Q.2a. What is TCP/IP Model? Explain the functions, protocols and services of each layer. (10)

Answer:

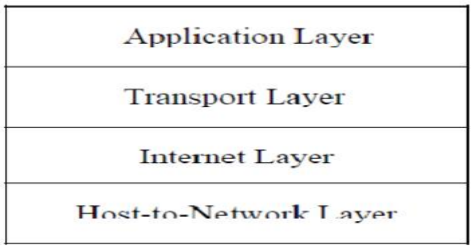
The TCP/IP MODEL:-

The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,

1. To connect multiple networks together so that they appear as a single network.
2. To survive after partial subnet hardware failures.
3. To provide a flexible architecture.

Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,

1. Host-to-Network Layer
2. Internet Layer
3. Transport Layer
4. Application Layer



Application Layer

Transport Layer

Internet Layer

Host-to-Network Layer

TCP/IP Reference model

1. Host-to-Network Layer:

The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

2. Internet Layer:

This layer, called the internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have they travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The internet layer defines an official packet format and protocol called IP (Internet Protocol). The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer.

3. The Transport Layer:

The layer above the internet layer in the TCP/IP model is now usually called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

The second protocol in this layer, UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. Since the model was developed, IP has been implemented on many other networks.

4. The Application Layer:

The TCP/IP model does not have session or presentation layers. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP), as shown in Fig.6.2. The virtual terminal protocol allows a user on one machine to log onto a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it. Many other protocols have been added to these over the years: the Domain Name System (DNS) for mapping host names onto their network addresses, NNTP, the protocol for moving USENET news articles around, and HTTP, the protocol for fetching pages on the World Wide Web, and many others.

b. What is meant by Data Communication? Explain its characteristics. (6)

Answer:

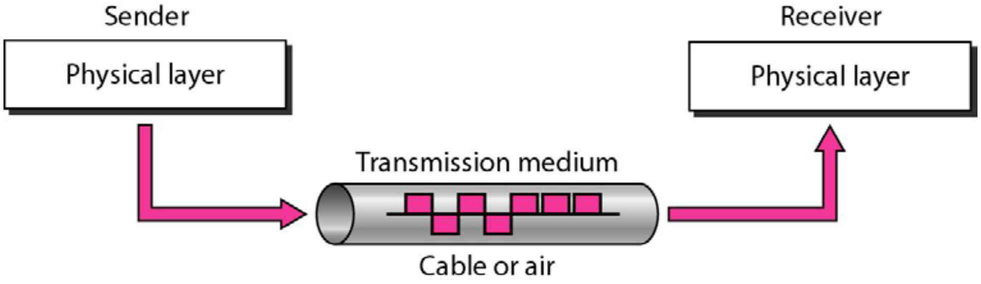
Data communications means the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery:** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. Accuracy: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. Timeliness: The system must deliver data in a timely manner. 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 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 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

Q.3 a. Explain guided and unguided transmission media. (6)

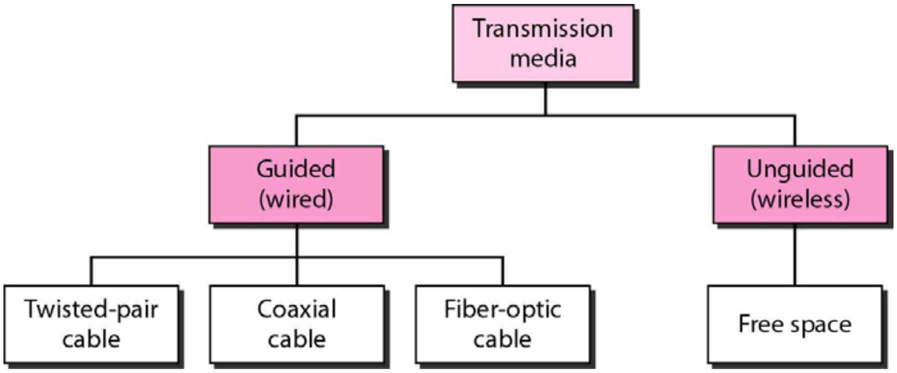
Answer:

Transmission media are actually located below the physical layer and are directly controlled by the physical layer. The following figure shows the position of transmission media in relation to the physical layer.



A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane.

In telecommunications, transmission media can be divided into two broad categories: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space as shown in the following figure.



b. What is the advantage of synchronous transmission? (4)

Answer:

When the data in continuous manner with a random speed than synchronous transmissionis used.The various advantages of this transmission are listed below:

- The speed is synchronous transmission is very fast as compared to asynchronous transmission.
- It can handle large amount of information.
- In this transmission no start and stop bits are required to identify the data bits.
- Lower overhead and thus , greater throughput.
- No gap between two successive groups of data bits.
- The bit stream is continuous.

c. Two computers using TDM take up turns to send 100- bytes packet over a shared channel that operates at 64000 bits per second. The hardware takes 100 microseconds after one computer stops sending before the other can begin. How long will it take for each computer to send one megabyte data file? (6)

Answer:

channel rate is 64000 bits/second or 8000 bytes per second.

Therefore 100bytes size packet will take 100/8000 seconds that is .0125 seconds.

One megabyte file will contain 1000000/100 = 10000 packets of 100 bytes size each. two system sending one megabyte file each means 20000 packets will

be sent Therefore, 20000 packets will take 20000 X .0125 =

250.000 seconds Hardware take 100 micro second or 0.0001

seconds.

Computer send packets turn by turn between every two consecutive packets there will be 0.0001 second gap for 20000 packets gap is 20000 X 0.0001 = 2.0 seconds.

Total time will 250 + 2 = 252 seconds a computer.

Q.4 a. Write the comparison between analog and digital signal. (8)

Answer:

Description	Analog Signal	Digital Signal
Signal	Analog signal is a continuous signal which represent physical measurement	Digital signals are discrete time signals generated by digital modulation.
Waves	Denoted by sine wave	Denoted by square wave
Representation	Uses continuous range of values to represent information	Use descrete or discontinuous values to represent information
Example	Human voice in air,analog electronic devices	Computers,CDs,DVDs and other digital electronic devices
Technology	Analog technology records waveforms as they are	Sample analog waveforms into a limited set of numbers and records them
Data transmission	Subjected to deterioration by noise during transmission and write/read cycle	Can be noise-immune without deterioration during transmission and write/read cycle
Response to noise	More likely to get affected reducing accuracy	Less affected since noise response are analog in nature
Flexibility	Analog hardware is not flexible	Digital hardware is flexible in implemention
Application	Thermometer	PCs,PDAs
Bandwidth	Analog signal processing can be done in real time and consumes less bandwidth	There is no guarantee that digital signal processing can be done in real time and consumes more bandwidth to carry out the same

		information
Memory	Stored in the form of wave signal	Stored in the form of binary bit
Cost	Low cost and portable	Cost is high and not easily portable
Impedance	Low	High order of 100 megaohm
Errors	Analog instruments usually have a scale which is cramped at lower end and give considerable observational errors	Digital instruments are free form observational errors like parallax and approximation errors

b. Explain various error detection techniques in digital data transmission. (8)

Answer:

Most error detection techniques work the same way,an error detection value is first calculated by the sender and transmitted along with the data.At the receiving end,the error detection value is recalculated and checked against the received value. If the two values are the same,the data received correctly.If they differ, an error has occurred and the data needs to be sent again. Three common forms of error detection techniques used are given below:

1. Parity Checking
2. Longitudinal Redundancy Checking
3. Polynomial Checking

1.**Parity Checking Method**: Errors may occur in recording data on magnetic media due to bad tracks,sectors on the recording surface.Errors may also be caused by electrical disturbances during data transmission between two distant computer.

Parity Checking is one of the oldest and simplest error detection techniques. At the receiving end,the parity bit is recalculated.If one bit has been transmitted in error the received parity bit will differ from the recalculated one.

Suppose the sender wants to send the world.In ASCII the five characters are coded as:
1110111 1101111 1110010 1101100 1100100
The following shows the actual bits send
11101110 11011110 11100100 11011000 11001001
There are mainly two types of parity checks:

- **Even Parity:** Assume we are using even parity with 7-bit ASCII. The letter V in 7-bit ASCII is encoded as 0110101. Because there are four 1’s(an even number), Parity is set to 0, so that the sum of all the bits remains even.This would be transmitted as 01101010.
- **Odd parity:** Assume we are using odd parity with 7-bit ASCII.Againthe letter V in 7-bit ASCII is encoded as 0110101. Because there are four 1’s(an even number), Parity is set to 1, so that the sum of all the bits remains odd .This would be transmitted as 01101011.

2. Longitudinal Redundancy Checking(LRC): In this error detection method, a block of bits is organized ina tale with rows and columns.Then the parity bit for each column is calculated and new row of eight bits,which are the parity bits for the whole block,iscreated.Better that the new calculated parity bits are attached to the original data and sends to the receiver.

LCR increases the likelihood of detecting burst error.In LRC of n bits can easily detect a burst error of n bits .however if two bits in data unit are damaged and two bits n exactlythe same position in another data unit are also damaged,the LRC checkerwill not detect an error.
10100011 00110011 11011101 11100111
10101010(LRC)

3. **Polynomial Checking**: Polynomial Checking has a 98 percent error detection rate,which is reasonably good,but it is still not perfect. Like LRC , Polynomial Checking adds a character or series of characters to the end of the message based on a mathematical algorithm.One of the most popular of polynomial error checking schemes redundancy

checks(CRC). CRC producing error detection rate above 99 percent is cyclical. Polynomial checking also includes checksum.

(a) Checksum:In the checksum, the sender follows these steps:

- The unit is divided into k sections, each of n bits.
- All sections are added using one's complement to get the sum.
- Time –Division Multiple Access(TDMA)
- Code –Division Multiple Access (CDMA)
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data.

The receiever follows these steps:

- The unit is divided into k sections, each of n bits.
- All sections are added using one's complement to get the sum.
- The sum is complemented.If the results is zero,the data are accepted:otherwise, rejected.

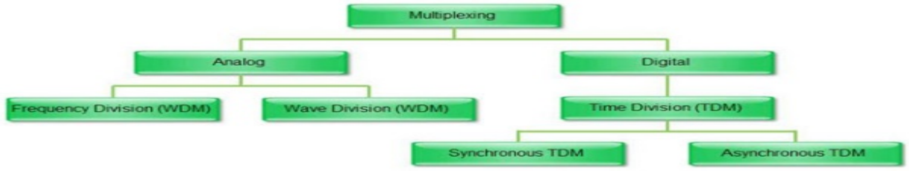
Q.5 a. What is multiplexing? Explain the various types of multiplexing techniques. (8)

Answer:

The technique of transmitting multiple signals over a single medium is defined as Multiplexing. It is a technique showed at physical layer of OSI model.The different types of multiplexing technologies are as below

- Wavelength Division Multiplexing (WDM)
- Frequency Division Multiplexing (FDM)
- Dense Wavelength Division Multiplexing (DWDM)
- Conventional Wavelength Division Multiplexing (CWDM)
- Reconfigurable Optical Add-Drop Multiplexer (ROADM)
- Orthogonal Frequency Division Multiplexing (OFDM)
- Add/Drop Multiplexing (ADM)
- Inverse Multiplexing (IMUX)

Types of Multiplexer



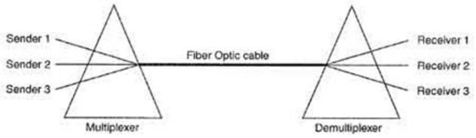
Frequency Division Multiplexing

Frequency Division Multiplexing is a technique which uses various frequencies to combine many streams of data for sending signals over a medium for communication purpose. It carries frequency to each data stream and later combines various modulated frequencies to transmission.Television Transmitters are the best example for FDM, which uses FDM to broad cast many channels at a time.

Wavelength Division Multiplexing

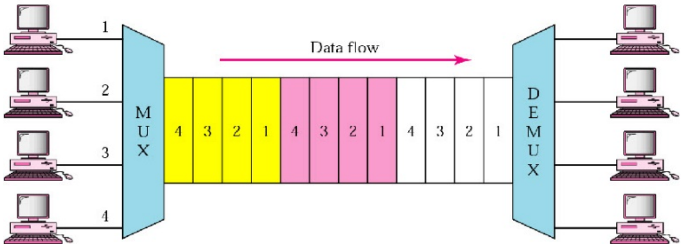
Wavelength Division Multiplexing (WDM) is analog multiplexing technique and it modulates many data streams on light spectrum. This multiplexing is used in optical fiber. It is FDM optical equivalent.Various signals in WDM are optical signal that will be light and were transmitted through optical fiber.WDM similar to FDM as it mixes many signals of different frequencies into single signal and transfer on one link.Wavelength of wave is reciprocal to its frequency, if wavelength increase then frequency decreases.Several light waves from many sources are united to get light signal which will be transmitted across channel to receiver.

Wavelength Division Multiplexing
The main principle in using prisms is that they bend a light beam depending on angle of incidence and frequency of light wave or ray. At receiver end the light signal is split into different light waves by demux. This type of merging and breaking of light wave made by a prism. Single prism is used at the end of sender for multiplexing and other prism is used at receiver end for demultiplexing as shown in fig.



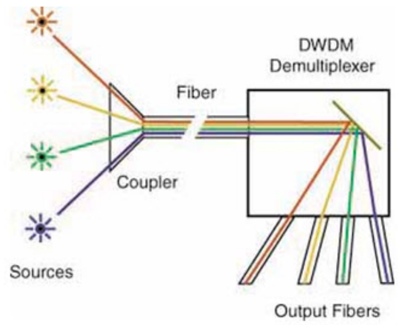
Usage of PRISM in WDM
WDM used in Synchronous Optical Network (SONET). It utilizes various optical fiber lines that are multiplexed and demultiplexed.

Time Division Multiplexer
TDM is one of types of multiplexers which join data streams by allotting every stream different time slot in a set. It frequently transfers or sends various time slots in an order over one transmission channel. TDM attaches PCM data streams.



Time Division Multiplexer

Dense Wavelength Division Multiplexer
In Dense Wavelength Division Multiplexing, an optical technology used to expand bandwidth onto fiber optic. Bit rate and protocol are independent and these are the main advantage of DWDM. Dense Wavelength Division Multiplexing (DWDM) operated by combining different signals simultaneously at different wavelengths. On fiber is changed to multiple fibers. By increasing the carrier capacity of fiber from 2.5Gb/s to 20 Gb/s, an eight OC 48 signals can be multiplexed into single fiber.Singlefibers are able to transfer data at a speed upto 400 GB/s due to DWDM.DWDM transfers data or information in IP, SONET, ATM and Ethernet It also carries different type of traffic at a range of speeds on an optical channel.



Dense Wavelength Division Multiplexer

Statistical Multiplexer

It allows to share a single line of data for multiplexer RS-232 devices. Error correction will be performed in order to ensure the transmission an error-free one. The word “Statistical” refers to its capability to receive advantage of statics of many RS-232 devices means terminal and PC users.Each PC averages less than 5% of its potential data rate.
This type of multiplexer permits the sum of terminal and PC rates in which it extends composite link speed between multiplexers. This is due the reason that the keyboards are idle. These types of multiplexers requires buffer.

b. Write short notes on the following: **(4×2)**
(i) Flow control
(ii) High-Level Data Link Control (HDLC)

Answer: (i) **Flow control (data)**

In data communications, **flow control** is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node. Flow control should be distinguished from congestion control, which is used for controlling the flow of data when congestion has actually occurred. Flow control mechanisms can be classified by whether or not the receiving node sends feedback to the sending node.

Flow control is important because it is possible for a sending computer to transmit information at a faster rate than the destination computer can receive and process it. This can happen if the receiving computers have a heavy traffic load in comparison to the sending computer, or if the receiving computer has less processing power than the sending computer.

Stop-and-wait

Stop-and-wait flow control is the simplest form of flow control. In this method, the receiver indicates its readiness to receive data for each frame, the message is broken into multiple frames. The sender waits for an ACK (acknowledgement) after every frame for specified time (called time out). It is sent to ensure that the receiver has received the frame correctly. It will then send the next frame only after the ACK has been received.

Operations

1. **Sender:** Transmits a single frame at a time.
2. **Receiver:** Transmits acknowledgement (ACK) as it receives a frame.
3. Sender receive ACK within time out.
4. Go to step 1.

If a frame or ACK is lost during transmission then it has to be transmitted again by sender. This retransmission process is known as ARQ (automatic repeat request).

The problem with Stop-and wait is that only one frame can be transmitted at a time, and that often leads to inefficient transmission, because until the sender receives the ACK it cannot transmit any new packet. During this time both the sender and the channel are unutilised.

Pros and cons of stop and wait

Pros

The only advantage of this method of flow control is its simplicity.

Cons

The sender needs to wait for the ACK after every frame it transmits. This is a source of inefficiency, and is particularly bad when the propagation delay is much longer than the transmission delay.

Stop and wait can also create inefficiencies when sending longer transmissions. When longer transmissions are sent there is more likely chance for error in this protocol. If the messages are short the errors are more likely to be detected early. More inefficiency is created when single messages are broken into separate frames because it makes the transmission longer

(ii) High-Level Data Link Control

High-Level Data Link Control (HDLC) is a bit-oriented code-transparent synchronousdata link layerprotocol developed by the International Organization for Standardization (ISO). The original ISO standards for HDLC are:

- ISO 3309 – Frame Structure
- ISO 4335 – Elements of Procedure
- ISO 6159 – Unbalanced Classes of Procedure
- ISO 6256 – Balanced Classes of Procedure

The current standard for HDLC is ISO 13239, which replaces all of those standards.

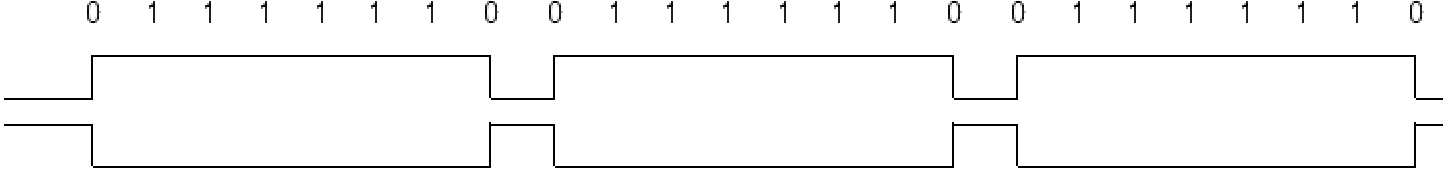
HDLC provides both connection-oriented and connectionless service.

HDLC can be used for point to multipoint connections, but is now used almost exclusively to connect one device to another, using what is known as Asynchronous Balanced Mode (ABM). The original master-slave modes Normal Response Mode (NRM) and Asynchronous Response Mode (ARM) are rarely used.

Framing

HDLC frames can be transmitted over synchronous or asynchronousserial communication links. Those links have no mechanism to mark the beginning or end of a frame, so the beginning and end of each frame has to be identified. This is done by using a frame delimiter, or *flag*, which is a unique sequence of bits that is guaranteed not to be seen inside a frame. This sequence is '01111110', or, in hexadecimal notation, 0x7E. Each frame begins and ends with a frame delimiter. A frame delimiter at the end of a frame may also mark the start of the next frame. A sequence of 7 or more consecutive 1-bits within a frame will cause the frame to be aborted.

When no frames are being transmitted on a simplex or full-duplex synchronous link, a frame delimiter is continuously transmitted on the link. Using the standard NRZI encoding from bits to line levels (0 bit = transition, 1 bit = no transition), this generates one of two continuous waveforms, depending on the initial state:



This is used by modems to train and synchronize their clocks via phase-locked loops. Some protocols allow the 0-bit at the end of a frame delimiter to be shared with the start of the next frame delimiter, i.e. '011111101111110'.

For half-duplex or multi-drop communication, where several transmitters share a line, a receiver on the line will see continuous idling 1-bits in the inter-frame period when no transmitter is active.

Since the flag sequence could appear in user data, such sequences must be modified during transmission to keep the receiver from detecting a false frame delimiter. The receiver must also detect when this has occurred so that the original data stream can be restored before it is passed to higher layer protocols. This can be done using bit stuffing, in which a "0" is added after the occurrence of every "11111" in the data. When the receiver detects these "11111" in the data, it removes the "0" added by the transmitter.

Synchronous framing

On synchronous links, this is done with bit stuffing. Any time that 5 consecutive 1-bits appear in the transmitted data, the data is paused and a 0-bit is transmitted. This ensures that no more than 5 consecutive 1-bits will be sent. The receiving device knows this is being done, and after seeing 5 1-bits in a row, a following 0-bit is stripped out of the received data. If, after 5 consecutive 1-bits, the following bit is also a 1-bit, the receiving device knows that either a flag has been found (if the sixth 1-bit is followed by a 0-bit) or an error has occurred (if the sixth 1-bit is followed by seventh 1-bit). In the latter case, the frame receive procedure, depending on state, is generally either aborted or restarted.

This also (assuming NRZL with transition for 0 encoding of the output) provides a minimum of one transition per 6 bit times during transmission of data, and one transition per 7 bit times during transmission of flag, so the receiver can stay in sync with the transmitter. Note however, that for new protocols, newer encodings such as 8b/10b encoding are better suited.

HDLC transmits bytes of data with the least significant bit first (not to be confused with little-endian order, which refers to byte ordering within a multi-byte field).

Asynchronous framing

When using asynchronous serial communication such as standard RS-232serial ports, bits are sent in groups of 8, and bit-stuffing is inconvenient. Instead they use "control-octet transparency", also called "byte stuffing" or "octet stuffing". The frame boundary octet is 01111110, (7E in hexadecimal notation). A "control escape octet", has the bit sequence '01111101', (7D hexadecimal). If either of these two octets appears in the transmitted data, an escape octet is sent, followed by the original data octet with bit 5 inverted. For example, the data sequence "01111110" (7E hex) would be transmitted as "01111101 01011110" ("7D 5E" hex). Other reserved octet values (such as XON or XOFF) can be escaped in the same way if necessary.

Q.6 a. Why is packet switching important? Give at least two reasons. (4)

Answer:

Packet switching is important because of the following to reasons:

1 . A sender and the receiver need to coordinate transmission to ensure that data arrives correctly. Dividing the data into small blocks helps a sender and receiver determines which block arrive intact and which do not .

2. Second , because communication circuits and the associated modem hardware

are expansive, multiple computers often share underlying connections and hardware . To ensure that all computers receive fair, prompt access to a shared communication facility, a network system allows one computer to deny access to others . Using small packets helps ensure fairness .

b. What is the chief advantage of using virtual packets instead of frames? (5)

Answer:

The router cannot transfer a copy of a frame from one type of network to another because the frame formats differ. More importantly, the router cannot simply reformat the frame header because the two networks may use incompatible address format.

To overcome heterogeneity, Internet protocol software defines an inter packet format that is independent of the underlying hardware . This is called virtual packet and can be transferred across the underlying hardware . The underlying hardware does not understand or recognize the Internet packet format, the protocol software creates and handles Internet packets .

c. How congestion is controlled in TCP? (7)

Answer:

One of the most important aspects of TCP is a mechanism for congestion control.In most modern internets, packet loss or extreme long delays are more likely to be caused by congestion than a hardware failure . Interestingly, transport protocols that retransmit can exacerbate the problem of congestion by injecting additional copies of a message.

To avoid such a problem,TCP always uses packet loss as a measure of congestion and responds to congestion by reducing the rate at which it retransmits data .

TCP does not compute an exact transmission rate .In stead, TCP bases transmission on buffers . That is, the receiver ad vertises a window size and the sender can transmit data to fill the receiver's window before an ACK is received . To control the data rate, TCP imposes a restriction on the window size – by temporarily reducing the window size , the sending TCP effectively reduces the data rate.

Q.7 a. Explain the basic difference between IEEE 802.3 and switched Ethernet. (4)

Answer:

In Ethernet (IEEE 802.3) the topology, though physically is start but logically is BUS. i.e. the collision domain of all the nodes in a LAN is common. In this situation only one frame can send the frame, if more than one station sends the frame, there is a collision.

In Switched Ethernet, this collision domain is separated. Hub is replaced by a switch, a device that can recognize the destination address and can route the frame to the port to which the destination station is connected, the rest of the media is not involved in the transmission process. The switch can receive another frame from another station at the same time and can route this frame to its own final destination.

b. Discuss various types of network topologies in computer network. (8)

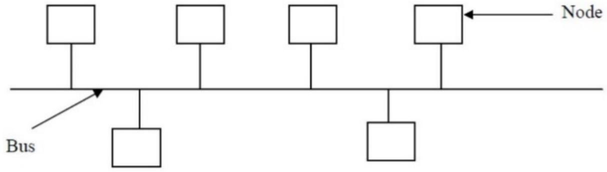
Answer:

Network topologies:

Network topology defined as the logical connection of various computers in the network. The six basic network topologies are: bus, ring, star, tree, mesh and hybrid.

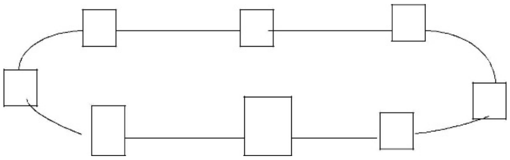
1. Bus Topology:

In bus topology all the computers are connected to a long cable called a bus. A node that wants to send data puts the data on the bus which carries it to the destination node. In this topology any computer can data over the bus at any time. Since, the bus is shared among all the computers. When two or more computers to send data at the same time, an arbitration mechanism are needed to prevent simultaneous access to the bus.



2. Ring Topology:

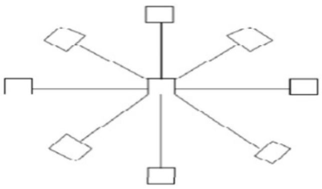
In ring topology, the computers are connected in the form of a ring. Each node has exactly two adjacent neighbors. To send data to a distant node on a ring it passes through many intermediate nodes to reach to its ultimate destination.



A ring topology is as to install and reconfigure. In this topology, fault isolation is easy because a signal that circulates all the time in a ring helps in identifying a faulty node. The data transmission takes place in only one direction. When a node fails in ring, it breaks down the whole ring. To overcome this drawback some ring topologies use dual rings. The topology is not useful to connect large number of computers.

3. Star Topology:

In star topology all the nodes are connected to a central node called a hub. A node that wants to send some six data to some other node on the network, send data to a hub which in turn sends it the destination node. A hub plays a major role in such networks.



Star topology is easy to install and reconfigure. If a link fails then it separates the node connected to link from the network and the network continues to function. However, if the hub goes down, the entire network collapses.

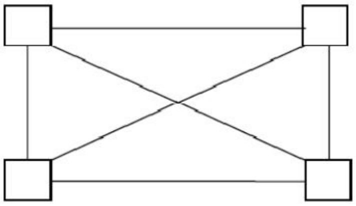
4. Tree Topology:

Tree topology is a hierarchy of various hubs. The entire nodes are connected to one hub or the other. There is a central hub to which only a few nodes are connected directly. The central hub, also called active hub, looks at the incoming bits and regenerates them so that they can traverse over longer distances. The secondary hubs in tree topology may be active hubs or passive hubs. The failure of a transmission line separates a node from the network.

5. Mesh Topology:

A mesh topology is also called complete topology. In this topology, each node is connected directly to every oilier node in the network. That is if there are n nodes then there would be n(n — 1)/2 physical links in the network.

As there are dedicated links, the topology does not have congestion problems. Further it does not need a special Media Access Control (MAC) protocol to prevent simultaneous access to the transmission media since links are dedicated, not shared. The topology also provides datasecurity. The network can continue to function even in the failure of one of the links. Fault identification is also easy. The main disadvantage of mesh topology is the complexity of the network and the cost associated with the cable length. The mesh topology is not useful for medium to large networks.



6. Hybrid Topology:

Hybrid topology is formed by connecting two or more topologies together. For example, hybrid topology can be created by using the bus, star and ring topologies.

c. Why does ethernet specify a minimum frame size? (4)

Answer:

the current frame, which means that stray bits and pieces of frames appear on the cable all the time . To make it easier to distinguish valid frames from garbage, Ethernet specifies that valid frame must be atleast 64 bytes long from destination address Ethernet frame specifies a minimum frame size of 46 bytes . While a data field of zero byte is legal , it causes a problem . When a transceiver detects a collision , it truncates to checksum . If data portion of frame is less the pad field is used to fill out the frame to the minimum size .

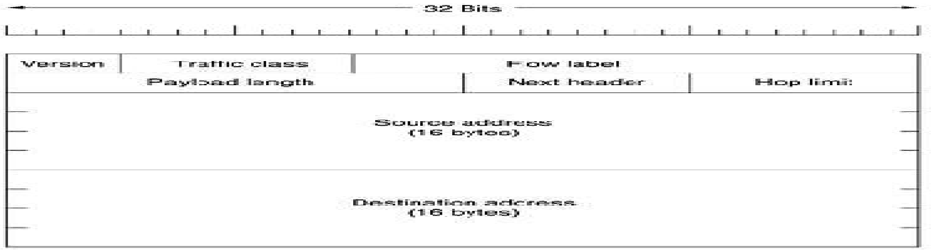
Q.8 a. What is IPv6? Explain its advantages over IPv4. Also explain its frame format. (8)

Answer:

IPv4 provides the host-to-host communication between systems in the Internet. Although IPv4 is well designed, data communication has evolved since the inception of IPv4 in the 1970s. IPv4 as some deficiencies that make it unsuitable for the fast-growing Internet.

- Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.
- The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.
- The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

To overcome these deficiencies, IPv6 (Internetworking Protocol, version 6), also known as IPng (Internetworking Protocol, next generation), was proposed and is now a standard. In IPv6, the Internet protocol was extensively modified to accommodate the unforeseen growth of the Internet. The format and the length of the IP address were changed along with the packet format. Related protocols, such as ICMP, were also modified. Other protocols in the network layer, such as ARP, RARP, and IGMP, were either deleted or included in the ICMPv6 protocol (see Chapter 21). Routing protocols, such as RIP and OSPF (see Chapter 22), were also slightly modified to accommodate these changes. Communications experts predict that IPv6 and its related protocols will soon replace the current IP version. In this section first we discuss IPv6. Then we explore the strategies used for the transition from version 4 to version 6. The adoption of IPv6 has been slow. The reason is that the original motivation for its development, depletion of IPv4 addresses, has been remedied by short-term strategies such as classless addressing and NAT. However, the fast-spreading use of the Internet, and new services such as mobile IP, IP telephony, and IP-capable mobile telephony, may eventually require the total replacement of IPv4 with IPv6.



IPv6 Packet Format

1. Version (4 bits)
   The constant 6 (bit sequence 0110).
2. Traffic Class (8 bits)
   The bits of this field hold two values. The 6 most-significant bits are used for DSCP, which is used to classify packets. The remaining two bits are used for ECN, priority values subdivide into ranges: traffic where the source provides congestion control and non-congestion control traffic.
3. Flow Label (20 bits)
   Originally created for giving real-time applications special service. Flow Label specifications and minimum requirements are described, and first uses of this field are emerging.
4. Payload Length (16 bits)
   The size of the payload in octets, including any extension headers. The length is set to zero when a Hop-by-Hop extension header carries a Jumbo Payload option.
5. Next Header (8 bits)
   Specifies the type of the next header. This field usually specifies the transport layer protocol used by a packet's payload, when extension headers are present in the packet this field indicates which extension header follows. The values are shared with those used for the IPv4 protocol field, as both fields have the same function (see List of IP protocol numbers).
6. Hop Limit (8 bits)
   Replaces the time to live field of IPv4. This value is decremented by one at each intermediate node the packet visits. When the counter reaches 0 the packet is discarded.
7. Source Address (128 bits)
   The IPv6 address of the sending node.
8. Destination Address (128 bits)
   The IPv6 address of the destination node(s)

b. What is the chief advantage of Classless Inter Domain Routing (CIDR) over the original classful addressing scheme? (8)

Answer:

CIDR (Classless Inter- Domain Routing) is a new addressing scheme for the Internet, which allows for more efficient allocation of IP address than the old classful scheme.

There are a maximum number of networks and hosts that can be assigned using 32-bit classful addressing scheme . Some addresses are reserved (for broadcasting etc.), and there were a lot of wasted addresses also.

For example if you needed 100 addresses you would be assigned the smallest class addresses (class C), but that still means 154 unused addresses. The overall result was Interest was running out of unassigned addresses.

A related problem was the size of the Internet global routing tables . As the number of networks on the Internet increased, so did the number of route.

Instead of being limited to network identifiers of 8 ,16 or 32 bits , CIDRcurrently uses prefixes anywhere between13 to 27. Thus, block of addresses can be assigned to networks as small as 32 hosts or to those with over 5000,000 hosts.A CIDR address includes standard 32-bit IP address and also information on how many bits are used for the network prefix .

In the CIDR address 206.13.01.48/25, the 25 indicate the first 25 bit s are used to identify the unique network leaving the remaining bits to identify the specific hosts .

CIDR addressing scheme also enables rout e-aggregation in which single high-level rout e entry can represent many lower level routes in the global routing table.

Q.9 a. When web pages containing emails are sent out they are prefixed by MIME Header. Why? (8)

Answer:

Initially email consisted messages containing simple text written in English and expressed in ASCII. Now a days on worldwide internet messages can be sent in languages with accents like French and German, languages without alphabet like Chinese and Japanese etc . the basic idea of MIME is to add structure to the message body and define encoding rule for non-ASCII messages .

MIME defines five additional message headers to the RFC822 format.

Header	Meaning
MIME Version	Identifies the MIME version
Content Description	Readable string telling about mess age
Content-ID	Unique Identifier
Content transfer encoding	How the body is wrapped for transmission
Content Type	Nature of the message

b. What is the advantage of dividing an email address into two parts? (4)

Answer:

The division of an e-mail address into two parts is important because it achieve two goals . First, the division allows each computer system to assign mailbox identifiers independently. Second, the division permits the user on arbitrary computer systems to exchange e-mail messages . E-mail software on the sender's computer uses the second part to determine which computer to contact, and the e-mail soft are on the recipient computer uses the first part of the address to select a particular mailbox into which message should be placed .

c. Can SMTP be used as transfer protocol for Web pages? Why? (4)

Answer:

SMTP is a simple mail transfer protocol. It uses ASCII text for all communication.SMTP requires reliable delivery-the sender must keep a copy of the message until the receiver has stored a copy in nonvolatile memory.

SMTP can not be used as transfer protocol for web pages as it is not necessarily use hypertext and its header needs information of sender and receiver mail ID which is not required for web pages.

Text Book

1. Data and Computer Communication , Eight Edition (2007), William Stallings, Pearson Education Low Price Edition .