The Internet and TCP/IP

CIW EXAM OBJECTIVE AREAS COVERED IN THIS CHAPTER:

✓ Define the Internet infrastructure, including but not limited to: the National Science Foundation network (NSFnet), the Internet Society (ISOC), key internetworking protocols.

✓ Identify essential elements of the Internet and locate Requests for Comments (RFCs) that define them, including but not limited to: the Open Systems Interconnection (OSI) reference model, the Internet architecture model, Transmission Control Protocol/Internet Protocol (TCP/IP), various Internet protocols.

✓ Define the functions of application-layer Internet protocols, including but not limited to: Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP).
The success of many businesses, academic institutions, hospitals, and even governments can be chalked up to networks. Networks provide an efficient system of connections so that users can file-share, communicate, create, research, and learn together, even though the associated users are miles or even continents apart.

Networks are extremely popular for a very basic reason: they allow users to share data quickly. In the past, users had to place files on a floppy disk or print them and physically deliver them to the destination. Such “sneakernet” solutions may be appropriate or necessary in some situations, but when it comes to organizing and expediting the daily operation of a business, no better means exists than a well-run network.

Networks allow information to be distributed quickly and easily between two or more computers. This is achieved with a system of protocols, cables, hardware, and (in some instances) other media, such as wireless technology.

A network is two or more computers that share information via a physical medium and a protocol. Networking can include a small business network in one building, for instance, which is called a local area network (LAN), and a network can also connect many different LANs over a long distance in a wide area network (WAN). A series of WANs can extend to a worldwide “internetwork” that connects millions of users, such as the Internet. Before you learn more about the Internet, internetworking, and the protocols involved with networking, you must understand how networks have traditionally functioned.
Networking Past and Present

Traditionally, whenever an organization chose a network, it tried to ensure that it chose and used only one type of network product. Such choices began the era of homogeneous, vendor-centric networks. Most organizations chose one vendor, such as Novell, IBM, or Microsoft, to provide their networking solution because a one-vendor network ensures a minimum of training for employees and IT professionals. The reasoning was that using the same network type made network communication as simple as possible.

As you pursue your career, it is quite possible that you will work with many different types of networks, such as Unix, Novell NetWare, Windows NT, and Windows 2000. At one time, you would probably have used only one type of network at each company. Thus, you would have had to familiarize yourself with the new network and networking protocol or topology with each new job. After learning the latest protocols in order to pass the CIW Internetworking Professional exam, however, you will have learned all you need to know to apply yourself to any available network.

Over the past decade, a fundamental change has occurred in networking. Before, you would have had to learn each networking system separately in order to run any one of them; now, many different types of networks can be connected to ensure that different organizations and divisions can communicate directly with one another in a timely way. The task of working with different, or heterogeneous, systems such as the Internet has been given its own name: internetworking. This type of networking represents quite a change. With a traditional networking solution, an organization could communicate with itself on its own network. However, to communicate with others, it had to resort to non-network delivery methods, such as traditional mail. The motivation behind the developments that allow networks to connect with one another has been the need for different organizations to transfer information across large geographic areas as rapidly as possible.

Given this change in how organizations operate with various networks, you will probably have to connect different types of networks into a single logical network in which each type can communicate with the others.
Overview of TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of rules that allows computers from different vendors with various operating systems and capabilities (mainframes to desktop computers) to communicate. Since it was adopted in 1983 by the major networks that made up the Internet, TCP/IP has far exceeded expectations. Today, it is the most widely used networking protocol suite in the world and is the protocol that powers the Internet, the world's largest WAN.

In this section, we’ll discuss Internet architecture and common protocols used on the Internet, including more about TCP/IP and serial link protocols. We will also discuss and analyze Request for Comments (RFC) documents, which define and reference Internet protocols.

TCP/IP and Interoperability

Even though TCP/IP is the most popular network protocol, many networks today use protocols other than TCP/IP. The default networking protocol for Novell NetWare networks was IPX/SPX until Novell NetWare 5 was released and the default became TCP/IP. Many Novell networks still use both IPX/SPX and TCP/IP and are very productive as a result, but non-TCP/IP networks need not completely abandon the networking protocol they have traditionally used in order to function with other networks. In fact, they can use one protocol internally and use TCP/IP as the protocol that will transport information between their network and another.

If one network used a networking protocol such as NetBEUI and another used IPX/SPX, they could not communicate with each other. Networks in this situation could employ special devices, called gateways, to translate between different networking protocols, but a much more effective solution would be to adopt TCP/IP to help the two networks communicate.

As you can see in Figure 1.1, TCP/IP can allow different types of networks to communicate with one another. Using something as simple as a router, TCP/IP allows your existing LAN or WAN to operate with another.

It may also function in parallel with other protocols operating through the same NIC. Because of this, it serves as an ideal bridge that allows existing LANs and WANs to act as backbones for an enterprise.
Internetworking and the Corporate Network

TCP/IP has emerged as the dominant internetworking protocol because it allows different systems to work together. Such cross-platform capability means that legacy systems, such as IBM SNA, can communicate with newer client/server solutions, such as Unix, Windows NT, Windows 2000, Macintosh, and Novell networks. Older mainframe networks and the latest PC-based networks can communicate with one another, as well. Because it is vendor-neutral, TCP/IP allows internetworking professionals to connect each system without sacrificing the strengths inherent in any operating system or networking method.

TCP/IP for internetworking has been attractive because it allows corporations and networks to use past investments as wisely as possible. Therefore, even though the Internet and internetworking are revolutionary, this protocol presents an attractive alternative to businesses that do not want to discard an entire system. With careful planning and problem solving, organizations can make sure that their older systems can communicate with any other system on their internetwork.
Evolution of the Internet

The Internet was formed in 1968, when the U.S. Department of Defense Advanced Research Projects Agency (ARPA) funded what would become the first global computer network, the Advanced Research Projects Agency Network (ARPANET). The ARPANET was launched in 1969 and connected four universities: two University of California campuses, the Stanford Research Institute, and the University of Utah. The network allowed university and government engineers to research and work from any location on the network. ARPANET’s design featured multiple hosts and multiple connections among those hosts (see Figure 1.2), which greatly reduced the chances of total network failure. There was no central hub, which would have created a point of vulnerability; rather, control was spread throughout the network. This decentralization resulted in a robust and reliable network that would continue to function even if many of the hosts were incapacitated.

FIGURE 1.2 Multiple connections among hosts

In the early 1980s, the Unix operating system from University of California, Berkeley, supported TCP/IP, and in 1981 TCP/IP became an official Internet standard. On January 1, 1983, TCP/IP was adopted as the Internet’s official protocol. In the late 1980s, the Department of Defense decommissioned the ARPANET, and all sites transferred to the National Science Foundation (NSF) network, called the NSFnet. The NSF is an independent agency of the U.S. government that promotes the advancement of science and engineering. The NSF increased the number of NSFnet supercomputers to five in 1986 and added access to more networks, expanding the range of sites for businesses, universities, and government and military installations. These centers were
connected with 56Kbps telephone lines that created regional networks, with each supercomputing “center” as a hub for connections in a given region. In 1987, the NSFnet became known as the Internet.

Traffic on the network increased significantly. In 1989, the NSFnet was upgraded to support a 1.5Mbps connection speed by contracting Merit Network, Inc. In the years that followed, more private companies joined the Internet, and new technologies exist to reach speeds over 1Gbps. The hardware and communications links required to connect to the Internet were funded by a combination of private and government money. In 1995, the NSF decommissioned the NSFnet and gradually turned the Internet over to a consortium of private telecommunication companies, including Sprint, UUNet, PSINet, and MCI.

If you want to expand on the history of the Internet, a good resource is a book by Katie Hafner and Matthew Lyon, “Where Wizards Stay Up Late: The Origins of the Internet” (Simon & Schuster, 1996; also available in several e-book formats). The book focuses on the people, universities, and technologies that helped create the Internet.

**Internet-Related Authorities**

The authority for the Internet rests with the *Internet Society (ISOC)*. ISOC is a voluntary membership organization whose objective is to promote global information exchange using Internet technology. You can visit the Internet Society at [www.isoc.org](http://www.isoc.org).

ISOC elects volunteers who are responsible for the technical management and direction of the Internet; these volunteers are called the *Internet Architecture Board (IAB)*.

Another volunteer organization, called the *Internet Engineering Task Force (IETF)*, meets regularly to discuss operational and near-term Internet technical problems. Recommendations made via working groups within the IETF can be sent to the IAB to be declared Internet standards. The IETF chairman and the area managers form the *Internet Engineering Steering Group (IESG)*.

Another organization, called the *Internet Research Task Force (IRTF)*, is responsible for network research and the development of new technology. The *Internet Research Steering Group (IRSG)* sets priorities and coordinates research activities. Figure 1.3 displays the ISOC structure.
Requests for Comments (RFCs)

Requests for Comments (RFCs) are published documents of interest to the Internet community. They include detailed information about standardized Internet protocols, such as IP and TCP, and those in various stages of development. They also include informational documents regarding protocol standards, assigned numbers (e.g., port numbers), host requirements (e.g., Data-Link, Network, Transport, and Application OSI layers), and router requirements.

RFCs are identified by number. The higher the number, the more recent the RFC. Be sure you are viewing the most recent RFC during your research. A recommended RFC reference site is located at www.rfc-editor.org/rfc.html.

If an RFC has been updated, the index listing (i.e., the RFC editor query results) will state the replacement RFC number. Be aware that not all sites update RFCs regularly, so verify that your mirror site is current, or go directly to rfc-editor.org.

Protocol States

Before a protocol becomes a standard, it passes through several maturity-level states: experimental, proposed, draft, and standard. If a protocol becomes obsolete, it is classified as historic. To progress through the steps,
the protocol must be recommended by the Internet Engineering Steering Group (IESG) of the Internet Engineering Task Force (IETF).

**Maturity-Level Protocol States**

Maturity level of protocol states simply indicates the level of review and testing that has been performed with a protocol state. Like many other characteristics of the Internet, there are no hard and fast rules regarding how long or how many people review a protocol before it moves from one state to another.

- **Experimental** Protocols that should be used only in a lab situation. They are not intended for operation on systems other than those participating in the experiment.

- **Proposed** Protocols that may be considered for future standardization. Testing and research are encouraged—optimally, by several groups. These protocols will most likely be revised before progressing to the next stage.

- **Draft** Protocols being seriously considered by the IESG to become Internet standards. Testing is encouraged, test results are analyzed, and feedback is requested. All input should be sent to the IESG. Changes are often made at the draft stage; the protocol must then return to the proposal stage.

- **Standard** Protocols determined by the IESG to be official standard protocols on the Internet. Standard protocols are of two types: those that apply to the entire Internet and those that apply only to certain networks.

**Additional Protocol States**

The Additional Protocol States are ones that exist distinct from maturity level, but are not directly tied to developmental state.

- **Historic** Protocols that have been replaced by more recent ones or that never received enough interest to develop. Historic protocols are very unlikely to become Internet standards.

- **Informational** Protocols developed outside of the IETF/IESG (e.g., protocols developed by vendors or other standardization organizations). These protocols are posted for the benefit of the Internet community.

**Internet Standards**

A protocol, or set of related protocols, that has been standardized is indexed as an STD (Standard), such as STD 5. All protocols, even STDs, are indexed as RFCs because RFCs are never deleted, but only change protocol states. For
instance, TCP is STD 7, as well as RFC 793. In some cases, several RFCs may become one STD. For instance, IP, ICMP, and IGMP are indexed as STD 5, even though three RFCs exist: RFCs 791, 792, and 1112, respectively. You will learn about these protocols in the next section.

**Reference RFCs**

You should be familiar with the following important reference RFCs.

- **Internet Official Protocol Standards, RFC 2800, STD 1** Lists the current Internet protocol standards, as well as the current protocol state of all RFCs.

- **Assigned Numbers, RFC 1700** Lists the current status of parameters, such as numbers and keywords, used on the Internet. It includes the assigned Internet protocol numbers for Internet protocols. For instance, IP is represented by the decimal number four. It also includes well-known and registered port assignments. You will learn about assigned numbers throughout the book.

- **Requirements for Internet Hosts, RFC 1122 and 1123** A pair of RFCs that define Internet host software requirements. They define the unique requirements of protocols within the Internet architecture and list the features and implementation details of the protocols, (e.g., protocol specifications identified as must, must not, should, should not, and may).

- **Requirements for IP Version 4 Routers, RFC 1812** Defines the unique requirements of IPv4 Internet routers. It updates the historic RFC 1716, Router Requirements, to include current router technology.

**OSI Reference Model**

The Open Systems Interconnection reference model (OSI/RM) was defined by the International Organization for Standardization (ISO). Introduced in 1983, the OSI/RM has three practical functions:

- It gives developers necessary, universal concepts so they can develop and perfect protocols.

- It explains the framework used to connect heterogeneous systems. In other words, it allows clients and servers to communicate even if they are using different applications and operating systems. All they need is a common protocol, such as TCP/IP or IPX/SPX.
- It describes the process of packet creation. You will learn more about packet creation shortly.

Network function can be described using the OSI model, and network protocols can be created to function as described by the model, just as a building is constructed from a blueprint. For instance, Novell NetWare, Microsoft Windows NT, Windows 2000, and Unix are network operating systems supporting various protocol suites that can be described using the OSI/RM. This common framework allows these network operating systems (NOSs) to interoperate, and may help an internetworking professional to architect a network or troubleshoot a problem. Also, when protocols, such as IP and IPX, are discussed, they are usually linked to their OSI layer. For example, both IP and IPX are found at the OSI/RM Network layer. The OSI/RM provides the concepts and nomenclature you need to be able to discuss packet creation and networking protocols.

Table 1.1 lists the seven layers of the OSI/RM and describes each layer’s function.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Layer Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>7</td>
<td>The interface to the end user in an OSI environment; supports file transfer, network management, and other services.</td>
</tr>
<tr>
<td>Presentation</td>
<td>6</td>
<td>Responsible for providing useful transformations on data to support a standardized application interface and general communication services. For example, it converts text from American Standard Code for Information Interchange (ASCII) to Extended Binary Coded Decimal Interchange Code (EBCDIC).</td>
</tr>
<tr>
<td>Session</td>
<td>5</td>
<td>Establishes, manages, and terminates connections (sessions) between cooperating applications. This layer adds traffic flow information, as well.</td>
</tr>
</tbody>
</table>
How the Layers Communicate

As shown in Figure 1.4, the OSI model describes interaction between the individual layers, as well as between hosts on a network.
A client/server example will be used to explain how the OSI/RM typically works. In the figure, the left column contains the seven OSI/RM layers that exist on the client. The right column contains the same seven layers that exist on the server.

If the client sends a request to the server, the request might begin with a mouse click by the user on a web page hyperlink (Application layer). The request travels down the OSI/RM until it reaches the Data-Link layer, where it is placed onto a wire, cable, or whatever network medium is used (the Physical layer).

The client’s request travels across the wire until it reaches the server. The server’s Data-Link layer pulls the request off the wire (Physical layer) and sends it up the server’s OSI/RM. When the request arrives at the server’s Application layer, the request is processed. The server then returns a response—for instance, a new web page—to the client, using the same method.

In networking, information such as the client’s request and the server’s response is sent across the network in packets. Packets are discussed in the next section.
Packets

A packet is a fixed piece of information sent across a network. Whenever you send information across any network, you begin the packet creation process. A packet consists of three elements: a header, the actual data, and a trailer.

Many networking professionals use the terms “packet,” “datagram,” and “frame” interchangeably. Although this usage is accurate most of the time, “packet” is a generic term for any piece of information passed through a network. A datagram is a packet at the Network layer of the OSI/RM. A frame is a packet at the Data-Link layer (used to traverse an Ethernet network). Although they have distinct, strict meanings, these terms are used synonymously, even by networking professionals. It may be important to infer correct meaning from context, or to verify usage by another professional by referring to the appropriate OSI layer.

As shown in Figure 1.5, the header contains several different pieces of information, such as addressing information or an alert signal to the incoming computer.

**Figure 1.5** Packet structure

The preceding figure also shows that the packet contains the original data, such as a portion of an e-mail message. The trailer usually contains information
that validates the packet. For example, it could contain cyclic redundancy check (CRC) information.

**Cyclic Redundancy Check**

A CRC is a mathematical calculation that allows the receiving computer to verify that the packet is valid. When a sending host transmits a packet, it calculates a CRC, then adds this information to the trailer. When the receiving host reads the packet, it runs its own CRC, then compares it with the CRC stored in the trailer. If the two match, the packet is not damaged, and the receiving host processes the packet. If the CRCs do not match, the receiving host discards the entire packet.

**Packet Creation: Adding Headers**

The packet creation process begins with Layer 7 of the OSI/RM (the Application layer), and continues through Layer 1 (the Physical layer). For example, when you send an e-mail message or transfer a file from one computer to another, this message or file undergoes a transformation from a discrete (i.e., complete) file into smaller pieces of information called packets. Beginning with the Application layer of the OSI/RM, the file continues to be divided until the initial, discrete message becomes a number of smaller, more manageable pieces of information sent at the Physical layer.

As shown in Figure 1.6, each layer adds its own information, called a header, to the packet. This information enables each layer to communicate with the others, and also allows the receiving computer to process the message.

**FIGURE 1.6** Headers added at each level of OSI/RM
Packet Creation: Removing Headers

You have already seen how a sending host creates a packet. When a receiving host processes a packet, it reverses the packet creation process and removes each header, beginning with Layer 1 (the Physical layer) and ending with Layer 7. All that is left at the end of this process is the original, unaltered data, which the host can then use. This procedure of network communication by packet creation, transmission, and processing is similar regardless of network topology or protocol. Many networking protocol suites exist that follow this process of network packet creation, and models for both general and specific network technologies exist. However, the OSI reference model is just that, a reference model that may be applied to any other specific model or protocol.

TCP/IP

On January 1, 1983, the major networks that made up the Internet adopted the Transmission Control Protocol/Internet Protocol (TCP/IP) suite as the Internet’s official protocol. One reason for the Internet’s explosive growth and powerful communication ability is its adoption of this suite, which was originally developed in Berkeley, California.

TCP/IP is the default protocol for the following network operating systems:

- Windows NT 4.0, 2000
- Unix
- NetWare 5 and newer

Currently, the Internet fully supports TCP/IP version 4. However, TCP/IP version 6 (known as IPv6) is being tested and is expected to gain full support in the coming decade.

You will learn more about TCP/IP in future chapters, but some of its basic principles are discussed in the following section.

A Collection of Protocols

TCP/IP is a suite of protocols that includes Transmission Control Protocol (TCP), Internet Protocol (IP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and many
others that will be discussed later in this book. Each of these protocols has a specific function.

TCP  TCP ensures reliable communication and uses ports to deliver packets. It also fragments and reassembles messages, using a sequencing function to ensure that packets are reassembled in the correct order.

IP   IP is a connectionless protocol responsible for providing addresses of each computer and for performing routing. IP version 4 uses 32-bit addresses. The address scheme falls into five classes, only three of which are available for standard network addressing. The original plan was to assign Class A addresses to large networks, Class B to medium-sized networks, and Class C to smaller networks. Class D addresses are used for multicasting, and Class E addresses are experimental. You will learn more about these classes later in this book.

Thirty-two-bit IP addresses are divided into halves: the network portion and the host portion. The subnet mask helps determine which bits form the network and host portions.

An Open Standard

TCP/IP is not tied to any one vendor, and therefore allows heterogeneous networks to communicate efficiently. It uses the Internet architecture model that divides its protocols into four layers. Each layer is responsible for specific communication tasks and coincides with layers in the OSI/RM. Note that several Internet architecture models exist, each slightly different from the others. A four-layer version was selected for this book.

Throughout this book we will often refer to the OSI reference model. Both the OSI/RM and the Internet model are often referenced by internetworking professionals. The CIW Internetworking Professional exam references the Internet model.

Internet Architecture and Protocols

Similar to other networking models, the Internet architecture model divides protocols into layers. Each layer is responsible for specific communication tasks. The Internet architecture model consists of four layers, each
coinciding with layers in the Open Systems Interconnection (OSI) reference model. Figure 1.7 illustrates the Internet architecture model, and Table 1.2 describes the OSI reference model and the Internet architecture equivalents.

FIGURE 1.7 Internet architecture model

<table>
<thead>
<tr>
<th>OSI Reference Model Layer</th>
<th>Internet Architecture Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Application</td>
</tr>
<tr>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td>Transport</td>
</tr>
<tr>
<td>Transport</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Internet</td>
</tr>
<tr>
<td>Data-Link</td>
<td>Network Access</td>
</tr>
<tr>
<td>Physical</td>
<td></td>
</tr>
</tbody>
</table>

Each layer of the Internet architecture involves protocols, and each protocol has an associated RFC. This section describes common protocols used on the Internet by layer. These protocols will be discussed in detail throughout the book. Each protocol is listed with its respective RFC(s). Figure 1.8 illustrates their relationships within the Internet architecture.
Network Access Layer

The Network Access layer corresponds to the Physical and Data-Link layers of the OSI reference model. The Network Access layer accepts higher-layer packets and transmits them over the attached network, handling all the hardware details of interfacing with the network media. This layer usually consists of:

- The operating system’s device driver
- The corresponding interface card
- The physical connections

For Ethernet-based local area networks, the data sent over the media is referred to as Ethernet frames, which range in size from 64 to 1,518 bytes (1,514 bytes without the cyclic redundancy check).

The Network Access layer components can vary considerably, depending on the technologies that are responsible for placing data on the network media and pulling data off. Examples include:

- Local area networks (LANs) Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI)
Chapter 1 • The Internet and TCP/IP

Wide area networks (WANs)  Frame Relay, serial lines, and asynchronous transfer mode (ATM)

Internet Layer

The Internet layer corresponds to the Network layer of the OSI model. It is responsible for addressing and routing packets on TCP/IP networks. A packet received from the Transport layer is encapsulated in an IP packet. Based on the destination host information, the Internet layer uses a routing algorithm to determine whether to deliver the packet locally or send it to a default gateway.

The following are protocols used at the Internet layer:

- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)

The Internet layer of the Internet architecture uses the following protocols to address and route packets on TCP/IP networks.

Internet Protocol (IP)—RFC 791, STD 5

The Internet Protocol (IP) is the basic data-transfer method used throughout the Internet. It is responsible for IP addressing and performs the routing function, which selects a path to send data to the destination IP address.

Data is sent in the form of packets, also called datagrams. A packet is self-contained, independent of other packets; it does not require an acknowledgment and carries information sufficient for routing from the originating host to the destination host.

IP defines how routers are to process packets, when error messages are to be generated, and under what conditions packets are to be discarded.

Internet Control Message Protocol (ICMP)—RFC 792, STD 5

The Internet Control Message Protocol (ICMP) is the troubleshooting protocol of TCP/IP. ICMP is specified in RFCs 844, 1256, and 1788. It allows...
Internet hosts and gateways to report errors through ICMP messages. If a problem occurs on a TCP/IP network, an ICMP message will probably be generated.

**Internet Group Management Protocol (IGMP)—**
**RFC 1112, STD 5**

The Internet Group Management Protocol (IGMP) is used for multicasting. In multicasting, one source sends a message to a group of subscribers (multicast groups). For multicast delivery to be successful, members must identify themselves and the groups that interest them to local multicast-enabled routers. IGMP allows users to join and maintain membership in multicast groups.

**Address Resolution Protocol (ARP)—RFC 826, STD 37**

The Address Resolution Protocol (ARP) translates Internet addresses to physical addresses, such as an Ethernet's 48-bit physical address, also called Media Access Control, or MAC, addresses.

For example, assume two hosts are on a network, node1 and node2. Node1 knows the IP address of node2. However, if node1 wants to send a packet to node2, it must know the physical, or hardware, address of node2. To resolve the IP address to the hardware address, ARP sends a local broadcast and obtains the hardware address.

Once the address resolution is complete, ARP stores the information in an ARP cache for future requests. The ARP cache entry remains in the ARP cache for different lengths of time, depending on the operating system.

**Reverse Address Resolution Protocol (RARP)—**
**RFC 903, STD 38**

The Reverse Address Resolution Protocol (RARP) performs (as its name implies) the reverse function of ARP. It uses a node’s hardware address to request an IP address. RARP is generally used during initialization for diskless workstations to obtain an IP address.

For example, when a diskless workstation initializes, RARP reads the node’s unique hardware address and broadcasts a RARP request over the network, asking for an IP address. A RARP server responds to the request and provides an IP address.
Transport Layer

The Transport layer of the Internet architecture corresponds to the Transport and Session layers of the OSI model. The Transport layer accepts Application layer data and provides the flow of information between two hosts. The following two protocols are found at the Transport layer:

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

The Transport layer also divides the data received from the Application layer into smaller pieces (i.e., packets) before passing them to the Internet layer.

The Transport layer is also known as the Host-to-Host layer, the End-to-End layer, or the Source-to-Destination layer.

The Transport layer of the Internet architecture uses the following protocols to provide a flow of information between hosts.

Transport Control Protocol (TCP)—RFC 793, STD 7

The Transport Control Protocol (TCP) provides session management between the source and destination systems. It ensures that data is delivered in sequence, and that no duplicate data is sent. TCP is used with applications that communicate by establishing a session before transferring data, such as FTP and Telnet.

User Datagram Protocol (UDP)—RFC 768, STD 6

The User Datagram Protocol (UDP) provides a simple packet form of communication. One UDP packet is created for each output operation by an application, and a session is not necessary. Unlike TCP, UDP does not provide congestion control or packet sequencing, or send acknowledgments. It also does not retransmit lost packets or guarantee reliability. UDP is a connectionless protocol that is used by the Trivial File Transfer Protocol (TFTP) and the Simple Network Management Protocol (SNMP).

Application Layer

The Application layer of the Internet architecture corresponds to the Presentation and Application layers of the OSI model. The Application layer interacts with the Transport layer protocols to send or receive data.
Users can invoke application programs such as remote terminal protocol (Telnet), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) or Simple Network Management Protocol (SNMP) for access to nodes on the Internet.

The Application layer is also referred to as the Process layer.

The Application layer of the Internet architecture uses the following protocols to process and transmit data.

**Hypertext Transfer Protocol (HTTP)—RFCs 1945 and 2616**

The Hypertext Transfer Protocol (HTTP) is used to transport HTML documents (web pages) across the Internet. HTTP requires a client program on one end (a browser) and a web server on the other, both running TCP/IP. HTTP establishes a web server session and transmits HTML pages to a client browser. HTTP 1.0 establishes a new protocol connection for each page requested, which creates unnecessary Internet traffic. HTTP 1.1 uses persistent connections, which allow multiple downloads with one connection. Both the client and server must support HTTP 1.1 to benefit.

**File Transfer Protocol (FTP)—RFC 959, STD 9**

The File Transfer Protocol (FTP) is a system for transferring files between computers on a TCP/IP network. FTP offers an efficient and quick way to transfer files because it does not require the encoding and decoding data, which is necessary when using other methods such as sending files as e-mail attachments. FTP allows files to be uploaded to a server. HTTP usually allows only client downloads from the server.

**Trivial File Transfer Protocol (TFTP)—RFC 1350, STD 33**

Trivial File Transfer Protocol (TFTP) is used for initializing diskless systems. It works with the Bootstrap Protocol (BootP). TFTP uses UDP, whereas FTP uses TCP. Because TFTP is simple and small, it can be embedded in ROM, which is ideal for diskless workstations seeking network configurations upon initialization.

**Telnet (Remote Terminal Protocol)—RFCs 854 and 855, STD 8**

Telnet is a terminal emulation protocol developed for ARPANET. It allows a user to log on and run programs from a remote system. Telnet is normally used by a client terminal, or terminal emulator software on a PC.
Network News Transfer Protocol (NNTP)—RFC 977

The Network News Transfer Protocol (NNTP) allows sites on the Internet to exchange Usenet news articles, which are organized into topics such as “programming in C++” or “international trade issues.” To use newsgroups, you must have access to an NNTP server with which you are authorized to read and post news.

Gopher—RFC 1436

Gopher is a menu-based program used to find resources on the Internet. It is very similar in concept and practice to today’s Web: Users follow links from site to site in search of information. It was one of the first tools developed to pull the Internet together so users could access the entire Internet rather than just one site. Gopher servers have been largely replaced by web servers.

Simple Mail Transfer Protocol (SMTP)—RFC 821, STD 10

The Simple Mail Transfer Protocol (SMTP) is the Internet standard protocol for transferring e-mail messages from one computer to another. It specifies how two mail systems interact. SMTP is often used with Post Office Protocol 3 (POP3), which is a standard Internet mail server that uses SMTP’s messaging protocol. POP3 stores incoming e-mail until users authenticate and download it. POP3 is defined in RFC 1939 and STD 53.

Simple Network Management Protocol (SNMP)—RFC 1157, STD 15

The Simple Network Management Protocol (SNMP) is used for managing TCP/IP networks. It is a standardized management scheme that vendors can support. Thus all SNMP-compliant network devices can be centrally managed by an SNMP manager. SNMP also offers low resource requirements, portability, and wide acceptance.

Domain Name System (DNS)—RFCs 1034 and 1035, STD 13

The Domain Name System (DNS) is a mechanism used on the Internet to translate host computer names into Internet (IP) addresses. It is one of the most universal methods of centralized name resolution. For example, when a user requests the fully qualified domain name (FQDN) www.companyname.com, DNS servers translate the name to the IP address 201.198.24.108.
Bootstrap Protocol (BootP)—RFCs 951 and 2132

The Bootstrap Protocol (BootP) is an alternative to RARP. BootP allows diskless workstations to determine not only their IP addresses but also additional parameters, such as default gateways, and the addresses of particular servers, such as a DNS server. RARP provides only an IP address.

Dynamic Host Configuration Protocol (DHCP)—RFC 2131

The Dynamic Host Configuration Protocol (DHCP) is based on BootP. Like BootP, it is designed to assign Internet addresses and additional parameters, such as default gateways and DNS servers, to nodes on a TCP/IP network. Unlike BootP's, DHCP addresses and parameters can change with time (hence the term “dynamic”). DHCP servers can temporarily lease addresses and parameters for a fixed period of time to a client, then reassign the information to another client when the lease expires.

OSI/RM Protocol Examples

The networking protocols listed in this section are examples of common protocols that operate within the OSI/RM layers. It is important to recognize that each of these protocols exists in the Internet architecture model. They are provided here in the context of the OSI reference model for the additional detail provided by that model.

Application Layer Protocols

Application layer protocols, often called Upper-Layer protocols, allow applications to speak to one another across a network. More common Application layer protocols include:

- **Simple Mail Transfer Protocol (SMTP)**  
  Used to send e-mail messages from host to host.

- **Bootstrap Protocol (BootP)**  
  Responsible for sending TCP/IP address configuration information to hosts.

- **File Transfer Protocol (FTP)**  
  Used to transfer files between two hosts.

- **Hypertext Transfer Protocol (HTTP)**  
  TCP/IP suite protocol to interconnect World Wide Web servers with browsers requesting web pages.
The Internet and TCP/IP

AppleTalk Filing Protocol (AFP)  Used exclusively in AppleTalk networks; allows such networks to exchange files.

Simple Network Management Protocol (SNMP)  TCP/IP protocol suite for troubleshooting and managing networks, regardless of architecture.

Server Message Block (SMB) Protocol  Used in Microsoft networks; allows clients to work closely with servers. Specifically, it allows clients and servers to access files and request other services.

X.500 Protocol  Manages online directories of users and resources; an OSI directory protocol. The Lightweight Directory Access Protocol (LDAP) is used to access X.500 directories.

NetWare Core Protocol (NCP)  Allows files and printers to be shared on a Novell NetWare network.

Network File System (NFS) Protocol  Allows files and printers to be shared on a Unix network.

Transport Layer Protocols

The Transport layer provides reliable data delivery. Protocols used at this layer include:

Transmission Control Protocol (TCP)  Part of the TCP/IP suite; helps provide reliable delivery and manages sessions.

Sequenced Packet Exchange (SPX) Protocol  Part of the IPX/SPX protocol suite; similar to TCP in that it manages communication sessions.

NWLink Protocol  The Microsoft implementation of IPX/SPX protocol.

AppleTalk Transaction Protocol (ATP)  Part of the AppleTalk networking suite; provides reliable transmissions between hosts.

NetBEUI Protocol  Allows different applications on different computers using NetBIOS to communicate with one another; a nonroutable protocol.

Network Layer Protocols

Network layer protocols provide routing information to routers and addresses to hosts. Network protocols include:

Internet Protocol (IP)  Part of the TCP/IP suite; responsible for addressing hosts and routing packets in any network running TCP/IP, including the Internet.
Internetwork Packet Exchange (IPX) Provides addressing services for the Novell IPX/SPX suite.

NWLink Protocol The Microsoft implementation of IPX/SPX.

Datagram Delivery Protocol (DDP) Part of the AppleTalk networking suite; a best-effort packet (also called datagram) delivery protocol.

NetBEUI Allows different applications on different computers using NetBIOS to communicate with one another; a nonroutable protocol.

Data-Link Layer Protocols

Data-Link layer protocols provide reliable data transfer across the physical link. Data-Link layer protocols include:

Ethernet This LAN protocol was created by Xerox, Digital Equipment Corporation, and Intel. It is the most popular LAN technology.

Frame Relay This WAN protocol uses variable-length packets and allows high-speed connections using shared network facilities.

X.25 This WAN protocol is a precursor to Frame Relay technology. It was developed in the early 1970s and was the first packet-switching network standard.

You will learn more about many of these protocols throughout this book.

Major Networking Protocols Suites

Several networking protocols and architectures exist, all based on the OSI/RM. You were introduced to TCP/IP and IPX/SPX briefly in a previous section; however, many additional protocols are used for networking. This section will explain several important networking protocol properties. Following are some important networking protocols:

- TCP/IP
- IPX/SPX
- NetBEUI
- AppleTalk
- Data-Link Control (DLC)
- Systems Network Architecture (SNA)
Protocol Characteristics

Understanding TCP/IP is central to internetworking, and is dealt with throughout this book. This section will deal with the other identified major networking protocols. There are some characteristics that can be used to classify and differentiate the behavior and use of protocols.

Connection-Oriented (Stateful) and Connectionless (Stateless) Protocols

Some network protocols require that a host establish a connection, or session, before it transfers information. Because of this requirement, connection-oriented (i.e., connection-oriented) protocols are often called stateful protocols. A state is the name given to a session. Connection-oriented protocols are more reliable because they first gain a system’s attention, prepare it to receive information, then send the information. However, connection-oriented protocols require more system overhead, and are not always appropriate for certain networking tasks. An example of a connection-oriented protocol is TCP.

Other network protocols do not require a previously established session; they rely on a “best-effort” technology that sends the information, hoping that it will reach the other system. This protocol type is called connectionless, or stateless. An example of a stateless protocol is IP, which provides addresses for the TCP/IP suite. Many connectionless protocols send information by means of short messages called datagrams.

Receiving a phone call, for example, is a connection-oriented activity, mainly because it requires you to establish a continuous session before you can communicate. You can also immediately acknowledge that you received the information a caller has sent you, and this acknowledgment is part of that session.

Sending a message via the U.S. Postal Service, however, is a connectionless activity because you do not initiate a continuous connection to transmit the message. You simply send the message and hope that it arrives. Rather than being able to send an immediate acknowledgment that the package was received, the recipient would have to send another message indicating that your message arrived.

Although it might be tempting to regard a connection-oriented protocol as more important or reliable, this is not necessarily the case. Each protocol type has its own use in a network.
Routable and Nonroutable Protocols

Some protocols can travel through LANs and WANs and beyond because they can pass through a router. Routable protocols include TCP/IP and IPX/SPX. Nonroutable protocols use predefined, or static, routes that cannot be changed. Some protocols are nonroutable because they do not use the functions of the OSI/RM Network layer. Nonroutable protocols include NetBEUI, NetBIOS, Systems Network Architecture (SNA), Local Area Transport (LAT), and the Data-Link Control (DLC) protocols. You will learn more about routing later in the book.

To effectively use a nonroutable protocol, you can add a bridge (discussed later in the book) to your network or encapsulate the nonroutable protocol within a routable protocol, such as TCP/IP. Encapsulation is also called tunneling.

IPX/SPX

Novell, Inc. developed this once-dominant LAN and WAN protocol. Like TCP/IP, IPX/SPX is a protocol suite rather than a single protocol. Microsoft also supports IPX/SPX, although the corporation has renamed it NWLink (NetWare Link).

IPX

Internetwork Packet Exchange (IPX) is a connectionless protocol that resides at the Network layer of the OSI/RM. It is responsible for network addressing and forwarding packets to their destination, an action called routing.

SPX

Sequenced Packet Exchange (SPX) is a connection-oriented Transport layer protocol that uses services provided by IPX. SPX provides reliability to IPX: It ensures that packets arrive intact at their destination. Because this protocol resides at the Transport layer, it ensures reliable data delivery and manages sessions.

IPX/SPX Advantages and Disadvantages

IPX/SPX is not a vendor-neutral protocol. It was developed by Novell and is used mostly with Novell NetWare networks. TCP/IP has eclipsed IPX/SPX.
as the standard enterprise protocol due to its open nature. However, IPX/SPX is still common and it has always performed better than TCP/IP.

Although IPX/SPX is not supported on the Internet, thousands of IPX/SPX WANs use private networks or virtual private networks (VPNs) to communicate over long distances (you will learn about WANs, private networks, and VPNs later in this book).

Novell has adopted TCP/IP as its default protocol in Novell NetWare 5, although the company still supports IPX/SPX.

**IPX/SPX Frame Type**

IPX/SPX can use different frame types. Administrators can choose between the IEEE 802.2 or IEEE 802.3 frame types (you will learn about IEEE standards later in this book). Novell NetWare 3.12 and later default to the IEEE 802.2 frame type. Previous versions defaulted to IEEE 802.3. If you are using IPX/SPX and cannot make a connection, check to see whether your system’s frame type is compatible with those used by the rest of the network.

**Novell NetWare Layers**

Novell NetWare protocols can be classified using the Internet architecture model. Each layer includes the following protocols:

- **Network Access layer protocols** Ethernet, token ring, and ARCNET
- **Internet layer protocol** IPX
- **Transport layer protocols** SPX and Packet Exchange Protocol (PEP)
- **Application layer protocols** Error, Echo, Service Advertisement Protocol (SAP) and others

Figure 1.9 lists several Novell NetWare protocols.

**FIGURE 1.9** Novell NetWare protocols
NetBEUI

*NetBEUI* (pronounced “Net-boo-ee”) is an acronym for Network Basic Input/Output System (NetBIOS) Enhanced User Interface. It was first developed by IBM, but Microsoft has since implemented it as a solution for its peer-to-peer networks. NetBEUI is a nonroutable protocol, which limits its usefulness to small non-routed networks.

NetBIOS

*NetBIOS* stands for Network Basic Input/Output System. It was originally designed as a standard to let computers communicate with a local area network. NetBEUI extended this standard, hence the name NetBIOS Enhanced, or Extended, User Interface. Because NetBEUI is declining in popularity, NetBIOS is mainly used as a programming interface for applications. It resides at the Session layer (Layer 5) of the OSI/RM. NetBIOS can operate over NetBEUI, as well as over routable protocols such as TCP/IP and IPX/SPX. Microsoft Windows computers up to and including NT use NetBIOS names to identify one another and communicate on a network. Windows 2000 includes support for NetBIOS but does not require it.

AppleTalk

AppleTalk is used only in Apple networks, and is thus proprietary. AppleTalk Phase II allows this protocol to work with others. Rather than using the term “domain” or “network,” AppleTalk divides groups of computers into zones.

Data-Link Control (DLC)

IBM originally developed DLC to enable client machines to work with mainframes. However, Hewlett-Packard for a period of time had adopted DLC as a means to connect its laser printers to LANs.

Systems Network Architecture (SNA)

IBM introduced SNA in 1974 as a mainframe network architecture. Because it is an architecture, it includes a network topology and a series of protocols. The SNA model is quite similar to the OSI/RM. In fact, SNA inspired the creation of the OSI/RM.
The SNA market is valued at about $20 billion per year. Even though it is an older architecture, it is still widely used within mainframe networks, in some AS-400 implementations, and on many Unix platforms that connect to these networks.

**Multiprotocol Networks**

Networks commonly use two routable protocols, such as TCP/IP and IPX/SPX, although this combination could cause problems with system overhead in large, heavily visited sites. Such a combination provides system redundancy and can speed connectivity.

Sometimes routable and nonroutable protocols should be combined, even in a routed network. A nonroutable protocol such as NetBEUI could be quite useful in a LAN and WAN situation because it can deliver traffic to local computers without the overhead associated with TCP/IP. If a user sends a message to an employee in the same LAN, NetBEUI will handle all of this transaction. However, if someone sends a message to a recipient on another LAN (activity that involves a router), the system will automatically use a routable protocol such as TCP/IP.

You should also consider, however, that using multiple protocols can increase the time it takes to maintain and troubleshoot a network. In addition, the more protocols you use, the more system overhead you create.

**De-multiplexing**

*De-multiplexing* is the process a destination computer uses to strip each layer of headers from the incoming packet resulting in the payload. It is an excellent way to show how the Internet protocols work within the Internet architecture. Figure 1.10 displays the de-multiplexing process. You can refer to this diagram throughout the book.
FIGURE 1.10  De-multiplexing of protocols

As a packet is received by a network operating system, each layer’s header is removed, and the packet is passed to the appropriate protocol at the next layer. Thus, although many Ethernet datagrams may be received, some will be RARP or ARP, while others will be IP. While each of these would have a similar header at the Physical layer, the uncovered layers further define which protocols and applications receive each type of communication.

Specialized Serial Interface Protocols

Many users access the Internet from home using a modem. The point of presence (POP) is the location where a user dials into the Internet via a modem. Usually the POP is an Internet Service Provider (ISP). The term may also be used to denote the point where a long-distance carrier connects to a local telephone company. If a local company does not exist, the POP is the line connected to the user.

Modem connections are often made over a standard telephone and use the Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP) to connect to an ISP. The following sections describe these protocols. Serial Line Internet Protocol (SLIP) is a protocol devised to allow a computer with a modem to connect to the Internet over a phone line. Point-to-Point Protocol (PPP) is an improved version of SLIP that includes more options for authentication and more robust communication control.
Point-to-Point Protocol (PPP)—RFC 1661, STD 51

Point-to-Point Protocol (PPP) is an encapsulation method for sending IP packets over a serial link. It was created in 1991 by the IETF and supports both asynchronous and synchronous links. Therefore, it can run on standard phone lines, full-duplex links such as Integrated Services Digital Networks (ISDNs), and high-speed T1 and T3 lines.

PPP uses the Link Control Protocol (LCP) to establish, configure, and test a connection during the logon process. This protocol allows both computers to negotiate, and provides greater reliability. PPP also enables password protection using the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP).

PPP has a family of specific Network layer protocols, called Network Control Protocols (NCPs). NCPs exist for IP, AppleTalk, and DECnet. For example, the NCP for IP allows hosts to negotiate compression headers. Figure 1.11 displays the basic components and process for PPP and SLIP, which is discussed in the next section.

Multilink Point-to-Point Protocol (PPP-MP)—RFC 1990

If a user connects to his or her ISP using a standard ISDN line, PPP typically uses one 64Kbps B channel for transmission. To obtain a higher transmission speed, two or more B channels can be bridged using Multilink PPP. For example, two ISDN 64Kbps B channels can be combined for a transmission rate of 128Kbps.
Serial Line Internet Protocol (SLIP)—RFC 1055, STD 47

Serial Line Internet Protocol (SLIP) is a simple form of encapsulation for sending IP packets over serial lines. SLIP can be used on RS-232 serial ports and is usually used to connect home users to the Internet with a standard phone line. SLIP supports asynchronous links. Automated scripts are generally used to automate the logon process.

SLIP is an older protocol that has been widely replaced by PPP for the following reasons:

- SLIP supports only IP, whereas PPP has implementations that support protocols in addition to IP.
- SLIP does not support authentication. Authentication is the process of identifying a user who is logging on to a system. It usually requires a username and a password.

Summary

In this chapter, you defined the term “internetwork” and compared it with traditional networking. You learned about the importance of TCP/IP and the corporate environment, and how TCP/IP can use your existing LANs and WANs as backbones for interoperability. Next, you studied the evolution of the Internet and its organizations, including the ISOC, IAB, IETF, and IRTF, as well as how TCP/IP relates to standards such as the OSI/RM and IPX/SPX. You reviewed the four layers of the Internet architecture model: Application, Transport, Internet, and Network Access, and aligned the Internet architecture model with the OSI reference model. You reviewed RFCs, including the different states of protocols, STDs versus RFCs, and reference RFCs. You also defined common Internet protocols and matched them to their corresponding Internet layers as well as to the RFC/STD for each. You identified key internetworking protocols and explained the need for multiprotocol networks.
Key Terms

Before you take the exam, be certain you are familiar with the following terms:

- ARP
- ARPANET
- BootP
- Challenge Handshake Authentication Protocol (CHAP)
- cyclic redundancy check (CRC)
- de-multiplexing
- DHCP
- DNS
- draft
- Ethernet
- experimental
- Frame Relay
- FTP
- fully qualified domain name (FQDN)
- Gopher
- header
- HTTP
- ICMP
- IGMP
- Internet architecture
- Internet Architecture Board (IAB)
- NCP
- NetBEUI
- NetBIOS
- network
- NFS
- NNTP
- nonroutable
- NOS
- NSFnet
- OSI/RM
- packet
- Password Authentication Protocol (PAP)
- Point-to-Point Protocol (PPP)
- POP
- proposed
- RARP
- Requests for Comments (RFCs)
- routable
- Serial Line Internet Protocol (SLIP)
- SMB
- SMTP
Be able to define “internetwork” and explain this concept’s importance in today’s data communications marketplace. An internetwork is a group of several LANs and WANs that operate under different network operating systems and are connected and function together, sharing information between corporate, government, or individual entities. Internetworking has eliminated the need for IS administrators to learn networking protocols for all network operating systems, allowing them to communicate using TCP/IP.

Understand how TCP/IP can use your existing LANs and WANs as backbones for interoperability. TCP/IP can function in parallel with existing protocols, allowing heterogeneous equipment and protocols to speak a common language and communicate.

Be able to relate internetworks to the concept of the corporate enterprise network. A series of WANs may create an “internetwork” consisting of private or public networks. Historically, a corporate enterprise network...
was private, with leased lines connecting corporate network nodes. With the rise of the Internet, corporations use public Internet connections to quickly and inexpensively expand corporate network access points, and individuals have personal access to published information.

**Know the evolution of the Internet.** The Internet grew from ARPANET, which connected four universities in 1969, into a global research network in the 1980s, called NSFnet until it was dubbed “the Internet” in 1987. In 1995 the National Science Foundation network was decommissioned, as a consortium of private telecommunications companies provided global connectivity that continues to expand.

**Be able to define and discuss Internet-related organizations, such as ISOC, IAB, IETF, and IRTF.** These are all volunteer organizations dedicated to maintaining and enhancing the Internet and promoting global information exchange. The Internet Society (ISOC) is the global authority for the Internet. The Internet Architecture Board (IAB) is responsible for managing long-term technical direction of the Internet, while the Internet Engineering Task Force (IETF) focuses on solving operational and short-term technical problems. The Internet Research Task Force (IRTF) researches and develops new network technologies.

**Understand how TCP/IP relates to standards such as SNA, OSI, and IPX/SPX.** TCP/IP is an open standard, while SNA and IPX/SPX are proprietary standards. The OSI reference model is the basis for all of these networking protocols.

**Be able to identify key internetworking protocols and explain the need for multiprotocol networks.** TCP/IP can function in parallel with other protocols such as SNA, IPX/SPX, and NetBEUI, allowing for interoperability between heterogeneous systems. Each protocol has strengths and weaknesses, although TCP/IP has been shown to be extremely robust and flexible. In some situations, a proprietary protocol such as SNA or IPX is desired or offers advantages, which results in multiprotocol networks.

**Be able to define and describe the Internet architecture model.** The Internet architecture model uses four layers to describe the relationship and communication of different network elements. The Application layer includes both layers 6 and 7 of the OSI/RM. The Transport layer includes both layers 4 and 5 of the OSI/RM.
Know the nature, purpose, and operational essentials of TCP/IP. TCP/IP is an open set of protocols that uses ports and Internet addresses to allow computers with different operating systems, network topologies, and protocols to communicate. Important elements of IP are TCP, UDP, and ICMP. TCP and UDP reside at Layer 4 of the OSI/RM while ICMP is at Layer 3.

Be able to define and describe various Internet protocols. DNS associates a fully qualified domain name with an IP address.

ARP resolves an IP address to a Media Access Control (MAC) address.

RARP resolves a Media Access Control (MAC) address to an IP address.

Understand the operation of Point-to-Point Protocol (PPP) and Multilink PPP. PPP is an encapsulation method for sending IP packets over a serial link, either synchronously or asynchronously. PPP uses Link Control Protocol (LCP) to establish and configure a connection, including authenticating with PAP or CHAP. After connecting, PPP uses Network Control Protocols (NCPs) to negotiate communication with various protocols (e.g., IP). PPP can also bridge ISDN B channels in order to attain a higher transmission rate.

Be able to find RFCs and download them from the Internet. Requests for Comment can be found at www.rfc-editor.org/rfc.html. Some important RFCs are 2800, 1700, 1122, 1123, and 1812. Many other RFCs are important in various contexts.
Review Questions

1. Internetworking is defined as:
   A. the application of vendor-centric networking principles.
   B. the drive to simplify network communication.
   C. the method used by an organization to communicate with itself.
   D. the task of working with different, or heterogeneous, systems.

2. Which of the following items does TCP/IP use to allow a LAN to operate with another LAN?
   A. A network interface card
   B. A router
   C. A repeater
   D. A protocol gateway

3. Which of the following statements describes the advantages TCP/IP offers to corporate networks?
   A. TCP/IP encourages corporate networks to rely on single platforms.
   B. TCP/IP discourages corporations from relying on older mainframe networks.
   C. TCP/IP requires corporations to rely on a single vendor.
   D. TCP/IP allows corporations to use legacy systems to communicate with any other system on their internetwork.

4. What was the purpose of ARPANET?
   A. It was designed to allow government and researchers to interact and to work from any location on the network.
   B. It was designed to decrease the number of connections among hosts in a network.
   C. It was designed to concentrate network control within a central hub.
   D. It was designed to safely shut down a network in which many of the hosts were incapacitated.
5. When did the NSFnet become known as the Internet?
   A. 1969
   B. 1980
   C. 1986
   D. 1987

6. Which of the following protocols is often used with POP and IMAP on a server?
   A. HTTP
   B. FTP
   C. SMTP
   D. SNMP

7. Which of the following statements accurately describes the relationship of TCP/IP to IPX/SPX?
   A. TCP/IP and IPX/SPX are both networking protocols.
   B. TCP/IP and IPX/SPX are both vendor-neutral protocols.
   C. TCP/IP and IPX/SPX are both vendor-specific protocols.
   D. TCP/IP provides better performance than IPX/SPX.

8. The packet creation process begins with:
   A. Layer 2 (the Data-Link layer) of the OSI/RM.
   B. Layer 4 (the Transport layer) of the OSI/RM.
   C. Layer 1 (the Physical layer) of the OSI/RM.
   D. Layer 7 (the Application layer) of the OSI/RM.
9. Which of the following features accurately describes multiprotocol networks?
   A. They decrease the time it takes to troubleshoot a network.
   B. They combine routable protocols only.
   C. They increase the time it takes to maintain a network.
   D. They combine nonroutable protocols only.

10. The Internet architecture divides protocols into:
    A. packets
    B. layers
    C. nodes
    D. Ethernet frames

11. Which of the following terms is used to classify a protocol being seriously considered as an Internet Standard?
    A. Proposed
    B. Informational
    C. Draft
    D. Common

12. Which of the following Internet architecture layers is responsible for addressing and routing packets on TCP/IP networks?
    A. The Internet layer
    B. The Application layer
    C. The Transport layer
    D. The Network Access layer
13. Which of the following protocols is known as the troubleshooting protocol of TCP/IP?
   A. File Transfer Protocol (FTP)
   B. Hypertext Transfer Protocol (HTTP)
   C. Address Resolution Protocol (ARP)
   D. Internet Control Message Protocol (ICMP)

14. Which of the following statements accurately describes the Point-to-Point Protocol (PPP)?
   A. It supports only asynchronous links.
   B. It uses the Dynamic Host Configuration Protocol (DHCP) to establish and test a connection during the logon process.
   C. It supports both asynchronous and synchronous links.
   D. It is designed to assign Internet addresses.

15. Requests for Comments (RFCs) are identified by:
   A. length
   B. number
   C. content
   D. author

16. In the Internet architecture model, the physical media exists at which layer?
   A. Transport
   B. Network
   C. Internet
   D. Network Access
17. Which group holds authority for the Internet?
   A. IAB
   B. IETF
   C. ISOC
   D. IRTF

18. Which group creates Internet standards?
   A. IAB
   B. ISOC
   C. IETF
   D. IRTF

19. Which RFC governs behavior of multicasting?
   A. 1112
   B. 792
   C. 1945
   D. 1256

20. RFC 793 pertains to which OSI and Internet architecture layers?
    A. Network Access
    B. Transport
    C. Application
    D. Internet
Answers to Review Questions

1. D. Internetworking deals with connecting different systems, or connecting networks that communicate using different protocols, often crossing vendor-centric and vendor-neutral principles, sometimes making the network more complex rather than simpler.

2. B. A router is used to connect LANs, while a network interface card connects to a LAN, and a repeater extends a single LAN. A protocol gateway performs a specific function between networks, but does not connect the LANs at the network level like a router does.

3. D. TCP/IP allows multiprotocol networks to communicate, using an open standard that is implemented by many vendors in order to communicate between single-vendor, proprietary systems.

4. A. ARPANET originally connected four universities in California, Utah, and Connecticut, so that university and government researchers could work collaboratively from any of those locations.

5. D. In 1980 the ARPANET was decommissioned and turned over to the National Science Foundation, and renamed NSFnet. The network expanded with regional hubs and 56Kbps connections, and became known as the Internet in 1987.

6. C. Simple Mail Transport Protocol (SMTP) is used to transfer e-mail between servers, and is often run in conjunction with POP3 and IMAP, protocols for client e-mail access.

7. A. Both are networking protocols, but it is important to recognize the errors in the other answers. IPX/SPX is vendor-specific and comes from Novell, while TCP/IP is vendor-neutral. Absolute statements about performance are never absolutely true, and case studies and research can be usually be found to support opposing sides, but IPX/SPX typically outperforms TCP/IP.

8. D. Applications initiate packets, thus packet creation begins at Layer 7 of the OSI/RM.
9. C. Multiprotocol or heterogeneous networks have become common, combining both routable and nonroutable protocols, increasing both troubleshooting and maintenance time for networks.

10. B. The Internet architecture defines four layers: Network Access, Internet, Transport, and Application.

11. C. The Draft stage of RFCs immediately precedes the Standard stage. However, if changes are made during consideration as a Draft RFC, the RFC must return to Proposal stage.

12. A. The Internet layer is responsible for addressing and routing packets. This should not be confused with its peer in the OSI/RM, the Network layer, which is not analogous to the Internet architecture Network Access layer.

13. D. ICMP operates at the Internet layer of the Internet architecture model, below the Transport layer, so that ICMP messages may pass information about errors in the Transport layer.

14. C. PPP supports synchronous and asynchronous links over modems and other connection methods.

15. B. RFCs are sequentially numbered.

16. D. The Physical layer and Data-Link layer reside within the Network Access layer of the Internet architecture model.

17. C. The Internet Society (ISOC) is a voluntary membership organization whose objective is to promote global information exchange using Internet technology.

18. C. The Internet Engineering Task Force (IETF), creates standards, known as Request for Comments (RFCs), which progress through Experimental, Proposed, Draft, and Standard stages.
