Unit 5
Networks—LANs and WANs

Unit Objectives

After completion of this unit you will be able to identify and describe the following concepts:

1. OSI 7-layer model
2. Network Topologies
3. LAN—Types and Equipment
4. TCP/IP—Protocol and Applications
5. The Internet—Access techniques and terminology

5-1 OSI 7-Layer Model

In 1977, the International Standards Organization (ISO) established a subcommittee (SC16) for Open Systems Interconnect (OSI). The ISO OSI reference model is a formal logical structure of the interactions and functions necessary to allow for communications services to the user. The OSI reference model allows for communications systems with different architectures and different operating systems, to communicate with each other.

The OSI model consists of 7 layers, each having specific associated functions. We will take a look at each of these layers and their respective functions before going further. Starting at the upper layers. Layers 4 through 7 are referred to as the upper layers. The upper layer functions typically reside in terminal equipment.

	Upper Layers
Layer 7	**Application** Layer—Services to user applications
Layer 6	**Presentation** Layer—Data representation, format and code interpretation
Layer 5	**Session** Layer—Establish, maintain and control sessions between two entities
Layer 4	**Transport** Layer—End-to-end control of data transfer, multiplexing and mapping

The three lower layers are more relevant to digital communications network equipment (routers, switches, etc.), so we will focus on them. It is important to note that as we process information in the network, the **higher layers are typically slower**. This is due to the greater amount of processing that takes place at higher layers. The **fastest layer is the physical layer**.

	Lower Layers
Layer 3	**Network** Layer—Routing, controlling congestion, address translation
Layer 2	**Data Link** Layer—Establish, maintain and release links; error detection
Layer 1	**Physical** Layer—Electrical, mechanical and functional control of data circuits

We have considered the physical layer in the previous units. T-carriers and SONET (unit 3) are physical layer protocols. A **protocol**, in telecommunications, is a set of rules governing the transport of information. Line codes and modulation techniques (unit 2) are physical layer functions. Transport media, such as optical fiber (unit 4), work at the physical layer.

Just as each layer has a function, the name of the Protocol Data Unit (PDU) at each layer has a name. Refer to the following table for names associated with each layer.

Layer	PDU Name
Application	Message (or PDU)
Presentation	Format (or PDU)
Session	Dialog (or PDU)
Transport	Segment
Network	Packet
Data Link	Frame (or Cell)
Physical	Bits

So far we have defined the seven layers as far as function and name of PDU. Each layer also has overhead associated with it. As user data moves down the protocol stack, overhead is added. This adding of overhead is referred to as **encapsulation**. At the intermediate nodes in a network, the overhead associated with a specific layer is used for error control, route selection, etc. At the receiving end, the overhead aids in reassembling the data into the proper format for the end user application. From the end user point of view, the overhead does not exist. The applications appear to interact directly. This process is illustrated in Figure 5.1.

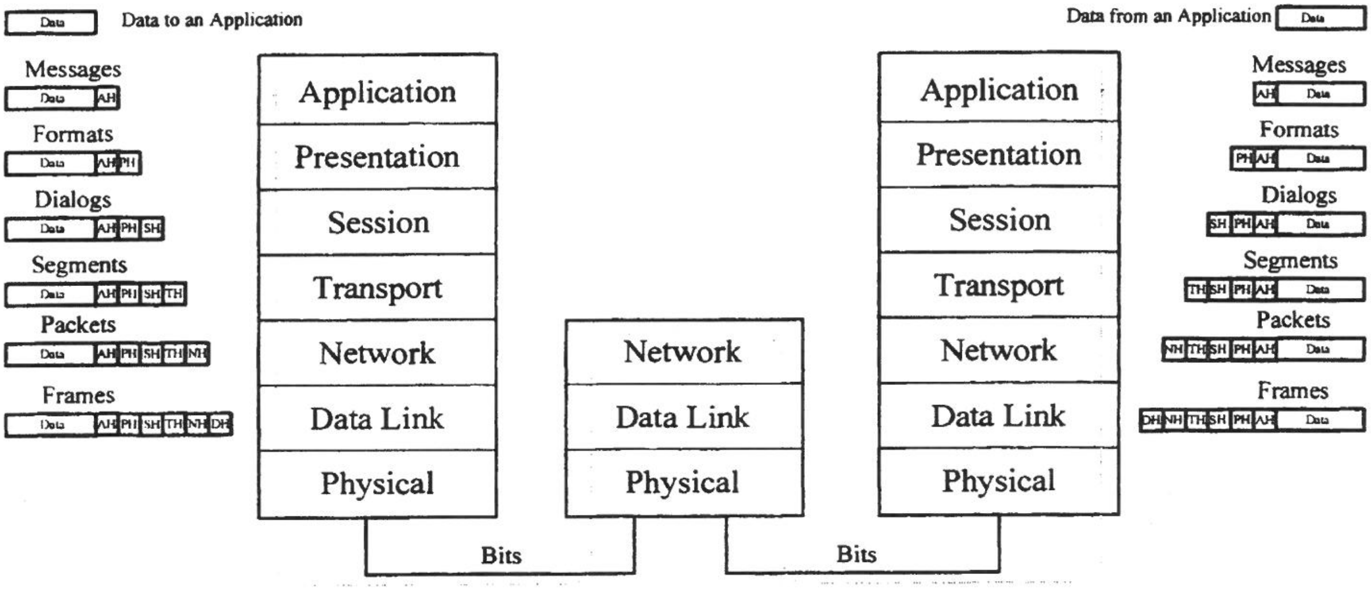

Figure 5.1 Layered Transport Process between Two End Systems

We have had a look at the layers and general functions associated with each. When we consider different network protocols, we will use the 7-layer model as a **reference to compare against other protocol stacks.**

5-2 Network Topologies

When considering network topologies it is important to make the distinction between **physical** and **logical topologies**. A physical topology is the actual layout of equipment. A logical topology addresses actual data flow characteristics. The physical and logical are often the same, but they can be different. When they are different it is important to know which topology (physical or logical) is being discussed.

Refer to Figure 5.2. A Token Ring is a good example of how the two topology references can differ for the same network. In a ring network, the signal passes through each node in a clock-wise (or counter-clockwise) direction. The Token Ring is **logically a ring** (A), but physically implemented as a **star** (B) with a centrally located MAU (Multi-station Access Unit) for ease of wiring. The actual traffic travels through each site to get to the next (dashed gray line in B). This is because the wiring layout is centralized, but the data flows in a ring pattern.

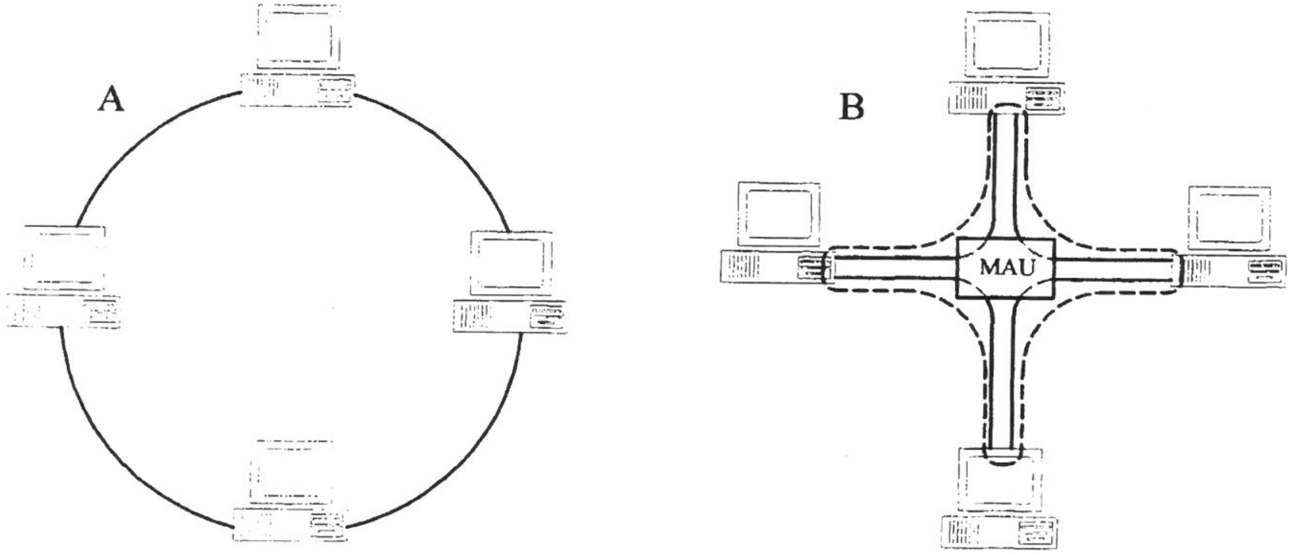

Figure 5.2 Token Ring: A Logical Ring and Physical Star

Before we go any further, let's take a look at different topologies. Refer to Figure 5.3.

- **Star**—Also referred to as hub/spoke or point to multi-point. Each node is connected to a central point. It is common to all types of networks, local area networks (LANs) and wide area networks (WANs).
- **Mesh**—Each node is connected to all other nodes. This provides maximum connectivity and rerouting capability. It is used in WANs when link availability is the critical design factor. The disadvantage of a mesh configuration is the expense.
- **Ring**—Traffic passes through each node, in turn. This is common to both LANs and WANs. Self-healing ring implementations—such as dual, counter-rotating **ring**—allow for high reliability transport. An example of a wide area network using a self-healing ring topology is SONET.

- ✓ **Bus**—All nodes are connected together by a single medium. Each node broadcasts information. Typically used in a LAN (Example: Ethernet) environment, sharing the medium among all users on a first come first served basis.
- ✓ **Tree**—A hierarchical star network topology. Typical of telecommunications networks.
- ✓ **Hybrid**—A combination of topologies. For example, a mesh network is reliable but expensive. So a hybrid network could be a combination of a mesh, on critical routes, and a star connecting small terminal nodes. Due to the need to balance reliability and cost, hybrid topologies are common in WANs.

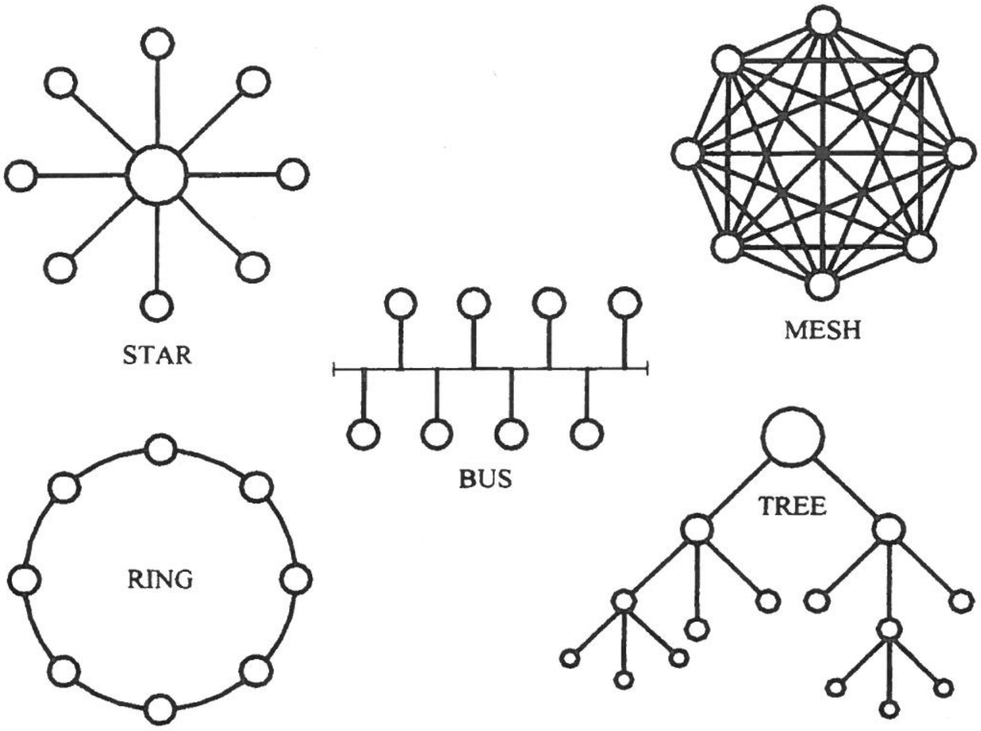

Figure 5.3 Topology Types

5-3 Local Area Networks (LANs)

A Local Area Network is a network that covers a small geographic area, such as a building, and provides high data rates to users. A LAN connects and supports PCs (Personal Computers) and allows for sharing of peripherals (printers, scanners, etc.) and information among users. Users are typically connected via a **shared medium**, accessing the medium in turn. The medium can be coaxial cable, twisted pair and optical fiber. Some modern LANs are even wireless.

LAN protocols typically work at the physical and data link layers. Node addresses are pre-assigned by the manufacturer in the Network Interface Cards (NIC). The two most common LAN standards in use today are Token Ring and Ethernet. Since Ethernet is the most flexible and therefore most popular, we will focus primarily on it.

5-3.2 LAN Access Techniques

Before we look at access techniques, we need to define some basic terms regarding various networking protocols.

- ✓ **Connectionless**—A protocol for the transfer of information between two nodes without a pre-coordinated connection between them. The PDUs transported by a connectionless protocol are referred to **datagrams**.
- ✓ **Connection-oriented**—A protocol for the transfer of information between two nodes after a logical connection (also called a virtual circuit) has been established between them.
- ✓ **Full-duplex**—A communications link allowing both parties (nodes or hosts) to transfer information simultaneously.
- ✓ **Half-duplex**—A communications link in which parties alternate (take turns) transferring information.

Access techniques are protocols (sets of rules) regarding how and when to access a **shared medium**. We will consider two basic LAN access techniques: Token passing and Carrier Sense Multiple Access with Collision Detection (CSMA/CD). These access techniques are connectionless, relying on a higher level protocol to establish a connection.

Token Passing

Token passing is common to both Token Ring and Fiber Distributed Data Interface (FDDI). FDDI was initially a Metropolitan Area Network (MAN) technique, but is now most often used in LAN environments. Token passing is a **deterministic technique** that employs a "token", which is passed in turn around a ring. The token is regenerated at each node in the ring as it passes through it. Figure 5.4 shows an example of this process.

As the token circulates from node to node (1), if a node has traffic it needs to send, and the token is free, the node (node C in the example) will seize the token and add it to the beginning of its information (2). The token will become part of the information "header". Assume that the information is addressed to node B. The information will pass through nodes D and A, being examined by each node to determine if it is the addressee. When it finally reaches node B, node B will remove the information and free up the token. The token will now continue to circulate until it is seized by another node for access.

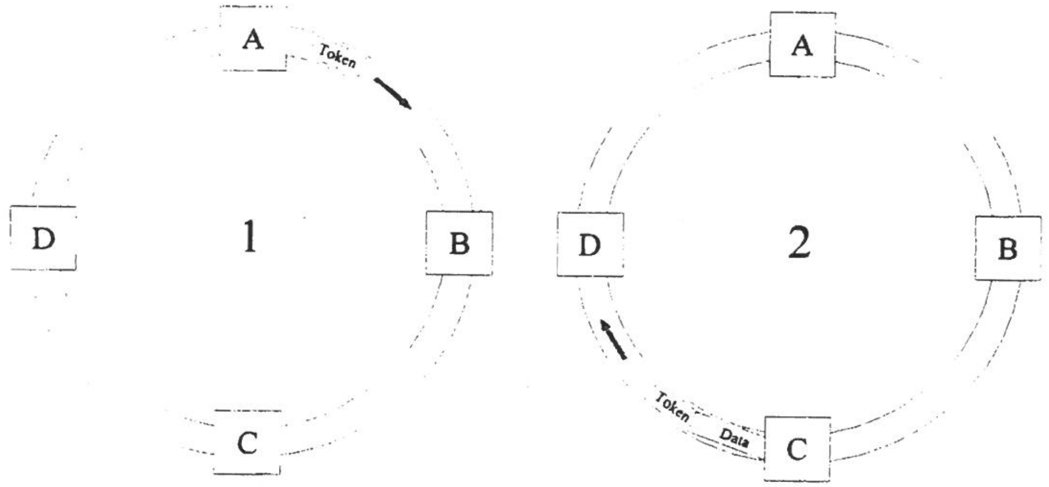

Figure 5.4 Token Passing

CSMA/CD

CSMA/CD is used in Ethernet for access to the shared medium. In order to understand how CSMA/CD works we must first take a look at the Ethernet topology. Actually, we must look at the original type of Ethernet topology. This was a physical and logical bus topology based on a combination of coaxial cable and optical fiber.

Refer to Figure 5.5. The original Ethernet was called 10base5. This is shorthand for **10** Mbps, **base**band signal and **500** meters segments. The original 10base5 Ethernet LAN (referred to as "thick Ethernet") consisted of 5 segments—3 coaxial and 2 fiber connected by **repeaters**. A **repeater is a physical layer device** that performs the function of regenerating a signal. The fiber segments were for interconnecting buildings and were not meant to have nodes attached to them. The nodes were attached to the coaxial segments via transceiver modules.

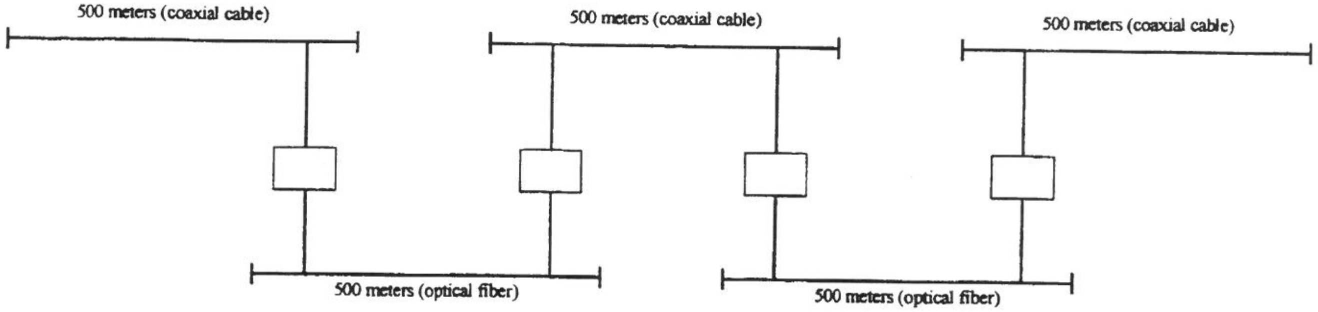
500 meters (coaxial cable)
500 meters (coaxial cable)
500 meters (coaxial cable)
500 meters (optical fiber)
500 meters (optical fiber)

Figure 5.5 Original 10base5 Ethernet Configuration

The segment limitation of 500 meters was based on signal attenuation and the need to regenerate it. CSMA/CD is a random access technique. A node gains access in the following manner:

1. Listen to see if anyone is using the medium (**carrier sense**)
2. If there is no traffic on the medium, transmit information
3. If there is traffic, wait until the link is clear and then transmit information

This seems to be a reasonable access technique. But what happens when a node at one end of the LAN determines that there is no traffic and begins sending its information at the same time that a node at the other end of the LAN performs the same function? Now there are two nodes simultaneously transmitting. **A collision will occur**. This is why a **collision detection** technique is needed.

When traffic from two users collide, it is due to the propagation delay of the medium. Both hear nothing when listening and both decide to transmit at approximately the same time. When one of the transmitting nodes detects another signal while it is transmitting, it immediately stops and sends a "jam signal". This alerts all users that a collision has occurred. When the other node receives the jam signal it stops transmitting as well. Both nodes will then wait a random length of time before making another attempt.

Ethernet nodes only listen for a collision while they are transmitting. Therefore, once a node begins transmitting, it must continue to do so long enough for the most distant device (2500 meters in 10base5) to receive at least the beginning of the frame, plus the time required to receive a jam signal from that distant device if a collision occurs. This is referred to as **round trip time** (RTT). So, in order to reduce the number of collisions there must be a **minimum**

frame size equal to RTT over the 2500 meters. The minimum frame size for Ethernet of **64 bytes** is based on this requirement.

The problem with 10base5 Ethernet was the thick coaxial cable that had to be laid out in a bus configuration using expensive transceivers for node attachment. The next step in the evolution of Ethernet came with 10base2, also called "thin Ethernet". Thin Ethernet uses a smaller coaxial cable and no transceivers. The problem with the smaller cable was the greater attenuation reduced the length of a given segment down to 185 meters (the 2 in 10base2). The topology of 10base2 is the same as 10base5—a bus.

A physical bus topology is not an easy one to implement or modify. So, Ethernet finally went to a **physical star** topology (refer to Figure 5.6) called 10base-T. The T stands for twisted pair cable. Since twisted pair has a higher attenuation than coaxial cable, the maximum distance from a node to the hub is 100 meters. Going to a physical star and using less expensive twisted pair cable makes implementation and management much easier. As you can see in Figure 5.6, the star topology is implemented with a **central hub**. The hub is really a multi-port repeater, providing access to an Ethernet bus.

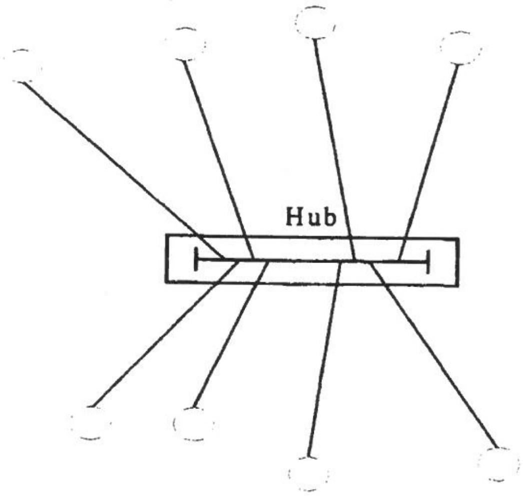

Figure 5.6 Ethernet 10Base-T Physical Star Topology

Let's take a look at a comparison table of the various LANs that we have considered. This is not a comprehensive list. Ethernet also works at 100 Mbps and 1 Gbps, but we are only considering the fundamental concepts of Ethernet.

LAN Type	Bit Rate Mbps	Medium	Access Technique	Distance Limitation**	Topology Physical	Topology Logical
Token Ring	4 and 16	STP*	Token Passing		Star	Ring
Ethernet						
10Base5	10	UTP	CSMA/CD	500 meters	Bus	Bus
10Base2	10	UTP	CSMA/CD	185 meters	Bus	Bus
10Base-T	10	UTP	CSMA/CD	100 meters	Star	Bus

* STP—Shielded Twisted Pair, UTP—Unshielded Twisted Pair

**Distance limitation due to attenuation

The problem with 10base5, 10base2 and 10base-T is that any collision occurring on segments connected by repeaters is propagated to all users. This is referred to as a **collision domain**. We will consider how to deal with this problem in the next section.

5-3.3 Types of LAN Equipment

Now that we have considered some LAN access techniques, the next issue is equipment types. We will list the equipment types and discuss each one in turn, considering its function and position in the 7-layer model.

Repeaters

As previously mentioned, repeaters work at the **physical layer**. They perform the function of regenerating the signal between segments. They also **propagate** (pass-on to the next segment) **collisions in Ethernet LANs**, limiting the total distance (based on minimum frame size) and number of users.

Bridges

Bridges forward frames between LAN segments based on the firmware addresses of the Network Interface Cards. These MAC (Media Access Control) addresses are pre-assigned by the NIC manufacturer. A bridge works at the **Data Link Layer** and **does not propagate collisions**. This means that we can **segment LANs into separate collision domains with a bridge**.

Refer to Figure 5.7 showing two LANs connected by a bridge. A bridge works by reading **all** traffic on its ports and forwarding traffic with a source address that it does not associate with the specific port. The bridge develops a lookup table by listening to the source addresses (SA) on a specific port. When information is sent, it compares the destination address (DA) with the SAs in its table. If there is a match, it does not forward the traffic to another port. If there is no match, it will forward the information. For example, node 53 on LAN segment B is sending to node 24 on LAN segment A. The bridge will not have a source address entry on its LAN B port for node 24, so it will forward the frame to LAN A.

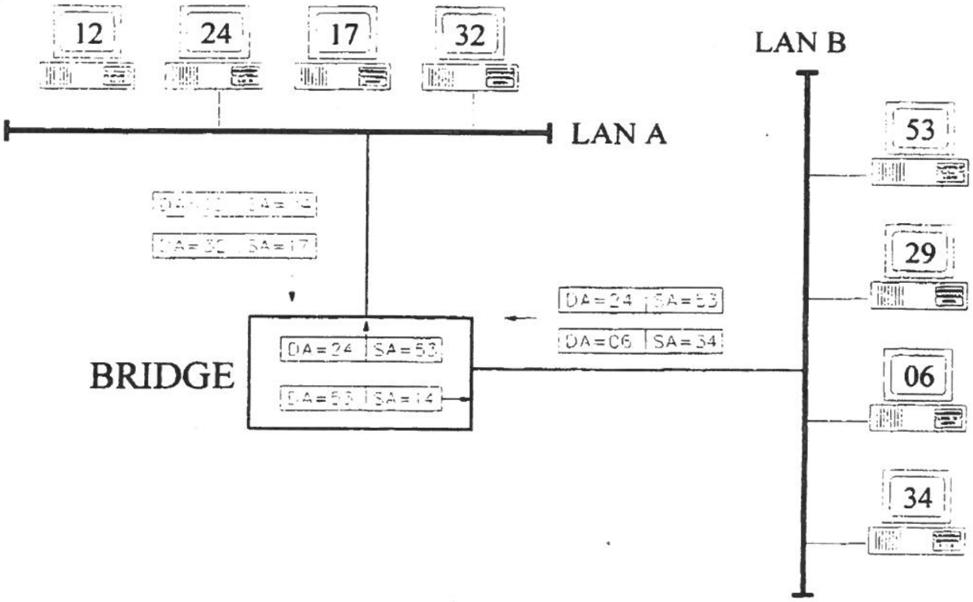

Figure 5.7 Bridge Example

Layer Two Switches

A bridge segments LANs into collision domains. There can be many users sharing a single collision domain. A way of reducing the number of users in a collision domain is to have bridges with many ports, assigning smaller groups (referred to as work groups) to each port. That was the original implementation of layer two switches—a multi-port bridge. Individual nodes can be attached directly to a layer two switch, each having its own collision domain. Figure 5.7 could illustrate this concept if there were more ports.

Layer two switches have evolved, since the original multi-port bridge, into very high speed switching devices, practically eliminating the need for bridges. Ethernet was originally a half-duplex access technique. Layer two switches have allowed for full-duplex operation, effectively doubling the bit rate of an Ethernet LAN.

Routers

Bridges and layer two switches forward traffic they do not recognize. This is a problem with **broadcast traffic.** Since the destination **address of a broadcast is all 1s**, a bridge (or layer two switch) would not see the address in its lookup table. This means that **all broadcast traffic is forwarded by bridges and layer two switches**. This is called a **Broadcast Domain.** Routers work at the Network layer and forward traffic based on the Network layer address of the destination host (node). So, routers do not forward broadcasts.

Routers select a path based on information in its routing table. A routing table can be statically built by a qualified LAN manager or dynamically built based on network conditions. A dynamic routing table is built and maintained by a **routing protocol**. A few examples of routing protocols are RIP (Routing Information Protocol), OSPF (Open Shortest Path First) and EGP (Exterior Gateway Protocol). Routing protocols allow the routers to adapt to changing conditions in the network without human intervention.

Exercise 5-1 LANs—Equipment and Topologies

Fill in the blanks

1. A ____________ is a physical layer type of LAN equipment.
2. Collision domains are segmented by a ___________.
3. A 10base5 LAN has a physical _________ topology and a logical ________ topology.
4. A _________ topology is highly reliable, but expensive to implement.
5. The ___________ layer of the 7-layer model is responsible for end-to-end control of data transfer.
6. A ___________ forwards broadcasts because it does not recognize the destination address.
7. A ___________________ protocol establishes a logical connection before information can be transferred.
8. The use of a layer two switch allows for ________ duplex operation of an Ethernet LAN.
9. Unshielded twisted pair has a lower maximum distance requirement than coaxial cable because of its higher ______________.
10. A ______________ protocol allows routers to dynamically respond to network changes.
11. A Packet is a PDU at the __________ layer which encapsulates a __________ working at the ____________ layer.
12. ___________ and ___________ ________ ______________ are equipment types that work at the data link layer.

5-4 TCP/IP (Transmission Control Protocol/Internet Protocol)

We will now take a look at a very common protocol stack. A protocol stack is a family of protocols. As the term stack indicates, a protocol stack is a multi-layer model. A very common protocol stack in use today is TCP/IP. It is common because it is the protocol of the **Internet**. TCP/IP is an evolving network protocol with core components capable of networking heterogeneous hosts. The following is a brief list of TCP/IP attributes.

- ✓ Capable of operation on different vendor platforms (computers)
- ✓ Major applications allow for e-mail, remote login and file transfers
- ✓ Two distinct Transport layer mechanisms—connection-oriented (TCP) and connectionless (UDP)
- ✓ IP addressing scheme allows for relatively simple connection of different networks
- ✓ Capable of operating with a variety of data link level protocols over different media types

Refer to Figure 5.8. In order to understand TCP/IP, we will first relate it to the OSI 7-layer reference model. You will notice that TCP/IP specific protocols are relevant to the Network, Transport and Application layers of the TCP/IP protocol stack. The concept of layering allows for many different types of Physical and Data Link layer protocols to support TCP/IP.

Since this section is a general overview of TCP/IP, Figure 5.8 shows only a few of the TCP/IP applications. The applications shown in the protocol stack will be considered later in this section.

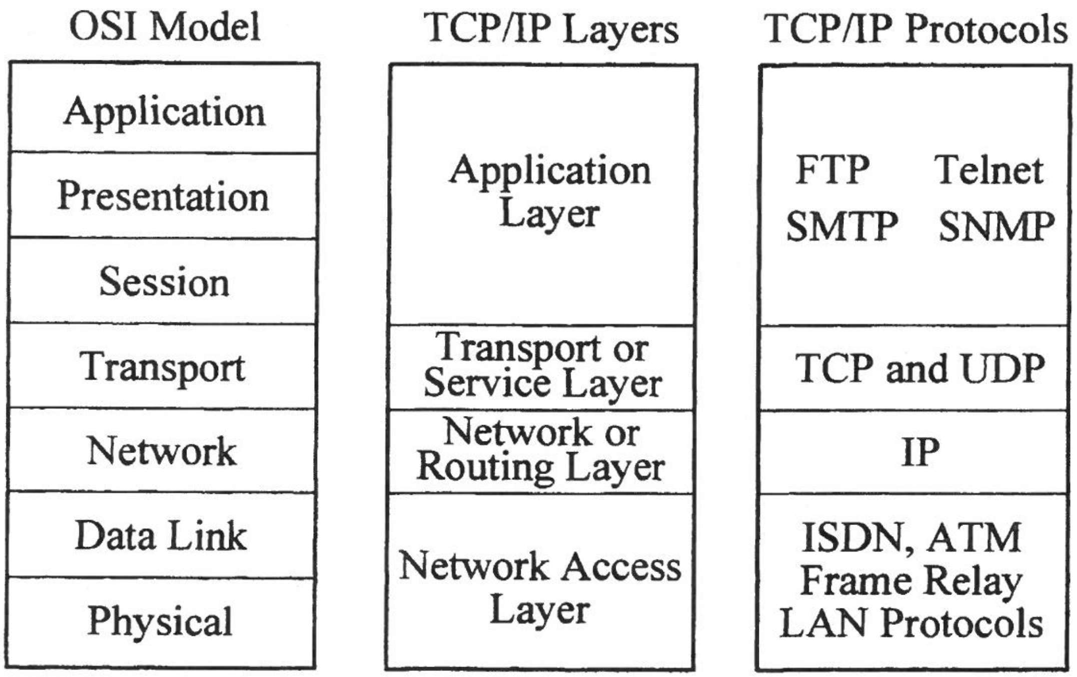

Figure 5.8 TCP/IP Protocol Stack and Protocols

5-4.2 Internet Protocol (IP)

We have already considered some of the protocols at the Network Access Layer (OSI Model Physical and Data Link layers). We will take a closer look at ISDN, ATM and Frame Relay in the next unit (unit 6). We will now take a look at Internet Protocol (IP).

The purpose of IP is to transport information across a network. It is a **connectionless, routed** protocol. The most common version of IP in use today is IP version 4 (IPv4). It uses a **32 bit** (4 octets) addressing scheme, identifying the network and host (node). We often see these addresses in what is called dotted decimal format—212.042.118.078. The dots (periods) separate the 4 octets, making them easier to read. There is a version 6 (IPv6), which uses a **128 bit** addressing scheme, but we will only consider IPv4.

Refer to Figure 5.9. Let's take a look at an Ethernet frame encapsulating an IP packet (datagram). You will recall that the minimum Ethernet frame is 64 octets, due to the minimum round trip time. As illustrated, this consists of at least 46 octets of payload and 18 octets of overhead. The Ethernet type field, in this case, will show that the payload is IP. The IP header is part of the payload containing the following information:

- ✓ IP version
- ✓ Length of header (default is 20 octets) and information
- ✓ Protocol of next layer (Transport layer)
- ✓ Control information
- ✓ Header error detection
- ✓ Source and destination network addresses

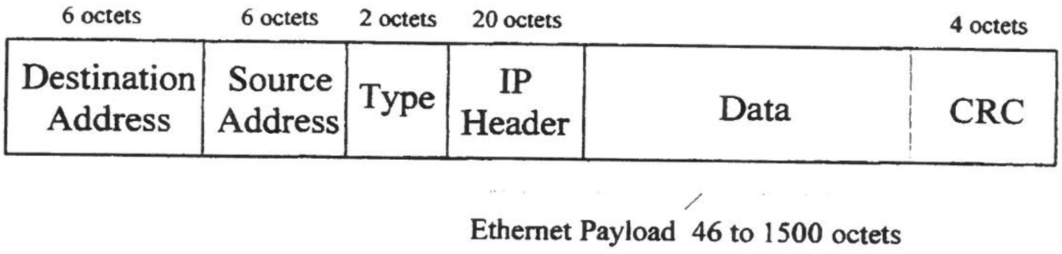

Figure 5.9 Ethernet Frame Encapsulating an IP Datagram

5-4.3 Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

TCP/IP has two different Transport level protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is a **connection-oriented** protocol, providing **retransmissions** and reliable data transfer. TCP manages data that is handed down to it from the application layer. Through a series of messages, TCP establishes and maintains a reliable end-to-end path for information transfer between applications. TCP maintains a reliable connection by requiring an acknowledgement for each **segment** sent. While this acknowledgement scheme allows for reliable transmission, it also increases end-to-end delay.

As data rates continue to increase, the TCP acknowledgement scheme becomes **delay limited**. This means that no matter how fast the transport rate is, the amount of end-to-end delay in a network reduces the effective data rate due to the need to wait for an acknowledgement before sending another segment of information.

UDP is a connectionless protocol. It **does not provide retransmissions** or guarantee reliable data transfer. It also **does not require an acknowledgement** for information sent. Due to its connectionless nature and lower overhead (8 octets) UDP is often used by custom programs for specific purposes. An example of a use for UDP is IP Telephony. Since IP Telephony is a real-time application, low delay is more important than reliable transport.

The use of these two different protocols at the Transport layer allows TCP/IP to have a high level of flexibility. The higher overhead (at least 20 octets) of TCP allows for reliable transport of data, while the lower overhead and connectionless nature of UDP allows for real-time and low priority applications. **TCP and UDP segments are encapsulated**, as shown in Figure 5.10, **in IP packets**. The following is some of the information in a TCP header:

- ✓ Source and destination application processes (referred to as "ports")
- ✓ Sequence and acknowledgement numbers
- ✓ Protocol of next layer (Transport layer)
- ✓ Control information
- ✓ Header error detection

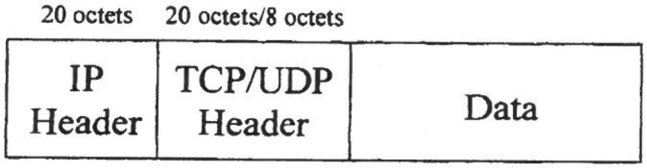

Figure 5.10 A TCP Segment in an IP Packet

Now that we have had a brief introduction to TCP/IP, let's take a look at some of the associated applications.

5-4.4 TCP/IP Applications

There are many applications associated with TCP/IP. There are applications for mapping IP addresses to MAC layer addresses—Address Resolution Protocol (ARP), mapping names (j.doe@somewhere.com) to IP addresses (192.183.140.213)—Domain Name System (DNS) and many others. We will take a look at some common, end-user applications. The first three applications considered are referred to as client/server applications.

A client/server application is based on a client, which invokes a process, and a server which provides a service in response to a client's request. The three client/server applications we will consider are FTP, Telnet and SMTP.

FTP (File Transfer Protocol)

FTP is an application that **allows a user on one system to log on to another system and issue basic commands** that are native to that other system. It will allow the remote user to change a directory, delete files and perform other functions that are supported by the other operating system. A common use for FTP is to copy files from one system to another.

Telnet

Telnet is an application that provides remote login capabilities. Telnet **allows a user on one system to log on to another system and run programs and manipulate data.** The user has the perception of being physically logged into the system.

SMTP (Simple Mail Transfer Protocol)

SMTP is an electronic mail (e-mail) application that enables users to exchange messages. It allows for sending, receiving, storing and mass mailing of messages among users.

SNMP (Simple Network Management Protocol)

The last TCP/IP application that we will consider is SNMP. As the name implies, SNMP is a simple protocol for network management. SNMP enables network managers to remotely monitor and control bridges, routers, end systems and other types of telecommunications equipment in a multi-vendor environment. Some of the management functional areas are the following:

- ✓ Fault management—detection of failures
- ✓ Configuration management—identify and modify equipment configuration
- ✓ Performance management—evaluate behavior of managed objects
- ✓ Security management—protect managed objects

5-5 The Internet

The Internet (capital "I") is the largest network of networks (internet with a small "i") in the world. It is made up of large national backbone networks and many regional and local networks world-wide. The origin of the Internet is considered to be ARPANet (Advanced Research Projects Agency Network), a worldwide network created in the 1960's that was maintained by the U.S. Department of Defense to facilitate communications between research facilities and universities.

The Internet uses the TCP/IP protocol stack. Since we have briefly considered TCP/IP, the focus of this section will be addressing the terminology (and TCP/IP protocols) associated with the Internet.

Anyone who has accessed the Internet is familiar with the World Wide Web. It is a collection of electronic documents loosely connected by a concept called "hypertext" by which documents connect to each other through clickable "hyperlinks." In order to access the Web, you need to run a browser program (example: Netscape Navigator).

Let's consider some of the terms associated with accessing and using the Internet.

ISP (Internet Service Provider)
An ISP is a company that provides direct access to the Internet.

URL (Uniform Resource Locator)
The URL describes the location and access method of a resource on the Internet. This is also known as the "Web site address."

Browser
An application that displays a Web page. Also known as a Web browser.

HTML (Hypertext Markup Language)
The standard for adding tags to a text file, allowing the file to be interpreted by a Web browser.

HTTP (Hypertext Transfer Protocol)
The Internet protocol that the Web uses to send information to the client, so the client browser can view Web pages.

Search Engine
A search engine is a utility that locates resources via searches for keywords and phrases.

Firewall
A firewall is software or hardware that limits certain kinds of access to a computer from a network or other outside source.

MIME (Multipurpose Internet Mail Extension)
MIME types are extensions to files that inform your computer as to what kind of program is needed to view the file.

Cookie
A set of data that a web site server gives to a browser the first time that the user visits the site. It is then updated with each return visit.

5-5.2 Accessing the Internet

We have defined an ISP as a company that provides direct access to the Internet. How do we access the ISP? In the past, we mostly used dial-up modems. These are still in use today, but running at faster speeds than we were originally using. In the old days of text-based downloads, 9600 bps was considered very fast. The fastest dial-up access modems in use today run at up to 56 kbps (actually up to approx. 52 Kbps, depending on line conditions). Because of the widespread use of graphics on the Internet, this is considered by many to be too slow.

Over the past few years, many high-speed options for access have been developed. We will take a quick look at some of them.

Dial-up Modems
Some common dial-up modem speeds are 14.4 Kbps, 19.2 Kbps, 28.8 Kbps and the previously mentioned 56 Kbps. Although these modem speeds do not seem as fast as they once were, the advantage of a dial-up modem is that you can keep your access costs low by using your existing phone line.

Cable Modems
Cable modems provide full time access to the Internet via your local cable TV provider. Connection speeds can run around 400 Kbps and up. A cable modem and NIC is required for access. This uses a technique that shares access bandwidth among users.

Direct Satellite Access
Satellite access allows for about 400 Kbps on the downlink (towards the user) and a lower rate, via the phone line, from the user.

ISDN (Integrated Services Digital Network)
ISDN can provide access at around 128 Kbps (BRI) and up to 1.5 Mbps (PRI). We will consider ISDN in the next unit.

ADSL (Asymmetrical Digital Subscriber Line)
ADSL can provide access speeds from 128 Kbps up to multi-megabits in the downstream direction (towards the user). This is a service carried over your phone line, so distance to the central office will determine the access rate. We will consider this technology in the next unit.

That was a brief overview of some of the most popular access techniques. Wireless access techniques are gradually increasing in speed. The third generation wireless networks will provide speeds from 144 Kbps up to 2 Mbps. This type of access will also increase user mobility.

Exercise 5-2 TCP/IP and the Internet

Fill in the blanks

1. TCP/IP is a ______ layer protocol stack.
2. In the TCP/IP protocol stack, _______ and _______ are connectionless protocols.
3. Both TCP and IP provide _____________ ______________ for their header fields.
4. IPv4 uses ________ bits for node addresses.
5. _______ is used for reliable transport of information and ________ is used for real-time applications.
6. A protocol that allows a user to remotely access files on another system is ________.
7. The function of mapping a host IP address to a MAC level address is performed by _______.
8. A protocol that allows a user to send information in a format that can be read by a browser is called _________.
9. Another name for a Web site address is a ________.
10. The speed of access using ADSL is a function of ____________.

Unit 5 Summary

- ✓ The OSI 7-layer model defines different functions for each level.
- ✓ As information moves down the protocol stack, overhead is added. This concept is called encapsulation.
- ✓ The PDU at each level in the 7-layer model has a unique name.
- ✓ A physical topology shows how equipment is placed in a network.
- ✓ A logical topology shows how information flows in a network.
- ✓ Connection-oriented protocols establish a logical end-to-end connection before transporting information.
- ✓ Modern LANs are typically laid out in a physical star topology for ease of implementation and maintenance.
- ✓ Early Ethernet implementations used a bus topology (physical and logical), sharing the medium by using a random access technique called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
- ✓ Ethernet collision domains are separated by bridges and layer two switches. This is referred to as segmentation.
- ✓ Layer two switches allow Ethernet users to have full-duplex access.
- ✓ Routers work at layer 3 of the OSI 7-layer model and do not forward broadcast traffic.
- ✓ Routing protocols allow routers to dynamically respond to changing network conditions.
- ✓ TCP/IP is a four-layer protocol stack used by the Internet.
- ✓ IP is a connectionless network layer protocol used for carrying packets across a network.
- ✓ TCP is a connection-oriented transport layer protocol that is encapsulated by IP.
- ✓ UDP is a connectionless transport layer protocol.
- ✓ FTP, Telnet and SMTP are client/server examples of TCP/IP applications.
- ✓ SNMP is a TCP/IP application used for network management.
- ✓ The Internet can be accessed via an ISP, using dial-up or dedicated techniques.

The purpose of this unit is to provide a general understanding of the subject areas addressed. For more information on the topics covered in this unit, refer to the Web sites and reference books listed in the **Study Guide for the Digital Communications and Computer Literacy Test.**

Answers to Exercises

Exercise 5-1 LANs—Equipment and Topologies

1. A _repeater_ is a physical layer type of LAN equipment.
2. Collision domains are segmented by a _bridges_.
3. A 10base5 LAN has a physical _bus_ topology and a logical _bus_ topology.
4. A _mesh_ topology is highly reliable, but expensive to implement.
5. The _transport_ layer of the 7-layer model is responsible for end-to-end control of data transfer.
6. A _bridge_ forwards broadcasts because it does not recognize the destination address.
7. A _connection-oriented_ protocol establishes a logical connection before information can be transferred.
8. The use of a layer two switch allows for _full_ duplex operation of an Ethernet LAN.
9. Unshielded twisted pair has a lower maximum distance requirement than coaxial cable because of its higher _attenuation_.
10. A _routing_ protocol allows routers to dynamically respond to network changes.
11. A Packet is a PDU at the _network_ layer which encapsulates a _segment_ working at the _transport_ layer.
12. _Bridges_ and _Layer_ _two_ _switches_ are equipment types that work at the data link layer.

Exercise 5-2 TCP/IP and the Internet

1. TCP/IP is a _4_ layer protocol stack.
2. In the TCP/IP protocol stack, _IP_ and _UDP_ are connectionless protocols.
3. Both TCP and IP provide _error_ _detection_ for their header fields.
4. IPv4 uses _32_ bits for node addresses.
5. _TCP_ is used for reliable transport of information and _UDP_ is used for real-time applications.
6. A protocol that allows a user to remotely access files on another system is _FTP_.
7. The function of mapping a host IP address to a MAC level address is performed by _ARP_.
8. A protocol that allows a user to send information in a format that can be read by a browser is called _HTTP_.
9. Another name for a Web site address is a _URL_.
10. The speed of access using ADSL is a function of _distance_.