1.2 BUILDING NETWORK AND ITS TYPES

Local Area Network

A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus as shown in figure 1.2.1. Depending on the needs of an organization, a LAN can be as simple as two PCs and a printer in someone's home office, or it can extend throughout a company and include audio and video devices.

Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and the destination host's addresses.

Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts. The switch manage the traffic in the LAN and allows more than one pair to communicate with each other at the same time if there is no common source and destination among them.

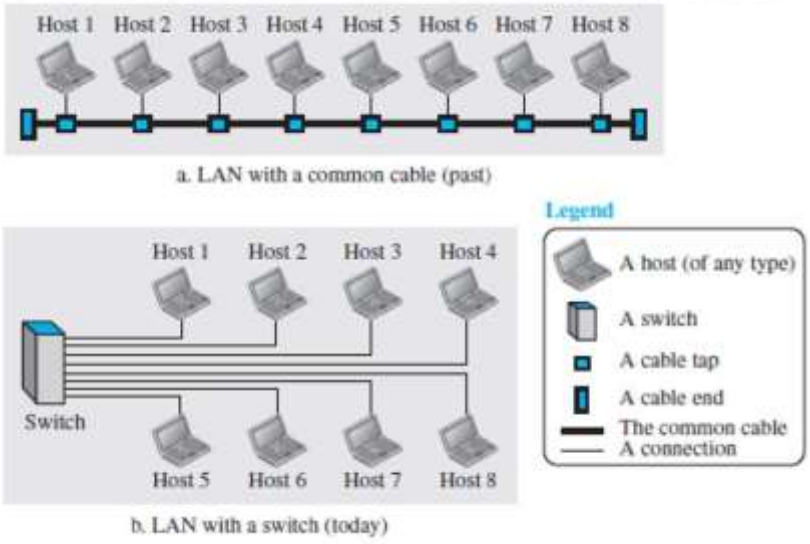

Fig1.2.1: LAN connections.

[Source :" Data Communications and Networking" by Behrouz A. Forouzan,Page-13]

Wide Area Network

A wide area network (WAN) is interconnection of devices capable of communication. There are some differences between a LAN and a WAN. A LAN is normally limited in size, spanning an office, a building, or a campus; A WAN has a wider geographical span, spanning a town, a state, a country, or even the world.

A LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems. A LAN is normally privately owned by the organization that uses it; a WAN is normally created and run by communication companies and leased by an organization that uses it.

Point-to-Point WAN

A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air) as in figure 1.2.2 .

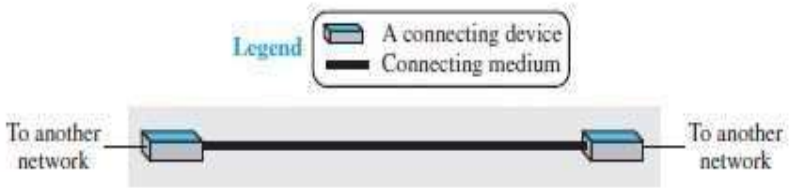

Fig1.2.2: Point-to-point WAN.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-14]

Switched WAN

A switched WAN is a network with more than two ends. We can say that a switched WAN is a combination of several point-to-point WANs that are connected by switches.

Figure 1.2.3 shows an example of a switched WAN.

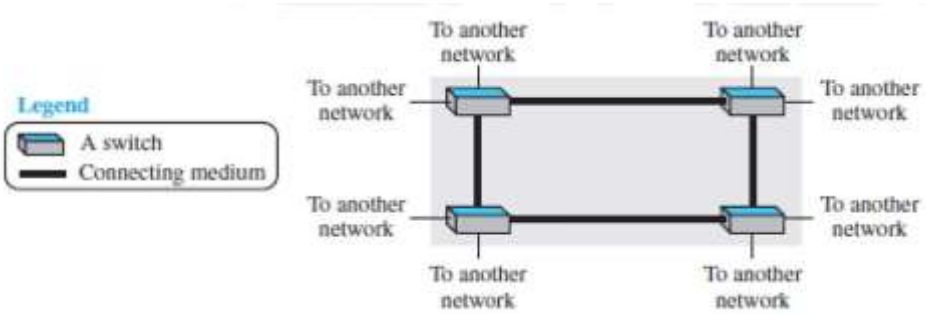

Fig1.2.3: Switched WAN.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-14]

Internetwork

When two or more networks are connected, they make an internetwork, or internet.

As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. Each office has a LAN that allows all employees inthe office to communicate with each other.

Switching

An internet is a switched network in which a switch connects at least two links together. A switch needs to forward data from a network to another network when required.The two most common types of switched networks are circuit-switched and packet-switched networks.

Circuit-Switched Network

In a circuit-switched network, a dedicated connection, called a circuit, is always available between the two end systems (or between two computers) ; the switch can only make it active or inactive. Figure 1.2.4 shows a very simple switched network that connects four telephones to each end.

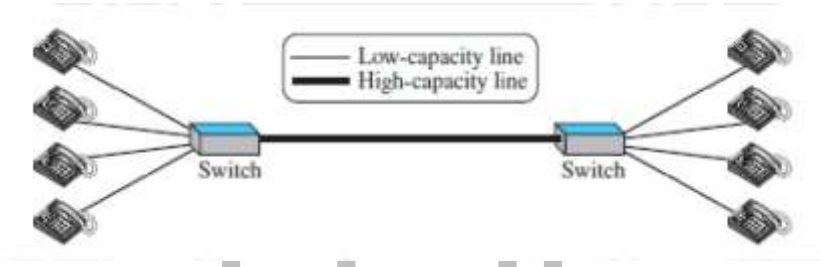

Fig1.2.4: Circuit-switched network.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-16]

The four telephones at each side are connected to a switch. The switch connects a telephone set at one side to a telephone set at the other side.The thick line connecting two switches is a high-capacity communication line that can handle four voice communications at the same time; the capacity can be shared between all pairs of telephone sets.

Packet-Switched Network

In a network as in figure 1.2.5, the communication between the two ends is done in blocks of data called packets. Instead of the continuous communication between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers. This allows us to make the switches function for both storing and forwarding because a packet is an independent entity that can be stored and sent later.A router in a packet-switched network has a queue that can store and forward the packet.

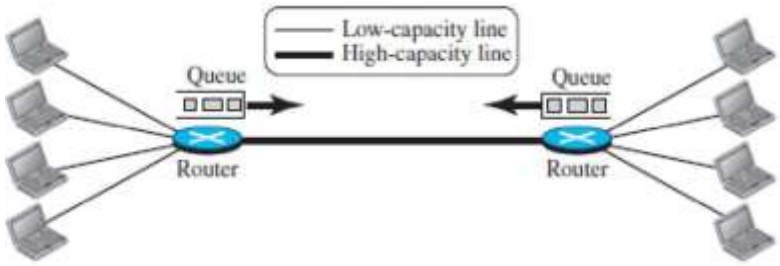

Fig1.2.5: Packet-Switched Network.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-17]

Overview of Internet

An internet (lowercase *i*) is two or more networks that can communicate with each other. The most notable internet is called the Internet(uppercase I), and is composed of thousands of interconnected networks.

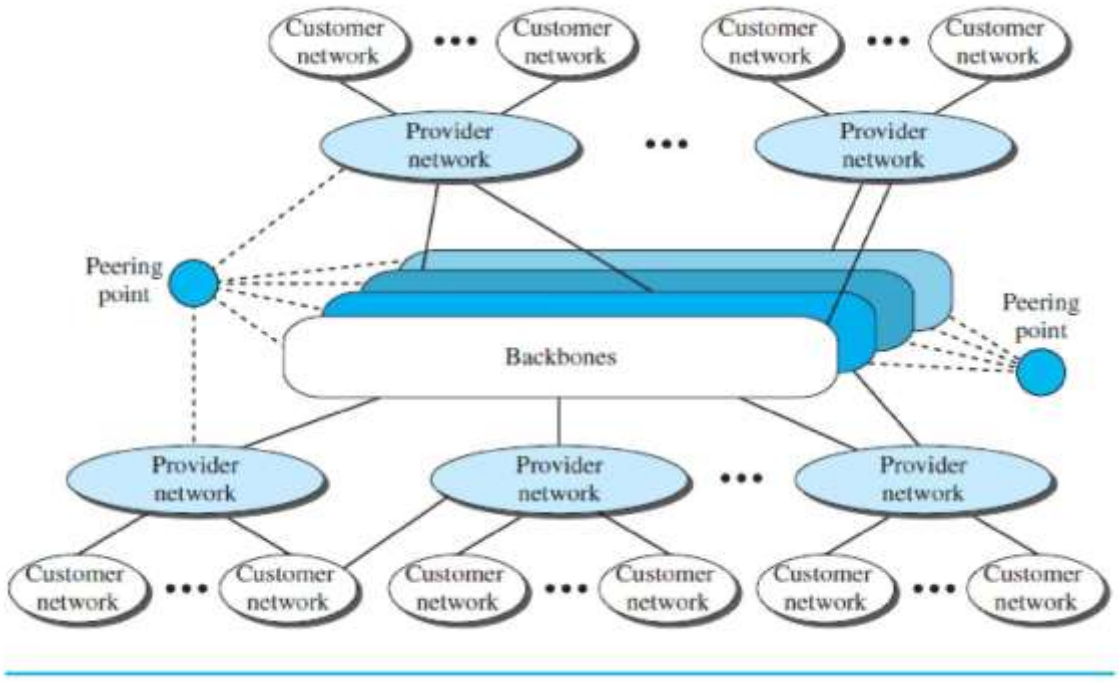

Fig1.2.6: Internet.

[*Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-18]*

The figure1.2.6, shows the Internet as several backbones, provider networks, and customer networks.

At the top level, the backbones are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT. The backbone networks are connected through some complex switching systems, called peering points.

At the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee.The provider networks are connected to backbones and sometimes to other provider networks.

The customer networks are networks at the edge of the Internet that actually use the services provided by the Internet.

Accessing the Internet

The Internet today is an internetwork that allows any user to become part of it. The user, however, needs to be physically connected to an ISP. The physical connection is done through a point-to-point WAN.

Using Telephone Networks

Since most telephone networks have already connected themselves to the Internet, one option for residences and small businesses to connect to the Internet is to change the voice line between the residence or business and the telephone center to a point-to-point WAN. This can be done in two ways.

Dial-up service. The first solution is to add to the telephone line a modem that converts data to voice. The software installed on the computer dials the ISP and imitates making a telephone connection.

DSL Service

The DSL service allows the line to be used simultaneously for voice and data communication.

Using Cable Networks

The cable companies have been upgrading their cable networks and connecting to the Internet.

Using Wireless Networks

A household or a small business can use a combination of wireless and wired connections to access the Internet. Small business centres can be connected to the Internet through a wireless WAN.

For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.

1.4 OVERVIEW OF DATA AND SIGNALS

Communication at application, transport, network, or data-link is logical; communication at the physical layer is physical.

Data need to be transmitted and received, but the media have to change data to signals. Both data and the signals that represent them can be either analog or digital in form.

Analog and Digital Data

Data can be analog or digital. The term analog data refers to information that is continuous; digital data refers to information that has discrete states.

For example, an analog clock that has hour, minute, and seconds gives information in a continuous form; the movements of the hands are continuous.

On the other hand, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06. Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal.

Digital data take on discrete values. For example, data are stored in computer memory in the form of 0s and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

Analog and Digital Signals

Like the data they represent, signals can be either analog or digital.

An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path. A digital signal, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0. The simplest way to show signals is by plotting them on a pair of perpendicular axes. The vertical axis represents the value or strength of a signal. The horizontal axis represents time.

Figure 1.4.1, illustrates an analog signal and a digital signal.

The curve representing the analog signal passes through an infinite number of points. The vertical lines of the digital signal, demonstrate the sudden jump that the signal makes from value to value.

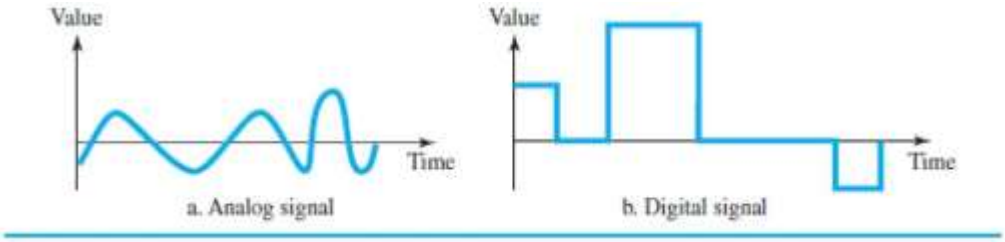

Fig1.4.1: Comparison of Analog and Digital Signal.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-55]

Periodic and Nonperiodic

Both analog and digital signals can take one of two forms: periodic or non periodic.

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle.

An example for periodic analog signal is the Sine wave as shown in figure 1.4.2.

A non periodic signal changes without exhibiting a pattern or cycle that repeats over time.

Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves.

The sine wave is the most fundamental form of a periodic analog signal. When we visualize it as a simple oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow. A sine wave can be represented by three parameters: the peak amplitude, the frequency,and the phase. These three parameters fully describe a sine wave.

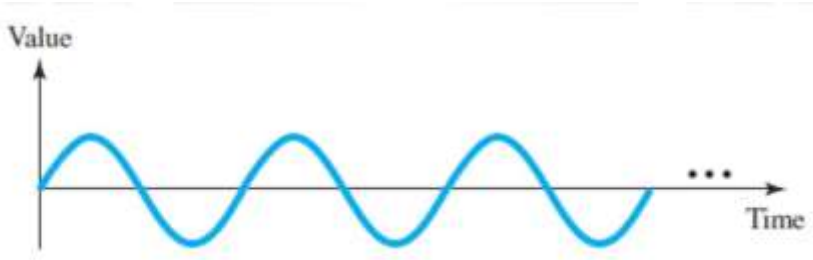

Fig1.4.2: Sine wave.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-56]

1.8 ERROR DETECTION AND CORRECTION

Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal. The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1 as shown in figure 1.8.1. The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

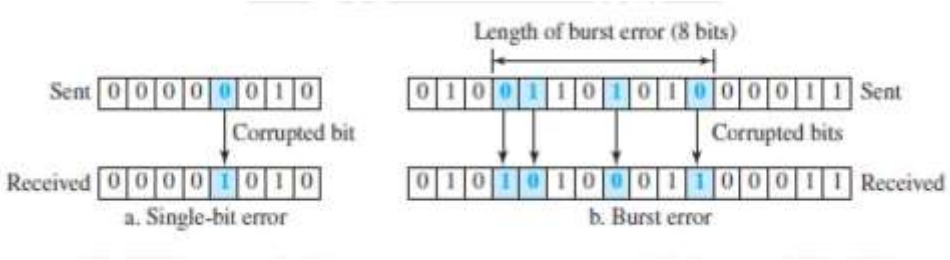

Fig1.8.1: Effect of a single-bit and a burst error on a data unit.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-258]

Redundancy

The central concept in detecting or correcting errors is redundancy. To detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.

Detection versus Correction

The correction of errors is more difficult than the detection. In error detection, if any error has occurred. A single-bit error is the same for us as a burst error. In error correction, we need to know the exact number of bits that are corrupted and, their location in the message.

Coding

Redundancy is achieved through various coding schemes. The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits.The receiver checks the relationships between the two sets of bits to detect errors.

Linear Block Codes

Almost all block codes used today belong to a subset of block codes called linear block codes.

Minimum Distance for Linear Block Codes

It is simple to find the minimum Hamming distance for a linear block code. The minimum hamming distance is the number of 1s in the nonzero valid codeword with the smallest number of 1s.

Parity-Check Code

The most familiar error-detecting code is the parity-check code. This code is a linear block code. In this code, a k-bit dataword is changed to an n-bit codeword where n = k + 1. The extra bit, called the parity bit, is selected to make the total number of 1s in the codeword even as shown in figure1.8.2 . Some implementations specify an odd number of 1s.The minimum Hamming distance for this category is dmin = 2, which means that the code is a single-bit error-detecting code.

The code in Table (below) is a parity-check code with k = 4 and n = 5.

Dataword	*Codeword*	*Dataword*	*Codeword*
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100
0011	00110	1011	10111
0100	01001	1100	11000
0101	01010	1101	11011
0110	01100	1110	11101
0111	01111	1111	11110

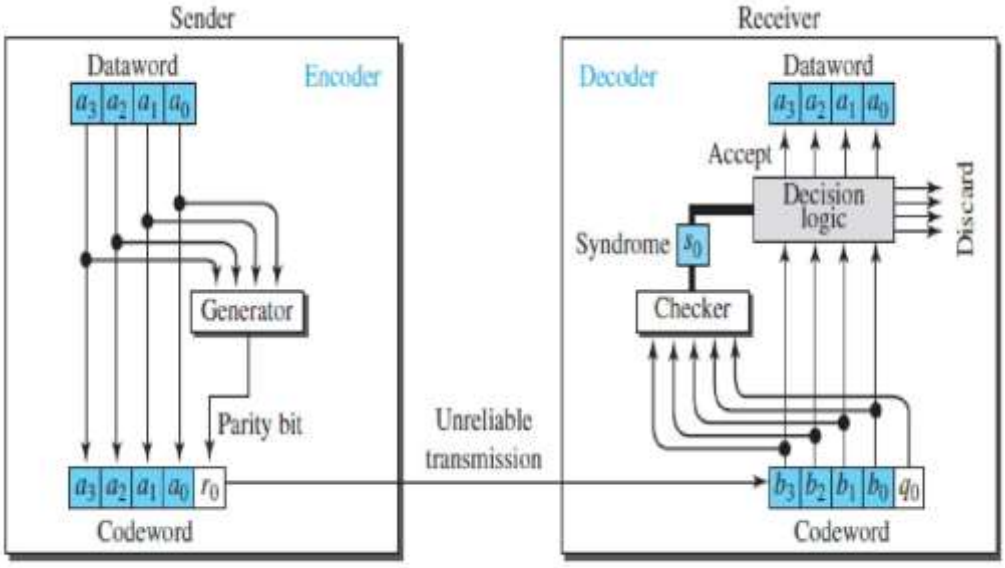

Fig1.8.2: Encoder and decoder for simple parity-check code

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-263]

The calculation is done in modular arithmetic . The encoder uses a generator that takes a copy of a 4-bit dataword (*a*0, *a*1, *a*2, and *a*3) and generates a parity bit r0. The dataword bits and the parity bit create the 5-bit codeword.

The parity bit that is added makes the number of 1s in the codeword even. This is normally done by adding the 4 bits of the dataword (modulo-2); the result is the parity bit. In otherwords, r0 =a3+a2+a1+a0 (modulo-2)

If the number of 1s is even, the result is 0; if the number of 1s is odd, the result is 1.

In both cases, the total number of 1s in the codeword is even. The sender sends the codeword, which may be corrupted during transmission. The receiver receives a 5-bit word.The checker at the receiver does the same thing as the generator in the sender with one exception: The addition is done over all 5 bits. The result is called the syndrome, is just 1 bit. The syndrome is 0 when the number of 1s in the received codeword is even; otherwise, it is 1. s0 = b3 + b2 + b1+ b0 + q0 (modulo-2)

The syndrome is passed to the decision logic analyzer.

If the syndrome is 0, there is no detectable error in the received codeword; the data portion of the received codeword is accepted as the dataword; **if the syndrome is 1**, the data portion of the received codeword is discarded. The dataword is not created.

CYCLIC CODES

Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.

For example,if 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword. In this case, if we call the bits in the first word *a*0 to *a*6, and the bits in the second word*b*0 to *b*6, we can shift the bits by using the following: *b*1=*a*0*b*2=*a*1*b*3 =*a*2*b*4=*a*3*b*5=*a*4*b*6=*a*5*b*0=*a*6

Cyclic Redundancy Check

The **cyclic redundancy check (CRC)**, is used in networks such as LANs and WANs.

In the encoder, the dataword has *k* bits (4 here); the codeword has *n* bits (7 here).

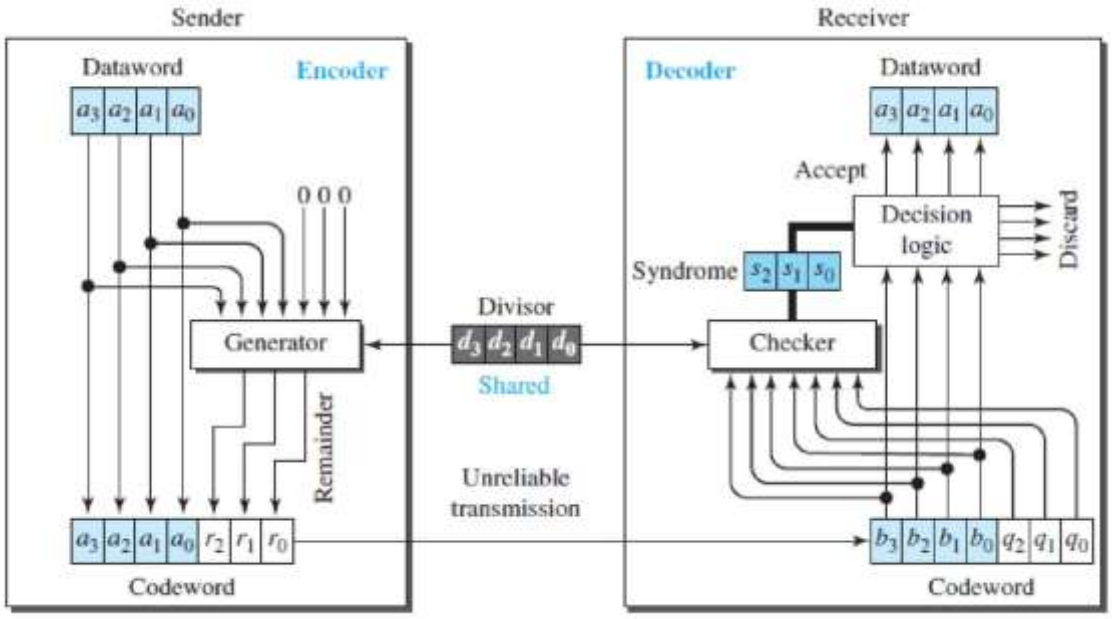

Fig1.8.3: CRC encoder and decoder.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-265]

The size of the dataword is augmented by adding n -k (3 here) 0s to the right-hand sideof the word. The n-bit result is fed into the generator. The generator uses a divisor of size n -k (4 here), predefined and agreed upon. The generator divides the augmented dataword by the divisor (modulo-2 division).

The quotient of the division is discarded;the remainder (r2r1r0) is appended to the data word to create the codeword.The decoder receives the codeword (possibly corrupted in transition). A copy of all n bits is fed to the checker, which is a replica of the generator.

The remainder produced by the checker is a syndrome of n-k (3 here) bits, which is fed to the decision logic analyzer.The analyzer has a simple function. If the syndrome bits are all 0s, the 4 leftmost bits of the codeword are accepted as the dataword (interpreted as no error); otherwise,the 4 bits are discarded (error).

Encoder

The encoder shown in figure 1.8.4, takes a dataword and augments it with n-k number of 0s.

It then divides the augmented dataword by the divisor.

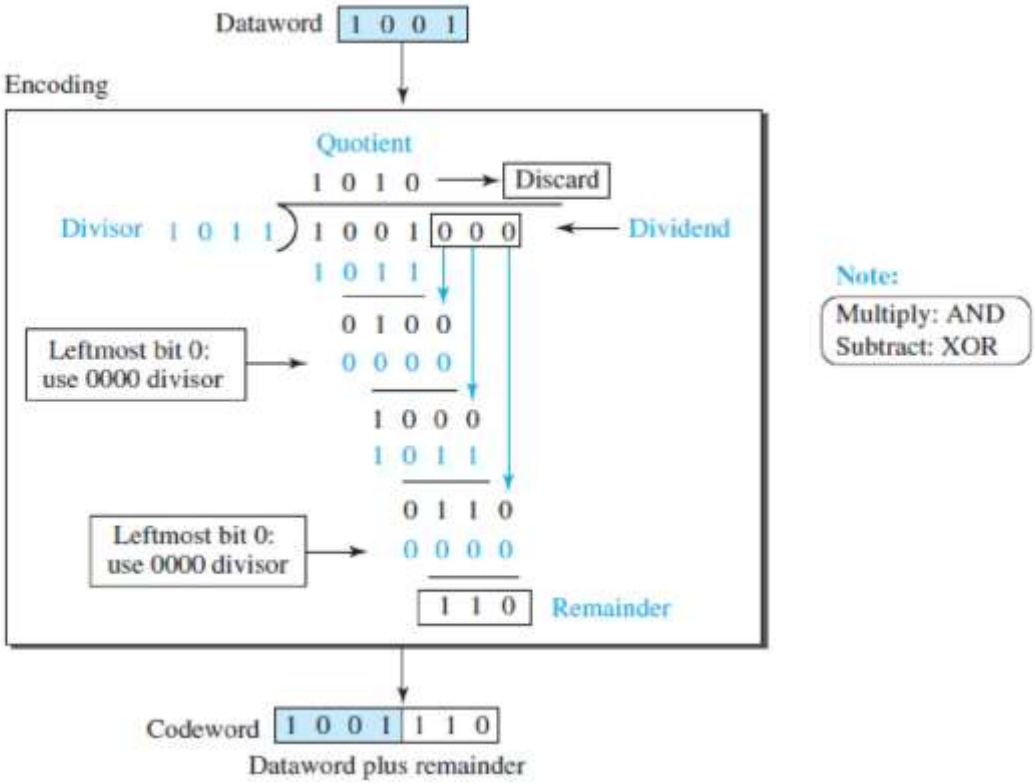

Fig1.8.4: Division in CRC encoder.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-266]

As in decimal division, the process is done step by step. In each step, a copy of the divisor is XOR ed with the 4 bits of the dividend. The result of the XOR operation(remainder) is 3 bits (in this case), which is used for the next step after 1 extra bit is pulled down to make it 4 bits long. There is one important point we need to remember in this type of division.

If the leftmost bit of the dividend (or the part used in each step)is 0, the step cannot use the regular divisor; we need to use an all-0s divisor.When there are no bits left to pull down, we have a result. The 3-bit remainder forms the check bits (r2, r1, and r0). They are appended to the dataword to create the codeword.

Decoder

The codeword can change during transmission. The decoder does the same division process as the encoder. The remainder of the division is the syndrome. If the syndrome is all 0s, there is no error with a high probability; the dataword is separated from the received codeword and accepted. Otherwise, everything is discarded.

Figure 1.8.5 shows two cases: The left-hand figure shows the value of the syndrome when no error has occurred; the syndrome is 000. The right-hand figure shows the case in which there is a single error. The syndrome is not all 0s (it is 011).

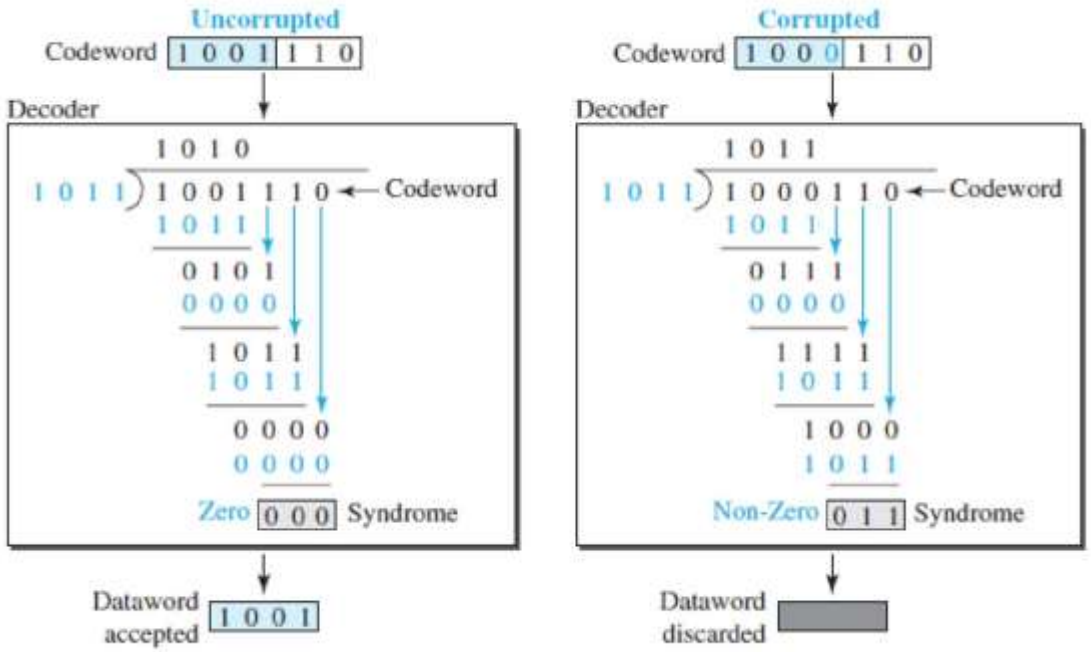

Fig1.8.5: Division in decoder.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-267]

CHECKSUM

Checksum is an error-detecting technique that can be applied to a message of any length.

At the source, the message is first divided into m-bit units as in figure 1.8.6. The generator then creates an extra m-bit unit called the checksum, which is sent with the message.

At the destination, the checker creates a new checksum from the combination of the message and sent checksum.

If the new checksum is all 0s, the message is accepted; otherwise,the message is discarded. In the real implementation, the checksum unit is not necessarily added at the end of the message; it can be inserted in the middle of the message.

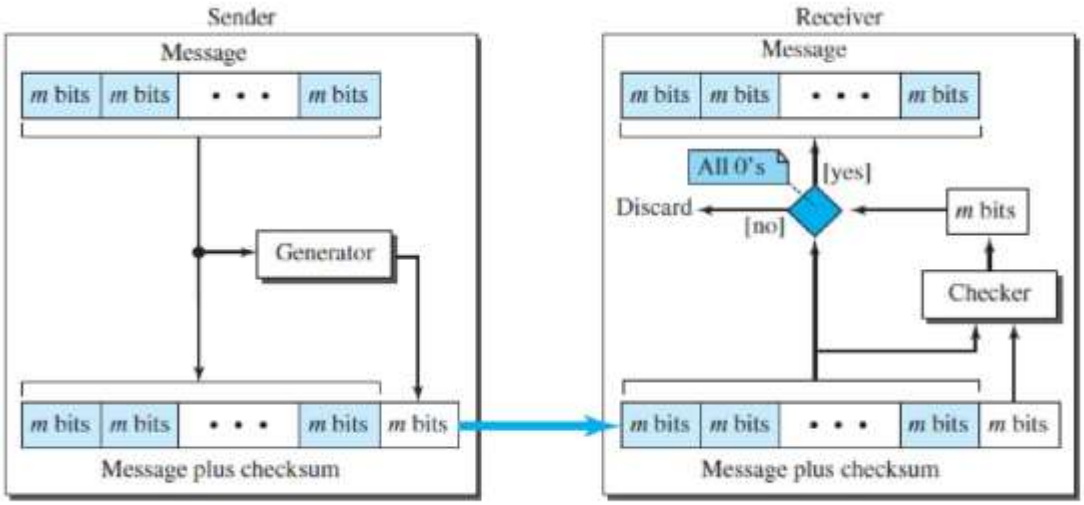

Fig1.8.6:Checksum.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-278]

Concept

The idea of the traditional checksum is simple.

Example

Suppose the message is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers. For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12, 0, 6, 36), where 36 is the sum of the original numbers.

The receiver adds the five numbers and compares the result with the sum. If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise ,there is an error somewhere and the message is not accepted.

One's Complement Addition

The previous example has one major drawback. Each number can be written as a 4-bitword (each is less than 15) except for the sum.

One solution is to use one's complement arithmetic. In this arithmetic, we can represent unsigned numbers between 0and 2m -1 using only m bits. If the number has more than m bits, the extra leftmost bits need to be added to the m rightmost bits (wrapping).

Example

In the previous example, the decimal number 36 in binary is (100100)2. To change it to a 4bit number we add the extra leftmost bit to the right four bits as shown below. Instead of sending 36 as the sum, we can send 6 as the sum (7, 11, 12, 0, 6, 6).

The receiver can add the first five numbers in one's complement arithmetic. If the result is 6, the numbers are accepted; otherwise, they are rejected.

We can make the job of the receiver easier if we send the complement of the sum, the **checksum**. In one's complement arithmetic, the complement of a number is found by completing all bits (changing all 1s to 0s and all 0s to 1s). This is the same as subtracting the number from 2^m -1.

In one's complement arithmetic, we have two 0s: one positive and one negative, which are complements of each other. The positive zero has all m bits set to 0; the negative zero has all bits set to 1 (it is 2m -1).

If we add a number with its complement, we get a negative zero (a number with all bits set to 1). When the receiver adds all five numbers (including the checksum), it gets a negative zero. The receiver can complement the result again to get a positive zero.

Example

The sender adds all five numbers in one's complement to get the sum 6. The sender then complements the result to get the checksum 9,which is 15 -6.

Note that 6 (0110)2 and 9 (1001)2; they are complements of each other.

The sender sends the five data numbers and the checksum (7, 11, 12, 0, 6, **9**). If there is no corruption in transmission, the receiver receives (7, 11, 12, 0, 6, **9**) and adds them in one's complement to get 15. The sender complements 15 to get 0. This shows that data have not been corrupted. Figure 1.8.7 shows the process.

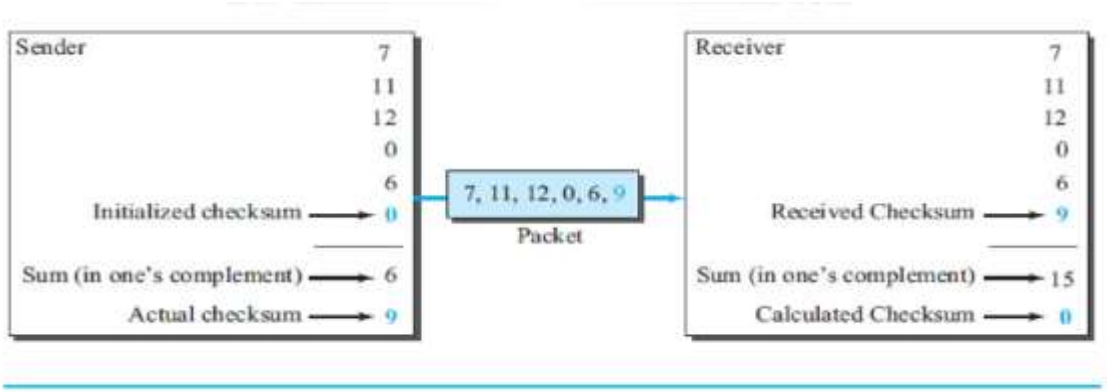

Fig1.8.7: Checksum Process.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-279]

6 .6 INTRODUCTION TO DATA-LINK LAYER

The Internet is a combination of networks combined together by connecting devices (routers or switches). If a packet is to travel from a host to another host, it needs to pass through these networks. Figure1.6.1 shows the scenario of Communication at the data-link layer .

Communication at the data-link layer is made up of five separate logical connections between the data-link layers in the path.

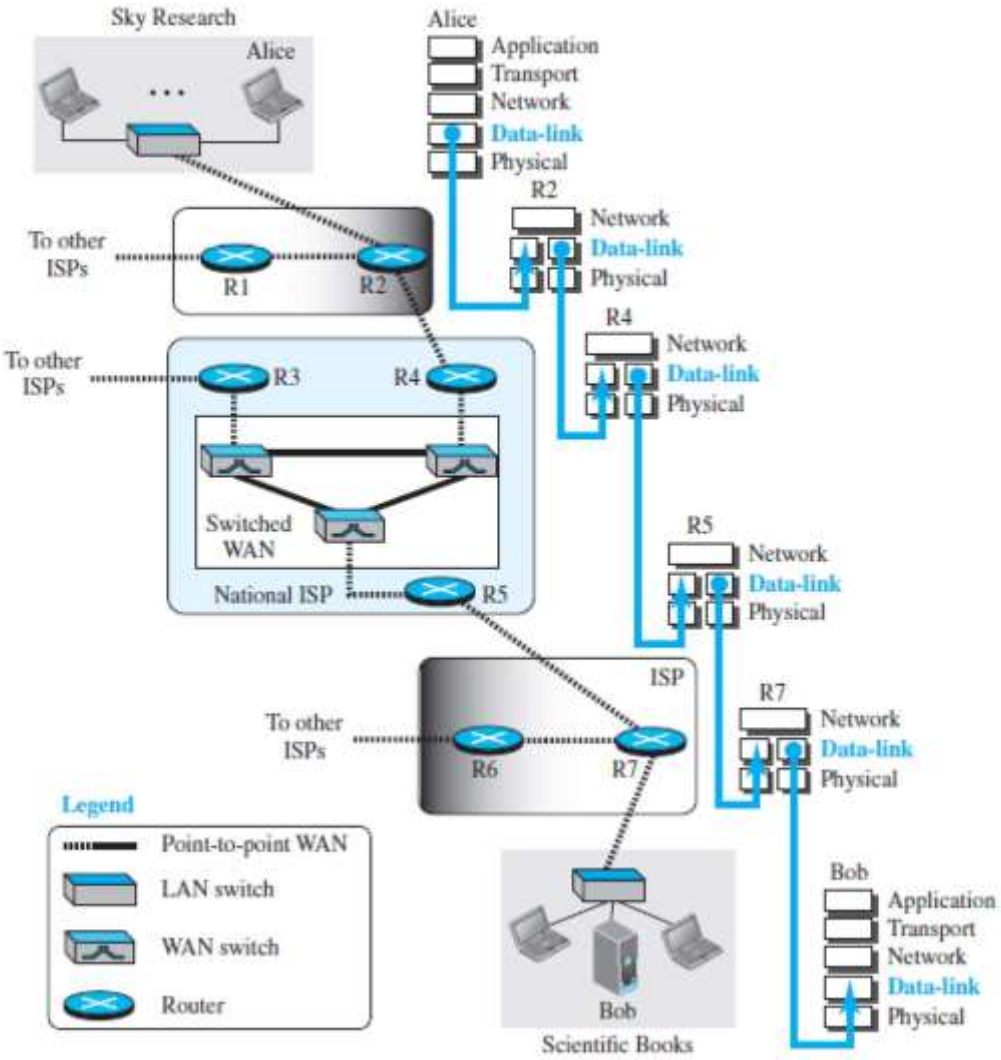

Fig1.6.1:Communication at the data-link layer.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-238]

The data-link layer at Alice's computer communicates with the data-link layer at routerR2.

The data-link layer at router R2 communicates with the data-link layer at router R4, and so on. Finally, the data-link layer at router R7 communicates with the data-link layer at Bob's computer. Only one data-link layer is involved at the source or the destination, but two data-link layers are involved at each router.The reason is that Alice's and Bob's computers are each connected to a single network, but each router takes input from one network and sends output to another network.

Nodes and Links

Communication at the data-link layer is node-to-node. A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point.Theses LANs and WANs are connected by routers. It is customary to refer to the two end hosts and the routers as nodes and the networks in between as links.

Figure 1.6.2 shows a simple representation of links and nodes when the path of the data unit is only six nodes.

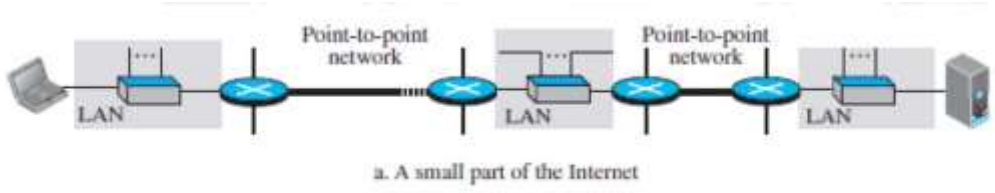

Fig1.6.2: Nodes and links.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-239]

The first node is the source host; the last node is the destination host. The other four nodes are four routers. The first, the third, and the fifth links represent the three LANs; the second and the fourth links represent the two WANs.

Services

The data-link layer is located between the physical and the network layers. The data link layer provides services to the network layer; it receives services from the physical layer.

Services provided by the data-link layer.

The duty scope of the data-link layer is node-to-node.

When a packet is travelling in the Internet, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path.

The data-link layer of the source host needs only to encapsulate, the data-link layer of the destination host needs to decapsulate, but each intermediate node needs to both encapsulate and decapsulate.

Assume a person needs to travel from her home to her friend's home in another city. The traveller can use three transportation tools. She can take a taxi to go to the train station in her own city, then travel on the train from her own city to the city where her friend lives, and finally reach her friend's home using another taxi. Here we have a source node, a destination node, and two intermediate nodes.

The traveller needs to get into the taxi at the source node, get out of the taxi and get into the train at the first intermediate node (train station in the city where she lives), get out of the train and get into another taxi at the second intermediate node (train station in the city where her friend lives), and finally get out of the taxi when she arrives at her destination.

A kind of encapsulation occurs at the source node, encapsulation and decapsulation occur atthe intermediate nodes, and decapsulation occurs at the destination node. Figure 1.6.3 shows the encapsulation and decapsulation at the data-link layer.

For simplicity, we have assumed that we have only one router between the source and destination.

The datagram received by the data-link layer of the source host is encapsulated in a frame.

The frame is logically transported from the source host to the router. The frame is decapsulated at the data-link layer of the router and encapsulated at another frame.

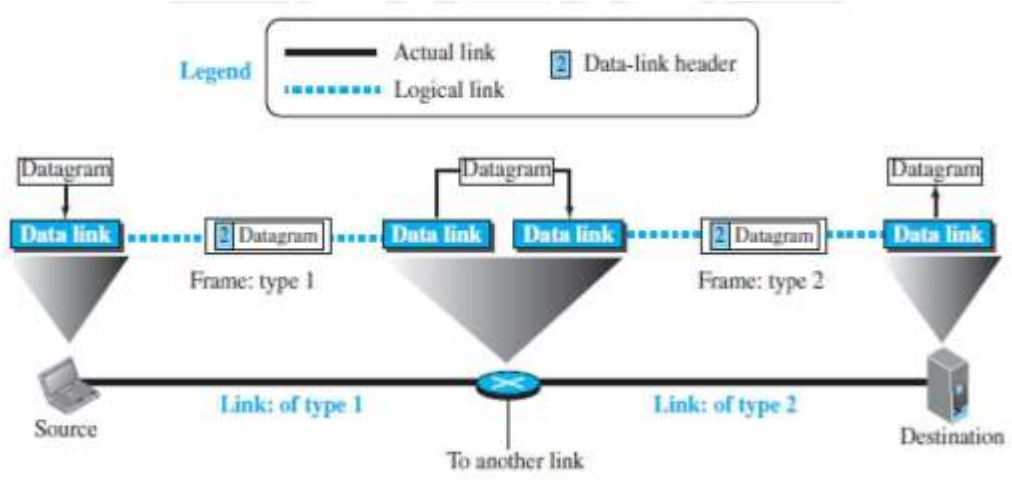

Fig1.6.3: Communication with three nodes.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-240]

Framing

The first service provided by the data-link layer is framing. The data-link layer at each node needs to encapsulate the datagram (packet received from the network layer) in a frame before sending it to the next node.

The node also needs to decapsulate the datagram from the frame received on the logical channel. A packet at the data-link layer is normally called a frame.

Flow Control

Whenever we have a producer and a consumer, we need to think about flow control. If the producer produces items that cannot be consumed, accumulation of items occurs. The sending data-link layer at the end of a link is a producer of frames; the receiving data-link layer at the other end of a link is a consumer.

If the rate of produced frames is higher than the rate of consumed frames, frames at the receiving end need to be buffered while waiting to be consumed (processed).

Error Control

At the sending node, a frame in a data-link layer needs to be changed to bits, transformed to electromagnetic signals, and transmitted through the transmission media.

At the receiving node, electromagnetic signals are received, transformed to bits, and put together to create a frame. Since electromagnetic signals are affected by error, a frame is also get affected by error.The error should be detected. After detection, it needs to be either corrected at the receiver node or discarded and retransmitted by the sending node.

Congestion Control

A link may be congested with frames, which may result in frame loss, most data-link-layer protocols do not directly use a congestion control to prevent congestion, although some wide-area networks do.

In general, congestion control is considered an issue in the network layer or the transport layer because of its end-to-end nature.

Two Categories of Links

1. Point-to-point link 2.Broadcast link.

   In a point-to-point link, the link is dedicated to the two devices; in a broadcast link, the link is shared between several pairs of devices.

The data-link layer has two sublayers:

Data link control (DLC) and media access control (MAC).

The data link control sub layer deals with all issues common to both point-to-point and broadcast links; the media access control sub layer deals only with issues specific to broadcast links.

1 **LINK-LAYER ADDRESSING**

A link-layer address is called a link address, called a physical address, and sometimes a MAC address. Since a link is controlled at the data-link layer, the addresses need to belong to the data-link layer.

When a datagram passes from the network layer to the data-link layer,the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header.These two addresses are changed every time the frame moves from one link to another.

Figure 1.7.1 shows, IP addresses and link-layer addresses in a small internet.

This is easy to understand.

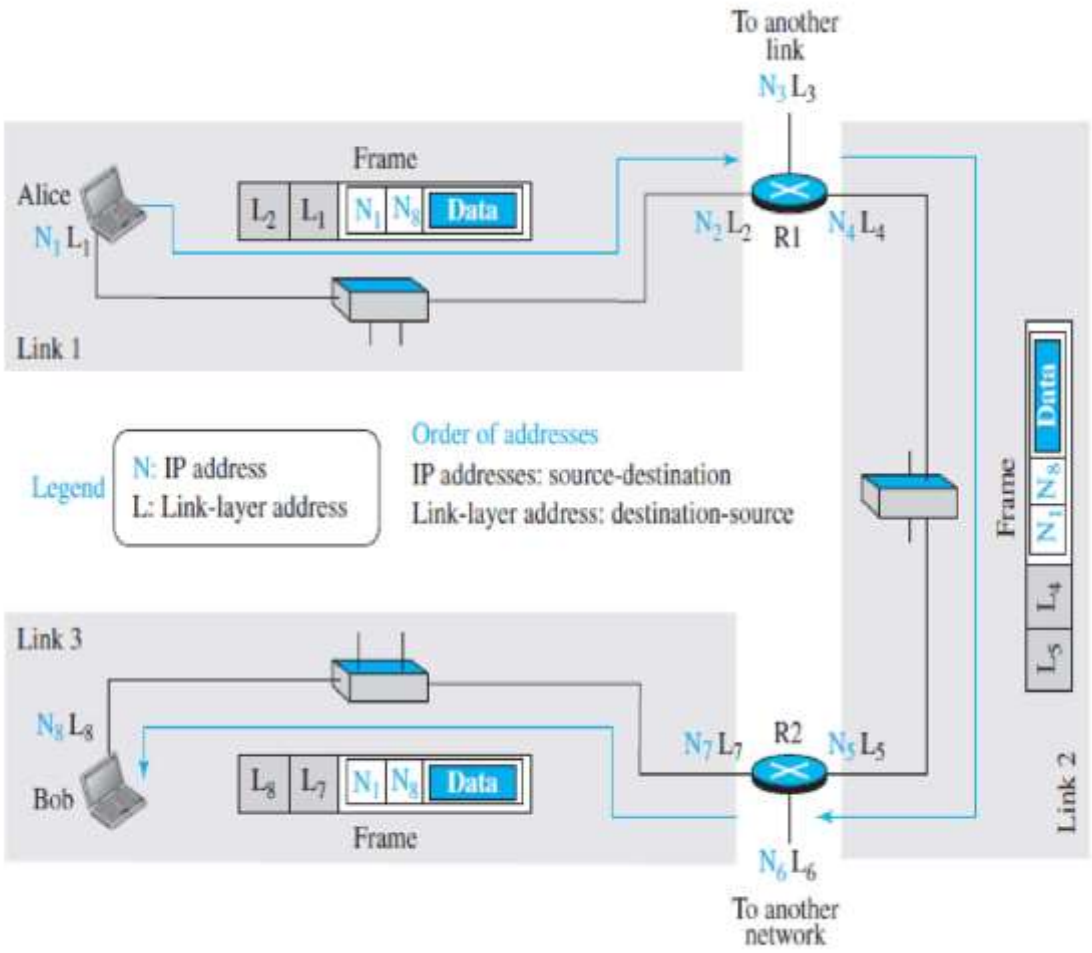

Fig1.7.1: IP addresses and link-layer addresses in a small internet.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-243]

Here we have three links and two routers. We have two hosts: Alice (source) and Bob (destination). For each host, we have shown two addresses, the IP addresses (N) and the link-layer addresses (L).

We have three frames, one in each link.Each frame carries the same datagram with the same source and destination addresses (N1 and N8), but the link-layer addresses of the frame change from link to link. In link 1, the link-layer addresses are L1 and L2. In link 2, they are L4 and L5. In link 3, they are L7 and L8.

Note that the IP addresses and the link-layer addresses are not in the same order**.** For IP addresses, the source address comes before the destination address; for link-layer addresses, the destination address comes before the source.

Unicast Address

Each host or each interface of a router is assigned a unicast address. Unicasting means one to-one communication. A frame with a unicast address destination is destined onlyf or one entity in the link.

Example

The unicast link-layer addresses in the most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons; for example, the following is a link-layer address of a computer.

A3:34:45:11:92:F1

Multicast Address

Some link-layer protocols define multicast addresses. Multicasting means one-to many communication.

Example

The multicast link-layer addresses in the most common LAN,Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons.The second digit, needs to be an even number in hexadecimal. The following shows a multicast address:

A2:34:45:11:92:F1

Broadcast Address

Some link-layer protocols define a broadcast address. Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

Example

The broadcast link-layer addresses in the most common LAN,Ethernet, are 48 bits, all 1s, that are presented as 12 hexadecimal digits separated by colons.

The following shows a broadcast address: FF:FF:FF:FF:FF:FF .

Address Resolution Protocol (ARP)

The ARP protocol is one of the protocols defined in the network layer, as shown in Figure 1.7.2 . It belongs to the network layer. It maps an IP address to a logical-link address. The main work of ARP : It accepts an IP address from the IP protocol, maps the address to the corresponding link layer address, and passes it to the data-link layer.

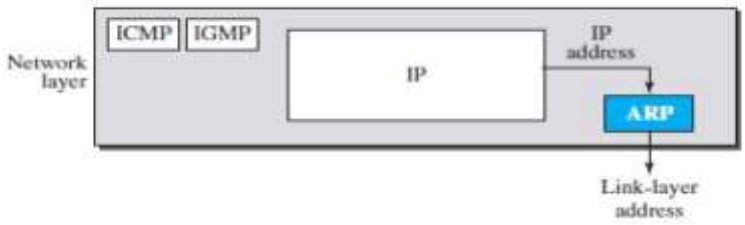

Fig1.7.2: ARP.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-245]

If a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet.The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link using the link-layer broadcast address.

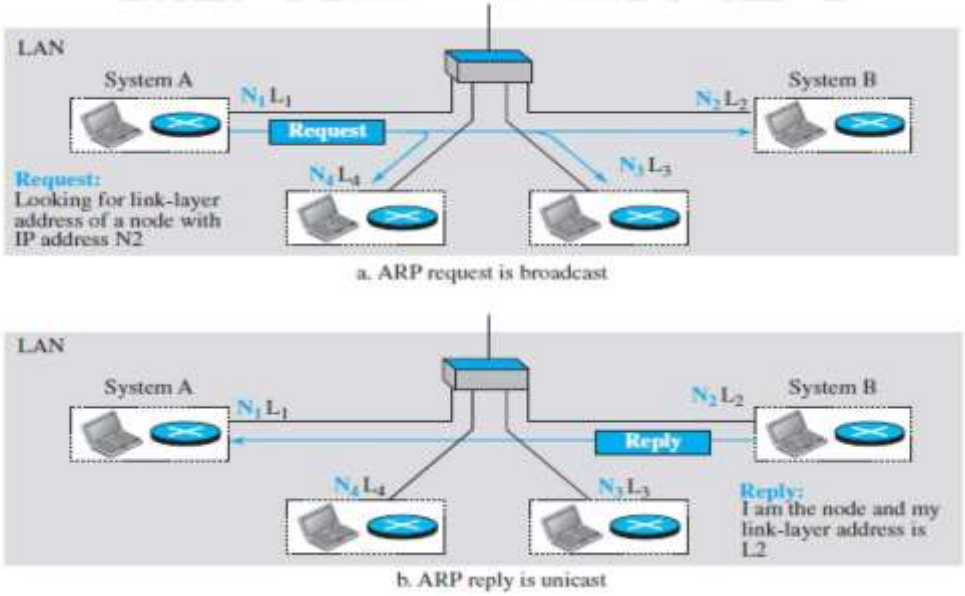

Fig1.7.3: ARP Operation.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-246]

Every host or router on the network receives and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.

The response packet contains the recipient's IP and link-layer addresses. The packet is unicast directly to the node that sent the request packet.

In Figure 1.7.3, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address N2. System A needs to pass the packet to its data-link layer for the actual delivery, but it does not know the physical address of the recipient. It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IP address of N2.This packet is received by every system on the physical network, but only system B will answer it, as shown in Figure 1.7.3b.System B sends an ARP reply packet that includes its physical address. Now system A can send all the packets it has for this destination using the physical address it received.

Packet Format

Figure 1.7.4 shows the format of an ARP packet. The hardware type field defines the type of the link-layer protocol; Ethernet is given the type 1. The protocol type field defines the network-layer protocol: IPv4 protocol is (0800)16.

The source hardware and source protocol addresses are variable-length fields defining the link-layer and network-layer addresses of the sender. The destination hardware address and destination protocol address fields define the receiver link layer rand network-layer addresses.

An ARP packet is encapsulated directly into a data-link frame. The frame needs to have a field to show that the payload belongs to the ARP and not to the network-layer datagram.

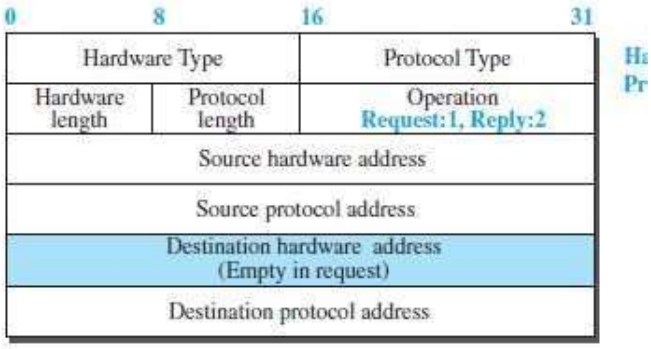

Fig1.7.4: ARP packet.

[Source :"Data Communications and Networking" by Behrouz A. Forouzan,Page-248]

1.5 OSI MODEL

OSI model is developed by the International Standards Organization (ISO).

This model is called ISO OSI (Open Systems Interconnection) Reference model because it deals with connecting open systems (systems that are open for communication with other systems).

Seven layers of the OSI model

Physical Layer

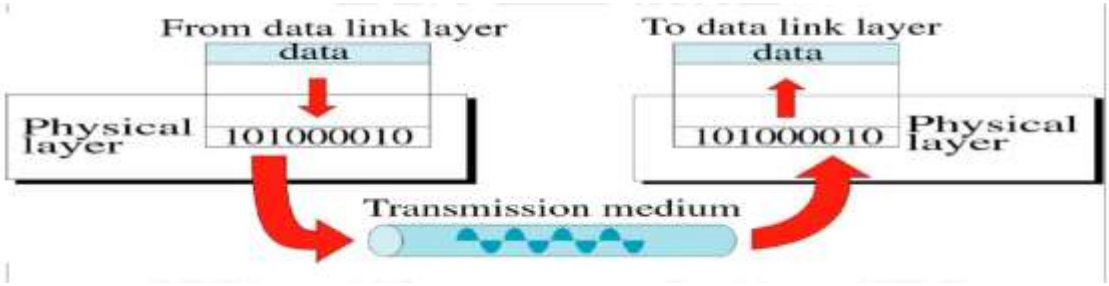

Fig1.5.1: Physical layer.

["Source : Data Communications and Networking" by Behrouz A. Forouzan,Page- 33]

It is the bottom layer of OSI Model. It is responsible for the actual physical connection between the devices. Such physical connection may be made by using twisted pair cable. It is concerned with transmitting bits over a communication channel as shown in figure 1.5.1.

Physical Layer Functions

Provides synchronization of bits by a clock.

- Physical layer manages the way a device connects to network media.
- It defines the transmission rate.
- It defines the way in which the devices are connected to the medium.
- It provides physical topologies
- It can use different techniques of multiplexing.

Data Link Layer

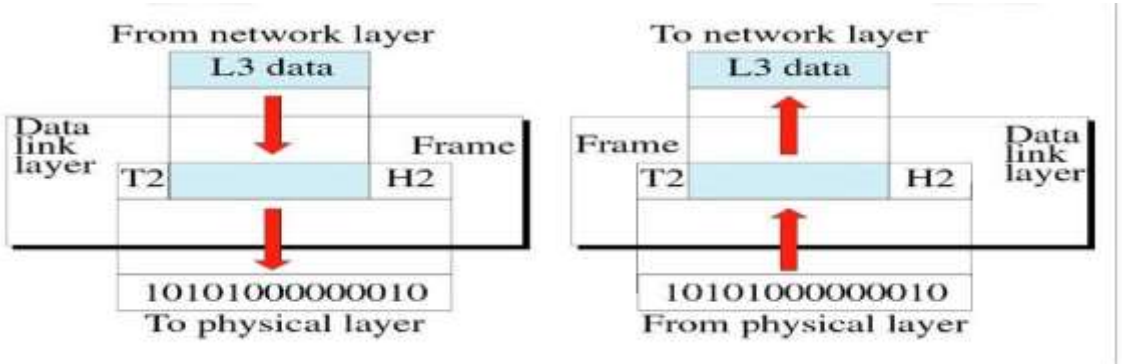

Fig1.5.2: Datalink layer.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-34]

It is responsible for node-to-node delivery of data as shown in figure 1.5.2.

It receives the data from network layer and creates frames , add physical address to these frames & pass them to physical layer

It consist of 2 layers:

Logical Link Layer (LLC) : Defines the methods and provides addressing information for communication between network devices.

Medium Access Control (MAC): Establishes and maintains links between communicating devices.

Functions of Data Link Layer

Framing :DLL divides the bits received from N/W layer into frames. (Frame contains all the addressing information necessary to travel from S to D).

Physical addressing: After creating frames, DLL adds physical address of sender/receiver (MAC address) in the header of each frame.

Flow Control: DLL prevents the fast sender from drowning the slow receiver.

Error Control: It provides the mechanism of error control in which it detects & retransmits damaged or lost frames.

Access Control: A single communication channel is shared by multiple devices, MAC layer of DLL provides help to determine which device has control over the channel.

Network Layer

It is responsible for the source to destination delivery of a packet across multiple networks as shown in figure 1.5.3. If two systems are attached to different networks with devices like routers, then N/W layer is used.

Thus DLL overseas the delivery of the packet between the two systems on same network and the network layer ensures that the packet gets its point of origin to its final destination.

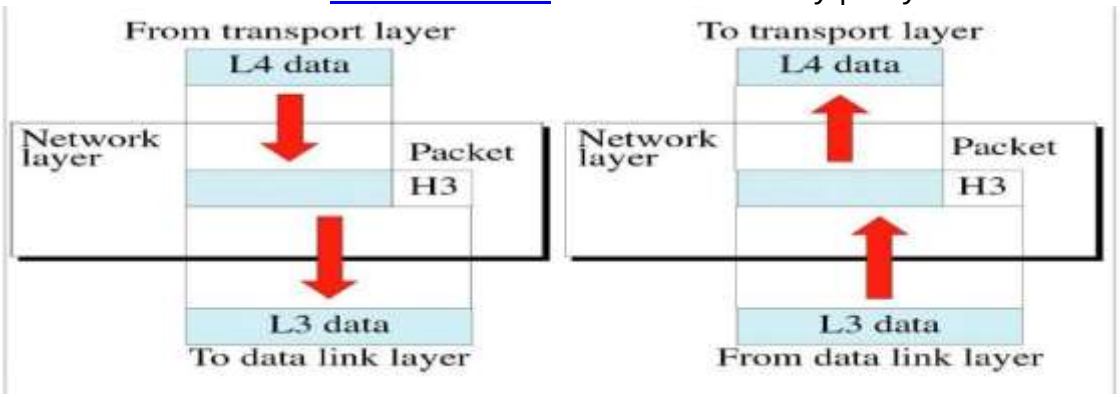

Fig1.5.3: Network layer.

[Source:"Data Communications and Networking" by Behrouz A. Forouzan,Page- 36]

Functions of Network Layer

It provides Internetworking.

Logical Addressing: When packet is sent outside the network, N/W layer adds Logical (network) address of the sender & receiver to each packet.

Network addresses are assigned to local devices by network administrator and assigned dynamically by special server called DHCP (Dynamic Host Configuration Protocol).

Routing: When independent network are connected to create internetwork several routes are available to send the data from Source to Destination.

These n/w are interconnected by routers & gateways that route the packet to final destination.

Transport Layer

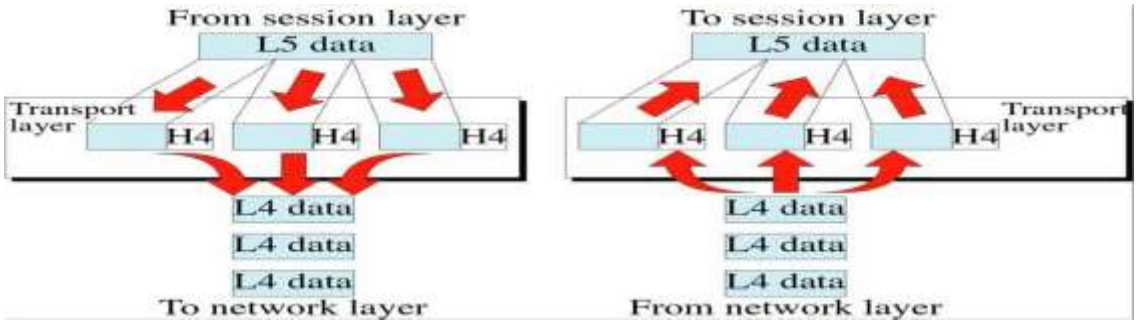

Fig1.5.4: Transport layer.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan.Page- 38]

It is responsible for process-to-process delivery of the entire message as shown in figure 1.5.4. Transport Layer looks after the delivery of entire message considering all its packets & make sure that all packets are in order. On the other hand n/w layer treated each packet independently.

At the receiver side, TL provides services to application layer & takes services form n/w layer.

At the source side, TL receives message from upper layer into packets and reassembles these packets again into message at the destination.

Transport Layer provides **two types of services**:

Connection Oriented Transmission: In this type of transmission the receiving devices sends an acknowledge back to the source after a packet or group of packet is received. It is slower transmission method.

Connectionless Transmission: In this type of transmission the receiving devices does not sends an acknowledge back to the source. It is faster transmission method.

Segmentation of message into packet & reassembly of packets into message.

Port addressing: Computers run several processes. TL header include a port address with each process.

Flow Control: Flow control facility prevents the source form sending data packets faster than the destination can handle.

Error control: TL ensures that the entire message arrives at the receiving TL without error.

Session Layer

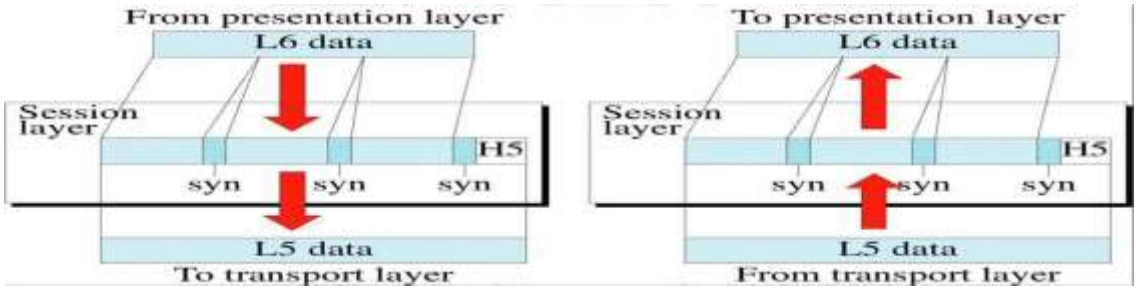

Fig1.5.5: Session layer.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page- 40]

It has the responsibility of beginning, maintaining and ending the communication between two devices as illustrated in figure 1.5.5 called session. It also provides for orderly communication between devices by regulating the flow of data.

Functions of Session Layer

Establishing, Maintaining and ending a session: When sending device first contact with receiving device, it sends syn(synchronization) packet to establish a connection & determines the order in which information will be sent.

Receiver sends ack (acknowledgement). So the session can be set & end.

Dialog Control: This function determines that which device will communicate first and the amount of data that will be sent.

Dialog separation: Process of adding checkpoints & markers to the stream of data is called dialog separation.

Presentation Layer

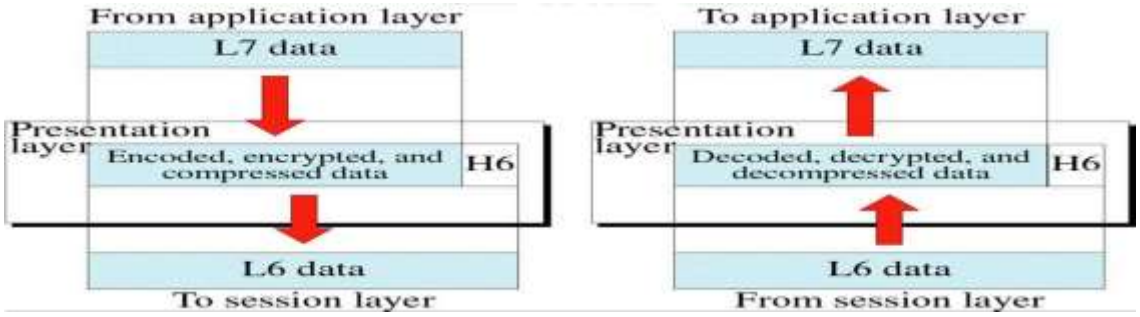

Fig1.5.6: Presentation layer.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page- 40]

It is concerned with the syntax & semantics of the information exchanged between the two devices.

It was designed for data encryption, decryption and compression as shown in figure 1.5.6.

Functions of Presentation Layer

Data Presentation or Translation: Because different computers use different encoding systems. It ensures that the data being sent is in the format that the recipient can process.

Data Encryption: PL provides this facility by which hides the information from everyone except the person who originally sent the information & the intended recipient. When encrypted data arrives at destination, PL decrypts the message.

Data Compression: PL shrinks large amount of data into smaller pieces i.e. it reduces the size of data.

Application Layer

It enables the user to access the network.

It provides user interface & supports for services such as e-mail, file transfer, access to the world wide web as shown in figure 1.5.7. So it provides services to different user applications.

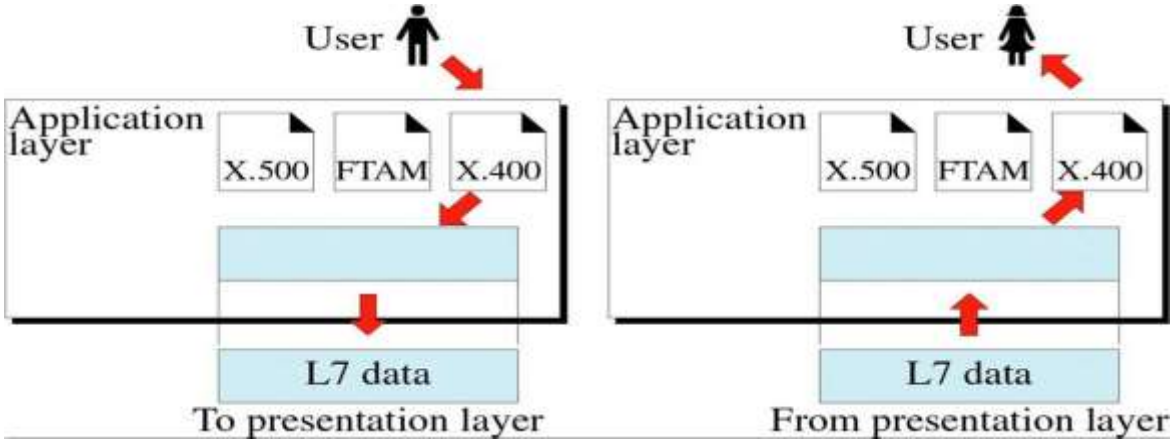

Fig1.5.7: Application layer.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-41]

Functions of Application Layer

Mail Services: This application provides various e-mail services.

File transfer & Access: It allows users to access files in a remote host, to retrieve files from remote computer for use etc.

Remote log-in: A user can log into a remote computer and access the resources of that computer.

Accessing the World Wide Web: Most common application today is the access of the World Wide Web.

UNIT I - FUNDAMENTALS AND LINK LAYER

1.1 OVERVIEW OF DATA COMMUNICATIONS

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

For data communications to occur,the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

The effectiveness of a data communications system depends on four characteristics: delivery,accuracy, timeliness, and jitter.

1. **Delivery.** The system must deliver data to the correct destination. Data must be received by the Receiver device .
2. **Accuracy.** The system must deliver the data accurately. Data that have been altered (changed during transmission) in transmission and left uncorrected are unusable.
3. **Timeliness.** The system must deliver data in exact time. Data delivered late are useless.

In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without (any delay) significant delay. This kind of delivery is called real-time transmission.

4. **Jitter.** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

For example, let us assume that video packets are sent every 30 ms.If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video occurs.

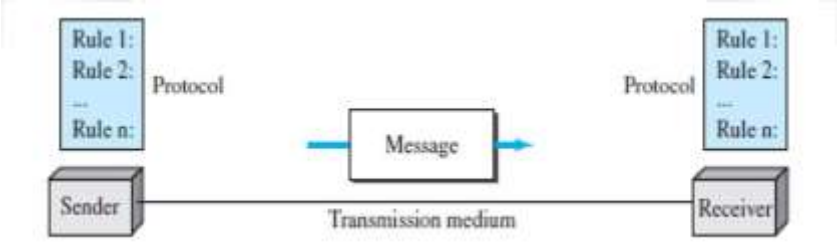

Fig1.1.1: Five Components of Data Communication.
[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-4]

1.Message. The message is the information (data) to be communicated as shown in figure 1.1.1. Popular forms of information include text, numbers, pictures, audio, and video.

2. Sender. The sender is the device that sends the data message. It can be a computer,workstation, telephone handset, video camera, and so on.

3.Receiver. The receiver is the device that receives the message. It can be a computer,workstation, telephone handset, television, and so on.

Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver.

Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

Protocol. A protocol is a set of rules that govern data communications.

It represents an agreement between the communicating devices (Between sender and Receiver). Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Representation

Information today (available) comes in different forms such as text, numbers, images, audio, and Video.

a. Text:

Text is represented as a bit pattern, a sequence of bits (Os or 1s).

What is bit pattern? All data inside a computer is transmitted as a series of electrical signals that are either on or off. Therefore, in order for a computer to be able to process any kind of data, including text, images and sound, they must be converted into binary form.

Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding.

b. Numbers:

Numbers are also represented by bit patterns. The number is directly converted to a binary number to simplify mathematical operations.

ie: Conversion of decimal to binary

c. Images: Images are also represented by bit patterns.

Representing image by bit pattern: Images also need to be converted into binary in order for a computer to process them so that they can be seen on our screen.

Digital images are made up of pixels. Each pixel in an image is made up of binary numbers.

If we say that 1 is black (or on) and 0 is white (or off), then a simple black and white picture can be created using binary.

d. Audio:

Audio refers to the recording or broadcasting of sound or music. It is continuous, not discrete.

e. Video:

Video refers to the broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex.

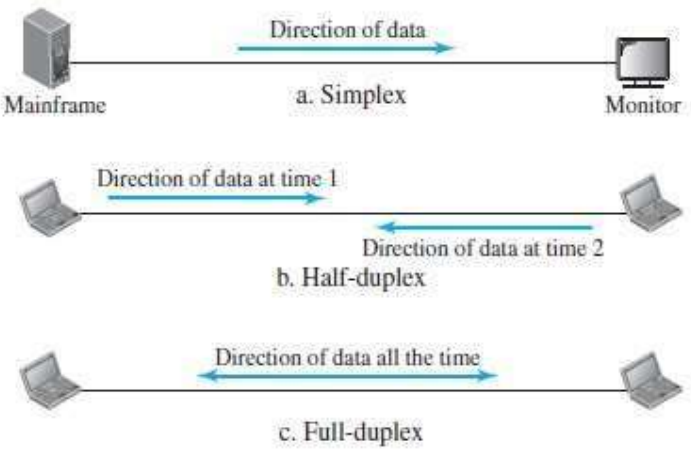

Fig 1.1.2: Mode of Communication.

[Source : *"Data Communications and Networking" by Behrouz A. Forouzan,Page-6]*

a. Simplex:

In simplex mode, the communication is unidirectional, as on a one-way street.

Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.1.2a).

Keyboards and traditional monitors are examples of simplex devices.

b. Half-Duplex:

In half-duplex mode, each station can both transmit and receive, but not at the same time.

When one device is sending, the other can only receive, and vice versa (see Figure 1.1.2b).

Walkie-talkies are both half-duplex systems.

c. Full-Duplex:

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously (at the same time), (see Figure 1.1.2c).

Example of full-duplex communication is the telephone network.When two people are communicating by a telephone line, both can talk and listen at the same time.

NETWORKS

A network is the interconnection of a set of devices capable of communication.

Here , a device can be a host (called as end system) such as a large computer, desktop, laptop, workstation, cellular phone, or security system.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another.

Response time is the elapsed time between an inquiry and a response.

The performance of a network depends on a number of factors.

1.the number of users 2.the type of transmission medium 3.the capabilities of the connected hardware 4.the efficiency of the software.

Performance is often evaluated by two networking metrics: throughput and delay**.**

Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from data losses.

Physical Structures

Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another.

Point-to-Point: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices .

Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure1.1.3 below).

In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

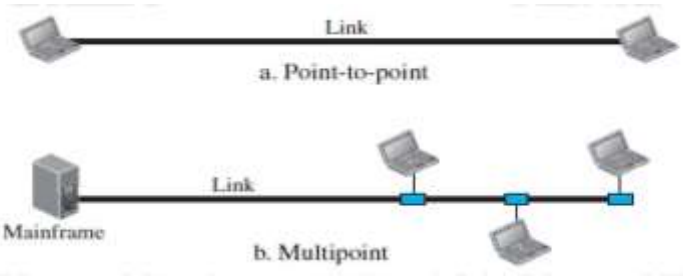

Fig1.1.3: Types of Connections.

[Source : *"Data Communications and Networking" by Behrouz A. Forouzan,Page-9]*

Physical Topology

The physical layout of a network is called Topology. Two or more devices connect to a link; two or more links form a topology.The topology of a network is the geometric representation of the relationship of all the links and linking devices (called nodes) to one another.

There are four basic Topologies: mesh, star, bus, and ring.

Mesh: In a mesh topology, every device has a dedicated point-to-point link as in figure 1.1.4,to every other device. A fully connected mesh network with n nodes has n(n -1) /2 physical channels.

Fig1.1.4: Mesh topology.

[Source : *"Data Communications and Networking" by Behrouz A. Forouzan,Page-10]*

Advantages:

The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

Point-to-point links make fault identification and fault isolation easy.

Disadvantages:

Every device must be connected to every other device, installation and reconnection are difficult.

More number of wire connections make it greater than the available space (in walls, ceilings, or floors) which can accommodate.

The hardware required to connect each link (I/O ports and cable) can be expensive.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology: In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.

The devices are not directly connected to one another. Unlike a mesh topology, A star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure 1.1.5).

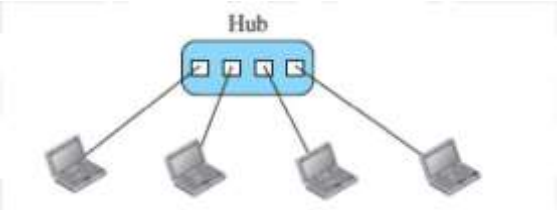

Fig1.1.5: Star topology.

[Source : *"Data Communications and Networking" by Behrouz A. Forouzan,Page-10]*

Advantages:

Less expensive than a mesh topology.

Easy to install and reconfigure. Less cables are required, and additions, and deletions involve only one connection: between that device and the hub.

It is Robust. If one link fails, only that link is affected. All other links remain active.

Disadvantages:

The topology depends on one single point, the hub. If the hub goes down, the whole system is dead. A star requires far less cable than a mesh; each node must be linked to a central hub. The star topology is used in local-area networks (LANs). High-speed LANs also use a star topology with a central hub.

c. Bus Topology: A bus topology is multipoint. One long cable acts as a backbone to link allthe devices in a network (see Figure 1.1.6).

Nodes are connected to the bus cable by drop lines and taps.A drop line is a connection between the device and the main cable.

A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat.

Therefore, the signal becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps used in this topology.

Fig1.1.6: Bus Topology.

[Source : *"Data Communications and Networking" by Behrouz A. Forouzan,Page-11]*

Advantages:

Ease of installation.

Less cabling

Disadvantages:

Difficult reconfiguration and fault isolation, Difficult to add new devices, Signal reflection at top can cause degradation in quality. If any fault in backbone occurs ,then it can stop all transmission. Ethernet LANs can use a bus topology, but they are less popular now.

Ring Topology: In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. When a device receives a signal intended for another device, its repeater regenerates the bits and passes along them (see Figure 1.1.7).

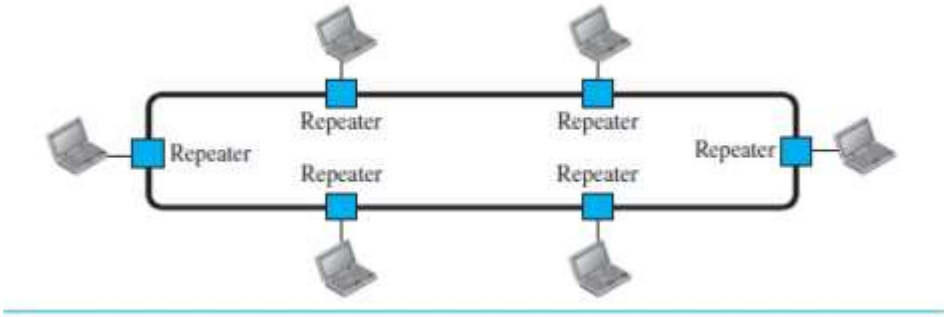

Fig1.1.7: Ring Topology.

[Source : *"Data Communications and Networking" by Behrouz A. Forouzan,Page-12]*

Advantages:

Easy to install.

Easy to reconfigure.

Fault identification is easy.

Disadvantages:

Unidirectional traffic.

Break in a single ring can break entire network.

1.3 PROTOCOL LAYERING

When communication is simple,we need only one simple protocol; when the communication is complex, we need to divide the task between different layers, in which case we need a protocol at each layer .

Dividing the task between different layers is called Protocol layering.

Scenarios

Two simple scenarios are available to understand the need for protocol layering.

First Scenario

In the first scenario, communication is simple that it can occur in only one layer.

Assume Maria and Ann are neighbors with a lot of common ideas. Communication between Maria and Ann takes place in one layer, face to face, in the same language, as shown in Figure 1.3.1.

Fig1.3.1: Single layer protocol.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-32]

Set of rules followed in this scenario:

First, Maria and Ann know that they should greet each other when they meet. **Second**,they know that they should confine their vocabulary to the level of their friendship. **Third**, each party knows that she should refrain(not talking) from speaking when the other party is speaking.**Fourth**, each party knows that the conversation should be a dialog. **Fifth**, they should exchange some nice words when they leave.

Second Scenario

In the second scenario, we assume that Ann is offered a higher-level position in her company, but needs to move to another branch located in a city very far from Maria.The two friends still want to continue their communication and exchange ideas because they have come up with an innovative project to start a new business when they both retire.They decide to continue their conversation using regular mail through the post office. They agree on an encryption/decryption technique.

The sender of the letter encrypts it to make it unreadable by an intruder; the receiver of the letter decrypts it to get the original letter.

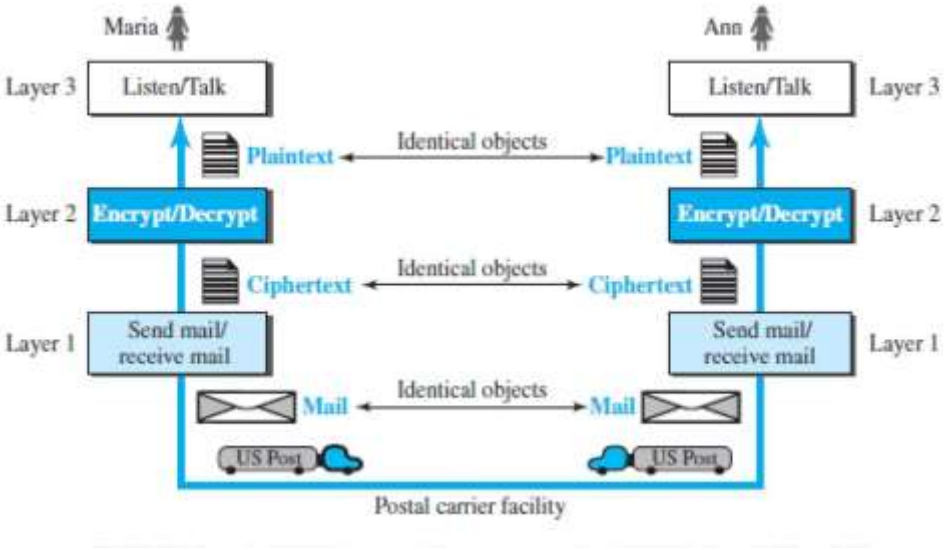

Fig1.3.2: Three layer protocol.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-33]

Consider that Maria sends the first letter to Ann. Maria talks to the machine at the third layer as though the machine is Ann and is listening to her. The third layer machine listens to what Maria says and creates the plaintext (a letter in English), which is passed to the second layer machine.

The second layer machine takes the plaintext ,encrypts it, and creates the ciphertext, which is passed to the first layer machine. The first layer machine, takes the ciphertext, puts it in an envelope,adds the sender and receiver addresses, and mails it.

Protocol layering enables us to divide a complex task into several smaller and simpler tasks.

For example, in the Figure 1.3.2, we could have used only one machine to do the job of all three machines. However, if Maria and Ann decide that the encryption/decryption done by the machine is not enough to protect their secrecy, they would have to change the whole machine. In the present situation, they need to change only the second layer machine; the other two can remain the same. This is referred to as modularity.

Principles of Protocol Layering

First Principle

If we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction. For example, the third layer task is to listen (in one direction) and *talk* (in the other direction).

The second layer needs to be able to encrypt and decrypt. The first layer needs to send and receive mail.

Second Principle

The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.

For example, the object under layer 3 at both sites should be a plaintext letter. The object under layer 2 at both sites should be a cipher text letter. The object under layer 1 at both sites should be a piece of mail.

Logical connection between each layer is shown in Figure 1.3.3.

We have layer-to-layer communication. Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer.

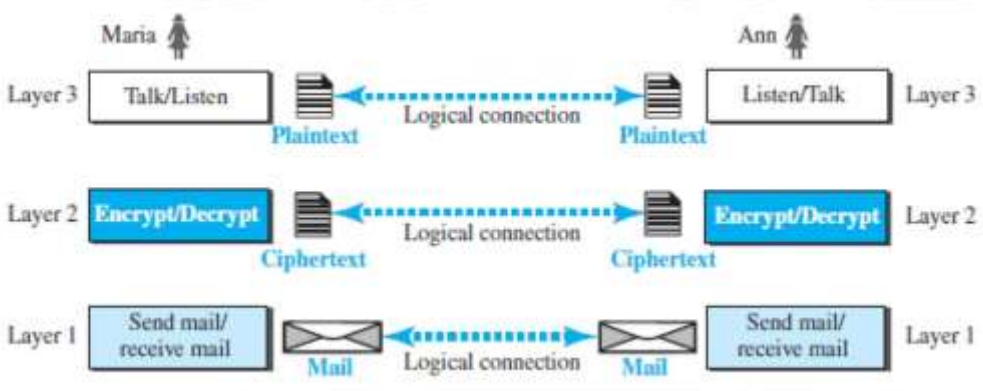

Fig1.3.3: The concept of logical connection between layers.

[Source : "Data Communications and Networking" by Behrouz A. Forouzan,Page-35]