LORDS™

Refresher on
COMPUTER NETWORKS-I
(BTCS-403)

WITH UPTO-DATE PREVIOUS QUESTION PAPERS CHAPTERWISE
& LORDS MODEL TEST PAPERS (UNSOLVED)

For

B.E., B.Tech (P.T.U/M.R.S.S.T.U)

4th Semester

(Computer Science Engg. & Information Technology

New Edition February 2017

By

DEEPIKA VADHERA

LORDS PUBLICATIONS™

36, Chandan Nagar, Jalandhar City.

Published by :

For LORDS PUBLICATIONS™

36, Chandan Nagar, Jalandhar.
Tel. : 0181-2621630
Mob. : 98781-31031, 98154-65088

New Edition February 2017

PRICE ₹ 115.00

ISBN : 978-93-81184-79-0

As publishers, we have tried our best to serve the student with the best of our resources. We have taken great care to eliminate all possible errors However, if readers want to give suggestion of any kind that will be welcomed by us. For suggestions please contact us on our male ID : lordspub2007@gmail.com

Sole Distributor for Chandigarh :

JOGINDRA BOOK DEPOT
SCF 7, Sec. 27-D, CHANDIGARH
Ph. : 0172-4623895

MOHINDRA BOOK DEPOT
SCO 41, Sec. 31-D, CHANDIGARH
Ph. : 0172-2601550, 5002746

Sole Distributor for Ambala :

SUNIL BOOK DEPOT
Main Market, LALRU MANDI
Ph. : 01762-274185 Mob. : 9888555722

Typesetting by : Sunshine Computers, Jalandhar.

Printed at : Dolphin Printers, Jalandhar.

~ Syllabus ~

PART-A

1. INTRODUCTION TO COMPUTER NETWORKS

Data Communication System and its components, Data Flow, Computer network and its goals, Types of computer networks: LAN, MAN, WAN, Wireless and wired networks, broadcast and point to point networks, Network topologies, Network software: concept of layers, protocols, interfaces and services, ISO-OSI reference model, TCP/IP reference model.

2. PHYSICAL LAYER

Concept of Analog & Digital Signal, Bandwidth, Transmission Impairments: Attenuation, Distortion, Noise, Data rate limits : Nyquist formula, Shannon Formula, Multiplexing : Frequency Division, Time Division, Wavelength Division, Introduction to Transmission Media : Twisted pair, Coaxial cable, Fiber optics, Wireless transmission (radio, microwave, infrared), Switching: Circuit Switching, Message Switching ,Packet Switching & their comparisons.

3. DATA LINK LAYER

Design issues, Framing, Error detection and correction codes: checksum, CRC, hamming code, Data link protocols for noisy and noiseless channels, Sliding Window Protocols: Stop & Wait ARQ, Go-back-N ARQ, Selective repeat ARQ, Data link protocols: HDLC and PPP.

4. MEDIUM ACCESS SUB-LAYER

Static and dynamic channel allocation, Random Access: ALOHA, CSMA protocols, Controlled Access: Polling, Token Passing, IEEE 802.3 frame format, Ethernet cabling, Manchester encoding, collision detection in 802.3, Binary exponential back off algorithm.

PART-B

5. NETWORK LAYER

Design issues, IPv4 classful and classless addressing, subnetting, Routing algorithms: distance vector and link state routing, Congestion control: Principles of Congestion Control, Congestion prevention policies, Leaky bucket and token bucket algorithms.

6. TRANSPORT LAYER

Elements of transport protocols: addressing, connection establishment and release, flow control and buffering, multiplexing and de-multiplexing, crash recovery, introduction to TCP/UDP protocols and their comparison.

7. APPLICATION LAYER

World Wide Web (WWW), Domain Name System (DNS), E-mail, File Transfer Protocol (FTP), Introduction to Network security.

~ Contents ~

PUNJAB TECHNICAL UNIVERSITY QUESTION PAPERS

UNIVERSITY QUESTION PAPER, DEC.–2012

SECTION-A

Q 1. (a) Compare LAN and MAN.

Ans. *Refer to Chapter No. 1 Q.No. 12 on Page No. 5*

(b) What are the disadvantages of bus topology?

Ans. *Refer to Chapter No. 1 Q.No. 65 on Page No. 24*

(c) What is a protocol?

Ans. *Refer to Chapter No. 1 Q.No. 66 on Page No. 25*

(d) What is the difference in UTP and STP cable?

Ans. *Refer to Chapter No. 2 Q.No. 68 on Page No. 55*

(e) List the different error detection codes.

Ans. *Refer to Chapter No. 3 Q.No. 57 on Page No. 78*

(f) What is a hamming distance?

Ans. *Refer to Chapter No. 3 Q.No. 56 on Page No. 78*

(g) What is IEEE 802.4 standard?

Ans. *Refer to Chapter No. 4 Q.No. 27 on Page No. 92*

(h) Compare switch and router.

Ans. *Refer to Chapter No. 5 Q.No. 52 on Page No. 121*

(i) Define the term collision in data communication.

Ans. *Refer to Chapter No. 6 Q.No. 11 on Page No. 98*

(j) What is a firewall?

Ans. *Refer to Chapter No. 7 Q.No. 9 on Page No. 141*

SECTION-B

Q 2. Explain the process of signal transmission in optical fibre.

Ans. *Refer to Chapter No. 2 Q.No. 70 on Page No. 56*

Q 3. Difference between pure ALOHA and slotted ALOHA.

Ans. *Refer to Chapter No. 4 Q.No. 9 on Page No. 85*

Q 4. Compare IEEE standard 802.3 and 802.4.

Ans. *Refer to Chapter No. 4 Q.No. 8 on Page No. 84*

Q 5. Explain the working of leaky bucket congestion control algorithm.

Ans. *Refer to Chapter No. 5 Q.No. 41 on Page No. 114*

Q 6. How TCP is different from UDP? Which of the two protocols is more favourable for real time applications and why?

Ans. *Refer to Chapter No. 6 Q.No. 8 on Page No. 127*

SECTION-C

Q 7. Compare OSI and TCP/IP models.

Ans. *Refer to Chapter No. 1 Q.No. 64 on Page No. 24*

Q 8. Explain the working of sliding window flow control using diagram.

Ans. *Refer to Chapter No. 3 Q.No. 59 on Page No. 79*

Q 9. Write short notes on :

(a) DNS

Ans. *Refer to Chapter No. 7 Q.No. 8 on Page No. 139*

(b) Email.

Ans. *Refer to Chapter No. 7 Q.No. 11 on Page No. 141*

UNIVERSITY QUESTION PAPER, MAY–2013

SECTION-A

Q 1. (a) What is difference between http and https?

Ans. HTTP is used mainly to access data on www. This protocol transfer data in the form of plain text, hypertext audio, video etc. The function of HTTP is like a combination of PPP and SMTP. HTTP's is a secure socket layer. It is basically used to secure the information.

(b) Difference between LAN, MAN and WAN.

Ans. *Refer to Chapter No. 1 Q.No. 30 on Page No. 11*

(c) What are the different types of cryptography?

Ans. There are few basic types of cryptography :

1. Encryption	Symmetric cipher
3. Decryption	Public key cryptography
3. Key	One time pad
4. Secure line	Steganography
5. Public line	

(d) What is difference between simplex and half duplex?

Ans. *Refer to Chapter No. 1 Q.No. 13 on Page No. 6*

(e) Give some examples of serial devices.

Ans. Devices in linux have major and minor numbers. The serial port HySx (X = 0, 1, 2 etc.) is major number 4. You can see this by typing "ls – 1 Hy S" in the /dev directory. To see the devices names for various devices, see the devices file in Kernel documentation.

(f) On which layer do switches and routers work?

Ans. Router : It can connect two or more networks.

Switch : It is a point to point device.

Both router and switches are used in network layer.

(g) What is need of modems?

Ans. A modem (modulator-demodulator) is a device that modulates an analog carrier signal to encode digital information, and also demodulates such as carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data.

(h) IP defines how many bits for representing an IP and MAC address?

Ans. MAC address (Media Access Control) is a 48-bit or 64-bit address associated.

IP address (Internet protocol) is 32 bit or 64 bit address associated.

(i) How are VLANs useful?

Ans. VLAN is a virtual LAN (where LAN is short for local area network). The virtual LAN is pretty much what is sounds like – a virtual separate network, but across the save physical network.

(j) How many bits are consumed by IPV4 and IPV6 addresses respectively?

Ans. IPV4 contains 32 bits (four byte) addresses which limits the address space to 4294967296 (232) addresses.

IPV6 contains 128 bits.

SECTION-B

Q 2. Which of the following address does not belong to the same network? Explain why?

1. **130.31.23.31**
2. **130.31.24.22**
3. **130.32.23.21**
4. **130.31.21.23**

Ans. 1. 130.31.23.31 – The subnet mask i.e. network mask is 255.255.255.**254**
2. 130.31.24.22 – The subnet mask i.e. network mask is 255.255.255.**0**
3. 130.32.23.21 – The subnet mask i.e. network mask is 255.255.255.**0**
4. 130.31.21.23 – Network mask is 255.255.255.**0**

Q 3. What are two reasons for using layered protocols? What do you mean by link to link layers of OSI reference model? Explain their functions briefly.

Ans. 1. Addressing : For every layer, it is necessary to have a mechanism to identify senders and receivers. Since there are multiple possible destinations, some form of addressing is required in order to specify a specific destination.

2. Direction of Transmission : Another point is the direction of data transfer. Based on whether the system communications only in one direction or otherwise, the communication systems are classified as under :

(i) Simplex System (ii) Half Duplex System (iii) Full Duplex System.

3. Error Control : Physical communication circuits are not perfect. Error detection and connection both are essential. Many error detecting and correcting codes are known out of which those agreed by sender and receiver should be used. The receiver should be able to tell the sender by some means, that it has received a correct message.

4. Avoid Loss of Sequencing : All the communication channels cannot preserve the order in which messages are sent on it. So there is a possibility of loss of sequencing. To avoid this, all the pieces should be numbered so that they can be put back together at the receiver in the appropriate sequence.

5. Ability of Receiving Long Messages : At several levels, another problem should be solved which is inability of all processes to accept arbitrarily long messages. So, a mechanism needs to be developed to disassemble transmit and then reassemble message.

Host to host : Data Link Layer :

1. It provides synchronization and error control for the information which is to be transmitted over the physical link.
2. To enable the error detection, it adds error detection bits to the data which is to be transmitted.
3. The encoded data is then passed to the physical layer.
4. There error detection bits are used by the data link or other side to detect the correct errors.

Q 4. Identify the address class of following IP addresses : 200.58.20.165 ; 128.167.23.20 ; 16.196.128.50 ; 50.156.10.10 ; 250.10.24.96.

Ans. 200.58.20.165

11001000.00111010.00010100.10100101

Class C

128.167.23.20
10000000.10100111.00010111.00010100
Class B

16.196.128.50
00010000.11000100.10000000.00110010
Class A

150.156.10.10
10010110.10010110.00000010.00000010
Class B

250.10.24.96
11111010.00000010.00011000.01100000
Class E

Q 5. Explain the physical and logical structrue of Internet. Explain how the DNS allows a large number of DNS lookups to be processed.

Ans. ❑ Register its name in DNS.

- ❑ Name resolution.
- ❑ Caching response to name resolution queries.
- ❑ Removes previously names from the cache when it receives a negative response for the name.
- ❑ Negative caching.
- ❑ Keep track of transistory.
- ❑ Maintain connection-specific domain name suffixes.

Q 6. Contrast link state and distance vector routing protocols, giving an example of each. What is count to infinity problem?

Ans. *Refer to Chapter No. 5 Q.No. 31 & 40 on Page No. 107 & 112*

SECTION-C

Q 7. (a) What is packet switching? Explain two different approaches to packet switching.

Ans. *Refer to Chapter No. 2 Q.No. 36 on Page No. 40*

(b) Discuss the different factors affecting congestion control algorithms.

Ans. *Refer to Chapter No. 5 Q.No. 42 on Page No. 115*

Q 8. (a) Suppose a machine is attached to several physical networks. Why does it need a different IP address for each attachment?

Ans. *Refer to Chapter No. 5 Q.No. 39 on Page No. 111*

(b) Suppose a computer is moved from CSE Department to Electrical Department in same engineering college. Does the physical address need to change? Does the IP address need to change? Does it make a difference that the machine is a desktop or a laptop?

Ans. It will depend upon the layout of your network. If the other department is on the same building its highly unlikely that you have to change the address if does matter you using static or DHCP.

Q 9. Explain pure-ALHOA and slotted-ALOHA systems. Give the expression for throughout for each, clearly explaining the various terms. Explain 1-persistent, p-persistent and 0-persistent CSMA giving strong and weak points of each.

Ans. *Refer to Chapter No. 4 Q.No. 5 & 6 on Page No. 82 & 83*

UNIVERSITY QUESTION PAPER, DEC.–2013

SECTION-A

Q 1. (a) What is the difference between the protocol ARP and RARP?

Ans. ARP : Address Resolution Protocol is utilized for mapping IP network address to the hardware address that user data link protocol.

RARP : Reverse Address Protocol is a protocol using which a physical machine in a LAN could request to find its IP address from ARP table or cache from a gateway server.

(b) Explain as to how error detection at the data link level is achieved.

Ans. *Refer to Chapter No. 3 Q.No. 29 on Page No. 66*

(c) What does the subnet mask : 255.255.255.0 signifies?

Ans. 255.255.255.0 subnet mask if of a class it signifies

11111111.11111111.11111111.00000000

(Binary)

(d) In OSI network architecture, the dialogue control and token management are responsibilities of which layer?

Ans. In session layer the dialogue control and token management are responsible.

(e) Four bits are used for packed sequence numbering in a sliding window protocol used in a computer network. What is the maximum window size?

Ans. It depends upon what kind of sliding window protocol are we using for

(i) Selective repeat window size here will be

(ii) For go back n window size will be

$$16 - 1 = 15$$

maximum size is 15.

(f) What is the difference between simplex and half duplex?

Ans. *Refer to Chapter No. 1 Q.No. 13 on Page No. 6*

(g) Which protocol is used for sending email on the internet?

Ans. SMTP protocol is used for sending email on the internet?

(h) IP defines how many bits for representing an IP and MAC address?

Ans. MAC address (Media Access Control) is a 48-bit or 64-bit address associated IP address (Internet protocol) is 32 bit or 64-bit address associated.

(i) What are the two types of transmission technology available?

Ans. Two types of transmission technology are :

- Broadband
- Point to point.

(j) What is the difference between the communication and transmission?

Ans. Transmission is a kind of one way data transfer but communication is a two way interactive process in which all the participants actively share their data.

SECTION-B

Q 2. What are the various transmission media available? State advantages and disadvantages of each.

Ans. *Refer to Chapter No. 2 Q.No. 66 & 69 on Page No. 53 & 55*

Q 3. Explain different methods of error detection and error correction. Which method requires more number of bits and why?

Ans. *Refer to Chapter No. 3 Q.No. 44 on Page No. 72*

Q 4. (a) What is the difference between the bit rate and baud rate of a signal?

Ans. Bit rate : Bit rate is measure of the number of the data bits (0 and 1) transmitted in one second.

Baud rate : Baud rate means the number of times a signal in a communication channel changes state.

(b) What are the advantages and disadvantages for static and dynamic channel allocation?

Ans. *Refer to Chapter No. 4 Q.No. 3 & 4 on Page No. 82*

Q 5. Describe how email works. Describe the key components and flows. Identify key standards that apply.

Ans. *Refer to Chapter No. 7 Q.No. 11 on Page No. 141*

Q 6. Why is multiple access required in LAN technologies? Compare FDM, TDM, and SDM in terms of their ability to handle groups of stations.

Ans. *Refer to Chapter No. 2 Q.No. 33 on Page No. 38*

SECTION-C

Q 7. (a) What is the difference between congestion control and flow control?

Ans. *Refer to Chapter No. 5 Q.No. 41 on Page No. 114*

(b) Give one advantage and one disadvantage of window-based flow control vs. rate-based flow control.

Ans. *Refer to Chapter No. 5 Q.No. 29 on Page No. 107*

Q 8. (a) List two reasons why intra-domain routing protocols are not suitable for inter-domain routing.

Ans. *Refer to Chapter No. 5 Q.No. 9 on Page No. 97*

(b) Why does distance-vector routing scale better than link-state routing?

Ans. *Refer to Chapter No. 5 Q.No. 30 on Page No. 107*

Q 9. (a) What is a bridge? What is a switch? What are the motivations to use bridges and switches?

Ans. A bridge is a device that separates two or more network segments within one logical network (e.g. a single IP-subnet).

A bridge is usually placed between two separate groups of computers that talk with each other, but not that much with the computers in the other group. A good example of this is to consider a cluster of macintoshes and a cluster of unix machines. Both of these groups

of machines tend to be quite chatty amongst themselves, and the traffic they produce on the network causes collisions for the other machines who are typing to speak to one another.

A switch is a device for making and breaking the connection in an electric circuit. An act of changing to or adopting one thing in place of another. In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer and sometimes the network switch.

(b) Describe the forwarding and learning algorithm for transparent bridges.

Ans. *Out of syllabus.*

UNIVERSITY QUESTION PAPER, MAY–2014

SECTION-A

Q 1. (a) List the important features of WAN.

Ans. List of the important features of WAN

1. Hardware is spread over a wide geographical area : A WAN consists of terminal and computing equipment connected over a large area, usually in excess of two kilometres.

2. Third party telecommunication equipment is used : Because the hardware is spread out, telephone, radio or satellite communication links are used, which the organisation does not own. Telecommunication companies provide the links and each of these has its own rules, regulations and service charges.

(b) What is attenuation ?

Ans. Attenuation refers to decreasing in signal magnitude between two points. These points may be along a radio path, transmission line or other devices.

(c) Define noise.

Ans. *Refer to Chapter No. 2 Q.No. 12 on Page No. 30*

(d) What is framing ?

Ans. *Refer to Chapter No. 3 Q.No. 6 on Page No. 59*

(e) Differentiate between static and dynamic channel allocation.

Ans.

Point of difference	Static Channel allocation	Dynamic Channel allocation
1. Performance	Better under heavy traffic	Better under low/moderate traffic
2. Flexibility in channel allocation	Nil	High
3. Suitability	Suitable for large networks	Suitable for small/medium sized networks.
4. Overall flexibility	Low	High
5. Suggested application	Long-duration voice calls	Voice calls of short duration data transmission
6. Management overheads	Low	High
7. Call/Transmission set-up delay	Low	High
8. Signaling load	Low	High
9. Control	Centralized	Centralized or distributed.

(f) Differentiate between leaky bucket and token bucket algorithms.

Ans. *Refer to Chapter No. 5 Q.No. 19 on Page No. 102*

(g) What is silly windows syndrome in TCP ?

Ans. Silly window syndrome is a problem in computer networking caused by poorly-implemented TCP flow control. If a server with this problem is unable to process all incoming data, it requests that its clients reduce the amount of data they send at a time (the "window" setting on a TCP packet). If the server continues to be unable to process all incoming data, the window becomes smaller and smaller, sometimes to the point that the data transmitted is smaller than the packet header, making data transmission extremely inefficient. The name of this problem is due to the window size shrinking to a "silly" value.

Silly window syndrome is avoided by

- The receiver not advertising small windows, this is accomplished by not advertising a larger window until the window size can be increased by either one maximum segment size or by 1/2 of the remote host's current window size.
- The sender must not transmit data unless :
- A packet is at least as large as the maximum segment size.
- A packet with data which is half of the remote host's window size may be sent.
- All of the output data may be sent and there is no unacknowledged data or the NAGLE algorithm is disabled.

(h) Define ports at transport layer.

Ans. Each process that wants to communicate with another process identifies itself to the TCP/IP protocol suite by one or more ports. A port is a 16-bit number, used by the host-to-host protocol to identify to which higher level protocol or application program (process) it must deliver incoming messages.

There are two types of port :

- **Well Known :** Well-known ports belong to standard server, for example, Telnet uses port 23. Well known port numbers range between 1 and 1023.
- **Ephemeral :** Ephemeral port numbers have values greater than 1023, normally in the range 1024 to 65535.

(i) List the important features of MIME .

Ans. The MIME standard provides several important features such as :

- Specifications for other character sets.
- Definitions for content types such as applications, images, and other multimedia files types.
- A method to include several different objects with in a single message.
- An extended set of possible headers.
- Standard encoding methods such as base64 and quote printable

(j) What is Manchester encoding ?

Ans. Manchester encoding, also known as Phase Encoding (PE), is a synchronous clock encoding technique used by the physical layer to encode the clock and data of a synchronous bit stream.

Manchester encoding is used in the Ethernet media systems. Manchester coding provides a simple way to encode arbitrary binary sequences without ever having long periods without level transitions, thus preventing the loss of clock synchronisation, or bit errors from low frequency drift on poorly-equalized analog links. In this technique, the actual binary data to be transmitted over the cable are not sent as a sequence of logic 1's and 0's (known technically as non Return to zero (NRZ)). Instead, the bits are translated into a slightly different format that has a number of advantages over using straight binary encoding (i.e. NRZ)

SECTION-B

Q 2. Compare the important features of OSI model and TCP/IP architecture.

Ans. *Refer to Chapter No. 1 Q.No. 64 on Page No. 24*

Q 3. State and explain the Shannon theorem. What are its uses ?

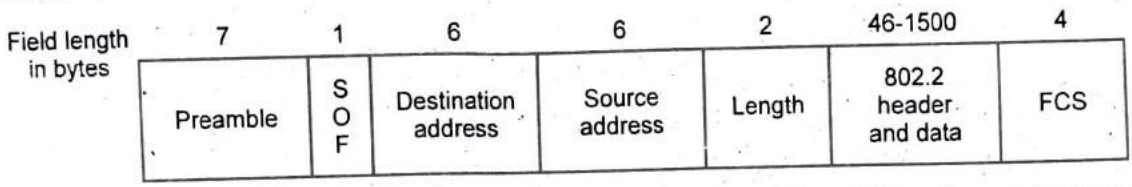
Ans. *Refer to Chapter No. 2 Q.No. 28 on Page No. 36*

Q 4. Explain the design issues of data link layer.

Ans. *Refer to Chapter No. 3 Q.No. 2 on Page No. 58*

Q 5. Explain the meaning of various fields of IEEE 802.3 frame format.

Ans.



SOF = Start-of-frame delimiter ; FCS = Frame check sequence

802.3 frame begin with an alternating pattern of Is and 0s called a preamble.

The preamble tells receiving stations that a frame is coming.

The byte before the destination address in an IEEE 802.3 frame is a start-of-frame (SOF) delimiter.

This byte ends with two consecutive one bits, which serve to synchronize the frame reception portions of all stations on the LAN.

Immediately following the preamble in IEEE802.3 LANs are the destination and source address fields.

IEEE 802.3 addresses are 6 bytes long. Addresses are contained in hardware on the IEEE 802.3 interface cards. The source address is always a unicast (single node) address, while the destination address may be unicast, Multicast (group), or broadcast (all no des).

In IEEE 802.3 frames, the 2-byte field following the source address is a length field, which indicates the number of bytes of data that follow this field and precede the frame check sequence (FCS) field.

Following the length field is the actual data contained in the frame. After physical layer and link-layer processing is complete, this data will eventually be sent to an upper-layer protocol. In the case of IEEE 802.3, the upper-layer protocol must be defined with in the data portion of the frame, if at all. If data in the frame is insufficient to fill the frame to its minimum 64-byte size, padding bytes are inserted to ensure at least a 64-byte frame.

After the data field is a 4-byte FCS field containing a cycle redundancy check (CRC) value. The CRC is created by the sending device and recalculated by the receiving device to check for damage that might have occurred to the frame in transit.

Q 6. Explain the meaning of various fields of UDP header.

Ans.

UDP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source Port																Destination port															
4	32	Length																Checksum															

The UDP header consists of four fields, each of which is 2 (bytes) 16 bits.

Source port : This field identifies the sender's port when meaning ful and should be assumed to be the port to reply to if needed. It not used, then it should be zero. If the source host is the client, the port number is likely to be an ephemeral port number. If the source host is the server, the port number is likely to be a well-known port number.

Destination port : This field identifies the receiver's port and is required. Similar to source port number, if the client is the destination host then the port number will likely be an ephemeral port number and if the destination host is the server then the port number will likely be a well-known port number.

Length : A field that specifies the length in bytes of the UDP header and UDP data. The minimum length is 8 bytes since that's the length of the header. The field size sets a theoretical limit of 65,535 bytes (8 byte header + 65,527 bytes of data) for a UDP datagram.

Checksum : The checksum field is used for error checking of the header and data. If no checksum is generated by the transmitter, the field uses the value all-zero.

SECTION-C

Q 7. What is distance vector routing ? Explain the steps involved with suitable example.

Ans. It is a routing protocol used in routing of packet switched networks in computer communications. They use the Bellman Ford Algorithm examples of distance-vector routing protocols include RIPv1 or 2 and IGRP.

The distance vector routing protocol assumes a network connected through several routers, each of which is connected to two or more computer networks. Each network may be connected to one or more routers.

The description below describes a very simple distance-vector routing protocol :

1. In the first stages, the router makes a list of which networks it can reach, and the cost to reach them (cost is protocol dependent, in RIP case, the cost is measured by number hops). In the outset this will be the two or more networks to which this router is connected.

The number of hops for these networks will be 1. This table is called a routing table.

2. Periodically (typically every 30 seconds) the routing table is shared with other routers on each of the connected networks via some specified inter-router protocol. These routers will add 1 to every hop-count in the table, as it associates a hop cost of 1 for reaching the router that sent the table. This information is just shared between physically connected routers ("neighbors"), so routers on other networks are not reached by the new routing tables yet.

3. A new routing table is constructed based on the directly configured network interfaces, as before, with the addition of the new information received from other routers. The hop-count is used as a cost measure for each path. The table also contains a column stating which router offered this hop count, so that the router knows who is next in line for reaching a certain network.

4. Bad routing paths are then purged from the new routing tables. If two identical paths to the same network exist, only the one with the smallest hop-count is kept. When the new table has been cleaned up, it may be used to replace the existing routing table used for packet forwarding.

5. The new routing table is then communicate to all neighbors of this router. This way the routing information will spread and eventually all routers know the routing path to each network, which router, it shall use to reach this network and to which router it shall route next.

Distance vector routing protocols are simple and efficient in small netwoks, and require little,for management. However they do not scale well, and have poor convergence properties, which has led to the development of more complex but more scalable link state routing protocols for use in large networks. They suffer from the "Count to infinity problem".

Now let us explain its example IGRP (Interior Gateway Routing Protocol). It used by routers to exchange routing data within an autonomous system. IGRP was created in part to overcome the limitations of RIP (maximum hop count of only 15, and a single routing metric) when used within large netwroks. IGRP supports multiple metrics for each route, including bandwidth, load, delay and reliability ; to compare two routes these metrics are combined together into a single metric, using a formula which can be adjusted through the use of pre-set constants. The maximum hop count of IGRP routed packet is 255 (dafault 100). IGRP is considered a classful routing protocol. As the protocol has no filed for a subnet mask the router assumes is that all interface addresses have the same subnet mask as the router itself. This contrasts with classless routing protocols that can use variable length subnet mask. Classful protocols have become less popular as they are wasteful of ip address space. Its sucessor is EIGRP, that adds DUAL, ideas to the basic distance vector mechanism of IGRP.

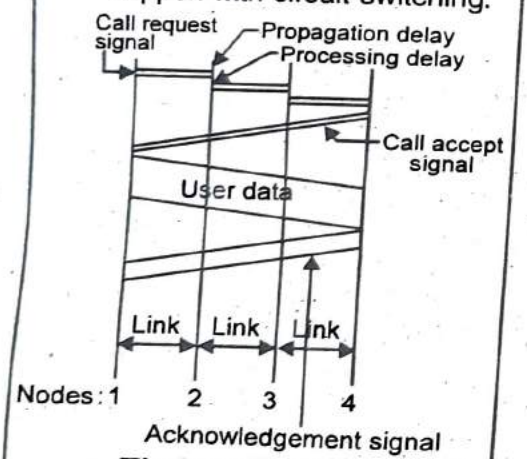
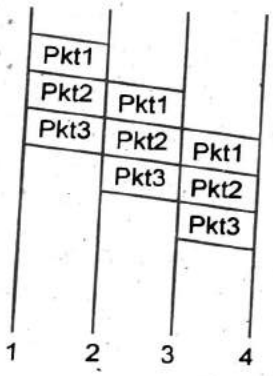
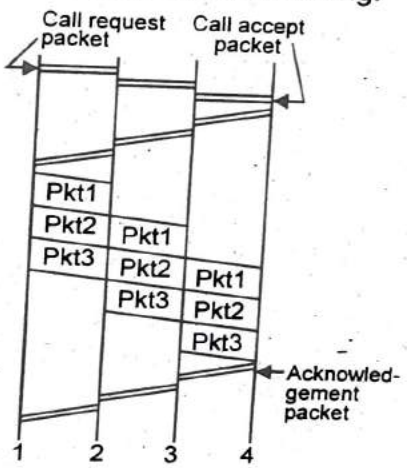
Q 8. What is sliding window ? Explain the various sliding window protocols for error and flow control with example.

Ans. *Refer to Chapter No. 3 Q.No. 49 on Page No. 74*

Q 9. What is Switching ? Compare circuit, message and packet switching.

Ans. Switching : *Refer to Chapter No. 2 Q.No. 23 on Page No. 33*

Comparison of circuit, packet and message switching :

Circuit Swithcing	Packet Switching	Message Swithcing
1. There is physical connection between transmitter and receiver.	No physical path is established between transmitter and receiver.	No physical path is set in advance between transmitter and receiver.
2. All the packet uses same path.	Packet travels independently.	Packets are stored and forward.
3. Needs an end to end path before the data transmission.	No needs of end to end path before data transmission.	Same as packet switching.
4. Reverses the entire bandwidth in advance.	Does not reverse the bandwidth in advance.	Same as packet switching.
5. Charge is based on distance and time, but not on traffic.	Charge is based on both number of bytes and connect time.	Charge is based on number of bytes and distance.
6. Waste of bandwidth is possible.	No waste of bandwidth.	No waste of bandwidth.
7. Congestion occur for per minute.	Congestion occur for per packet.	No congestion or very less congestion.
8. It cannot support store and forward transmission.	It support store and forward transmission.	It also support store and forward transmission.
9. Not suitable for handling interactive traffic.	Suitable for handling interactive traffic.	Same as circuit Switching.
10. Recording of packet can never happen with circuit switching.	Recording of packet is possible.	Same as packet switching.
 **Timing diagram**	 **Timing diagram**	 **Timing diagram**
11. Message to be transmitted is jn the form of packets	Message to be transmitted is in the form of packets.	Message to be transmitted is in the form of blocks.
12. Store-and-forward technique is not used.	Store-and-forward technique is used.	Store and froward technique is used.
13. It can be used with real-time applications	It can be used with real-time applications.	It cannot be used with real time applications.
14. It is used in telephone network for bi-directional fast and real-time data transfer.	It is used for the internet.	It was used in the transmission of voice signals and messages.

UNIVERSITY QUESTION PAPER, DEC.–2014

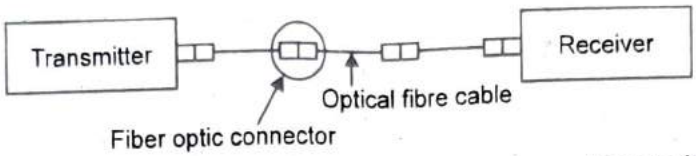
SECTION-A

Q 1. (a) What are the major advantages of STP over UTP ?

Ans. 1. STP has protective sheathing
2. STP offers better performance at lower data rates.
3. Less interference.

(b) Describe the components of fibre optic cable. Draw a picture.

Ans.



The basic elements found in fiber optic systems are a transmitter, fiber optic cable, receiver and connector.

Three components are required :

1. Light source : Typically a Light Emitting Diode (LED), or laser diode.

2. Fiber medium : Current technology carries light pulses for tremendous distance (e.g. 100s of Kilometers) with virtually no signal loss (i.e. no amplifiers or repeaters are needed)

3. Detector : Which detects the light and converts it to electric signals.

(c) What is the difference between network layer delivery and transport layer delivery?

Ans.

Network layer delivery	Transport layer delivery
1. The network layer is responsible for the source-to-destination delivery of packet across multiple network links.	1. The transport layer is responsible for source-to-destination delivery of the entire message.
2. The network layer must be present on all systems and delivers packets hop-by-hop between adjacent intermediate systems (routers or gateways or end systems (hosts).	2. The transport layer can technically be absent from intermediate systems and delivers packet content end-to-end between hosts.
3. The network layer is usually "unreliable" and connectionless.	3. The transport layer often adds a measure of reliability (such as resending missing or errored packet content) and connections to the network layer.
4. The network layer has the network address.	4. The transport layer focuses on ports and multiplexing application's traffic on the network.

(d) How can a device have more than one IP address ?

Ans. If a device has more than one interface to the internetwork, it will have more than

one IP address. The most obvious case where this occur is with routers, which connect together different network and thus must have an IP address for the interface on each one. It is also possible for hosts to have more than one IP address, however, such a device is sometimes said to be multihomed.

(e) Which control bit is involved in setting up a TCP session ?

Ans. A TCP/IP connection is made between two computers, using their address and, depending on the application using TCP, port numbers. The SYN and ACK bits in the TCP header are important components used to establish this initial connection.

(f) What are the factors that affects the data rate of a link ?

Ans. The data rate of a link depends on the type of encoding used and the bandwidth of the medium.

(g) What are the advantages of FDDI over a basic token ring ?

Ans.

- The data rate on FDDI is about 100Mbps whereas a Token ring supports only 4 or 16 Mbps.
- FDDI uses fiber optic cable, which is free of EMI, while Token Ring uses shielded twisted pair cable, which is more susceptible to noise.
- The distance over which a FDDI network can cover is much greater than that of a Token ring network.

(h) What is the purpose of the timer at the sender in systems using ARQ ?

Ans. The sender starts a timer when it sends a frame. If an acknowledgment is not received within an allotted time period, the sender assumes that the frame was lost or damaged and resends it.

(i) Is there any drawback of using piggybacking ?

Ans. The major drawback with piggybacking link protocol is that if the receiver (or sender) has no data frames to be transmitted, then the acknowledgment frames have to either wait until they fetch the packets from their respective network layer or transmit the acknowledgement frame separately. This obviously makes the protocol inefficient.

(j) How many bits are consumed by IPv4 and IPv6 addresses respectively ?

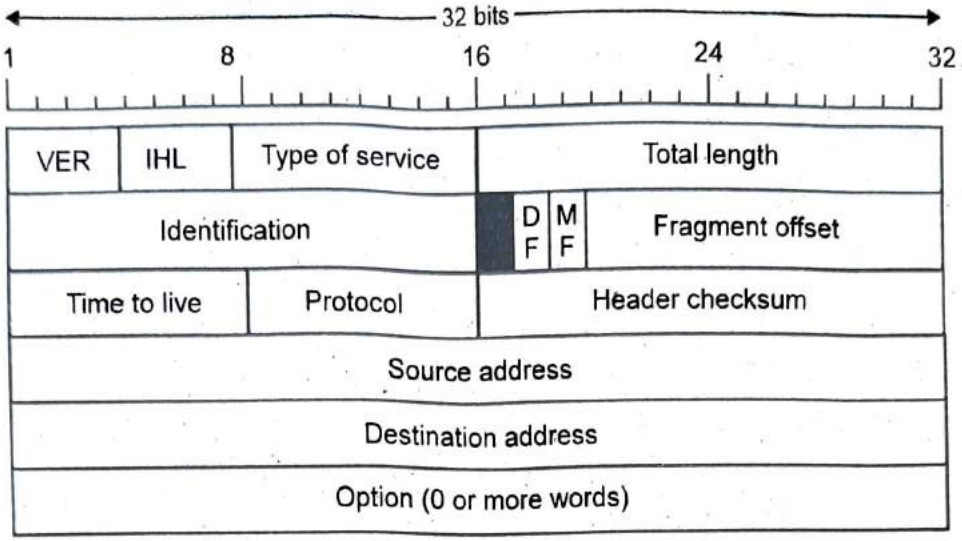
Ans. *Refer to Q.No. 1 (j) of May 2013.*

SECTION-B

Q 2. Draw the IP datagram header format. "IP datagram has a checksum field still it is called an unreliable protocol". Justify ?

Ans. Data transmitted over an internet using IP is carried in messages called IP datagrams. Like all network protocol messages, IP uses a specific format for its datagrams. We are of course looking here at IP version 4 and so we will examine the IPv4 datagram format, which was defined in RFC 791 along with the rest of IPv4. The IPv4 datagram is conceptually divided into two pieces : the header and the payload. The header contains addressing and control fields, while the payload carries the actual data to be sent over the internetwork. Unlike some message formats, IP datagrams do not have a footer following the payload.

The IP datagram header format :



Header Checksum : A checksum computed over the header to provide basic protection against corruption in transmission. This is not the more complex CRC code typically used by data link layer technologies such as Ethernet; it's just a 16-bit checksum. It is calculated by dividing the header bytes into words (a word is two bytes) and then adding them together. The data is not checksummed, only the header. At each hop the device receiving the datagram does the same checksum calculation and on a mismatch discards the datagram as damaged.

Q 3. What are the two reasons for using layered protocols ? What do you mean by link to link layers of OSI reference model ? Explain their functions briefly ?

Ans. *Refer to Q.No. 3 of May 2013*

Q 4. A binary signal is sent over a 3-khz channel whose signal-to-noise ratio is 20db. Calculate the maximum achievable data rate ?

Ans. In this we are given both the number of levels in the signal (binary, i.e. 2) and the signal-to-noise ratio of the channel. We therefore need to consider both the Nyquist limit and Shannon limit and take the lesser value as the answer.

From Shannon's theorem :

$$\text{Max Data Rate} = W\log_2\left(1+\frac{S}{N}\right)$$

Note that the signal to noise ratio (SNR) given here is a power ratio, yet we are given the SNR in decibels.

We therefore need to convert back to a power ratio :

$$\text{SNR in dB} = 10\log_{10}\left(\frac{S}{N}\right)$$

$$\text{therefore } \frac{S}{N} = 10^{(20/10)}$$

$= 100$

Therefore, the maximum data rate according to Shannon's theorem is :

$$\text{Max Data Rate} = W\log_2\left(1+\frac{S}{N}\right)$$

$$= 3000\times\log_2(1+100)$$

$$= 20\text{kbps}.$$

The Nyquist limit for binary signalling over a 3KHz channel is

$$\text{Max Data Rate} = 2W\log_2 M$$

$$= 2 \times 3000 \times \log_2 2$$

$$= 6\text{kbps}.$$

Therfore, the maximum achievable data rate is 6kbps.

(To achieve higher rates than this (up to the Shannon limit), one would have to use a different signalling method).

Q 5. Contrast link state and distance vector routing protocols, giving an example of each. What is count to infinity problem ?

Ans. *Refer to Chapter No. 5 Q.No. 31 & 40 on Page No. 107 & 112*

Q 6. How does a token ring network work ? In what way is it different from Ethernet?

Ans. A token ring network uses a special frame called a token that rotates around the ring when no stations are actively sending information. When a station wants to transmit on the ring, it must capture this token frame. The owner of the token is the only station that can transmit on the ring, unlike the Ethernet topology where any station can transmit at any time. once a station captures the token, It changes the token into a frame format so data can be sent. As the data traverses the ring, it passes through each station on the way to the destination station. Each station receives the frame and regenerates and repeats the frame on to the ring. As each station repeats the frame, it performs error checks on the information within the frame. If an error is found a special bit in the frame called the error detection bit is set so other stations will not report the same error.

Onces the data arrives at the destination station, the frame is copied to the destination's token ring card buffer memory. The destination station repeats the frame on to the ring, changing two series of bits on the frame. These bits, called the Address Recognized Indicator (ARI) and the Frame Copied Indicator (FCI), determines if the destination station had seen the frame and has had ample buffer space available to copy the frame into memory. If the frame is not copied into memory it is the responsibility of the sending station to retransmit the frame.

The frame continues around the ring, arriving back at the source station who recognizes the sending address as it's own. The frame is then stripped from the ring, and the source station sends a free token downstream. Token ring is single access, meaning there is only one token. Thus, at any given time only one station is able to use the LAN. Ethernet is a shared access medium, where all stations have equal access to the network at the same time.

SECTION-C

Q 7. (a) What is packet switching ? Explain two different approaches of packet switching ?

Ans. *Refer to Chapter No. 2 Q.No. 36 on Page No. 40*

(b) Discuss the different factors affecting congestion control algorithms ?

Ans. *Refer to Chapter No. 5 Q.No. 42 on Page No. 115*

Q 8. Consider the three-way handshake in TCP connection setup.

(a) Suppose that an old SYN segment from station A arrives at station B, requesting a TCP connection. Explain how the three-way handshake procedure ensures that the connection is rejected.

(b) Now suppose that an old SYN segment from station A arrives at station B; followed a bit later by an old ACK segment from A to a SYN segment from B.Is this connection request also rejected ?

Ans. (a) In a three - way handshake procedure, one must ensure the selection of the initial sequence number is always unique. If station B recives an Old SYN segment from A,B will acknowledge the request based on the old sequence number. When A receives the acknowledgement segment from B, A will find out that B received a wrong sequence number. A will discard the acknowledgement packet and reset the connection.

(b) If an old SYN segment from A arrives at B, followed by an old ACK segment from A to a SYN segment from B, the connection will also be rejected. Initially, when B receives an old SYN segment, B will send a SYN segment with its own distinct sequence number set by itself. If B receives the old ACK from A, B will notify A that the connection is invalid since the old ACK sequence number does not match the sequence number previously defined by B. Therefore, the connection is rejected.

Q 9. (a) If a size of a window is 3 bits, how many packets can be sent using Sliding Window protocol? Explain your answer. Explain the factors which will determine the length of the sliding window.

Ans. *Refer to Chapter No. 3 Q.No. 52 on Page No. 77*

(b) Explain the following ARQ technique in detail.

(i) Stop and wait ARQ

(ii) Selective repeat ARQ

Ans. *Refer to Chapter No. 3 Q.No. 49 on Page No. 74*

UNIVERSITY QUESTION PAPER, MAY–2015

SECTION-A

Q 1. (a) How does TCP differ from UDP ?

Ans. *Refer to Chapter No. 6 Q.No. 8 on Page No. 127*

(b) Differentiate between Polling and Token passing.

Ans. Polling : The mechanism of polling roll-call performed in a classroom. Just like the teacher, a controller, a controller sends a message to each node in turn. The message

contains the address of the node being selected for granting access. Although all nodes receive the message, only the addressed node responds and then it sends data, if any. If there is no data, usually a "poll reject" message is sent back. In this way, each node is interrogated in a round-robin fashion, one after the other, for granting access to the medium. The first node is again polled when the controller finishes with the remaining codes.

Token Passing : In token passing scheme, all stations are logically connected in the form of a ring and control of the access to the medium is performed using a token. A token is a special bit pattern or a small packet, usually several bits in length, which circulate from node to node. Token passing be used with both broadcast (token bus) and sequentially connected (token ring) type of network with some variation.

(c) For n devices in a network, what is the number of cable links required in Mesh and Bus topology ?

Ans. Mesh = $n(n-1)/2$

Bus = $n-1$

(d) Which class of IP addresses is used for multicasting ?

Ans. class D

(e) What do you mean by Packet Switched Network ?

Ans. *Refer to Chapter No. 2 Q.No. 55 on Page No. 46*

(f) A 10kHz baseband channel is used by digital transmission system. Ideal pulses are sent at the Nyquist rate, and the pulses can take 8 levels. What is the channel capacity of the system ?

Ans. $H = 1000$ Hz

Number of levels $V = 8$

Bandwidth = 10kHz

Therefore, Channel capacity according to Nyquist rate is

$= 2\log_2 V$ bits/sec $= 2\times10000\times\log_2 8$bits/sec

$= 20000 \times \log_{10} 8/\log_{10} 2$bits/sec

$= 20000 \times 0.903/0.301$ bits/sec

$= 20000 \times 3$bits/sec

$= 60000$ bits/sec

(g) What is the difference between connection oriented and connectionless services (give at least one example for each) ?

Ans.

S.No.	Connection oriented	Connection less
1.	A connection is established between sender and receiver.	No connection establishment.
2.	Packets are numbered.	Packets are not numbered.
3.	Acknowledgement for each packet.	No acknowledgement.

(h) What is the difference between WWW and FTP ?

Ans. *Refer to Chapter No. 7 Q.No. 1 & 16 on Page No. 138 & 144*

(i) Why IP version6 is required ?

Ans. Internet Protocol version 6 is a network layer protocol that enables data

communications over a packet switched network. IP version 6 was developed to increase the amount of available IP address space.

With its 128-bit address format, IPV6 can support 3.4×10^{38} or 340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456 unique IP addresses. This number of addresses is large enough to configure a unique address on every node in the internet and still have plenty of addresses left over. It is also large enough to eliminate the need for NAT, which has its own inherent problems.

IPV_6 has the following additional advantages :

- Simplified header-format for efficient packet handling.
- Larger payload for increased throughput and transport efficiency.
- Support for widely deployed routing protocols.
- Increased number of multicast addresses.

(j) A telephone line has a bandwidth of 3000Hz. Compute its data transfer capacity if the signal to noise ratio is 30dB.

Ans. *Refer to Chapter No. 2 Q.No. 28 on Page No. 36*

SECTION-B

Q 2. What do you mean by Switching ? Describe in brief the various switching methods.

Ans. *Refer to Chapter No. 2 Q.No. 59 on Page No. 49*

Q 3. Discuss the frame format of IEEE 802.3.

Ans. *Refer to Q.No. 5 of May 2014.*

Q 4. Explain the functioning of Go back-N protocol by taking some suitable example.

Ans. *Refer to Chapter No. 3 Q.No. 45 on Page No. 73*

Q 5. Describe in brief the design issues of Network layer.

Ans. *Refer to Chapter No. 5 Q.No. 1 on Page No. 94*

Q 6. Name various Error Detection and Correction techniques. Also find the CRC using a polynomial, P = 110011, for a given data, M = 11100011.

Ans. *Refer to Chapter No. 3 Q.No. 44 on Page No. 72*

CRC using a polynomial :

```
                1 0 1 1 0 1 1 0
            ---------------------
1 1 0 0 1 1 | 1 1 1 0 0 0 1 1 0 0 0 0 0
              1 1 0 0 1 1
              -----------
                1 0 1 1 1 1
                1 1 0 0 1 1
                -----------
                  1 1 1 0 0 0
                  1 1 0 0 1 1
                  -----------
                    1 0 1 1 0 0
                    1 1 0 0 1 1
                    -----------
                      1 1 1 1 1 0
                      1 1 0 0 1 1
                      -----------
CRC =                   1 1 0 1 0
```

SECTION-C

Q 7. Name various services and protocols of MAC layer. How CSMA/CD method handles the collisions and what should be the minimum size of the message. Discuss in detail.

Ans. Services of MAC layer :

1. Broadcast message control;
2. Connectionless message control;
3. Multi-bearer control.

Following Protocols are used by Medium Access layer :

1. ALOHA
2. Carrier Sensed Multiple Access (CSMA)
3. CSMA/CD (Carrier Sense Multiple Access/Collision Detection)
4. CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance etc)

CSMA/CD augments the algorithm to handle the collision.

Step 1 : Apply one of the persistent methods and a station sends a frame.

Step 2 : The station monitors the medium to see if the transmission was successful.

Step 3(1) : If transmission was successful, the station is finished.

Step 3(2) : If, however, a collision is detected.

- ❑ The station immediately aborts transmission.
- ❑ Send a Jamming signal that enforces the collision in case other stations have not yet sensed the collision.
- ❑ Wait T_B time, back-off, and go to STEP 1.

Where $T_B = T_P \times$ random $[0, 2^k-1]$ or $T_{fr} \times$ random $[0, 2^k-1]$

Where, K : Number of attempts

T_p : Maximum propagation time

T_{fr} : Average transmission time for a frame

T_B : Back-off time.

Q 8. Explain in detail the design issues of Transport layer.

Ans. *Refer to Chapter No. 6 Q.No. 2 on Page No. 125*

Q 9. Write short notes on any two :

(a) Time division Multiplexing

(b) Wireless Transmission Media

(c) Transmission Impairments

Ans. (a) *Refer to Chapter No. 2 Q.No. 60 on Page No. 50*

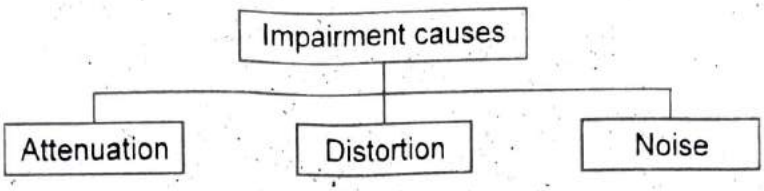
(b) Wireless medium is used in WLAN as well as in mobile and satellite communications. Wireless communication and wireless networks have evolved as a result of rapid development in communication technologies, computing and people's need for mobility. Wireless networks fall one of the following three categories depending on distance as follows :

- ❑ **Restricted Proximity Network :** This network involves local area networks (LANs) with a mixture of fixed and wireless devices.
- ❑ **Intermediate/Extended Network :** This wireless network is actually made up of two fixed LANs components joined together by a wireless component. The bridge may be connecting LANs in two nearby buildings or even further.

- **Mobile Network :** This is fully wireless network connecting two network elements. One of these elements is usually a mobile unit that connects to the home network (fixed) using cellular or satellite technology.

These three types of wireless networks are connected using basic media such as infrared, laser beam, narrow-band, and spread-spectrum radio, microwave and satellite communication.

(c) Transmission Impairments : Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise.



UNIVERSITY QUESTION PAPER, DEC.–2015

SECTION-A

Q 1. (a) Explain the term WWW.

Ans. *Refer to Chapter No. 7 Q.No. 1 on Page No. 138*

(b) Compare circuit, message and packet switching.

Ans. *Refer to Q.No. 9 of May 2014.*

(c) Compare pure and slotted Aloha protocols.

Ans. *Refer to Chapter No. 4 Q.No. 9 on Page No. 85*

(d) What is multiplexing ? Explain.

Ans. *Refer to Chapter No. 6 Q.No. 21 on Page No. 133*

(e) Briefly explain HDLC protocol.

Ans. *Refer to Chapter No. 3 Q.No. 43 on Page No. 71*

(f) What do you mean by Domain Name System ? Discuss.

Ans. *Refer to Chapter No. 7 Q.No. 29(i) & 30 on Page No. 149 & 150*

(g) What are CSMA protocols ? Discuss.

Ans. *Refer to Chapter No. 4 Q.No. 7 on Page No. 83*

(h) Discuss FTP protocol.

Ans. *Refer to Chapter No. 7 Q.No. 14 on Page No. 143*

(i) Discuss IEEE 802.3 frame format.

Ans. *Refer to Q.No. 5 of May 2014.*

(j) What is polling ? Discuss.

Ans. *Refer to Chapter No. 3 Q.No. 5 on Page No. 59*

SECTION-B

Q 2. Compare and contrast the two transport layer protocols : TCP and UDP.

Ans. *Refer to Chapter No. 6 Q.No. 14, 10 & 8 on Page No. 130, 128 & 127*

Q 3. Discuss the TCP/IP model with functioning of each layer.

Ans. *Refer to Chapter No. 1 Q.No. 40 on Page No. 14*

Q 4. Discuss the Leaky Bucket congestion control algorithm.

Ans. *Refer to Chapter No. 5 Q.No. 41 on Page No. 114*

Q 5. Explain the topologies used in a LAN. Write their advantages and disadvantages also.

Ans. Star, Bus and Ring are three commonly used topologies used in local area networks.

Star topology : All the connections radiate out from a common point. It means that all the modes and networked devices are directly and centrally connected to communication controller called hub. Each networked device in a star topology can access the media independently. All the networked devices shares the hub's available bandwidth. Failure of central controller results in the failure of entire network.

Advantage :

- ❑ Easy to install and wire
- ❑ No disruptions to the network while connecting or removing devices.
- ❑ Easy to detect faults and to remove parts.

Disadvantages :

- ❑ Requires more cable length than a linear topology.
- ❑ If the hub or concentrator fails, the nodes attached are disabled.
- ❑ More expensive than the linear bus topologies because of the cost of the concentrators.

Bus topology : In a bus topology all the networked nodes are connected peer to peer, using a single, open-ended cable. It does not allow any external electronics such as repeaters, thus it is simple and inexpensive. All connected devices listen to bussed transmission and accept those packets addressed to them. Failure of any node does not affect the network, while a node is transmitted, it completely posses all available bandwidth and does not allow any other node to transmit.

Advantages :

- ❑ Easy to add/connect a computer or peripheral to a linear bus.
- ❑ Requires less cable length than other topologies.

Disadvantages :

- ❑ The entire network shuts down if there is a break in the main cable.
- ❑ Terminators are required at both ends of the backbone cable.
- ❑ Difficult to identify the problem if the entire network shuts down.
- ❑ Not meant to be used as a stand-alone solution in a large building.

Ring topology : It is a peer-to-peer LAN topology, in which each networked workstation has two connections one to each of its neighbours. Each workstation acts as a repeater, accepting and responding to packets addressed to it and forwarding other packet to the next workstation on a ring..

It uses a token passing scheme in round-robin fashion.

Advantages :

- ❑ All computers have equal access to data. During peak use periods, the performance is equal for all users. Ring networks perform well with heavy network traffic.

Disadvantages :

- Ring topologies are relatively expensive and difficult to install. If one node fail, the entire network fails.

Q 6. Explain different framing methods with examples.

Ans. *Refer to Chapter No. 3 Q.No. 50 on Page No. 75*

SECTION-C

Q 7. Explain in detail various transmission media used for data communication in detail.

Ans. Transmission media can be classified into the following two main categories : Guided media and Unguided media. The difference between the two is the fact that :

1. Guided media use physical cable for data transmission, whereas in the case of unguided media, air is the transmission medium.

In this media, no cabling is required. The signal is broadcasted in the air and can be made available to anyone who has the device capable of receiving the signal.

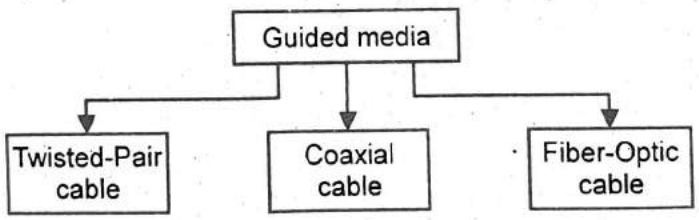
2. Twisted-pair cable, coaxial cable and optical fiber are the three main types of guided media. Unguided media can be radio, microwave, satellite, infra-red, LASER or cellular phones.

3. Guided transmission media is mainly suited for point to point line configuration whereas unguided is mainly used for broadcasting purpose.

4. In guided the signal propagates in the form of voltage, current or photons whereas in unguided the signals propagates in the form of electromagnetic waves.

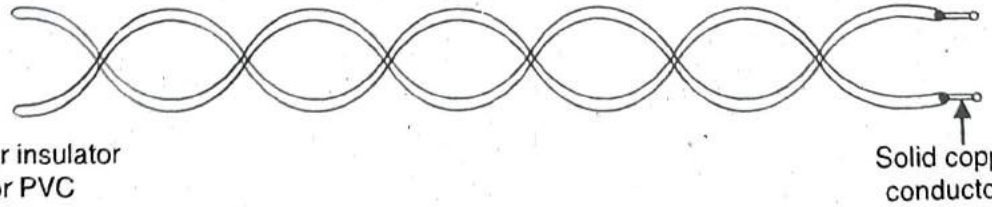
Guided transmission media : A physical path along which the signals are propagated. For guided transmission media the transmission capacity interms of either data rate or bandwidth depends on

1. Distance
2. Whether the medium is point to point or multipoint.



1. Twisted-pair Cable : It is used to transmit both analog and digital signals. Most inexpensive and widely used guided transmission medium is twisted-pair.

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together as shown below :



One of the wires is used to carry signals to the receiver and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal send by the sender on one of the wires, interference (noise) and crosstalk may effect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources. This results in a difference at the receiver. By twisting the pairs, a balance is maintained.

Applications :

1. In the telephone system, the residential telephone sets are connected to the local telephone exchange by twisted pair wires.
2. It is used within a building for LAN supporting personnel computers.

Twisted pair cable are of two types :

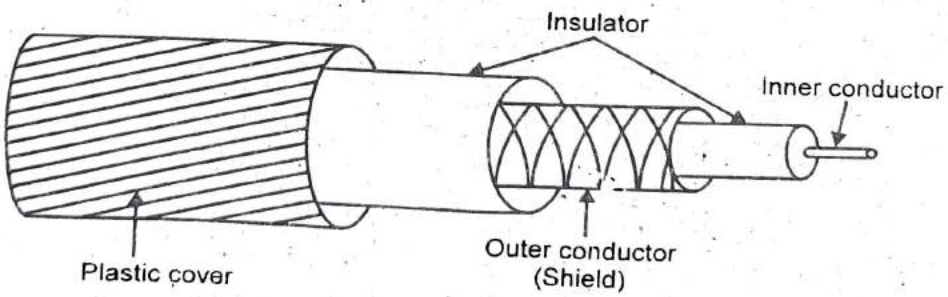
(i) Shielded twisted pair : Shielded means cable has a protected shealth which is made up of aluminium or a polyesters between outer jackets and two wires, but still the problem of interference still remains. Shielded twisted pair (STP) is expensive. It is difficult to install. Its capacity is upto 500 mega bits per second and it is less suffer from electromagnetic interference.

(ii) Unshielded twisted pair (UTP) : Unshielded means cables has no protected shealth to prevent the signal from interference. For example : Telephone cables. In UTP there are different types of variety that are available.

(a) Three-twisted pair
(b) Five-twisted pair

UTP is not expensive and it is easy to install. Its capacity is upto 100 mega bits per second and it suffer more from electromagnetic interference.

2. Coaxial cable : Coaxial cable is copper wire with better shielding than twisted pair so that it can cover longer distance at higher speed. Coaxial cable (or coax) carries signals of high frequency ranges than twisted pair cables.



Frequency range of coaxial cable is 100 kHz to 500 MHz.

There are two types of coaxial cable :

(i) Base band
(ii) Broad band

Base band coaxial cable is 50 OHM wire commonly used for digital transmission.

Broad band coaxial cable is 75 OHM commonly used for analog transmission.

Coaxial cable is better than twisted pair because it support high band width and high data rate.

It suffer less from interference and corsstalk than twisted pair. They are also used in LAN and telephone lines.

Coaxial cable standards :

RG-8, used in thick ethernet
RG-9, used in thick ethernet
RG-11, used in thick ethernet
RG-58, used in thin ethernet
RG-59, used for TV.

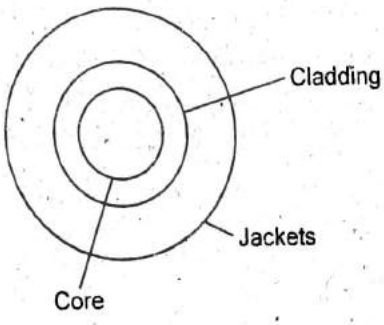
3. Optical fiber : Optical fiber is used for transmitting light wave rather than electrical signal. An optical fiber is a thin, flexible medium which guide the optical ray.

It consist of three concentric section :

1. Core : It is the inner most section which consist of fibre made up of glass and plastic that conducts light.

2. Cladding : The core is surrounded by cladding which is a layer of glass and plastic that has optical properties different from those of the core. The interface between the core and cladding act as a reflector that reflect the light back into the core and does not allows it to escape.

3. Jacket : It is the outermost layer which is made up of plastic and other material layered to protect against moisture and other requiremental dangers.



Basically four components are required :

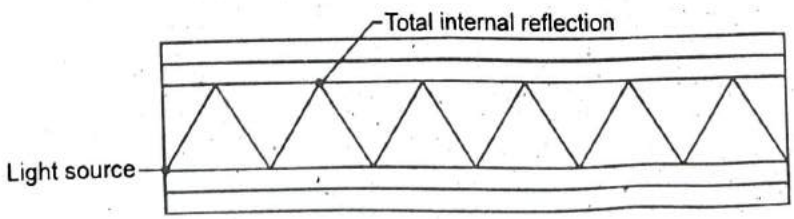
1. Light source : Light emitting diode (LED) or laser diode.

2. Fibre : It is the transmission medium that carries light pulses.

3. Detector : Which detects the light and convert it to electrical signal.

4. Convertor : Converter are placed toward the source side and at the sink side to convert electric signal into lightwave and vice-a-versa.

Working : When a ray passes from one medium to another the ray is refracted at a boundary but a light ray incident at or above the critical angle is trapped inside the fibre and thus it can propagate for many kilometers with out any loss.



Applications :

1. **LAN :** It can support thousand of station in a large buildings.
2. **Metropolitan trunks :** It is used in metropolitan trunk circuits for over a distance of 12km and support 1 lakh voice channel.

Advantages :

1. It is smaller in size and light in weight.
2. It suffers less from attenuation, electromagnetic interference, noise and cross-talk.
3. Greater capacity because of high band width and high data rate.

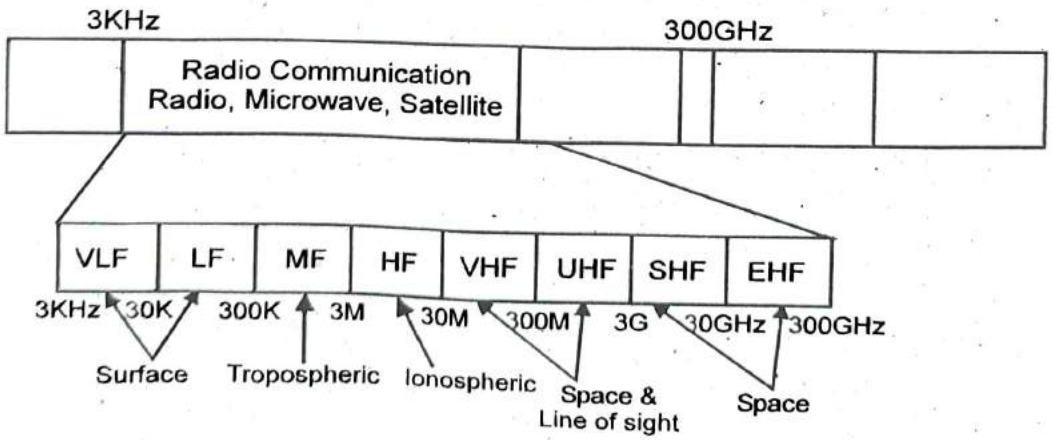
Guided media provide a physical path along which the signals are propagated whereas unguided media employ an antenna for transmitting through air, vacuum or water. Traditionally, twisted pair has been the warhorse for communication of all sorts. Higher data rates over longer distances can be achieved with coaxial cable, and so coaxial cable has often been used for high speed local area network and for high-capacity long-distance trunk applications. However, the tremendous capacity of optical fiber has made that medium more attractive than coaxial cable, and thus optical fiber has taken over much of the market for high speed LANs and for long distance applications. Whereas unguided transmission techniques commonly used for information communications include broadcast radio, terrestrial microwave, and satellite. Infrared transmission is used in some LAN applications.

Unguided media : Unguided media is also known as unbounded or wireless transmission media. In unguided media, air is the transmission medium. In this media, no cabling is required. The signal is broadcasted in the air and can be made available to anyone who has the device capable of receiving the signal. So unguided transmission media is mainly used for broadcasting purpose. In unguided transmission media the signals propagates in the form of electromagnetic waves.

Various unguided media are :

1. Microwave communication
2. Terrestrial microwave communication
3. Satellite
4. Radio transmission
5. Infrared

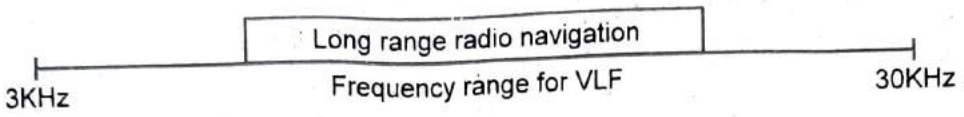
Radio frequency allocation :



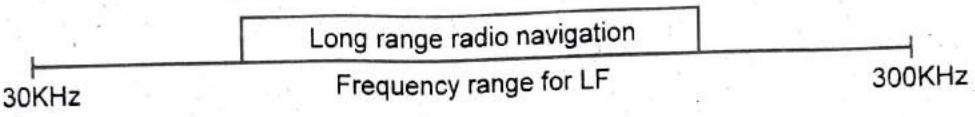
Types of propagation :

1. Surface propagation
2. Tropospheric propagation
3. Ionospheric propagation
4. Line of sight propagation
5. Space propagation

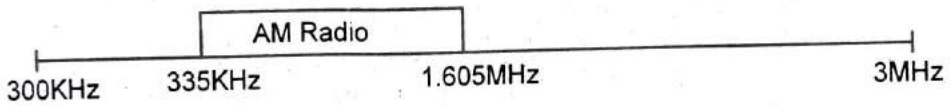
1. Very Low Frequency (VLF) :



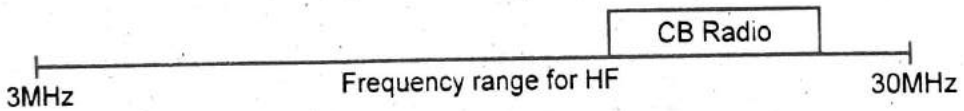
2. Low Frequency (LF) :



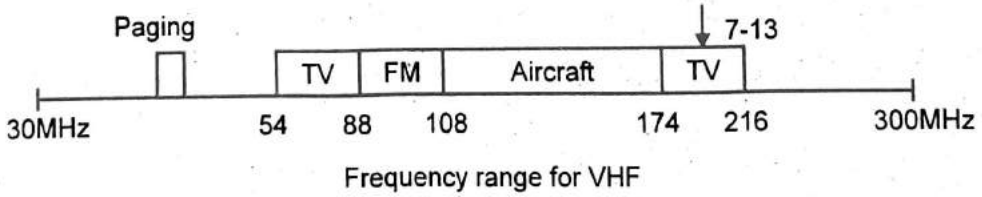
3. Middle Frequency (MF) :



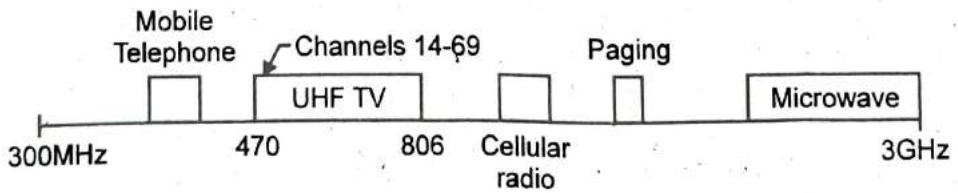
4. High Frequency (HF) :



5. Very High Frequency (VHF) :



6. Ultra High Frequency (UHF) :

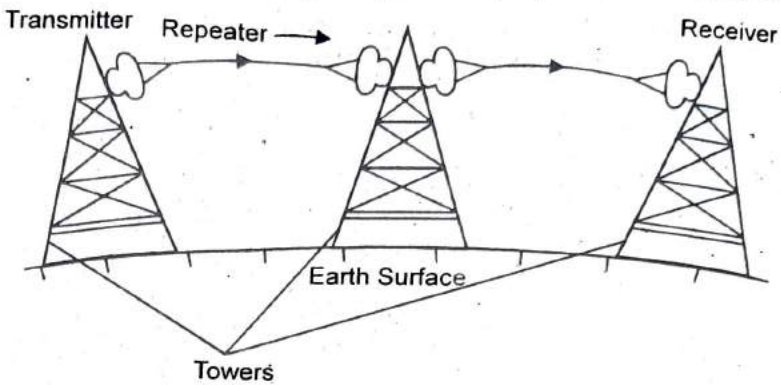


7. Super High Frequency (SHF) :

3 GHz → Microwave → 30 GHz for SHF range

8. 30 GHz → Microwave → 300 GHz for EHF range

1. Microwave communication : Microwave use the line of sight method of propagation, as the signals do not travel along the surface of the earth. Therefore, the two antennas must be in a straight line, able to look at each other without any obstacle in between. The taller the antennas, the more is the distance that these waves travel. Usually the antennas are positioned on mountain tops to avoid obstacles. Microwave signals travel only in one direction at a time. This means that for two-way communication such as in telephony, two frequencies need to be allowed. At both ends a transceiver is used which is a combination of a transmitter and a receiver operating at the two respective frequencies. Therefore, only one antenna can serve both the functions and cover both the frequencies. Repeaters are used along with the antennas to enhance the signal. The data rates offered are 1Mbps -10Gbps.



Advantages :

- Microwave is not expensive as compare to fiber optics system.

2. Terrestrial communication : Terrestrial microwave communication are directional parabolic antennae which sends and receive signals. They do not use cables. The signal are focused according to the line of sight. Microwave link are used to connect several building where cabling can be too expensive, difficult to install and prohibited.

For example : If two buildings are separated by a public road then it become difficult to get permission to install cable over and under the road. So microwave use are such type of situation.

Advantage :

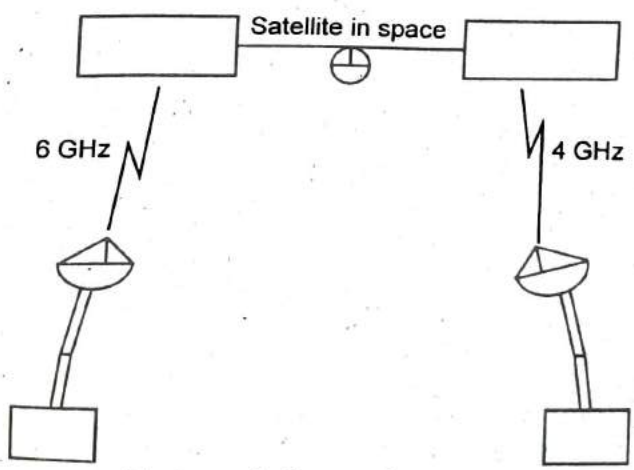
1. They are suitable for short distance upto a range of hundred of meter.
2. It is not expensive.
3. No attenuation problem.

Disadvantage :

- Rain, fog and electromagnetic interference effects the signal.

3. Satellite : Satellite microwave system transmit signal between parabolic antennae which must be in line of sight. In Satellite system one of the antennae is on the satellite in geosynchronous orbit. And is placed at 36km above the equator where its orbit speed exactly matches the earth rotational speed and so it appears to be stationary relative to the earth and always remains at the same point with respect to the earth.

Microwave signals at 6 gega hertz are transmitted from the transmitter to the earth but it becomes weak with distance.



Transmitting microwave

The transponder in the satellite emplifies the signal and since back to the earth at the frequency of 4-gega hertz which are received by the receiving station on the earth.

The transmitting frequency is different from the receiving frequency of the satellite to avoid interference.

Advantage :

1. Satellite microwave system can reach the remotest places on earth and can communicate with even mobile devices.

2. If an error is detected in transmission of information by the satellite, then the data is retransmitted.

Disadvantage :

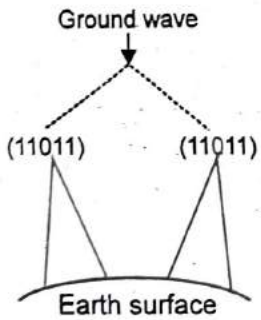
- High cost of manufacturing and launching the sattellite in the orbit.

4. Radio transmission : Radio wave can be broadcasted, OMNI directional. OMNI direction means that they travel in all the direction from the source. So, the transmitter and the receiver do not have to careful about the physical. The power of the radio frequency signal is determine by the antennae and the transreceiver.

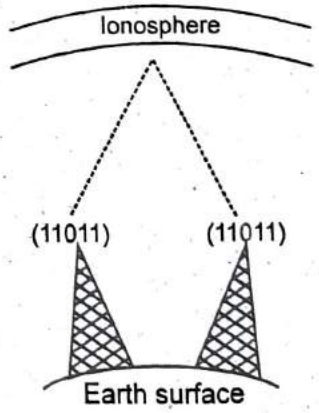
Properties :

1. They can travel long distance.
2. Easy to generate.

A different radio wave like short time, low frequency wave, very low and medium frequency wave which follow the ground where as high frequency wave and very high frequency wave that reach the ionosphere a layer of charge particle circuiling the earth at the height of 100 to 500 km are refracted by it and sent back to the earth.



For low, very low and medium frequency



Very high and ultra high frequency

Advantage :

1. Omni direction
2. Easy to generate

Disadvantage :

At all frequence radio wave suffer from electrical interference.

5. Infrared : Infrared signals can be used for short range communication in a closed area using line-of-sight propagation.

Q 8. Explain in detail various sliding window protocols.

Ans. *Refer to Chapter No. 3 Q.No. 49 on Page No. 74*

Q 9. What is routing ? Explain the important properties that a routing protocol should satisfy. Discuss link state routing algorithm.

Ans. Routing : *Refer to Chapter No. 5 Q.No. 2 on Page No. 94*

Link State Routing : Link state protocols of IP are classless protocols. In link routing protocol, each router floods information about the state of the links that connect it to its neighbours. Link state protocols use an arbitrary metric.

Functions of route in link state routing is as follows :

1. Router discover its neighbours and learn their network addresses.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

Link state routing protocols use event driven updates rather than periodic updates. Link state routine is widely used in actual networks. OSPF protocol uses in a link state algorithm.

Link state routing protocols are as follows :

1. OSPF, open shortest path first
2. Netware link services protocol (NLSP)
3. Apple's AURR
4. ISO's Intermediate system-Intermediate system (IS-IS).

❑❑❑

UNIVERSITY QUESTION PAPER, MAY–2016

SECTION-A

Q 1. (a) Define baud rate.

Ans. *Refer to Chapter No. 1 Q.No. 61 on Page No. 23*

(b) What is open loop congestion control ?

Ans. Open loop congestion control : The open loop congestion control aims to prevent the aims to prevent the congestion from occuring by using some policies. Either the source or destination handles the congestion.

The open loop congestion control method adopts certain policies to prevent the congestion. Some of these policies are described as follows :

1. Retransmission policy
2. Acknowledgement policy
3. Discarding policy
4. Admission policy

(c) Define throughput.

Ans. Throughput : The throughput is a measure of how fast we can actually send data through a network.

(d) Why FTP uses two connections ?

Ans. FTP uses two connections between a client and a server. One connection is used for the actual file's data transfer, and the other is used for control information (commands and responses). This separation of data transfer and commands makes FTP more efficient.

(e) List the important features of LAN.

Ans. *Refer to Chapter No. 1 Q.No. 63 on Page No. 23*

(f) What is RS 232C ?

Ans. RS 232C : RS 232C is a long-established standard that describes the physical interface and protocol for relatively low-speed serial data communication between computers and related devices. RS 232C can provide good performance at low cost. RS 232C interface uses single common ground for all the signals. Hence effect of noise is maximum. RS 232C is easy to use because the IC is available for RS 232C. Data transfer rate is slow. Baud rate is 20K baud for less than 50 ft.

(g) Why twisted pair cable is twisted ?

Ans. Twisted pair cable is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference from external sources; for instance, electromagneic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs.

(h) Define interface between layers.

Ans. *Refer to Chapter No. 1 Q.No. 48 on Page No. 18*

(i) What is fading ?

Ans. Fading : Where there are obstacles between the base station and the terminal (For example; hills, building etc.) the signal strength goes down further, which is known as fading.

(j) Differentiate between pure aloha and slotted aloha.

Ans. *Refer to Chapter No. 4 Q.No. 9 on Page No. 85*

SECTION-B

Q 2. What are the goals of computer networks ? Explain in brief.

Ans. There are several goals of computer networks. The goals of computer networks are as follows :

1. To provide sharing of resources such as information or processors.
2. To provide inter-process communication among users and processors.
3. Computer networks provides the network user with maximum performance at minimum cost.
4. Computer networks provides centralized control for a geographically distributed system.
5. Computer networks provides compatibility of dissimilar equipment and software.
6. It provides centralised management and allocation of network resources.
7. It provides distribution of processing functions.

Q 3. Differentiate between asynchronous and synchronous TDM.

Ans. *Refer to Chapter No. 2, Q.No. 18 on Page No. 32*

Q 4. Explain the stop and wait ARQ mechanism.

Ans. *Refer to Chapter No. 3 Q.No. 36 & 58 on Page No. 69 & 79*

Q 5. A company is granted the site address 201.70.64.0 The company needs six subnets. Design the subnets.

Ans. The number of 1s in the default mask in 24.The company needs six subnets. This number 6 is not a power of 2. The next number that is a power of 2 is 8 (2^3). We need 3 more 1s in the subnet mask. The total number of 1s in the subnet mask is 27 (24 + 3).

The total number of 0s is 5 (32 – 27). The mask is

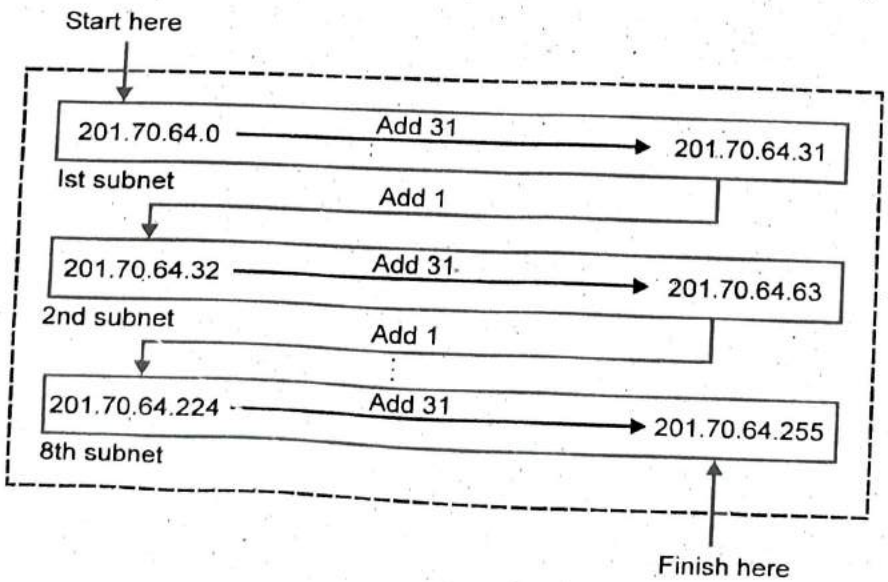
11111111 11111111 11111111 11100000

or

255.255.255.224

The number of subnets is 8.

The number of addresses in each subnet is 2^5 (5 is the number of 0s) or 32.

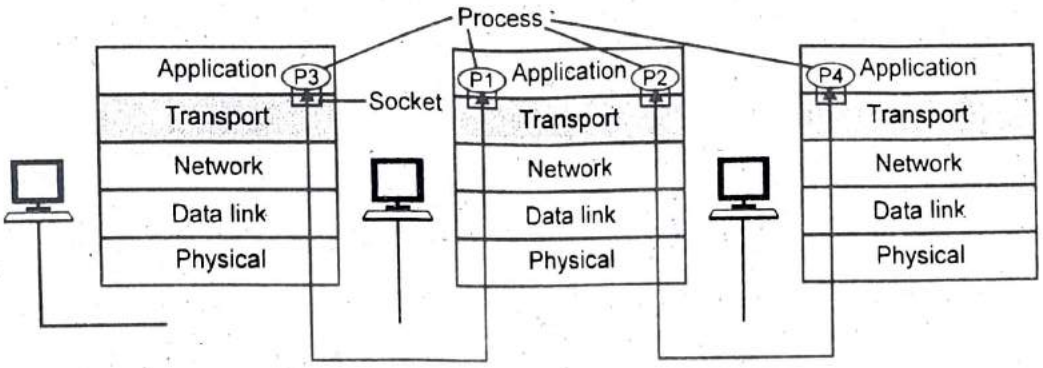


Q 6. What is multiplexing and de-multiplexing at transport layer ? Explain in brief with example.

Ans. Multiplexing and de-multiplexing are the two very important functions that are performed by transport layer.

Transport layer at the sender side receives data from different applications, encapsulates every packet with a transport layer header and pass it on to the underlying network layer. This job of transport layer is known as multiplexing.

At the receiver's side, the transport gathers, the data, examines it socket and passes the data to the correct application. This is known as De-multiplexing.



A socket is the interface through which a process (application) communicates with the transport layer

- Each process can potentially use many sockets.
- The transport layer in a receiving machine receives a sequence of segments from its network layer. In this delivering segments to the correct socket is called demultiplexing and assembling segments with the necessary information and passing them to the network layer is called multiplexing. These both are needed whenever a communications channel is shared.

SECTION-C

Q 7. What is link state routing ? Explain the steps involved with an example.

Ans. Link State routing : *Refer to Q.No. 9 of Dec. 2015*

Link state routing essentially involves four steps :

1. The first step is to measure the delay or cost to each neighbouring router. For example, each router can send out a special echo packet that gets bounced back almost immediately. If a timestamp were placed on the packet as it left and again as it returned, the router would know the transfer time to and from a neighboring router.

2. The second step is to construct a link state packet containing all of this timing information.

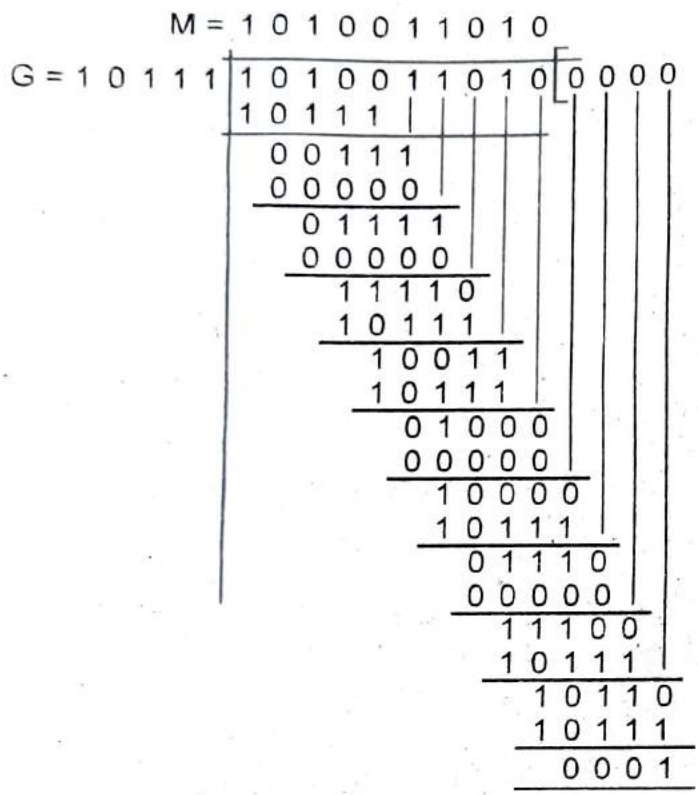
3. The second step is to distribute the link state packets via flooding. In addition to using flooding, the link state routing algorithm is a distributed algorithm.

4. The fourth and final step is to compute new routes based on the updated information.

Once a router collects a full set of link state packets from its neighbors, it creates its routing table, usually using Dijkstra's least-cost algorithm.

Q 8. Give the data word 1010011010 and the divisor 10111 :
(a) Show the generation of the codeword at the sender site (using binary division)
(b) Show the checking of the codeword at the receiver site (assume no error).
Ans.

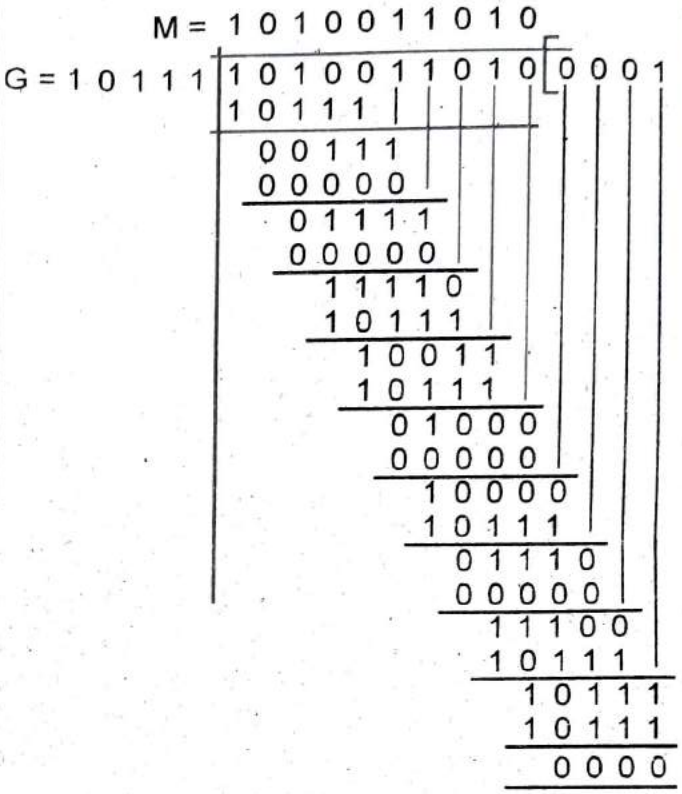
(a) Binary division case



T = 1010011010 0001
Original message CRC checksum

CRC checksum was 0001
Codeword was 1010011010

(b) Receiver using binary division.



Remainder was 0000 as required.

Q 9. What is DNS ? Differentiate between recursive and iterative queries. Explain the formats of the query and response message used in DNS.

Ans. DNS : *Refer to Chapter No. 7 Q.No. 29 (Point 1) on Page No. 149.*

Difference between recursive and iterative queries :

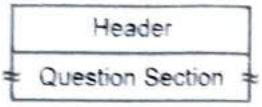
In recursive name query, the DNS client requires that the DNS server respond to the client with either the requested resource record or an error message i.e. the record or domain name does not exist. If DNS server is not able to resolve the requested query then it forwards the query to another DNS server until it gets an answer or the query fails.

An iterative name query is one in which a DNS client allows the DNS server to return the best answer it can give based on its cache or zone data. If the queried DNS server does not have an exact match for the queried name, the best possible information it can return is a referral.

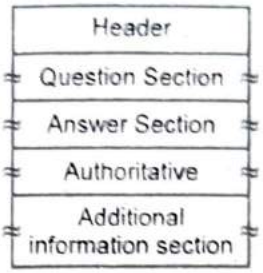
Formats of the query and response messages used in DNS : DNS has two types of messages :

1. Query
2. Response

Both have the same format. The query message consists of the header and the question records, the response message consists of a header, question record, answer record, authoritative record and additional records.



Query



Response

Header : Both query and response messages have the same header format with some fields set to zero for the query message, the header is 12 byte and its format is as follows:

- identification
- flags

Question Section : This is a section consisting of one or more question records. It is present on both query and response messages.

Answer section : Consisting of one or more resource records. It is present only in response messages. This section includes answer from the server to the client.

Authoritative section : This section is also contained only in response messages of DNS, and gives information about domain names regarding authoritative servers for the query.

Additional information section : This section provides additional information to help the resolver and present only in response part of DNS message format.

UNIVERSITY QUESTION PAPER, DEC.–2016

SECTION-A

Q 1. (a) Explain terms LAN and MAN.

Ans. *Refer to Chapter No. 1 Q.No. 9 on Page No. 4*

(b) Define protocol.

Ans. *Refer to Chapter No. 1 Q.No 66 on Page No. 25*

(c) Write the full form of HDLC and PPP.

Ans. HDLC : High-level Data link Control Protocol

PPP : Point to Point Protocol

(d) What is Nyquist's theorem ?

Ans. Nyquist's Theorem : The Nyquist theorem is also known as sampling theorem. According to Nyquist theorem, the sampling rate should be atleast two times of the highest frequency contained in the signal to regenerate the original analog signal at the receiver end.

(e) What are the issues of Data Link Layer ?
Ans. *Refer to Chapter No. 3 Q.No. 2 on Page No. 58*
(f) Define Bandwidth.
Ans. *Refer to Chapter No. 2 Q.No. 4 on Page No. 28*
(g) What is the difference between port number and IP address ?
Ans. *Refer to Chp. No. 6 Q.No. 4 on P.No. 126 and Chp. No. 5 Q.No. 23 on P.No. 103*
(h) Write the difference between Network Layer delivery and Transport Layer delivery.
Ans. *Refer to Q.No. 1(c) of Dec. 2014*
(i) What is WWW ?
Ans. *Refer to Chapter No. 7 Q.No. 1 on Page No. 138*
(j) Define subnetting.
Ans. *Refer to Chapter No. 4 Q.No. 23 on Page No. 91*

SECTION-B

Q 2. Discuss about pros and cons of different Network Topologies.
Ans. *Refer to Q.No. 5 of Dec. 2015*
Q 3. What are Transmission Impairments ?
Ans. *Refer to Q.No. 9 (c) of May 2015*
Q 4. Explain any one Error detection and correction code method.
Ans. *Refer to Chapter No. 3 Q.No. 44 on Page No. 72*
Q 5. Explain how Leaky Bucket protocol used for congestion control.
Ans. *Refer to Chapter No. 5 Q.No. 41 on Page No. 114*
Q 6. Explain Transmission Control protocol in brief.
Ans. *Refer to Chapter No. 1 Q.No. 40 on Page No. 14*

SECTION-C

Q 7. Explain the functions of different layers of OSI Model.
Ans. *Refer to Chapter No. 1 Q.No. 49 on Page No. 18*
Q 8. (a) Discuss about Stop & Wait ARQ Sliding Window protocol.
Ans. *Refer to Chapter No. 3 Q.No. 49 & 36 on Page No. 75 & 69*
(b) Explain IP addressing.
Ans. *Refer to Chapter No. 5 Q.No. 4 & 23 on Page No. 95 & 103*
Q 9. Write short notes on following :
(a) Coaxial Cable
(b) DNS
(c) Distance Vector Routing Algorithm.
Ans. (a) *Refer to Q.No. 7 (Point 2) of Dec. 2015*
(b) *Refer to Chapter No. 7 Q.No. 8 on Page No. 139*
(c) *Refer to Chapter No. 5 Q.No. 31 on Page No. 108*

❑❑❑

Chapter 1

Introduction to Computer Networks

Contents

Data Communication System and its components, Data Flow, Computer network and its goals, Types of computer networks : LAN, MAN, WAN, Wireless and wired networks, broadcast and point to point networks, Network topologies, Network software: concept of layers, protocols, interfaces and services, ISO-OSI reference model, TCP/IP reference model.

POINTS TO REMEMBER

- ☞ Data communication is exchanged of data between two devices via some transmission medium for the data communication to occur.
- ☞ The seven layer OSI model provides guidelines for the development of universally compatible architecture, hardware and software.
- ☞ Transmission mode is used to define the direction of signal flow between two linked devices. Types of transmission modes are simplex, half duplex and full duplex.
- ☞ A network is an interconnection of several heterogeneous computers.
- ☞ Simplex transmission means that data flow in one direction only.
- ☞ Half-duplex transmission allows data to flow in both directions, but not at the same time.
- ☞ Full duplex transmission allows data to flow in both directions at the same time.
- ☞ The physical, data link and network layers on the network support layers.
- ☞ The session, presentation and application layers are the user support layers.
- ☞ LAN is a data communication system within a building, plant or campus or between nearly building.
- ☞ A MAN is a data communication system spanning states, an area the size of a town or city.
- ☞ A WAN is a data communication system spanning states, countries or whole world.
- ☞ An internet is a network of networks.
- ☞ The international standards organisation creates a model called the open system interconnection, which allows diverse systems to communicate.
- ☞ A network can be categorized as a local area network (LAN), a metropolitan area network (MAN) or a wide area network (WAN).

- In multipoint line configuration, two and only devices are connected by a dedicated link.
- A line configuration defines the relationship of communication devices to a communication pathway.
- Topology refers to the physical or logical arrangement of a network. Devices may be arranged in a mesh, star, bus or hybrid topology.
- The transport layer links the network support and the user support layers.
- The physical layer co-ordinates the functions required to transmit a bit stream over physical medium.
- The data link layer is responsible for the source-to-destination delivery of a packet across multiple network links.
- The transport layer is responsible for the source to destination delivery of the entire message.
- The session layer establishes, maintains and synchronizes the interactions between communicating devices.
- TCP/IP a five layer hierarchical protocol suit developed before the OSI model is the protocol suite used in the Internet.

QUESTION-ANSWERS

Q 1. What is data communication?

Ans. It is exchange of data between two devices via some transmission medium for the data communication to occur, the communicating devices must be part of communication system made up of hardware and software.

Data communication depends upon the three characteristics :

1. Delivery
2. Accuracy
3. Timeliness.

Q 2. Explain the basic elements of a data communication.

Ans. A data communication system consists of five basic components :

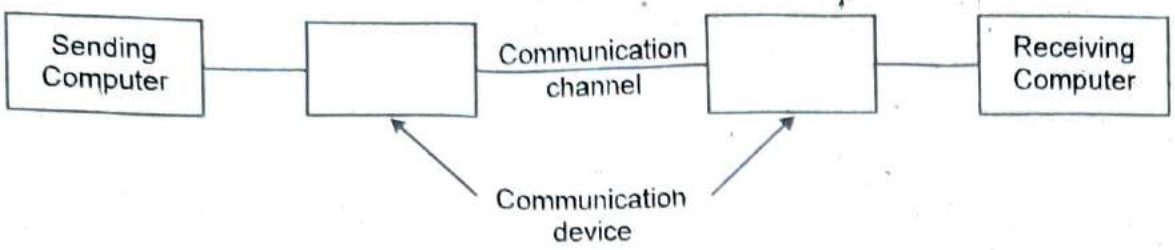
1. The sending/originating computer : It transmits the data which consists of a file on a disk or may be entered through a keyboard and transmitted as it is typed.

2. Data communication device : Which is attached to the sending computer. It converts data in a suitable form so it can be transmitted.

3. Communication channel : It is a communication link which actually carries the data from one computer to the other.

4. Data communication device : Which is attached to the receiving computer. It converts data into a form that can be understood by the receiving computer.

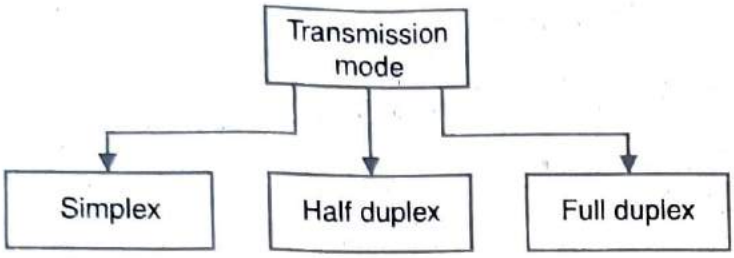
5. The receiving computer : Which receives data and displays it on the screen or stores it on disk or prints a hard copy of the data.



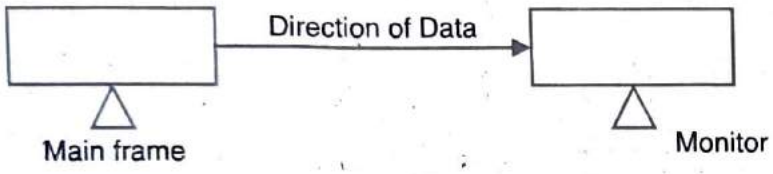
Elements of data communication system.

Q 3. What do you mean by transmission mode?

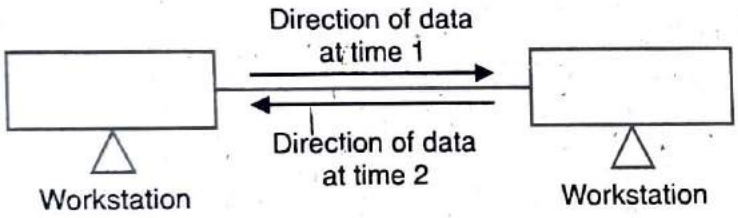
Ans. Transmission mode is used to define the direction of signal flow between two linked devices.



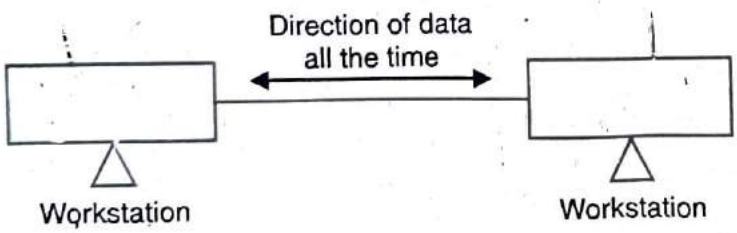
1. Simplex : In this mode the communication is unidirectional. Only one of the two stations on a link can transmit, the other can only receive.



2. Half duplex : In this case each station can both transmit and receive, but not at the same time.



3. Full duplex : Full duplex mode is like a two-way street with traffic flowing in both directions at same time.



Q 4. What is network computer?

Ans. A network is an interconnection of several heterogeneous computers. These computers may be in close proximity to each other or may be several miles apart or even located in different countries. In order to connect various computers to make a network various hardware components like network interface card, hub, switches, various types of cables are required.

Q 5. Explain the need of networking.

Ans. There is a need for networking due to following advantages.

1. Resource sharing : The most fundamental advantage of networking is resource sharing when all programs, equipment and especially data is shared.

2. Reliability : Networking improves reliability due to alternative sources of supply.

3. Cost saving : Smaller computers have a better cost/performance ratio. A mainframe works about ten times faster than PC but also costs a thousand times. So network improves the cost saving.

4. Scalability : Networking allows scalability, i.e., as the workload increases, performance can be enhanced by adding more processes.

Q 6. What do you understand by the term protocol used in a networking environment?

Ans. A protocol is a technical guide or custom that formally governs the exchange of data transmission and reception between computers. A protocol specifies the exact order in which data may be transferred. Only those devices used the same set of communication protocols can directly communicate with one another.

Q 7. Explain the components of computer network. **(PTU, May 2006)**

Ans. A computer network, often simply referred to as a network is a collection of computers and devices interconnected by communication channels hot facilitates communication among users and allows users to store resources.

1. Network interface cards
2. Repeaters
3. Hubs
4. Bridges
5. Routers.

Q 8. What do you mean by network reliability?

Ans. By the use of network, alternative resources can be made available. If one particular resource goes out of orders or failed due to certain reasons, others may be used at reduced speed and performance. This is called network reliability.

Q 9. Explain the types of networks.

Ans. Networks can be categorized according to their size into three basic types :

(i) Local Area Network (LAN) : A LAN is a network of computers which are located relatively near each other. Typically a LAN exists within a single building or group of adjacent

buildings where two or three or several hundred computers of different types are interconnected.

2. Metropolitan Area Network (MAN) : MANs are spread over a city or group of offices and may be private or public. For example, a TV cable network that is spread over a city may be termed as MAN.

3. Wide Area Network (WAN) : Most commonly a WAN is two or more LAN's connected across a wide geographical area which is huge as compared to area covered by LAN or MAN.

Q 10. What do you understand by term protocol?

(PTU, Dec. 2009, 2006 ; May 2008)

Ans. Protocol is defined a set of formal operating rules, it may also be defined as a set of rules governing the exchange of data between two entities.

1. Syntax
2. Sematics
3. Timing.

Q 11. Explain broadcast network and point to point networks.

(PTU, Dec. 2005 ; May 2005)

Ans. Broadcast Network : A computer network which has a single communication channel. A packets that are sent contain the address of the receiving computer. Each computer check this field to see if it matches its own address. If it does not, then it is usually ignored ; if it does, then it is read broadcast networks are usually small, localized network known as local area network.

Point to point network : A communication network that uses such devices as telephone lines, satellite dishes or radio waves to span a larger geographical area, then can be covered by a LAN.

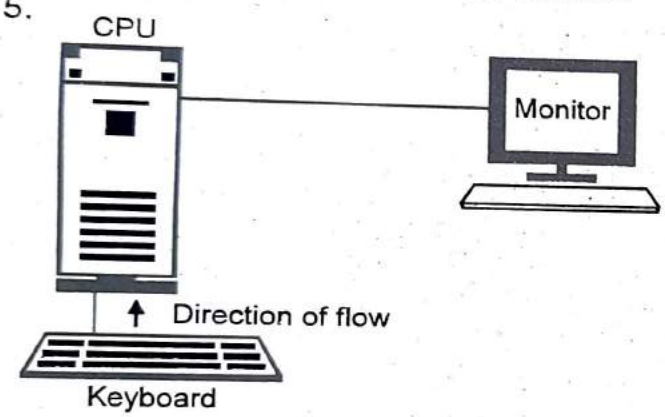
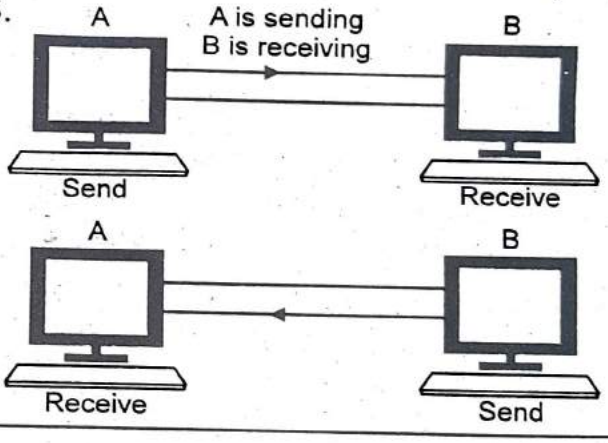
Q 12. Differentiate between LAN and MAN. **(PTU, Dec. 2012 ; May 2009)**

Ans. Difference between LAN and MAN is given below :

S.No.	Parameters	LAN (Local area network)	MAN (Wide area network)
1.	Ownership of network	Private	Private or public
2.	Area covered	Small	Moderate
3.	Design and maintenance	Easy	Not easy
4.	Communication medium	Coaxial cable	Coaxial cables, PSTN, optical fibre cables
5.	Data rates	High	Moderate
6.	Mode of communication	Each station can transmit and receive	Each station can transmit and receive
7.	Principle	Operates on principle of broadcasting	Operates on principle of broadcasting and switching
8.	Propagation delay	Short	Moderate

Q 13. Comparison between simple and half duplex.

Ans.

Simplex	Half duplex
1. In simplex mode, data can be sent in one direction only at all times.	1. In half duplex, data can be sent in both the directions, but only in one direction at a time.
2. Devices connected in simplex mode are either send only or receive only i.e. one device can only send, other can only receive.	2. Both the connected devices can transmit as well as receive data but not simultaneously.
3. Communication is unidirectional.	3. Communication is bidirectional.
4. Examples of simplex system are : keyboard and traditional monitors, loudspeaker system and fire alarms.	4. Example of HDX system is walkie-talkie which can send as well as receive transmission but not simultaneously.
5. 	5. 

Q 14. What is advantage of multipoint connection over point to point connection?

Ans. In multipoint configuration multiple devices are attached to a single link whereas point to point network uses dedicated link between the devices. The multipoint configuration has following advantages :

1. The entire capacity of the link is shared for the transmission between all the devices connected to a link.
2. As single link is shared by all the devices the line cost is less.
3. Multipoint connection also provides broadcasting and multicasting in a better way.

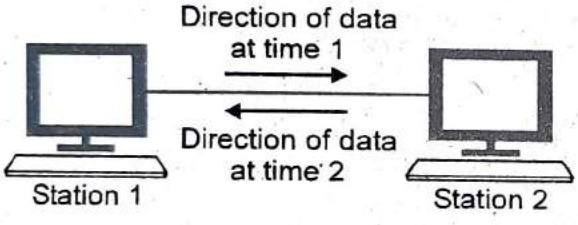
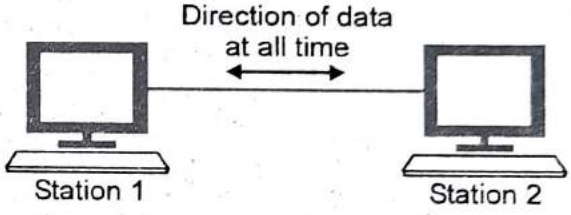
Q 15. Explain broadcast corfiguration.

Ans. 1. Broadcasting is the process in which a single packet is received and processed by all the machines in the network. It is made possible by using a special code in the address field of the packet.

2. Broadcast network provides the provision for broadcasting and multicasting.

Q 16. Comparison between half duplex and full duplex. **(PTU, May 2005)**

Ans.

Half Duplex	Full duplex
1. Data can be sent in both the directions but not simultaneously.	1. Data can be sent in both the directions simultaneously.
2. In half duplex, devices can transmit and receive but not at the same time. When one device is sending, the other is receiving and vice-versa.	2. In full duplex, devices can transmit and receive at the same time i.e. each device can send as well as receive data simultaneously.
3. Example of half duplex system is walkie-talkie where one person speaks and other listens and vice-versa.	3. Example of full duplex is the telephone system where both the persons can speak and listen simultaneously.
4. Diagrammatically half duplex is represented as : 	4. Diagrammatically full duplex is represented as : 

Q 17. Comparison between point to point network and broadcast network.

Ans.

Point to point network	Broadcast Network
1. This network uses dedicated link between the two devices.	1. In broadcast networks, all devices are attached to a single communication line.
2. The entire capacity of link between two devices is used for transmission between those two devices only.	2. The entire capacity of the single communication link is shared by all the devices in a network.
3. In point to point network, several different routes are available from one device to another.	3. No such alternate routes are possible in broadcast networks.

Q 18. What are the uses of computer networks? **(PTU, Dec. 2010)**

Ans. Computer Networks : A network is a set of device often referred to as nodes connected by media links. A node can be a computer, printer or any other device capture of sending or receiving data generated other nodes on the network. Also, the links connecting the devices are called communication channels.

Uses of computer network : The computer networks are playing an important role in providing services to large organizations as well as to the individual common man. Many organizations have a large number of computers in organization.

1. Resource sharing
2. For providing high reliability
3. To save money
4. It can provide a powerful communication medium.

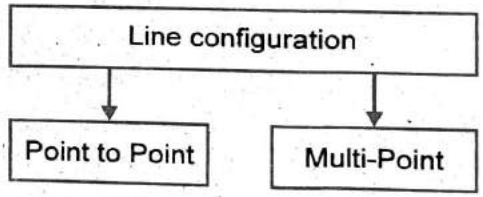
Q 19. Differentiate between LAN and WAN. **(PTU, Dec. 2009)**

Ans.

S.No.	Parameters	LAN (Local area network)	WAN (Wide area network)
1.	Ownership of network	Private	Private or public
2.	Area covered	Small	Very large (States or Countries)
3.	Design and maintenance	Easy	Not easy
4.	Communication medium	Coaxial cable	PSTN or satellite links
5.	Data rates	High	Low
6.	Mode of communication	Each station can transmit and receive	Each station cannot transmit
7.	Principle	Operates on principle of broadcasting	Switching
8.	Propagation delay	Short	Long

Q 20. Explain the line configuration.

Ans. Line configuration refers to the way two or more communication devices attach to the link.



1. Point to point configuration : It provides the link between two devices. The entire capacity of the channel is reserved for the transmission of data between two devices.

2. Multipoint configuration : Multipoint line configuration is one in which more than two specific devices share a single link.

Q 21. What are the advantages of layered architecture? **(PTU, Dec. 2009 ; May 2009)**

Ans. Advantages of layered architecture are :

1. Layered architecture, includes the division of process into groups and layers which result in decrease in complexity.
2. Standardized interface allows for "plug and play" compatibility and multi-vendor integration.
3. Facilitates modularization-developers "swap" out new technology at each level keeping the integrity of the network architecture.

4. Accelerates evolution of technology developers focus on technology at one layer while preventing the changes from effecting another layer.

5. Simplifies learning-processes broken up into groups divides the complexities.

Q 22. Write down the different types of networking devices.

Ans. 1. Switches
2. Routers
3. Gateway
4. Bridges
5. Repeaters.

Q 23. What is the difference between bridge and router?

Ans.

S.No.	Parameters	Router	Bridge
1.	Layer in OSI model	Network layer	Physical or data link layer
2.	Used for	Connecting networks	Connecting different-2 computers
3.	Principle of operation	Uses hardware and software	Uses tables relating the address and ports
4.	Operation	Connects two or more networks	Regeneration, check MAC address

Q 24. List advantages and disadvantages of International standards.

(PTU, Dec. 2007)

Ans. Advantages :

1. It enforces the uniformity in operation.
2. It helps to achieve optimal quality.

Disadvantages :

1. It is financially overhead of small organization.

Q 25. Explain network topology and types of topology.

(PTU, Dec. 2009 ; May 2010, 2009)

Ans. Network topology can be defined as the physical or logical arrangement of the elements of a network. The different kinds of topologies are :

1. Bus Topology
2. Star Topology
3. Ring Topology
4. Tree Topology
5. Mesh Topology
6. Hybrid Topology
7. Graph Topology
8. Multidrop Topology

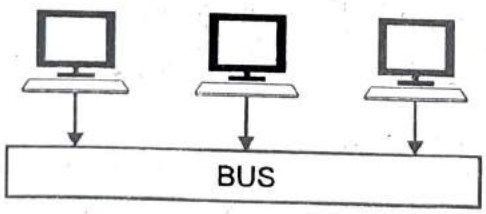
Q 26. Comparison between TCP/IP and OSI architecture. (PTU, Dec. 2006)

Ans.

OSI	TCP/IP
1. OSI is truely a general model.	1. TCP/IP cannot be used for any other application.
2. It has seven layers.	2. It has four layers.
3. Transport layer guarantees delivery of packets.	3. Transport layer does not guarantee delivery of packets.
4. It has separate session layer.	4. No session layer.
5. Network layer provides both connectionless and connection-oriented services.	5. Network layer provides only connectionless services.
6. The protocols are better hidden and can be easily replaced by others as the technology changes.	6. It is not easy to change the protocols.
7. It has a problem of protocol fitting into a model.	7. The model does not fit any other protocol stack.
8. it uses horizontal approach.	8. It uses vertical approach.

Q 27. Explain bus topology.

Ans. This is one of the simplest ways to organize network. In bus topology, all computers are linked to the same transmission line. Bus topologies are multipoint electrical circuit that can be implemented using coaxial cable, UTP or STP.



In this topology data can be transmitted bidirectionally.

Advantages :

1. It is easy to implement.
2. It is highly vulnerable.

Disadvantages : Whole network gets down if one of the connections is defective.

Q 28. In case I open two different websites from the same computer, is my source port no. and destination port no. going to be different? Explain. (PTU, May 2010)

Ans. Port number can be same for two different computers, but it cannot be same for two different applications running on same pc. So source port number of two different websites should be different on a similar pc but these can be same as to destination port numbers on other pc.

Q 29. Difference between wired and wireless network.

Ans.

Wired media	Wireless media
1. The signal energy is contained and guided within a solid medium.	1. The signal energy propagates in the form of unguided electromagnetic waves.
2. Twisted pair wires, coaxial cable, optical fiber cables are the examples of wired media.	2. Radio and infrared light are the examples of wireless media.
3. Used for point to point communication.	3. Used for radio broadcasting in all directions.
4. Wired media leads to discrete network topologies.	4. Wireless media leads to continuous network topologies.
5. Additional transmission capacity can be procured by adding more wires.	5. It is not possible to procure additional capacity.
6. Installation is costly, time consuming and complicated.	6. Installation needs less time and money.
7. Attenuation depends exponentially on the distance.	7. Attenuation is proportional to square of the distance.

Q 30. Difference between LAN, MAN and WAN. **(PTU, Dec. 2010)**

Ans.

S.No.	Parameters	LAN	WAN	MAN
1.	Ownership of network	Private	Private or Public	Private or Public
2.	Area covered	Small	Very large	Moderate
3.	Design and maintenance	Easy	Not easy	Not easy
4.	Communication Medium	Coaxial cable	PSTN or satellite links	Coaxial cables, PSTN, optical fibre cables, wireless
5.	Date rates	High	Low	Moderate
6.	Mode of communication	Each station can transmit and receive	Each station cannot transmit	Each station can transmit or receive
7.	Principal	Operates on the principle of broadcasting	Switching	Both
8.	Propagation delay	Short	Long	Moderate

Q 31. Explain optical fibre cables.

Ans. 1. It consists of an inner glass core surrounded by a glass cladding which has a lower refractive index.

2. Digital signals are transmitted in the form of intensity-modulated light signal which is trapped in the glass core.

3. Light is launched into the fibre using a light source such as a light emitting diode or laser.

Characteristics of optical fibre cables :

1. Higher bandwidth, therefore, can operate at higher data rates.
2. Reduced losses as the signal attenuation is low.
3. Distortion is reduced hence better quality is assured.
4. They are immune to electromagnetic interferences.
5. Small size and light weight.

Q 32. Differentiate between the Peer-to-Peer and Primary-Secondary Relationship. **(PTU, Dec. 2004)**

Ans. Peer-to-Peer and Primary-Secondary Relationship.

Peer-to-Peer	Primary-Secondary Relationship
1. Peer-to-peer is a type of network connection where the devices share the link equally.	1. Primary-secondary relationship is that where one device controls traffic and others must transmit through it.
2. Example : Ring, Mesh Topology.	2. Example : Tree Topology.

Q 33. Differentiate between Radio and Satellite broadcast networks. **(PTU, Dec. 2004)**

Ans. Radio Broadcast : Radio broadcast is a one way transmission over radio waves intended to reach a wide audience. Stations can be linked in radio network to broadcast common programming, either in syndication or simulcast or both. Audio broadcasting also can be done via cable FM, local wire networks satellite and the Internet.

Satellite Broadcast is the distribution of video content over a satellite network. The audio and video signals are acquired at the origination point and transmitted through an uplink truck to a geo-synchronous satellite. The orbit satellites retransmit the signals to predetermined geographical area over an "open" or secure channel. Small inexpensive "downlinks" receive the signals and display the content on television monitor.

Q 34. If there are n devices in mesh topology, then how many links are required?

Ans. If there are n devices in a mesh network, then the 2n links are required.

Q 35. What are two reasons for using layered protocol? **(PTU, May 2005)**

Ans. 1. Protocol layering in a common technique to simplify the network designs by dividing. Then into functional layers and assigning protocol to perform each layer's task.

2. Protocol layering produces simple protocol, each with a few will define tasks. These protocols can then be assembled into a useful whole.

Q 36. Differentiate between connection oriented and connectionless services. (PTU, May 2007)

Ans.

S.No.	Characteristic	Connectionless Service	Connection Oriented Service
1.	Example of Protocol	UDP (User Datagram Protocol)	TCP (Transmission control protocol).
2.	General Description	Simple, high-speed, low functionality "wrapper" that interfaces applications to the network layer.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
3.	Connection set-up	Data is sent without set-up i.e. connectionless.	Connection must be established prior transmission.
4.	Data Interface to Application	Message-based ; data is sent in discrete packages by the applications.	Stream-based ; data is sent by the application with no particular structure.
5.	Reliability and Acknowledgements	Unreliable, best efforts delivery without acknowledgements.	Reliable delivery of messages ; all data is acknowledged.
6.	Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed and lost data is retransmitted automatically.
7.	Features provided to manage flow of data	None	Flow control using sliding windows ; window size adjustment heuristics ; congestion avoidance algorithm.
8.	Overhead	Very low	Low
9.	Transmission speed	Very high	High, but not as high as UDP
10.	Data quantity suitability	Small to moderate amounts of data.	Small to very large amounts of data.

Q 37. Explain merits and demerits of OSI model.

Ans. An OSI model is a layered framework for the design of network system that allows for communication across all types of computer systems. The purpose of each layer is to offer certain services to higher layer. Layer n on one machine carries on a conversation with layer n on another machine.

Merits of OSI model :

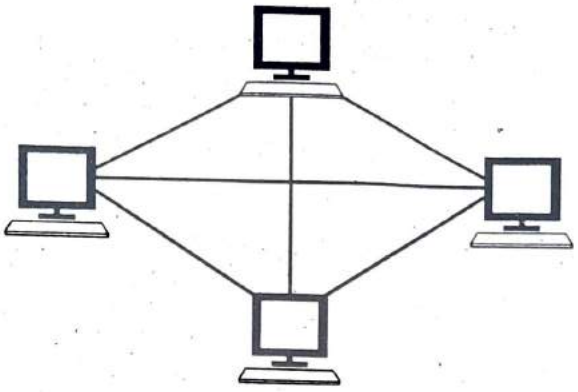
1. OSI model is truely a general model.
2. This model supports connection oriented as well as connectionless services.
3. It distinguishes very clearly between the services, interfaces and protocols.

Demerits of OSI model :

1. Sessions and presentation layers are not of much use.
2. This model was devised before the protocols were invented.

Q 38. Explain advantages of mesh topology.

Ans. In a mesh topology every device has a dedicated point to point link to every other device.



The term dedicated means that the link carries traffic only between two devices it connects.

Advantages :

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating traffic problem.
2. A mesh topology is robust because the failure of any one computer does not bring down the entire network.
3. It provides security and privacy.

Disadvantages :

1. Cabling cost is high.
2. The hardware required to connect each link input/output and cable is expensive.

Q 39. Enumerate two important properties of WAN. **(PTU, May 2004)**

Ans. The two important properties of WAN :

1. It is cheaper and more efficient to use the phone network for the links.
2. A WAN provides long distance transmission of data, video and voice image to a whole world.

Q 40. Describe in brief the architecture of TCP/IP model.

(PTU, Dec. 2010, 2007 ; May 2009)

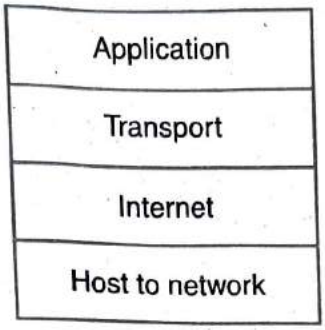
OR

Explain in detail the purpose of each layer of TCP/IP model. Is OSI model used in practice. **(PTU, May 2010 ; Dec. 2009, 2008)**

Ans. TCP/IP is a short form of transmission control protocol and internet protocol. These two protocols describe the movement of data between the host computer on internet. In TCP/IP protocol suit, there are various layers, with each layer being responsible for different facts of communication. TCP/IP offers a simple naming and addressing scheme whereby

different resources on internet can be easily located. Using TCP protocol, a single large message is divided into a sequence of packets and each is put into an IP packet. The packets are passed from one network to another until they reach their destination, IP protocol is used to put a mesage into a "packet".

TCP/IP model is shown below :



TCP/IP Reference Model

Description of TCP/IP reference model is shown below :

1. Host-to-network Layer : This is the lowest layer in TCP/IP reference model. The host has to connect to the network using some protocol, so that it can send the IP packets over it. This protocol varies from host to host and network to network.

Various host-to-network protocols are :

ARPANET, SATNET, LAN, packet radio.

2. Application Layer : The layer on top of transport layer is called as application layer. This layer provides services that can be used by other applications. In application layer some of important protocols are simple mail transfer protocol (SMTP), File transfer protocol (FTP), TELNET, DNS, HTTP, NNTP, etc.

3. Transport Layer : The layer above the application layer is called as transport layer. This layer allows the peer entities of the source and destination machines to converse with each other. The end to end protocols used here are TCP and UDP. TCP is a connection oriented protocol. TCP also handles the flow control. UDP (user datagram protocol) is the second protocol used in the transport layer. It is an unreliable, connectionless protocol and used for the application. Which do not want the TCPs sequencing or flow control.

4. Internet Layer : Top layer is called internet layer. The task of this layer is to allow the host to insert packets into any network and then makes them travel independently to the destination. The order in which the packets are received can be different from the sequence in which they were sent.

OSI model used in practice

Yes, OSI is used in practice. It is used to ensure that nationwide and worldwide data communication systems can be developed and are compatible to each other.

Q 41. Define X.400. **(PTU, May 2004)**

Ans. X.400 is an ITU-T (International Telecommunication Union-Telecommunication Standard for electronic mail and message handling.

Q 42. Comparison of bus and star topology.

Ans.

Bus topology	Star topology
1. It uses a single cable to connect all the nodes.	1. All the nodes are connected to central control hub.
2. There is no master or controller that controls the communication between the nodes.	2. Hub acts as controller and controls the communication between the nodes.
3. Data collisions occur frequently.	3. Chances of data collision are less.
4. Expansion of network i.e. addition of new node is difficult.	4. Expansion is easier.
5. Fault identification and isolation is not easier.	5. Fault identification and isolation is relatively easier.
6. Failure of central line/cable collapses the entire system.	6. Failure of central controller or hub collapses the entire system.

Q 43. Comparison between ring and star topology.

Ans.

Ring Topology	Star Topology
1. All nodes are connected in form of ring : each device in a ring is connected to two devices on either side of it.	1. All the nodes are connected to central controller called hub.
2. Each node has dedicated point to point link with two devices only.	2. Each node has a dedicated point to point link only to central hub.
3. There is no central controller in ring networks that controls the communication between the nodes.	3. Central controller controls the communication between any two nodes in a network.
4. Ring network is relatively difficult to reconfigure and troubleshoot.	4. Star network is easy to configure and troubleshoot.
5. Failure of one node can affect the whole network.	5. Failure of one node or link does not affect the whole network.

Q 44. Explain benefits of computer network.

Ans. 1. Sharing of information : Computer networks enable us to share data and information with the computers that are located geographically large distance apart.

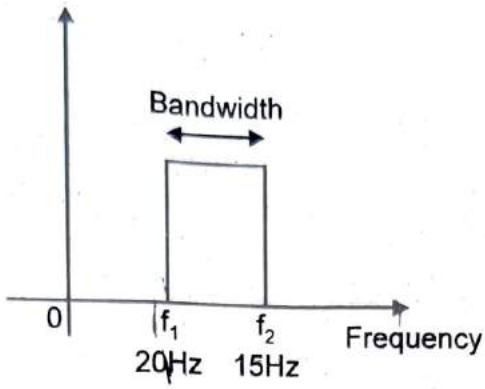
2. Sharing of resources : Networks enable us share various kinds of hardware and software resources.

3. Facilitates centralized management : In client server networks, central server can look after the maintenance activity, backup of data and the management of software installed on the server.

4. Communication speed is increased : With the use of computer network communication has become faster.

Q 45. Write a short note on bandwidth, bitrate and error rate. (PTU, Dec. 2004)

Ans. Bandwidth : Bandwidth is defined as the portion of electromagnetic spectrum occupied by a signal. We may also define the bandwidth as the frequency range over which an information signal is transmitted.



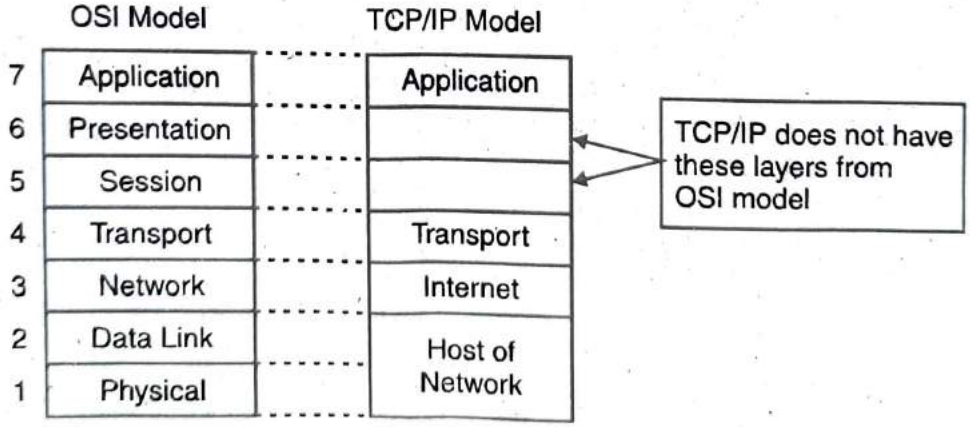
Bit rate : Bit rate is the number of bits transmitted or sent in one second. It is expressed in bits per second (bps).

$$\text{Bit rate} = \frac{1}{\text{Bit interval}}.$$

Error rate : It is defined as number of errors occurring per by transmitted byte.

Q 46. Diagrammatically explain TCP/IP concept.

Ans.



Description of TCP/IP Model :

Internet Layer : This layer holds the whole architecture together. It allows the host to insert packets into any network and then make them travel independently to the destination. The order in which the packets are received can be different from the sequence in which they were sent. Then the higher layers are supposed to arrange them in the proper order. It is supposed to deliver IP packets to their destinations.

Transport Layer : This layer allows the peer entities to the source and destination machines to converse with each other. The end to end protocols used here TCP and UDP. TCP is a reliable connection oriented protocol, it allows a byte stream transmitted from one

machine to be delivered to the other machine without introducing any errors. UDP is the second protocol used in the transport layer.

Application Layer : TCP/IP model does not have session or presentation layers because they are of little importance in most applications. The layer on top of transport layer is called as application layer. The protocols related to this layer are all high level protocols such as TELNET, FTP, SMTP, etc.

Host to Host Network Layer : This is the lowest layer in TCP/IP model. The host has to connect to the network using some protocol so that it can send IP packets over it.

Q 47. Explain network software.

Ans. 1. Network software is one of the highly structured components.

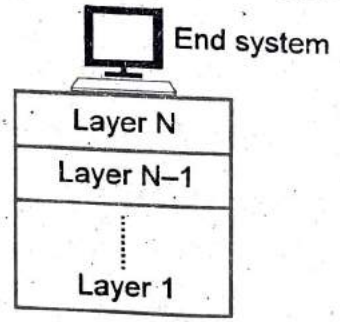
2. Network software is defined in such a way so that it can handle different protocols and services in an efficient manner.

It contains **network architecture**

Network architecture refers to the set of layers and protocols used in the network.

Layers :

- Networks are organized as a stack of different layers or levels.
- These layers are usually built one upon the other.



Protocols : Protocol refers to set of methods and rules used in a particular layer.

Q 48. Explain interfaces.

Ans. 1. Interface exists between each pair of adjacent layer.

2. Interface defines rules and procedure for hierarchical communication.

3. It defines the various primitive operations and services that the lower layers make available to upper layers.

Q 49. With neat diagrams give an account of OSI layering. Discuss in brief functions of each layer with emphasis on the network layer and its services to above layers. **(PTU, May 2008)**

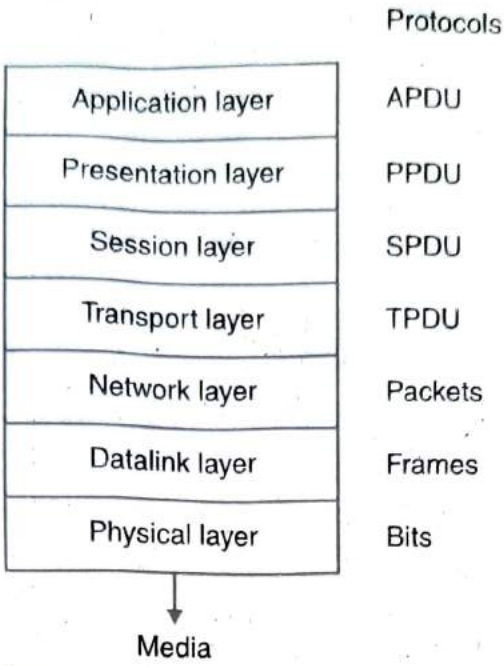
OR

Explain the role of different layers of OSI-ISO reference model? Also compare at with TCP/IP protocol architecture. **(PTU, Dec. 2011, 2006)**

OR

Explain the various layers of OSI model and compare it with TCP/IP model. **(PTU, May 2012)**

Ans. OSI reference model is a seven layer model. A seven layer reference model is shown below :



Functions of different layers :

Layer 1 : The Physical Layer :

1. To activate, maintain and deactivate the physical connection.
2. To define voltages and data rates needed for transmission.
3. To convert the digital bits into electrical signal.
4. To decide whether the transmission is simplex, half duplex or full duplex.
5. It does not detect or correct errors.

Layer 2 : Data Link Layer :

1. It provides synchronization and error control for the information which is to be transmitted over the physical link.
2. To enable the error detection, it adds error detection bits to the data which is to be transmitted.
3. The encoded data is then passed to the physical layer.
4. There error detection bits are used by the data link or other side to detect the correct errors.

Layer 3 : Network Layer :

1. To route the signals through various channels to the other end.
2. To act as the network controlled by deciding which route data should take.
3. To divide the outgoing messages into packets.

Layer 4 : Transport Layer :

1. It decides if the data transmission should take place or parallel path or single path.
2. It does the function such as multiplexing, splitting or segmenting on the data.
3. Transport layer guarantees transmission of data from one to other end.

Layer 5 : Session Layer :

1. This layer manages and synchronize conversion between two different applications.
2. It controls logging on and off.

Layer 6 : The Presentation Layer :

1. The presentation layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.
2. The form and syntax of the two communication systems can be different.

Layer 7 : Application Layer :

1. It is at the top of all, it provides different services such as manipulation of information in various ways.
2. The function such as login, or password checking.

Difference between OSI and TCP/IP model :

OSI	TCP/IP
1. OSI has seven layers. 2. Transport layer guarantees delivery of packets. 3. Horizontal approach. 4. Separate session layer. 5. Separate presentation layer. 6. OSI is truely a general model.	1. TCP/IP has four layers. 2. Transport layer does not guarantee delivery of packets. 3. Vertical approach. 4. No session layer. 5. No presentation layer. 6. TCP/IP cannot be used for any other application.

Q 50. What is session layer? **(PTU, Dec. 2006)**

Ans. The session layer is layer 5 of the seven-layer OSI model of computer networking. The session layer provides the mechanism for opening, closing and managing. A session between end-user application process i.e. a semi-permanent dialogue.

Session layer services are commonly used in application environments that make use of remote procedure calls (RPCs).

Q 51. Explain where the following fit in the OSI reference model.
(i) A 4 kHz analog connection across the telephone network.
(ii) A 33.6 kbps modem connection across the telephone network.
(PTU, Dec. 2008)

Ans. 1. Physical iayer
2. Physical layer.

Q 52. Write about the following terms SDU, IDU, SAP. **(PTU, May 2007)**

Ans. SDU : Service data unit.

IDU : Interface data unit.

SAP : It is service access point. It is a type of address that is used to identify the user of a protocol.

Q 53. Explain the architectural structure of DQDBMAN. **(PTU, May 2007)**

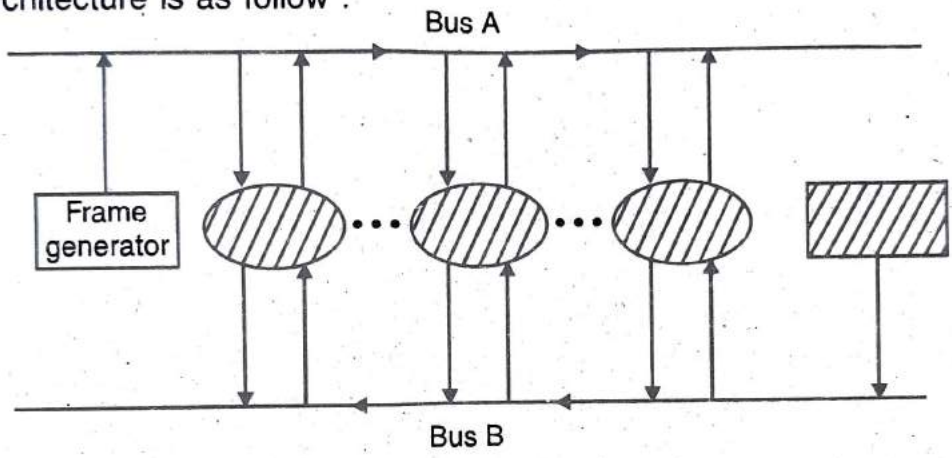
Ans. DQDB : Distributed queue dual bus defined in IEEE 802.6 DQDB is a Data-link layer communication protocol for metropolitan area nework (MAN), specified in the IEEE

802.6 standard, designed for use in MANs. DQDB is designed for data as well as voice and video transmission based on cell switching technology. DQDB, which permits multiple systems to interconnect using two unidirectional logic buses, is an open standard that is designed for compatibility with carrier transmission standards such as SMDS, which is based on the DQDB standards.

For, a MAN to be effective it requires a system that can function across long distance of several miles, have a low susceptibility to error, adopt to the number of nodes attached and have variable bandwidth distribution.

The DQDB is composed of a two bus lines with stations attached to both and a frame generator at the end of each bus. The buses run in parallel in such a fashion as to allow the frames generated at the end of each bus. The buses run in parallel in such a fashion as to allow the frames generated to travel across the stations in opposite directions.

The architecture is as follow :



Q 54. List two important functions of data link layer. **(PTU, May 2004)**

Ans. 1. To enable the error detection, it adds error detection bits to the data which is to be transmitted.

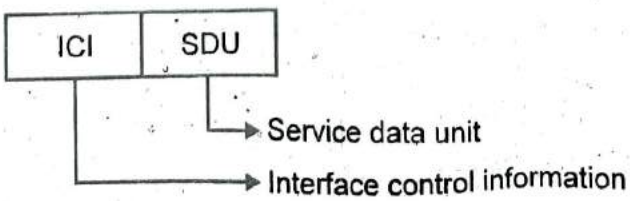
2. Functions of the data link layer are synchronization and error control for the information which is to be transmitted over the physical link.

Q 55. Explain services.

Ans. 1. The services between the adjacent layers entities are using for carries out function properly and is provided by SAP.

2. Each SAP supports one communication path and has a unique address for its identification.

3. For successful exchange of information between two layers, a set of rules about the interface should be presented.



Q 56. Explain the advantages of layered protocols in brief.
(PTU, May 2006 ; Dec. 2005)

Ans. 1. Addressing : For every layer, it is necessary to have a mechanism to identify senders and receivers. Since there are multiple possible destinations, some form of addressing is required in order to specify a specific destination.

2. Direction of Transmission : Another point is the direction of data transfer. Based on whether the system communications only in one direction or otherwise, the communication systems are classified as under :

(i) Simplex System
(ii) Half Duplex System
(iii) Full Duplex System.

3. Error Control : Physical communication circuits are not perfect. Error detection and connection both are essential. Many error detecting and correcting codes are known out of which those agreed by sender and receiver should be used. The receiver should be able to tell the sender by some means, that it has received a correct message.

4. Avoid Loss of Sequencing : All the communication channels cannot preserve the order in which messages are sent on it. So there is a possibility of loss of sequencing. To avoid this, all the pieces should be numbered so that they can be put back together at the receiver in the appropriate sequence.

5. Ability of Receiving Long Messages : At several levels, another problem should be solved which is inability of all processes to accept arbitrarily long messages. So, a mechanism needs to be developed to disassemble transmit and then reassemble message.

Q 57. What are the X.25 layers? How does each relate to OSI model?
(PTU, Dec. 2004 ; May 2004)

OR

Explain X.25 levels 2 and 3.
(PTU, May 2006)

Ans. X.25 is a standard used by many older public networks specially outside the US. The packet switching networks use X.25 protocol. The X.25 recommendations were first prepared in 1976. The protocol is based on the protocols used in early packet switching networks such as ARPANET, DATAPAC, TRANSPAC, etc.

A protocol X.21 which is a physical layer protocol is used to specify the physical electrical and procedural interface between the host and network. The problem with this standard is that it needs digital signal rather than analog signals on telephone lines. The data link layer standard has a no. of variations. It is designed for error detection and corrections. The network layer protocol standard has flow control, delivery configuration, etc.

X.25 is a connection oriented service, it supports switched virtual circuit is established between a computer and network. When the computer sends a packet to the network requesting to make a call to other computer.

In order to allow the computers which do not use the X.25 to communicate with the X.25 protocol. Three layers of X.25 :

1. Physical Layer
2. Data Link Layer
3. Packet Layer.

Q 58. What do you mean by network reliability? **(PTU, Dec. 2009 ; May 2009)**

Ans. By the use of network, alternative resources can be made available. If one particular resource goes out of orders or failed due to certain reasons, others may be used at reduced speed and performance. This is called network reliability.

Q 59. Differentiate between primary server and a secondary server.

(PTU, Dec. 2007)

Ans. The only real difference between a primary and secondary server is how they get the data for the domain for which they have authority. A primary server gets its data from a local file. A secondary server gets its data through a 'zone transfer' from another server (usually, but not necessarily primary server). That is the entire difference any given name server can be a 'primary server for some domain and a secondary server for other domains.'

Q 60. What does the following address corresponds to (unicast, multicast or broadcast) : 4A:30:10:21:10:1A

(PTU, Dec. 2011)

Ans. To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast.If it is odd, the address is multicast.If all digits are F's, the address is broadcast. Therefore this is a unicast address because A in binary is 1010.

Q 61. Define baud rate.

(PTU, May 2012)

Ans. In telecommunication and electronics, baud is synonymous to symbols per second or pulses per second. It is the unit of symbol rate also known as baud rate or modulation rate, the number of distinct symbol changes made to the transmission medium per second in a digitally modulated signal or a line code. The baud rate is related to but should not be confused with gross bit rate expressed in bit/s. The symbol duration time, also known as unit interval, can be directly measured.

Q 62. What are TLD servers?

(PTU, May 2012)

Ans. A TLD (Top-Level domain) is the highest level of domain names in the root zone of the DNS of the Internet. For all domains in lower levels, it is the last part of the domain name, that is, the label that follows the last dot of a fully qualified domain name. In other words, the last part of an Internet domain name that follows the final dot of a fully qualified domain name.

Q 63. List two important features of LAN. **(PTU, May 2012)**

Ans. LAN is a local area network that is used to create network in small areas.

Importance of LAN :

1. Limited geographic operation.
2. High speed data transfer rates.
3. Cabling is a primary transmission medium.

Q 64. Compare OSI and TCP/IP models. **(PTU, Dec. 2012)**

Ans. OSI stands for open source interconnection and TCP/IP stands for transmission control protocol/internet protocol.

OSI Model	TCP/IP Model
1. OSI stands for open system interconnection. It is called so because it allows any two different systems to communicate open regardless of their architecture.	1. TCP/IP stands for transmission control protocol/internet protocol. It is named after these two protocols, being part of this model.
2. It is complex model.	2. It is comparatively simple model.
3. OSI model has seven layers : Physical, Data link, Network, Transport, Session, Presentation and application layer.	3. TCP/IP model has four layers : Host-to-network, Network, Transport and Application layer.
4. Session and presentation layers are present in this model.	4. There is no session and presentation layer in this model.
5. This model provides clear distinction between services, interfaces and protocols.	5. It does not clearly distinguish between services, interfaces and protocols.
6. Protocols do not fit well into the model, because model was defined first before implementation takes place.	6. TCP and IP protocols fit well in this model as model is defined after protocols were implemented.
7. OSI model supports both connectionless and connection oriented communication in network layer.	7. TCP/IP model supports only connectionless communication in network layer.
8. OSI model provides quality of service.	8. It does not provide quality of service.
9. In OSI model two independent full duplex connections can be established.	9. In TCP one connection can be established.
10. Minimum size of OSI header is 5 bytes.	10. Minimum size of TCP header bytes.
11. The OSI model uses seven different TPDUs.	11. TCP/IP model uses only one TPDU.

Q 65. What are the disadvantages of bus topology? **(PTU, Dec. 2012)**

Ans. In bus topology, there is a single communication line or cable that is shared by all the nodes in a network.

Disadvantages :

1. If the main central line fails, the entire network collapse.

2. In this topology, only limited number of devices can be included. Signal reflection at tap causes degradation in quality. This degradation can be controlled by limiting the number and distance between these taps.

3. It is difficult to diagnose a fault in the system as single communication channel is shared by the network.

4. Sharing a single communication channel results in slower access time.

Q 66. What is a protocol? **(PTU, Dec. 2012, 2009 ; May 2008)**

Ans. Protocols are set of rules and regulations that uniquely identify the situation. There are many protocols like TCP/IP, TPDU, Elementary protocol like HDLC, SDLC and sliding window protocol.

There are some of the elementary data link protocols :

1. An unrestricted simplex protocol.
2. A simplex stop and wait protocol.
3. A simplex protocol for noisy channel.

Q 67. Explain about MAN. **(PTU, May 2008 ; Dec. 2006)**

Ans. Metropolitian Network (MAN) : MAN falls between LAN and WAN, it interconnects computer within a city, it uses DQDB architecture, it is also called as distributed dual queue bus. It has two unidirectional cables to which computers are connected. It is governed by IEEE 802.6 standard. The implementation of MAN provides transfer rate from 34 Mbp/s to 15 Mbp/sec. It is not as slow as LAN. It is designed with unidirectional bus. They use broadband cables as transmission media. They also use fibre optic cables.

❑❑❑

Chapter 2

Physical Layer

Contents

Concept of Analog and Digital Signal, Bandwidth, Transmission Impairments : Attenuation, Distortion, Noise, Data rate limits : Nyquist formula, Shannon Formula, Multiplexing : Frequency Division, Time Division, Wavelength Division, Introduction to Transmission Media : Twisted pair, Coaxial cable, Fiber optics, Wireless transmission (radio, microwave, infrared), Switching: Circuit Switching, Message Switching, Packet Switching and their comparisons.

POINTS TO REMEMBER

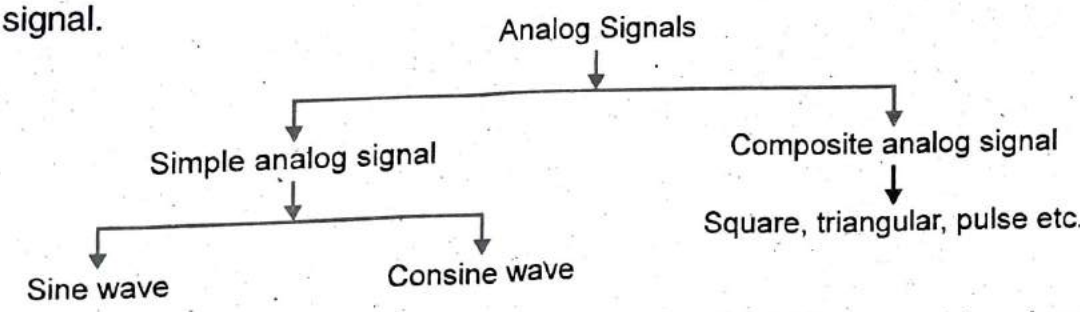
- A digital signal is a discrete time signal having finite number of amplitudes. A (zero) is represented by zero values or volts.
- Digital transmission can be either parallel or serial in mode.
- In parallel transmission, a group of bits is sent simultaneously with each bit on a separate line.
- Multiplexing is the simultaneous transmission of multiple signals across a single data link.
- A DTE is a source or destination for binary digital data.
- In serial transmission, there is only one line and the bits are sent sequentially.
- In asynchronous serial transmission, each byte is framed with a start bit and a stop bit. There may be a variable length gap between each byte.
- In synchronous serial transmission, bits are sent in a continuous stream without start and stop bits and without gaps between bytes.
- Space and time division switches may be combined.
- Switching is a method in which multiple communication devices are connected to one another efficiently.
- A switch is intermediary hardware or software that links device together temporarily.
- A modem is a DCE that modulates and demodulates signal.
- A modem changes digital signal to analog signals using ASK, FSK, PSK or QAM modulation.
- ASK modulation is especially susceptible to noise.

- Signal travels from transmitter to receiver.
- TDM can be classified as either synchronous or asynchronous.
- The bit interval is the time required to send one single bit.
- Bandwidth is defined as the portion of the electromagnetic spectrum occupied by a signal.
- Bit rate is the number of bits transmitted or sent in one second.
- FDM is an analog technique that can be applied when the bandwidth of link is greater than the combined bandwidth of the signals to be transmitted.
- Wave division multiplexing is conceptually same as FDM, except that the multiplexing and demultiplexing involve light signals transmitted through fibre optical channels.
- In packet switching message is divided into many segments or packets. Each packet is treated as separate communication.
- In telegraphy the text message is encoded using the morse code into sequence of dots and dashes.
- PSTN is an example of circuit-switched network.
- A DTE is a source or destination for binary digital data.

QUESTION-ANSWERS

Q 1. Explain analog signals.

Ans. These are the signals which can have infinite number of different magnitudes or values. They vary continuously with time. Sine wave, triangular wave, etc. are the examples of analog signal.



1. Simple Analog Signal : It is the analog signal which cannot be decomposed into simpler signals.

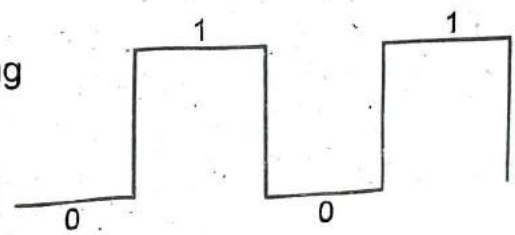
2. Composite Analog Signal : It is composed of or made of multiple sine or cosine waves.

Q 2. Explain digital signal.

Ans. A digital signal is a discrete time signal having finite number of amplitudes.

A zero (0) is represented by zero volts

1 by some positive voltage.



Q 3. Explain bit interval and bit rate.

Ans. Bit interval : The bit interval is the time required to send one single bit.

Bit rate : Bit rate is the number of bits transmitted or sent in one second. It is expressed in bits per second (bps).

$$\text{Bit rate} = \frac{1}{\text{Bit interval}}.$$

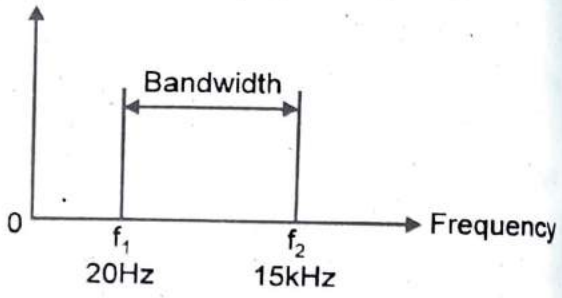
Q 4. Explain bandwidth.

Ans. 1. Bandwidth is defined as the portion of the electromagnetic spectrum occupied by a signal.

2. Bandwidth can also define as the frequency range over which an information signal is transmitted.

3. Bandwidth is the difference between the upper and lower frequency limits of the signal.

$$BW = f_2 - f_1$$
$$= 15000 - 20$$
$$= 14980 \text{ Hz}.$$

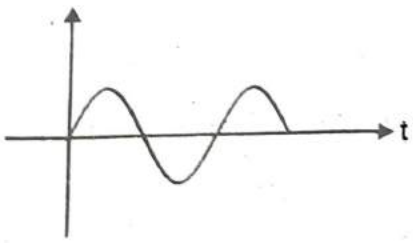
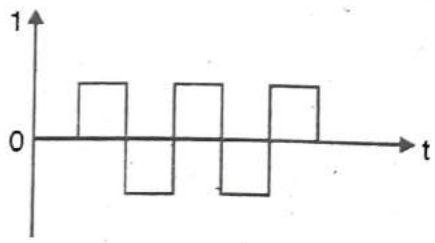


Q 5. Contrast and difference between analog and digital signal.

Ans. The two types of signals that are used in data communication are :

(a) Analog signal

(b) Digital signal

Analog Signal	Digital Signal
1. They have infinite number of different magnitudes or values.	1. They have finite number of predetermined distinct magnitudes.
2. They are generated by signal generators transducers.	2. Digital signals are generated by computers.
3. They continuously vary with time.	3. They are discrete in nature.
4. Sine, wave, triangular waves are examples of analog signals.	4. Binary signals are examples of digital signals.
5. 	5. 

Q 6. What are the units of period and frequency?

Ans. Period : Period is the reciprocal of the frequency. It is the duration of one cycle in repeating even unit of period is second. The period is denoted by T, is length of time taken by one cycle and is reciprocal of frequency.

$$T = \frac{1}{f}$$

Frequency : It is the number of occurrence of repeating event per unit time. S.I. unit of frequency is hertz (Hz).

Q 7. Explain the data transmission concept.

Ans. Data transmission is movement of data which is in the form of bits between two or more digital devices. The data transmission takes place over some physical medium from our system to another system.

Data transmission can be of two types :

1. Serial transmission
2. Parallel transmission.

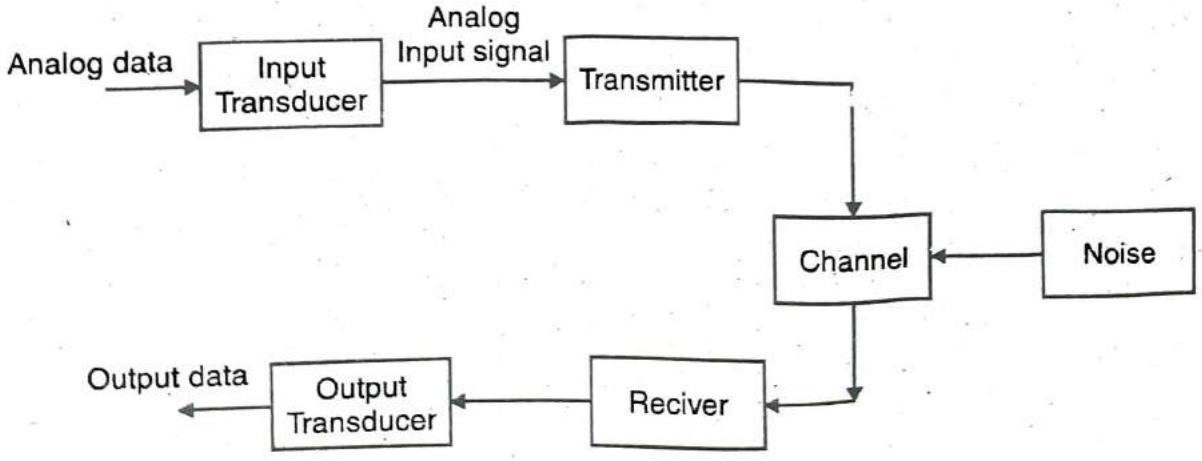
Q 8. Define the difference between synchronous transmission and asynchronous transmission. **(PTU, May 2008)**

Ans.

Synchronous Transmission	Asynchronous Transmission
1. In this transmission, transmitter and receiver need to be synchronized.	1. In this transmission, there is no need of synchronization.
2. Speed of transmission is higher than asynchronous transmission.	2. Asynchronous transmission is slow because of the use of start and stop bits.
3. No need of start and stop bits for defining the start and end of transmission.	3. This transmission need start and stop bits for the starting and ending of the data.
4. Gap between data blocks is absent.	4. Gap between data blocks is present.

Q 9. Explain analog data transmission.

Ans. Analog data transmission consists of analog signals which has narrower bandwidth as compared to digital signals.



The analog data is firstly converted into electrical signal by input transducer. It then modulates some high carrier frequency inside the transmitter to produce modulated signal.

Q 10. Name various operations of physical layer.

Ans. Various operations of physical layer :

1. To activate, maintain and deactivate the physical connection.
2. To define voltages and data rates needed for transmission.
3. To convert the digital bits into electrical signal.
4. To decide whether the transmission is simplex, half duplex or full duplex.

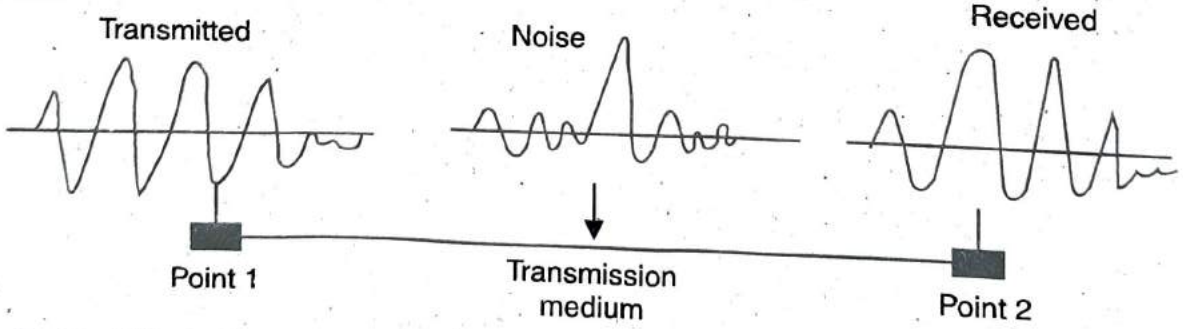
Q 11. Explain the difference between analog and digital communication.

Ans.

Analog Communication	Digital Communication
1. These signals transmitted are analog in nature.	1. Signals transmitted are digital in nature.
2. Noise immunity is poor.	2. Noise immunity is excellent.
3. Bandwidth is less.	3. High bit rate, there for higher bandwidth.
4. Not suitable for secret information.	4. Suitable for secret information.
5. Coding is not possible in the analog communication.	5. Coding techniques are possible.

Q 12. Explain noise.

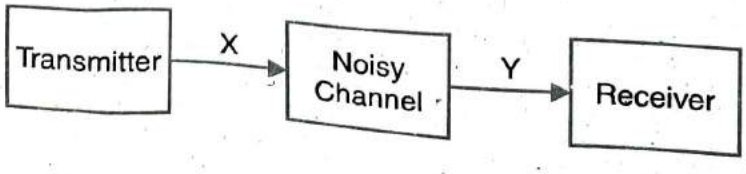
Ans. It is another problem, several types of noise such as thermal noise induced the signal. Thermal noise is the random motion of electrons in a wire that creates an extra signal not originally sent by transmitter. Induced noise comes from sources such as motors and appliances. These devices act as sending antenna and transmission medium acts as receiving antenna.



Q 13. What do you understand by shannon capacity? **(PTU, Dec. 2009)**

Ans. It defines the notion of channel capacity and provides a mathematical model by which one can compute it. Capacity of channel is given by the maximum of the mutual information between the I/P and O/P of channel. When the maximization is with respect to the I/P distribution.

Definition



Let X represent the space of signals that can be transmitted and Y the space of signals received, during a block of time over the channel

Py/x (y/x)

be the conditional distribution function of Y given X treating the channel as a known statistic system $P_{Y/X}$ (y/x) is an inherent fixed property of the communication channel. Then the joint distribution $P_{X,Y}$ (x, y) and X and Y is completely determined by the channel and by the choice of

$$P_X(x) = \int_y P_{X,Y}(x,y)\, dy$$

the marginal distribution of signal we choose to send over the channel. The joint distribution can be removed by using the identity.

$$P_{X,Y}(x, y) = P_{Y/X}\left(\frac{y}{x}\right) P_X(x)$$

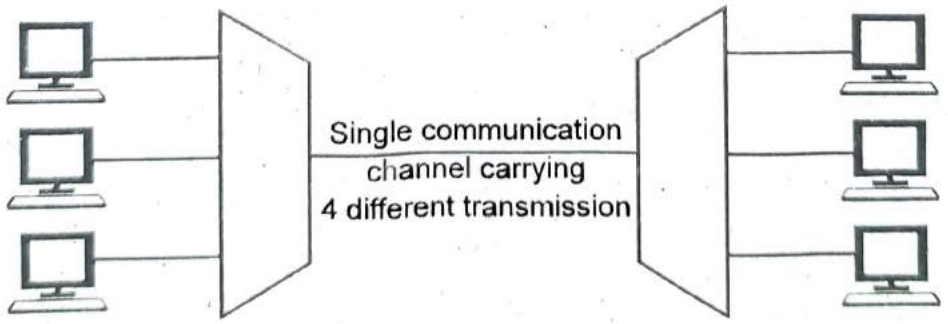
next maximize the amount of information that one can communicate over channel. Measure for this is the mutual information I (X, Y) and maximum mutual information is called channel capacity and given by

$$C = \text{SUP}\, I(X ; Y)\, P_X$$

Q 14. Define multiplexing.

Ans. It is the process of sending signals from two or more different sources simultaneously over a single communication channel. Therefore, in multiplexing, single communication line carries signal transmission or conversation at the same time.

Multiplexing is done by using a device called multiplexer (MUX) that combines n input lines one output line i.e. (many to one). Therefore, multiplexer (MUX) has several inputs and one output.



Q 15. Write types of multiplexing.

Ans. There are three different techniques used for multiplexing :

1. Frequency Division Multiplexing (FDM)
2. Wave Division Multiplexing (WDM)
3. Time Division Multiplexing (TDM).

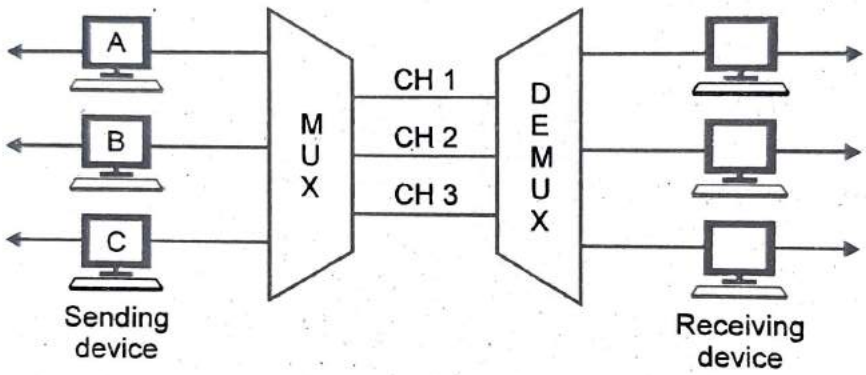
Q 16. Distinguish between baseband transmission and broadband transmission.

Ans. In a baseband transmission, the entire bandwidth of the cable is consumed by single signal. In broadband transmission, signals are sent on multiple frequencies, allowing multiple signals to be sent simultaneously.

Baseband transmission	Broadband transmission
1. Use digital signalling.	1. Uses analog signalling.
2. Bidirectional transmission.	2. Unidirectional transmission.
3. No frequency division multiplexing.	3. Frequency division multiplexing.
4. Signal travels over short distance.	4. Signal can travel over long distances.

Q 17. What is FDM? **(PTU, Dec. 2005)**

Ans. FDM : Frequency division multiplexing is an analog technique that can be applied when the bandwidth of link is greater than the combined bandwidth of the signals to be transmitted.



Q 18. Difference between synchronous and asynchronous TDM.

Ans. 1. In synchronous TDM, fixed time slots are allocated to each input line but in asynchronous TDM, time slot is available only when any input device has data to send.

2. Asynchronous TDM supports the same number of input lines as synchronous TDM with a lower capacity link.

3. In synchronous TDM, as the time slots are fixed and preassigned, a slot may be empty when given device is not transmitting and that much capacity is wasted. Asynchronous TDM avoids wastage of capacity of link by assigning time slots to the device which has data to be transmitted.

4. There is no need to add address of a receiver in case of synchronous TDM because time slots are fixed and preassigned to each device, so very little overhead information is required only for synchronization.

Q 19. Write short note on space division switches and time division switches.

Ans. Space division switches . These switches provide a separate physical connection between inputs and outputs. Space division switches were designed initially for the analog networks. These switches are known as non-blocking switches because they do not reject a connection request.

Time division switches : In these switches N input lines are scanned sequentially form a frame consisting of N slots.

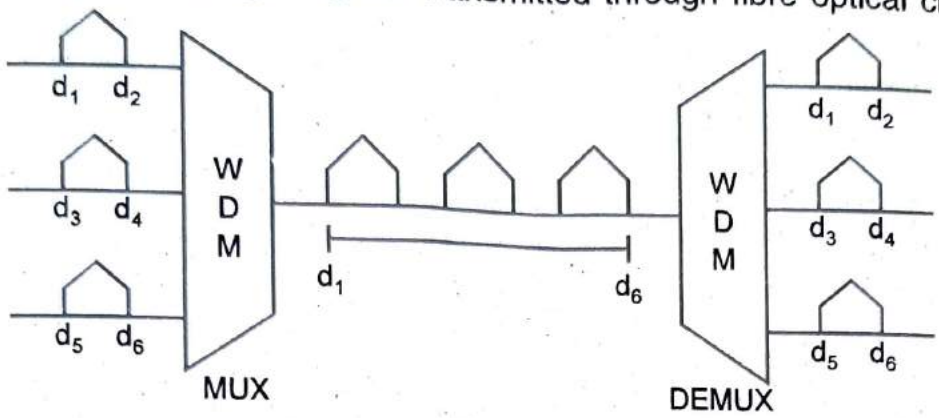
Types of **Time division** switches :

(a) Time-slot interchange

(b) TDM bus.

Q 20. What is WDM?

Ans. Wave division multiplexing is conceptually same as FDM, except that the multiplexing and demultiplexing involve light signals transmitted through fibre optical channels.



Q 21. Differentiate between guided and unguided media. **(PTU, Dec. 2011)**

Ans. Guided Media : Guided transmission media uses a cabling system that guides the data signals along a specific path. The data signals are found by the cabling system. Guided media is also known as Bound media.

Unguided Media : Unguided transmission media consists of a means for the data signals to travel but nothing to guide them along a specific path.

Q 22. Differentiate between baseband coaxial cable and broadband coaxial cable. **(PTU, May 2011, 2007)**

Ans. Data signals can be sent over a network cable in one of two ways : broadband or baseband. One good example of broadband signaling would be how you view different channels through your cable box and a signal coaxial cable carrying muliple signals in cable television. Whereas baseband signaling only sends a single signal over the cable. This type of signalling is typically used in Ethernet networks. With the exception of 10 broad 3 standard. Baseband uses very simple transceiver device that send and receive signals on a cable. The simplicity behind baseband signaling is that only three states need to be distinguished : one, zero and idle. Broadband transceivers are much more complex because they must be able to distinguish those same states, but on multiple channels within the same cable. Because of its simplicity, base band signaling is used on most Ethernet networks.

Q 23. What is switching? **(PTU, Dec. 2010, 2006)**

Ans. Switching of network can be of various types like :

1. Circuit switching
2. Packet switching
3. Message switching.

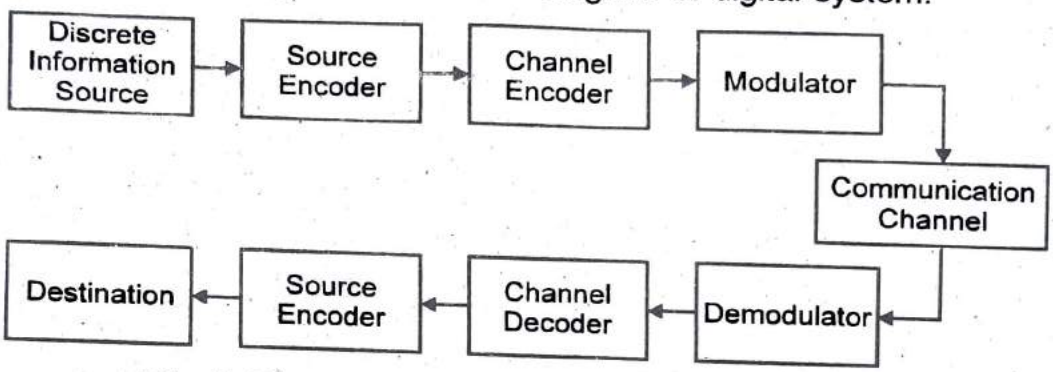
The switched network consists of series of interlink nodes called switches. Switches are hardwired software devices capable of creating temporary connections between two or more

devices. Link to a switch but not to each other. The nodes are connected through common devices and some nodes are used for the purpose of routing packages. The point to point line configuration creates a dedicated link between 2 devices and the channel is resend for transmission between those two devices.

The configuration uses actual length of wire to connect both ends but the options could be microwave or satellite link.

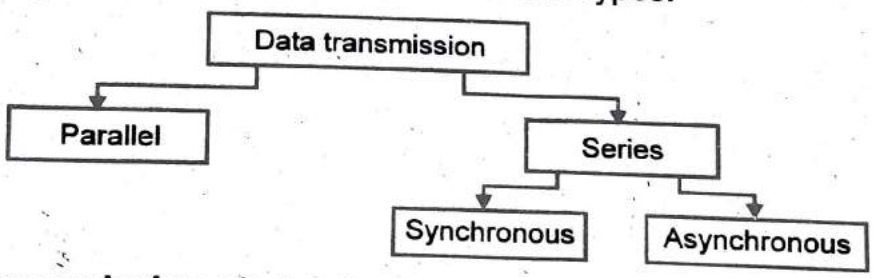
Q 24. Explain Digital data Transmission. **(PTU, Dec. 2006 ; May 2006)**

Ans. Digital data transmission, the message to be transmitted is digital in nature. The concept can be explained using the basic block diagram of digital system.

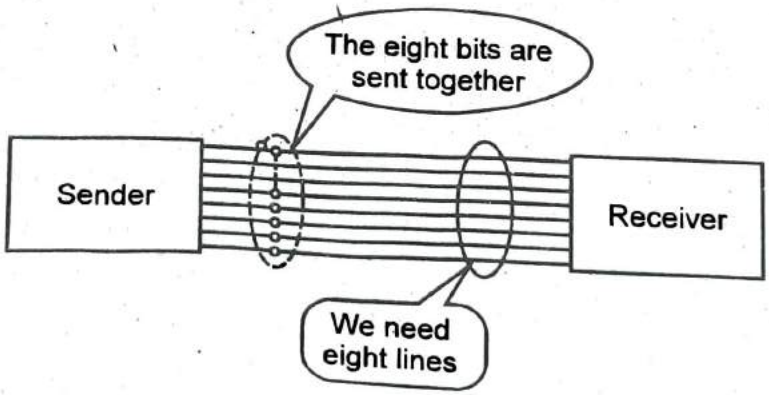


Block Diagram of Digital Data Transmission

- Digital data transmission is divided into two types.



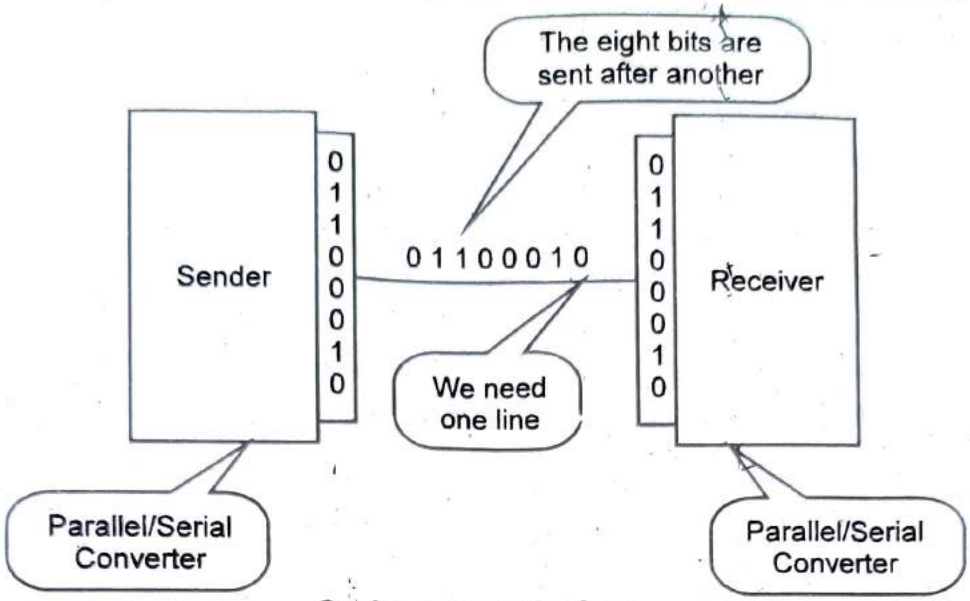
Parallel transmission : In this transmission, by grouping we can send data n bits at a time instead of one. This is called parallel transmission.



Parallel transmission

The advantage of parallel transmission is speed. Parallel transmission is usually limited to short distances.

Serial transmission : In serial transmission one bit follows another, so we need only one communication rather than n to transmit data between two communicating devices.



Serial transmission

The advantage of serial over parallel transmission is that with only one communication channel serial transmission reduces the cost of transmission over parallel.

Serial transmission is further divided into two types :

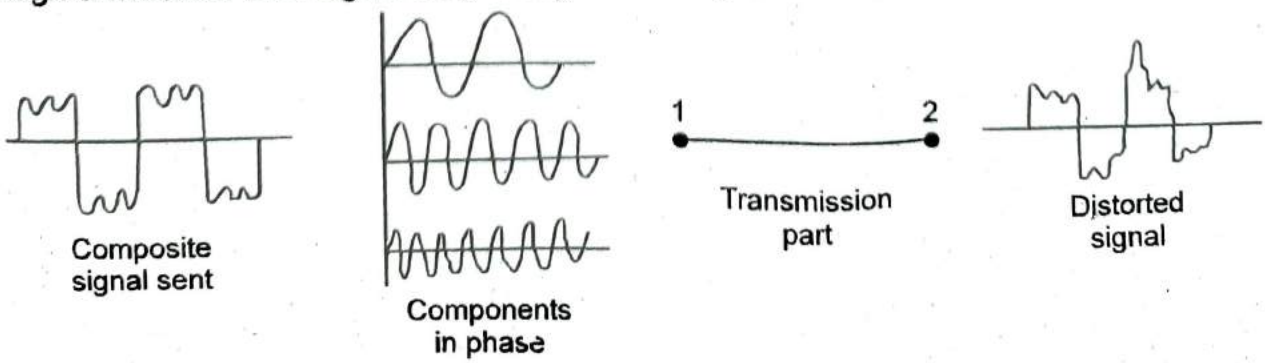
1. Synchronous
2. Asynchronous.

Q 25. What is packet switching? **(PTU, Dec. 2005)**

Ans. In packet switching message is divided into many segments or packets. Each packet is treated as separate communication, These packets are then sents to each station in a continuous sequence. The packets from various messages may be transmitted together and packets of same message may be dispatched over many different lines. Each packet has a header with a packet address and source and destination address. The packets are reassemble into their original message when they reach their destination.

Q 26. Explain distortion.

Ans. Distortion is change in the shape and form of signal. Composite signals which are made-up of different frequencies and each signal component has its own propagation speed through a medium and signal may delay in arriving at the final destination.



Q 27. What are the major advantages and disadvantages of microwave transmission?

Ans. Advantages :

1. No cables needed.
2. Multiple channels available.
3. Wide bandwidth.

Disadvantages :

1. Line of sight will be disrupted if any obstacle, such as new buildings are in the way.
2. Signal absorption by the atmosphere. Microwaves suffer from attenuation due to the atmosphere conditions.
3. Towers are expensive to build.

Q 28. Write a short note on Shannon's theorem. **(PTU, May 2007)**

Ans. Shannon's theorem : Shannon's theorem gives an upper bound to the capacity of a link, in bits per second (bps), as a function of the available bandwidth and the signal-to-noise ratio of the link.

The theorem can be stated as

$C - B^* \log 2 (1 + S/N)$

Where C – achievable channel capacity ; B – Bandwidth of the line

S – Average signal power ; N – Average noise power

The signal to noise ratio (S/N) is usually expressed in decibels (dB) given by the formula

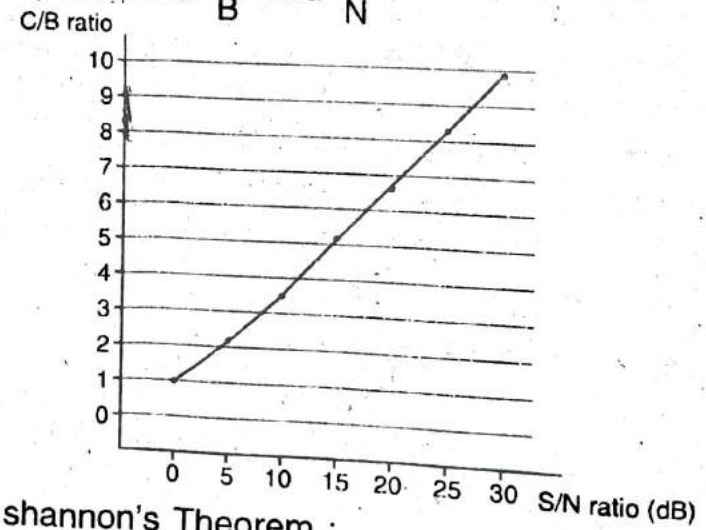
$10 * \log 10 (S/N)$

for example signal to noise ratio of 1000S is commonly expressed as :

$10 * \log 10 (1000) = 30$ dB

Here is a graph showing the relationship between $\frac{C}{B}$ and $\frac{S}{N}$

S/N ratio	C/B ratio
0	1.0
5	2.19
10	3.46
15	5.03
20	6.66
25	8.31
30	9.97



Here are two examples of the use of shannon's Theorem :

1. Modem : For a typical telephone line with a signal-to-noise ratio of 30dB and an audio bandwidth of 3KHz, we get a maximum data rate of

$C = 3000 * \log2 (1001)$

which is a little less than 30 Kbps.

2. Satellite TV channel : For a satellite TV channel with a signal-to noise ratio of 20dB and a video bandwidth of 10 MHz, we get a maximum data rate of

$C = 10000000 * \log2 (101)$

which is about 66 Mbps.

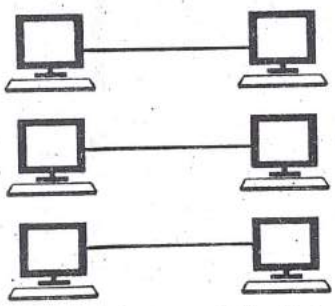
Q 29. Comparison between FDM and WDM.

Ans.

FDM	WDM
1. FDM stands for frequency division multiplexing.	1. WDM stands for wave division multiplexing.
2. In FDM, signals of different frequencies are combined to form a composite signal.	2. In WDM, signals of different wavelength are combined into a single composite signal.
3. The medium used for FDM is usually air.	3. The medium used for WDM is usually optical fibres.
4. FDM is used for FM and AM radio broadcasting.	4. WDM is used in SONET (synchronous optical networks).

Q 30. Explain advantages of multiplexing.

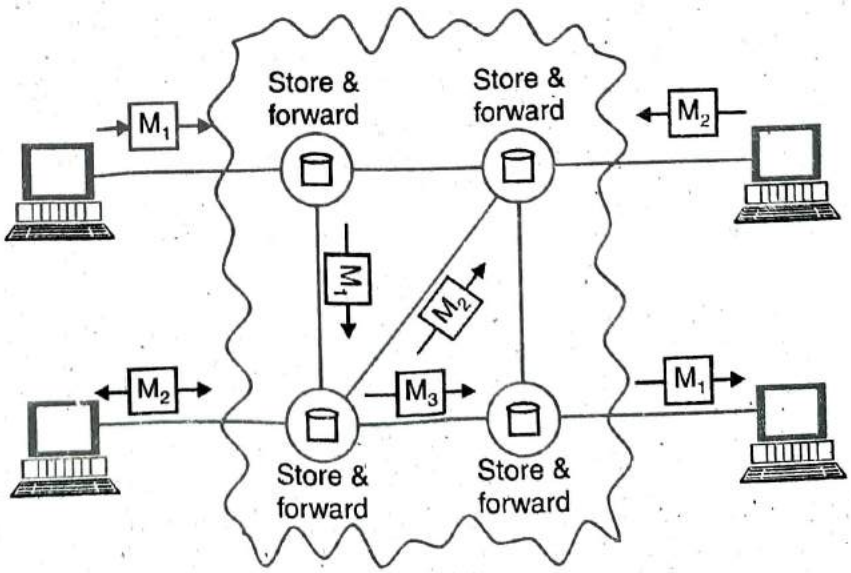
Ans. If no multiplexing is used between the users at two different sites that are distance apart, then separate communication lines would be required.



This is not only costly but also becomes difficult to manage. If multiplexing is used, then only one line is required. This leads to the reduction in the line cost and also would be easier.

Q 31. Explain message switching.

Ans. Message switching : In telegraphy the text message is encoded using the morse code into sequence of dots and dashes. Each dot or dash is communicated by transmitting short and long pulses of electrical current over a copper wire.



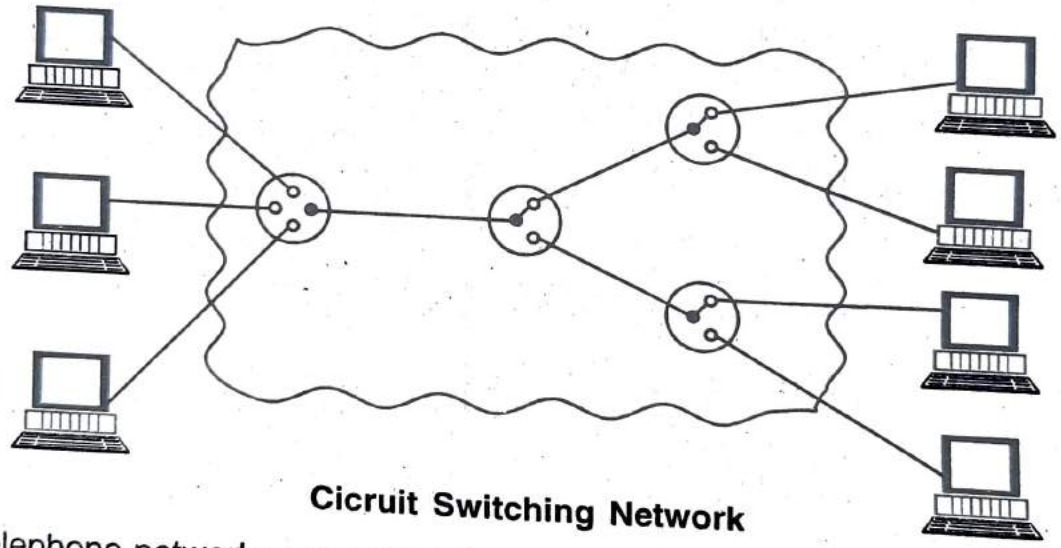
Message switching does not establish a dedicated path between two communication devices. In message switching, each message is treated as an independent unit.

Advantages :

1. It provides efficient traffic management by assigning priorities to the messages to be switched.
2. It reduces network traffic congestion between because it is able to store message until a communication channel becomes available.
3. With message switching, the network devices share the data channels.

Q 32. Explain circuit switching.

Ans. Circuit switching : The telephone network provides telephone services which involves real time circuit switching. The network connection allows electrical current and the associated voice signal to flow between the two users. The end to end connection is maintained for the duration of the call.



Cicruit Switching Network

The telephone networks are connection oriented because they require the setting up of a connection before the actual transfer of information can take place.

Advantages :

1. The major advantage of circuit switching is that the dedicated transmission channel the computers establish provides a guaranteed data rate.
2. In circuit switching because path, there is no delay in data flow.

Disadvantages :

1. The disadvantage of circuit switching is that, since the connection is dedicated it cannot be used to transmit any other data even if the channel is free.
2. Dedicated channels require more bandwidth.
3. It takes long time to establish connection.

Q 33. Why is multiple access required in LAN technologies? Compare FDM, TDM and SDM in terms of their ability to handle groups of stations. (PTU, May 2011, 2009)

Ans. Ethernet technology is the most widely used of all LAN technologies and it has

been standarized by IEEE 802.3 comittee one standards. The IEEE 802.3 standards define the medium access control (MAC) layer and the physical layer. The Ethernet MAC is a carrier sense multiple access with collision detection (CSMA/CD) system.

1. Frequency Division Multiplexing (FDM) : Frequency division multiplexing is a type of multiplexing technique in which signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequency are separated by enough bandwidth to accomodate the modulated signal.

2. Time Division Multiplexing (TDM) : TDM is a digital process that can be applied when the data rate capacity of the transmission medium is greater than the data rate required by the sending and receiving devices. In such a case, multiple transmissions can occupy a single link by subdividing them and interleaving the portions.

3. Wave Division Multiplexing (WDM) : It is same as FDM, except that the multiplexing and demultiplexing involve high signals transmitted through fibre optic channels. The idea is the same. We are combining different signals of different frequencies.

Q 34. Differentiate between infrared and light wave. **(PTU, Dec. 2010)**

Ans. Infrared light lies between the visible and microwave portions of the electromagnetic spectrum. Infrared light has a range of wavelengths, just like visible light has wavelengths that range from red light to violet. "Near infrared" light is closed in wavelengths to visible light and "for infrared" is closer to the microwave region of the electromagnetic spectrum. The longer, for infrared wavelengths are about the size of a pin head and shorter, near infrared ones are the size of cells or are microscopic.

Q 35. What is the main use of multiplexing? Explain various ways in which multiplexing can be done. **(PTU, May 2010)**

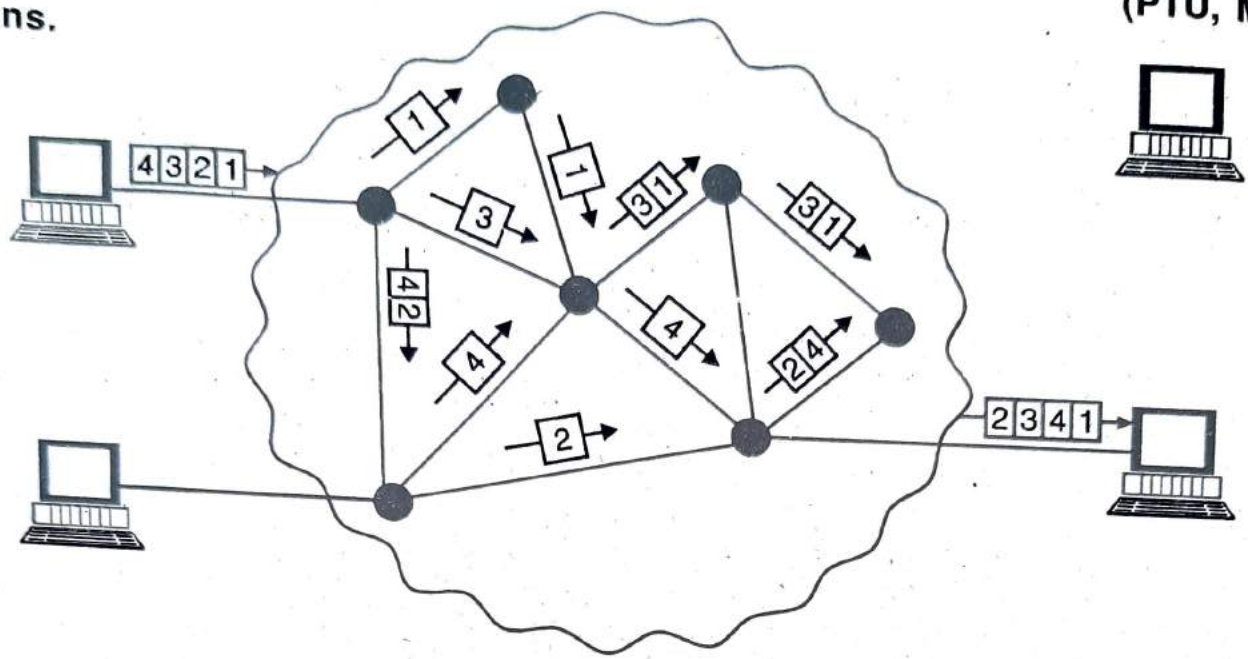
Ans. Multiplexing is the process of simultaneously transmitting two or more individual signals over a single communication channel. Due to multiplexing it is possible to increase the number of communication channels so that more information can be transmitted. The typical applications of multiplexing are in telementry and telephony or in the satellite communication. The multiplexing is used so that number of signals can be transmitted through a single channel at a same time separated from each other either in frequency domain or in time domain. The different types of multiplexing are :

1. Frequency Division Multiplexing (FDM) : Frequency division multiplexing is a type of multiplexing technique in which signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by enough bandwidth to accommodate the modulated signal.

2. Wave Division Multiplexing (WDM) : It is same as FDM, except that the multiplexing and demultiplexing involve high signals transmitted through fibre optic channels. The idea is the same. We are combining different signals of different frequencies.

Q 36. Using the diagram approach, explain the switching technique for packet switching. **(PTU, May 2006)**

Ans.



Packet switching

In packet switching, messages are broken into packets, each of which includes a header with source, destination and intermediate node address information individual packets take different routes to reach the destination independent routing of packets give two advantages.

1. Bandwidth is reduced by splitting data onto different routes in a busy circuit.
2. If a certain link in the network goes down during the transmission, the remaining packets can be sent through another route.

There are two methods of packet switching :

1. Datagram Packet Switching : In this method, a message is divided into a stream of packets. Each packet is separately addressed and treated as an independent unit with its own control instructors.

Before transmission starts, the sequence of packets and their destinations are established by the exchange of control information between the sending terminal, the network and the receiving terminal.

2. Virtual Circuit Packet Switching : It establishes a logical connection between the sending and receiving devices called virtual circuit. The sending device starts the conversation by communicating with the receiving device and agreeing as communication parameters. Once this virtual circuit is established, the two devices use it for the rest of the conversation.

Q 37. Why do we need multiplexing?

Ans. Multiplexing is a set of techniques that allows the simultaneous transmission of multiple signals across a single data link. Multiplexing is needed because of following : **(PTU, May 2009)**

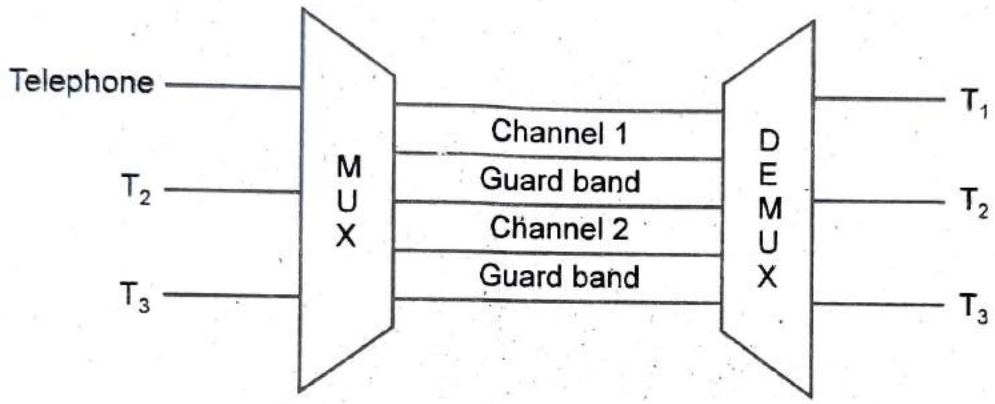
1. Because of multiplexing, it becomes possible to transmit more than one signal over a single channel.
2. It increases channel capacity.
3. It increases the efficiency of network.
4. It increases channel bandwidth.

Q 38. Differentiate infrared with light wave. **(PTU, May 2007)**

Ans. Infrared light lies between the visible and microwave portions of the electromagnetic spectrum. Infrared light has a range of wavelengths, just like visible light has wavelengths that range from red light to violet. "Near infrared" light is closet in wavelengths to visible light and "far infrared" is closer to the microwave region of the electromagnetic spectrum. The longer, far infrared wavelengths are about the size of a pin head and shorter, near infrared ones are the size of cells or are microscopic.

Q 39. What is the purpose of guard band in FDM?

Ans. In FDM, signals of different frequencies are combined into a single composite signal and are transmitted on the single link. Thus, each signal having different frequency forms a particular logical channel on the link and follows this channel only. These channels are then separated by the strips of unused bandwidth called guard bands.



Q 40. Explain radio wave transmission system.

Ans. Radio wave transmission system : Radio waves have frequencies between 10 kHz and 1 GHz. The range of electromagnetic spectrum between 10 kHz and 1 GHz is called radio frequency. Radio waves include the following types :

(i) Short wave used in AM radio.

(ii) Very high frequency used in FM radio and TV.

(iii) Ultra high frequency used in TV.

The radio frequency bands are regulated and require a license from the regulatory body. Unregulated frequency bands are also presented which operate at less than 1 watt transmitted power. Radio waves can broadcast omni directionally or directionally. Various kinds of antennas are used to broadcast these signals.

Q 41. Explain the advantages and disadvantages of optical fibre cable. **(PTU, Dec. 2010)**

Ans. Advantages of Optical Fibres : Some of the advantages of fibre optic communication over the conventional means of communication are as follows :

1. Small Size and Light Weight : The size of the optical fibre is very small (it is comparable to the diameter of human hair). Therefore, a large number of optical fibres can fit into a cable of small diameter.

2. Easy Availability and Low Cost : The material used for manufacturing of optical

fibres is "silica glass". This material is easily available. So the optical fibres cost lower than the cables with metallic conductors.

3. No Electrical or Electromagnetic Interference : Since the transmission takes place in the form of light rays the signal is not affected due to any electrical or electromagnetic interference.

4. Large Bandwidth : As the light rays have a very high frequency in the GHz range, the bandwidth of the optical fibre is extremely large. This allows transmission of more number of channels. Therefore, the information carrying capacity of an optical fibre is much higher than that of a co-axial cable.

Disadvantages of Optical Fibre : Some of the disadvantages of optical communication system are :

1. Sophisticated plants are required for manufacturing optical fibres.
2. The initial cost incurred is high.
3. Joining the optical fibres is a different job.

Q 42. Explain difference between hub and switch.
Ans.

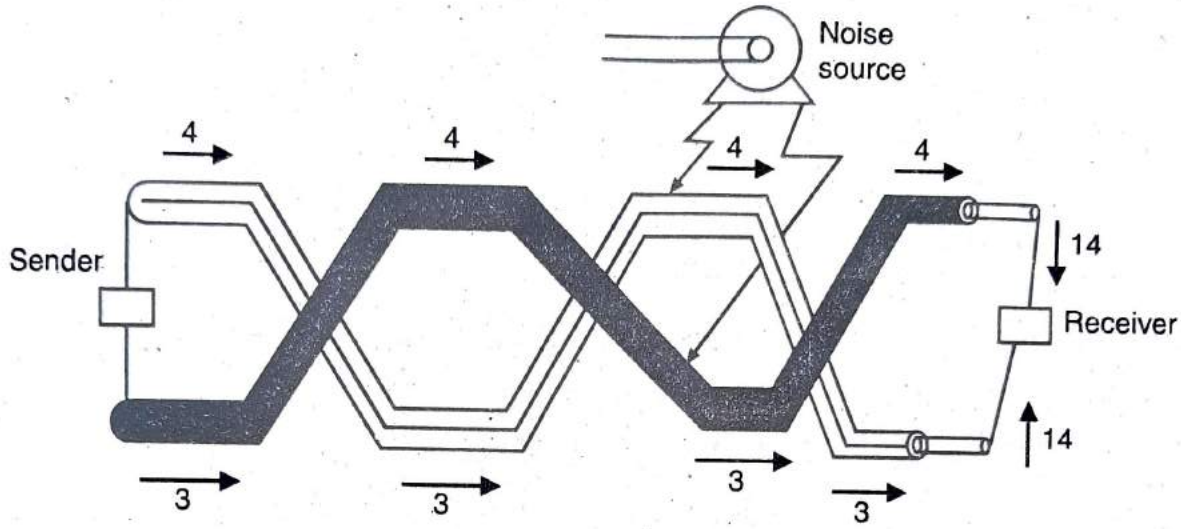
	Hub		Switch
1.	It is a broadcast device.	1.	It is a point to point device.
2.	It operates at physical layer.	2.	It operates on data link layer.
3.	It is not an intelligent device.	3.	It is an intelligent device.
4.	It simply broadcasts the incoming packet.	4.	It uses switching table to find the correct destination.
5.	It cannot be used as repeater.	5.	It can be used as repeater.
6.	Not very costly.	6.	Costly.

Q 43. Comparison between fibre optical cable and copper wire.
Ans.

	Fibre optical cable		Copper Wire
1.	Fibre optical cable carries data in form of light.	1.	Copper wire carries data in form of electrical signal.
2.	Optical fibres offer higher bandwidth than copper wire.	2.	Copper wire offers lower bandwidth.
3.	It is usually thin, lighter in weight and small in size as compared to other medias.	3.	Copper wire is heavier and thick as compared to optical fibre.
4.	There is no cross talk problem in optical fibres.	4.	Cross talk problem is prevalent in copper wires.
5.	The installation cost for optical fibre is high.	5.	Copper wire incurs less installation cost.

Q 44. Why are the wires twisted in a UTP (unshielded twisted-pair) cable used for data transmission? **(PTU, Dec. 2005)**

Ans. Wires are twisted in a UTP cable to avoid the damage of signal due to noise and interference. Two wires are twisted around each other at regular intervals and each wire is closer to the noise source for half the time and farther away for the other half. Therefore, commulative effect of interference is equal on both wires just because of twisting.



Total effect is 14 – 14 = 0

In fig., each section of wire has a load of 4 when it is on the top of the twist and 3 when it is on the bottom. The total effect of noise will, therefore, is (14 – 14). So wires are twisted so as to nullify the impact of noise.

Q 45. Comparison between fibre optical and twisted pair.

Ans.

	Twisted Pair		Fibre Optical
1.	Transmission of signal takes place in electrical form.	1.	Transmission of signal takes place in optical form i.e. with light.
2.	It consists of metallic conducting wires.	2.	It consists of glass fibre.
3.	It can be affected by external magnetic field.	3.	Cannot be effected by external magnetic field.
4.	Cost is less.	4.	Cost is high.
5.	Supports lower bandwidth.	5.	Supports very high bandwidth.
6.	Attenuation is very high.	6.	Attenuation is very low.

Q 46. Name various operations of physical layer. **(PTU, May 2009)**

Ans. Various operations of physical layer are :

1. To activate, maintain, deactivate the physical connection.
2. To define voltages and data rates needed for transmission.
3. To convert the digital bits into electrical signal.
4. To decide whether the transmission is simplex, half duplex or full duplex.

Q 47. Explain the difference between packet switching and message switching (PTU, May 2005)

Ans.

Packet switching	Message switching
1. The information is in the binary format.	1. The information can be in Mouse, Bandot or ASCIII format.
2. Each packet routed independently.	2. Packets routed namely.
3. Hierarchical addresses are used.	3. Geographical addresses are used.
4. Packet multiplexing shared media access networks.	4. Character or message multiplexing is done.
5. It places a tight upper limit on block size.	5. There is not limit on the block size.
6. The computer is the end terminal.	6. The telegraphs are the end terminals.

Q 48. What do you mean by virtual circuit?

Ans. Virtual Circuit : It establishes a logical connection between the sending and receiving devices called virtual circuit. All the packets travel through this virtual connection. The sending device starts the conversation by communicating with the receiving device.

Q 49. Is bit padding a technique for FDM or TDM? Is the framing bit used in FDM or TDM?

Ans. Bit Padding : It is the addition of one or more extra bits to transmission or storage unit to make it conform to standard size.

Framing : The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

Q 50. What is difference between frame and packet?

Ans. Frame : A group of bits representing a block of data.

Packet : Synonym for data unit, mostly used in network layer.

Q 51. How is WDM similar to FDM? How are they different? (PTU, May 2009)

Ans. WDM is conceptually same as FDM because in WDM different signals of different frequencies are combined.

WDM is different than FDM because in WDM light signals are multiplexed and demultiplexed rather than electrical signal and the frequencies to be multiplexed are of very high frequency as compared to the frequencies used in FDM.

Q 52. Mention the diffence between packet and circuit switching. (PTU, May 2008)

Ans. Packet Switching : In this technique, messages are broken up into packets and these packets include a header block which contains source, destination and intermediate node address information. Packets can take different routes to reach destination.

Circuit Switching : In this technique, a dedicated link is established and maintained between sender and receiver for the entire duration of conversation. Link is established then data is transmitted and after that link is terminated.

Difference between packet and circuit switching :

Packet Switching	Circuit Switching
1. In this switching, transmission is in form of packets.	1. In this switching, transmission is continuous.
2. Packets are stored until delivered.	2. Message cannot be stored.
3. This technique may have transmission delay.	3. It has negligible transmission delay.
4. It acquires and releases bandwidth as and when required.	4. It reserves the required bandwidth in advance.
5. Dynamic use of bandwidth.	5. Fixed bandwidth transmission.
6. No transparency.	6. Circuit switching is transparent.
7. Digital data is transmitted over various transmission media.	7. Analog and digital data can be transmitted over to media.
8. End terminal is computer.	8. End terminal is telephone or modem.
9. Overhead bits are in each packet for extra information.	9. No overhead bits after call set-up.
10. Speed and code conversion is required.	10. No speed or code conversion.
11. Each packet is routed independently.	11. Routing is done after call set up.
12. Small switching nodes are used.	12. Electromechanical or computerized switching nodes are used.
13. Used in computers i.e. internet.	13. Used nin telephone networks for bidirectional transfer of voice signals.

Q 53. Explain about circuit switch and folded switch. **(PTU, Dec. 2008)**

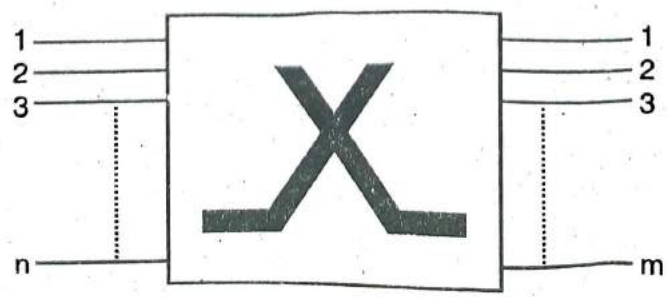
OR

What are two types of switches used in circuit switching?

(PTU, Dec. 2009 ; 2007)

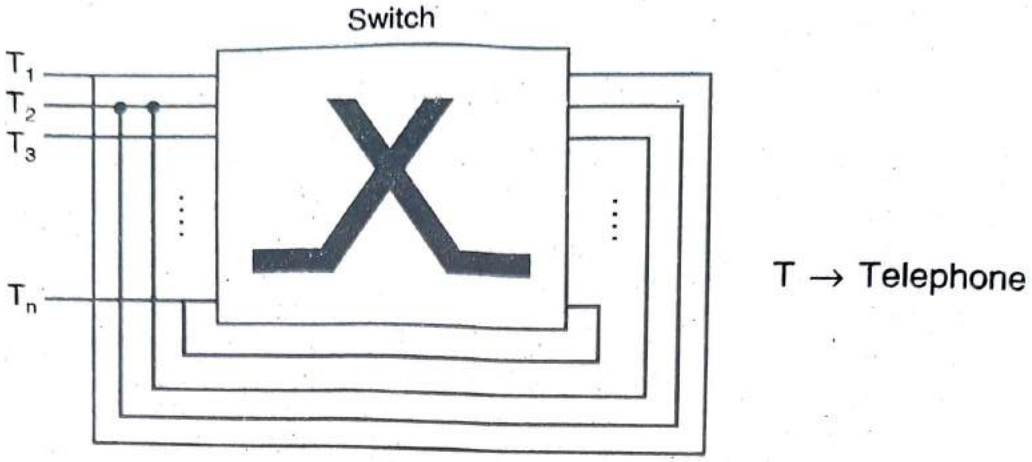
Ans. 1. Circuit switch 2. Folded switch.

Circuit Switch : It is a device with n input and m output that creates a temporary connection between an input link and an ouput link. The number of inputs does not have to match the number of outputs.



A Circuit Switch

Folded Switch : An n-by-n folded switch can connect n lines in full-duplex mode. For example, it can connect n telephones in such a way that each phone can be connected to every other phone.



A Folded Switch

Q 54. Comparison between various wireless medias.

Ans.

Radio Wave	Microwave	Infrared
1. Omni directional in nature.	1. Unidirectional.	1. Unidirectional.
2. Can penetrate solid objects and walls at low frequency. But at higher frequencies bounce off the obstacle.	2. Can penetrate solid objects at low frequencies. At higher frequencies cannot pass through solid objects.	2. Cannot pass through any solid object or walls.
3. Frequency range is between 3 kHz to 1 GHz.	3. Frequency range between 1 GHz to 300 GHz.	3. Frequency range between 300 GHz to 400 tHz.
4. Offers poor security.	4. Offers medium security.	4. Offers high security.
5. Attenuation is high.	5. Attenuation is variable.	5. Attenuation is low.
6. Set-up and usage cost is high.	6. Setup and cost is high.	6. Usage cost is very less.

Q 55. What are packet switched networks? **(PTU, May 2005)**

OR

What do you mean by packet switched network? **(PTU, Dec. 2009 ; May 2009)**

Ans. Packet-switched network is a type of network in which data to be transmitted is divided in smaller blocks of variable length blocks called packets. The maximum length of packet is established by the network. Longer transmissions are broken up into multiple packets.

Each packet contains not only data but also a header with control information such as priority codes and source and destination addresses. There are two popular approaches to packet switching :

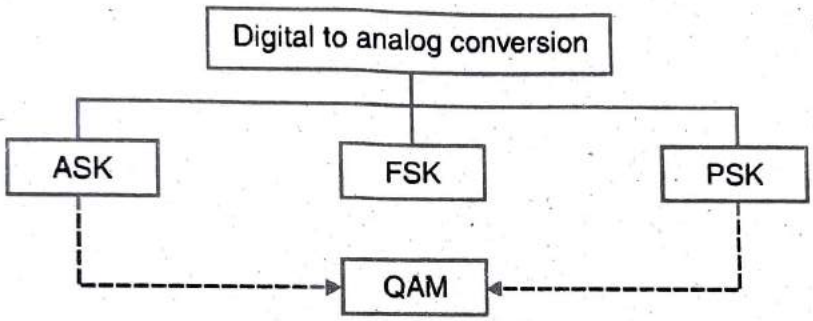
1. Datagram approach
2. Virtual circuit approach.

Q 56. What is the use of modulation? **(PTU, Dec. 2009)**

Ans. 1. It increases signal strength.
2. It increase the bandwidth of signal.
3. Reduces signal distortion.
4. Increases signal to noise ratio.
5. Modulated signals can travel long distance.
6. It increases the amplitude of signal.

Q 57. With a neat flow chart give all digital-to-analog methods and explain their relevance to modems with an example. **(PTU, May 2008)**

Ans. Flow chart for digital-to-analog conversion methods are :



Modem is a composite word that refers to the two functional entities that make up the device : a signal modulator and a signal demodulator. A modulator converts a digital signal into a analog signal using ASK, FSK, PSK or QAM. A demodulator converts an analog signal into digital signal. While a demodulator resembles an analog-to-digital converter. It does not sample a signal to create a digital fascimile, it merely reverse the process of modulation, that is, it performs demodulation.

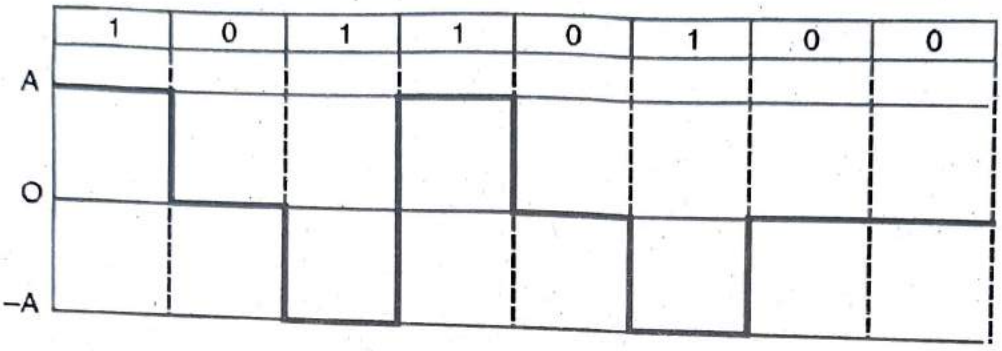
Q 58. What is line encoding? List the factors considered for selecting a line-encoding format. Draw and explain line-encoding formats for AMI and Manchester code. **(PTU, May 2008)**

Ans. Line encoding consists of representing the digital signal to be transported by an amplitude and time discrete signal that is optimally tuned for the specific properties of the physical channel. The waveform pattern of voltage or current used to represent the 1's and 0's of a digital signal on a transmission link is called line encoding. The common types of line encoding are unipolar, polar and bipolar and manchester encoding. Various factors that are considered for selecting a line encoding format are :

1. Transmission bandwidth
2. Power efficiency
3. Error detection and correction capability
4. Favourable power spectral density
5. Adequate timing content
6. Transparency.

Alternate Mark Inversion (AMI) : AMI is known as biplar non-return to zero or bipolar NRZ. In this format, the successive '1' are represented by pulses with alternate polarity and '0' are represented by no pulses. Fig. illustrates the bipolar NRZ or AMI waveform. If there are even numbers of 1's the DC component of waveform would be zero. The advantage of this format is that the ambiguities due to transmission signal inversions are eliminated.

Binary Sequence



Bipolar NRZ Format (AMI)

Manchester Code (Split Phase Manchester Code) : The waveform for Manchester code is shown below :

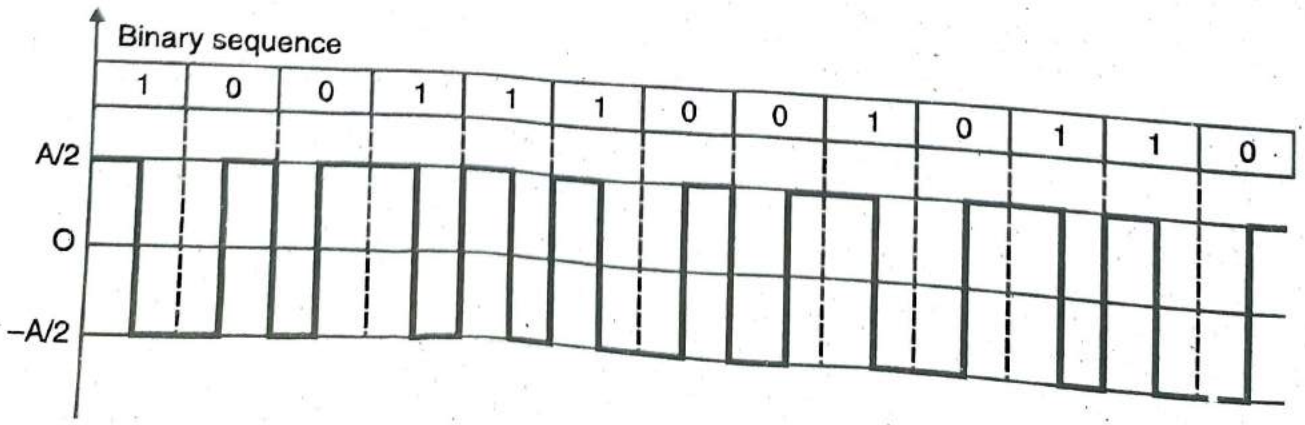
If symbol '1' is to be transmitted, then

$$x(t) = \begin{cases} \frac{A}{2}, \text{ for } 0 \le t \le \frac{T_b}{2} \\ -\frac{A}{2}, \text{ for } \frac{T_b}{2} \le t \le T_b \end{cases}$$

If symbol '0' is to be transmitted, then

$$x(t) = \begin{cases} -\frac{A}{2}, \text{ for } 0 \le t \le \frac{T_b}{2} \\ \frac{A}{2}, \text{ for } \frac{T_b}{2} \le t \le T_b \end{cases}$$

Wave Form



Split phase Manchester formal

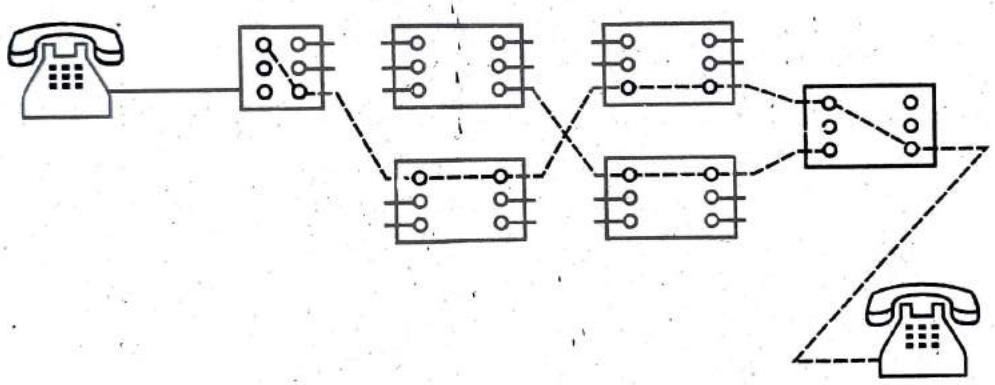
Q 59. What do you mean by switching? Describe in brief the various switching methods. **(PTU, Dec. 2011 ; May 2009)**

Ans. The switched network consist of series of interlink nodes called switches. Switched are hard wired software devices capable of creating temporary connections between two or more devices. Link to a switch but not to each other. The nodes are connected through common devices and some nodes are used for the purpose of routing packages. The point to point line configuration creates a dedicated link between 2 devices and the channel is resend for transmission between those two devices. The configuration uses actual length of wire to connect both ends but the options could be microwave or satellite link.

Various switching methods are :

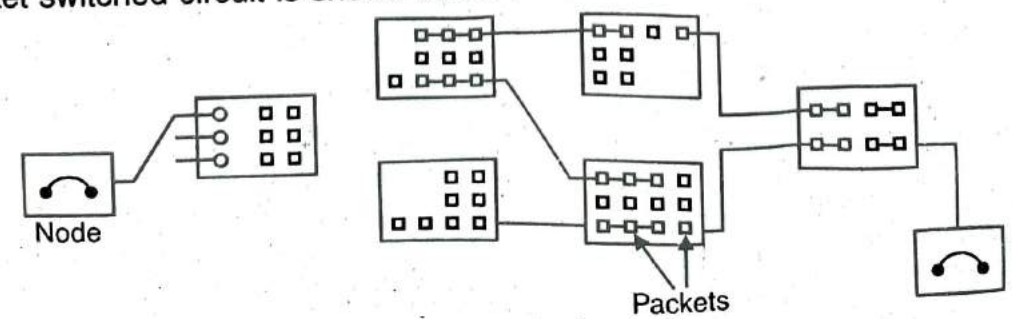
1. Circuit Switching
2. Packet Switching
3. Message Switching.

1. Circuit Switching : It is type of switching in which physical connection is set up when the call is made from transmitter to receiver telephone. Once a call is setup dedicated path between both ends exist. It will continue to exist untill the call is disconnected circuit switched (telephone network is shown below) :



2. Packet Switching : In packet switching message is divided into many segments or packet. Each packet is treated as separate communication. These packets are then send to each station in a continuous sequence. The packet from various message may be transmitted together and packets of same message may be dispatched over many different line. Each packet has a header with a packet address and source and destination address. The packets are reassemble into their original message when they reach their destination. The packet switching common network is made up of stations, nodes and transmitted parts.

Packet switched circuit is shown below :



3. Message Switching : In message switching network, the central switching station receives all the communication sent to all computer system connected to the network. If then stores a message in its buffer memory. Each message carries its destination address. As soon as lines are available, the messages are forwarded to their addresses. Message switching is also called store and forward method. Separate lines requirement for message switching are $= \frac{N(N-1)}{2}$

where N = No. of computer nodes.

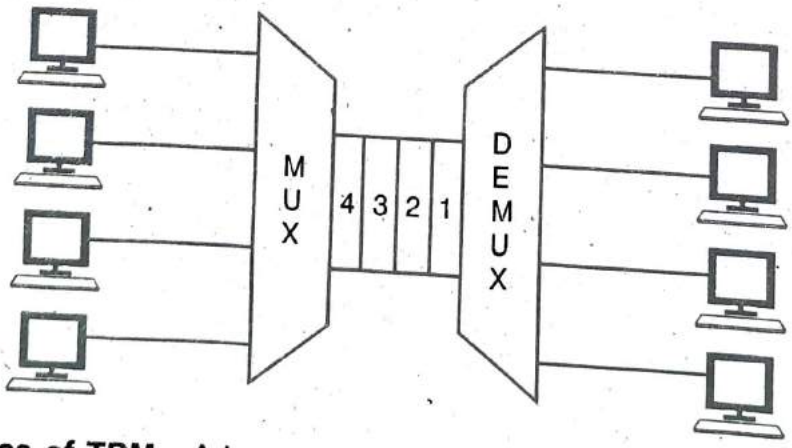
Q 60. What is TDM? With the help of a block diagram, explain how it works. What is statistical TDM? What is its advantage? Discuss its frame format.

(PTU, May 2008, 2005)

Ans. Time Division Multiplexing (TDM) : TDM is a digital process that can be applied when the data rate capacity of the transmission medium is greater than the data rate required by the sending and receiving devices. In such a case, multiple transmissions can occupy a single link by sub dividing them and interleaving the portions. Fig. gives a conceptual view of TDM. Note that the same link is used as in FDM ; here however, the link is shown sanctioned by time rather than frequency. In TDM figure, portions of signals 1, 2, 3 and 4 occupy the link sequentially. As an analogy, imagine a ski lift that serves several runs. Each run has its own line and the skiers in each line take turns getting on the lift. As each chair reaches the top of the mountain, the skier riding it gets off and skis down the run for which he or she waited in line.

TDM can be implemented in two ways :

1. Synchronous TDM
2. Asychronous TDM



Advantages of TDM : Advantages of TDM are :

1. Full available channel bandwidth can be utilized for each channel.
2. Intermodulation distortion is absent.
3. TDM circuitry is not very complex.
4. The problem of cross talk is not severe.

Q 61. Explain the structure of a switch. How is it different from a Hub?
(PTU, Dec. 2008)

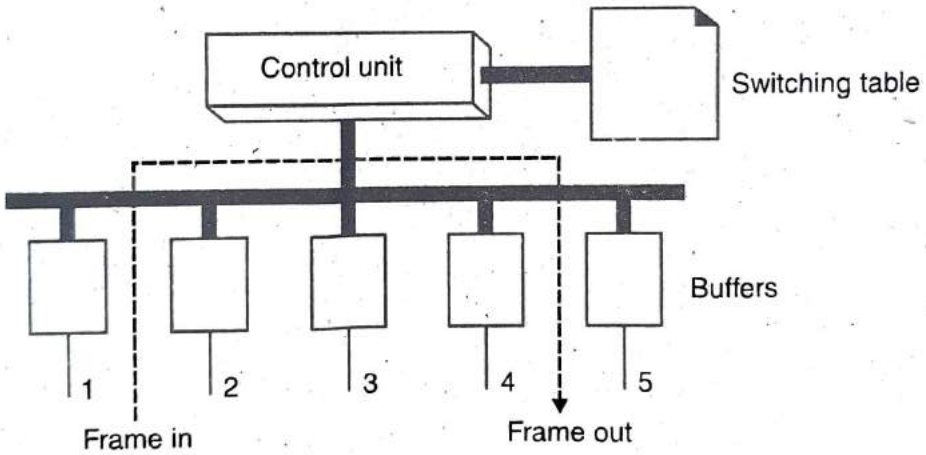
Ans. A switch is a devic which provides bridging functionality with greater efficiency. A switch acts as a multiport bridge to connect devices or segment in a LAN. The switch has a buffer for each link to which it is connected. When it receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link. If the outgoing link is free, the switch sends the frame to that particular link.

Switch are of two types :

1. Store-and-forward Switch
2. Cut-through Switch.

A store and forward switch stores the frame in the input buffer until the whole packet has arrived.

A cut-through switch, forward the packet to the output buffer as soon as the destination address is received. Concept of a switch is shown in fig. As shown in fig. a frame arrives at port 2 and is stored in the buffer. The CPU and the control unit, using the information in the frame consult the switching table to find the output port. The frame is then sent to port 5 for transmission.



Difference between hub and switch :

Hub	Switch
1. It is a broadcast device.	1. It is a point to point device.
2. It operate at physical layer.	2. It operates at datalink layer.
3. It is not an intelligent device.	3. It is an intelligent device.
4. It simply broadcasts the incoming packet.	4. It uses switching table to find the correct destination.
5. It can not be used as repeater.	5. It can be used as repeater.
6. Not a sophisticated device.	6. It is a sophisticated device.
7. Not very costly.	7. Costly.

Q 62. List and explain different digital-to-analog conversion methods.
(PTU, Dec. 2009)

Ans. The different digital-to-analog conversion methods are :

1. Amplitude Shift Keying (ASK) : ASK or ON-OFF keying is the simplest digital modulation technique. In this type of modulation, amplitude of the carrier signal is switched depending on the input signal.

2. Frequency Shift Keying (FSK) : It is a type of digital to analog modulation technique in which frequency of the sinusoidal carrier is switched depending upon the input digital signal.

3. Phase Shift Keying (PSK) : It is a type of modulation technique in which phase of carrier signal is switched depending upon the input digital signal.

4. Quadrature Amplitude Modulation (QAM) : It is a combination of ASK and PSK.

Q 63. What is the difference between simplex and half duplex?

(PTU, May 2011)

Ans. Simplex : In these systems the information is communicated in only one direction. For example the radio or TV broadcasting systems can only transmit. They cannot receive.

Half Duplex : These systems are bi-directional. They can transmit as well as receive but not simultaneously.

Q 64. With reference to X.25, explain

(a) Switched virtual circuit.

(b) Permanent virtual circuit.

(c) Protocols used at the link level.

(d) State diagram to explain call setup and call clearing. **(PTU, Dec. 2008)**

Ans. (a) Switched Virtual Circuit : In a network, a switched virtual circuit (SVC) is temporary virtual circuit that is established and maintained only for the duration of data transfer session. A permanent virtual circuit (PVC) is continuously dedicated virtual circuit. Virtual circuit is one that appears to be a discrete, physical circuit available only to the user but that is actually a shared pool of circuit resources used to support multiple users as they require the connections. Switched virtual circuits are part of an X.25 network. Conceptually, they can also be implemented as part of a frame relay network.

(b) Permanent Virtual Circuit : A permanent virtual circuit (PVC) is a software-defined logical connection in a network such as a frame relay network. A feature of frame relay that makes it a highly flexible network technology is that users (companies or clients of network providers) can define logical connections and required bandwidth between end points and let the frame relay network technology worry about how the physical network is used to achieve the define connections and manage the traffic. In frame relay, the end points and a stated bandwidth called a committed information rate (CIR) constitute a PVC, which is defined to the frame relay network devices. The bandwidth may not exceed the possible physical bandwidth.

(c) Protocols Used at Link Level : The protocol referred to as X.25 encompasses the first three layers of the OSI 7 layered architecture as defined by the international standards organisation (ISO).

The OSI-7 layered architecture is a "tempelate" which describes in general terms the functional design of data communication protocols. The purpose of this template is to simplify

all protocols interfaces when changes are required because of new technologies or because of requirements to co-internetwork between vendors or national adminstrations X.25 as defined by the CCITT is considered to be a close implementation of the first three layers of OSI-7 layered architecture.

Layer 1. Physical layer includes several well-known standards

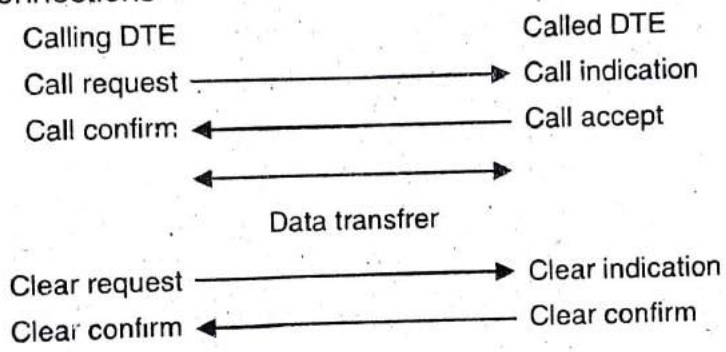
- V.35
- RS-232
- X.21 bis.

Layer 2. Commonly referred to as high-level data link control (HDLC) it is actually an implementation of the ISO HDLC standard called link access procedure balanced (LAPB).

Layer 3. This is simply referred to as the packet layer protocol (PLP).

(d) State Diagram to explain call setup and call clearing : The DTE to DTE connections shown in the following diagram illustrates how a call is set up, used and cleared. The call uses a virtual circuit for the duration of the call. This circuit can be reused once the call is over.

DTE to DTE connections



Data sent during the call is divided up into units. The size of these units is the packet size. Packet size applies to the size of each data packet, not all packets. The default packet size is 128 bytes. When one unit of data needs to be sent that is greater than the packet size, a number of packets are sent. This sequence of packets is marked to indicate that it makes up one unit of data through use of a flag called the more or M-bit.

Q 65. Explain microwave transmission system.

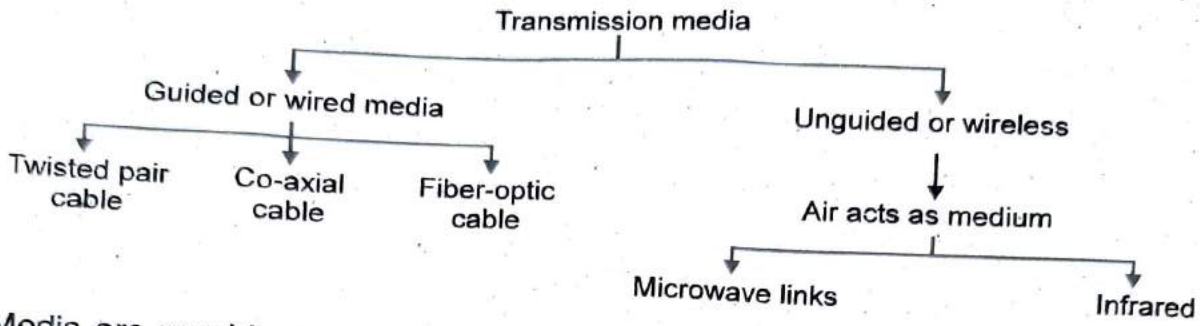
Ans. It makes use of the lower giga hertz frequencies of the electromagnetic spectrum. These frequencies are higher than the RF and they produce better throughput and performance. Microwaves are basically electromagnetic waves having frequencies between 1 and 300 GHz. These are unidirectional has line of sight propagation.

These systems used directional parabolic antennas to transmit and receive signals to the lower in Hz.

Q 66. What are various transmission media used? Explain about each of them.
(PTU, May 2011, 2005 ; Dec. 2005)

Ans. Media are what the messages is transmitted over. In other words a communication channel is called as a medium. Different media have different properties and uses in different environment for different purpose.

Classification of Transmission Media



Media are roughly grouped into two classes.

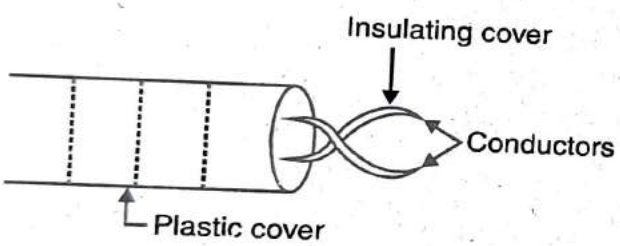
1. Guided Media
2. Unguided Media

1. Guided Media : It is a communication medium which allows the data to get guided along it. For this the media need to have a point to point physical connection.

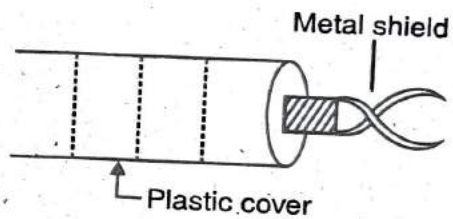
2. Unguided Media : The wireless media is also called unguided media.

Guided or wired media are further classified as :

(i) Twisted Pair Cables :



(a) UTP

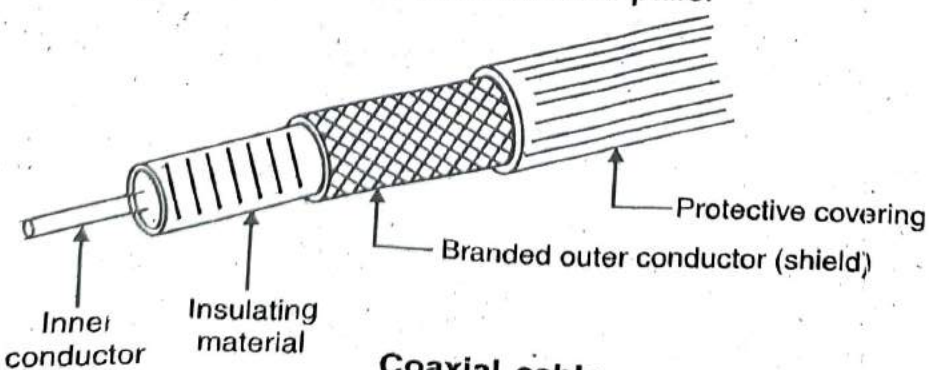


(b) STP

(a) UTP (Unshielded Twisted Pair Cable) : A twisted pair consists of two insulated conductor twisted together in the spiral form as shown.

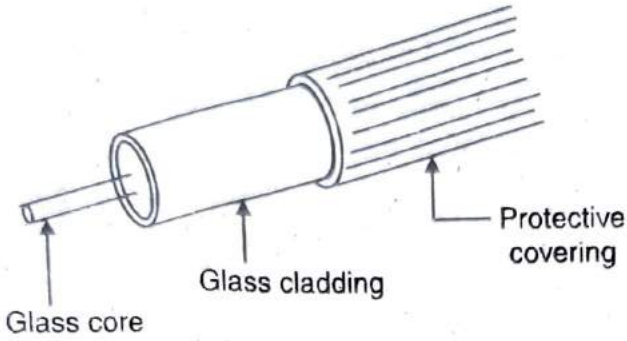
(b) STP (Shielded Twisted Pair Cable) : STP cable has a metal foil or braided mesh to cover each pair of insulating conductors.

(ii) Co-axial Cable : The cable consist of two concentric conductors separated by a dielectric material. The external conductor is metallic braid and used for the purpose of shielding. The co-axial cable may contain one or more co-axial pairs.



Coaxial cable

(iii) Optical Fibre Cable : It consists of an inner glass core surrounded by a glass cladding which has a lower refractive index. Digital signals are transmitted in the form of intensity modulated light signal which is tapped in the glass core.



Q 67. What is terrestrial microwave? **(PTU, May 2012)**

Ans. A terrestrial microwave which utilizes microwave line of sight, method, technology or service such as multichannel multipoint distribution service, which utilizes microwave line of sight communications between sending and receiving unit located on the ground or on towers, as opposed to a sender and/or receiver antenna being located on a communication satellite used for instance, for telephone, TV, and/or data service.

Q 68. What is the difference in UTP and STP cable? **(PTU, Dec. 2012)**

Ans.

	Factors	UTP	STP
1.	Foil or braided mesh	Absent	Present
2.	Cross talk and interference	Very high	Less or compared to UTP
3.	Cost	Lowest	Moderate
4.	Termination	Difficult	Easy
5.	Installation	Easy	Fairly easy
6.	Bandwidth	1-555 mbps (typically 10 mbps)	1-555 mbps (typically 16 mbps).

Q 69. List the advantages and disadvantages of optical fibre transmission media. **(PTU, May 2012)**

Ans. Advantages :

1. They are not affected by electrical and magnetic interference as the data travel in form of light.
2. Optical fibre offers higher bandwidth than twisted pair or coaxial cable.
3. Optical fibres ar thin, lighter in weight and small in size as compared to other wired medias.
4. Glass is more resistant to corrosive materials as compared to copper. Hence can be laid in different environments.
5. In optical fibres, attenuation is very low. Therefore, these fibres can run several kilometres without amplification.

6. Fibres do not leak light and are quite difficult to tap. So, they provide security against potential wire tappers.

7. There is no cross-talk problem in optical fibres.

Disadvantages :

1. Fibre optic cables are fragile i.e. more easily broken than wires.
2. Being fragile, optical fibres need to be put deep into the land.
3. Optical fibres are unidirectional. For two-way communication, two fibres are required.
4. It is a newer technology and requires skilled people to administer and maintain them.

Q 70. Explain the process of signal transmission in optical fibre.

(PTU, Dec. 2012)

Ans. An optical fibre cable is made of glass or plastic and transmits the signals in form of light.

An optical transmission system has three basic components :

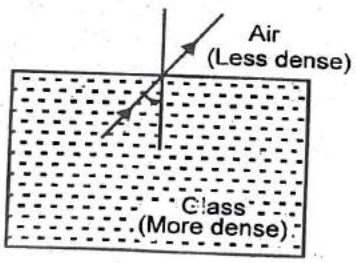
(a) Light source

(b) Transmission medium

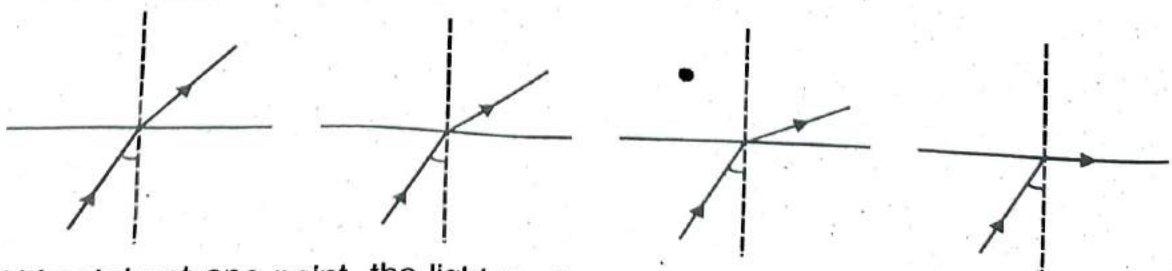
(c) Detector.

Working principle of optical fibre :

1. The working of optical fibre is based on the concept of Total Internal Reflection (TIR).
2. We know that light travels in a straight line as long as it is moving through a single uniform substance.
3. If a ray of light travelling through one substance suddenly enters another substance of different density, the ray of light changes its direction. This phenomenon is known as reflection.



4. As shown in fig. angle of incidence (the angle the ray makes with the line perpendicular to the interface between two substances).
5. If we gradually increase angle of incidence, the ray of light moves more and more closer to the surface.



6. Utimately at one point, the light ray bends along the interface.

❑❑❑

Chapter 3

Data Link Layer

Contents

Design issues, Framing, Error detection and correction codes : checksum, CRC, hamming code, Data link protocols for noisy and noiseless channels, Sliding Window Protocols : Stop and Wait ARQ, Go-back-N ARQ, Selective repeat ARQ, Data link protocols : HDLC and PPP.

POINTS TO REMEMBER

- Transmission errors are usually corrected at the data link layer of OSI model.
- Functions of DLL are synchronization and error control for the information which is to be transmitted over the physical link.
- In sliding window flow control, the sending of data is constrained by an imaginary window that expands and contracts according to the acknonwledgements received by the sender.
- Error control or how to handle lost or damaged data or acknowledgements is simply the transmission of data.
- Four common methods of error detection are :
  (a) Vertical redundancy check
  (b) Cyclic redundancy check
  (c) Checksum
  (d) Parity
- Checksum is used by the higher layer protocols (TCP/IP) for error detection.
- CRC is the most powerful detection technique and it is based on long division.
- Line discipline establishes the status of a device on a link.
- Data link protocols can be classified as synchronous or asynchronous.
- Synchronous protocols can be classified into two groups :
  (a) Character oriented protocols
  (b) Bit-oriented protocols.
- Control frames perform the functions like make a connection, control flow and error, release a connection.
- For sliding window flow control, go back n or selective reject ARQ is used.
- HDLC handles data transparency by adding a 0. Wherever there are five consecutive is

following a 0. This is called bit stuffing.

- Binary synchronous communication is the most well known character oriented protocols.
- In stop and wait ARQ, retransmission the unacknowledged frame.
- Retransmission of data is initated by Automatic Repeat Request (ARQ).
- Error control or how to handle lost or damaged data or acknowledgements is simply the transmission of data.
- A protocol in data communication is a group of specifications used to implement one or more layers of the OSI model.
- HDLC operates in half or full duplex mode in a point to point or multipoint link configuration.
- There are two types of BSC frames :
  (a) Control frames
  (b) Data frames.
- The second layer in the OSI model, the data link layer has three main functions : line discipline, flow control, error control.

QUESTION-ANSWERS

Q 1. Explain the functions of data link layer.

Ans. 1. Functions of data link layer are synchronization and error control for the information which is to be transmitted over the physical link.

2. To enable the error detection, it adds error detection bits to the data which is to be transmitted.

3. The encoded data is then passed to the physical layer.

4. These error detection bits are used by the data link on layer on the other side to detect and correct the errors.

5. At this level the outgoing messages are assembled into frames, and the system waits for the acknowledgements to be received after every frame transmitted.

Q 2. What are various data link layer design issues? **(PTU, May 2005)**

Ans. The data link layer is supported to carry out many specified functions.

For effective data communications between two directly connected transmitting and receiving stations the data link layer has to carry out a number of specific functions like :

1. Services provided to the network layer : A well defined service interfaces to the network layer. The principal service is transferring data from the network layer on source machine to the network layer on destination machine.

2. Frame synchronization : The source machine sends data in blocks called frames to be the destination machine. The starting and ending to each frame should be recognized by the destination machine.

3. Flow control : The source machine must not be sends data frames at a rate faster than the destination machines must be accepted them.

4. Error Control : The errors made in bits during transmission from source to destination machines must be detected and corrected.

5. Addressing : On a multipoint line, such as many machines connected together (LAN), the identification of the individual machine must be specified while transmitting the data frames.

Q 3. Explain service provided by data link layer to network layer.

Ans. Network layer is the layer 3 of OSI model and lies above the data link layer.

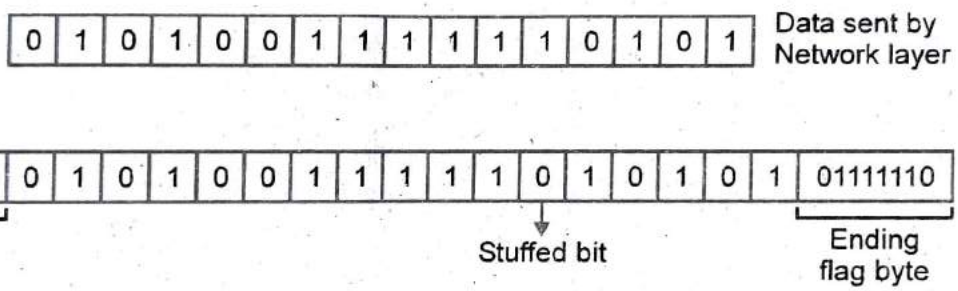
Three major types of service offered by data link layer are :

1. Unacknowledged connectionless service
2. Acknowledged connectionless service
3. Acknowledged connection oriented service.

Q 4. What is bit stuffing?

Ans. Bit stuffing is a technique used to solve the synchronization problem when the flag byte (011111110) appears in the data unit.

Whenever the sender data link layer detects the presence of five consecutive ones in data, it automatically stuffs a bit 0 into the outgoing bit stream. This is known as bit stuffing.



Q 5. Differentiate between polling and selecting.

Ans. Polling and selecting are the terms used in client server networks to determine which device [primary or secondary] has control over the shared link.

1. Polling : When the primary device wants to receive data it asks secondary devices if they have anything to send, this function is called polling.

2. Selecting : When the primary device wants to send data to any secondary device, it tells that device to be ready to receive data, this function is called selecting.

Q 6. Explain framing.

Ans. 1. Frames are the small data units created by the data link layer and the process of creating frames by the data link layer is known as framing.

2. On the source side, data link layer receives the bit stream from network layer and divides it into discrete frames.

3. On the destination side, data link layer receives these frames from physical layer and recomputes the checksum of each frame.

4. Data link layer then discards this erroneous frame and asks for retransmission.

Q 7. How a simplex stop and wait protocol works? (PTU, Dec. 2007)

Ans. In simplex stop and wait protocol, the communication control channel is assumed

to be error free and the data traffic is still simplex. The receiver requires a time Δt to execute from physical layer plus to network layer the sender must transmit at an average rate less than one frame per time Δt. Moreover, if we assume that no automatic buffering and queuing are done within the receiver's hardware, the sender must never transmit a new frame until the old one has been fetched by from physical layer, test the new one overwrite the old one.

Q 8. What is the purpose of flow control?

Ans. Any receiving device has a limited speed at which it can process incoming data and also a limited amount of memory (buffer) to store incoming data.

If the source is sending the data at faster rate than the capacity of receiver, there is a possibility of receiver being swapped. The receiver will keep loosing some of the frames simply because they are arriving too quickly and buffer is also getting filled up. This will generate waste frames on the network.

Therefore, receiving device must have some mechanism to inform the sender to send fewer frames or stop transmission temporarily.

Q 9. What is piggybacking?

Ans. Piggybacking is a technique of temporarily delaying the acknowledgement frame so that it can be hooked with next outgoing data frame.

Whenever a data frame is received, the receiver waits and does not send the control frame back to the sender immediately. The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.

Q 10. Difference between SLIP and PPP.

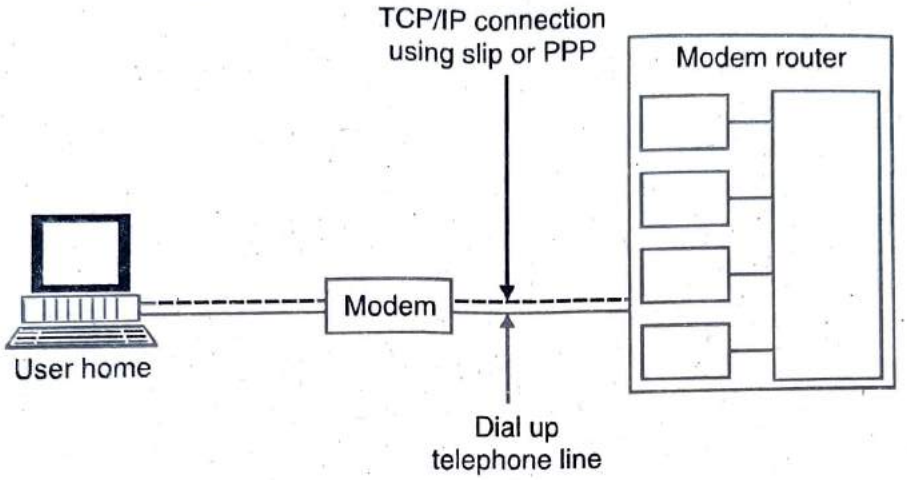
Ans.

SLIP	PPP
1. SLIP stands for serial line internet protocol.	1. PPP stands for point to point protocols.
2. SLIP does not perform error detection and correction.	2. PPP performs error detection and correction.
3. SLIP supports only IP.	3. PPP supports multiple protocols.
4. SLIP does not allow the IP address to be assigned dynamically i.e. IP address is assigned statically.	4. PPP allows the dynamic allocation of IP address.
5. It does not provide any authentication.	5. It provides authentication.

Q 11. Write how data link layer works in the Internet. **(PTU, May 2007)**

Ans. The internet consists of individual machines plus the information i.e. infrastructure required for communication between them. Internet is basically a wide area network which is built up from point to point leased line. In case of the internet, millions of individuals have the home connections to the internet using modems and dial up telephone lines. Generally the user's home PC calls up an internet provided (IP).

But in some situations the home PC functions as a character oriented terminal logged into the internet service providers time sharing system.



Q 12. Explain HDLC and its characteristics.

Ans. HDLC is a bit oriented protocol that supports both half duplex and full duplex communication over point to point and multipoint link.

Systems using HDLC are characterized by :

1. Station types
2. Configuration
3. Response modes

1. Station Types : To make HDLC protocol applicable to various possible network configurations, 3 types of stations are :

(a) Primary station

(b) Secondary station

(c) Combined station

(a) Primary Station : Primary station has complete control over the link at any time.

(b) Secondary Station : All the secondary stations work under the control of primary station.

(c) Combined Station : A combined station is one that can behave either as a primary or as a secondary.

2. Configuration : It means how the various stations are connected to a link.

(i) Unbalanced configuration

(ii) Symmetrical configuration

(iii) Balanced configuration.

Q 13. Explain asynchronous response mode (ARM) in HDLC.

Ans. ARM : The stations involved are of primary and secondary type. Therefore, it has primary-secondary relationship. In this mode, if channel is idle, the secondary station may initiate the transmission without seeking permission from the primary. If any secondary device wants to communicate with other secondary device, the transmission is done via primary station only.

Q 14. Which method is used for error correction at data link layer?
(PTU, May 2010)

Ans. Hamming codes are used for error correction at data link layer.

Error Correction Code : Hamming codes are error correcting and detecting codes. The hamming code data is now transmitted.

At the receiver it is decoded to get the data back.

The bits (1, 3, 5, 7), (2, 3, 6, 7) and (4, 5, 6, 7) are checked for even parity (or odd parity). If all the 4 bits groups mentioned above pass the even parity, then the received code word is correct i.e. it does not contain errors.

Given bit sequence : 10011101

Step 1. Number of parity bits will be 4 i.e. P1, P2, P3, P4

D_{12}	D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	0	1		1	1	0		1		

For $P1\ D_3\ D_5\ D_7 = 0101$

$P1 = 1$

For $P2\ D_3\ D_6\ D_7 = 1111$

$P2 = 1$

For $P4\ D_5\ D_6\ D_7 = 0011 \Rightarrow P4 = 0$

For $P8\ D_9\ D_{10}\ D_{11} = 1100 \Rightarrow P8 = 1$

D_{12}	D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	0	1	1	1	1	0	0	1	1	1

Q 15. Name the sub layers of data link layer and also their functions.

Ans. Sub layers of data link layer are :

1. Logical link layer
2. Medium access layer.

Logical link control sub layer's function :

(a) Error recovery

(b) It performs flow control operation

(c) User addressing

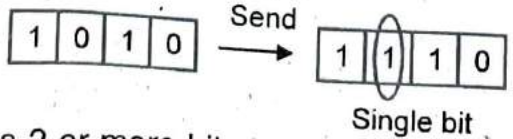
MAC layer's functions :

(a) To perform the control of access to media.

(b) It helps in error detection.

Q 16. What is difference between single bit errors and burst errors?

Ans. Single bit error : It means only 1 bit of given data unit is changed from 0 to 1 or 1 to 0. These errors occur in serial transmission.



Burst Errors : It means 2 or more bits in the data have changed 1 to 0 or 0 to 1.

Q 17. What do you mean by congestion in a network?

Ans. It is an issue in packet switching network when there are two many packets are present in a part of a subnet, the performance degrades, this situation is called congestion.

Q 18. Explain three types of redundancy checks used in data communication.

Ans. 1. Parity checking

2. Checksum error detection

3. Cyclic redundancy check.

1. Parity checking : It is the most common and least expensive error detection technique. In this method, we have to add an extra bit known as parity bit.

2. Checksum error detection : In this data bits are mixed up due to 8-bit addition.

3. Cyclic redundancy check : It is based on binary division for achieving a desired parity, the sequence of redundant bits is called cyclic redundancy check.

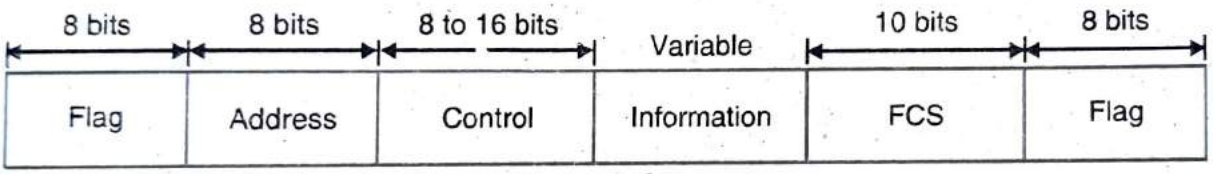
Q 19. Give limitations of parity checking.

Ans. 1. It is not suitable for detection of multiple errors (two, four, six, etc.).

2. The other limitation of parity checking method is that it cannot reveal the location of erroneous bit. It cannot control the error either.

Q 20. Explain frame structure in HDLC.

Ans. The frame in HDLC can have 6 fields.



1. Flag field : It is the 8 bit field that contains 01111110. This flag marks the beginning and end of a frame.

2. Address field : This field can be 1 byte long or multiple byte long depending on the need of the n/w.

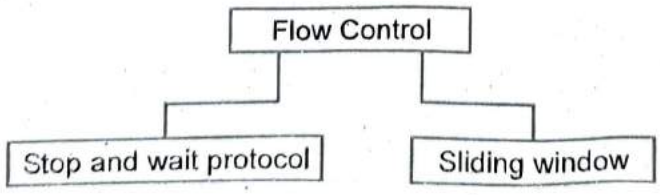
3. Control field : This field can be of 8 bits or 16 bits.

4. Information field : The length of this field varies with network i.e. different for different networks.

5. FCS field : It stands for frame check sequence.

Q 21. Differentiate between error control and flow control.

Ans. Flow Control : Flow control refers to set of procedures used to restrict the amount of data the sender can send before waiting for acknowledgement.



Error Control : Each control in the data link layer is based on automatic repeat request

(ARQ), which means retransmission of data in these cases ; damaged frame, host frame and lost acknowledgement.

Q 22. Discuss the concept of redundancy in error detection.

Ans. The main concept for detecting and correcting errors is redundancy for detecting and correcting errors, we need to send some extra bits with our data. These redundant bits are added by sender and removed by the receiver. Redundancy is achieved through various coding schemes.

Q 23. Explain checksum.

Ans. In this method, checksum generator subdivides the data unit into equal segments of n bits. This segments are added together using 1's complement arithmetic in such a way that the total is n bit long. That total is then complemented and appended to the end of the data unit.

At the receiver, the receiver sub divides the data unit again and add all segments together and complements the result. If the data unit is correct, the total value found by adding the data segments and checksum field should be zero.

For example, data to be sent

10101001 00111001

Now add it using one's complement arithmetic

```
  10101001
  00111001
 ----------
  11100000 sum
```

00011101 checksum

data to be sent

10101001 00111001 00011101

at the receiver side

10101001 00111001 00011101

Now add these three sections and check result :

```
  10101001
  00111001
  00011101
 ----------
  11111111 sum
  00000000 complement
 ----------
```

Q 24. Write note on error correction.

Ans. Error detection and correction are complemented either at data link or transport layer of OSI model.

Error correction can be implemented in two ways :

1. When an error is discovered, the receiver can have the sender retransmit the entire data unit.

2. In the other a receiver can use an error-correcting code, which automatically corrects certain errors.

Q 25. What kind of error is undetectable by the checksum?

Ans. Checksum detects all errors involving even or odd number of bits but if one or more bits of a data segment are corrupted and the corresponding bit or bits of opposite value in a second segment are also damaged, the sums of these columns will not change and error will not be detected.

So, a bit inversion is balanced by an opposite bit inversion in the corresponding digit of another segment, the error is invisible.

Q 26. Explain about error correction.

Ans. Types of error :

(a) Single bit error

(b) Burst error

Causes of errors : Whenever an electromagnetic signal flows from one point to another. It is subjected to unpredictable interference from heat, magnetism and other forms of electricity. This interference can change the shape or timing of signal, thus causing an error.

For any good communication, errors must be detected and corrected. Error detection and correction are implemented either at data link layer or transport layer of OSI model.

Q 27. What are sliding window protocol? (PTU, May 2010, 2009)

Ans. Sliding window protocols are set of three protocols that are more robust and bidirectional protocols. Sliding window refers to imaginary boxes at the transmitter and receiver.

1. One bit sliding-window protocol (Stop and wait area) : This protocol is called one bit protocol because the maximum window size here i.e. n is equal to 1. It uses the stop and wait technique.

The sender sends our frame and waits to get acknowledgement. Only after receiving the acknowledgement does it transmit the next frames.

2. Go back n area protocol : In this protocol sender does not wait for ACK signal for the transmisson of next frame. It transmits the frames continuously as long as it does not receive the NAK signal. NAK is –ve acknowledged.

3. Selective repeat area : In this method only the specified damaged or lost frame is retransmitted.

Q 28. Explain response mode of HDLC.

Ans. HDLC supports three modes of communication between stations :

1. Normal Response Mode (NRM)
2. Asynchronous Response Mode (ARM)
3. Asynchronous Balance Mode (ABM)

1. Normal Response Mode : In this mode primary station controls the link. Secondary station seeks permission from primary before transmitting data.

2. Asynchronous Response Mode : The stations involved are of primary and secondary type.

3. Asynchronous Balance Mode : This type of mode involves combined stations that are connected in point to point configuration.

Q 29. Name various error detection and correction techniques.

Ans. Error detection techniques are :

1. Redundancy
2. Vertical redundancy check/parity check
3. Longitudinal redundancy check (LRC)
4. Cyclic redundancy check (CRC)
5. Checksum

Error correction-detection techniques are :

1. Single bit error correction
2. Hamming code.

Q 30. Name various error detection and correction techniques. Explain in detail the Hamming error correction method. Also find the CRC using a polynomial, P = 110011, for a given data, M = 11100011. **(PTU, May 2009)**

Ans. Given data word = 11100011

Divisor = 110011

Step I. Divident = $\underbrace{11100011}_{\text{data word}}\ \underbrace{000000}_{\text{6 additional zeros}}$

```
                101101101
        ┌──────────────────
110011  │ 11100011000000
        │ -110011↓
        │ ------
        │  0010111
        │  00000↓
        │  ------
        │  101111
        │  110011↓
        │  ------
        │  0111000
        │  110011↓
        │  ------
        │  0010110
        │  00000↓
        │  ------
        │  101100
        │  110010↓
        │  ------
        │  0111001
        │  110011↓
        │  ------
        │  0011110
        │  00000↓
        │  ------
        │  111100
        │  110011
        │  ------
        │  001111
```

Code Word :

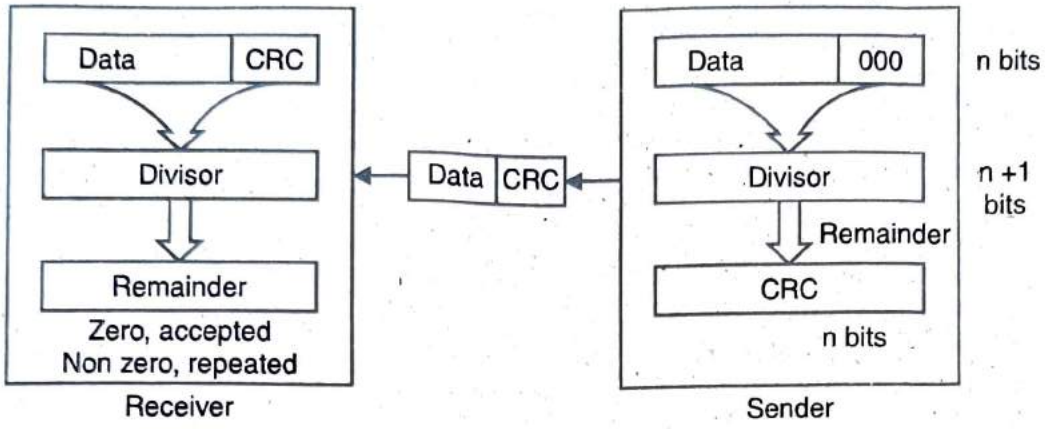
$$\begin{array}{r} 11100011000000 \\ \qquad\qquad\quad 1111 \\ \hline 11100011001111 \end{array}$$

which is required CRC code.

Q 31. Explain cyclic redundancy check method.

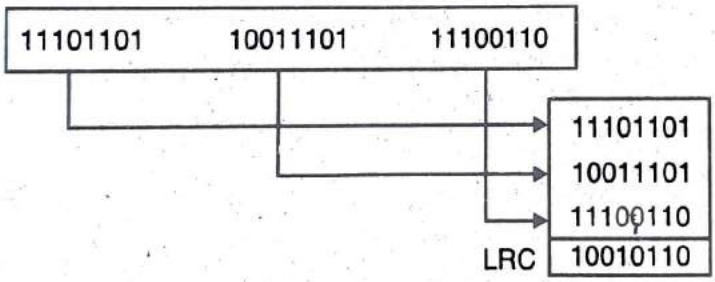
Ans. CRC is based on binary division. In this method, a sequence of redundant bits called CRC is appended to the end of a data unit so that resulting data unit becomes exactly

divisible by a second predetermined binary number. At the destination, the incoming data unit is divided by the same number. If the resulting remainder is zero, the data unit is undamaged and, therefore, accepted. A remainder indicates that data unit has been damaged and, therefore, rejected.

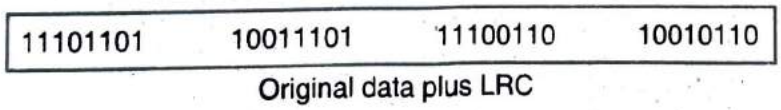


Q 32. Write a detailed note on : LRC.

Ans. Longitudinal Redundancy Check : In this method, a block of bits is organized in a table of rows and columns and then parity bit is calculated for each column and a new row of 8 bits is created, which are the parity bits for the whole block. These eight parity bits are attached to the original data and send them to the receiver.



Now,



Original data plus LRC

So, a block of bits is divided into rows and a redundant row of bits is added to the whole block. At the receiver, LRC is checked, for even parity and if source of the bits does not follow the even parity rule and then the whole block is discarded. But if bits follow the even parity rule, block will be accepted.

LRC increases the detection of burst errors. A burst error of more than n bits is also detected by LRC with very high probability.

Q 33. Define the four types of redundancy checks used on data communication. Explain.

Ans. These are four types of redundancy check as :

1. Vertical redundancy check (VRC)

2. Longitudinal redundancy check (LRC)
3. Cyclic redundancy check (CRC)
4. Checksum

1. VRC : It is also known as parity check. In this method a redundant bit called parity bit is appended to every data unit so that the total number of 1s in the unit becomes even.

2. LRC : In this method a block of bits is organized in a table. Suppose instead of sending a block of 32 bits, organize them in table of four rows and eight columns. Now calculate the parity bit for each column and create a new row of 8 bits which are the parity bits for the whole block.

Then attach the eight parity bits to the original data and send them to the receiver.

3. CRC : CRC is based on binary division. In this method a sequence of redundant bits called CRC is appended to the end of a data unit so that resulting data unit becomes exactly divisible by a second predetermined binary number.

4. Checksum : In this method checksum generator subdivides the data unit into equal segments of n bits. These segments are added together using 1's complement arithmetic in such a way that the total is n bit long. The total is then complemented and appended to the end of data unit.

Q 34. How does checksum checker know that the received data unit is undamaged?

Ans. It is based on the concept of redundancy the sender follows the following steps :

1. The unit is divided into K sections, each of n bits.
2. All sections are added together using 1's complement to get the sum.
3. The sum is complemented and becomes the checksum.
4. The checksum is sent with data.

Receiver follows the following steps :

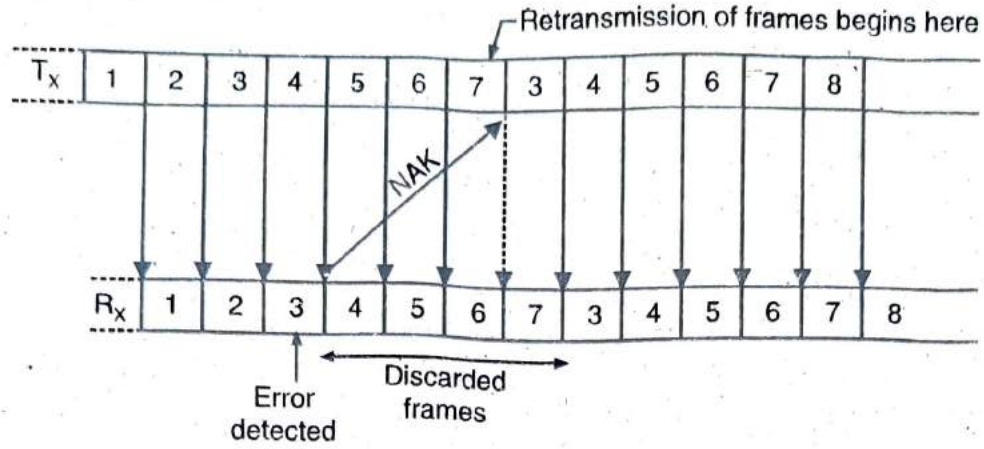
1. The unit is divided into K sections, each of n bits.
2. All sections are added together using 1's complement to get the sum.
3. The sum is complemented.
4. If the result is zero, then data is undamaged and data is accepted. Otherwise data is damaged and rejected.

Q 35. Explain the sliding window protocol with algorithm used.

Ans. The sliding window method of flow control several frames can be transmit at a time. The sliding window can hold the frame at either end and provides the upper limit on the number of frames that can be transmitted before requiring on acknowledgement.

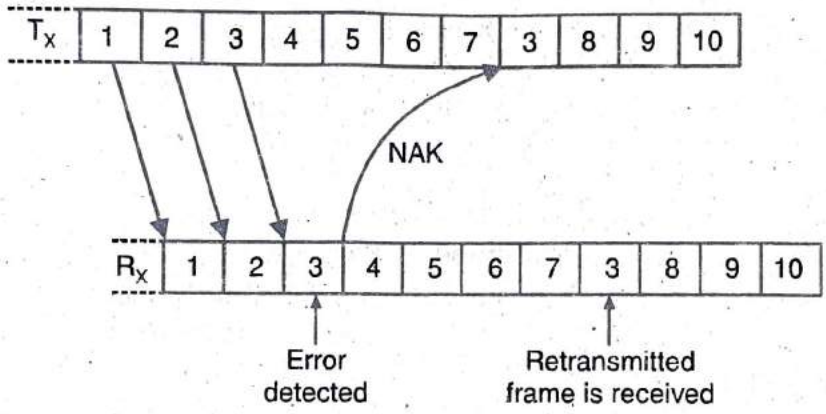
1. Go Back n ARQ : This protocol is based on ARQ (Automatic repeat request) which means retransmission of data in three cases : damaged frames, lost frames and lost acknowledgement. Go back n ARQ protocol is used to overcome the inefficiency of the stop and wait ARQ by allowing the transmitter to continue sending enough frames so that channel is kept busy while transmitter waits for acknowledgement.

It transmits the frames continuously as long as it does not receive 'NAK' signal.



2. Selective Repeat ARQ : Transmitter does not wait for ACK signals for the transmission of next code word.

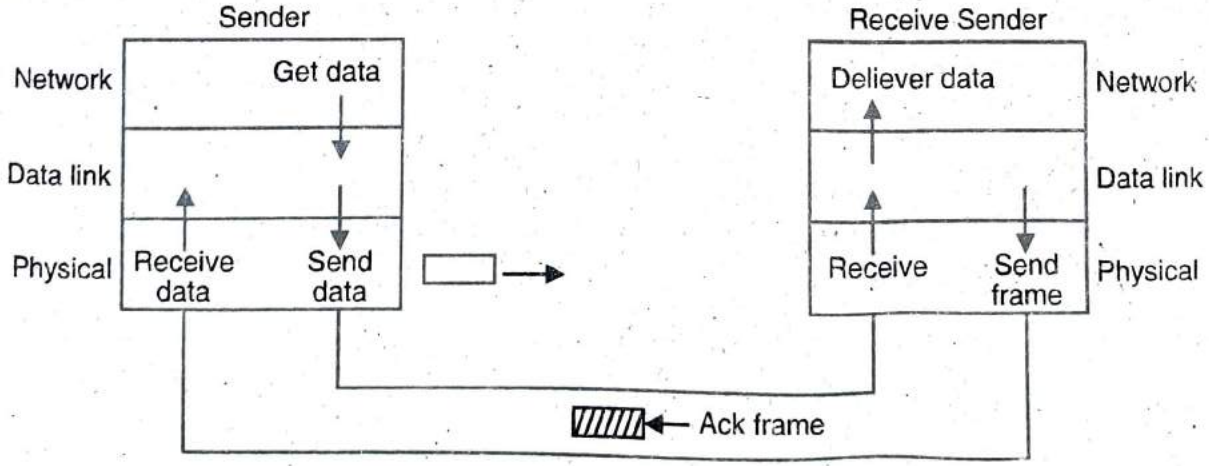
It transmits the code words continuously, it receives the 'NAK' signal from the receiver.



Q 36. Explain the stop and wait protocol.

Ans. If the data frames arrives at the receiver site faster than they can be processed the frames must be stored until their use. Normally, the receiver does have enough storage capacity specially if it is receiving data from many sources. This may result in the loss of the frames.

For preventing the receiver from becoming overwhelmed with frames, the sender has to slow down.



Q 37. Name various bit oriented protocols working at data link layer.
(PTU, Dec. 2004)

Ans. Bit oriented protocols working at data link layer are :
1. High level data link control (HDLC)
2. Synchronous data link control (SDLC)
3. Sliding window protocol.

Q 38. What is flow control?
(PTU, Dec. 2009)

Ans. Flow control is required when a sender that systematically wants to transmit frames faster than the receiver can accept them. This situation can easily occur when the sender is running on a fast computer and the receiver is running on a slow machine. The sender keeps pumping the frames out at a high rate until the receiver is completely swamped. Even if the transmission is error free, at a certain point the receiver will simply be unable to handle the frames as they arrive and will start to lose some.

Q 39. What is block parity?
(PTU, May 2009)

Ans. Parity is a form of error detection that uses a single bit to represent the odd or even quantities of '1' and '0' in the data. Parity usually consists of one parity bit for each eight bits of data. Because parity only identifies odd or even quantities, two incorrect bits can go undetected.

Q 40. Explain functions of data link layer.

Ans. It is responsible for reliable node to node delivery of the data. It accepts packets from the network layer and forms frames and gives it to the physical layer as shown :
1. Framing
2. Physical addressing
3. Flow control
4. Error control
5. Access control
(a) Logic link control
(b) Media access control.

Q 41. Write functions of media access control (MAC) sublayer.

Ans. The broadcast channels are also called multi-access channels or random access channels. In the broadcast networks, the most important point in the criteria to detemine who is allowed to use the channel when more than one user want to use it. A protocol is used to make this decision. Such a protocol, belongs to a sublayer of data link layer called the MAC.

Functions of MAC sublayer :
1. To perform the control of access to media.
2. It performs the unique addressing to stations directly connected to LAN.
3. Detection of errors.

Q 42. The channel allocation takes place at which layer of TCP/IP model.
(PTU, May 2010)

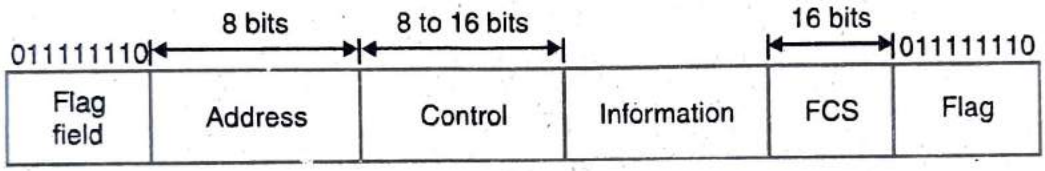
Ans. Channel allocation take place at host to network layer of TCP/IP model.

Q 43. What is HDLC? Explain its frame format and its various fields with a neat diagram. How is it superior to SDLC frame format? (PTU, May 2008)

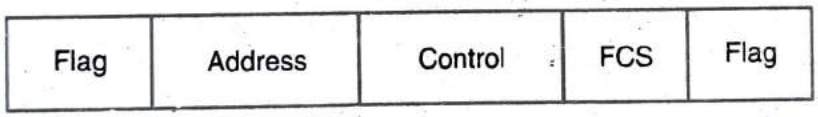
Ans. High Level Data Link Protocol (HDLC) : HDLC is a bit oriented data link protocol designed to support. Both half-duplex and full-duplex communication over point-to-point and multipoints links. HDLC protocol was developed by ISO. It is the most widely accepted data link protocol. It offer high level of flexibility, adaptability, reliability and efficiency of operation. To make HDLC protocol applicable to various possible network configuration, three types of stations has been defined :

1. Primary Station
2. Secondary Station
3. Combined Station.

Frame Structure in HDLC : The frame format of HDLC is defined so that it can accomodate the various data transfer modes. The HDLC uses two different frame formats as shown in fig. (a) and fig. (b). If we compare them, then it will be clear that except the information field both the frames are identical to each other. The frame is transmitted from left to right with the lowest order bit transmitted first.



(a) Information Transfer Frame



(b) Supervisory and Unnumbered Frames

Flag Field : The flag is a unique 8 bit-word pattern (01111110). It is used to identify the start and end of each frame as shown in fig. (a). It is also used to fill the idle time between consecutive frames.

Address Field : The address field consists of the address of secondary station irrespective of whether a frame is being transmitted by primary or secondary station. Address field consists of 8 bits hence it is capable of addressing 256 addresses.

Control Field : The control field usually consists of 8 bits but the number of bits can be extended to 16. It carriers the sequence number of the frame, acknowlegments request for transmission and other control commands and response.

Information Field : The field size of the information field is variable and it can consist of any number of bits. It consists of the user's data bit and it is completely transparent.

Frame Check Sequence (FCS) Field : This is a 16 bit field which is used for detection of errors in the address, control and information field. It is nothing else but a 16 bit CRC code for error detection.

HDLC, is superior to SDLC because HDLC supports three transfer modes, while SDLC supports only one ; LAPB, which is restricted to the ABM transfer mode and is appropriate only for combined stations ; IEEE 802.2 which is often referred to as LLC and has three types and QLLC, which provides the data-link control capabilities that are required to transport SNA data across X.25 networks.

Q 44. Explain briefly different error detection and correction methods. Construct the hamming code for the bit sequence 10011101. (PTU, Dec. 2009 ; May 2011, 2008)

OR

Compare error correcting and error detecting code. (PTU, May 2006)

Ans. Error Detecting Method : Various error detection methods are :

1. Parity checking
2. Checksum error detection
3. Cyclic redundancy check (CRC).

1. Parity Checking : This is the simplest technique for detecting errors is to add an extra bit known as parity bit. The parity of the 8-bit transmitted word can be either even or odd parity.

Even parity means number of 1's in the given word including the parity bit should be even and the odd parity means the number of 1's in the given word including the parity bit should be odd.

The parity bit can be set to 0 or 1 depending on the type of parity required. At receiving end parity of system is checked in order to detect the error.

2. Checksum Error Detection : Simple parity cannot detect two or even numbers of errors within the same word. So to overcome this problem checksum error detection method is used. In this method each successive word is added to the previous sum. This is called checksum. After transmitting a block of data bytes the checksum byte is also transmitted. The checksum byte is regenerated at the receiver separately by adding the received bytes. The regenerated checksum byte is then compared with the transmitted one. If both are identical then there is no error. If they are different then errors are present in the block.

3. Cyclic Redundancy Check : This is a type of polynomial code in which bit string is represented in form of polynomials with coefficients of 0 and 1. Polynomial arithmetic uses a modulo-2 arithmetic. For CRC code the sender and receiver should agree upon a generator polynomial G (x). A code word can be generated for a given data word polynomial M (x) with the help of long division.

Error Correction Code : Hamming codes are error correcting and detecting codes. The hamming code data is now transmitted. At the receiver it is decoded to get the data back. The bits (1, 3, 5, 7), (2, 3, 6, 7) and (4, 5, 6, 7) are checked for even parity (or odd parity). If all the 4-bits groups mentioned above possess the even parity then the received code word is correct i.e. it does not contain errors. But if the parity is not even then error exists. Such an error can be located by forming a three bit number out of the three parity checks.

Given Bit Sequence : 10011101

To construct a Hamming code :

Step I. Number of parity bits will be 4 i.e. P_1, P_2, P_3, P_4

D_{12}	D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	0	1		1	1	0		1		

Let us construct code for even parity system

$\therefore$ For $P_1\ D_3\ D_5\ D_7 = 0101$

$P_1 = 1$

For $P_2\ D_3\ D_6\ D_7 = 1111$

$P_2 = 1$

For $P_4\ D_5\ D_6\ D_7 = 0011 \Rightarrow P_4 = 0$

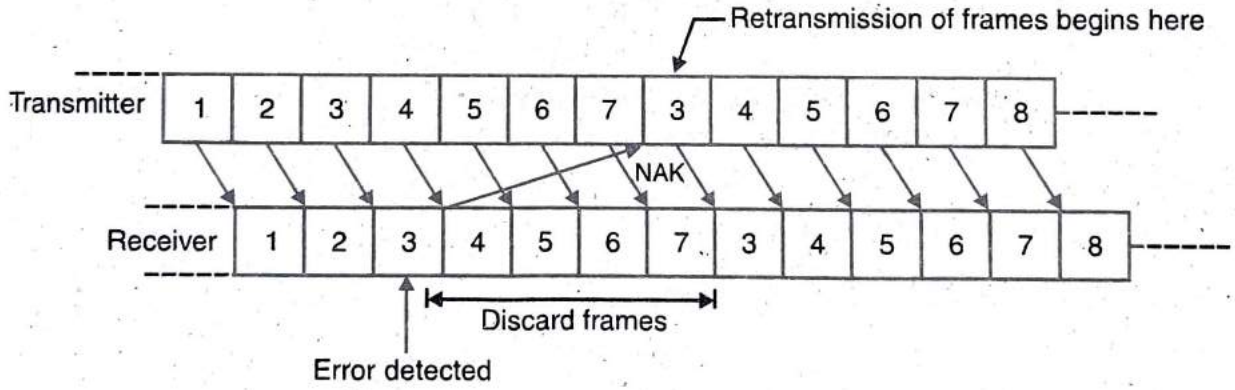
For $P_8\ D_9\ D_{10}\ D_{11} = 1100 \Rightarrow P_8 = 1$

i.e. Hamming code is

D_{12}	D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	0	1	1	1	1	0	0	1	1	1

Q 45. Explain the functioning of Go back by n protocol. **(PTU, Dec. 2009)**

Ans. Go back n protocol is a stop and wait protocol in which it was assumed that the transmission time required for a frame to arrive at the receiver plus the transmission time for the acknowledgement to come back is negligible. Also if one frame is damaged or lost, all frames are sent. Since the last frame acknowledged are transmitted. Consider the system given below :



Go Back n ARQ System

In this system sender does not wait for acknowledge signal for the transmission of next frame. It transmits the frame continously as long as it does not receive the 'NAK' signal. NAK is the negative acknowledgement signal sent by the receiver to the transmitter. When the receiver detects the error in the third frame as shown in fig., the receiver sends a NAK signal backs to sender. But this signal take some time to reach the transmitter. By that time the transmitter has transmitted frames upto 7. On reception of the NAK signal, the transmitter will retransmit all the frames from 3 onwards. The receiver discards all the frames it has received after 3 i.e. 3 to 7. It will then receive all the frames that are retransmitted by the transmitter.

Q 46. Write short note on Channel Allocation. **(PTU, May 2009)**

Ans. Channel Allocation : In any broadcast network, the key to issue is how to determine who gets to use the channel when there is competition for it. To make this point clear, consider a conference call in which six people, on six differen telephones are all connected so that each one can hear and talk to all the others. It is very likely that when one of them stops speaking, two or more will start talking at once, leading to chaos. In a face-to-face meeting, chaos is avoided by external means, for example at a meeting, people raise their hands to request permission to speak. When only a single channel is available, determining who should go next is much harder.

In the literature, broadcast channels are sometimes referred to as multiaccess channels or random access channels.

There are two ways to allocate the channel :

Static and dynamic channel allocation.

Q 47. Give limitations of parity checking. **(PTU, Dec. 2010)**

Ans. Limitations of Parity Checking :

1. Thus, the simple parity checking method has its limitations. It is not suitable for detection of multiple errors (two, four, six etc.)

2. The other limitation of parity checking method is that it cannot reveal the location of erroneous bit. It cannot correct the error either.

Q 48. Write functions of Media Access Control (MAC) sublayer. (PTU, Dec. 2010)

Ans. MAC : The broadcast channels are also called multi-access channels or random access channels. In the broadcast networks, the most important point is the criteria to determine who is allowed to use the channel when more than one users want to use it. A protocol is used to make this decision. Such a protocol, belongs to a sublayer of data link layer called the MAC (medium access control) sublayer. The MAC sublayer is very important in LANs because it is a broadcast network.

Functions of Media Access Control Sublayer :

(i) To perform the control of access to media.

(ii) It performs the unique addressing to stations directly connected to LAN.

(iii) Detection of errors.

Q 49. What are sliding window protocols? **(PTU, Dec. 2010)**

OR

What is sliding window ? Explain the various sliding window protocols for error and flow control with example. **(PTU, May 2014)**

Ans. Sliding window is a technique for controlling transmitted data packets between two network computers where reliable and sequential delivery of data packets is required, such as when using the Data Link Layer (OSI model) or Transmission control Protocol (TCP). In the sliding window technique, each data packet (for most data link layers) and byte (in TCP) includes a unique consecutive sequence number, which is used by the receiving computer to place data in the correct order. The objective of the sliding window technique is to use the sequence numbers to avoid duplicate data and to request missing data. Sliding window is also known as windowing.

Sliding window protocols are set of three protocols that are more robust and bi-directional

protocols. Sliding window refers to imaginary boxes at the transmitter and receiver. This window holds the frames at either ends and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment. Three sliding window protocols are :

1. One Bit Sliding Window Protocol (Stop and Wait ARQ) : This protocol is called one bit protocol because the maximum window size here i.e. n is equal to 1. It uses the stop and wait technique. The sender sends one frame and waits to get acknowledgement. Only after receiving the acknowledgement does it transmit the next frames. So one bit sliding window protocol is also called as stop and wait protocol.

2. Go Back n ARQ Protocol : In this protocol sender does not wait for ACK signal for the transmission of next frame. It transmits the frames continuously as long as it does not receive the NAK signal. NAK is the negative ACK signal sent by the receiver to the transmitter.

3. Selective Repeat ARQ : In this method only the specified damaged or lost frame is retransmitted. A selective repeat system differs from the go-back-n method in following ways :

(i) The receiver can do sorting of data frames and is also able to store frames received after a NAK has been sent until the damaged frame has been replaced.

(ii) The transmitter must contain a searching mechanism that allows it to find and select only the requested frame for transmission.

(iii) The window size in the method is less than or equal to (n+1)/2, whereas in case of go-back-n it is n – 1.

Q 50. What are different framing methods? **(PTU, Dec. 2010)**

Ans. Framing Methods : Following methods are used for carrying out methods :

(i) Character count

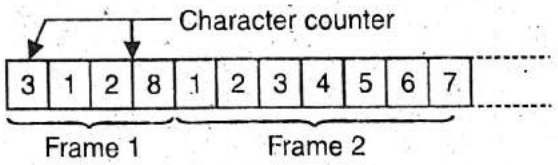
(ii) Starting and ending characters with character stuffing

(iii) Starting and ending flags with bit stuffing

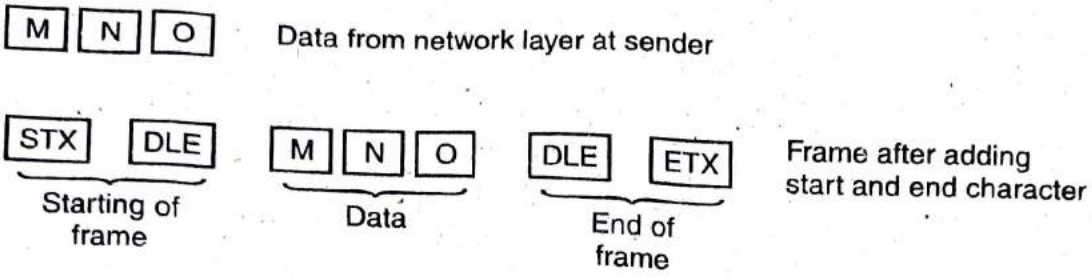
(iv) Physical layer coding violations.

(i) Character Count : In this method, a field in the header is used to specify the number of characters in the frame. This number helps the receiver to know the number of characters in the frame following this count. The character count method is illustrated in fig. 1.

The two frames shown in fig. 1 are of B and 8 characters respectively. The disadvantage of this method is that, an error can change the character count. If the wrong character count number is received then the receiver will get out of synchronization and will be unable to locate the start of next frame. The character count method is rarely used in practice.

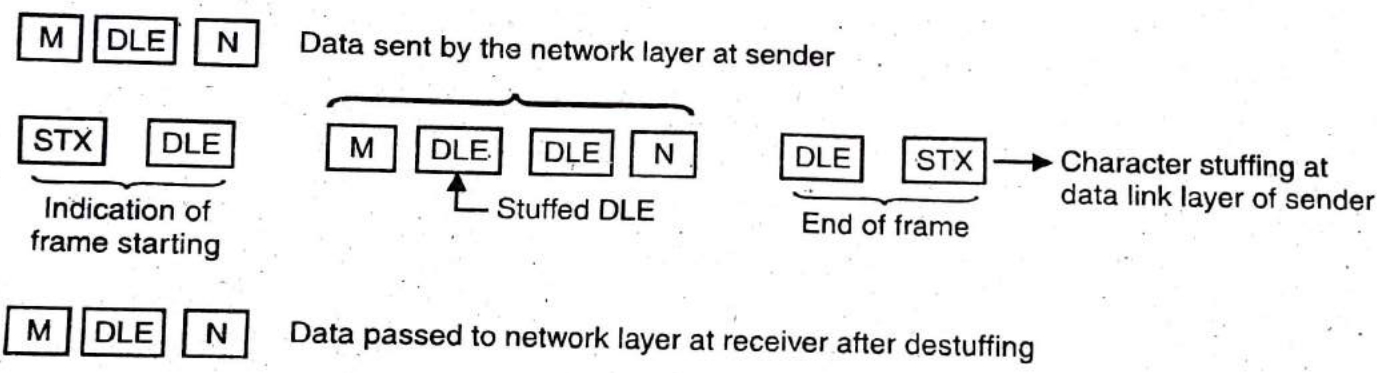


Starting and Ending Character With Character Stuffing : The problem of character count method is solved here by using a starting character before the starting of each frame and an ending character at the end of each frame. Each frame is preceded by the transmission of ASCII character sequence DLESTX (DLE stands for data link scape and STX is start of Text). After each frame, the ASCII character sequence DLEETX is transmitted. Here, DLE stands for data link escape and ETX stands for END of text. Hence, if the receiver loses the synchronization, it just has to search for the DLESTX or DLEETX characters to return back on track. This is shown in fig. 2.

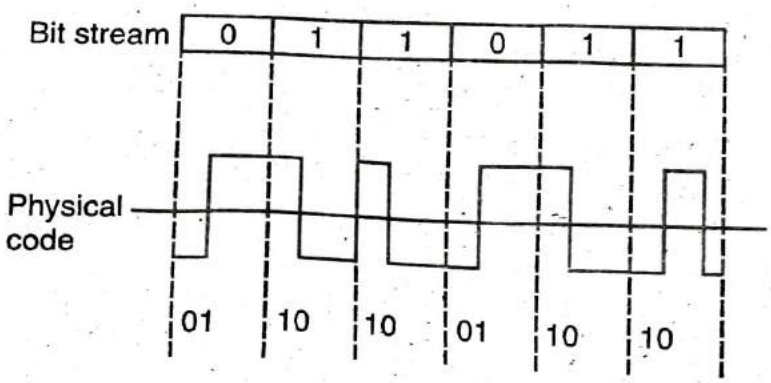


Character Stuffing : The problem with this system is that the characters DLE STX or DLE ETX can be a part data as well. If so, they will be misinterpreted by the receiver as start or end of frame. This problem is solved by using a technique called character stuffing. Which is as.

The data link layer at the sending end inserts an ASCII DLE character just before each accidental. DLE character in the data. The data link layer at the receiving end will remove these DLE characters before handing over the data to the network layer. Thus, the framing DLE STX or DLE ETX can be distinguished from the one in data because DLEs in the data are always doubled. This is called character stuffing and it is shown in 3. It may be noted that at the receiving end, the destuffing is essential.



Physical Layer Coding Violations : This method of framing is applicable only to the networks in which the encoding on the physical medium contains same redundancy. Some LANs encode each bit of data using two physical bits. The Manchester coding is generally used. Normally, a 1 bit is encoded into a 10 pair and a 0 bit is encoded into a 01 pair as shown in fig. 4. This use of invalid physical code is a part of 802 LAN standards.



Q 51. Explain as to how error detection at the data link level is achieved.
(PTU, May 2011)

Ans. To enable the error detection, it adds error detection bits to the data which is to be transmitted. These error detection bits are used by the data link on layer on the other side to detect the correct the errors.

Q 52. If a size of a window is 3 bits, how many packets can be sent using Sliding Window protocol? Explain your answer. Explain the factors which will determine the length of the sliding window.
(PTU, May 2011)

Ans. Buffers are used at each end of the TCP connection to speed up data flow when the network is busy. Flow Control is managed using the concept of a **Sliding Window**. A Window is the maximum number of unacknowledged bytes that are allowed in any one transmission sequence, or to put it another way, it is the range of sequence numbers across the whole chunk of data that the receiver (the sender of the window size) is prepared to accept in its buffer. The receiver specifies the current **Receive Window** size in every packet sent to the sender. The sender can send up to this amount of data before it has to wait for an update on the Receive Window size from the receiver. The sender has to buffer all its own sent data until it receives ACKs for that data. The **Send Window** size is determined by whatever is the smallest between the Receive Window and the sender's buffer. When TCP transmits a segment, it places a copy of the data in a retransmission queue and starts a timer. If an acknowledgment is not received for that segment (or a part of that segment) before the timer runs out, then the segment (or the part of the segment that was not acknowledged) is retransmitted.

Sliding Window Operation

1. The current sequence number of the TCP sender is **y**.
2. The TCP receiver specifies the current negotiated window size **x** in every packet. This often specified by the operating system or the application, otherwise it starts at 536 bytes.
3. The TCP sender sends a datagram with the number of data bytes equal to the receiver's window size **x** and waits for an **ACK** from the receiver. The window size can be many thousands of bytes!
4. The receiver sends an **ACK** with the value **y + x** i.e. acknowledging that the last **x** bytes have been received OK and the receiver is expecting another transmission of bytes starting at byte **y + x**.
5. After a successful receipt, the window size increases by an additional **x**, this is called the **Slow Start** for new connections.
6. The sender sends another datagram with **2x** bytes, then **3x** bytes and so on up to the **MSS** as indicated in the TCP **Options**.
7. If the receiver has a full buffer, then the window size is reduced to zero. In this state, the window is said to be **Frozen** and the sender cannot send any more bytes until it receives a datagram from the receiver with a window size greater than zero.

8. If the data fails to be received as determined by the timer which is set as soon as data is set until receipt of an ACK, then the window size is cut by half e.g. from **4x** to **2x**. Failure could be due to congestion e.g. a full buffer on the receiver, or faults on the media.
9. On the next successful transmission, the slow ramp up starts again.

Q 53. What is the role CRC in data link layer? **(PTU, Dec. 2011)**

Ans. The last two bytes of a message contain a 16-bit CCTTT.CRC is little-endian order. The algorithm for the initial is not known. It is indexed by the length i.e. the number of bytes over which CRC is taken.

Q 54. Name elementary data link protocols used in flow control mechanism. **(PTU, Dec. 2011)**

Ans. Data link protocols used in flow control mechanism are as follow :

- **Simplex :** Transmission in one direction. The receiver is always ready to receive the next frame (has infinite buffer storage
- **Stop and wait :** Such elementary protocols are also called PAR (Positive Acknowledgment with Retransmission) or ARQ (Automatic Repeat request). Data frames are transmitted in one direction (simplex protocols) where each frame is individually acknowledge by the receiver by a separate acknowledgment frame,
- **Sliding window protocol :** These protocols allow both link nodes (A, B) to send and receive data and acknowledgments simultaneously.
- **HDLC :** Bit-oriented protocol derived from IBM's SNA data link protocol SDLC (Synchronous Data Link Control). Uses sliding window with 3-bit sequence numbers.

Q 55. How does CRC checker know that the receiver data unit is undamaged? Explain it with example. **(PTU, Dec. 2011)**

Ans. The polynomial code, also known as a CRC (Cycle Redundancy Check). Polynomial codes are based upon treating bit strings as representation of polynomials with coefficients of 0 and 1 only. A K-bit frame is regarded as the coefficient list for a polynomial with k terms, ranging from x^{K-1} list is the coefficient of x^{K-1}, the next bit is the coefficient of x^{K-2}, and so on. When the polynomial code method is employed, the sender and receiver must agree upon a generator polynomial, G (x), in advance. Both the high and low order bits of the generator must be 1.

Q 56. What is a hamming distance? **(PTU, Dec. 2012 ; May 2012)**

Ans. Hamming code is technique developed by R.W. Hamming for error correction. The method corrects the error by finding the state at which the error has occurred. The specific number of redundancy bits is added to actual data unit.

Q 57. List the different error detection codes. **(PTU, Dec. 2012)**

Ans. When data is being transmitted from one machine to another, it may be possible that data becomes corrupted on its way.

Types of Errors :

1. Single bit error
2. Burst error

Error detection techniques :

1. Redundancy
2. Vertical redundancy check (VRC)
3. Longitudinal redundancy check
4. Cyclic redundancy check
5. Checksum

Q 58. Explain stop and wait data link protocol with suitable diagram.

(PTU, May 2012)

Ans. Method of flow control :

Stop and wait protocol or method :

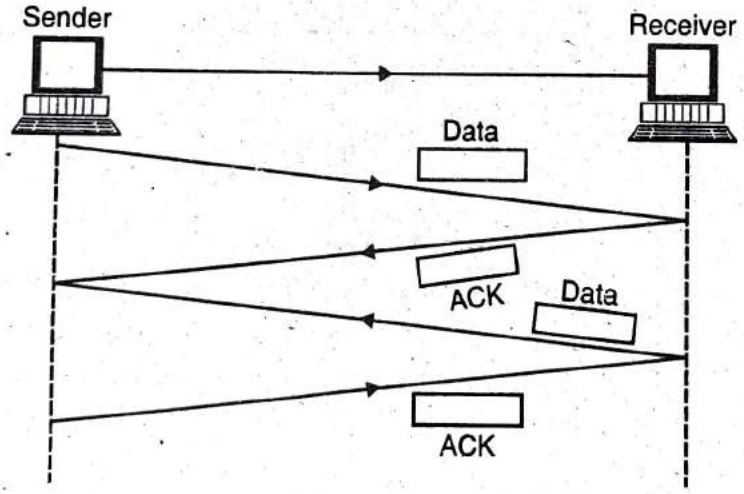
(i) In this method of flow control, the sender sends a single frame to receiver and waits for an acknowledgement.

(ii) The next frame is sent by sender only when acknowledgement of previous frame is received.

(iii) This process of sending a frame and waiting for an acknowledgement continues as long as the sender has data to send.

(iv) To end up the transmission sender transmits end of transmission (EOT) frame.

(v) The main advantage of stop and wait protocol is its accuracy. Next frame is transmitted only when the first frame is acknowledged. So, there is no chance being lost.



Stop and Wait Method

Q 59. Explain the working of sliding window flow control using diagram.

(PTU, Dec. 2012)

Ans. Sliding window protocol or method :

1. In sliding window method, multiple frames are sent by sender at a time before needing an acknowledgement.

2. Multiple frames sent by source are acknowledged by receiver using a single ACK frame.

Sliding Window :

1. Sliding window refers to an imaginary boxes that hold the frames of both sender and receiver sides.

2. It provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement.

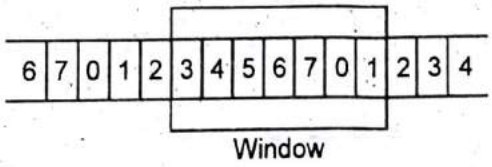
3. Frames may be acknowledged by receiver at any point even when window is not full on receiver side.

4. Frames may be transmitted by source even when window is not yet full on sender side.

5. The windows have a specific size in which the frames are numbered model on, which means they are numbered from 0 to n – 1. For example, if n = 8, the frames are numbered 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1.

6. The size of window is n – 1. For example, in this case it is 7. Therefore, a maximum of n – 1 frames be sent before an acknowledgement.

7. When the receiver sends an ACK, it includes the number of next frame it expects to receive, for example, in order to acknowledge the group of frames ending in frame 4, the receiver sends an ACK containing the number 5. When sender sees an ACK with number 5, it comes to know that all the frames up to number 4 have been received.



Sliding Window

❑❑❑

Chapter 4

Medium Access Sub-Layer

Contents

Static and dynamic channel allocation, Random Access : ALOHA, CSMA protocols, Controlled Access : Polling, Token Passing, IEEE 802.3 frame format, Ethernet cabling, Manchester encoding, collision detection in 802.3, Binary exponential back off algorithm.

POINTS TO REMEMBER

- MAC sub-layer of IEEE project 802 defines the specific access methods for each LAN.
- IEEE 802.4 standard for media access control is known as token bus.
- IEEE 802.5 standard is known as token ring.
- A ring consists of a collection of ring interfaces connected by point to point lines i.e. ring interface of one station is connected to the ring interfaces of its left station as well as right station.
- Token bus is a linear or tree shape cable to which the stations are attached.
- Token passing is method used in those networks where the stations are organized in a logical ring.
- Carrier sense multiple access/collision detection :
  Whenever multiple users have unregulated access to a single line, there is a danger of signals overlapping and destroying each other.
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA are chances of collision in pure ALOHA are very high.
- In pure ALOHA the stations transmit frames whenever they have data to send.
- Aloha was used for ground based radio broadcasting.
- CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance.
- In dynamic allocation method, none of the users is assigned fixed frequency or fixed time slot.
- In broadcast or multipoint networks, single channel is shared by several stations.

QUESTION-ANSWERS

Q 1. What is broadcast network?

Ans. In broadcast network, several stations share a single communication channel. The major issue in these networks is, which station should transmit data at a given time interval. This process of deciding the turn of different stations is known as channel allocation.

In broadcast network channel is also known as multi-access channel or random access channel.

Q 2. What is channel allocation?

Ans. In broadcast or multipoint networks, single channel is shared by several stations. This channel can be allocated only to one transmitting user at a time.

There are two different methods of channel allocation.

1. Static channel allocation
2. Dynamic channel allocation.

Q 3. What is static channel allocation in LANs and MANs?

Ans. 1. In static channel allocation method, a single channel is divided amongst various users either on the basis of frequency or on the basis of time.

2. The static channel allocation either uses FDM (frequency division multiplexing) or TDM (Time division multiplexing).

Q 4. What is dynamic allocation of channel?

Ans. In dynamic allocation method, none of the users is assigned fixed frequency or fixed time slot. Following assumptions are made in order to implement this method.

1. Station model : The model consists of N independent stations that may be a computer, telephone or personal communicator, etc.

2. Single channel : A single channel is available for all communications. All stations can transmit on it and all can receive from it.

3. Collision : If two stations transmit frames simultaneously, then these frames will overlap and the resulting signal is garbled. This is known as collision.

4. Continuous time : It means that frame transmission can begin at anytime.

5. Slotted time : It means the time is divided into slots or discrete intervals. Frame transmission begins at the start of slot. A slot may contain 0, 1 or more frames.

6. Carrier sense : It means the stations are able to sense the channel before transmission.

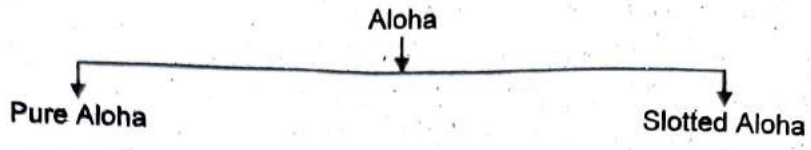
Q 5. What is aloha?

Ans. 1. Aloha was developed at university of Hawaii in early 1970s by Norman Abramson and his colleagues.

2. It was used for groundbased radio broadcasting.

3. In this method, stations share a common channel.

4. When two stations transmit simultaneously, collision occurs and frames are destroyed.
5. There are two different versions/types of ALOHA :
   (i) Pure Aloha
   (i) Slotted Aloha



Q 6. Comparison between 1-persistent, non-persistent and p-persistent CSMA.
Ans.

Characteristics	1-Persistent	Non-persistent	P-Persistent
1. Carrier sense	1. Sends with probability, when channel is idle.	1. Sends when channel is idle.	1. Sends with probability P when channel is idle.
2. Waiting	2. Continuously senses the channel or carrier.	2. Waits for random amount of time to check carrier.	2. Waits until next time slot.
3. Utilization	3. Above ALOHA as frames are sent only when channel is idle.	3. Above I-persistent as not all the stations constantly check channel.	3. Depends upon probability P.
4. Delay low load	4. Small as frames are sent when channel becomes idle.	4. Small as station will send whenever channel is found idle.	4. Large when P is small as station will not always send when idle.
5. Chances of collision	5. Highest	5. Less than I-persistent but more than P-persistent.	5. Less as compared to I-persistent and non-persistent.

Q 7. What is CSMA?

Ans. 1. CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance.

2. CSMA protocol is based on the principle of 'carrier sense'. The station senses the

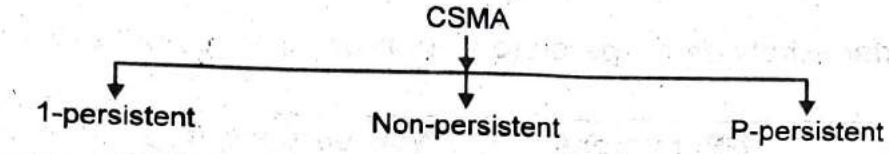
carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.

3. The chances of collision can be reduced to great extent if a station senses the channel before trying to use it.

4. Although CSMA can reduce the possibility of collision, but it cannot eliminate it completely.

5. The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations.

There are three different types of CSMA protocols.



Q 8. Compare IEEE standard 802.3 and 802.4. **(PTU, Dec. 2012)**

OR

Comparison of IEEE 802.3, 802.4 and 802.5 standard. **(PTU, Dec. 2010, 2007)**

Ans.

S.No.	Parameter	802.3 Ethernet	802.4 Token Bus	802.5 Token Ring
1.	Physical topology	Linear	Linear	Ring
2.	Logical topology	None	Ring	Ring
3.	Cable length	50 m to 2000 m	200 m to 500 m	50 m to 1000 m
4.	Cable type	Twisted pair, coaxial cable, fibre optic	Coaxial	Twisted pair and fibre optic
5.	Frequency	10 Mbps to 100 Mbps	10 Mbps	4 to 100 Mbps
6.	Frame structure	1500 bytes	8191 bytes	5000 bytes
7.	Contention	Random chance	By token	By token
8.	Addition of stations	A new station can be added almost anywhere on the cable at any time	Distributed algorithm is needed to add new stations	A new station must be added between two specified stations Stations must wait for
9.	Performance	Stations often transmit immediately under light loads, but heavy traffic can reduce effective data to nearly 0	Station must wait for token even if no other station is transmitting. It provides fair access to all	the token even if no other station is transmitting. Under heavy load token passing provides fair access to all stations.
10.	Maintenance	No central maintenance	Distributed algorithm provides maintenance	A designated monitor station performs maintenance.

Q 9. Difference between pure ALOHA and slotted ALOHA. (PTU, Dec. 2012, 2007)

Ans. Pure Aloha :

1. In pure ALOHA, the stations transmit frames whenever they have data to send.
2. When two or more stations transmit simultaneously, there is a collision and the frames are destroyed.
3. In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
4. If acknowledgement is not received within specified time, the station assumes that the frame has been destroyed.
5. If the frame is destroyed because of collision, the station waits for a random amount of time and sends it again. Thus, waiting time must be random otherwise same frames will collide again and again.
6. Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

Slotted Aloha :

1. Slotted Aloha was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
2. In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
3. The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
4. In slotted ALOHA, if any station is not able to place the frame on to the channel at the beginning of slot, i.e., it misses the time slot, then the station has to wait until the beginning of the next time slot.
5. Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one half.

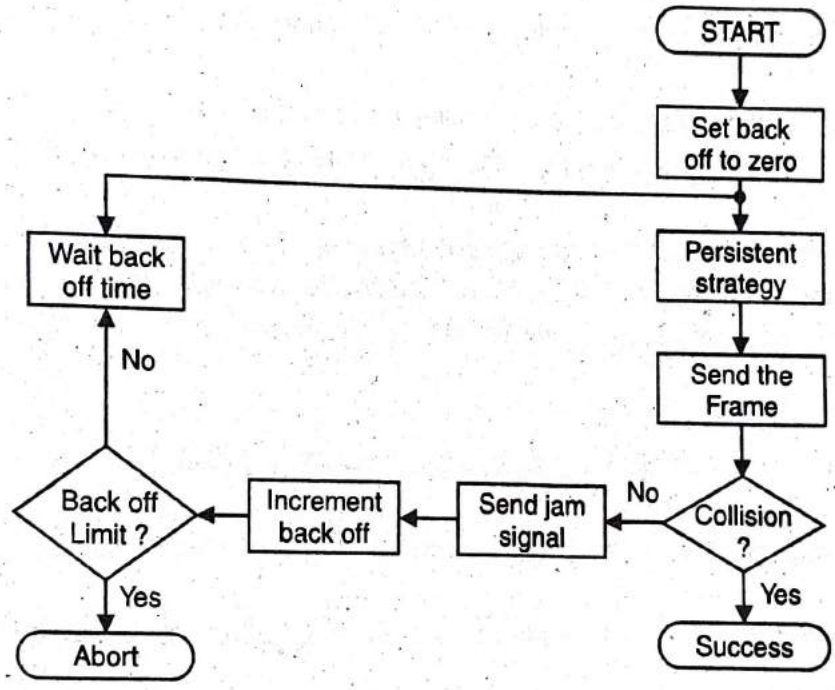
Q 10. What is CSMA/CD? (PTU, Dec. 2004)

Ans. Carrier Sense Multiple Access/Collision Detection (CSMA/CD) : Whenever multiple users have unregulated access to a single line, there is a danger of signals overlapping and destroying each other. Such overlaps, which turn the signals into unusable noise are called collisions. As traffic increases on a multiple-access link, so do collisions. A LAN, therefore, needs a mechanism to coordinate traffic, minimize the number of collisions that occur and maximize the number of frames that are delivered successfully. The access mechanism used in an Ethernet is called carrier sense multiple access with collision detection (CSMA/CD). In CSMA/CD the station wishing to transmit first listens to make certain the link is free, then transmits its data, then listens again. During the data transmission, the station checks the line for the extremely high voltage that indicates a collision. If a collision is detected, the transmitting station releases a jam signal. The jam signal will alert the other stations. The

stations then are not supposed to transmit immediately after the collision has occurred. Otherwise there is a possibility that the same frames would collide again. After some "back off" delay time the station will retry the transmission. If again the collision takes place then the back off time is increased progressively.

Q 11. How CDMA technology actually works? **(PTU, Dec. 2007)**

Ans. Flow chart of working of CDMA technology is given below :



CSMA/CD procedure

Explanation :

- The station that has a ready frame sets the back off parameter to zero.
- Then it senses the line using one of the presistent strategies.
- If then sends the frame if there is no collision for a period corresponding to one complete frame, then the transmission is successful.
- Otherwise the station sends the jam signal to inform the other stations about the collision.
- The station then increments the back off time and waits for a random back off time and sends the frame again.
- If the back off has reached its limit, then the station aborts the transmission.
- CSMA/CD is used for the traditional ethernet.

Q 12. A slotted ALOHA channel has an average 10% of the slots idle. What is the offered traffic G? Calculate the throughput and determine whether the channel is overloaded or underloaded? **(PTU, Dec. 2008)**

Ans. Idle slots = 10% = $\frac{10}{100}$ = .1

Slots occupied = 0.9

Offered traffic = $e^{-0.9}$ = 0.406 erlangs

$$\text{Throughput} = \frac{1}{0.9} \times e^{-0.9} = 0.45$$

As for slotted ALOHA maximum througput should be 0.3679, but there throughput is 0.45 so channel is overloaded.

Q 13. Explain the frame format of CSMA/CD.

Ans.

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1500 bytes	4 bytes
Preamble	Start frame delimiter	Destination address	Source address	Length	Data	Frame check sequence

1. Preamble : It is seven bytes (56 bits) that provides bit synchronization. It consists of alternating 0's and 1s. The purpose is to provide alert and timing pulse.

2. Start frame delimiter (SFD) : It is one byte field with unique pattern : 10101011. It marks the beginning of frame.

3. Source address : It is also a six byte field and contains the physical address of source or last device to forward the packet.

4. Destination address : It is six byte field that contains physical address of packet's destination.

5. Length : This two byte field specifies the length or number of bytes in data field.

6. Data : It can be of 46 to 1500 bytes.

7. Frame checksum sequence : This for byte field contains CRC for error detection.

Q 14. What is token passing?

Ans. 1. Token passing is method used in those networks where the stations are organized in a logical ring.

2. In ring network, each station has a predecessor and a successor.

3. In such networks, a special packet called token is calculated through the ring.

4. Whenever any station has some data to send, it waits for token. It transmits data only after it gets the possesson of token.

5. After transmission the data, the station releases the token.

Q 15. What is MAC?

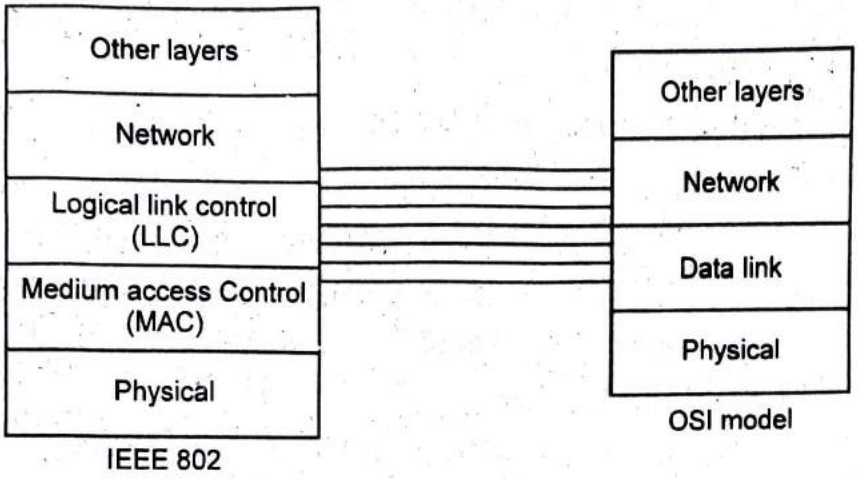
Ans. MAC sub-layer of IEEE project 802 defines the specific access methods for each LAN. For example, it defines CSMA/CD as the media access method for ethernet LANs and token passing method for Token Ring and Token Bus LANs.

Q 16. What is IEEE standards?

Ans. 1. The Institute of Electrical and Electronic Engineers (IEEE) has developed several standards for LANs. These standards are collectively known as IEEE 802 or Project 802.

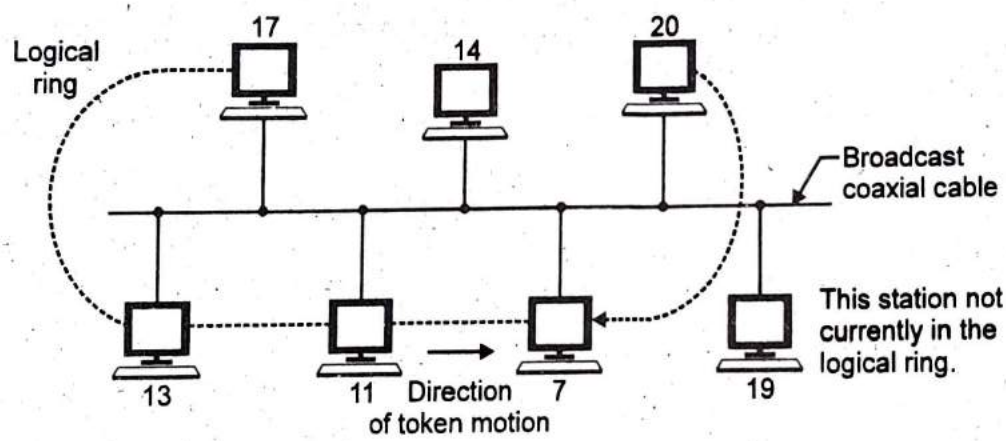
2. The various standards differ at the physical layer and MAC sub-layer but are compatible at the data link layer.

3. IEEE project 802 divides data link layer into two sub-layers : logical link control (LLC) and medium access control (MAC).



Q 17. What is token bus?

Ans. IEEE 802.4 standard for media access control is known as token bus.



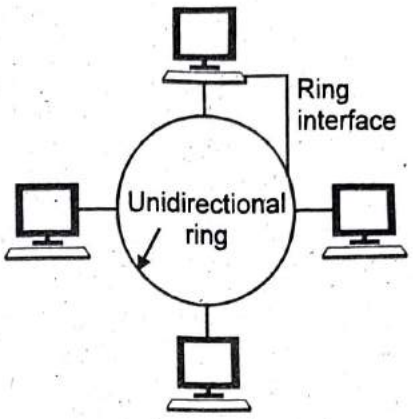
- Physically, the token bus is a linear or tree-shape cable to which the stations are attached.
- Logically, the stations are organized into a ring.
- Each station knowns the address of the station to its left and right i.e. address of the preceding station and the station following it.
- When the logical ring is initialized, the highest numbered station may send the first frame.
- After doing so, it passes the permission to its immediate neighbour by sending a special control frame to it. This control frame is called a token.
- In such a way, a token circulates round logical ring, and only the station holding a token is allowed to transmit data.
- In such a case, there is no collision as only one station possesses a token at any given time.

- In token bus, each station receives each frame, the station whose address is specified in the frame processes it and other stations discard the frame.

Q 18. What is token ring?

Ans.

- IEEE 802.5 standard is known as token ring.
- A ring consists of a collection of ring interfaces connected by point to point lines i.e. ring interface of one station is connected to the ring interfaces of its left station as well as right station.
- These point to point links can be created with twisted pair, coaxial cable or fibre optics.
- Each bit arriving at an interface is copied into a 1 bit buffer.



Q 19. Name various operations of Data link layer. **(PTU, Dec. 2009)**

Ans. Operations of data link layer are :

1. Function of data link layer are synchronization and error control for the information which is to be transmitted over the physical link.
2. To enable the error detection, it adds error detection bits to the data which is to be transmitted.
3. The encoded data is then passed to the physical layer.
4. These error detection bits are used by the data link on layer on the other side to detect the correct the errors.
5. At this level outgoing messages are assembled into frames and the system waits for the acknowledgements to be received after every transmitted.
6. Correct operation of data link layer ensures reliable transmission of each message. Example of data link layer protocols are HDLC, SDLC and X.25 protocol.

Q 20. Which IEEE standard is used for wired and wireless LANs?

(PTU, May 2010)

Ans. IEEE 802.3 is wired LAN network
and IEEE 802.11 is wireless LAN working group.

Q 21. What are the advantages and limitations of using frame relay over X.25 for communication? What are the various steps in congestion control handling in frame relay networks? **(PTU, Dec. 2008)**

Ans. The advantage of frame relay over X.25 include the following : Frame relay eliminates many protocol overheads inherent in the X.25 protocol. Frame relay supports a hgiher transmission rate and boosts a better performance than X.25.

The disadvantages of frame relay over X.25 include the following. Because frame relay does not support error correction or recovery, it is not designed to operate over erroneous transmission media. The results can be diastrous if frame relay is used over a transmission

media with high error rates. Therefore, frame relay requires better quality and more expensive physical cabling.

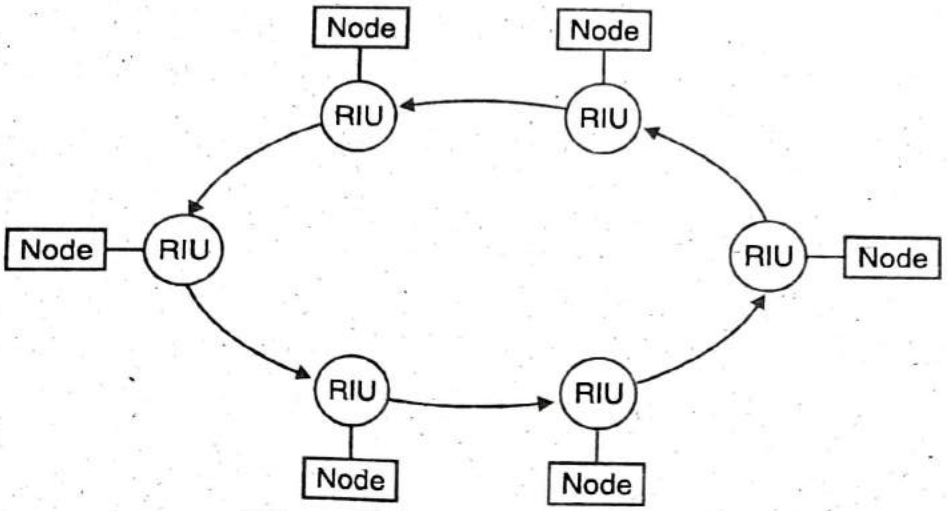
Q 22. Describe in detail the principle of CSMA/CD and Token ring protocol.
(PTU, Dec. 2008)

OR

With the help of neat diagrams, explain the 802.3 frame format and its working. How does 4B/5B encoding guarantee that there will be no sequences of four or more 0s in the data field?
(PTU, May 2008)

Ans. Carrier Sense Multiple Access/Collision Detection (CSMA/CD) : Whenever multiple users have unregulated access to a single line, there is a danger of signals overlapping and destroying each other. Such overlaps, which turn the signals into unusable noise are called collisions. As traffic increases on a multiple-access link, so do collisions. A LAN therefore needs a mechanism to coordinate traffic, minimize the number of collisions that occur and maximize the number of frames that are delivery successfully. The access mechanism used in an Ethernet is called carrier sense multiple access with collision detection (CSMA/CD). In CSMA/CD the station wishing to transmit first listens to make certain the link is free, then transmits its data, then listen again. During the data transmission, the station checks the line for the extremely high voltage that indicate a collision. If a collision is detected, the transmitting station release a jam signal. The jam signal will alert the other stations. The stations then are not supposed to transmit immediately after the collision has occurred. Otherwise there is a possibility that the same frames would collide again. After some "back off" delay time the station will retry the transmission. If again the collision takes place then the back off time is increased progressively.

Token Ring : Token ring is shown below :



Token ring works very differently from ethernet. In ethernet any node that has data can transmit until it has a collision with other node.

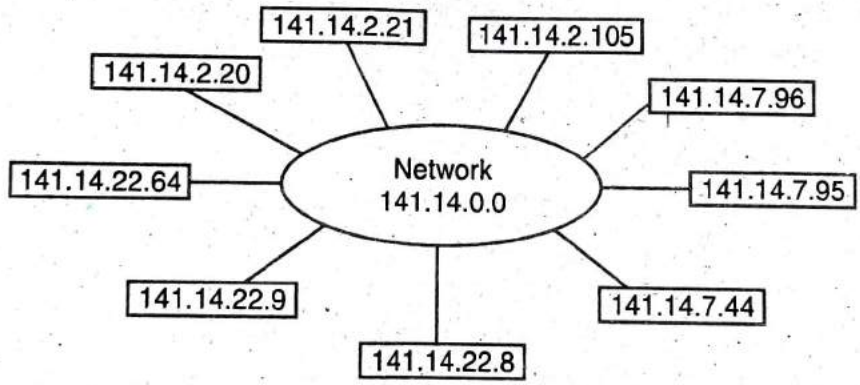
In token ring a single special packet is called a token which is fast around the network. When the node has a data to transmit, it waits untill data is available, it grabs it and retransmit

the data packet. Simultaneously releasing the token to the next node in line, then the next node grabs the token if it has a data to transmit. The wiring and physical arrangement are similar to star network. Instead of having a concentrated at the centre of ring, the network has a device called MAU.

It has same job as that HUB. But it works with token ring instead of ethernet network and handles communication between nodes slightly different. The token ring was developed by IBM as a highly reliable network. It is more complex than ethernet. Token ring is an IEEE 802.5 standard whose topology is physically star but logically a ring. The workstation connect to the bus by a RIU (Ring Interface Unit).

Q 23. What is subnetting? What it is used? **(PTU, Dec. 2010)**

Ans. As IP address is 32 bit long. One portion of the address indicates a net id and the other portion indicates the host on the network i.e. host id. This means that there is a sense of hierarchy in IP addressing. To reach a host on the internet, we must first reach the network using the first portion of address i.e. netid. Then we much reach the host itself using the second portion (hostid). In other words classes A, B and C in IP addressing are designed with two levels of hierarchy. However in many cases, these two levels of hierarchy are not enough. For example imagine an organisation with a class B address. The organisation has two level of hierarchy addresses but it cannot have more than one physical network as shown in fig.



With this scheme, the organisation is limited to two levels of hierarchy. The hosts cannot be organized into groups and all of the hosts are at the same level. The organisation has one network with many hosts. One solution of this problem is subnetting, the further division of a network into smaller networks called subnet.

For 1000 users, with each set of 256 users at different location.

Total of 1000 addresses are required. As for class C total 256 address are available. So we will use 4 blocks of class C each at a one location corresponding to 256 addresses.

Q 24. What is IEEE 802.11? What are various uses involve in IEEE 802.11 and also explain its security features. **(PTU, May 2011)**

Ans. Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well data transmission. The most widely used standard is 802.11 produced by the Institute and Electronic Engineers (IEEE). This is a standard defining all aspects of radio frequency wireless networking.

Issues involved in IEEE 802.11 : Since wireless devices need to be small and wireless networks are bandwidths limited, some of the key challenges in wireless networks are :

(a) Data Rate Enhancements (b) Low Power Networking (c) Security (d) Radio Signal Interfere (e) System Interoperability

Security Features of IEEE 802.11 :

(a) Data Compromise is any form of disclosure to unintended parties of information. Data compromise can be inappropriate access to payroll records by company employees whereby marketing plans are disclosed to a competitor.

(b) Denial of service is an operation designed to block or disrupt normal activities of a network or facility. This can take the form of false requests for login to a server.

(c) Unauthorized access is any means by which an unauthorized party is allowed access to network resources or facilities.

Q 25. What is CDMA? **(PTU, Dec. 2011)**

Ans. CDMA (Code Division Multiple Access) works completely differently. When CDMA was first proposed, the industry gave it approximately the same reaction that Columbus first got from Queen Isabella when he proposed reaching India by sailing in the wrong direction.

Q 26. Which MAC layer protocol is used by 802.11 WLAN? **(PTU, May 2011)**

Ans. IEEE 802.11 based MAC protocols are gaining widespread popularity as a layer-2 protocol for WLANs. The IEEE 802.11 standard covers both physical and MAC layer of open system interconnection (OSI) model.

Q 27. What is IEEE 802.4 standard? **(PTU, Dec. 2012)**

Ans. IEEE 802.4 : Token bus

- Physically the token bus is a linear or tree-shape cable to which the stations are attached.
- Logically the stations are organized into a ring.
- Each station knows the address of the station to its left and right i.e. address of the preceding station and the station following it.
- When the logical ring is initialized, the highest numbered station may send the first frame.
- After doing so, it passes the permission to its immediate neighbour by sending a special control frame to it. This control frame is called a token.

❑❑❑

Chapter 5

Network Layer

Contents

Design issues, IPv4 classful and classless addressing, subnetting, Routing algorithms: distance vector and link state routing, Congestion control: Principles of Congestion Control, Congestion prevention policies, Leaky bucket and token bucket algorithms.

POINTS TO REMEMBER

- Network layer is responsible for performing the functions such as internetworking, addressing, routing, packetizing, fragmenting.
- A connection-oriented service is one in which the user is given a reliable end to end connections.
- Network layer is responsible for carrying the packet from the source all the way to destination. In short it is responsible for host-to-host delivery.
- Routing algorithms are of two types :
  Non-adaptive and adaptive algorithm.
- For now adaptive algorithm, the routing decision is not based on the measurement of estimation of current traffic and topology.
- In a connection-oriented service is one in which the user is given a reliable end to end connections.
- In a connection less service, the user simply bundles his information together, puts an address on it and then send it off in the hope that it will reach its destination.
- Routing algorithm is a part of network layer software. It is responsible for deciding the output line over which a packet is to be sent.
- In shortest path routing a graph of subnet is built in which each node representing the router and each are representing a link or a communication line.
- Flooding is a type of algorithm in which every incoming packet is sent over an every out going line except the line or which it has arrived.
- The number of subnets in a network is determined by the number of extra 1s.
- The smaller parts of network are called subnets.
- An address mask determines which portion of an IP address identifies the network and which portion identifies the host.

- IP addresses are classified into five types :
  Class A
  Class B
  Class C
  Class D
  Class E
- IP address is an internetwork address which is universally unique.
- All the IP addresses are 32 bit long and they are used in the source address and destination address field of the IP address.
- Address resolution protocol is used to resolve MAC address from IP addresses.
- RARP (Reserve address resolution protocol) it is used to resolve IP address for MAC addresses.
- When two many packets are present in a part of a subnet, the performance degrates. This situation is called congestion.

QUESTION-ANSWERS

Q 1. Explain in brief network layer design issues. **(PTU, Dec. 2005)**

Ans. The network layer has been designed with the following goals :

1. The services provided should be independent of the underlying technology. Users of the services need not be aware of the physical implementation of the network.

2. There is no guarantee that the bundle will arrive. So a connectionless service is one reminiscent of the postal code.

3. A connection-oriented service is one in which the user is given a "reliable" end to end connection.

4. Finally, there is need for some uniform addressing scheme for network addresses :
(i) Connection oriented network services
(ii) Connectionless network services.

5. To communicate, the user requests a connection, then uses the connection to his content, and then closes the connection.

Q 2. What is routing and how is it done? Also discuss the various categories of routing algorithms available in network layer. **(PTU, Dec. 2011)**

OR

Write a short note on routing algorithms. **(PTU, Dec. 2009, 2005 ; May 2009)**

Ans. Routing Algorithms : Network layer one of the important function is to route the packets from source to destination machiine. The major area of network layer design includes the algorithms which choose the routes and the data structures which are used. Routing algorithm is a part of network layer software. It is responsible for deciding the output line over which packet is to be sent. Such a decision is dependent on whether the subnet is a virtual circuit or it is a diagram switching.

There are certain desirable properties of a routing algorithm that are :

1. Correctness
2. Robustness
3. Stability
4. Fairness
5. Optimality

Routing algorithms can be divided into two groups :

1. Non-adaptive algorithm
2. Adaptive algorithm.

Q 3. Explain subnet mask.

Ans. 1. Subnet mask uses the same format and representation technique as IP addresses.

2. Subnet mask has binary is in all bits specifying the network and subnetwork fields, and binary 0s in all bits specifying the host field.

3. A subnet address is created by borrowing the bits from host field.

Network	Network	Subnet	Host
11111111	11111111	111 11111	000 00000
255	255	255	0

Subnet mask for class B address

4. The subnet mask for a class C address 192.168.2.0 that specifies five bits of subnetting is 255.255.255.248 with five bits available for subnetting, $2^5 - 2 = 30$ subnets possible, with $2^3 - 2 = 6$ hosts per subnet.

Q 4. Explain logical addressing i.e. IP addressing.

Ans.

- In order to provide computer to computer communication via Internet, we need a global addressing scheme. Such an addressing is provided by Internet protocol (IP) at the network layer.
- Each host and router on the Internet is assigned a unique 32-bit logical address. This is called an IP address.
- This IP address is unique and no two devices on the Internet can have the same address at the same time.
- Each 32-bit IP address is divided into two main parts, the network number and the host number. The network number identifies a network. The host is number identifies a host on the network.
- A network number is assigned by the Internet Network Information Centre (Inter NIC).
- Since an IP address is 32-bit, the address space is 2^{32} or 4, 294, 967, 296.

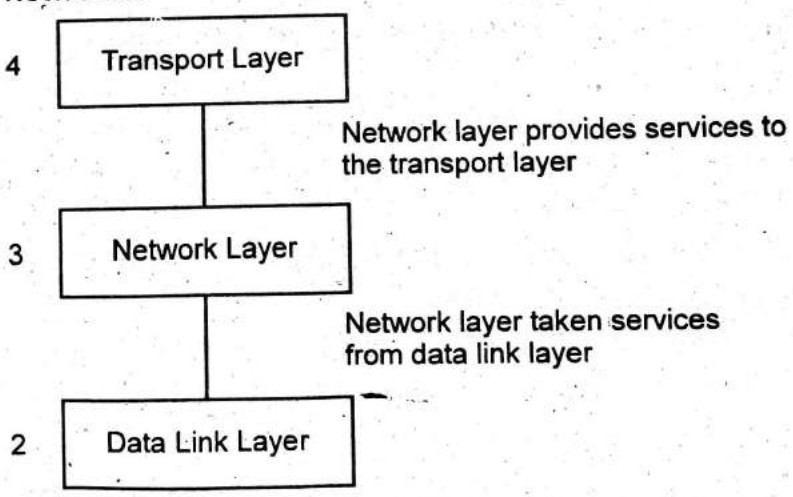
Q 5. Explain difference between virtual circuit subnet and datagram subnet.

Ans. The various features of virtual circuit subnet and datagram subnet are tabulated below :

Parameter	Virtual circuit subnet	Datagram subnet
1. Circuit setup	Required	Not required
2. Addressing	Each packet contains a short VC number.	Each packet contains full source and destination address.
3. Routing	Route is chosen when VC is setup. All packets follow same route.	No route is chosen before hand. Each packet follows independent routes.
4. State information	A table is required in router that holds state information.	Subnet does not hold any state information.
5. Effect of router failure	All virtual circuits passing through failed router are terminated.	Only the packets that are queued up in the router are lost.
6. Congestion control	Easy, if enough buffers are allocated in advance for each VC.	Difficult
7. Repairs	Difficult	Easy

Q 6. Explain functions of network layer.

Ans. Network layer : Network layer is responsible for the source to destination delivery of packets across multiple networks.



Functions of Network Layer : The various functions of network layer are :

1. Internetworking :

- It provides logical connection between different types of network.
- It provides internetworking between different networks.

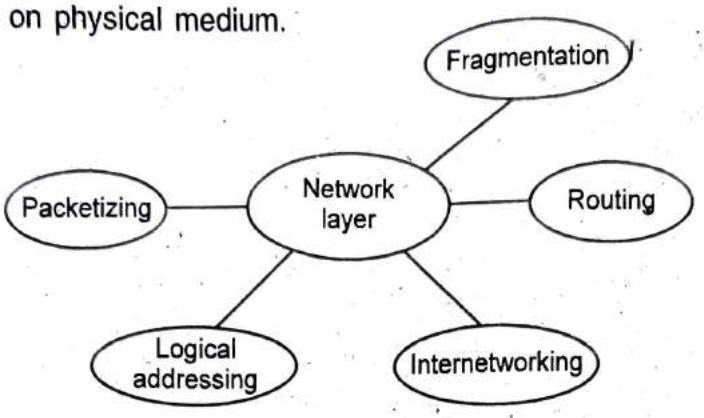
2. Logical addressing : Large number of different networks can be combined together to from bigger networks or internetworks.

3. Routing : When independent networks or links are combined together to create Internet works, multiple routes are possible from source machine to destination machine.

4. Packetizing : The network layer receives the data from the upper layers and creates its own packets by encapsulating these packets.

5. Fragmentation :

- Fragmentation means dividing the larger packets into small fragments.
- Sometimes the size of received packet may be greater than the maximum transportable size on physical medium.



Q 7. Explain flooding. Distinguish between static and alternate routing in a circuit switching network. (PTU, May 2006)

Ans. Flooding : Flooding is a static algorithm in which every incoming packet is sent out an every outgoing line except the line on which it has arrived. One disadvantage of flooding is that it generates a large number of duplicate packets. In fact, it produces infinite number of duplicate packets unless we somehow damp the process.

Static Routing	Alternate Routing
1. Each router maintains routing table indexed by and containing one entry for each router in the subnet.	1. It is advanced version of distance vector routing.
2. Algorithm took too long to converge.	2. Algorithm is faster.
3. Bandwidth is less.	3. Wide bandwidth is available.
4. Router measures delay directly with special echo packets.	4. All delays measured and distributed to every router.
5. It does not take line bandwidth into account when choosing the router.	5. It considers the line bandwidth into account when choosing the router.

Q 8. What is the need of subnet mask? (PTU, May 2011, 2010)

Ans. Subnet mask is needed in order to extract the subnet work address for IP address.

Q 9. Explain adaptive and non-adaptive routing criteria or algorithms.

Ans. Non-adaptive algorithm :

- For this type of algorithms, the routing decision is not based on the measurement estimation of current traffic and topology.

- However, the choice of the route is done in advance, off line and it is downloaded to the routers.
- This is called static routing.

Adaptive routing :

- For these algorithms the routing decisions can be changed if there are any changes in topology or traffic, etc.
- This is called as dynamic routing.

Q 10. What is Internet? **(PTU, Dec. 2006)**

Ans. This was the next stop of ARPANET and NSFNET. The Internet is a globally existing network of networks. Consisting of a huge number of computers situated in all the ports of the world. When limited number of computers are to be interconnected, the local area network (LAN) is used.

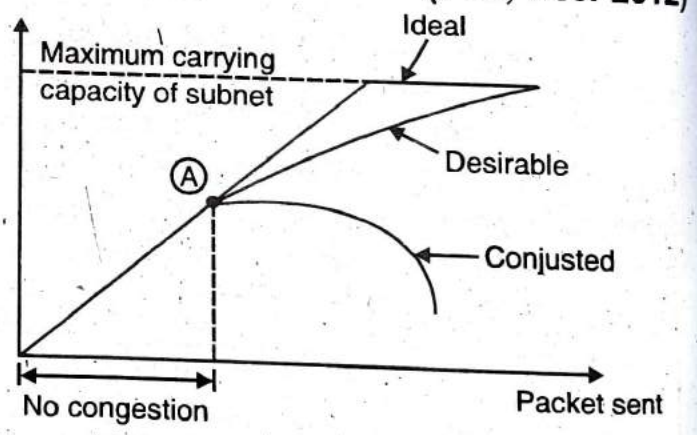
But in the internet the interconnection is achieved even via satellites.

Q 11. Define the term congestion. **(PTU, May 2012 ; Dec. 2009)**

OR

Define the term collision in data communication. **(PTU, Dec. 2012)**

Ans. When too many packets are present in a part of a subnet, the performance degrades. This situation is called as congestion. Congestion in a network may occur when the load on the network i.e. the number of packets sent to the network is greater than the capacity of the network. The fig. shown below explains the concept of congestion graphically.



Upto point (A), the number of packets dumped into the subnet by the host is within its carrying capacity, they are all delivered.

Q 12. Define the term subnet and its need. **(PTU, May 2009 ; Dec. 2006)**

Ans. When the network is split into several smaller networks internally but it acts like a single network to the outside world. This smaller parts of network are called as subnets.

Q 13. Explain any two shortest path routing protocols you have studied. Explain why adaptive routing techniques are superior to non-adaptive routing.

(PTU, May 2008)

Ans. Shortest path routing : This algorithm is based on the simplest and most widely used principle. Here a graph of subnet is built in which each node representing the router and each are representing a link or a communication line. So as to choose a path between a pair of routers, this algorithm simply finds the shortest path between them. There are many algorithms for computing the shortest path between two nodes. One of them is Dijkstra algorithm. The other one is Bellman-Ford algorithm.

Dijkstra's Algorithm : Dijkstra's algorithm is used for computing the shortest path from the root node to every other node in the network. The root node is defined as the node corresponding to the router when the algorithm is being run. The total number of nodes are divided into two groups namely the P group and T group. In the P group we have those nodes for which the shortest path has already been found. In T group the remaining nodes are placed. Every node in the T group should be reached by a path from a node which is already present in group P.

Non-adaptive Algorithms :

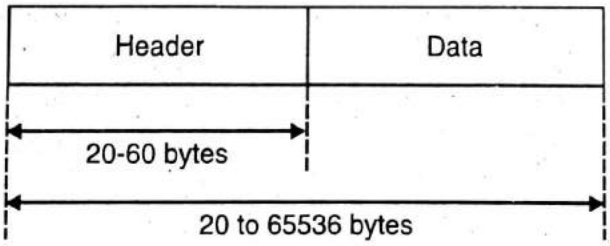
1. For this type of algorithms, the routing decision is not based on the measurement estimation of current traffic and topology.
2. However, the choice of the route is done in advances off line and it is downloaded to the routers.
3. This is called static routing.

Adaptive Algorithms :

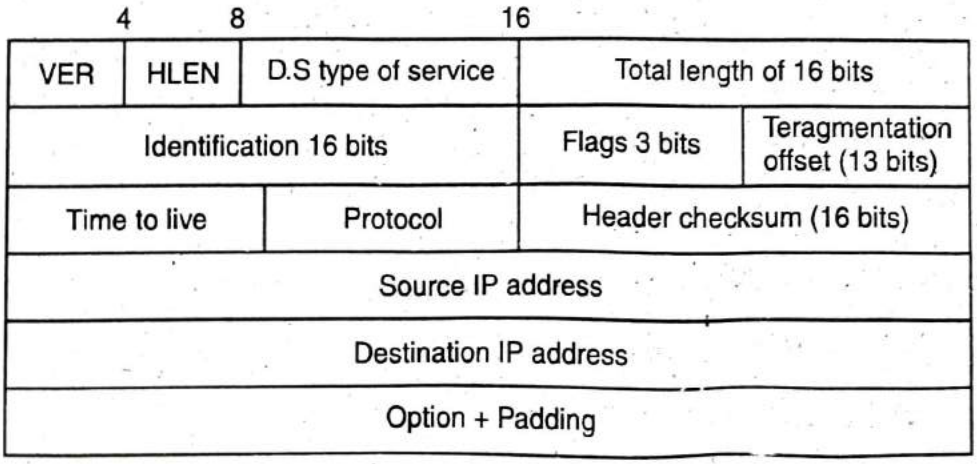
1. For these algorithms the routing decisions can be changed if there are any changes in topology or traffic, etc.
2. This is called as dynamic routing.

Q 14. Draw and discuss the IP diagram frame format. Discuss in detail the various fields. What is subnettng? (PTU, Dec. 2009 ; May 2008)

Ans. IP datagram format is :



Structure of IP header frame is shown below :



IP Header Structure

Various fields in the IP header are as follows :

1. Version (VER) : The field defines the version of IP. Current version of IP is IPV4.

2. Header Length (HLEN) : This field defines the length of the datagram header in 4-byte word. Its value must be multiplied by 4 to give the length in bytes.

3. Differential Services (DS) : This field defines the class of datagram for quality of services purpose.

4. Total Length : This field defines the total length of the IP datagram. The total length includes the length of header as well as data field.

5. Identification : This field identifies the data originating from source host. When a datagram is fragmented, the value in the identification field is copied into all fragments. The identification number helps the destination in reassembling the fragments of the datagram.

6. Flags : It is of three bits. First bit is reserved and it should be 0. Second bit is not fragment bit. If this bit is 1, then machine should not be fragment data. Third bit is "more fragment bit".

7. Fragmentation Offset : This is a 13 bit which shows the relative position of this fragment with respect to the whole diagram.

8. Time to Live : This is an 8 bit long field which controls the maximum number of routers visited by the datagram.

9. Protocol : This field defines the higher-level protocol which uses the services of the IP layer. An IP datagram can encapsulate data from various higher level protocols such as TCP, UDP, ICMP and IGMP.

10. Header Checksum : A checksum in IP packet covers on the header only. Since one header fields changes, this field is recomputed and verified at each point that the internet header is processed.

11. Source Address : This field is used for defining the IP address of the source.

12. Destination Address : This field is used for defining the IP address of the destination.

13. Options : Options are not required for every datagram. They are used for network testing and debugging.

Q 15. Define the concept of routing. **(PTU, May 2004)**

Ans. Routers are devices that connect two or more networks. They consist of a combination of hardware and software.

The software in a router are the operating system and routing protocol. Management software can also be used.

Q 16. Explain open loop control and closed loop control.

Ans. Open loop control : Open loop solutions try to solve the problem by excellent design to prevent the congestion from happening.

Closed loop control : This uses certain feedback which detects the congestion and locates it by monitoring the system.

Q 17. Explain congestion control policy used in different layers.

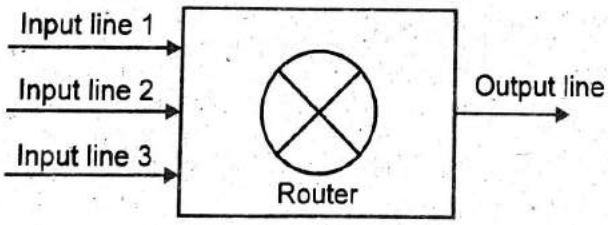
Ans. Different layers of OSI model use dfferent policies or techniques to control the congestion in subnet. The various policies used by data link layer, network layer and transport layer.

Layer	Policies
Data link layer	1. Retransmission policy 2. Out of order policy 3. Acknowledgement policy 4. Flow control policy
Network layer	1. Virtual circuit vs Datagrams include the subnet 2. Packet queueing and service policy 3. Packet discard policy 4. Routing algorithm
Transport layer	1. Transmission policy 2. Out of order caching policy 3. Acknowledgement policy 4. Flow control policy

Q 18. What are the causes of congestion?

Ans. The various causes of congestion in a subnet are :

1. If suddenly, a stream of packet starts arriving on three or four input lines and all need the same output line. In this case a queue will be built up.



If there is insufficient memory to hold all the packets, the packet will be lost.

2. Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table, etc. slowly.

3. Congestion is also caused by slow links. This problem will be solved when high speed links are used. But it is not always the case. Sometimes increases in link bandwidth can further deteriorate the congestion problem as higher speed links may make the network more unbalanced.

4. Congestion can make itself worse. If a router does not have free buffers, it starts ignoring/discarding the newly arriving packets. When these packets are discarded, the sender may retransmit them after timer goes off.

Q 19. Comparison between leaky bucket and token bucket algorithm.
Ans.

Leaky Bucket	Token Bucket
1. Leaky bucket is rigid algorithm as it outputs the data at an average rate and does not support bursty data.	1. Token bucket algorithm is flexible as it enables the bursty data to be sent immediately.
2. It does not credit the idle time of the host i.e. it does not generate tokens.	2. It credits the idle time of the host and accumulates it in form of the tokens.
3. The leaky bucket algorithm discards the incoming packets if the bucket (FIFO queue) is full.	3. The token bucket algorithm throws away tokens if bucket is full. It never discards packets when bucket is full.

Q 20. A class B network has subnet mask of 255.255.240.0. What is the maximum no. of hosts per subnet? **(PTU, May 2005)**

Ans. Let break this binary first

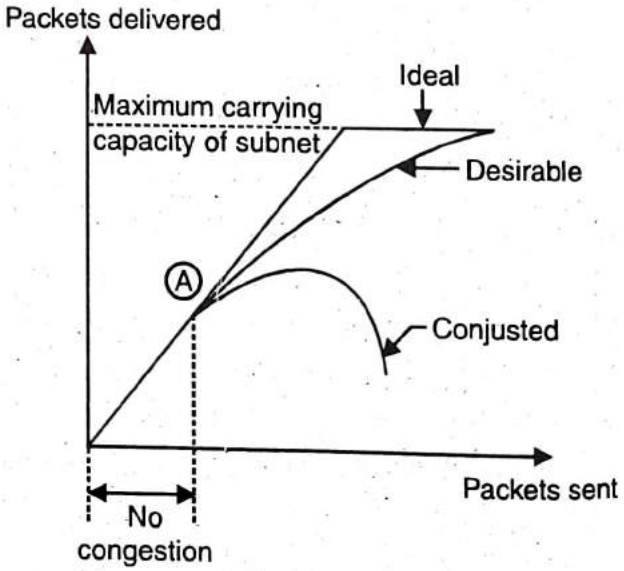
11111111 11111111 11110000 00000000

For a class b network, these are 16 bits available. We see that 4 of those have been borrowed already so we have 12 left.

$$2^{12} - 2 = 4096.$$

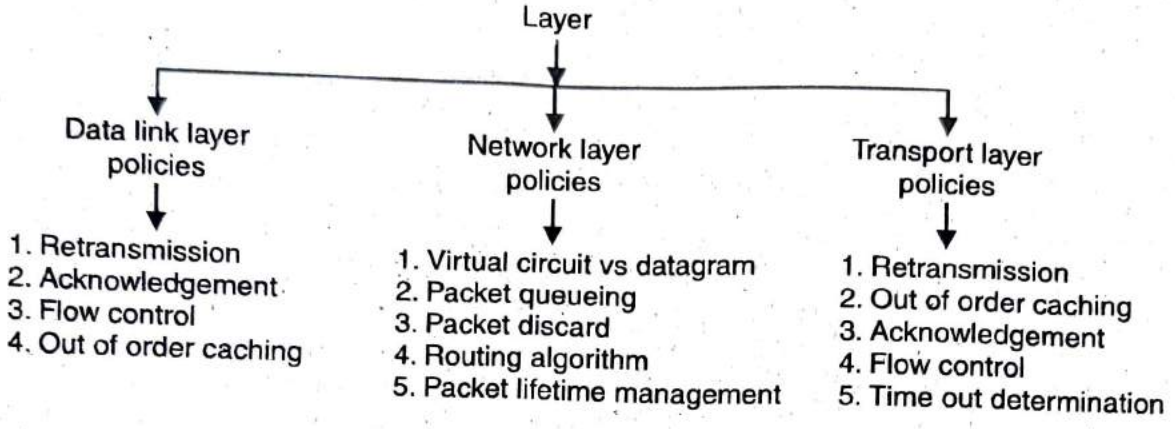
Q 21. Which are the policies that affect the congestion and how it could be prevented? **(PTU, Dec. 2007)**

Ans. Congestion : An important issue in a packet switching network is congestion. When too many packets are present in a part of a subnet, the performance degrades. This situation known as congestion. Congestion in a network may occur when the load on the network i.e. the number of packets sent to the network is greater than the capacity of the network (i.e. the number of packets a network can handle). Fig. explains the concept of congestion graphically. Upto point A in fig. the number of packets dumped into the subnet by the host is within its carrying capacity they are all delivered. In short, the number of packets delivered is proportional to number of packets sent and no congestion takes place. But after point A, the traffic increases too far. The routers cannot cope with the increased traffic and they begin to lose packets.



The congestion begins here. As the traffic increases further, the performance degrades more and more packets are lost and congestion worsens. At very high traffic, the performance collapses completely and almost all packets are lost. This is the worst possible congestion.

Congestion Prevention Policies : In this article, let us discuss the open loop congestion control systems. These systems try to avoid congestion by using the appropriate policies at different levels. Fig. depicts various policies corresponding to different layers for avoiding congestion.

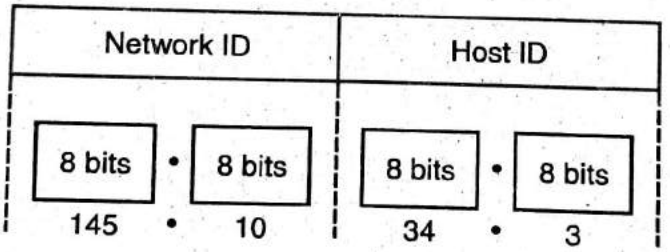


Q 22. What are attributes used for traffic control in frame relay?

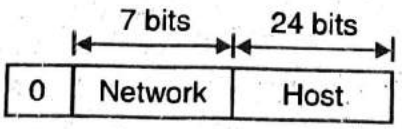
Ans. Attributes used for traffic control in frame relay are higher data rate, less overheads and acknowledgement from the network layer sent in data link layer frames.

Q 23. Write short note on IP addressing. **(PTU, May 2009)**

Ans. IP addressing : An IP address is an internetwork address. It is a universally unique address. Every protocol involved in internetworking requires IP addresses. All IP addresses are 32 bit long and they are used in the source address and destination address fields of IP header. IP address format

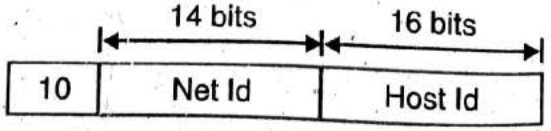


1. Class A Addresses : The format used for IP addresses is shown below :



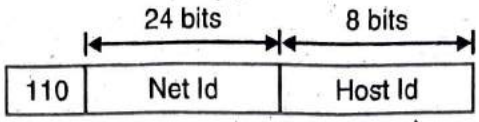
Here net id is 7 bit long and host field is 24 bit long. Host numbers will range from 0.0.0.0 to 127.255.255.255.

2. Class B Addresses : The class B address format is shown below :

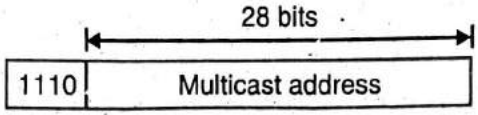


The first block covers the addresses from 128.00.0 to 128.255.255.255 and last block covers from 191.255.0.0 to 191.255.255.255

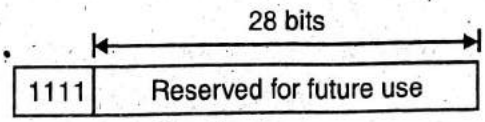
3. Class C Addresses :



4. Class D Address :



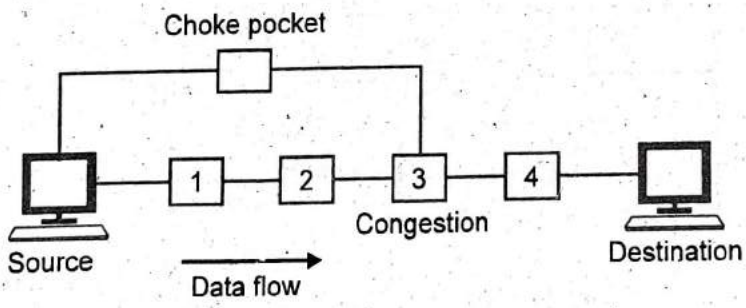
5. Class E Address :



Q 24. What is choke packet?

Ans. in this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.

Here, congested node does not inform its upstream node about the congestion as in back pressure method



Q 25. What is flooding?

Ans. Flooding : This is another static algorithm. In this algorithm, every incoming packet is sent out any every outgoing line except the line on which it has arrived. One disadvantage of flooding is that it generates a large number of duplicate packets. In fact, it produces infinite number of duplicate packets unless the somehow damp the process. There are various damping techniques as under :

(i) Using a hop counter

(ii) To keep a track of which packets have been flooded.

(iii) Selective flooding.

To prevent endless copies of packets circulating indefinitely through the network a hop count may be used to suppress onwards transmission of packets after a number of hops

exceeding the network diameter. The destination must be prepared to receive multiple copies of an incoming packet. Flooding has two interesting characteristics that arise from the fact that all possible routes are tried :

(i) As long as there is a route from source to destination, the delivery of the packet is guaranteed.

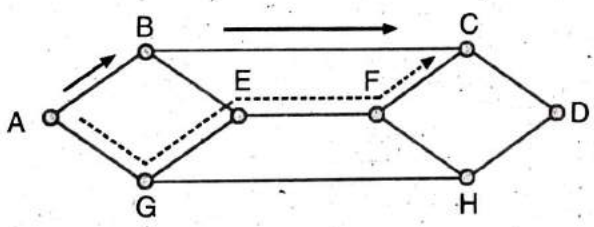
(ii) One copy of the packet will arrive by the quickest possible route.

Selective Flooding : This is slightly more practical variation of flooding. In this algorithm, every incoming packet is not sent out on every output line. In fact, packet is sent only on those lines which are approximately going in the right direction.

Application of Flooding : Flooding does have much practical applications. But, it is useful in military applications where a large number of routers are blown into pieces at any instant. In such applications, robustness of flooding is very much desirable.

Special application is in the distributed database applications. Flooding always chooses the shortest path so it produces the shortest possible delay.

Flow Based Routing : This is a static algorithm which uses topology and load condition (traffic) for deciding a route. For example, in fig. 3, there is always a huge traffic from A to B. Then, the traffic from A to C should not routed through B. Instead route it through AGEFC even though it is a longer path than ABC. This is called as a **flow based routing.** It is possible to optimise the routing by analysing the data flow mathematically. This is possible if the average traffic from one node to the other is known in advance and it is constant in time. The mathematical analysis is based on idea that for a given line if the capacity and average data flow are known, then, it is possible to calculate the mean packet delay using the queueing theory.



Take the route AGEFC instead of ABC

From the mean delays on all the lines, it is possible to calculate the mean packet delay for the whole subnet. To use the technique of flow based routing, the following information should be known in advance :

1. Subnet topology
2. Traffic matrix
3. Line capacity matrix which specifies capacity of each line.

Q 26. Do port address need to be unique? Why and why not? Why are port addresses shorter than IP addresses?

Ans. No, port addresses need not to be unique for different machines, but port addresses should be unique for each application running on same computer system. Whereas IP addresses should always be unique. So port address along with IP address should be unique. In order to identify each application running on each machine. Port addresses are shorter

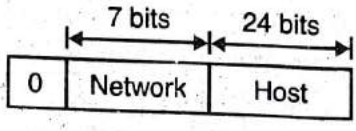
than IP addresses because as there are large address spaces for computer on network so large number of IP addresses exist, whereas port number of computers are limited and much less than number of computers on large network.

Q 27. What is random routing? Explain. **(PTU, May 2006)**

Ans. The modern computer networks normally use the random routing algorithms. Two random routing algorithms namely distance vector routing and link state routing are popular. Both these algorithms are suitable for the packet switched networks. Both these algorithms assume that a router knows the address of each neighbour and the cost of reaching each neighbour.

Q 28. Show by calculation how many hosts per network each IP address class A, B and C can have. **(PTU, May 2008)**

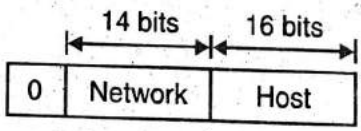
Ans. Class A :



Class A addresses begin with 0_{XXX}, or 1 to 126 decimal. IP addresses with a first octal i.e. octet from 1 to 126 are part of this class. The other three octets are used to identify each host. This means that there is 126 class A network each with 16, 777, 214 possible hosts for a total of 2, 147, 483, 648 unique IP addresses.

Net	Host or Node
115	24.53.107

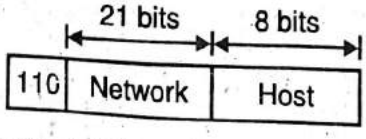
Class B :



Class B addresses begin with 10XX or 128 to 191 decimal. Class B is used for medium sized networks. IP addresses with a first octet from 128 to 191 are port of this class. Class B addresses also include the second octet as port of net ID.

Net	Host or Node
145	24.53.107

Class C :



Class C addresses begin with 110X or 192 to 223 decimal. Class C addresses are commonly used for small to mid size applicatons.

Net	Host or Node
195	24.53.107

Q 29. What is difference between open loop congestion control and closed loop congestion control? **(PTU, May 2007)**

Ans.

Open Loop Congestion Control	Closed Loop Congestion Control
1. Open loop congestion control is based on prevention of congestion.	1. Closed loop congestion control is based on the solution for removing the congestion.
2. It prevents the congestion from happening.	2. It removes the congestion, after it took place.
3. It does not need end-to-end feedback.	3. It adjust its cell-rate depending on some kind of feedback.
4. Open loop control is exercised by using the tools such as deciding when to accept the new packets, when to discard the packets, which packets are to be discarded and making the scheduling decisions at various points.	4. Closed loop control is based on (i) Detect the congestion and locate it by monitoring the system. (ii) Transfer the information about congestion to places where action can be taken. (iii) Adjust the system operations to correct the congestion.
5. E.g. : Prior reservation Hop-to-Hop flow control.	5. E.g. : TCP flow control BR rate control of an ATM network.
6. It has high speed.	6. It is slow speed.
7. It can be classified as : (a) Retransmission policy (b) Window policy (c) Acknowledgement policy (d) Discarding policy (e) Admission policy	7. It can be classified as : (a) Back pressure (b) Choke point (c) Implicit signalling (d) Explicit signalling.

Q 30. What is an IP address and explain about address formats? **(PTU, Dec. 2005)**

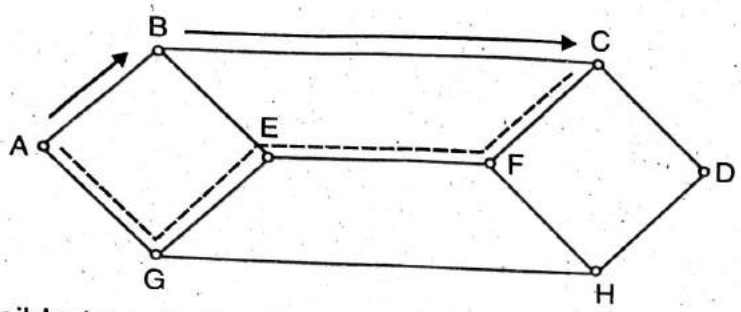
Ans. All the IP addresses are 32 bit long and they are used in the source address and destination address fields of the IP header. An IP address consists of two ports. The first port of the address, called the network number, identifies a network on the internet, the remainder, called the host ID, identifies on individual host on the network.

Address format : IP address format consists of two fields called network ID and host ID. The IP numbers of the hosts are assigned by the network administrator.

Q 31. Compare flow based routing with distance vector routing. **(PTU, May 2007)**

Ans. Flow based routing : This is static algorithm which uses topology and load

conditions for deciding a route. As in fig. there is always a huge traffic from A to B. Then the traffc from A to C should not be routed through B.



Take the route AGEFC instead of ABC

It is possible to optimise the routing by analysing the data flow mathematically. This is possible if the average traffic from one node to the other is known in advance and it is constant in time.

The mathematical analysis is based on idea that for a given line if the capacity and average data flow are known, then it is possible to calculate the mean packet delay using the queueing theory. From the mean delays on all the lines it is possible to calculate the mean packet delay for the whole subnet. To use the technique of flow based routing, the following information should be known in advance :

1. Subnet topology
2. Traffic matrix
3. Line capacity matrix which specifies capacity of each line.

Distance-Vector Routing : In this algorithm, each router maintains a table called vector, such a table gives the best known distance to each destination and the information about which line to be used to reach there. This algorithm is also called as Ford-Fulkerson algorithm and Distributed Bellman-Ford routing algorithm. In distance vector routing, each router maintains a routing table. It contains one entry for each router in the subnet. This entry has two parts :

1. The first part shows the preferred outgoing line to be used to reach the destination.
2. Second part gives an estimate of the time or distance to the destination.

The two fundamental routing algorithm in packet switched network are :

1. Distance vector routing
2. Link state routing.

Both these algorithms assume that a router knows the address of each neighbour and the cost of reaching each neighbour. In the distance routing, a node tells its neighbours about its distance to every other node in the network. Whereas in the link state routing, a node tells every other node in the network its distance to its neighbours.

Q 32. What is internetworking?

Ans. 1. When two or more different networks are connected together to form a bigger network, it is known as Internet of Internetwork.

2. These different networks may be based on different technologies and may use different protocols like TCP/IP, SNA, DECnet, NCP/IPX.

3. Besides protocols, there are several other parameters that differentiate network, for example, packet size, flow control, etc.

Q 33. What is multicast address?

Ans. 1. Class D addresses are called multicast address.

2. The first four bits of first octet in class D are always set to 1, 1, 1, 0.

3. The address range is 224.0.0.0 to 239.255.255.255.

Q 34. What is class A address in IP protocol?

Ans. 1. Class A addresses are designed for large organizatons with a large number of hosts or routers.

2. In this the first octet of the address identifies the network and the next three octets are used to identify the host.

3. The first bit of first octet is always 0 and remaining 7 bits are used to identify the network address.

4. The next three octets i.e. 24 bits are used to identify the host.

5. The class support addresses from 0.0.0.0 to 0.255.255.255.

Q 35. Explain open loop control policies.

Ans. 1. In this method, policies are used to prevent the congestion before it happens.

2. Congestion control is handled either by source or by the destination.

1. Retransmission Policy :

- The sender retransmits a packet, if it feels that the packet A has sent is lost or corrupted.
- However, retransmission in general may increase the congestion in the network. But we need to implement good retransmission policy.

2. Window Policy :

- To implement window policy, selective reject window method is used.
- Selective reject method is preferred over go-back-n window as in Go-back-n method, when timer for a packet times out, several packets are resent.

3. Acknowledgement Policy :

- The acknowledgement policy imposed by the receiver may also affect congestion.
- If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.

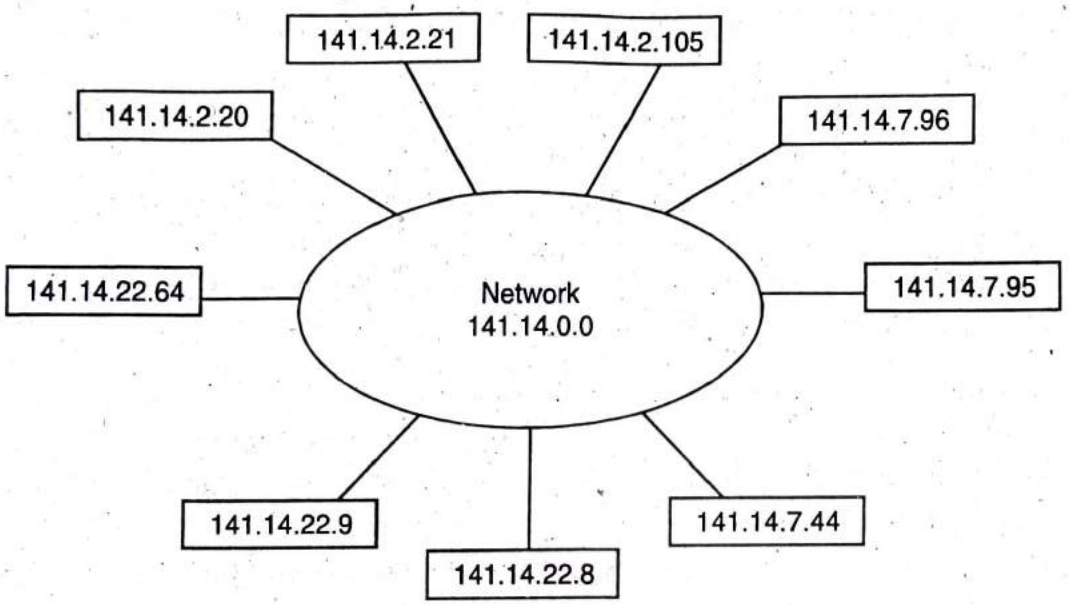
4. Discarding Policy : A router may discard less sensitive packets when a congestion is likely to happen.

5. Admission Policy : An admission policy, which is a quality of service mechanism, can also prevent congestion in virtual circuit networks.

Q 36.What is the role of subnetting? For a given network with 1000 total users, where each set of 256 users have different locations, which class of network and subnetting will be most suitable? (PTU, May 2010)

Ans. As IP address is 32 bit long. One portion of the address indicates a net id and the

other portion indicates the host on the network i.e. host id. This means that there is a sense of hierarchy in IP addressing. To reach a host on the internet, we must first reach the network using the first portion of address i.e. netid. Then we must reach the host itself using the second portion (hostid). In other words, classes A, B and C in IP addressing are designed with two levels of hierarchy. However, in many cases, these two levels of hierarchy are not enough. For example, imagine an organisation with a class B address. The organization has two-level of hierarchy addresses but it cannot have more than one physical network as shown in fig.



With this scheme, the organization is limited to two levels of hierarchy. The hosts cannot be organized into groups and all of the hots are at the same level. The organization has one network with many hosts. One solution to this problem is subnetting, the further division of a network into smaller networks called subnets.

– For 1000 users. with each set of 256 users at different locations.

Total of 1000 addresses are required. As for class C total 256 addresses are available. So we will use 4 blocks of class C each at a one location corresponding to 256 addresses.

Q 37. What is the need of having a different IP address and a MAC address?
(PTU, May 2010)

OR

IP defines how many bits for representing an IP and MAC addresses?
(PTU, May 2011)

Ans. An IP address is an internetwork address whereas the packet from source to destination hosts pass through physical networks. At the physical level the IP address is no useful because the host and routers are recognized by their MAC addresses. A MAC address is a local address. It is unique locally but not universally as IP addresses are.

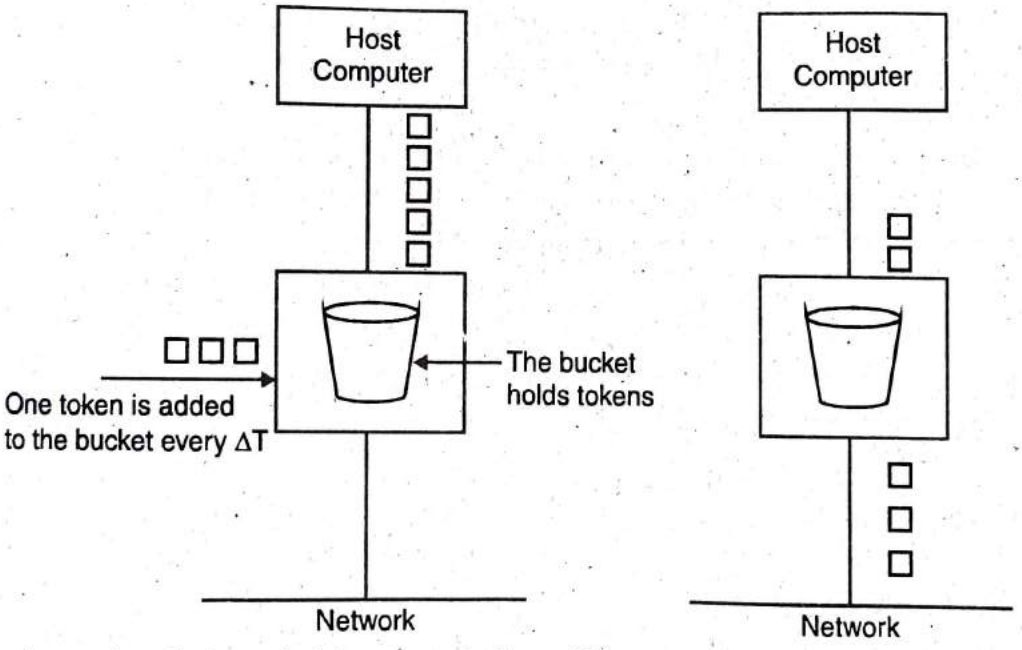
The MAC address and IP address are two different identifiers and both of them are needed, because a physical network can have two different protocols at the network layer at the same time. Similarly, a packet may pass through different physical networks. So as to

deliver packet to a host or a router, we require two levels of addressing namely IP addressing and MAC addressing.

Q 38. Discuss the Token Bucket congestion control algorithm. (PTU, Dec. 2010)

Ans. Token Bucket Algorithm : In case of leaky bucket the output rate is rigidity controlled to same average value, no matter how bursty the traffic is. For some application the data rate of the output should be increased. When large bursts of data arrive at the input, so the token bucket algorithm was developed. It is the modified version of leaky bucket algorithm. A variant on the leaky bucket is the token bucket. The bucket is filled with tokens at a certain rate. A packet must grab and destroy a token to leave the bucket. Packets are never lost, they just have to wait for an available token.

Algorithm : This algorithm is similar to the leaky bucket but it allows for varying output rates. This is useful when large burst of traffic arrives. It enforces a long-term average transmission rate while permitting bounded bursts. In this approach, a token bucket is used to manage the queue regulator that controls the rate of packet flow into the network. A token generator constanlly produces tokens at a rate of R tokens per second and places them into a token bucket with a depth of D tokens.



Assuming that each token grants the ability to transmit a fixed number of bytes, if the token bucket fills, newly generated tokens are discarded.

At the same time, an unregulated stream of packets arrive and are placed into a packet queue that has maximum length of L. If the flow delivers more packets then the queue can store, the excess packets are discarded.

Q 39. Suppose a machine is attached to several physical networks. Why does it need a different IP address for each attachment? (PTU, May 2010)

Ans. Machine attached to several physical networks requires a different IP address for each attachments because IP address are internetwork addresses that universally unique address. So IP address given to one attachment cannot be used by other attachment.

Q 40. Explain various static routing algorithms used by the network layer.
(PTU, Dec. 2010)

Ans. Static Algorithm : The examples of static algorithms may be listed as under :

(i) Shortest path routing

(ii) Flooding

(iii) Flow based routing.

Shortest Path Routing : This algorithm is based on the simplest and most widely used principle. How a graph of subnet is built in which each node representing the router and each arc representing a link or a communication line. Hence, as to choose a path between a pair of routers, the algorithm simply finds the shortest path between them.

Dijkstra's Shortest Path Algorithm : The algorithm translation of physical process is called Dijkstra's shortest path algorithm. The algorithm is based on the following observations:

(a) The distance from ball 1 to ball n cannot decrease after ball n rises from the floor.

(b) Consequently, if we keep track of an estimated distance from ball 1 to ball n, we know that this estimated distance eventually settles to the shortest distance and that this happens when the ball rises from the floor.

1. Now, here how do we know which ball rises next? Say that he ball k rises and let d be the distance from ball 1 to ball k. We update the estimates of the distance from ball 1 to the balls attached to ball k.

2. If some ball j is not jump yet and is attached to ball k with a string of length s, we replace the current estimated distance x from 1 to j by the minimum of x and d + s.

3. When we have updated all the neighbours of ball k, we must find the ball that will rise next. That ball is ball on the floor, say ball p, with the current smallest estimated distance away from ball 1. We can then continue the process with ball p.

4. We find to explain the algorithm on the simple network shown in fig. 1. The objective is to find the shortest path from A to all the other nodes. The lengths of the individual links are marked next to them.

5. On this small network, a simple inspection shows that the shortest path from A to bottom node has length 5 and goes through the right middle node. Dijkstra's algorithm is systematic procedure for discovering such a shorest path even in a large network. Next to each node, we mark the current estimate of the length of the shortest path from A to that node. The symbol ∞ means that the no path to that node has been found yet.

6. The algorithm starts by considering the node with the smallest label, in this case A. The algorithm explores the links going out of that node. The left link leads to the left middle node which can then be reached from A with a path of length 3. Accordingly, we reduce the label of that node from ∞ to 3. Since, the label is reduced by using that left link out of A, we mark the link as being the left middle node.

7. A similar step is performed for the right link out of A. We then shade node A to indicate that we have examined all its outgoing links. At the next step, we examine the unshaded node with the current smallest label. That node is the left middle node. We examine the outgoing link of that node and find a candidate shortest path to the bottom node with length

3 + 3 = 6. We shade that node and then examine the unshaded node with the smallest label; the right middle node.

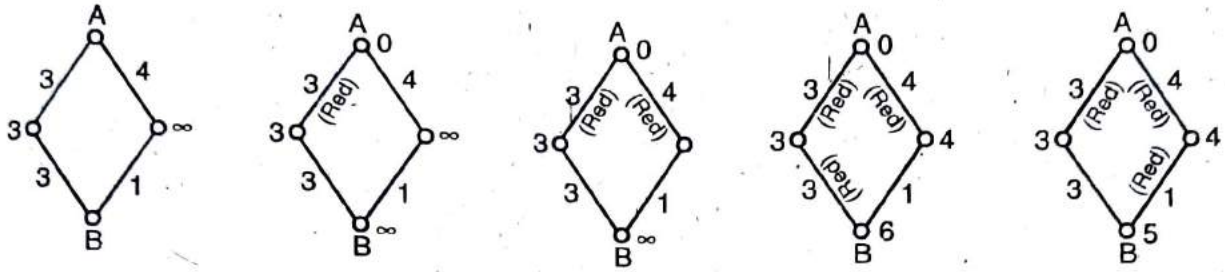


Fig. 1 Steps by Dijkstra's algorithm

8. With the link out of that node, we find a shorest path to the bottom node. Accordingly, we unmark the link from the left middle node to the bottom node because we know that the link is not on the shortest path to the bottom node.

9. In addition, we mark the link from the right middle node to the bottom node. Since the bottom node has no outgoing link, the algorithm terminates. The marked links define the shortest paths from A to the nodes.

10. Next we illustrate Dijkstra's shortest path algorithm with the example shown in fig. 1. We start with node A as the source and we mark each node with an estimated distance from A to the node. The initial estimates are infinite, except that of node A which is 0. The first node to rise from the floor is node A.

11. We shade that node A to remember that it is off the floor and we update the estimates of all the neighbours B, C, D of A. For instance, we replace the current infinite estimate of B by the sum of the estimate of node A (equal to 0) plus the length 4 of the link from A to B.

12. The new estimate (4, 3, 2) are underlined in the second part of the fig. 2. At that point, we determine the unshaded node with the smallest estimate. That node is node D and is, therefore, the next node to rise from the floor. We shade that node D.

Note that all the links from node A to its neighbours are coloured red to remember that these are candidates for shortest paths from A to other nodes since these links have provided us with the smallest estimates of distances to the nodes B, C, D so far.

13. In the third part of the fig. 2, we explore that neighbours of node D and we update their estimates and colour the links from D to these neighbours as red.

14. In the fourth part of the fig. 2, we have located node C as the unshaded node with the smallest estimate ; we shade C and we explore its neighbours and update their estimates.

Note that the link CF produces a smaller estimate (5) for node F. Accordingly, we change the link DF from red to black we colour the link CF as red.

15. In the last part of the fig. 2, we locate the unshaded node B with the smallest estimate; we shade node B and update the estimates of its neighbours. Note that the link from B to D does not reduce the estimate of node D because 4 + 4 > 2. However, the link from B to E reduces the estimate of E because 4 + 1 < 6.

Q 41. Describe the various congestion control algorithms with examples.
(PTU, Dec. 2009 ; May 2012, 2007, 2004)

OR

Explain the working of leaky bucket congestion control algorithm.
(PTU, Dec. 2012)

OR

What is congestion? Exlain the leakly bucket algorithm to control congestion. Explain how the drawbacks of this are overcome in a token bucket algorithm.
(PTU, Dec. 2008)

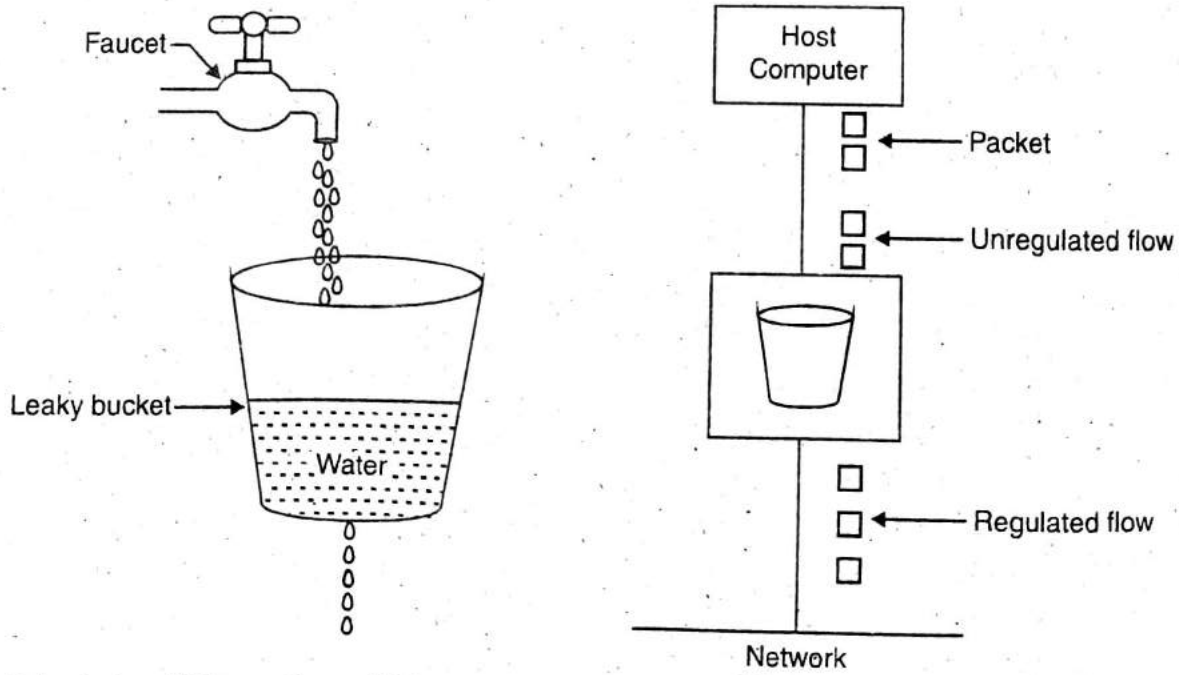
Ans. Congestion Control Algorithm : When too many packets are present in a part of subnet, the performance degrades. This situation is called as congestion. Congestion in a network may occur when the load on the network i.e. the number of packets sent to the network is greater than capacity of the network. The solution to congestion problem can be divided into two categories as :

1. Open Loop Control : Open loop solutions try to solve the problem by excellent design to prevent the congestion from happening.

2. Closed Loop Control : This uses certain feedback which detect the congestion and locate it by monitoring the system.

Congestion control algorithm are of two types :

1. The Leaky Bucket Algorithm : The principle of this algorithm is based on water flow related to leaky bucket as shown in fig. below :

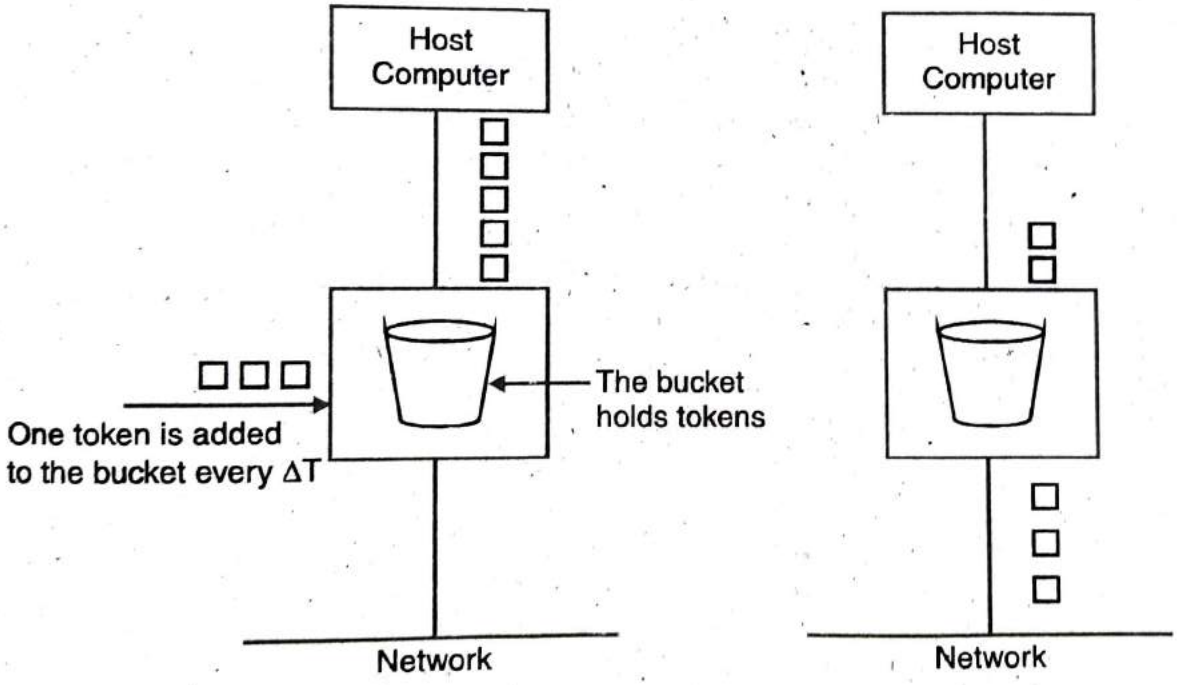


Principle of Operation : Take a bucket with a small hole at its bottom. Irrespective of the rate at which water enters the buckets, the water overflow take place at a constant rate. When there is any water in the bucket and the water outerflow is zero when the bucket is empty. Same technique is applied to control congestion in network traffic. Every host in the network is having a buffer with finite queue length. Packets which are put in the buffer when

buffer is full are thrown away. The buffer may drain onto the subnet either by some numbers of packets per unit time or by some total number of bytes per unit time. This is nothing but a single server queueing system with constant service time.

2. Token Bucket Algorithm : In case of leaky bucket the output rate is rigidly controlled to same average value, no matter how bursty the traffic is. For some applications the data rate of the output should be increased. When large bursts of data arrive at the input. So the token bucket algorithm was developed. It is the modified version of leaky bucket algorithm. A variant on the leaky bucket is the token bucket. The bucket is filled with tokens at a certain rate. A packet must grab and destroy a token to leave the bucket. Packets are never lost, they just have to wait for an available token.

Algorithm : This algorithm is similar to the leaky bucket but it allows for varying output rates. This is useful when large burst of traffic arrive. It enforces a long-term average transmission rate while permitting bounded bursts. In this approach, a token bucket is used to manage the queue regulator that controls the rate of packet flow into the network. A token generator constantly produces tokens at a rate of R tokens per second and places them into a token bucket with a depth of D tokens.



Assuming that each token grants the ability to transmit a fixed number of bytes, if the token bucket fills, newly generated tokens are discarded.

At the same time, an unregulated stream of packets arrive and are placed into a packet queue that has maximum length of L. If the flow delivers more packets than the queue can store, the excess packets are discarded.

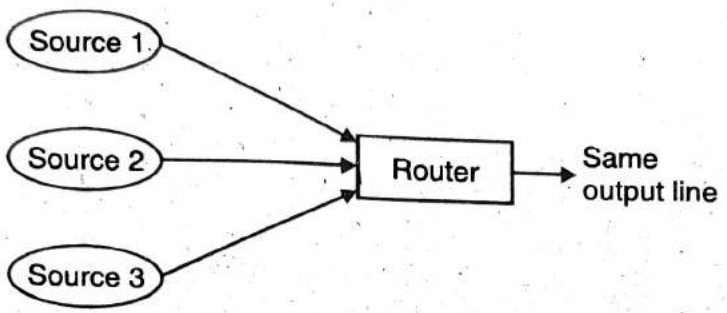
Q 42. Explain the difference causes of congestion in any network. Explain any one congestion control algorithm that can be used for detection and prevention of congestion. **(PTU, May 2010)**

OR

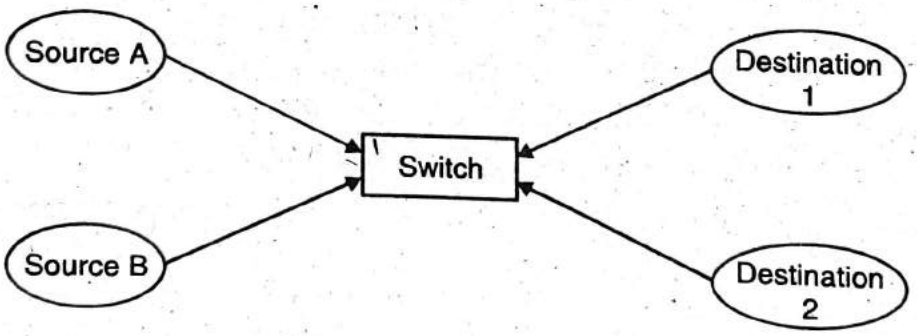
Explain the effect of congestions on the network. Discuss the various congestion control techniques used. **(PTU, May 2006)**

Ans. Causes of Congestion : Some of the causes of congestion are as follows :

1. If suddenly a stream of packets start coming on three or four input lines which all need the same output line. Then a queue will build up. If the memory capacity is not sufficient to hold all these packets, some of them will be lost. This is shown in fig. (a) below :



2. Congestion is caused by slow links. The problem will be solved when high speed links become available. It is not always the case, sometimes increases in link bandwidth can aggravate the congestion problem because higher speed links may make the network more unbalanced. For the configuration showed in fig. (b), if both of two sources begins to send to destination 1 at their peak rate, congestion will occur at the switch. Higher speed links can make the congestion condition in the switch worse.

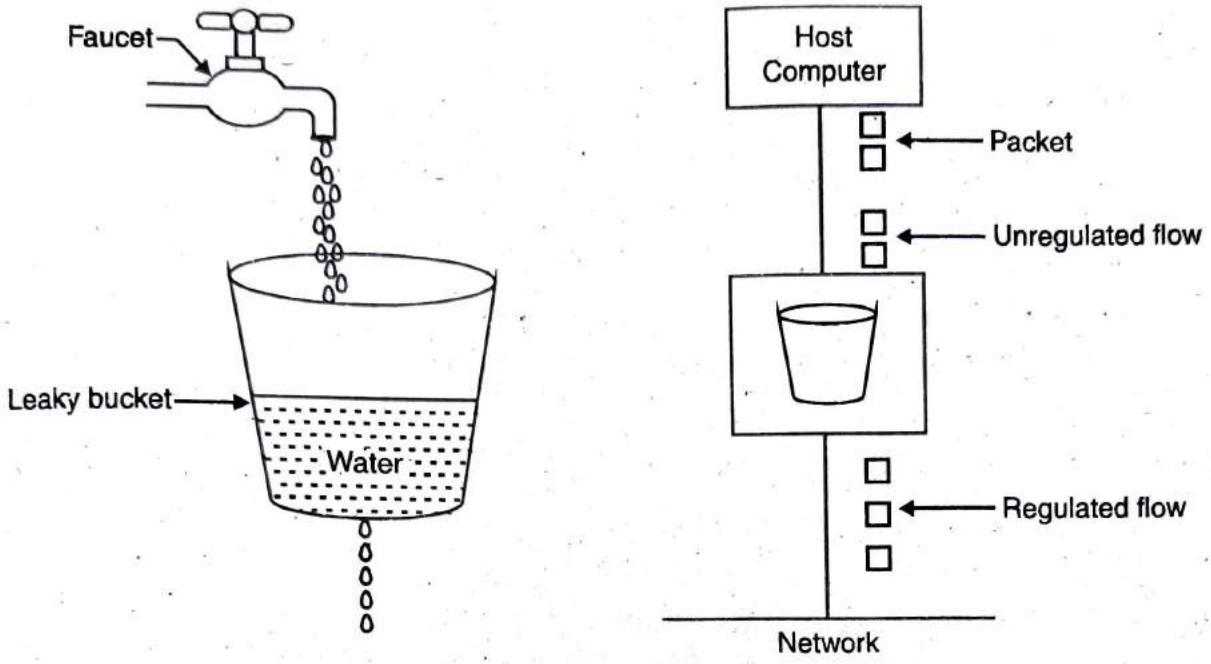


3. Congestion is caused by slow processors. The problem will be solved when processor speed is improved. Faster processors will transmit more data in unit time. If several nodes begin to transmit to one destination simultaneously at their peak rate, the target will be overwhelmed soon.
4. Congestion can make itself worse. But when a packet is discarded, the sender may retransmit it many times because it is not receiving the acknowlegement of the packet. This multiple transmission of packets will force the congestion to take place at the sending end.

The two congestion control algorithms are :

1. Leaky Bucket Algorithm
2. Token Bucket Algorithm.

1. The Leaky Bucket Algorithm : The principle of this algorithm is based on water flow related to leaky bucket as shown in fig. below :



Principle of Operation : Take a bucket with a small hole at its bottom. Irrespective of the rate at which water enters the buckets, the water overflow take place at a constant rate. When there is any water in the bucket and the water outerflow is zero when the bucket is empty. Same technique is applied to control congestion in network traffic. Every host in the network is having a buffer with finite queue length. Packets which are put in the buffer when buffer is full are thrown away. The buffer may drain onto the subnet either by some numbers of packets per unit time or by some total number of bytes per unit time. This is nothing but a single server queueing system with constant service time.

Q 43. How is wired transmission different from wireless transmission?
(PTU, May 2011)

Ans. Wireless transmission : Wireless transmission media sends communication signals by using broadcast radio, cellular radio, microwaves, satellites and infrared signals. Wireless transmission are used when it is inconvinient, impractical or impossible to install wires and cables examples of wireless transmission media include : Broadcast radio, Cellular radio, Microwaves, Communication satellite, Infrared.

Wired transmission : The wired transmission media is used to transfer information over a network such as twisted pair cable. There are many types of transmission media such as coaxial cables, telephone lines etc. Basically any form of wire use to transmit information over a network is considered a wired transmission media.

Q 44. Which fields in an IP header uniquely identifies a connection (when viewed from Network)? **(PTU, May 2011)**

Ans. Each TCP header contains the source and destination port number. These two values, along with the source and destination IP addresses in the IP header, uniquely identify

each connection. The combination of an IP address and a port number is sometimes called an endpoint or socket in the TCP literature.

Q 45. What is port number and what is its significance? **(PTU, Dec. 2011)**

Ans. A port is identified for each address and protocol by a 16-bit number, commonly known as port number. The port number completes the destination address for a communication, eg on a given host or interface UDP and TCP may use the same port number.

Q 46. Answer the following questions based on I.P. addressing scheme used in network layer :

(a) Draw a diagram with network address 8.0.0.0 that is connected through a router to a network with IP address 131.45.0.0. Choose IP address for each interface of the router. Show also some hosts on each network with their IP addresses. What is the class of each network?

(b) What is the sub network address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0

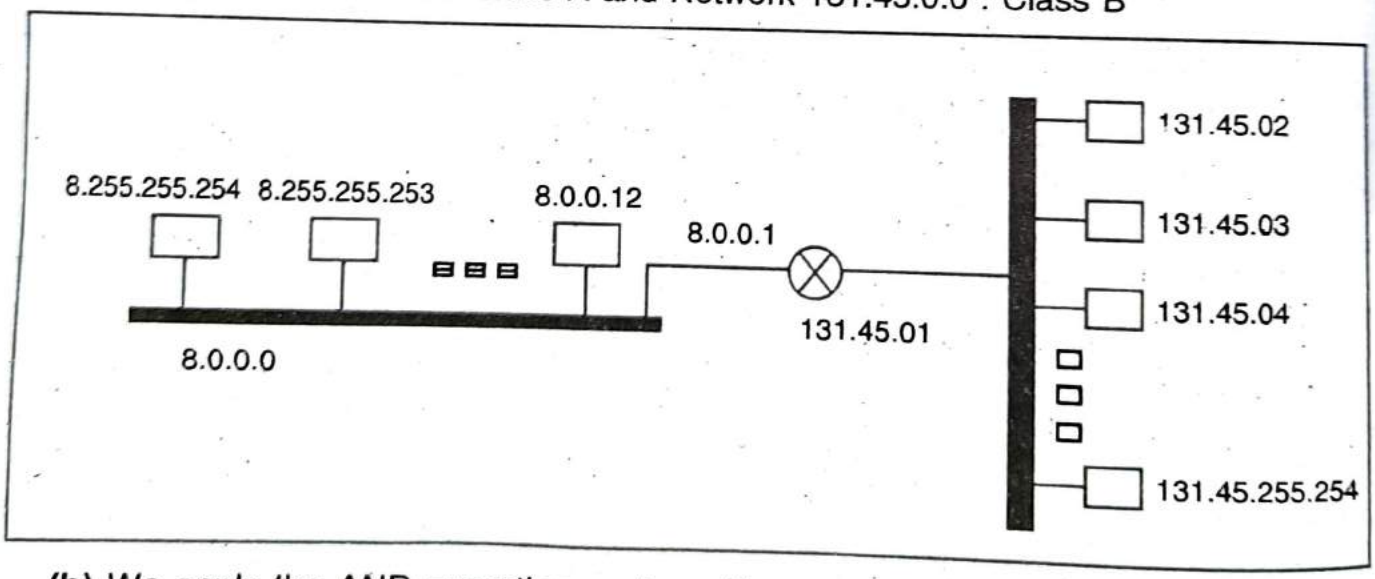
(c) Given the network address 17.0.0.0 find the class, net id, and range of the addresses.

(d) Given the address : 23.56.7.91, find the beginning address (network address).

(e) In the block of addresses, we know the IP address of one the host is 25.34.12.56/16. Find the first address, last address in this block. Also find no of addresses in the block.

(PTU, Dec. 2011)

Ans. (a) Network 8.0.0.0 class A and Network 131.45.0.0 : Class B



(b) We apply the AND operation on the address and the subnet mask.

Address →	11001000	00101101	00100010	00111000
Subnet Mask →	11111111	1111111	11110000	00000000
Subnetwork address →	11001000	00101101	00100000	00000000

The subnet work address is 200.45.32.0.

(c) The class is A because the first byte is between 0 and 127. The block has netid of 17. The addresses range from 17.0.0.0 to 17.255.255.255.

(d) The default mask is 255.0.0.0, which means that only the first byte is preserved and the other 3 bytes are set to 0s. The network address is 23.0.0.0.

(e) IP address is 25.34.12.56/16

So Network Address > 25.34.0.0

Broadcast Address > 25.34.255.255

Subnet Mask > 255.255.0.0

(i) Network address : 25.34.0.0 (set to 0's the host bits, which are the last two octets : 00000000 00000000 >> 0.0)

(ii) Broadcast address : 25.34.255.255 (set to 1's the host bits which are the last two octets : 1111111 11111111 >> 255.255).

Q 47. How is shortest patch found by a static routing algorithm? Which metric is generally considered for deciding routing patch in case of most of the routing algorithms and why? **(PTU, May 2011)**

Ans. Static routing algorithms are hardly algorithms at all, but are table mappings established by the network administrator prior to the begining of routing. These mappings do not change unless the network administor alters them. Algorithms that use static routers are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

Because static routing systems cannot react to network changes. They generally are considered unsuitable for today's large, changing networks. Most of the dominant routing algorithms in the 1990s are dynamic routing algorithms, which adjust to changing network circumstances by analyzing incoming routing update messages. If the message indicate that a network change has occured the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to return their algorithms and change their routing tables accordingly.

Q 48. Which one has more overhead, a bridge or a router? Also explain what is the role of router and bridge in networks. Also differentiate between the two by taking some examples. **(PTU, Dec. 2011)**

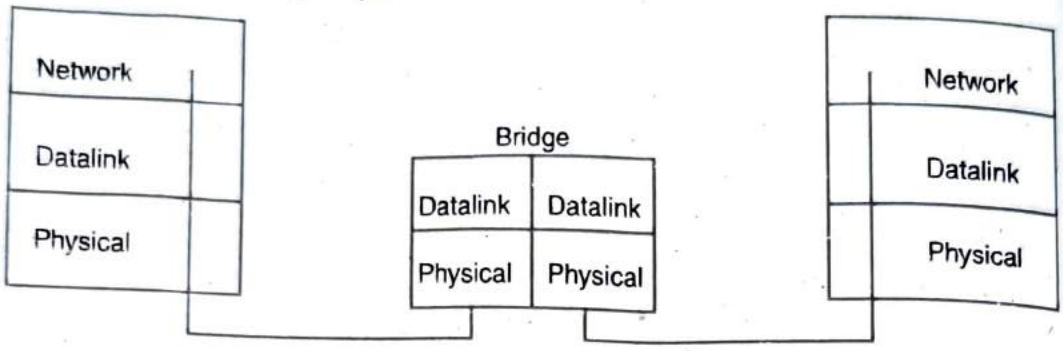
Ans. Bridge : A network bridge connects multiple network segments along data link layer. A bridge works at the data – link level of a network, copying a data frame from one network to the next network along the communications path. The bridge simply does what its name entans by. Connecting two sides from adjacent networks.

In networks, a bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol. A bridge examines each message on a LAN, "passing" those known to be within the same LAN, and forwarding those known to be on the other interconnected LAN or (LANs).

Purpose of a Bridge : The purpose of a bridge are :

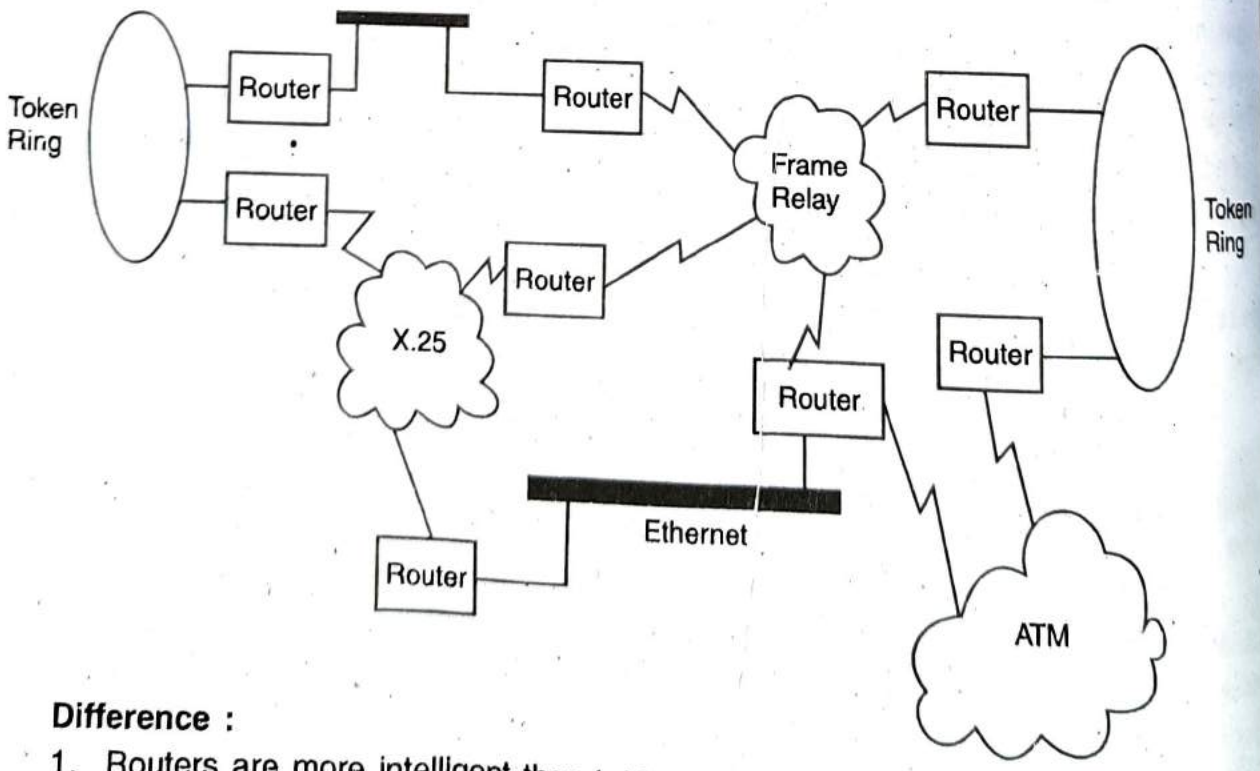
1. Isolates networks by MAC addresses.
2. Manages network traffic by filtering packets.
3. Translates from one protocol to another.

Bridge OSI Operating Layer :



Routers : A router is a device that interconnects networks and decides the best path over which to sent data between networks. Routers use the logical address information contained within ethernet features. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway, including each point of presence on the internet. A router is often included as part of a network switch.

Purpose of Routers : The purpose of a router is to connect nodes across an internetwork regardless of the physical layer and data link layer protocol used. Routers are not aware of the type of medium or frame used. Routers are aware of the network layer protocol used : Novell's IPX, Unix's IP, XNS, Apples DDP, etc.



Difference :

1. Routers are more intelligent than bridges.
2. Routers allow hosts that aren't practically on the same logical network to be able to communicate with each other, while bridges can only connect networks are logically the same.

3. Routers operate at the layer of the OSI model, while bridges are only at the layer 2 (Data link layer).
4. Routers understand and consider IP and IPX address, while bridges do not, and instead they recognize MAC address.
5. Routing is more efficient, and has better call management, than bridging.

Q 49. Differentiate between static and dynamic routing algorithms.

(PTU, May 2012)

Ans. Routing refers to the process of moving packets of information across a network. Static routing manually sets up the optimal path between the source and the destination computers. On the other hand, the dynamic routing uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers. The routers that use the static routing algorithms do not have any controlling mechanism so dynamic are used.

Q 50. What is subnetting? **(PTU, May 2012)**

Ans. A subnetwork, or subnet is a logical visible subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.

Network ID **Host ID**

Traffic between subnetworks is exchanged or routed with special gateways called routers which constitute the logical or physical boundaries between the subnets.

Q 51. How many classes are there for IP4 addresses? **(PTU, May 2012)**

Ans. For Internet protocol version 4 (IPU4), each TCP/IP host is identified by a logical IP address. The IP address is a network layer address and has no dependence on the data link layer address (such as MAC address).

Class	Range	Binary Start
A	0.0.0.0 to 127.255.255.255	0
B	128.0.0.0 to 191.255.255.255	10
C	192.0.0.0 to 223.255.255.255	110
D	224.0.0.0 to 239.255.255.255	1110
E	240.0.0.0 to 247.255.255.255	1111

Q 52. Compare switch and router. **(PTU, Dec. 2012)**

Ans.

Router	Switch
1. It can connect two or more networks.	1. It is a point to point device.
2. It uses hardware and software.	2. It is an intelligent device and can be used as repeator.
3. Used for connecting networks.	3. It uses switching table to find the correct destination.
4. It is less costly.	4. It is more costly.

Q 53. Discuss the design issues of network layer. **(PTU, May 2012)**

Ans. Network Layer : Network layer is responsible for end-to-end transmission.

Design issues of network layer :

1. Services provide to transport layer :

- The network layer provides services to transport layer at network layer/transport layer interface.
- The network layer services are designed to provide following goals :
  (i) The services should be independent of the subnet technology.
  (ii) The transport layer should be shielded from the number, type and topology of the subnets present.

2. Internal organization of the network layer :

- The subnets are organized by using two different approaches :
  (i) Connection oriented (ii) Connectionless.

3. Virtual circuit approach :

- In virtual circuit approach a route from source to destination is choosen.
- The route is choosen during the connection establishment phase.

4. Datagram approach : In datagram approach, no routes are established from source to destination.

Q 54. Explain flooding routing algorithm with example. **(PTU, May 2012)**

Ans. 1. Flooding is the static routing algorithm.

2. In this algorithm, every incoming packet is sent on all outgoing lines except the line on which it has arrived.

3. One major problem of this algorithm is that it generates a large number of duplicate packets on the network.

4. Several measures are taken to stop the duplication of packets :

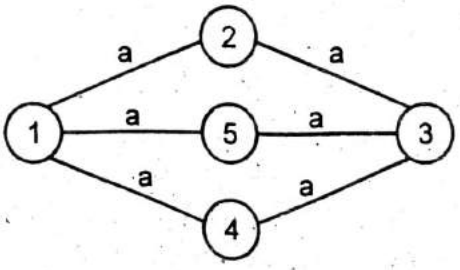
(i) One solution is to include a hop counter in the header of each packet.

(ii) Another technique is to keep the track of the packed that have been flooded, to avoid sending them the second time.

(iii) Another solution is to use selective flooding.

In selecting flooding the routers do not send every incoming packet out on every output line.

e.g.



In that case every one send A from all sides so at destination side flood is created.

❑❑❑

Chapter 6

Transport Layer

Contents

Elements of transport protocols : addressing, connection establishment and release, flow control and buffering, multiplexing and de-multiplexing, crash recovery, introduction to TCP/UDP protocols and their comparison.

POINTS TO REMEMBER

- The data link and transport layers perform many of the same duties. The data link layer functions in a single network, while the transport layer operates across an internet.
- The transport protocol data unit (TPDU) format consists of four fields :
  (a) Length
  (b) Fixed parameters
  (c) Variable parameters
  (d) Data
- The five types of transport classes are based on the reliability of the lower layers. Class TPU is similar to TCP in the TLP/IP suite.
- The transport layer provides two services types :
  (a) Connection-oriented transport service
  (b) Connectionless transport services.
- The transport layer is responsible for end-to-end delivery, segmentations and concatenation.
- Connection establishment and termination are both accomplished through three-way handshakes.
- Flow control at the transport level is handled by a three-walped sliding window.
- Transport layer provides node to node delivery of packets i.e. segments.
- The transport layer needs ports or service access points.
- Reliable delivery requires error control, sequence control, loss control, etc.
- In order to deliver the message from one process to another, an addressing scheme is required.
- The transport layer segments user data into smaller units and attaches a transport layer header to each unit.

- The transport layer also handles congestion.
- Transport layer provides end to end error control facility.
- A socket address is a combination of IP address and port number.
- Elements of transport layer
  (a) Addressing
  (b) Port numbers
  (c) Socket address
  (d) Multiplexing and demultiplexing.
- Ports are assigned to each communicating device.
- Flow control is performed end to end rather than across a single link.
- The UDP (user datagram protocol) is one of the core members of the Internet protocol suite, the set of network protocols used for the internet.
- Traffic shaping is also known as packet shaping. It is an attempt to control computer network traffic in order to optimize or gurantee performance.
- The transmission control protocol is one of the core protocols of the internet protocol suite.

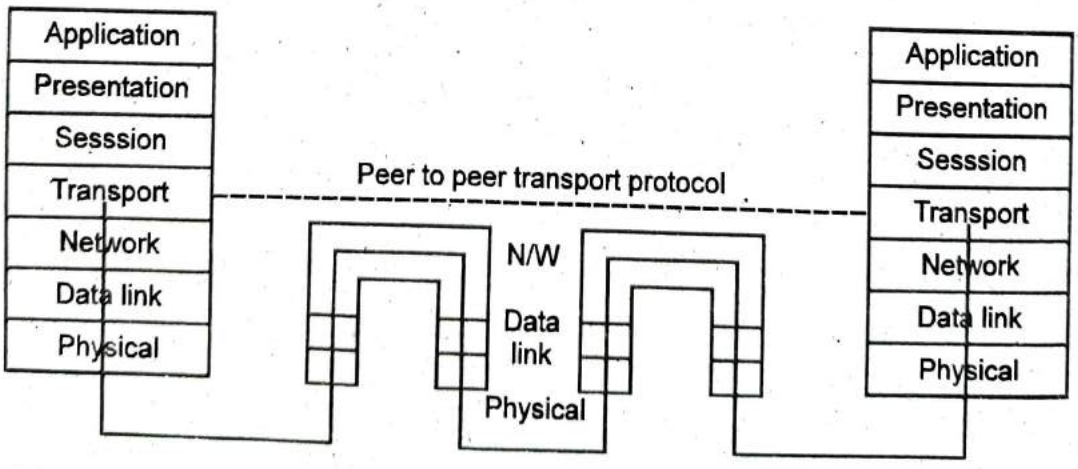
QUESTION-ANSWERS

Q 1. Explain transport layer.

Ans. 1. The transport layer is the fourth layer from the bottom in the OSI reference model.

2. Transport layer lies above the network layer in an end system.

3. While the network layer and the other lower layer resides in all the end systems and intermediate systems, the transport layer is implemented only in the end systems.



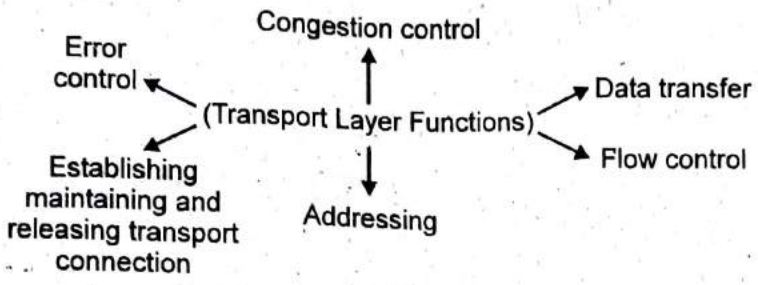
4. The interactions between peer transport layer entities are, therefore, end to end and these are made possible by the data transfer service provided by the network layer.

5. The network layer is responsible for host to host delivery and data link layer is responsible for node to node delivery of frames.

6. It is responsible for process to process delivery of message.

Q 2. Explain transport layer design issue.

Ans. The transport layer delivers the message from one process to another process running on two different hosts. Thus, it has to perform number of functions or duties to ensure the delivery of message.



1. Establishing, maintaining and releasing transport connection :

- The transport layer establishes, maintains and releases end to end transport connection on the request of the upper layers.

2. Addressing :

- In order to deliver the message from one process to another, an addressing scheme is required.
- Each communicating process has a specific port number.

3. Data transfer : The transport layer segments user data into smaller units and attaches a transport layer header to each unit forming a TPDU (Transport layer data unit).

4. Flow control :

- Like data link layer, transport layer also performs flow control.
- However, the flow control at transport layer is performed end to end rather than across a single link.

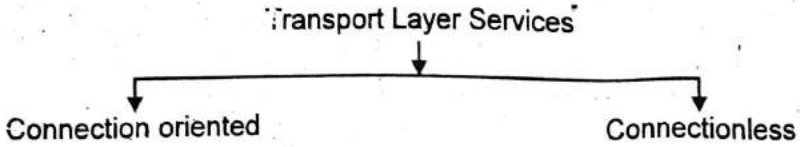
5. Error control :

- Transport layer provides end to end error control facility.
- Transport layer has a built in error control checksum mechanism that detects and corrects errors by retransmission of transport data units.

6. Congestion control : The transport layer also handles congestion in the subnets that are using datagram service internally.

Q 3. Explain transport layer services. **(PTU, Dec. 2005)**

Ans. A transport layer protocols can provide two types of services.



1. Connecton oriented service :

(i) In connection oriented services, a connection is first established between a sender and the receiver.

(ii) Then, transfer of the user data units takes place on this connection.

(iii) At the end, the connection is released.

2. Connectionless services :

(i) In this service the packets are sent from sender to receiver without the establishment or release of connection.

(ii) In such a service, packers are not numbered.

(iii) The packets may be lost, corrupted, delayed or disordered.

(iv) The transport layer protocol that provides this service is UDP.

Q 4. What is port number?

Ans. 1. Each communicating process is assigned a specific port number.

2. In order to choose among multiple processes running on the destination host, a port number of destination process is needed.

3. The port numbers are 16 bit integers between 0 and 65535.

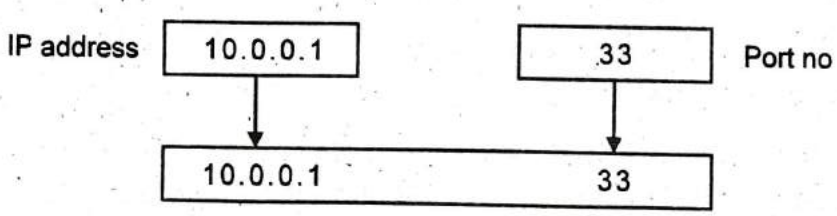
4. Port numbers are assigned by Internet Assigned Number Authority (IANA).

- **Well known ports :** The ports ranging from 0 to 1023.
- **Registered ports :** 1024 to 49,151.
- **Dynamic ports :** The ports ranging from 49,152 to 65535.

Q 5. What is socket address?

Ans. 1. A socket address is a combination of IP address and port number.

2. In order to provide communication between two different processes on different host, we need both the IP address as well as port address i.e. socket address.



Socket address

3. The client socket address defines the client process uniquely and the server socket address defines the server process uniquely.

Q 6. Define the elements of transport layer.

Ans. Transport layer guarantees process to process delivery of messages :

1. Addressing
2. Port numbers
3. Socket address
4. Multiplexing and demultiplexing.

Q 7. Explain flow control.

Ans. Like data link layer, transport layer also performs flow control. The flow control at transport layer is performed end to end rather than across a single link.

Flow control means when server sends data at fast speed but receiver does not get it at exact speed, it means that receiver speed is slow so flow control is required.

Q 8. Differentiate between TCP and UDP. (PTU, Dec. 2010 ; May 2011, 2006)

OR

How TCP is different from UDP? Which of the two protocols is more favourable for real time applications and why? (PTU, Dec. 2012 ; May 2005)

Ans. Difference between TCP and UDP :

TCP	UDP
1. TCP stands for transmission control protocol.	1. UDP stands for user datagram protocol.
2. It provides reliable, connection oriented services.	2. It provides unreliable connectionless services.
3. It offers error control and flow control facilities.	3. It does not offer error control and flow control.
4. TCP is used in those applications where we want to ensure accurate data delivery.	4. UDP is used for those applications that require prompt delivery.
5. TCP connection is byte stream.	5. UDP connection is message stream.
6. TCP packet is called segment.	6. UDP packet is called user datagram.

Real application protocols are :

Protocol	Full Form
Telnet	Terminal Network
SMTP	Simple Mail Transfer Protocol
FTP	File Transfer Protocol
DNS	Domain Name Server
HTTP	Hyper Text Transfer Protocol
NNTP	Network News Transfer Protocol

Q 9. Many of the duties of transport layer are also performed by data link layer. Is this a duplication or not, how? (PTU, Dec. 2004)

Ans. Some of the duties of transport layer are also performed by the data link layer, but this is not duplication. Such duties are as below :

1. Flow control : We know that data link layer can provide the flow control. Similarly, transport layer also can provide flow control. But this flow control is performed end to end rather than across a single link.

2. Error control : The transport layer can provide error control as well. But error control at transport layer is performed end to end rather than across a single link.

3. Congestion control : The congestion can take place in data link or network or transport layer.

4. Quality of services : Quality of service can be implemented in other layers but its actual effect is felt in the transport layer.

Q 10. What is UDP? **(PTU, Dec. 2006)**

Ans. The user datagram protocol **UDP** is one of the core members of the Internet protocol suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to datagrams, to other hosts on an internet protocol network without requiring prior communications to set up special transmission channels or data paths.

UDP uses a simple transmission model without implicit hand shocking, dialogues for providing reliability, ordering or data integrity.

Q 11. Are both UDP and IP unreliable to the same degree? Why or why not? **(PTU, Dec. 2007)**

Ans. User Datagram Protocol : The User Datagram Protocol is a very simple protocol. It adds little to the basic functionality of IP. Like IP, it is an unreliable, connectionless protocol. You do not need to establish a connection with a host before exchanging data with it using UDP, and there is no mechanism for ensuring that data sent is received. A unit of data sent using UDP is called a Datagram. UDP adds four 16-bit header fields (8 bytes) to whatever data is sent. These fields are : a length field, a checksum field and source and destination port numbers. Port number, in this context, represents a software port, not a hardware port. The concept of port number is common to both UDP and TCP. The port numbers identify which protocol module sent (or is to receive) the data. Most protocols have standard ports that are generally used for this. For example, the Telnet protocol generally uses port 23. The Simple Mail Transfer Protocol (SMTP) uses port 25. The use of standard port numbers make it possible for clients to communicate with a server without first having to establish which port to use. The port number and the protocol field in the IP header duplicate each other to some extent through the protocol field is not available to the higher level protocols. IP uses the protocol field to determine whether data should be passed to the UDP or TCP module.

UDP or TCP use the port number to determine which application protocol should receive the data. Although UDP is not reliable, it is still an appropriate choice for many applications. It is used in real-time applications like. Net audio and video where, if data is lost, it is better to do without it than send it again out of sequence. It is also used by protocols like the Simple Network Management Protocol (SNMP).

Purpose of UDP : User Datagram Protocol (UDP) provides a connectionless packet service that offers unreliable best effort delivery. This means that the arrival of packets is not guaranteed, nor is the correct sequencing of delivered packets. Applications that do not require an acknowledgement of receipt of data, for example, audio or video broadcasting uses UDP. UDP is also used by applications that typically trasnmit small amounts of data at one time, for example, the Simple

Source port	Destination port
Length	UDP checksum
Data	

Network Management Protocol (SNMP). UDP provides mechanism that application programs use to send data to other application programs. UDP provides protocol port numbers used to distinguish between multiple programs executing on a single device. That is, in addition to the data sent, each UDP message contains both a destination port number and a source port number. This makes it possible for the UDP software at the destination to deliver the message to the correct application program and for the application program to send a reply.

The UDP header is divided into the following four 16-bit fields :

1. Source Port : Source port is an optional field when meaningful, it indicates the port of the sending process and may be assumed to be port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

2. Destination Port : Destination port has a meaning within the context of a particular Internet destination address.

3. Length : This is the size in bytes of the UDP packet, including the header and data. The minimum length is 8 bytes, the length of the header alone.

4. UDP Checksum : This is used to verify the integrity of the UDP header. The checksum is performed on a psuedo header consisting of information obtained from the IP header (source and destination address) as well as the UDP header.

Q 12. Name various application services of TCP/IP. **(PTU, Dec. 2004)**

Ans. The various application services of TCP/IP are :

1. The application layer provides services that can be used by other applications. In the application layer some of the important protocols are simple mail transfer protocol (SMTP), file transfer protocol FTP and Telnet.

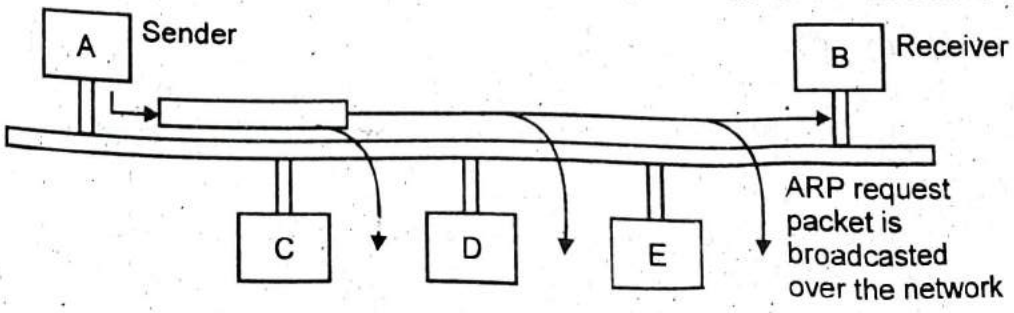
2. The SMTP provides a basic e-mail facility. The FTP is used to send files from one system to another system under user common.

Q 13. How does address resolution take place at the transport layer? Why is name resolution important? **(PTU, May 2010)**

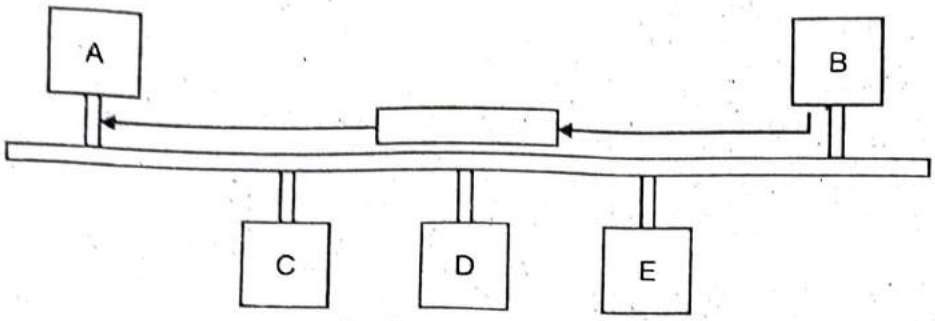
Ans. Address resolution is used for finding or resolving the MAC address from IP address. For a LAN each device has its own physical or station address as its identification. This address is imprinted on the NIC.

When a router or a host needs to find the MAC address of another host or network the sequence of even taking place is as follow :

1. The router or host A who wants to find the MAC address of some other router, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver B.
2. This request packet is broadcast over the network as shown below :



Every host and router on the network receives and processes the ARP request packet. But only the intended receiver (B) recognizes its IP address in the request packet and sends back an ARP response packet. The ARP response packet contains the IP and physical addresses of the receiver (B). This packet is delivered only to A using A's physical address in the ARP request packet. This is shown in fig.



ARP Response Unicast

Q 14. What is TCP? **(PTU, Dec. 2006)**

Ans. The transmission control protocol is one of the core protocols of the Internet protocol suite. TCP is one of the two original components of the suite, complementing the Internet protocol and, therefore, the entire suits is commonly referred to as TCP/IP. TCP provides the service of exchanging data directly between two network hosts, whereas IP handles addressing and routing message across one or more networks. In particular, TCP provides reliability, ordered delivery of stream of bytes from a program one computer to another programs at another computer.

Q 15. Explain the difference between connectionless unacknowledged service and connectionless acknowledged service. How do the protocols that provide these services differ? **(PTU, Dec. 2008)**

Ans. Connectionless service provides single free standing data unit for all transmissions. Each unit contains all of the protocols control information necessary for delivery but contains no provision for sequencing or flow control.

Q 16. List two important functions performed by transport layer.

Ans. The two important functions performed by transport layer :

1. This allows the peer entities of the source and destination machines to converse with each other.

2. TCP also handles the flow control.

Q 17. What is traffic shaping? **(PTU, May 2007)**

Ans. Traffic shaping is also known as packet shaping. It is an attempt to control computer network traffic in order to optimize or guarantee performance, low latency, and/or bandwidth of delaying packets.

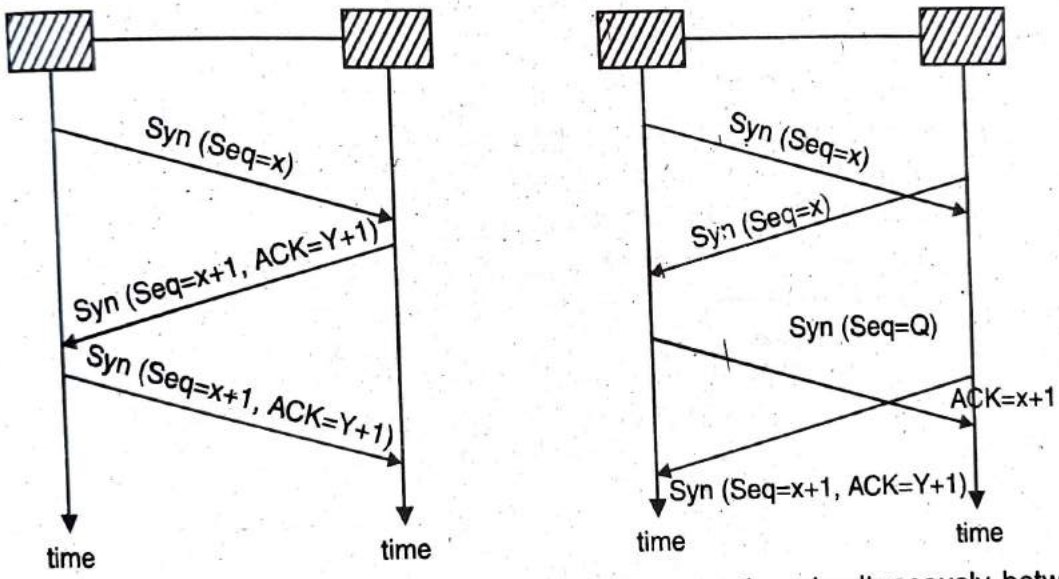
Traffic shaping is any action on a set of packets which imposes additional delay on those packets such that they conform to some predetermined constraint. Traffic shaping

provides a means to control the value of traffic being sent into a n/w in a specified period, or the maximum rate at which the traffic is sent or more complex criteria such as GCRA. This control can be accomplished in many ways and for many reasons : however, traffic shaping is always by delaying packets. Traffic shaping is commonly applied at the network edges to control traffic entering or by an element in the network.

Q 18. Explain how the connection is managed in transport layer.

(PTU, May 2004)

Ans. Connections are established in transport layer using three way handshake mechanism. To establish a connection, one side, say the server, passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, either specifying a particular other side or nobody in particular. The other side executes a connect primitive, specifying the IP and port to which it wants to connect, the maximum TCP segment size, possible other options and optionally some user data. The connect primitive sends a TCP segment with the synchronous bit on and the ACK bit off and waits for a response.



Call collision : If two hosts try to establish a connection simultaneously between the same two sockets then the sequence of events. Under such circumstances only one connection is established.

Q 19. What is the use of flags in a TCP header? **(PTU, May 2010)**

Ans. In TCP header there are six flags explained below :

1. Urgent Pointer (URG) : If this bit field is set, the receiving TCP should interpret the urgent pointer field.

2. Acknowledgement (ACK) : If this bit field is set, the acknowledgement field described earlier is valid.

3. Push Function (PSH) : If this bit field is set, the receiver should deliver this segment to the receiving application as soon as possible.

4. Reset the Connection (RST) : If this bit is present, it signals the receiver that the

sender is aborting the connection and all queued data and allocated buffers for the connection can be freely relinguished.

5. Synchronize (SYN) : When present, this bit field signifies that sender is attempting to "synchronize" sequence numbers. This bit is used during the initial stages of connection establishment between a sender and a receiver.

6. No More Data From Sender (FIN) : If set, this bit field tells the receiver that the sender has reached the end of its byte stream for the current TCP connection.

Q 20. Explain the format of TCP segment.

OR

Explain the meaning of various fields of the TCP header with example.

(PTU, May 2012)

Ans. 1. TCP segment is the unit of data transferred between two processes that uses TCP.

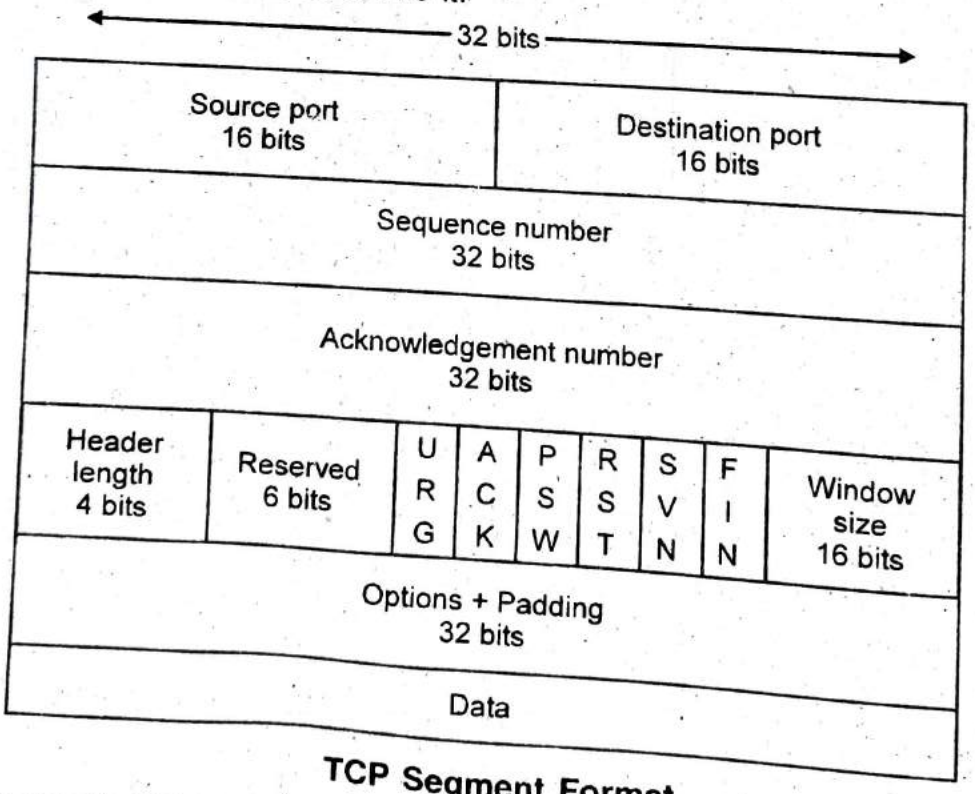
2. Each TCP segment consists of two parts : header part and data part.

3. A TCP header can be of 20 to 60 bytes. If it does not contain options, it is of 20 bytes only.

4. The size of TCP segment is decided by TCP software.

5. There are two factors that decide segment size :

- The payload field of IP packet is just 65,515 byte and each segment should be smaller than this size to fit into it.



TCP Segment Format

1. Source port : This field is of 2 bytes. It indicates the port number of a source process.

2. Destination port : This field is also of 2 bytes and specifies the port number of destination process or receiving process.

3. Sequence number : This field is of 32 bits or 4 bytes. It specifies the number assigned to the first byte of data in the current message.

4. Acknowledgement number : This field is of 32 bits or 4 bytes. This field is the piggybacked acknowledgement of all the previous data bytes.

5. Header length : It is a 4 bit field that indicates the number of 32 bit words in the TCP headers.

6. Reserved : This 6 bit field is reserved for future use.

7. Flags : This 6 bit field consists of 6 different flags.

UGR	Urgent pointer
ACK	Acknowledgement
PSH	Request for PUSH
RST	Reset the connection
SYN	Synchronize
FIN	Final or Terminate the connection

8. Window size : This 2 byte field specifies the size of sender's receive window.

9. TCP checksum : This 16 bit field contains the checksum.

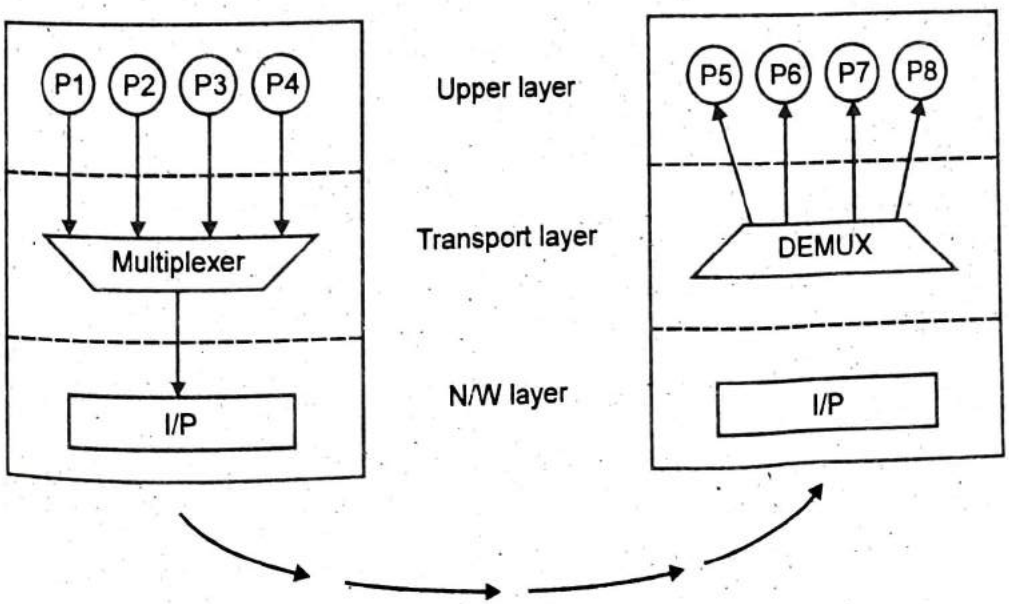
10. Urgent pointer : This 16 bit field is valid only if urgent pointer is set to 1. The value contained in this field is added to the value contained in sequence number field to obtain the number field to obtain the number of last urgent byte in the data section of the segment.

Q 21. What is multiplexing and demultiplexing?

Ans. 1. When there are several running applications that want to send packets and only one transport layer connection, then transport layer protocols may perform multiplexing.

2. The protocol accepts the message from different processes having their respective port numbers and add headers to them.

3. Then these packets are passed to n/w layer.



4. The transport layer at the receiver end performs demultiplexing to separate the messages for different processes that are coming on a single connection.

Q 22. What is multiplexing at transport layer? **(PTU, May 2012)**

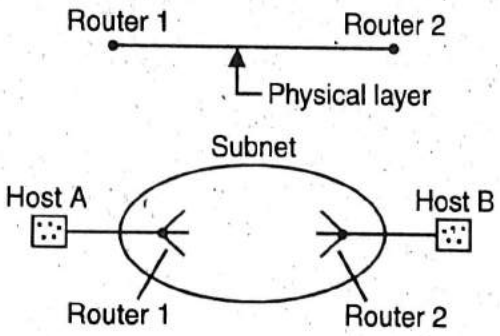
Ans. One basic function of transport layer is multiplexing and demultiplexing. Usually there are multiple application processes running on one host for example, a computer may be sending several files generated by filling in web forms, while at the same time sending e-mails. The network layer only cares about sending a stream of data out of the computer. Therefore, the transport layer needs to aggregate data from different applications into a single stream before passing it to the network layer.

Q 23. Discuss elements of transport protocols. **(PTU, Dec. 2010 ; May 2006)**

Ans. In order to implement the transport layer services between the two transport entities. We have to use a transport protocol. The transport protocols have to deal with the following tasks.

1. Error Control
2. Sequencing
3. Flow Control.

The transport protocols are similar to the data link protocols in many ways but there are some dissimilarities as well. At the data link layer two router communicate directly via a physical connection as shown :

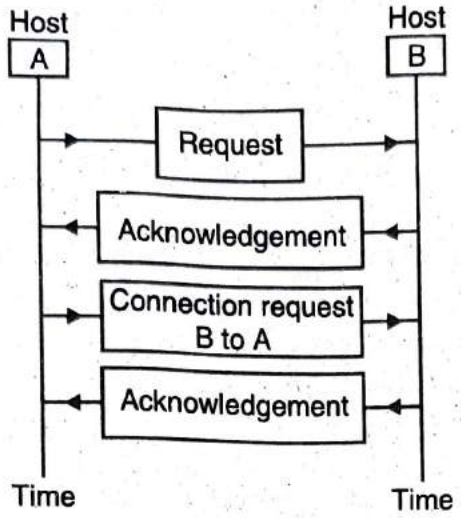


Router Connection at Transport Layer

Elements of Transport Protocols :

1. Addressing
2. Establishing a connection
3. Releasing a connection
4. Flow control and buffering
5. Multiplexing
6. Crash recovery.

At a very first step a transport address is to be defined. This is an address to which processes can listen for connection requests. Process to process delivery needs two identifiers one is IP address and other is port number after addressing a connection is established between source and destination. Then the data is transferred and at the end connection is released.



For flow control, a sliding window is needed on which connection to keep a fast transmitted from a slow receiver. The addressing mechanism allows multiplexing and demultiplexing. At the sending end, there are several processes that want to send packets. But there is only one transport layer protocol (UDP or TCP). At the receiving and, the demultiplexer done the opposite job of that of a multiplexer. The host and routers are subject to crashes and the recovery from such crashes is essential. Such crashes will result in loss of packets.

Q 24. Explain in detail the design issues of transport layer protocols.

(PTU, Dec. 2009 ; May 2009)

Ans. The transport layer is next to the network layer in OSI reference model from bottom. The transport layer provides a high level of control for moving information between systems, including more sophisticated error handling, prioritization and security features. The transport layer provides quality service and accurate delivery by providing connection-oriented services between two and systems. If control the sequence of packets, regulates traffic flow and recognizes duplicate packets. The transport layer assign packetized information a traffic number that is checked at the destination. If data is missing from the packet, the transport layer protocol at the receiving end arranges with the transport layer of the sending system to have packets re-transmitted. This layer ensures that all data is received and in proper order. Function of transport layer can be summarized as below :

1. Primary task is to hide all the network dependent characteristics from the layers above it.
2. Provides transparent data transfer.
3. So all the protocols defined for the transport layer will only need to be implemented on the host computers and not on any intermediate computers in the network.
4. System programmer interface to the network.
5. The transport layer establishes and maintains a logical connection with the corresponding transport layer on a remote host.
6. Use this connection to transfer date.

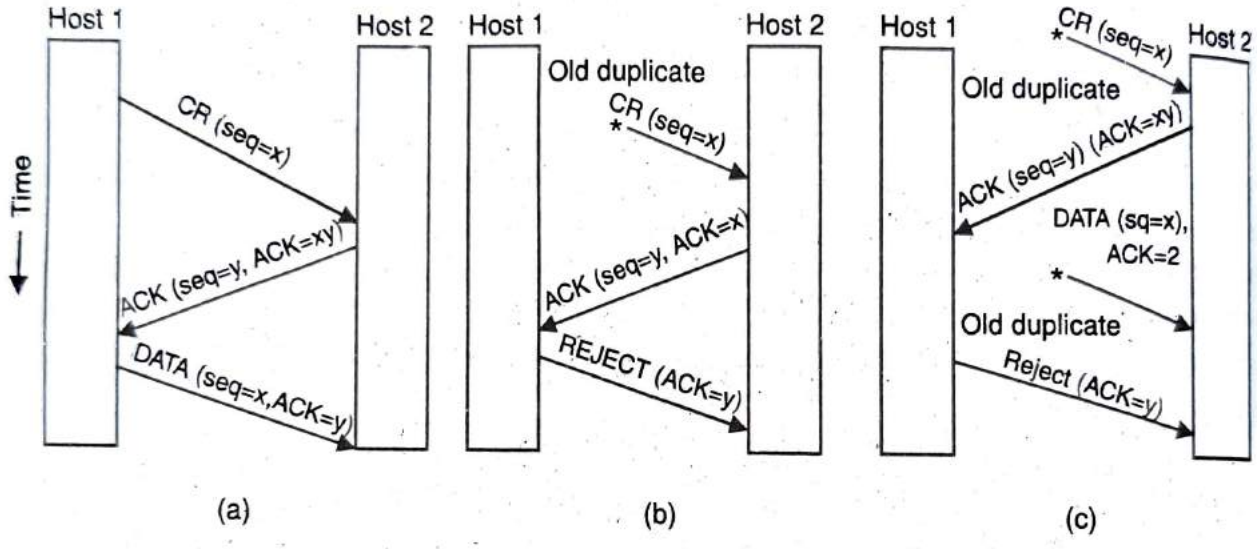
Q 25. Which layer provides End-to-end connectivity from host-to-host? **(PTU, May 2011)**

Ans. The transport layer provides End-to-end connectivity from host-to-host.

Q 26. Discuss the process of three way handshake in transport layer with the help of an example. **(PTU, Dec. 2011)**

Ans. The three way hand-shake : This establishment protocol does not require both sides to begin sending with the same sequence number, so it can be used with synchronization methods other than the global clock method.

These can be shown with the help of diagram :



Q 27. How buffering is handled in transport layer? **(PTU, May 2012)**

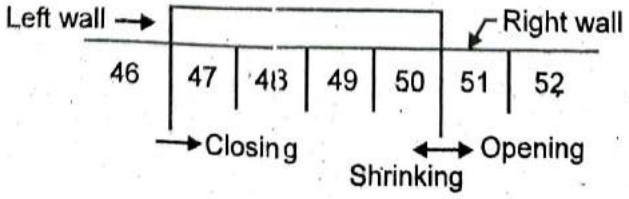
Ans. The transport layer delivers the message from one process to another process running on two different hosts.

TCP uses sliding window for flow control. Sliding window mechanisms allow a sender to transmit all the data units that are window without waiting for their acknowledgement. The sliding window of TCP has two important features :

1. Sliding window is byte oriented and contains data bytes rather than number of TCP segments that can be sent.

2. The size of sliding window is variable.

Sliding Window : The sliding window has two walls-left wall and right wall. These walls move independently and are controlled entirely by receiver.



❑❑❑

Chapter 7

Application Layer

Contents

World Wide Web (WWW), Domain Name System (DNS), E-mail, File Transfer Protocol (FTP), Introduction to Network security.

POINTS TO REMEMBER

- The uniform resource locator (URL) is a standard for specifying any kind of information on the world wide web.
- Privacy is achieved through encryption of the plain text and decryption of the ciphertext.
- The TCP/IP application layer corresponds to the combined session, presentation and application layer of OSI model.
- Each country domain specifies a country.
- FTP (file transfer protocol) is a TCP/IP client-server application for copying files from one host to another.
- HTTP is used mainly to access data on www.
- The www (world wide web) is an architectural framework for accessing documents which are spread out over a number of machines over internet.
- One server program can provide services for many client programs.
- Domain name system (DNS) is a client-server application that identifies each host on the internet with a unique user-friendly name.
- Multimedia includes a combination of text, audio, still images, animation, video and interactivity content forms.
- Simple mail transfer protocol it establishes a connection to port 25 of the destination machine so as to deliver an e-mail.
- One of the most popular network services is electronic mail. Simple mail transfer protocol is the standard machine for electronic mail in the internet.
- Telnet is a client-server application that allows a user to log on to remote machine, giving the user access to the remote system.
- There are seven generic domains, each specifying an organization type.

- Domain name space is divided into three sections : generic domain, country domain and inverse domain.
- The TCP/IP protocol that supports e-mail on the Internet is called simple mail transfer protocol (SMTP).
- The server program is on at all times while the client program is run only when needed.
- Technique that use both secret key encryption and public key encryption are efficient and provide for easy key distribution.
- In the client server model, the client runs a program to request a service and the server runs a program to provide the service. These two programs communicate with each other.
- Pretty and privacy (PGP) provides security for transmission of e-mail.

QUESTION-ANSWERS

Q 1. Explain world-wide-web. **(PTU, May 2009)**

Ans. The world wide web is an architectural framework for accessing documents which are spread out over a number of machines over internet. It has a colourful graphical interface which is easy for the beginners to use. It provides information on almost every subject. The web began in 1989 at CERN the European center for nuclear research. The growth of the world wide web today is simply phenomenal.

Q 2. Explain HTTP. **(PTU, Dec. 2011, 2005)**

Ans. HTTP is used mainly to access data on www. This protocol transfers data in the form of plain text, hypertext audio, video, etc. The function of HTTP is like a combination of PTP and SMTP. It uses services of TCP. It uses only one TCP connection. There is no separate control connection. Only the data transfer takes place between the client and server.

Q 3. Explain hypermedia.

Ans. 1. All pages may not be viewable in the conventional way, some pages may contain audio tracks, video-clips or both.

2. If the hypertext pages are mixed with other media, the result of such a mixing is called as hypermedia.

3. Some browsers are capable of displaying all kinds of hypermedia but others cannot do so.

4. Many web pages contain large images that take a long time to load. When the images are being loaded, the user does not have anything to see.

Q 4. Explain about URLs. **(PTU, Dec. 2005)**

Ans. URL is the unifor resource locator. The first port of the address is called a protocol identifier and it indicates what protocol to use and the second port is called a resource name and it specifies the IP address or the domain name where the resource is located. The protocol is identifier and the resource names are separated by a cain and two formed slashes.

Q 5. What is multimedia? **(PTU, May 2009 ; Dec. 2010)**

Ans. Multimedia includes a combination of text, audio, still images, animation, video and interactivity content forms. Multimedia is usually recorded and played, displayed or accessed by information content processing devices, such as computerized and electronic devices. But can also be a part of live performance multimedia also describes electronic media devices used to store and experience multimedia content. Multimedia may be broadly divided into linear and non-linear categories. Linear active content progresses without any navigation control for the viewer such as a cinema presentation.

Q 6. Explain SMTP and also define its problem.

Ans. SMTP : Simple mail transfer protocol. In Internet the source machine establishes a connection to port 25 of the destination machine so as to deliver an email. An email daemon which speaks SMTP is listening to this port.

Tasks are :

1. Accept the incoming connections and copy messages from them into appropriate mailboxes.
2. Return an error message to the sender, if a message is not delivered.

SMTP is a simple ASCII protocol. Once a TCP connection between a sender and port 25 of the receiver is established, the sending machine operates as a client and the receiving machine acts as a server.

Problems in SMTP : Some of the problems in SMTP may be listed as under :

1. Some older implementations are not capable of handling messages longer than 64 KB.
2. If client and server have different time-outs, then one of them may give up when the other is still busy.

Q 7. Explain features of e-mail system.

Ans. Some of the advanced features included in addition to the basic functions may be listed as under :

1. Forwarding an e-mail to a person away from his computer.
2. Creating and destroying mailboxes to store incoming e-mail.
3. Inspecting contents of mailbox, insert and delete messages from the mailboxes.
4. Sending a message to a large group of people using the idea of mail list.
5. To provide registered e-mail.
6. Automate notification of undelivered e-mails.
7. Carbon copies.
8. High priority e-mail.
9. Secret (encrypted e-mail).
10. Alternative recipient.

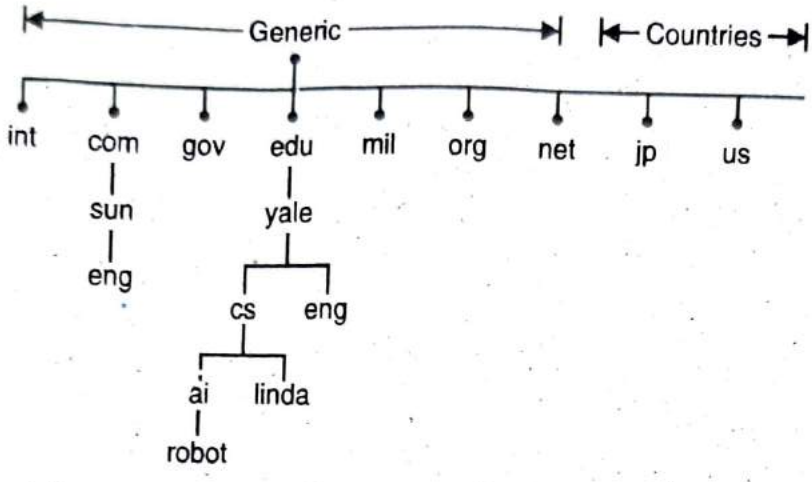
Q 8. What are the three domains of the domain name space? Also explain the purpose of the inverse domain. **(PTU, Dec. 2011, 2007)**

OR

Write short note on DNS. **(PTU, Dec. 2012)**

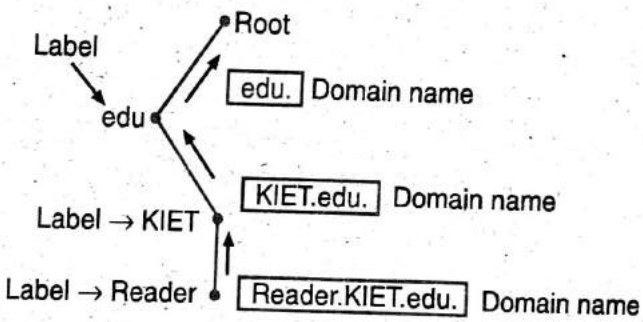
Ans. DNS : Conceptually, the internet has been divided into hundreds of top level

domains. Each domain covers many hosts. Each domain is divided into several subdomains and they are further partitioned and so on. These domains can be represented by a tree.



The top level domains are of two types namely generic and countries.

1. Generic Domains : The generic domains are com (commercial), edu (educational institutions), gov (government), int (some international organizations), mil (military), net (network providers), and org (nonprofit organizations). The country domains include one entry for every country. Each domain is named by following an upward path. The components are separated by dots, e.g., **eng.sum.com.** This is called hierarchical naming. Another example of hierarchical naming is shown in fig. The upward followed path has been shown by an arrow.



2. Label : Each node in the tree has a label (or component) and it can be specified using upto 63 characters. If we had to remember the IP addresses of all of the web sites, we visit every day, we would all go nuts. Human beings just are not that good at remembering strings of numbers. We are good at remembering words, however, and that is where domain names come in. You probably have hundreds of domain names stored in your head. For example :

- www.yahoo.com - the world's best-known name
- www.kiet.edu - a popular EDU name
- encarta.msn.com - a Web server that does not start with www
- www.bbc.co.uk - a name using four parts rather than three
- ftp.microsoft.com - an FTP server rather than a Web server

The COM, EDU and UK portions of these domain names are called the **top-level domain** or **first-level domain.** There are several hundred top-level domain names, including COM, EDU, GOV, MIL, NET, ORG and INT, as well as unique **two-letter combinations for every country.**

Within every top-level domain there is a huge list of **second-level domains.** For example, in the COM first-level domain, you have got :

- yahoo
- msn
- microsoft
- plus millions of others.

Every name in the COM top-level domain must be unique, but there can be duplication across domains. For example, **msn.com** and **msn.org** are completely different machines. In the case of bbc.co.uk, it is a third-level domain. Up to 127 levels are possible, although more than four is rare. The left-most word, such as **www** or **encarta** is the **host name.** It specifies the name of a specific machine (with a specific IP address) in a domain. A given domain can potentially contain millions of host names as long as they are all unique within that domain.

3. Absolute and Relative Domain Names : Domain names can be of two types : absolute or relative. An absolute domain name always ends with a dot (or period as it called). For example, eng.sun.com. But the relative domain does not end with a dot.

Q 9. What is a firewall? **(PTU, Dec. 2012)**

Ans. Firewall is used to protect or secure our network from organization. Firewall is like a hardware and software i.e. used to save or secure our network within organization. If somebody hacks the network, then in that case firewall is used to protect the network. Within a organization, there are some mechanism to protect our network so that no one can hack our important data or secure them from unauthorized user.

Q 10. What do you mean by spread spectrum? **(PTU, Dec. 2011)**

Ans. In frequently hopping spread spectrum, the transmitter hops from frequency to frequency hundreds of times per second. The other form of spread spectrum, direct sequence spread spectrum, which spreads the signal over a wide frequency band, is also gaining popularity in the commercial world.

Q 11. Explain e-mail architecture and services. **(PTU, Dec. 2010, 2007)**

OR

Write short note on Email. **(PTU, Dec. 2012)**

Ans. Electronic Mail (E-mail) : One of the most popular network services is electronic mail (e-mail). Simple mail protocol (SMTP) is the standard mechanism for electronic mail in the internet. The first e-mail systems simply consisted by file transfer protocols.

E-mail Architecture and Services : An e-mail system consists of two subsystems as under :

(i) User agents and

(ii) Message transfer agents

User Agents : They allow the people to read and send e-mail.

Message Transfer Agents : They move the messages from the source to the destination.

Basic Functions : E-mail systems support five basic systems which may be listed as under :

(i) Composition

(ii) Transfer

(iii) Reporting
(iv) Displaying
(v) Disposition.

Advanced features of E-mail systems :

1. Forwarding an e-mail to a person away from his computer.
2. Creating and destroying mail boxes to store incoming e-mail.
3. Inspecting contents of mailbox, insert and delete messages from the mailboxes.
4. Sending a message to a large group of people using the idea of mail list.
5. To provide registered e-mail.
6. Secret (encrypted e-mail).
7. Carbon copies.
8. High priority e-mail.

Q 12. What is use of reverse ARP? **(PTU, May 2010)**

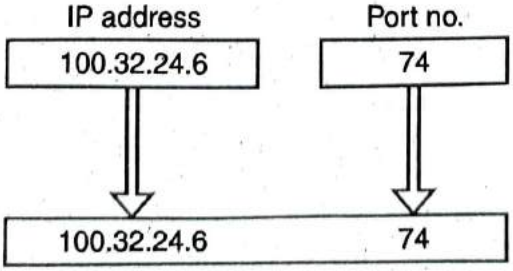
Ans. Reverse address resolution protocol (RARP) : This protocol is used to do the reverse of ARP i.e. this protocol is used to find the IP address when an ethernet address is given. Whereas ARP is used to find ethernet addresses from given IP address.

The problem of missing IP address occurs when booting a diskless workstation. The newly booted workstation is allowed to broadcast its ethernet address. The RARP server looks at his request, then it looks up the ethernet address in its configuration files and send back the corresponding IP address.

Q 13. Explain socket programming. **(PTU, May 2006 ; Dec. 2004)**

Ans. The communication structure that we need in socket programming is called as a socket. A socket acts as an end point. Two processes can communicate if and only if they have a socket at each end. The concept of sockets was developed in 1980s in the unix environment. A socket enables communication between a client and a server and may be connection-oriented or connectionless. A client socket in one computer uses an address to call a server socket on another computer. Once these sockets are engaged, the two computers can start exchanging the data. Internet applications such as TELNET and remote login make use of the sockets with the details hidden from the user. But it is possible to construct sockets within a program in languages such as C or java. This enables the programmer to easily support networking functions and applications. The socket programming mechanism is flexible enough to permit unrelated processes or different host to communicate.

Process to process delivery needs two identifiers, one is IP address and the other is port no. at each end to make a connection.



Socket Address

The client socket address defines the client process uniquely whereas the server socket address defines the server process uniquely. A transport layer protocol requires the client socket address as well as serves socket address. These two addresses contain four pieces. These four pieces go into the IP header and the transport layer protocol header. The IP header contains the IP addresses whereas TCP contains the port no's.

Q 14. Explain briefly any two application layer protocols. **(PTU, Dec. 2008)**

OR

Explain FTP. **(PTU, May 2004)**

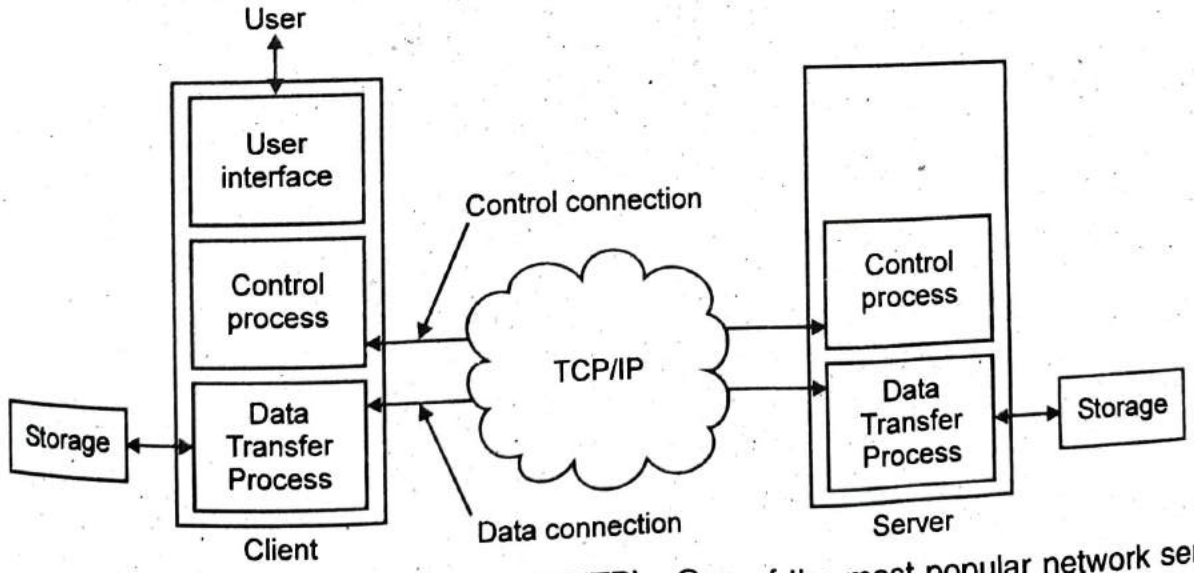
Ans. Various application layer protocols are :

Telnet, FTP, SMTP, DNS, HTTP, NNTP.

1. File Transfer Protocol (FTP) : FTP is standard mechanism provided by TCP/IP for copying a file from one host to another. Transferring files from one computer to another is one of the most common tasks expected from a networking or internetworking environment.

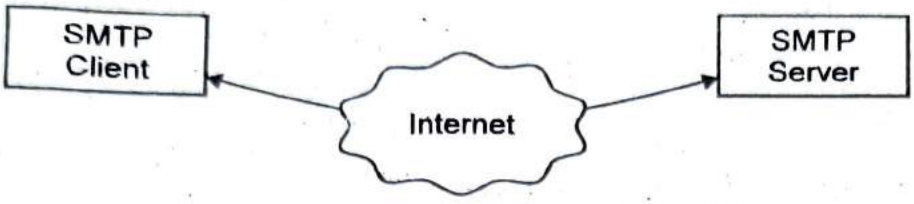
FTP differs from other client-server applications in that it establishes two connections between the hosts. One connection is used for data transfer the other for control information. Fig. below shows the basic model of FTP. The client has three components :

The user interface, the client control process, the client data transfer process. The server has two components. The server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer process. The control connections remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred.



2. Simple mail transfer protocol (SMTP) : One of the most popular network services is electronic mail. The TCP/IP protocol that supports electronic mail on the Internet is called simple mail transfer protocol (SMTP). It is a system for sending messages to other computer user based on e-mail addresses. SMTP provides for mail exchange between users on the same or different computers and supports.

1. Sending a single message to one or more recipients.
2. Sending message that include text, voice, video or graphics.
3. Sending message to users on networks outside the Internet.

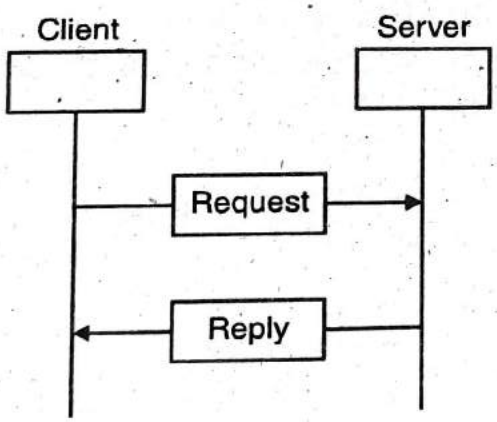


Q 15. How is HTTP similar to SMTP and FTP? Explain your answer.

(PTU, May 2007)

Ans. Hypertext Transfer Protocol (HTTP) : HTTP is used mainly to access data on www. This protocol transfers data in the form of plaintext, hypertext, audio, video, etc. The function of HTTP is like a combination of FTP and SMTP. It uses services of TCP. It uses only one TCP connection. There is no separate control connection. Only the data transfer takes place between the client and server. The data transfer in HTTP is similar to SMTP. The format of the messages is controlled by MIME like headers.

The principle of operation of HTTP is simple. A client sends a request. The server sends a response. The request and response messages carry data in form of letter with MIME like format. Fig. shows the HTTP transactions between client and server. The client initializes the transaction by sending a request message and server replies it by sending a response.



HTTP transaction

Q 16. Explain FTP. How does it work? **(PTU, May 2006)**

Ans. FTP : It is standard mechanism provided by the internet for copying a file from one host to the other.

FTP establishes two connections between the client and server. One is for data transfer and the other is for the central information. The central connection uses simple rules for communication. Only one line of command or a line of response is transferred at a time.

The server has two components : The central process and transfer process.

Q 17. What is FQDN and PQDN in DNS? **(PTU, May 2007)**

Ans. Fully Qualified Domain Name (FQDN) : It is an unambiguous domain name that

specifies the node position in the domain name service tree hierarchy absolutely. To distinguish an FQDN from a regular domain name a traling period is added.

Partially Qualified Domain Names (PQDN) : It is an ambiguous domain name, because it does not give the full path to domain. Thus, one can only use PQDN within the content of a particular parent domain, whose absolute domain name is known.

Q 18. Write a short note on Network File Server and Directory Server.

(PTU, Dec. 2004)

Ans. File Server is a computer responsible for the central storage and management of data files so that other computers on the same network can access the files. A file server allows the user to share information over a network without having to physically transfer files by floppy diskette or some other external storage device.

In other words, file server may be an ordinary PC that handles requests for files and sends them over the network.

Directory Server : A directory server is a type of network daemon that will store data in a manner accessible to external clients. Directory server typically uses LDAP or DSML for communication with clients, although some server uses other protocols like DAP or DNS.

Directory servers store data in a hierarchical form (called the directory information tree) and provide the ability for clients to interact with that information.

Q 19. Explain FTP transmission mode.

Ans. There are three modes of FTP :

1. Stream mode
2. Block mode
3. Compressed mode

1. Stream Mode : In this mode, the data is delivered from FTP to TCP in the form of continuous stream of bytes. TCP chops this data into segments of appropriate size.

2. Block Mode : In this mode, data can be delivered from FTP to TCP in blocks. Each such block is preceded by a 3 byte header.

3. Compressed Mode ; For big files data can be compressed. Generally a run length encoding is used for compression.

Q 20. Explain the difference between web and internet.

Ans. The web and internet are not the same thing. The web is a collection of standard protocols or instructions, sent back and forth over the internet to gain access to information. The internet, on the other hand, is a "network of networks" a more physical entity. Extending this to the internet a "website" is such a publically accessible notice board on the "server" or "host computer" connected to the internet. The technique used to address the documents on the web is called as "uniform resource locator".

Q 21. What kind of file types can FTP transfer? What are the three FTP transmission modes?

(PTU, May 2007)

Ans. FTP (File Transfer Protocol) : FTP is a standard mechanism provided by the

internet for copying a file from one host to the other.

FTP can transfer following three file types over the data connection :

1. ASCII File
2. EBCDIC File
3. Image File

- ASCII file is a text file, EBCDIC file can transferred if both ends use EBCDIC encoding.
- Image file is the default format for the transfer of binary files.
- With ASCII or EBCDIC files one more attribute must be added for defining the printability of the file. This attribute is non-print or TELNET.

Transmission Mode : FTP uses following types of mode for transfer of a file.

1. Stream Mode
2. Block Mode
3. Compressed Mode.

1. Stream Mode : In this mode, the data is delivered from FTP to TCP in the form of continuous stream of bytes. TCP chops this data into segments of appropriate size.

2. Block Mode : In this mode, data can be delivered from FTP to TCP in blocks. Each such block is preceded by a 3 byte header.

3. Compressed Mode : For big files data can be compressed. Generally a run length encoding is used for compression.

Q 22. Explain browser.

Ans. The program used for viewing pages is called browser. The job of browser is to fetch the page requested by the user, interprets the text and formatting commands which it contains, display the page with proper format on screen. A web page starts with a bitle and contains the following :

1. Some information
2. String of text, linked to other pages
3. E-mail address of the page's maintainer.

Q 23. Explain Telnet (Remote Login).

Ans. 1. Users anywhere on the internet can log into any other machine on which they have an account.

2. This is possible using the programs like Telnet or R Login.

3. Telnet is another application which allows the user to "logon" or connect to a remote computer system, from anywhere in the world. Telnet is a network application that is used to Logon to one computer on the Internet from another.

4. "Telnet" provides a convenient way of accessing your e-mail server from anywhere in the world. For example, an Internet user having an account on a VSNL server at Pune may want to check his e-mail when he is out of the city.

Q 24. Explain about multimedia. **(PTU, Dec. 2010, 2006)**

Ans. Multimedia : In general multimedia-includes a combination of text, audio, still images, animation, video and interactivity content forms.

Multimedia is usually recorded and played displayed or accessed by information content processing devices, such as computerized and electronic devices, but can also be part of a live performance. Multimedia also describes electronic media devices used to store and experience multimedia content.

Multimedia may be broadly divided into **linear** and **non-linear** categories. **Linear active content** progresses without any navigation control for the views such as a cinema presentation. **Non-linear content** offers user intreactivity to control progress as used with a computer game or used in self-raced computer based training. Non-linear content is also known as hypermedia content.

Multimedia presentation can be live or recorded. A recorded presentation may allow interactivity via a navigation system. A live multimedia presentation may allow interactivity via interaction with the presenter or performer.

Multimexia finds its application in various areas including, but not limited to advertisements, art, education, entertainment, engineering, medicine, mathematics, business, scientific research and spatial temporal applications.

Q 25. What is the use of network file server? (PTU, May 2006, 2004)

Ans. 1. A file server helps in regular backing up of all files stored into it. So whenever a file gets deleted or is misplaced from your PC, this file can be retrieved. Also, if there is a hard disk failures the files saved on the network will not be affected.

2. The file stored on the file server can be accessed directly by each person on the network, this allows them to directly work on the document if required.

Q 26. What is an E-mail Gateway? (PTU, May 2006, 2005 ; Dec. 2005)

Ans. The e-mail gateway allows you to intiate scripts by sending an email message to a reserved address. This product can be used to automatically process email messages from customers, or begin processes in response to monitoring applications that send mail notification etc.

Q 27. What devices will you like to use in a LAN to enable network security? (PTU, May 2010)

Ans. Network security include four main expects :

1. **Privacy :** It means that the sender and receiver expect confidentiality.
2. **Authentication :** It means that the receiver is sure of sender's identity.
3. **Integrity :** It means that the data must arrive at the receiver exactly as it was sent.
4. **Non-Repudiation :** It means that a receiver must be able to prove that a received message came from a specific sender.

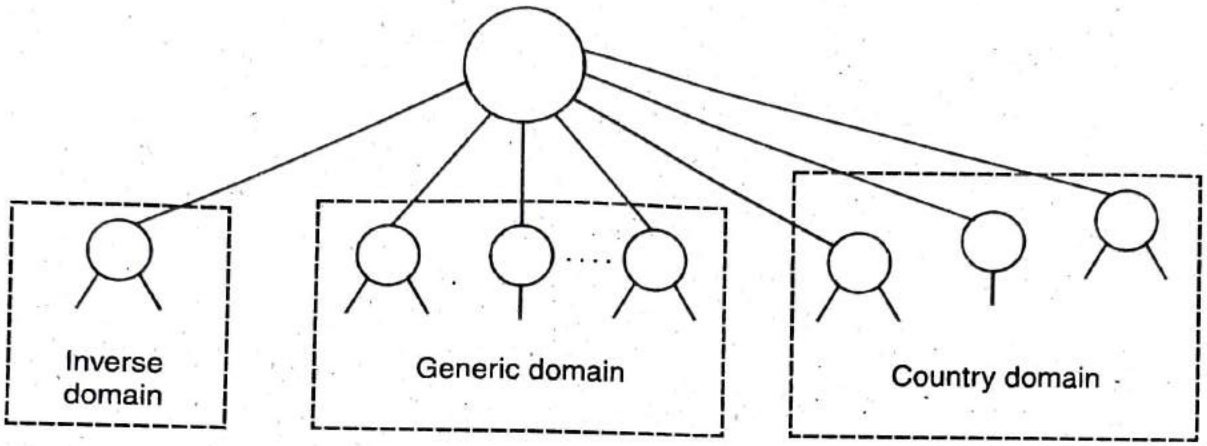
So, in order to attain all this data encryption and decryption device should be attached in LAN.

Q 28. What is the use of DNS protocol? What will happen in case DNS protocol is not present in the TCP/IP model? (PTU, May 2010)

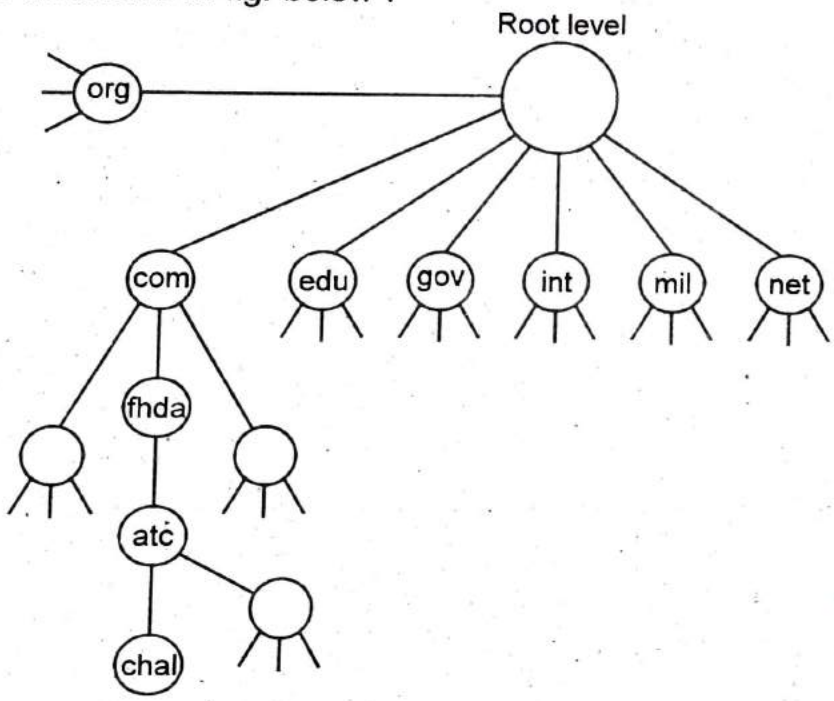
Ans. To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the internet. However, people prefer to use names instead of

addresses. Therefore, we need a system that can map a name to an address and conversly an address to a name. In TCP/IP, this is the domain name system (DNS).

DNS is a protocol that can be used in different protocols. In the internet, the domain name space (tree) is divided into three different sections : generic domains, country domains and inverse domain. Fig. shows DNS in internet.



Generic Domain : Generic domain define registered hosts according to their generic behaviour. Each node is the tree defines a domain, which is an index to the domain name space database as shown in fig. below :

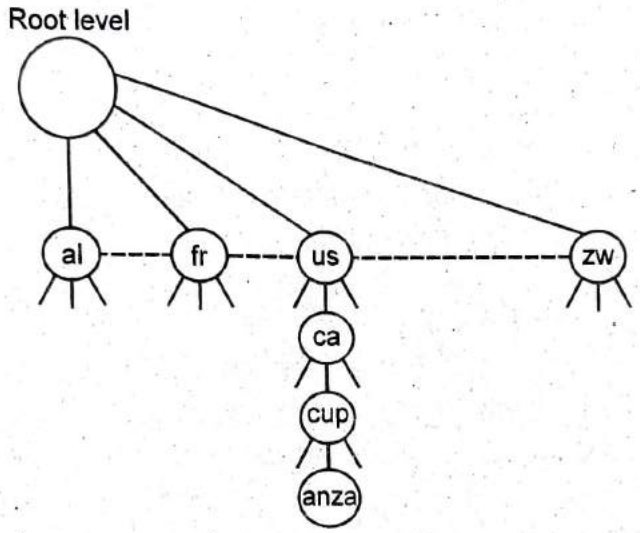


Looking at tree, we see that the first level in the generic domain section allows seven possible three-character labels. These labels describe the organisation types as :

com – Commerical organisation
edu – Educational institutions
gov – Government institutions
int – International organisation

mil – Military groups
net – Network support centre
org – Non-profit organisation

Country Domain : The country domain section follow the same format as the generic domains but uses two character country abbreviations (e.g "US" for United States) in place of the three-character organizational abbreviations at the first level, second level labels can be organizational, or they can be more specific, national designations. The united states, for example, uses state abbreviations as a subdivision of "US". Fig. below shows the country domain.



Inverse Domain : The inverse domain is used to map an address to a name. This may happen, for example when a server has received a request from a client to do a task. Whereas the server has a file that contains a list of authorized clients, the server lists only the IP address of the client. To determine if the client is on the authorized list, it can send a query to the DNS server and ask for a mapping of address to name.

Q 29. Describe in brief the terms : DNS, World Wide Web, E-mail. (PTU, Dec. 2009)

OR

Differentiate between E-mail and DNS services. (PTU, May 2009)

Ans. 1. Domain Name System (DNS) : To identify an entity, TCP/IP protocol uses the IP address, which uniquely identifies the connection of a host to the internet. However people prefer to use names instead of addresses. Therefore we need a system that can map a name to an address and conversely an address to a name. In TCP/IP, this is called domain name system.

2. World Wide Web (WWW) : The WWW, or web is a repository of information spread all over the world and linked together. The WWW has unique combination of flexibility, portability and user friendly features that distinguish if from other services provided by the internet. It may also be defined as an architectural framework for accessing documents which are spread out over a number of machines over internet. It has a colourful graphical interface which is easy for the beginners to use.

3. E-mail (Electronic Mail) : E-mail, like most other forms of communication is just the electronic message passed from one computer to another in the network.

Q 30. What is the main use of DNS? **(PTU, May 2011)**

Ans. DNS (Domain Name System) was created to organize machines into domains and map host names onto IP addresses. Since than DNS has become a generalized distributed database system for storing a variety of information related to naming.

Q 31. Explain how the DNS allows a large number of DNS lookups to be processed. Which protocol is used by DNS on TCP/IP protocol stack and why? (PTU, May 2011)

Ans. A DNS look up uses an internet domain name to find an IP address, where a reverse DNS lookup is using an Internet IP address to find a domain name. Reverse DNS lookup technique is able to identify if the sending e-mail server is legitimate and has a valid host name.

Many spammers use microconfigured hosts to disguise the source of the spam. DNS lookup not always a good solution. Many legitimate mail servers are incorrectly configured, or have intentionally not registered a name with DNS, so a reverse query does not return a matching host name. Also, this anti-spam method runs DNS queries on a large number or e-mails and consumes valuable network resources.

Ways to do DNS lookup :

Reverse DNS lookup : This method is time-consuming and it is rarely used. The receiving server performs a reverse DNS lookup on the IP address of the incoming connection and checks if there is a valid domain name associated to it.

Helo lookup : The receiving server will get the host name of the sending e-mail server from the SMTP HELO Command, perform a simple DNS query and verify that IP address is indeed the IP address does not match the incoming connection IP address, e-mail is rejected.

Sender's address lookup : When ISPs check whether an incoming e-mail is accepted, they can do a DNS check on the sender's e-mail address. For example : if your address is user@domain.com, then the ISP does an nslookup on domain.com. If no records are found – the message is rejected.

Q 32. Explain briefly how the network security is taken care of in application layer. **(PTU, Dec. 2009)**

OR

Elaborate various services that network security can provide in networks. **(PTU, Dec. 2011 ; May 2009)**

Ans. Network security problems can be divided roughly into four closely interwinded areas : seceracy, authentication, no repudiation and integrity control. Seceracy deals with keeping information out of hands of unauthorized users. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Do repudiation deals with signature.

Issues such as users authentication and non-repudiation can only be handled in the application layer. Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter. Verifying the identity of a remote process in the face of malicious, active intruder is surprisintly difficult and requires complex protocols based on cryptography.

❑❑❑

LORDS MODEL TEST PAPERS

(Unsolved)

LORDS MODEL TEST PAPER – 1

Time : 3 hrs. **Maximum Marks : 60**

Instruction to Candidates :

Note : Section A is compulsory. Attempt any four questions from section B and two questions from section C.

SECTION – A

Q 1. (a) What is block parity?
(b) Explain broadcast network and point to point networks.
(c) Which MAC layer protocol is used by 802.11 WLAN?
(d) What are sliding window protocol?
(e) What is the need of subnet mask?
(f) What is channel allocation?
(g) Differentiate between TCP and UDP.
(h) Difference between LAN, MAN and WAN.
(i) Elaborate various services that network security can provide in networks.
(j) Define the difference between synchronous transmission and asynchronous transmission.

SECTION – B

Q 2. (a) Write a short note on bandwidth, bitrate and error rate.
(b) What is subnetting? What it is used?
Q 3. What are various transmission media used? Explain about each of them.
Q 4. Describe the various congestion control algorithms with examples.
Q 5. (a) What are two types of switches used in circuit switching?
(b) Explain the meaning of various fields of the TCP header with example.
Q 6. What is HDLC? Explain its frame format and its various fields with a neat diagram. How is it superior to SDLC frame format?

SECTION – C

Q 7. Why is multiple access required in LAN technologies? Compare FDM, TDM and SDM in terms of their ability to handle groups of stations.
Q 8. What is the use of DNS protocol? What will happen in case DNS protocol is not present in the TCP/IP model?
Q 9. Write short notes on the following :
(a) Digital data Transmission
(b) Routing algorithms.
(c) IP addressing

LORDS MODEL TEST PAPER – 2

Time : 3 hrs. **Maximum Marks : 60**

Instruction to Candidates :

Note : Section A is compulsory. Attempt any four questions from section B and two questions from section C.

SECTION – A

Q 1. (a) What is a hamming distance?
(b) What do you mean by network reliability?
(c) What do you understand by shannon capacity?
(d) What is CSMA/CD?
(e) Define the term congestion.
(f) Explain about multimedia and WWW.
(g) How buffering is handled in transport layer?
(h) Differentiate between baseband coaxial cable and broadband coaxial cable.
(i) What is the role CRC in data link layer?
(j) What is a protocol?

SECTION – B

Q 2. (a) Comparison of IEEE 802.3, 802.4 and 802.5 standard.
(b) Difference between pure ALOHA and slotted ALOHA.

Q 3. What is difference between open loop congestion control and closed loop congestion control?

Q 4. What is the main use of multiplexing? Explain various ways in which multiplexing can be done.

Q 5. (a) Explain the advantages and disadvantages of optical fibre cable.
(b) Compare error correcting and error detecting code.

Q 6. What do you mean by switching? Describe in brief the various switching methods.

SECTION – C

Q 7. Explain the role of different layers of OSI-ISO reference model? Also compare at with TCP/IP protocol architecture.

Q 8. Draw and discuss the IP diagram frame format. Discuss in detail the various fields. What is subnettng?

Q 9. Write short notes on the following :
(a) DNS
(b) Email.

❑❑❑