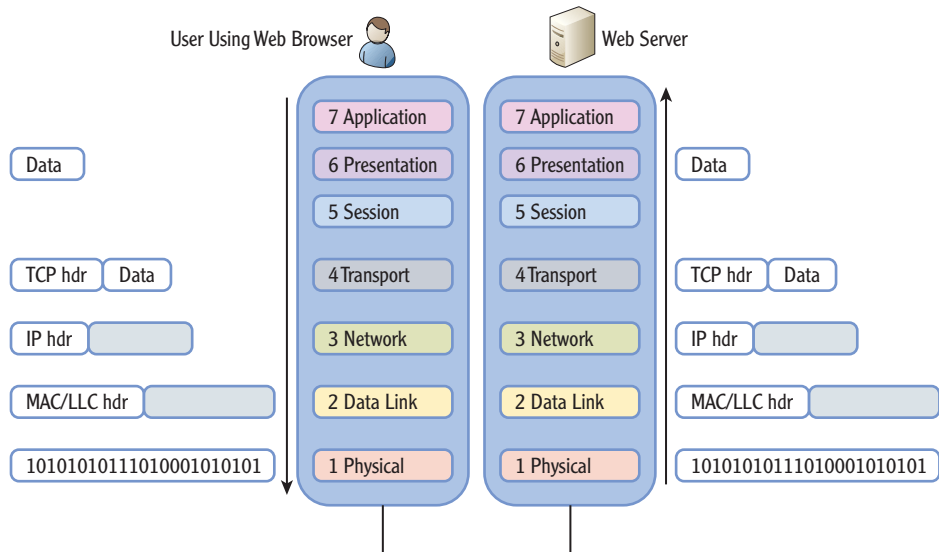


FIGURE 3.3 Data traveling up and down the OSI Model

The Transport layer then adds a TCP header. This header will include port information for the source and destination computers. Websites serve data using HTTP, and HTTP uses port 80, so the destination port is set as port 80. TCP assigns a port such as 49152 to Internet Explorer as the source port. The source port is to ensure that the return traffic is returned to Internet Explorer to display the page provided by the website.

At this point, you have two TCP ports assigned and added a part of the TCP header:

- ▶ Destination port: 80
- ▶ Source port: 49152

Next, the IP addresses are added at the Network layer. The IP address of the computer running the web server is added as the destination IP address, and the IP addresses of the user's computer is added as the source IP address. This information is added as the IP header and combined with the TCP header and the data. At this point, you have the following:

- ▶ Destination IP address and destination port: 80
- ▶ Source IP address and source port: 49152

Routers on the network use the destination IP address to route the packet to the destination computer. When it arrives, the destination port is used to send the data to the service, application, or protocol associated with the port.

When the packet reaches the network where the destination computer is located, the Data Link layer discovers the MAC address of the destination computer. The MAC address is then added to the packet so that the destination computer processes the data.


The Physical layer converts the data into 1s and 0s and places it on the wire. When the data reaches the destination computer, the process is reversed. Information at the different layers is stripped off, and it's passed to the next layer.

In the example, the data will be passed to the service handling HTTP at the Application layer. The user's request is processed, and a web page is built and sent back. The entire encapsulation process is repeated on the server and then sent back to the computer that originally requested the data.

Packets and Frames

Although the terms *packets* and *frames* are often used interchangeably, this isn't entirely accurate. The actual name depends on the layer of the OSI Model.

Figure 3.4 shows the names of the encapsulated data at the different layers of the OSI Model. Although there are multiple protocols throughout the OSI



Notice how the packet grows as it travels down the OSI Model. Lower layers add additional information to the previous layer.

Model, this chapter has primarily focused on the TCP and UDP protocols on the Transport layer (using port numbers) and the IP protocol (using IP addresses) on the Network layer.

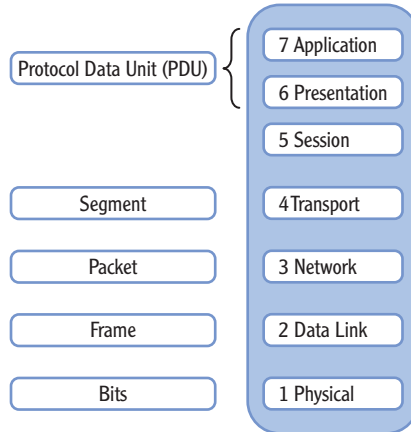


FIGURE 3.4 Encapsulated data names

Protocol Data Unit (PDU) Data units at layers 5, 6, and 7 are called *protocol data units*.

Segment At layer 4, the Transport layer, a TCP unit of data is called a *segment*. Remember that data is divided into smaller segments at this layer. This layer uses source and destination ports to identify the protocol, service, or application that will process the segment.

Packet At the Network layer, a unit of data is called a *packet*. This layer uses IP addresses to get the packets from the source to the destination.

Frame At the Data Link layer, a unit of data is called a *frame*. MAC addresses are defined here.

Bits At the Physical layer, the data is simply bits, or ones and zeros.

Some sources identify a datagram as a unit of data on the Transport layer (layer 4) using the User Datagram Protocol. Since *Datagram* is in the UDP name, this makes a lot of sense. It implies that the terms *segment* and *datagram* are interchangeable. However, official reference sources don't support this usage. At this point, you should be able to name each of the seven layers of the OSI Model and their layer number. You should also be able to identify the location of various protocols (such as TCP, UDP, and IP) on the OSI Model and the names of encapsulated data at different layers.

Segment has two meanings. On a physical network, it's a common connection between multiple computers. On the OSI Model, it's the data at layer 4.

WHAT ABOUT DATAGRAMS?

You may come across the term *datagram* in your studies. However, depending on what source you use, the term *datagram* can mean different things. Conventional sources indicate that a datagram is simply another name for a packet.

RFC 1594 (www.faqs.org/rfcs/rfc1594.html) identifies a datagram as “A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.”

That’s a mouthful. What RFC 1594 is saying is that a datagram is on the layer doing routing, which is layer 3, the Network layer. This implies that the terms *packet* and *datagram* are interchangeable.

Ideally, you should be able to draw a diagram similar to Figure 3.4 (without looking at the diagram). If you can do it now, great, but it does take a little practice. Use your favorite mnemonic (All People Seem To Need Data Processing, Please Do Not Throw Sausage Pizza Away, or another one you’ve learned) to help.

Understanding the TCP/IP Model

The *TCP/IP Model* is a four-layer model created in the 1970s by the U.S. Department of Defense (DoD). It’s also called the DoD Model. The TCP/IP Model works similarly to the OSI Model; it just has fewer layers.

Figure 3.5 shows the four layers of the TCP/IP Model in comparison with the OSI Model.

Notice that the layers on the TCP/IP Model correlate to layers of the OSI Model. The TCP/IP *Application layer* maps to layers 5, 6, and 7 of the OSI Model. The TCP/IP *Transport layer* maps to layer 4 of the OSI Model. The TCP/IP *Internet layer* maps to layer 3 of the OSI Model. The TCP/IP *Link layer* maps to layers 1 and 2 of the OSI Model.

Application Layer Protocols on this layer are used by applications to access network resources. Protocols include DNS, SMB, HTTP, FTP, SMTP, POP3, IMAP4, and SNMP.

Transport Layer Protocols on this layer control data transfer on the network by managing sessions between devices. The two primary protocols are TCP and UDP.



Note that the TCP/IP Model was created in the United States for the DoD before the OSI Model, and the OSI Model was created by the ISO as an international standard.

The Transport layer is also known as the host-to-host layer.



TCP/IP MODEL LAYERS

As you study different models, you may notice that there are different names given to the TCP/IP Model layers.

Microsoft documentation typically labels these layers as Application, Transport, Internet, and Link. For example, Microsoft online resources identified as preparation materials for the Microsoft Technology Associates (MTA) Networking Fundamentals exam (98-366) use these labels. If preparing for this exam, you should know these labels with these names.

Some networking textbooks label these layers as follows:

- ▶ Application
- ▶ Host-to-host
- ▶ Internet, Internetwork, or Internet Protocol
- ▶ Network Access or Network Interface

Many consider the IETF as the official source for these models and reference RFC 1122 (<http://tools.ietf.org/html/rfc1122>) and RFC 1123 (<http://tools.ietf.org/html/rfc1123>). These documents identify the layers as follows:

- ▶ Application
- ▶ Transport
- ▶ Internet Protocol
- ▶ Link

Internet Layer Protocols on the Internet layer control the movement and routing of packets between networks. Protocols on this layer include IPv4, IPv6, IGMP, ICMP, and ARP.

Link Layer This layer defines how data is transmitted onto the media. It includes multiple protocols such as Ethernet, token ring, frame relay, and ATM.

▶
The Link layer is also known as the Network Interface or Network Access layer.

Mapping Devices on the OSI and TCP Models

The OSI and TCP/IP models are reference points for the devices used on your network. These devices may include NICs, hubs, switches, routers, and firewalls. Figure 3.6 shows these models with their associated network devices.

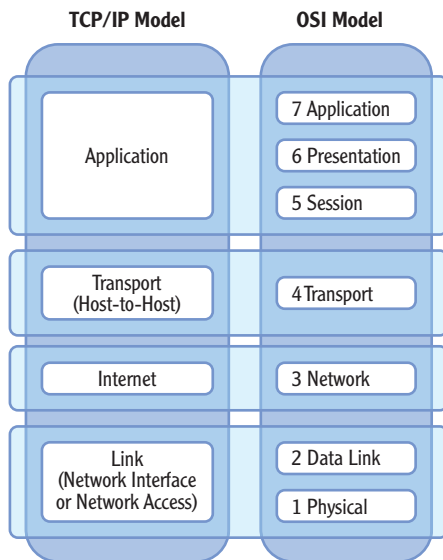


FIGURE 3.5 TCP Model

Devices on the lower levels (such as layer 1, the Data Link layer) have very little intelligence. As you move up the layers, though, the devices are more and more sophisticated. For example, an advanced firewall on the Application layer (layer 7) can analyze traffic within a session and make decisions to block or allow the traffic.

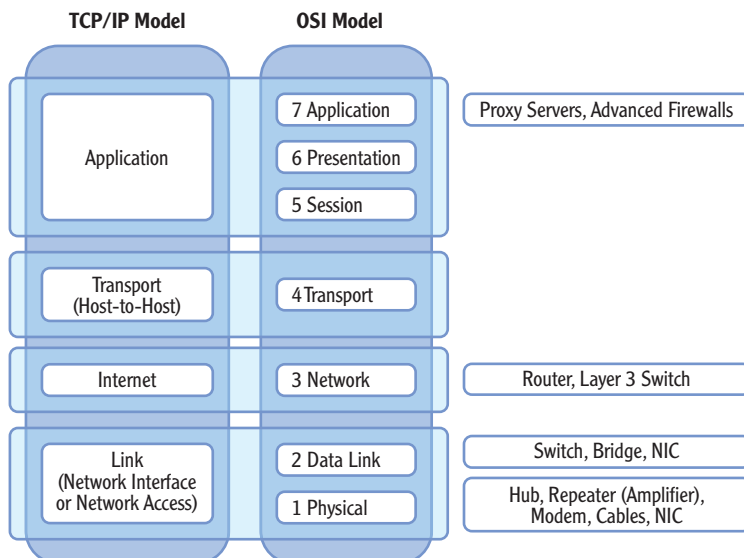


FIGURE 3.6 Mapping devices on the OSI and TCP/IP models

A hub (on layer 1) is unable to make any decisions and simply transfers all the data received on one port to all other ports of the hub. Switches (on layer 2) learn which port computers are connected to and internally switch the traffic. Routers (on layer 3) can talk to other routers and learn the best path to any subnet within a network.

▶
Some hiring managers include basic troubleshooting questions about the OSI Model and/or TCP/IP Model during interviews.

If you can map devices to specific layers of the OSI or TCP/IP models, you will be a better network troubleshooter. For example, consider a problem where a computer is not communicating on the network.

There are multiple reasons why communication is not working. If there are no green lights at the NIC card or switch, you may have a layer 1 problem. The physical connection has failed. This could be a faulty cable or faulty NIC. The NIC connects to a hub or a switch, so the problem could also be a faulty network device or faulty port on the network device.

If the NIC LED is not lit, it's important to realize the problem is a layer 1 problem. There is no need to troubleshoot the configuration of TCP/IP, the operating system, or the applications that are on different layers.

This is similar in concept to troubleshooting car problems. Imagine if you turn the ignition key but nothing happens. There's no sound, no clicking, nothing. You probably won't waste your time checking the oil or gas. The problem is more likely with the battery or ignition system.

Physical Layer

Devices at the Physical layer are concerned only with the physical aspects of communication—actual data transmission through physical connectivity. The Physical layer does not understand logical addressing with IP addresses or physical addressing with the MAC addresses.

At the Physical layer, you will find cables, cable connectors, NICs, hubs, modems, and amplifiers or repeaters.

The hub is a common device found at the Physical layer. It enables network expansion by allowing multiple devices to be plugged into a central point. As a layer 1 device, the hub is not aware of any addressing and ignores layer 2 MAC addresses and layer 3 IP addresses. It simply passes data received on one port to all other ports.

You may notice that NICs are listed on both the Physical layer and the Data Link layer. A NIC provides simple feedback with a lit LED indicating that the NIC is plugged in. This is a function performed at layer 1.

The NIC can also analyze traffic to determine whether received traffic is addressed to the computer based on the MAC address. If the traffic is addressed to the computer, the NIC processes the traffic and passes it to the internal

processor. This process occurs on layer 2, making a NIC both a layer 1 and layer 2 device.

The modem is also found at layer 1 of the OSI. The modem is a modulator–demodulator; it converts digital signals from your computer into analog signals used over the telephone line. Demodulation is the conversion from an analog-to-digital signal.

Repeaters and amplifiers are sometimes referred to as the same thing, but there is a subtle difference. The repeater will regenerate a digital signal, and the amplifier will regenerate an analog signal. Both boost signal strength as it travels along a cable, allowing a signal to travel further before reaching its destination. For example, if a cable is only able to carry a signal 100 meters, you can put a repeater between two 100 meter cables to extend the distance to 200 meters.

Data Link Layer

Devices on the Data Link layer include switches, bridges, and NICs. Switches and bridges create separate collision domains.

Switch The switch is a layer 2 device that learns MAC addresses of devices to segment traffic. These MAC addresses tell the switch which devices are connected to which port within a subnet. The switch then internally switches traffic to create separate collision domains.

Bridge The bridge learns the MAC addresses of devices that are connected to a port similar to how a switch learns these MAC addresses. However, a bridge will typically have multiple computers connected to each bridge port via a hub.

Network Interface Card The NIC is shared between the Data Link layer and Physical layer. The NIC contains the layer 2 MAC address that is used at layer 2. It analyzes traffic at this layer and determines whether the traffic should be processed by the computer. If the traffic is addressed to the computer, it passes the traffic to the central processor.

Network Layer

The router is the primary device on the Network layer. It routes packets based on their logical IP address.

Routers route IP traffic to different subnets within a network. They can communicate with other routers using routing protocols such as RIP and OSPF. Routers use these routing protocols to learn about multiple subnets within a network.

Layer 3 switches also operate on the Network layer. They are advanced switches that have the ability to route traffic on layer 3 similar to how a router routes traffic.



Although modems aren't common in urban areas, they are still popular with rural users who don't have broadband connections.



Chapter 8 provides much more depth on basic layer 2 and advanced layer 3 switches.



Chapter 9 covers routers in more depth, including how they communicate with other routers to learn new routes.

Chapter 11 covers proxy servers and firewalls in more depth.

Application Layer

Proxy servers and advanced firewalls work on the Application layer. They have the ability to examine traffic and make decisions based on the content. For example, a proxy server can block access to specific Internet websites based on the website address.

Any firewall can block traffic based on source or destination data contained within packets. Basic firewalls do this by blocking traffic based on IP addresses or ports in each individual packet. Advanced firewalls can analyze multiple packets within a session and make decisions to block or allow the traffic to continue.

Mapping Protocols on the OSI and TCP/IP Models

It's also important to understand where protocols operate on the OSI and TCP/IP models. Figure 3.7 shows a mapping of many of the protocols introduced in this chapter.

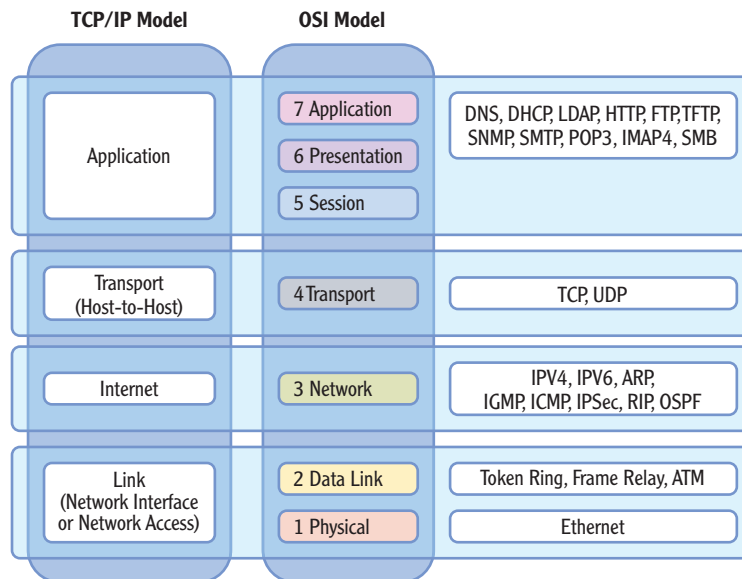


FIGURE 3.7 Mapping protocols on the OSI and TCP/IP models

You probably don't have a full grasp of the details of these protocols at this point. That's expected. These protocols have only been introduced and mapped to the different layers.

As you move through the chapters in the book, you'll learn much more about these protocols. Return to these diagrams to remind yourself where the protocols operate and where the devices operate.

Chapter 4 covers these protocols in more depth.

THE ESSENTIALS AND BEYOND

In this chapter, you learned the basics of the OSI Model. The model is a framework, or set of guidelines, used to develop and standardize networking protocols. This model has seven layers known as the Application, Presentation, Session, Transport, Network, Data Link, and Physical layers. The TCP/IP Model includes four layers: Applications, Transport, Internet, and Link. Protocols and devices are designed to work on specific layers of the OSI and TCP/IP models, and you learned the layers associated with specific protocols and devices.

ADDITIONAL EXERCISES

- ▶ Draw the OSI Model, and label the seven layers with their names and numbers.
- ▶ Identify the ASCII decimal codes for the phrase *Networking Essentials*.
- ▶ Draw the TCP/IP Model, and map its layers to the OSI Model.
- ▶ Map as many protocols as you can to the layers of the OSI and TCP/IP models.

To compare your answers to the author's, please visit www.sybex.com/go/networkingessentials.

REVIEW QUESTIONS

1. The OSI Model has _____ layers
2. Write down a mnemonic you use to remember the OSI Model.
3. True or false. TCP is a connectionless protocol.
4. What is a unit of data called at the Transport layer?

A. Packet	C. Frame
B. Segment	D. Protocol data unit (PDU)
5. Which of the following could be a valid MAC address for a server named Server 1?

A. Server1	C. A4-BA-DB-FA-60-AD
B. 192.168.1.5	D. G4-BA-10B-FA-60-AT

(Continues)

THE ESSENTIALS AND BEYOND *(Continued)*

6. IPv4 operates on the _____ layer of the OSI Model.
7. List the protocols that operate on the Transport layer of the OSI Model.
8. True or false. Devices that operate on layer 7 of the OSI Model are more intelligent than devices that operate on layer 1.
9. Routers operate on which of the following layers of the OSI Model?
 - A. Layer 1
 - B. Layer 2
 - C. Layer 3
 - D. Layer 4
 - E. None of the above
10. Proxy servers operate on which of the following layers of the OSI Model?
 - A. Layer 1
 - B. Layer 2
 - C. Layer 3
 - D. Layer 4
 - E. None of the above