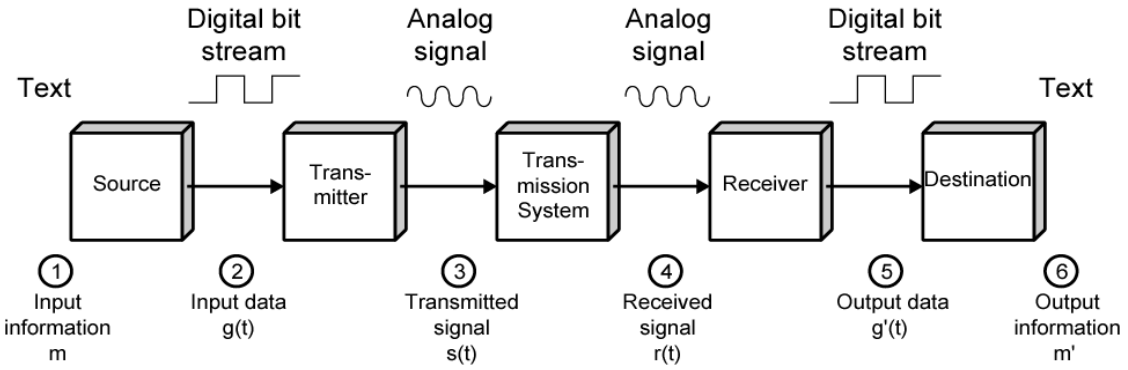
Q2a) With neat block diagram explain data communication model

Ans: Block diagram



The key elements of this model are:

- Source - generates data to be transmitted
- Transmitter - converts data into transmittable signals
- Transmission System - carries data from source to destination
- Receiver - converts received signal into data
- Destination - takes incoming data

Source:
Source may be analog or digital signal. If source is analog it will be converted into digital by means of sampling and quantization.
Transmitter:
It will modulate the digital data using shift keying technique before transmission. The different shift keying technique are ASK, FSK and PSK.
Transmission system:
It is the media between transmitter and receiver. It can be either wired or wireless.
Wireless system corresponds to free space and wired may be open wire, co-axial cable or optical fiber.

Receiver:
It is used to demodulate the received signal. The type of demodulation depends on the type of modulation used at transmitter.
Destination:
Here data will be put in original form like voice, image or Text.

b) Explain the functions performed by the following layers of OSI model.

(i) Data link layer
(ii) Network layer
(iii) Session layer

Ans:

Application layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data link Layer
Physical Layer

Figure2b) Layers of ISO –OSI model

i) Data link layer:

The data link layer is concerned with issues like;

i) Transmission block starting and ending.[Frame formation]
ii) Transmission error detection
iii) Error control to get an error free link.

The design of data layer involves;

- Framing and link management
- Error control and flow control
- Service to the network layer
- Error detection and correction
- Error correcting codes and detecting codes
- Data link protocols and protocol performance

ii) Network layer:

The network layer provides a connection path for data transfer between a pair of transport entities. The network layer,

- Provides services to the transport layer
- Determine routing of packets from source to destination
- Provides congestion control when the traffic is heavy.
- Helps internetworking when the source and destination minicomputers are in different networks.

iii) Session layer:

The session, presentation and application are the upper layers concerned with user oriented services and the protocols are referred to as high level protocols. These 3 layers are present in IMP's. The session layer,

- Provides service to presentation layer
- Provides a means for 2 applications to establish and use a connection called a session
- Does data Exchange, dialogue management.
- Does checking and recovery when failure occurs between checkpoints provided by session layer.

c) Compare LAN and WAN

Ans:

LAN	WAN
Have diameter of not more than a few kms.	Have diameter of more than a few hundreds of kms
Total data rates of several Mbps	Total data rates is below 1 Mbps
Complete ownership by a single organization	Owned by multiple organization
Confined to a room, building, campus	Spans entire city, country continent
Error rate is less	Errors rate is greater than LAN
Simpler protocol can be used	Protocol will be relatively complex
LAN cable is highly reliable	WAN cables are less reliable

Q3a) Define the following terms with refers to data communication

- Crosstalk
- Data rate
- Bandwidth
- Noise
- Error rate

Ans:

i) Crosstalk: It is an unwanted coupling between signal paths. It can occur by electrical coupling between nearby twisted pairs or coax cable carrying multiple signals.

ii) Data rate: The rates in bits per second (bps) at which the data can be communicated.

iii) Bandwidth: The range of frequency used for communication. It depends on the nature of medium used, it is expressed in Hz.

iv) Noise: Any un wanted signal in communication is referred as noise. It can be within the system (internal noise) or outside the system (external noise)

v) Error rate: The rate at which the error occur. Error refers to reception of a 1 when a 0 was transmitted or vice versa.

b) Compare guided and un-guided transmission media.

Ans: 4.1 and 4.2 of Textbook

c) Assuming that a PSTN has a bandwidth of 3000 Hz and a typical S/N power ratio of 30db, determine the maximum theoretical (data) rate that can be achieved.

Ans:

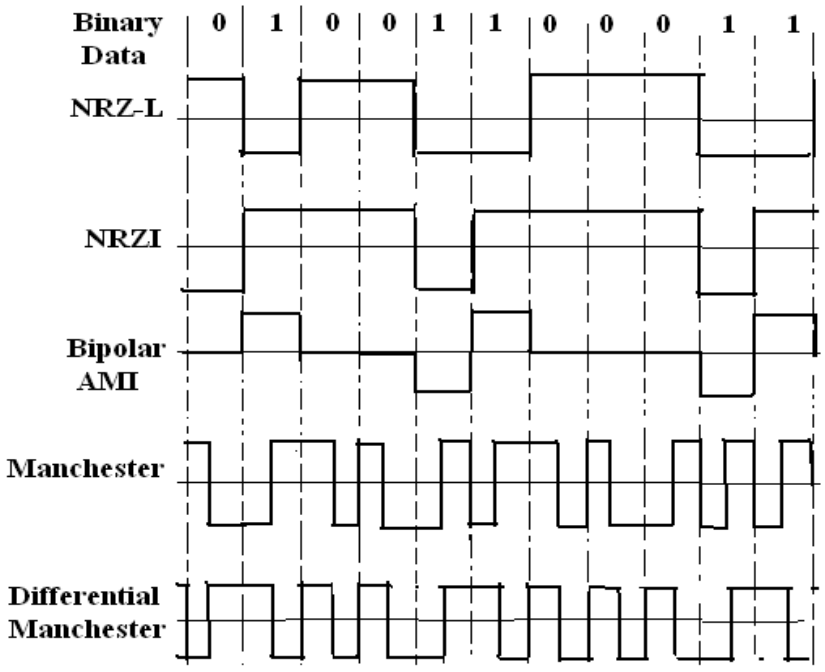
B=3000Hz, (S/N) dB=30db
(S/N) ratio=Antilog (30/10) =1000
$C=B \log_2(1+(S/N)r)=3000 \log_2(1+1000)=29884.32$kbps

Q4a) Represent the binary data 01001100011 in

(i) NRZ-L
(ii) NRZI
(iii) Bipolar –AMI
(iv) Manchester
(v) Differential Manchester Encoding format

Ans: The binary data 01001100011 in

i) NRZ-L
ii) NRZI
iii) Bipolar –AMI
iv) Manchester
v) Differential Manchester Encoding format
vi)



b) What are the factors to be considered while selecting digital encoding format?

Ans: The factors to be considered while selecting digital encoding format are

1) Signal spectrum
2) Clocking
3) Error detection
4) Signal interference and noise immunity
5) Cost and complexity

1) Signal spectrum:
Signal should have minimum or no dc components. The spectrum of the signal should match with the bandwidth of the channel, otherwise distortion will occur.
Manchester will take double the bandwidth as compared to NRZ signals.

2) Clocking:
Code should be able to extract the clock from the received signal for synchronization. In this aspect Manchester will be best suited.

3) Error detection:
Code should be able to detect the errors. In this aspect bipolar AMI is best suited because in this code if two bits are received in the same direction it will violet the rule and indicates an error.

4) Signal interference and noise immunity:
NRZ codes are more immune to noise as compared to RZ codes.

5) Cost and complexity:
The higher the signaling rate to achieve cost rate increases. Select suitable code which transmit data at high rate with low cost.

c) For the binary data 1101001 plot differ digital shift keying modulated wave form and explain the same.

Ans: Differ digital shift keying modulation are

1. Amplitude Shift Keying[ASK]
2. Frequency Shift Keying[FSK]
3. Phase Shift Keying[PSK]
   The waveform for the binary data 01101 for these modulations are as shown in figure 4(c)

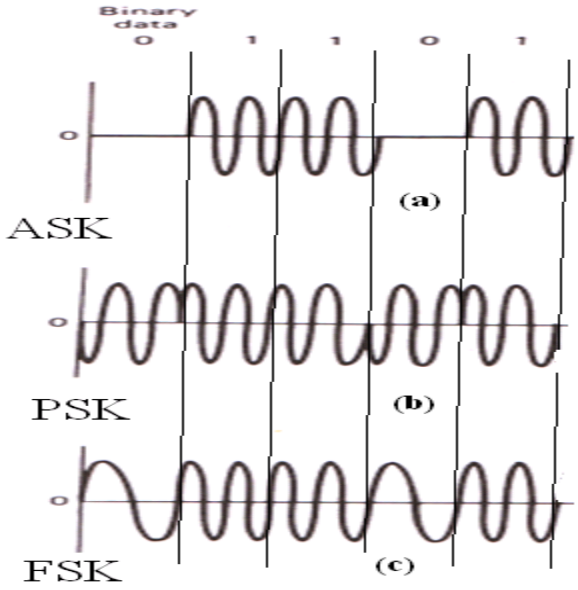


Figure 4(c).

Amplitude-shift-keying (ASK): ASK describes the technique the carrier wave is multiplied by the digital signal b(t). For symbol 1 carrier is transmitted, whereas for symbol 0 no carrier is transmitted.

Frequency-shift-keying (FSK): FSK describes the modulation of a carrier (or two carriers) by using a different frequency for a 1 or 0. The resultant modulated signal may be regarded as the sum of two amplitude-modulated signals of different carrier frequency.

Phase-shift-keying (PSK): In PSK for symbol 1 carrier is transmitted, whereas for symbol 0 carrier with 180 degree phase shift is transmitted.

Q5a) What is the need of multiplexing? Explain different types of multiplexing used in computer networks

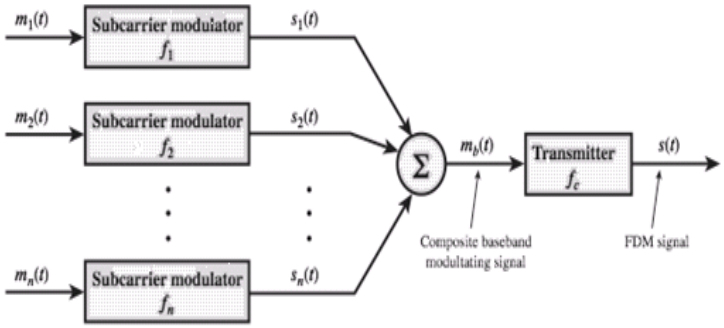
Ans: Multiplexing refers to transmitting more than one information (or data) over a common channel

Different multiplexing techniques are:

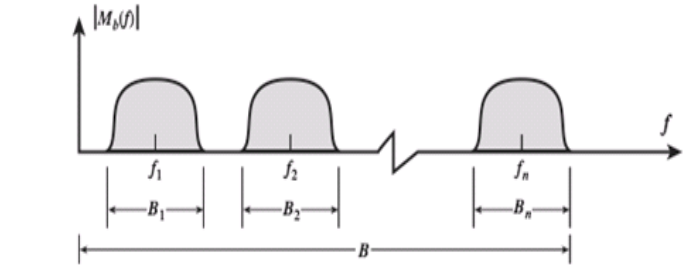
- FDM (Frequency Division Multiplexing)
- TDM (Time Division Multiplexing)
- WDM (Wavelength Division Multiplexing)

Frequency division multiplexing can be used with analog signals. A number of signals are carried simultaneously on the same medium by allocating to each signal a different frequency band. FDM is possible when the useful bandwidth of the transmission medium exceeds the required bandwidth of signals to be transmitted. A number of signals can be

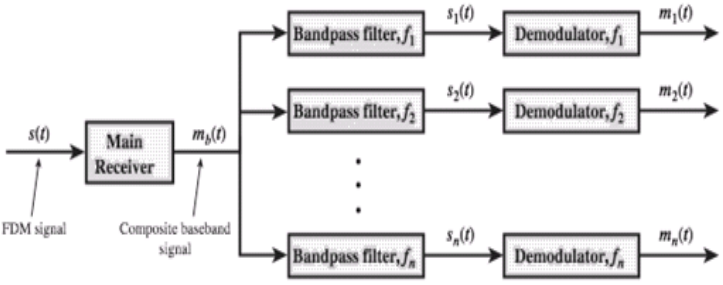
carried simultaneously if each signal is modulated onto a different carrier frequency and the carrier frequencies are sufficiently separated that the bandwidths of the signals do not significantly overlap.



(a) Transmitter



(b) Spectrum of composite baseband modulating signal



(c) Receiver

TDM [Time Division Multiplexing]:

Time division multiplexing (TDM) is a channel access method for shared medium (usually radio) networks. It allows several users to share the same frequency channel by dividing the signal into different timeslots. The users transmit in rapid succession, one after the other, each using his own timeslot. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only the part of its bandwidth they require.

Stations take turns in accessing medium and transmission from stations is separated in time.

Stations transmit information in their slots allotted in each TDM cycle

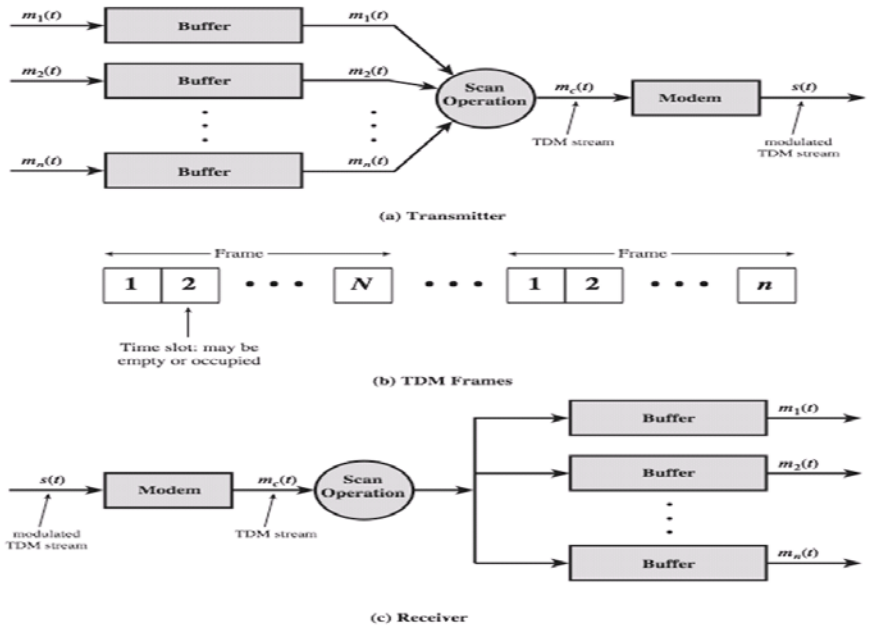
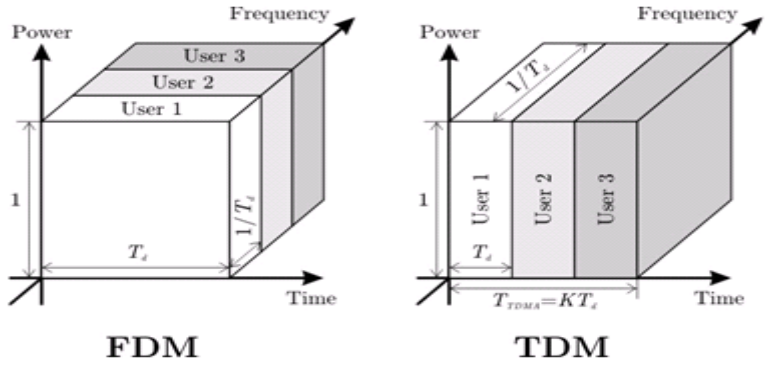


Figure Synchronous TDM System



Wavelength Division Multiplexing:
The true potential of optical fiber is fully exploited when multiple beams of light at different frequencies are transmitted on the same fiber. This is a form of frequency division multiplexing (FDM) but is commonly called wavelength division multiplexing (WDM). With WDM, the light streaming through the fiber consists of many colors, or wavelengths, each carrying a separate channel of data.

b) With neat diagram explain sliding window protocol

Ans:

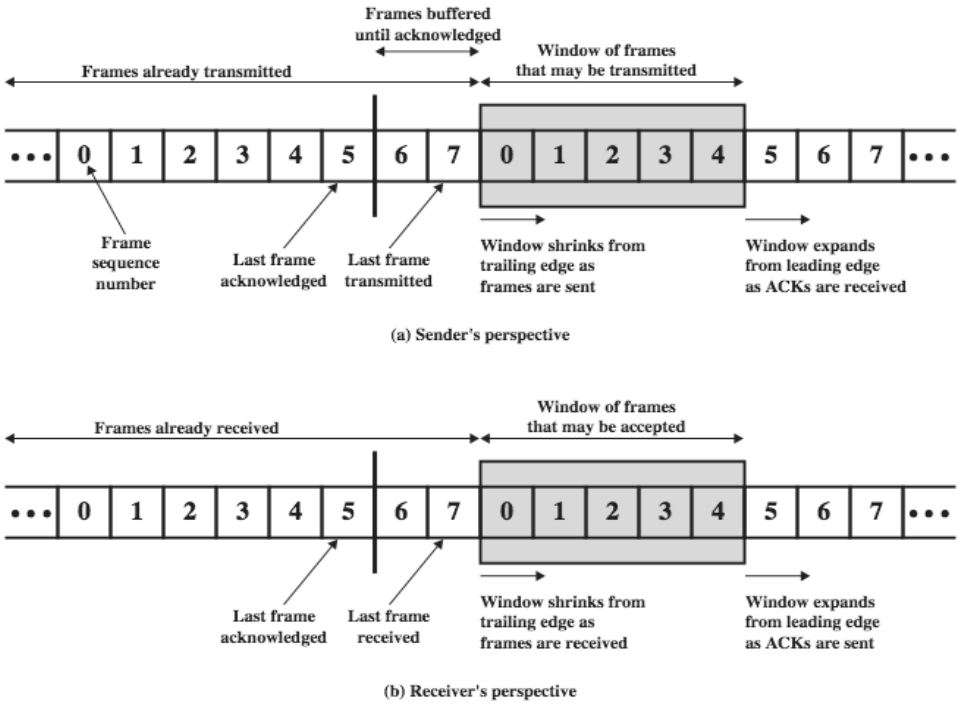


Figure: Sliding Window Diagram

Efficiency can be greatly improved by allowing multiple frames to be in transit at the same time. Consider two stations, A and B, connected via a full-duplex link. Station B allocates buffer space for W frames. Thus, B can accept W frames, and A is allowed to send W frames without waiting for any acknowledgments. To keep track of which frames have been acknowledged, each is labeled with a a k-bit sequence number. This gives a range of sequence numbers of 0 through $2^k - 1$, and frames are numbered modulo 2^k, with a maximum window size of $2^k - 1$. The window size need not be the maximum possible size for a given sequence number length k. B acknowledges a frame by sending an acknowledgment that includes the sequence number of the next frame expected. This scheme can also be used to acknowledge multiple frames, and is referred to as sliding-window flow control. Most data link control protocols also allow a station to cut off the flow of frames from the other side by sending a Receive Not Ready (RNR) message, which acknowledges former, frames but forbids transfer of future frames. At some subsequent point, the station must send a normal acknowledgment to reopen the window. If two stations exchange data, each needs to maintain two windows, one for transmit and one for receive, and each side needs to send the data and acknowledgments to the other. To provide efficient support for this requirement, a feature known as piggybacking is typically provided. Each data frame includes a field that holds the sequence number of that frame plus a field that holds the sequence number used for acknowledgment.

c) Using CRC a bit stream 1001011011 is to be transmitted. If the generator polynomial is $g(x)= 1+X^3+X^4$, find the transmitted code. In the received code by adding single error explain decoding procedure

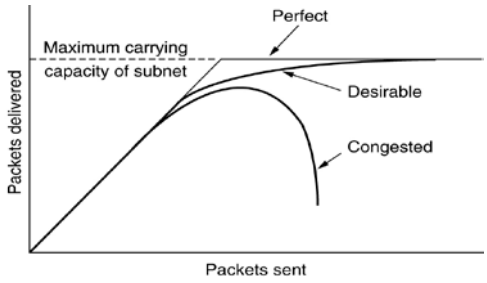
Ans: Frame:1001011011
Generator: 10011
Message after appending 4-zer bits: 10010110110000

```
                1100001010
            ____________________
10011  |  10010110110000
          10011
          -----
           10011
           10011
           -----
            00001
            00000
            -----
             00010
             00000
             -----
              00101
              00000
              -----
               01011
               00000
               -----
                10110
                10011
                -----
                 01010
                 00000
                 -----
                  10100
                  10011
                  -----
                   01110
                   00000
                   -----
                    1110   <-- remaider
```

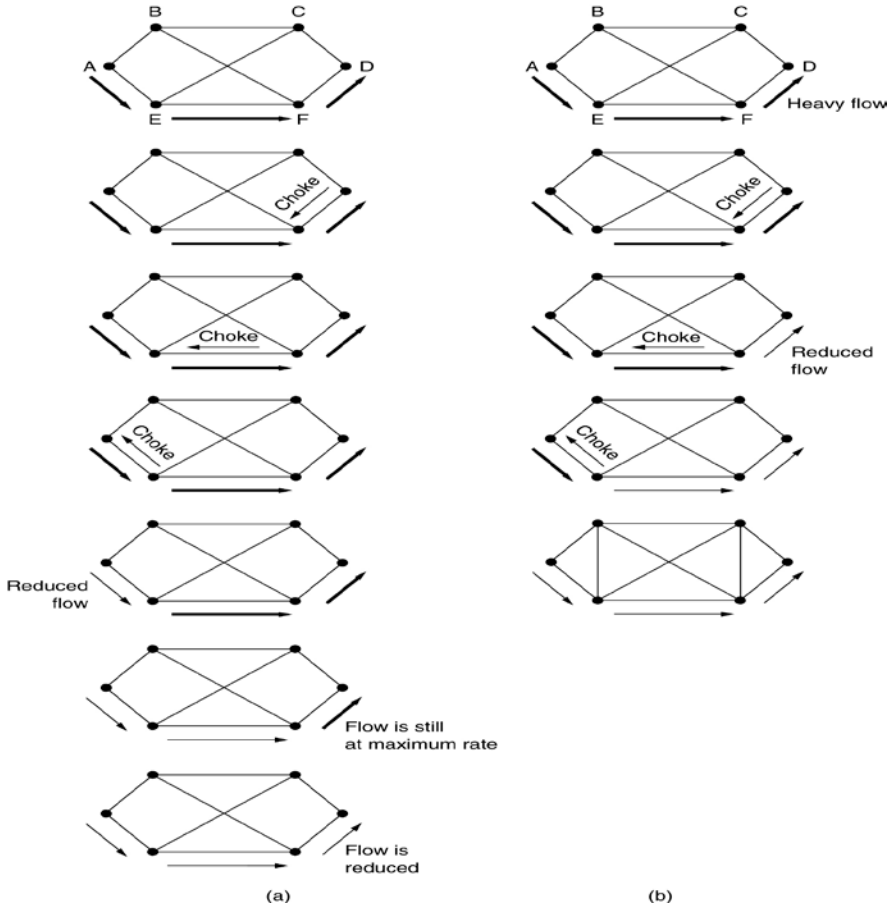
Transmitted frame is: 10010110111110
At the receiver to check error divide the received data [after adding single bit error] by the generator polynomial if the remainder is zero then there will be no error from the received data.

Q6a) What is congestion? Explain choke packet type of congestion control technique.

Ans: Congestion: In a network if the number of packets sent exceeds the capacity then the performance of the network will degrade, this condition is referred as congestion.



Choke packet: It is a technique used for congestion control. In this technique a choke packet is generated at a congestion node and transmitted back to the source node to restrict the traffic flow. An example of a choke packet is the ICMP source quench packet. Either a router or a destination end system may send this message to a source system, requesting that it reduce the rate at which it is sending traffic to the internet destination. On receipt of a source quench message, the source host should reduce its rate of transmission.



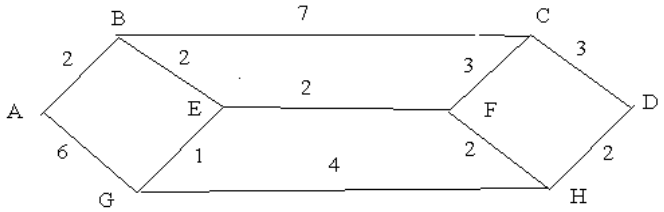
(a) A choke packet that affects only the source.
(b) A choke packet that affects each hop it passes through

b) Give the comparisons between circuit switching and datagram.

Ans: The comparisons are

Factors	Circuit Switching	Datagram
Path	Dedicated transmission path	No dedicated path
Data type	Continuous transmission data	Transmission of packets
Speed	Only path set up time is required	path set up time is not required
Storage of data	Message are not stored	Packets may be stored until delivered.
Routing	The same path is establishes for entire conversation	Each packet is routed independently.

c) Explain Dijkstra algorithm and using Dijkstra algorithm find the shorted path from A to D.



Ans:

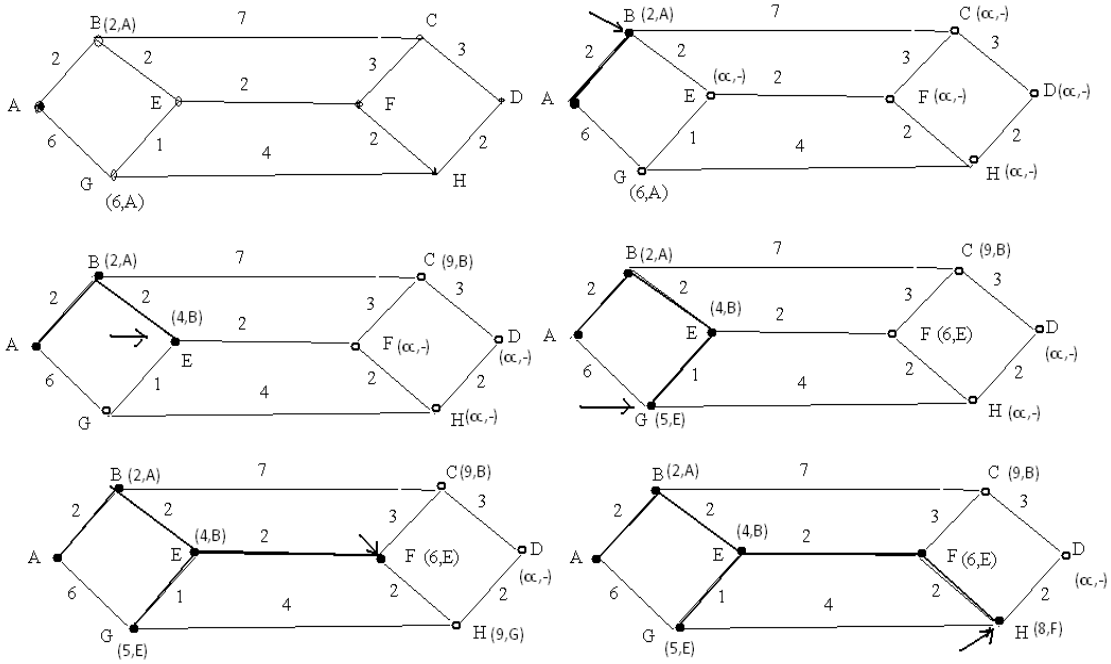
Dijkstra's algorithm:

Find the shortest paths from a given source node to all other nodes by developing the paths in order of increasing path length. The algorithm proceeds in stages. By the kth stage, the shortest paths to the k nodes closest to (least cost away from) the source node have been determined; these nodes are in a set T. At stage (k + 1), the node not in T that has the shortest path from the source node is added to T. As each node is added to T, its path from the source is defined

- Step 1 [Initialization]
  - T = {s} Set of nodes so far incorporated
  - L(n) = w(s, n) for $n \neq s$
  - initial path costs to neighboring nodes are simply link costs
- Step 2 [Get Next Node]
  - find neighboring node not in T with least-cost path from s
  - incorporate node into T
  - also incorporate the edge that is incident on that node and a node in T that contributes to the path
- Step 3 [Update Least-Cost Paths]
  - L(n) = min[L(n), L(x) + w(x, n)] for all n ϵ T

f latter term is minimum, path from s to n is path from s to x concatenated with edge from x to n

The shortest path from A to D is via ABEFHD as shown in the figures.



Q7a) Mention the functions of a bridge. Give an illustration of two LAN's by a bridge.

Ans: Page No 501 of Textbook (7th Edition)

b) Explain the working of CSMA/CA and CSMA/CD protocol

Ans: In CSMA, a station wishing to transmit has to first listen to the channel for a predetermined amount of time so as to check for any activity on the channel. If the channel is sensed "idle" then the station is permitted to transmit. If the channel is sensed as "busy" the station has to defer its transmission. This is the essence of both CSMA/CA and CSMA/CD..

- CSMA/CD (carrier sense multiple access/collision detection): CD (collision detection) defines what happens when two devices sense a clear channel, then attempt to transmit at the same time. A collision occurs, and both devices stop transmission, wait for a random amount of time, then retransmit.
- CSMA/CA (carrier sense multiple access/collision avoidance) : In CA (collision avoidance), collisions are avoided because each node signals its intent to transmit before actually doing so..

  [any one protocol]

c) Draw the architecture of IEEE 802.11 and explain its working. Mention any four services of IEEE 802.11

Ans: 17.3 of Textbook (7th Edition)

i). There must be no leading zero (045).
ii). There can be no more than four numbers.
iii). Each number needs to be less than or equal to 255.
iv). A mixture of binary notation and dotted-decimal notation is not

Q8a) With neat diagram explain IP-V4 header format

Ans:

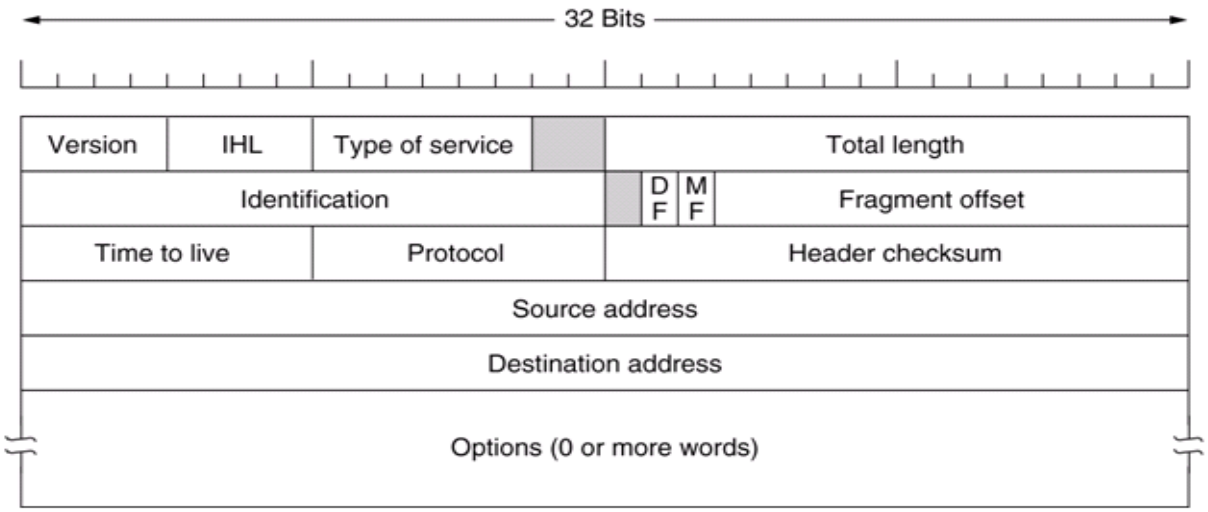


Fig: IP-4 header format

Figure shows the IP-4 header format. The IP header is built up in blocks of 32 bits. It will always be an integral number of 32-bit words. The IP header is divided up into fields.
The version field is 4 bits long. It indicates the release version of the IP that is used in this datagram.
The header length [IHL] field is 4 bits long. It identifies the length of the IP header in multiples of 32. The minimum value for a valid header is 5 (means 5*32Bit = 20 Bytes), Maximum is 15 (means 15*32Bit = 60 Bytes).
The Service Type TOS (Type of Service) Specifies the parameters for the type of service requested. The parameters may be utilized by networks to define the handling of the datagram during transport.

Total length. 16 bits contains the length of the datagram.

Identification: This field is needed to allow the destination host to determine which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same identification value.

DF: This flag indicates whether fragmentation is allowed or not. It is called the don't fragment (DF) bit. If the flag is set to 1 fragmentation is not allowed, and if it is set to 0 fragmentation is allowed. If the flag is set to 1, datagrams will be lost if they have to cross networks that can only handle smaller datagrams than the one presented to it. For this reason, it is prudent to set the flag to 0 and allow fragmentation.

MF: This flag is called the more fragments (MF) bit. It is used to indicate that there are more fragments to follow, so if a datagram is fragmented this is set on all but the last fragment. In the fragmentation process the header information in the original datagram must be copied into each of the fragments.

The fragment offset field is 13 bits long and is used to indicate the relative position of the fragment to the original datagram when fragmentation is carried out This is a 13-bit field, so offsets are calculated in units of 8 bytes, corresponding to the maximum packet length of 65,535 bytes. Using the identification number to indicate which message a receiving datagram belongs to, the IP layer on a receiving machine can then use the fragment offset to reassemble the entire message.

The TTL field indicates the "time to live" for the datagram. This field is used to limit packet lifetime. When it becomes zero, the packet is destroyed. The unit of time is second, allowing maximum lifetime of 255 sec.

The protocol field is 8 bits long and is used to identify the upper layer protocol that is to receive the IP data portion of the datagram. Higher- level protocol that provide data.
Source and destination address: The address is of 32 bits, which indicated both network address and host address. As the Internet address gets you to the correct host. The protocol identifier gets you to the correct service within the host.

The header checksum is 16 bits long. It holds the error check result for the entire header, which includes options, if they are present .

The option field is used for security, source routing, error reporting, debugging, time stamping and other information.

b) Compare IP-v4 and IPv6 protocol

Ans:

Subjects	IPv4	IPv6
Address Space	4 Billion Addresses	2^128
Configuration	Manual or use DHCP	Universal Plug and Play (UPnP) with or without DHCP
Broadcast / Multicast	Uses both	No broadcast and has different forms of multicast
Any cast support	Not part of the original protocol	Explicit support of anycast
Mobility	Uses Mobile IPv4	Mobile IPv6 provides fast handover, better router optimization and hierarchical mobility

c) Mention the type of address for the following IP address
i) 126.33.44.56:
ii) 195.55.23.96
iii)132.133.134.136
iv) 231.252.253.259

Ans:

i) 126.33.44.56: Class A
ii) 195.55.23.96: Class C
iii)132.133.134.136: Class B
iv) 231.252.253.259: Class D

- The characteristics of UDP are as follows
  - UDP service is unreliable
  - UDP does not guarantee the delivery of datagram to the destination
  - UDP does not required connection establishment prior to data transfer
  - UDP computes the checksum for the entire header plus data
  - No segmentation
  - No buffering

Q9a) Explain the working of User Datagram Protocol.

Ans:

The UDP header format is as shown in fig

0 1----------15----------31

Source Port number	Destination Port number
UDP length	checksum
Data	

UDP header is only 8 bytes long. Source Port number and Destination Port Number are two byte fields specifies the source and destination applications for the encapsulated data; UDP length indicates the length of the entire segment in bytes.
The checksum is optional in case of UDP, checksum covers the entire datagram (header + Data). When no checksums are used all the bits are set to 0's in the checksum field.

b) Explain MIME transfer encodings.

Ans: Page No. 722 of Textbook

c) Define the uses of the following domains:
1. info
2. museum
3. biz
4. pro
5. int

Ans: Page No. 741 of Textbook

TEXTBOOK

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