TABLE OF CONTENTS

Unit I

Unit II

Unit III

Unit IV

Unit V

Unit VI

Unit I

1 Data Communication and Network Models

1.1 : Introduction to Communication Theory

Q.1 Explain data communication and its components.

Ans. : Basics of data communication

- **Data communications** is the exchange of data between two devices by means of any transmission medium. The effectiveness of data communication system depends on three **fundamental characteristics** delivery, accuracy and timeliness.

1. **Delivery :** The data must be delivered to the intended device or user.
2. **Accuracy :** The data must be delivered accurately i.e. without alteration.
3. **Timeliness :** The system must deliver data in a timely manner.
4. **Jitter :** It refers to the variation in packet arrival time.

Data communication system

- A data communication system consists of five components.

1) Message 2) Sender 3) Receiver 4) Medium 5) Protocol

Fig. Q.1.1 shows components of data communication system.

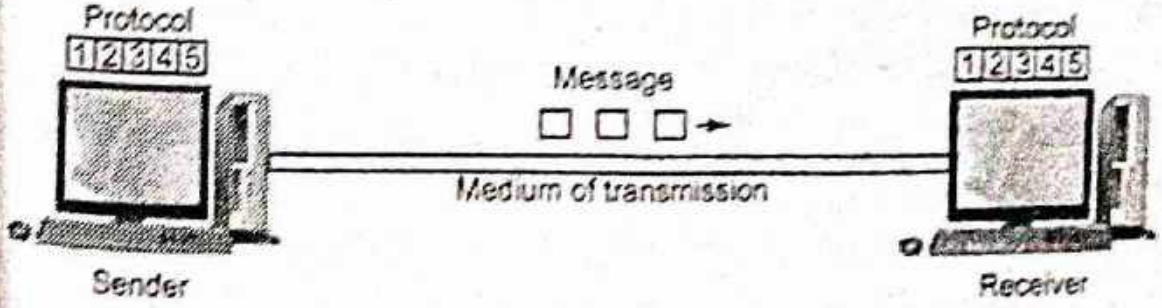


Fig. Q.1.1 Data communication components

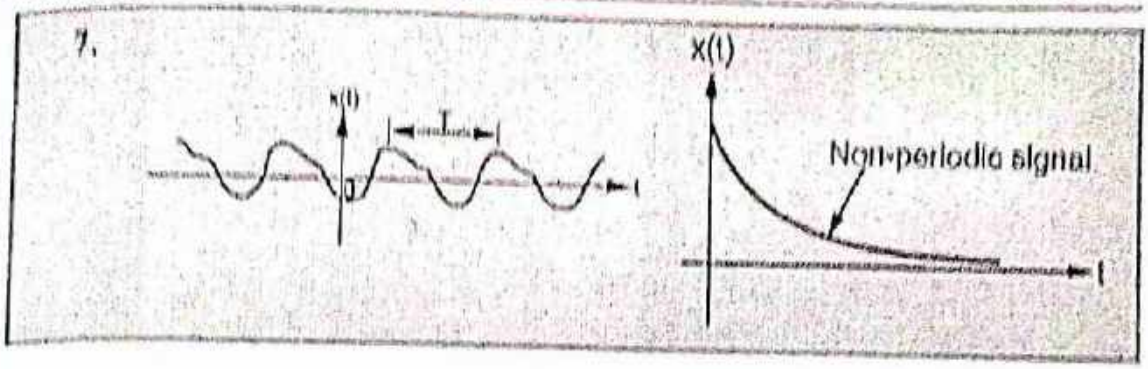
1. **Message :** The message is data or information to be communicated, can be text, numbers, pictures or sound.
2. **Sender :** The sender is device that sends data. Various devices can b used to send the data.
3. **Receiver :** The receiver receives the information/message transmitte by sender.
4. **Medium :** It is a physical path through which message passes fro sender to receiver. The transmission medium can be twisted-pair cable co-axial cable, fiber-optic cable or radiowaves.
5. **Protocol :** Protocol is a set of rules that governs data communications Protocol is a predecided terms for communication.

1.2 : Types of Signals

Q.2 Give comparison of periodic and aperiodic signals.

Ans. : Comparison of Periodic and Aperiodic Signals

Sr. No.	Periodic signal	Aperiodic signal
1.	A signal which repeats itself after a specific interval of time is called periodic signal.	A signal which does not repeat itself after a specific interval of time is called aperiodic signal.
2.	A signal that repeats its pattern over a period is called periodic signal.	A signal that does not repeats its pattern over a period is called aperiodic signal or non periodic..
3.	They can be represented by a mathematical equation.	They cannot be represented by any mathematical equation.
4.	Their value can be determined at any point of time.	Their value cannot be determined with certainty at any given point of time.
5.	They are deterministic signals	They are random signals
6.	Example : Since, cosine,square, sawtooth etc.	Example : Sound signals from radio, all types of noise signals.



1.3 : Signal Conversion Methods : A/D Conversion

Q.3 Draw and explain PCM and DM.

Sampling, Quantization, encoding. [SPPU : May-17,18, Dec.-17, Marks 7]

Or Explain pulse code modulation and delta modulation with suitable diagram. [SPPU : Dec.-19, Marks 6]

Ans. : PCM :

- The most common technique to change an analog signal to digital data is called pulse code modulation (PCM). With PCM, the pulses are of fixed length and fixed amplitude. PCM is a binary system where a pulse or lack of a pulse within a prescribed time slot represents either a logic 1 or a logic 0 condition.
- Fig. Q.3.1 shows a simplified block diagram of a single channel, simplex PCM system. The bandpass filter limits the frequency of the analog input signal to the standard voice band frequency range of 300 Hz to 3000 Hz.
- The analog signal is sampled every T_s where T_s is the sample interval or period. The inverse of the sampling interval is called the sampling rate or sampling frequency. The sample and hold circuit periodically samples the analog input signal and converts those samples to a multilevel PAM signal.
- The analog to digital converter converts the PAM samples to parallel PCM codes, which are converted to serial binary data in the parallel to serial converter and then outputted onto the transmission line as serial digital pulses.

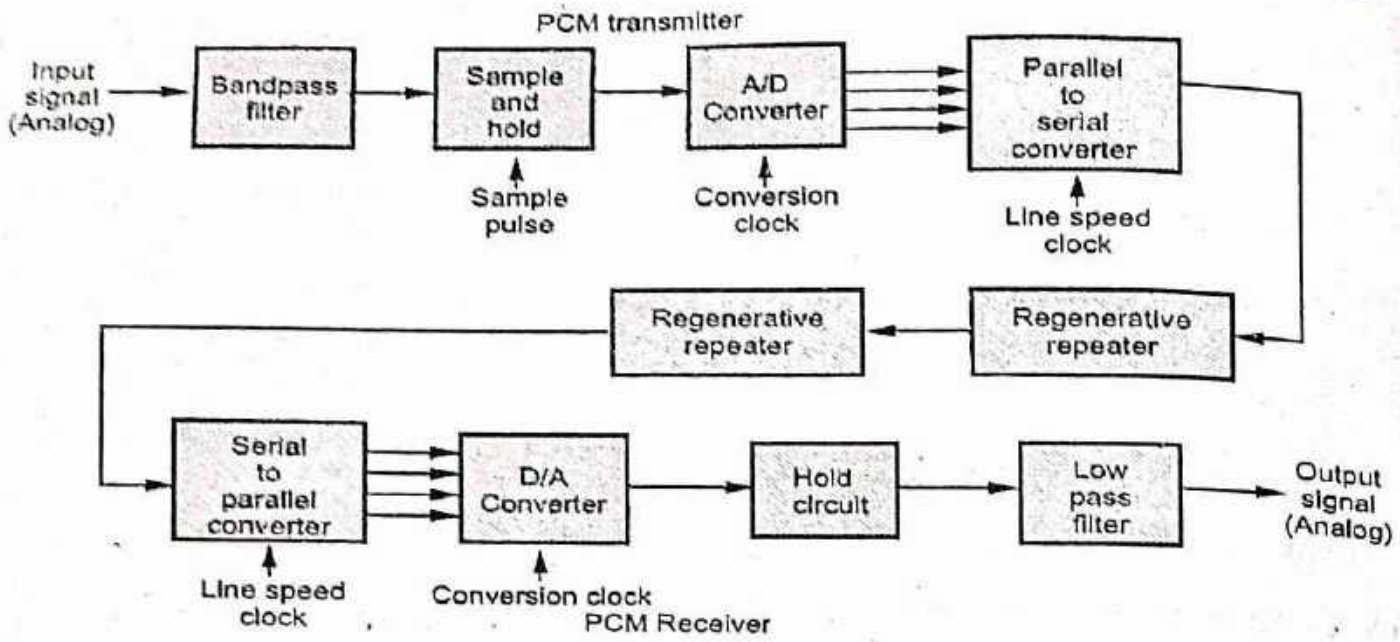
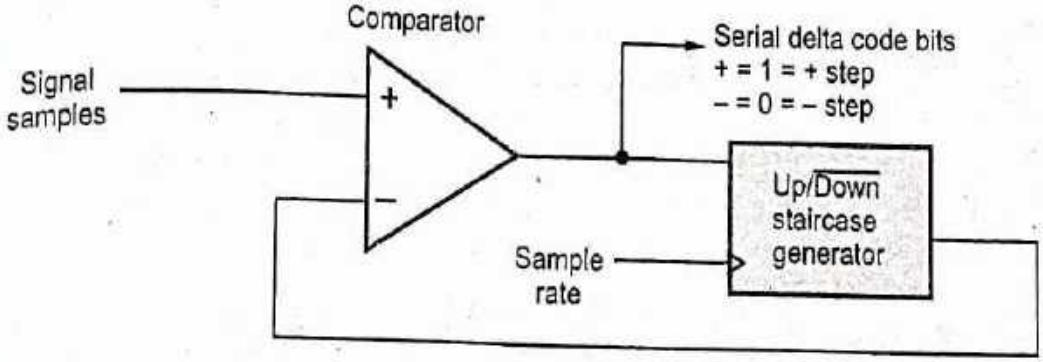


Fig. Q.3.1 PCM transmission system

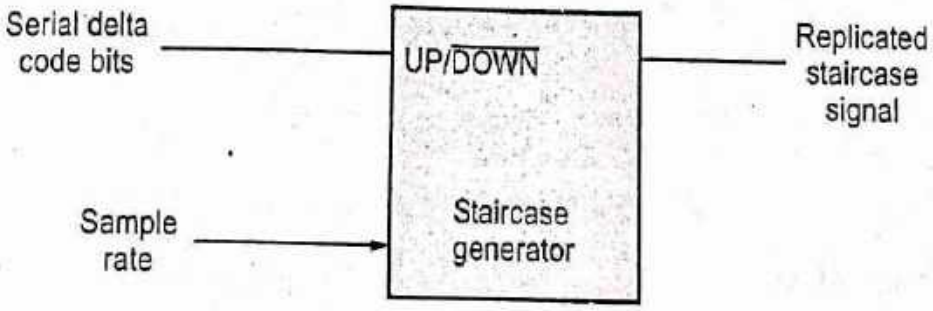
- Sampling methods are ideal, flat and natural.
- In ideal sampling, pulses from the analog signal are sampled. In natural sampling, a high speed switch is turned on for only the small period of time when the sampling occurs.

DM :

- Delta modulation minimize the effects of noise without increasing the number of bits being sent. This increases signal to noise ratio, improving system performance. Delta modulation take samples close enough to each other so that each samples amplitude does not vary by more than a single step size. Then instead of sending a binary code representing the step size, a single bit is sent signifying whether the sample size has increased or decreased by a single step.
- Fig. Q.3.2 shows the delta modulator and demodulator.
- Fig. Q.3.2 shows the functional block diagram. Samples from the original signal are compared to the output of a staircase generator. If the results of that comparison show the original signal to be larger than the staircase voltage, the comparator is set high. This is sent out as a logic 1 and causes the staircase generator to increase by a step. If the comparator indicates that the staircase voltage is greater than the



(a) Delta modulator



(b) Delta demodulator

Fig. Q.3.2 Delta modulator / demodulator

original signal, then the comparator goes low and causes the staircase generator to decrease by one step.

1.4 : D/A Conversion

Q.4 Explain the following shift keying techniques with suitable examples :

i) ASK ii) FSK iii) PSK ☞ **[SPPU : May-17, 18, Dec.-17, 19, Marks 7]**

Ans. : (I) ASK

- In ASK, the amplitude of carrier signal is varied in accordance with digital information, the frequency and phase remains constant.
- ASK is implemented using two levels only hence sometimes called as binary ASK or on-off keying. Fig. Q.4.1 shows binary ASK (BASK) waveform.

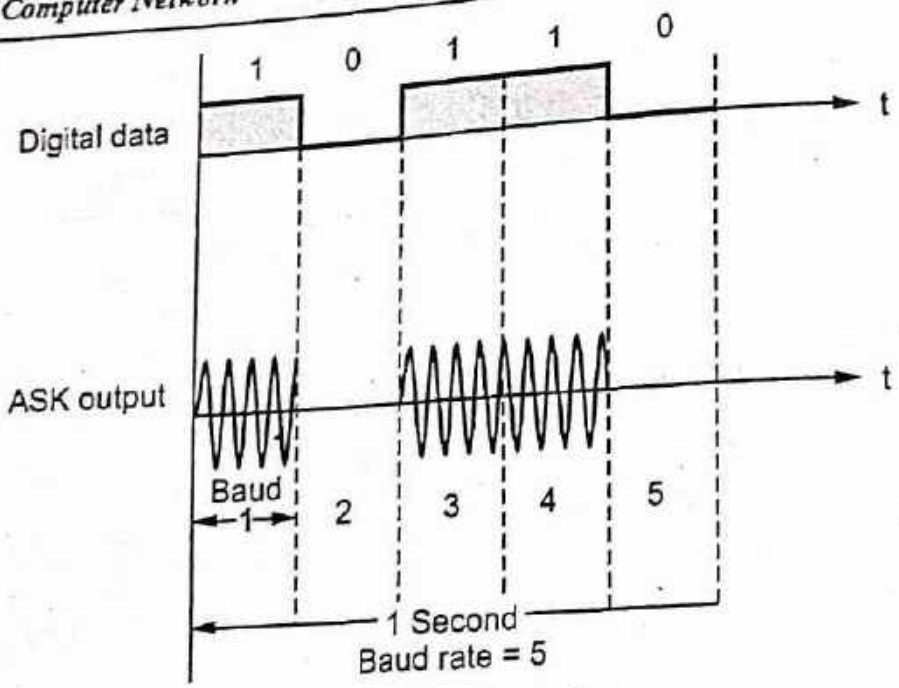


Fig. Q.4.1 ASK waveform

1. Bandwidth of ASK

- Actually, the bandwidth is proportional to the signal rate/baud rate but it depends on another factor d, that represents modulation and filtering process. The value of d is between 0 and 1.
- Bandwidth is given by :

$$B = (1+d)\ S$$

where,

S is signal rate and

B is bandwidth.

- Fig. Q.4.2 shows bandwidth of ASK.

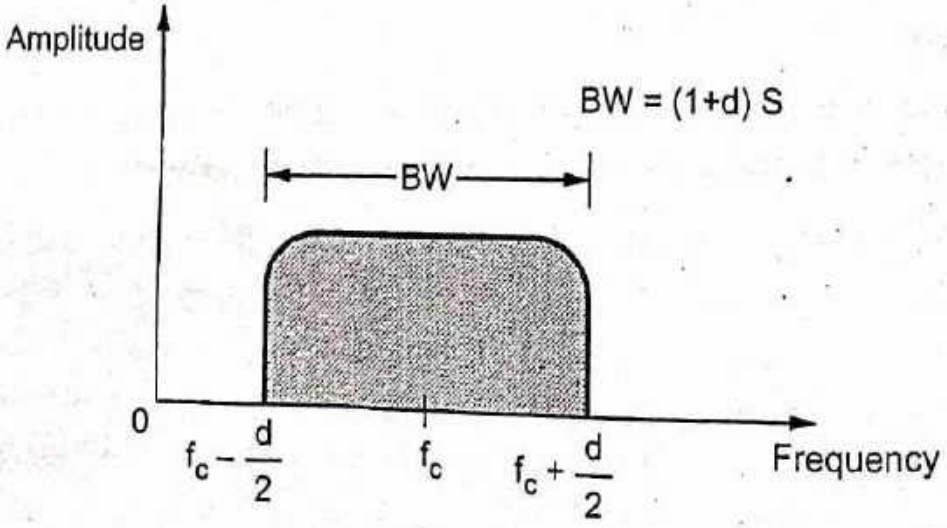


Fig. Q.4.2 BW of ASK

2. Implementation of ASK

- Fig. Q.4.3 shows simple implementation of ASK.

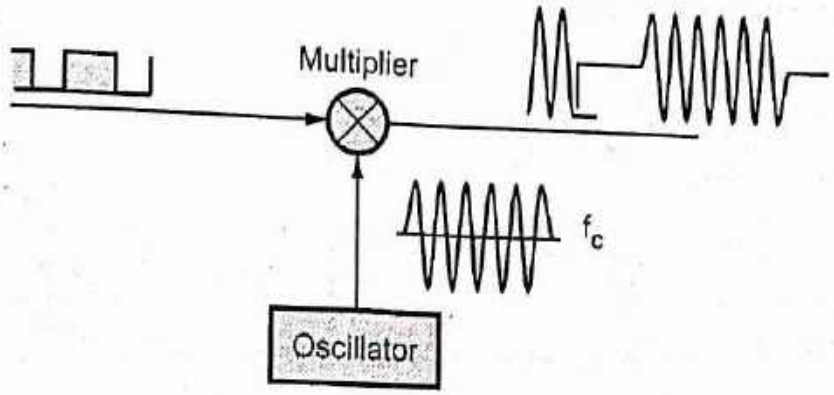


Fig. Q.4.3 Implementation of ASK

The digital data (unipolar NRZ) is multiplied by carrier signal generated by oscillator. When the amplitude of digital data is 1, the amplitude of carrier frequency is high, when the amplitude of digital data is 0, the carrier frequency amplitude becomes 0.

(ii) FSK

- In Frequency Shift Keying (FSK), the frequency of carrier signal is varied between two discrete values f_1 and f_2.
- When data element is 0, first carrier frequency f_1 is used and when data element is 1, second carrier frequency f_2 is used. Both carrier frequencies have same amplitude.
- Fig. Q.4.4 shows binary FSK waveforms.

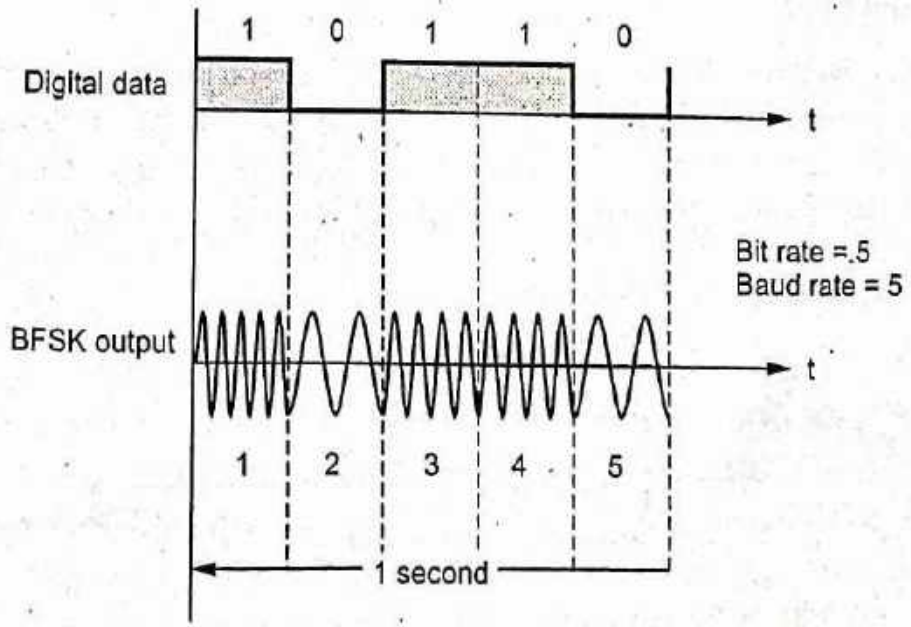


Fig. Q.4.4 FSK waveform

1. Bandwidth of BFSK

- The FSK modulation creates a nonperiodic composite signal. Fig. Q.4.5 shows frequency spectrum of FSK.

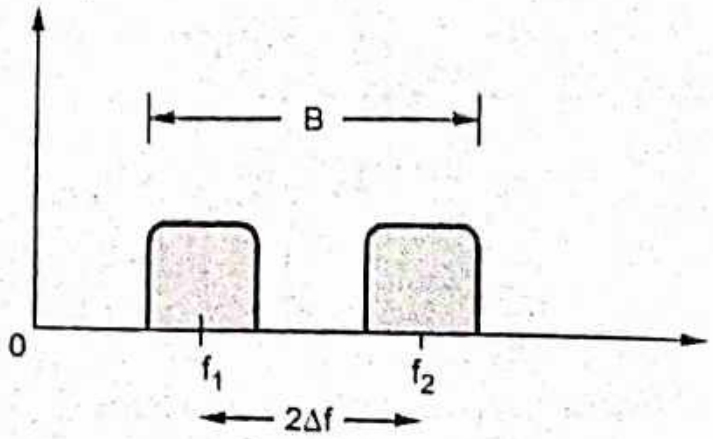


Fig. Q.4.5

- f_1 and f_2 are center frequencies of two carrier signal. If the difference between f_1 and f_2 is $2\Delta f$. The bandwidth expression can be written as -

$$B = (1+d)S + 2\Delta f$$

2. Implementation of BFSK

- There exists two variations of BFSK implementation noncoherent and coherent.

1) Noncoherent BFSK : In noncoherent BFSK, there is discontinuity in the phases of two consecutive signal element. The noncoherent BFSK is implemented by treating BFSK as two ASK modulations and using two carrier frequencies.

2) Coherent BFSK : In coherent BFSK, the phase continues through the two consecutive signal elements. The coherent BFSK can be implemented by using Voltage Controlled Oscillator (VCO) that changes its input frequency according to input voltage. Fig. Q.4.6 illustrate this implementation.

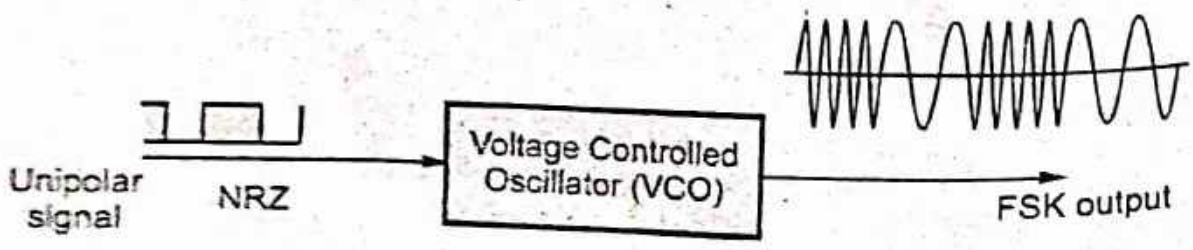


Fig. Q.4.6 Coherent BFSK implementation

The input to VCO is unipolar NRZ signal, when its amplitude is zero, the output has normal frequency and when input signal amplitude is high the frequency is increased.

(III) PSK

- The BPSK scheme is two level modulation scheme as therefore it represents two states of digital data (0 and 1), it decreases the baud rate and bandwidth.
- When BPSK uses two separate modulations one is in phase and other is out of phase (quadrature). Hence the scheme is called quadrature PSK or QPSK.
- Fig. Q.4.7 shows the QPSK waveform.

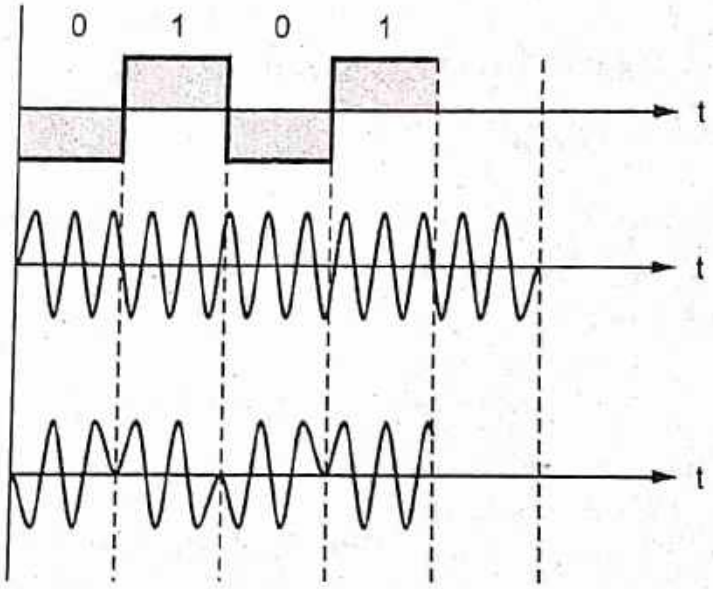


Fig. Q.4.7 QPSK waveform

Constellation diagram

- Constellation diagram specifies the amplitude and phase of a signal element. The signal element is represented as a dot. The bit or combination of bits it carry is written near the dot.
- Constellation diagram has two axes. X-axis represents carrier in-phase and Y-axis represents quadrature (out-of-phase) carrier. The projection of dot on X-axis gives amplitude of in-phase component. The projection of dot on Y-axis gives amplitude of quadrature components.

- Fig. Q.4.8 shows the concept of constellation diagram.

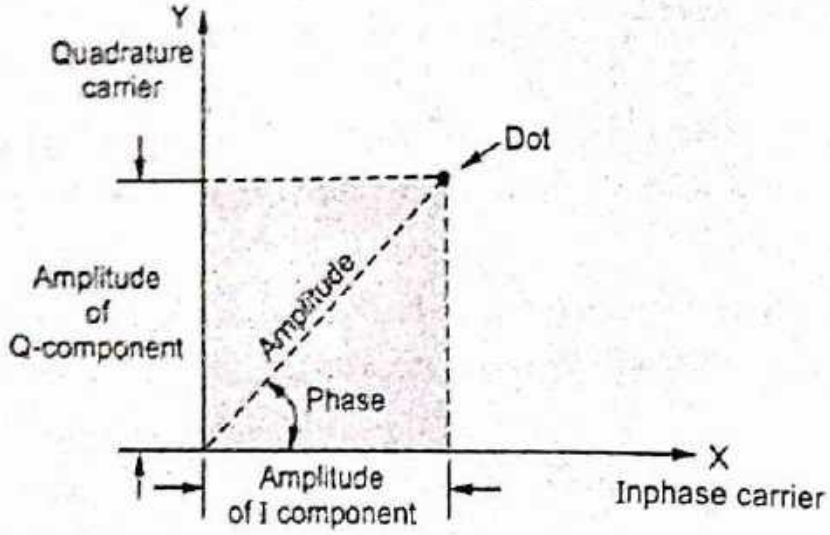


Fig. Q.4.8 Concept of constellation diagram

Constellation diagram of ASK

- Only one in-phase carrier is used. Two points on same axis.

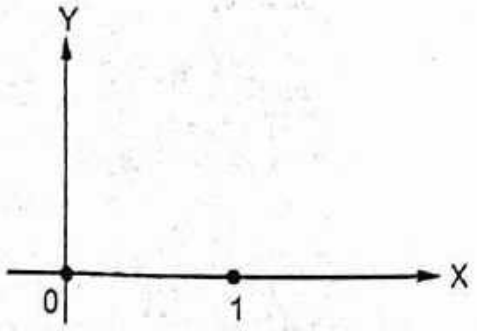


Fig. Q.4.9 Constellation diagram of ASK

Constellation diagram of BPSK

- Only one in-phase carrier is used. A polar NRZ modulation creates two opposite signal element.

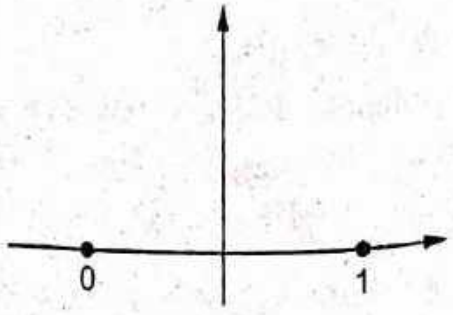


Fig. Q.4.10 Constellation diagram of BPSK

Constellation diagram of QPSK

QPSK uses two carriers in opposite phases.

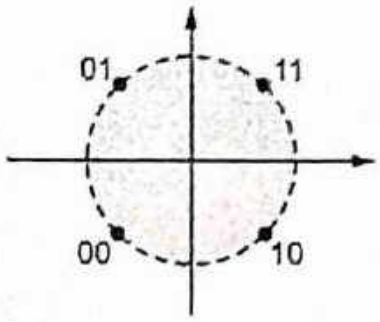


Fig. Q.4.11 Constellation diagram of QPSK

1.5 : A/A Conversion

Q.5 With the help of diagram explain AM. Write mathematical expression of AM modulated signal. ☞ **[SPPU : May-18, Dec.-19, Marks 6]**

Or What is an AM wave ? Derive a mathematical expression for AM wave. ☞ **[SPPU : Dec.-18, Marks 6]**

Ans. : • In amplitude modulation, it is the voltage level of the signal to be transmitted that changes the amplitude of the carrier in proportion.

- Fig. Q.5.1 (See Fig. Q.5.1 on next page) shows amplitude modulation.
- With no modulation, the AM carrier is transmitted by itself. When the modulating information signal (a sine wave) is applied, the carrier amplitude rises and falls in accordance. The carrier frequency remains constant during amplitude modulation.
- Amplitude modulation or AM as it is often called, is a form of modulation used for radio transmissions for broadcasting and two-way radio communication applications.
- The amplitude of a sinusoidal signal with fixed frequency and phase is varied in proportion to a given signal is called as **amplitude modulation.**
- In the modulation process, some characteristic of a high-frequency carrier signal (bandpass), is changed according to the instantaneous amplitude of the information (baseband) signal.

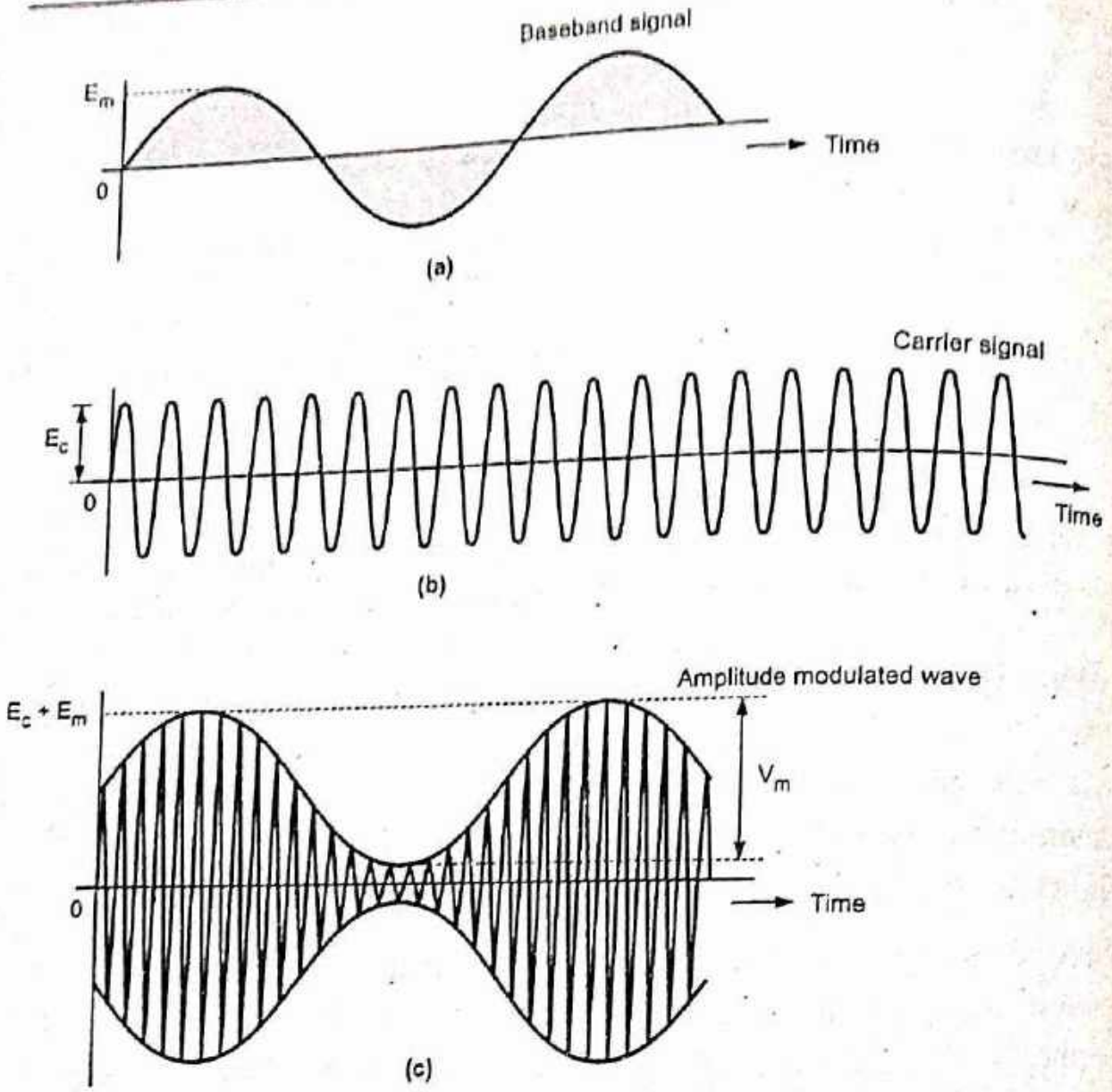


Fig. Q.5.1 (a) Sinusoidal modulating signal
(b) Sinusoidal high frequency carrier
(c) Amplitude modulated signal

- The amplitude of high-carrier signal is varied according to the instantaneous amplitude of the modulating message signal m(t). An AM signal is made up of a carrier (with constant frequency) in which its amplitude is changed (modulated) with respect to the signal (modulating signal) we wish to transmit (voice, music, data, binary).
- AM is the process of changing the amplitude of a relatively high frequency carrier signal in proportion to the instantaneous value of the modulating signal. It is relatively inexpansive, low quality form of

modulation that is used for commercial broadcasting of both audio and video signals.

- AM is also used for two way mobile radio communications, such as citizens band radio.
- AM modulators are two input devices. One input is a single, relatively high frequency carrier signal of constant amplitude, and the second input is comprised of relatively low frequency information signals that may be a single frequency or a complex waveform made up of many frequencies.
- The modulating signal modulates amplitude, frequency or phase of the carrier according to its variations in amplitude. This results in amplitude, frequency or phase modulation. The frequency and phase modulation is also called angle modulation.
- When the amplitude of the modulating signal is greater than the amplitude of the carrier, distortion will occur, causing incorrect information to be transmitted. In amplitude modulation, it is particularly important that the peak value of the modulating signal be less than the peak value of the carrier.

emodulation of AM Signals

Demodulation extracting the baseband message from the carrier. There are two main methods of AM demodulation :

1. Envelope or non-coherent detection or demodulation.
2. Synchronised or coherent demodulation.

dvantages of AM :

Simple implementation.

Less complex circuitry.

Cheaper components so easy to build AM transmitter and receiver.

sadvantages of AM :

- Power usage in modulation is not efficient.
- Bandwidth requirement is very high.
- Prone to noise and hence AM transmission is highly noisy.
- Difficult to tune in absence of the carrier.

Amplitude modulation techniques :
1. Double Sideband Suppressed Carrier (DSBSC)
2. Double Sideband Full Carrier (DSBFC)
3. Single Sideband (SSB)

Q.6 A carrier of 1000 W is modulated with a resulting modulation index of 0.8. What is the total power ? [SPPU : Dec.-17, Marks 6]

Ans. :

$$P_t = P_c\left(1 + \frac{\mu^2}{2}\right)$$

$$P_t = 1000\left(1 + \frac{0.8^2}{2}\right)$$

$$P_t = 1320 \text{ Watt}$$

Q.7 Draw frequency domain representation of AM wave. A standard AM broadcast station is allowed to transmit modulating frequencies upto 5 kHz. If the AM station is transmitting on a frequency of 920 kHz, what are sideband frequencies and total bandwidth ?

[SPPU : Dec.-17, Marks 6]

Ans. : Sideband frequencies are,

$$f_{USB} = f_c + f_m = 920 + 5 = 925 \text{ kHz}$$

$$f_{LSB} = f_c - f_m = 920 - 5 = 930 \text{ kHz}$$

$$\text{Total BW} = 2f_m = 2 \times 5 \text{ kHz} = 10 \text{ kHz}$$

Q.8 What is FM ? Derive a mathematical expression for FM wave.

[SPPU : May-19, Marks 6]

Ans. : • In Frequency Modulation (FM), the frequency of the carrier is varied according to amplitude variations in the modulating signal. But the amplitude of the frequency modulated signal remains constant. The frequency modulated carrier by sinusoidal modulation is shown in Fig. Q.8.1.

• When the modulating signal has zero amplitude, then the carrier has frequency of ω_c or f_c. As the amplitude of the modulating signal increases, the frequency of the carrier increases. Similarly, as the amplitude of the modulating signal is decreased, the frequency of carrier

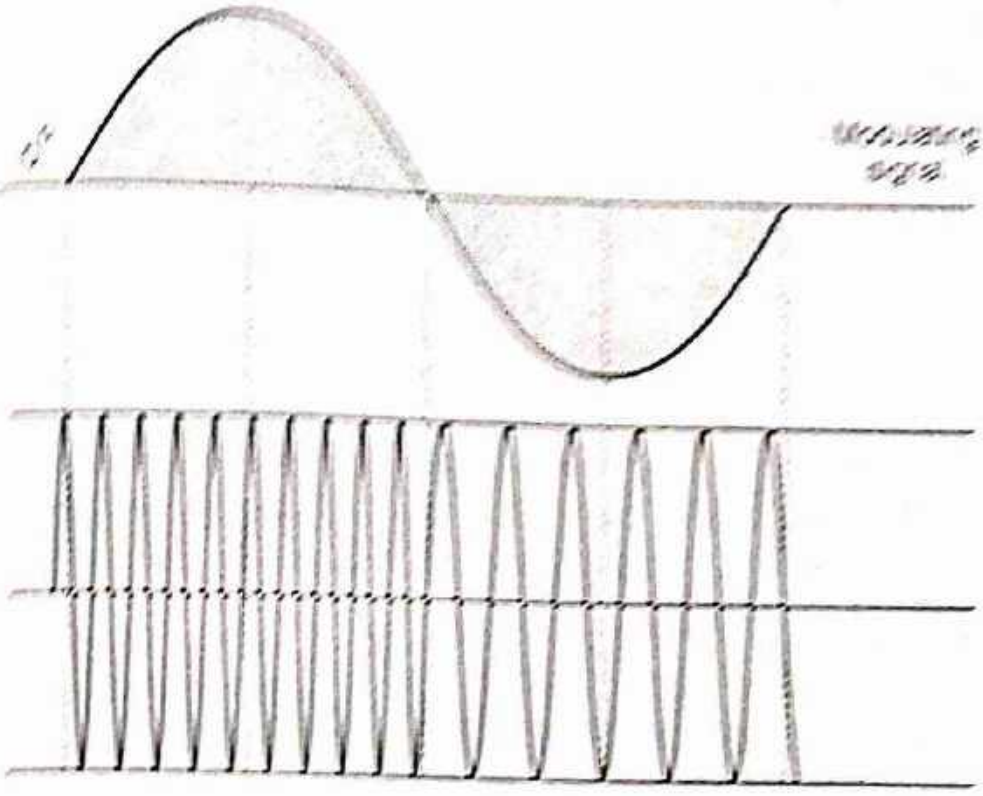


Fig. Q.8.1 Frequency modulation

is also decreased. Observe in Fig. Q.8.1 that the amplitude of frequency modulated carrier is constant.

- The mathematical equation of the FM signal is given as

$$e_{FM} = E_c \sin (\omega_c t + m_f \sin \omega_m t) \quad \ldots (Q.8.1)$$

Here e_{FM} is the instantaneous amplitude of FM signal.

E_c is maximum amplitude of the signal.

ω_c is the carrier frequency.

ω_m is the modulating frequency.

and m_f is the modulating index of FM.

1.6 : Multiplexing Techniques

Q.9 What is TDM ? Draw and explain TDM multiplexing and demultiplexing process. ☞ [SPPU : May-18, 19, Marks 6]

Ans. : • In a Time Division Multiplexing (TDM) system, a single path and carrier frequency is used. TDM is a digital technology. Each user is assigned a unique time slot for their operation. A central switch, or

multiplexer, goes from one user to the next in a specific, predictable sequence and time.

- TDM system 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. TDM is more efficient than FDM, in that it does not require guard bands and it operate directly in digital form.
- In TDM, the transmission between the multiplexers is provided by a single high speed digital transmission line. Each connection produce a digital information flow that is then inserted into the high speed line.
- A TDM system is a serial system, because the signal from each user follows, in time, the signal from another user. The overall bandwidth of the TDM result in much wider than the bandwidth of any individual user signal. This is because the TDM output is carrying much more information, and information requires bandwidth. The final bandwidth is approximately equal to the sum of the bandwidths of the individual signals.

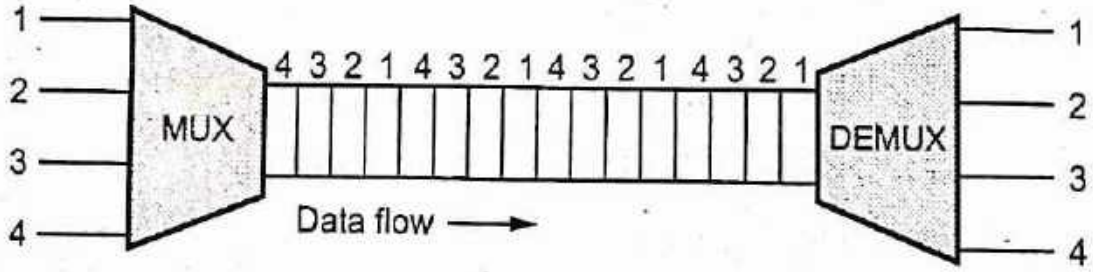


Fig. Q.9.1 TDM

- TDM is an alternative technique for splitting a big channel into many little channels. One modem would be used for the overall bandwidth W. Given m equal rate streams of binary data to be transmitted, the m bit streams would be multiplexed together into one bit stream. This is done by sending the data in successive frames. Each frame contains m slots, one for each bit stream to be multiplexed.
- The two basic forms of TDM are :
  1) Synchronous Time Division Multiplexing (STDM)
  2) Asynchronous Time Division Multiplexing (ASTDM) or statistical TDM (STATDM).

Q.10 Explain FDM multiplexing with their advantages and disadvantages.

☞ [SPPU : Dec.-19, Marks 6]

Ans. : • Frequency Division Multiplexing (FDM) is an analog multiplexing technique that combines analog signals.

- A number of signals can be carried simultaneously if each signal is modulated onto a different carrier frequency.
- In short, in FDM, the bandwidth is divided into a number of frequency slots, each of which can accommodate the signal of an individual connections.
- The most common examples of this are AM, FM and TV broadcasting, in which each station uses a different frequency band.
- An another example, voice grade channels are often frequency multiplexed together in the telephone network.
- In these examples, each multiplexed signal is limited to its own allocated frequency band to avoid interference with the other signals.
- FDM can be viewed as a technique for splitting a big channel into many little channels. Suppose that a physical channel has a usable bandwidth of m hertz and we wish to split it into n equal FDM subchannels, then each subchannel has m/n hertz available and thus m/n available quadrature samples per second for sending data.
- Fig. Q.10.1 shows the concept of FDM.

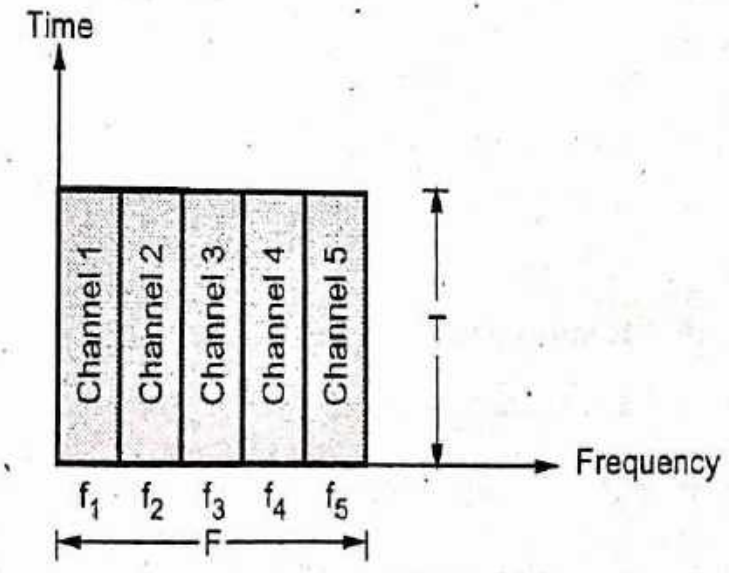


Fig. Q.10.1 Concept of FDM

• Fig. Q.10.2 illustrates FDM technique.

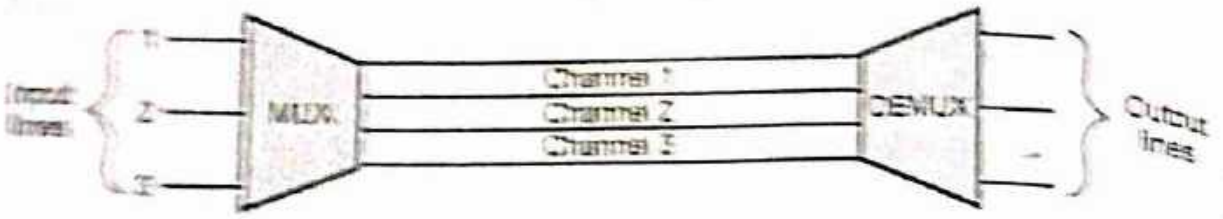


Fig. Q.10.2 FDM techniques

1.7 : Data Rate Limits

Q.11 Explain (i) Nyquist Bit Rate (ii) Shannon Capacity.

Ans. : (i) Nyquist bit rate

• Nyquist bit rate defines the theoretical maximum bit rate for a noiseless channel or ideal channel.

The formula for maximum bit rate in bits per second (bps) is :

$$\text{Maximum bit rate} = 2 \times BW \times \log_2 L$$

where, BW = Bandwidth of channel

L = Number of signal levels used to represent data.

(ii) Shannon capacity

• An ideal noiseless channel never exists. The maximum data rate for any noisy channel is :

$$C = BW \times \log_2\left(1 + \frac{S}{N}\right)$$

where,

C = Channel capacity in bits per second

BW = Bandwidth of channel

$\frac{S}{N}$ = Signal to noise ratio

The channel capacity is also called as Shannon capacity. The channel capacity do not depend upon the signal levels used to represent the data.

Q.12 Calculate the maximum bit rate of channel having bandwidth 1200 Hz if : i) S/N ratio is 0 dB ii) S/N ratio is 20 dB.

☞ [SPPU : May-17, Marks 7]

Ans. : BW = 1200 Hz

i) S/N = 0 dB

i.e. $0 = 10\log\left(\frac{S}{N}\right)$

$$\frac{S}{N} = 1$$

Maximum bit rate

$$C = BW \times \log_2\left(1 + \frac{S}{N}\right) = 1200 \times \log_2\left(1 + \frac{S}{N}\right)$$

$$= 1200 \times \log_2 (1 + 1)$$

$$= 1200 \times \left[\frac{\log_{10}(2)}{\log_{10}(2)}\right]$$

$$C = 1200 \text{ bits/sec.}$$ ... Ans.

ii) S/N = 20 dB

$$20 \text{ dB} = 10\log\left(\frac{S}{N}\right)$$

$$\frac{S}{N} = 100$$

$$C = BW \times \log_2\left(1 + \frac{S}{N}\right)$$

$$= 1200 \times \log_2 (1 + 100)$$

$$C = 1200 \times \left[\frac{\log_{10}(101)}{\log_{10}(2)}\right]$$

$$C = 7989.8$$

$$C \approx 7990 \text{ bits/sec.}$$ ...Ans.

Q.13 The power of signal is 10 mW and the power of noise is 1 μW. What are the values of SNR and SNR_{dB} ? ☞ [SPPU : Dec.-17, Marks 6]

Ans. :

$$SNR = \frac{10mW}{1\mu W} = 10,000$$

$$SNR_{dB} = 10 \log SNR$$

$$SNR_{dB} = 10 \log (10,000)$$

$$= 40 \text{ dB}$$

...Ans.

1.8 : Topologies

Q.14 Explain: (i) Star topology (ii) Ring topology (iii) Mesh topology

Ans. : (i) Star topology

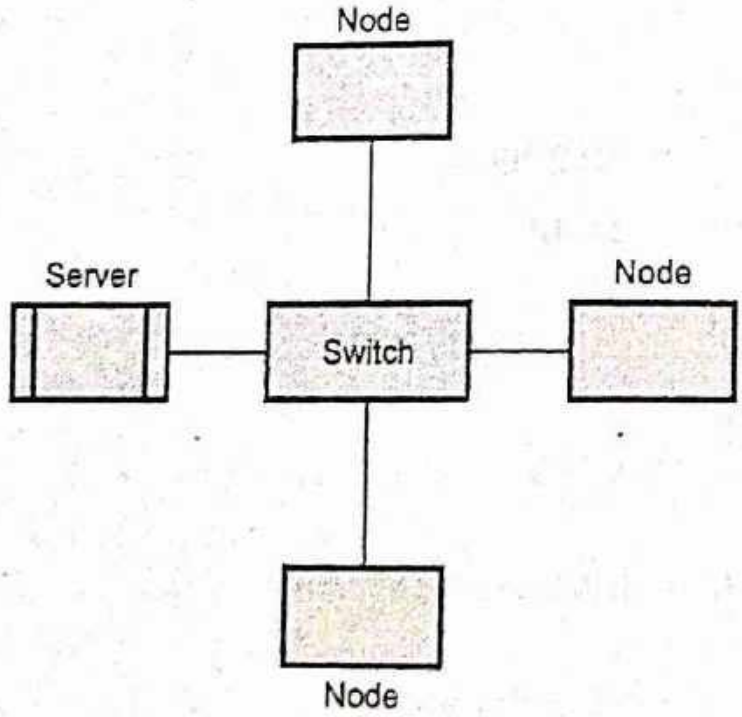


Fig. Q.14.1 Star topology

- A star topology consists of a number of devices connected by point-to-point links to a central hub.
- Easy to control and traffic flow is simple.
- Data travels from the sender to central hub and then to the receiver.

Advantages of star topology :

1) It is easy to modify and add new nodes to a star network without disturbing the rest of the network.
2) Troubleshooting techniques are easy.
3) Failures of any node do not bring down the whole star network.

Disadvantages of star network :

1) If the central hub fails, the whole network fails to operate.
2) Each device requires its own cable segment.
3) Installation can be moderately difficult, especially in the hierarchical network.

(ii) Ring topology

- In a ring topology, each computer is connected to the next computer, with the last one connected to the first. The signals travel on the cable in only one direction. Since each computer retransmits what it receives.
- Ring is an active network. Termination is not required.

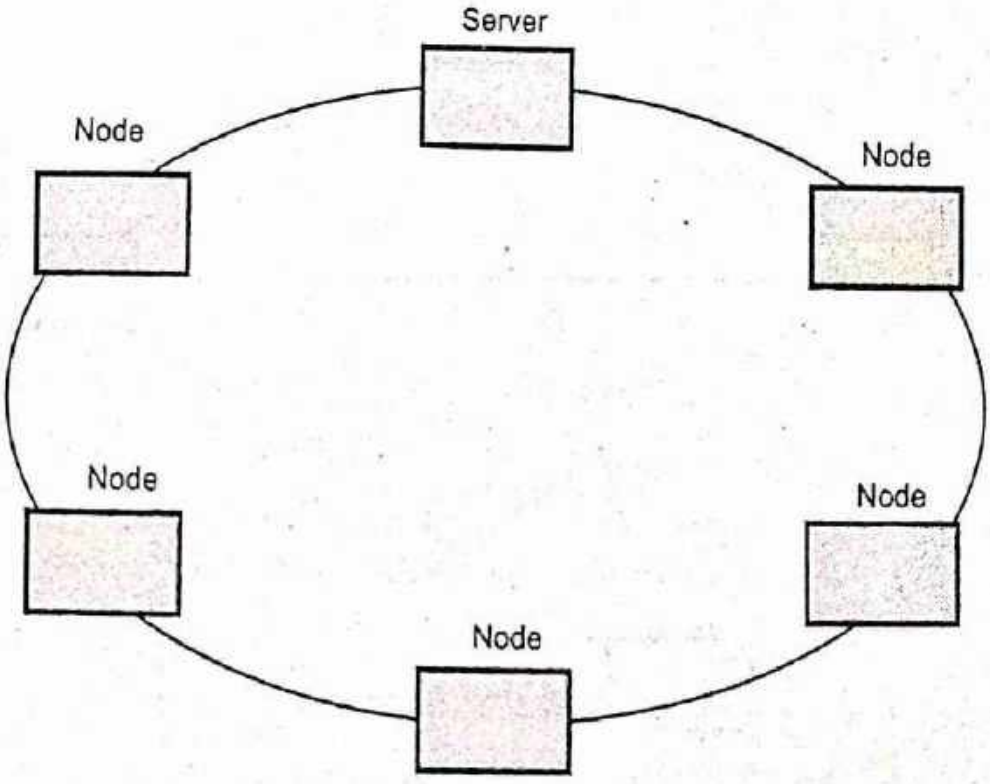


Fig. Q.14.2 Ring topology

Advantages of ring :

1) Cable failures are easily found.
2) Because every node is given equal access to the token, no one node can monopolize the network.

Disadvantages of ring :

1) Adding or removing nodes disrupts the network.
2) It is difficult to troubleshoot a ring network.
3) Failure of one node on the ring can affect the whole network.
4) Cost of cable is more in ring network.

(iii) Mesh topology

- The mesh topology has a link between each device in the network. It i more difficult to install as the number of devices increases.
- Mesh networks are easy to troubleshoot.
- Much of the bandwidth available in mesh configuration is wasted.
- Most mesh topology networks are not true mesh networks. Rather, the are hybrid mesh networks, which contain some most important site with multiple links.

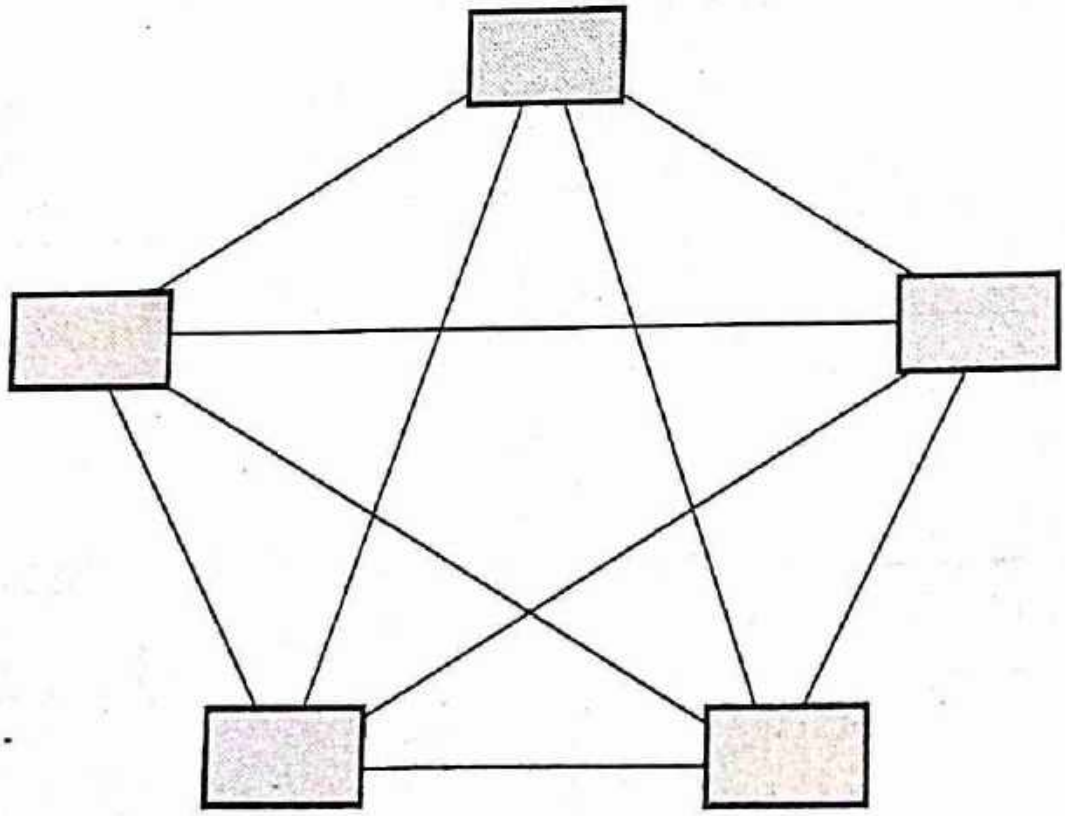


Fig. Q.14.3 True mesh topology

Advantages of Mesh :

1) Troubleshooting is easy. 2) Isolation of network failures is easy.

Disadvantages of mesh :

1) Difficulty of installation.
2) Costly because of maintaining redundant links.
3) Difficulty of reconfiguration.

1.9 : Noise

Q.15 Explain: (i) Thermal noise (ii) Intermodulation noise

Ans. : (i) Thermal noise

- Thermal noise is due to thermally agitated electrons in a conductor. As temperature increases more electrons and hence noise is generated.
- Since thermal noise is uniformally distributed across the frequency spectrum, therefore it is also called as **white noise.**
- Thermal noise is for bandwidth of W Hz is given by :

$$N = kTW$$

where, k = Boltzmann's constant = 1.3803×10^{-23} J/°K

T = Temperature in Kelvin

N = Noise in watt

(ii) Intermodulation noise

- Intermodulation noise is generated when signals of different frequencies share the same transmission medium.
- Because of intermodulation noise, different frequencies are produced which are sum, difference and multiplication of two frequencies.
- Intermodulation of signals take place when there is component malfunction such as nonlinearity in transmitter, receiver or in repeater. Another cause of intermodulation noise is use of excessive signal strength.

1.10 : Network Models

Q.16 Draw ISO/OSI model and explain functions of the following layers :
1) Physical 2) Data link 3) Network layer. ☞ [SPPU : Dec.-18, Marks 6]

Ans. : OSI model : • The ISO was one of the first organizations to formally define a common way to connect computers. Their architecture, called the Open System Interconnection (OSI).

- The International organization for standardization developed the **Open System Interconnection (OSI)** reference model. OSI model is the most widely used model for networking.
- OSI model is a seven layer standard.
- The OSI model does not specify the communication standard or protocols to be used to perform networking tasks.
- OSI model provides following services.
  1) Provides peer-to-peer logical services with layer physical implementation.
  2) Provides standards for communication between system.
  3) Defines point of interconnection for the exchange of information between system.
  4) Each layer should perform a well defined function.
  5) Narrows the options in order to increase the ability to communicate without expansive conversions and translations between products.

Principles in defining OSI layers

- Following principles are used in defining the OSI layers.
  1. Do not create so many layers as to make the system engineering task of describing and integrating the layers more difficult than necessary.
  2. Create a boundary at a point where the description of services can be small and the number of interrelations across the boundary are minimized.
  3. Create separate layers to handle function that are manifestly different in the process performed.

4. Collect similar functions into the same layer.
5. Select the boundaries at a point which past experience has demonstrated to be successful.
6. Create a layer of easily localized functions so that the layer could be totally redesigned and its protocols changed in a major way to take advantage of new advances in architecture, hardware or software technology without changing the services expected from and provided to the adjacent layers.
7. Create a boundary where it may be useful at some points in time to have the corresponding interface standardized.
8. Create a layer where there is a need for a different level of abstraction in the handling of data.
9. Allow changes of functions or protocols to be made within a layer without affecting other layers.
10. Create for each layer boundaries with its upper and lower layer only.

- Fig. Q.16.1 shows the OSI 7 layer reference model.

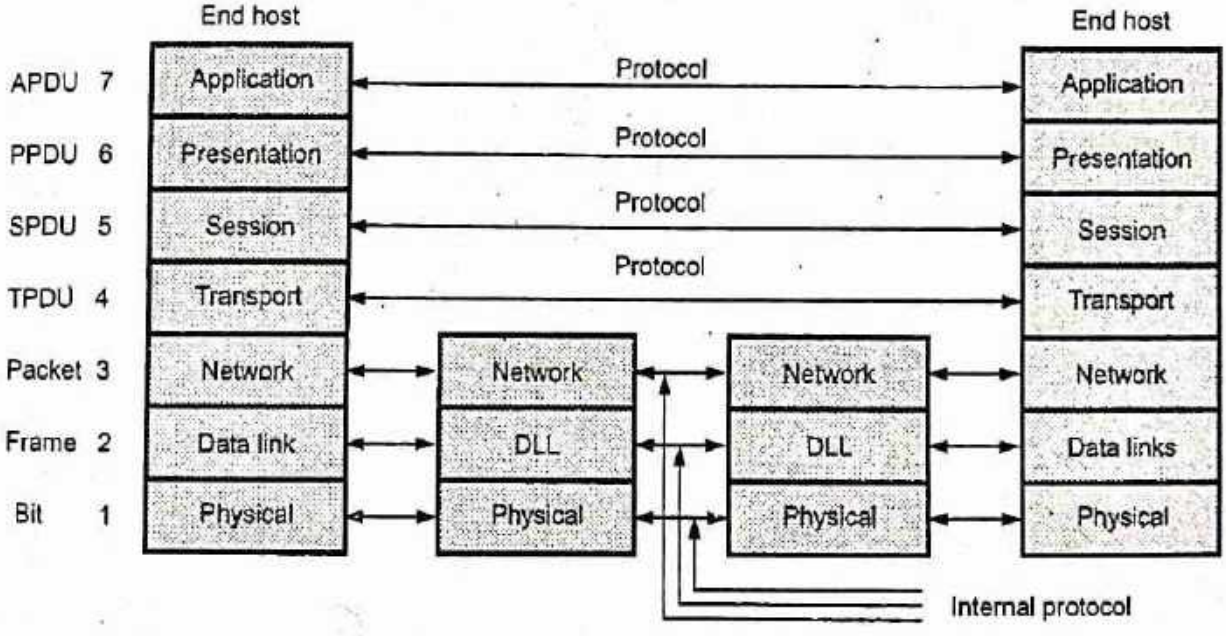


Fig. Q.16.1 Layer of OSI model

Layers in OSI Models

1. Physical layer

- Physical layer is the lowest layer of the OSI model. Physical layer co-ordinates the functions required to transmit a bit stream over a communication channel. It deals with electrical and mechanical

specifications of interface and transmission media. It also deals with procedures and functions required for transmission.

- The position of physical layer with transmission medium and the next layer (data link layer) is shown in Fig. Q.16.2.

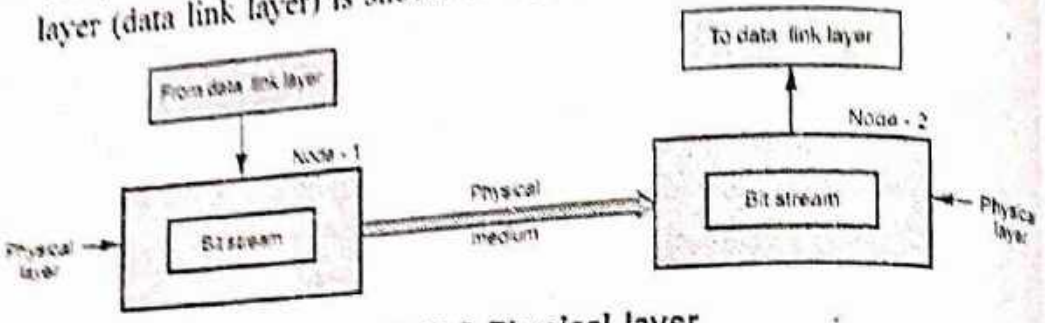


Fig. Q.16.2 Physical layer

Functions of Physical Layer

1. **Physical characteristics of interfaces and media :** The design issue of physical layer considers the characteristics of interface between devices and transmission media.
2. **Representation of bits :** Physical layer encodes the bit stream into electrical or optical signal.
3. **Data rate :** The physical layer defines the duration of a bit which is called as data rate or transmission rate.
4. **Synchronization of bits :** The transmission rate and receiving rate must be same. This is done by synchronizing clocks at sender and receiver. Physical layer performs this function.

2. Data link layer

- The data link layer is responsible for transmitting frames from one node to the next. It transforms the physical layer to a reliable link making it an error free link to upper layer. Fig. Q.16.3 shows data link layer. (See Fig. Q.16.3 on next page)

Functions of data link layer

1. **Framing :** The frames received from network layer is divided into manageable data units called frames.
2. **Physical addressing :** When frames are to be sent to different LANs the data link layer adds a header to the frame to define sender or receiver.
3. **Flow control :** When the rate of the data transmitted and rate of data reception by receiver is not same, some data may be lost. The data

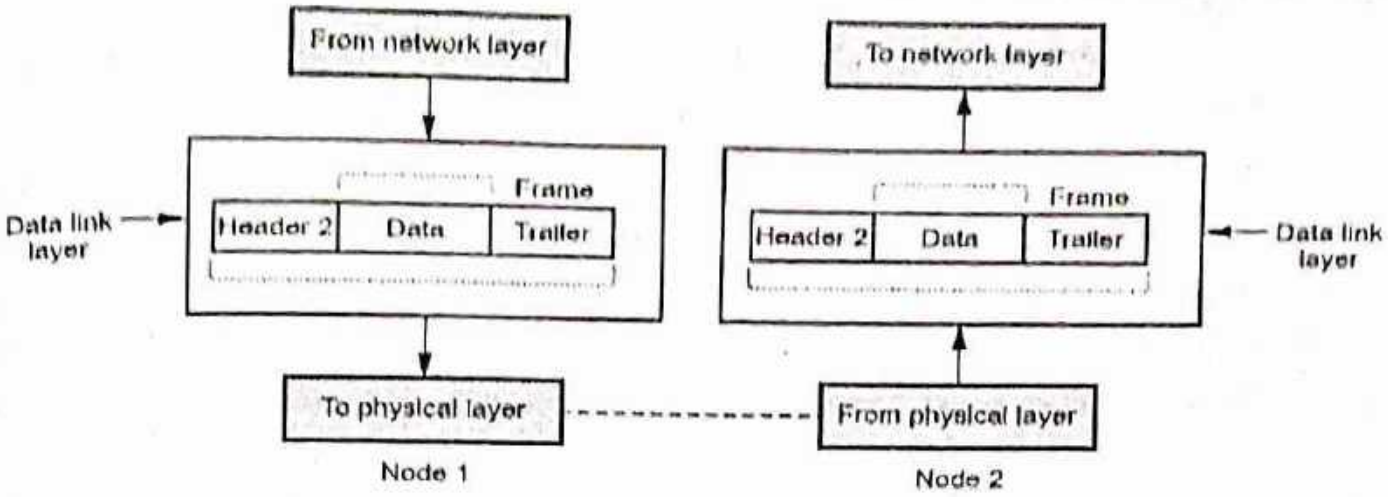


Fig. Q.16.3 Data link layer

link layer imposes a flow control mechanism to prevent overwhelming the receiver.

4. **Error control :** Data link layer incorporates reliability to the physical layer by adding mechanism to detect and retransmit damaged or lost frames.
5. **Access control :** When multiple devices are connected to same link, the data link layer determines which device has control over link.

3. Network layer :

- The network layer is responsible for the delivery of packets from the source to destination. Fig. Q.16.4 shows network layer.

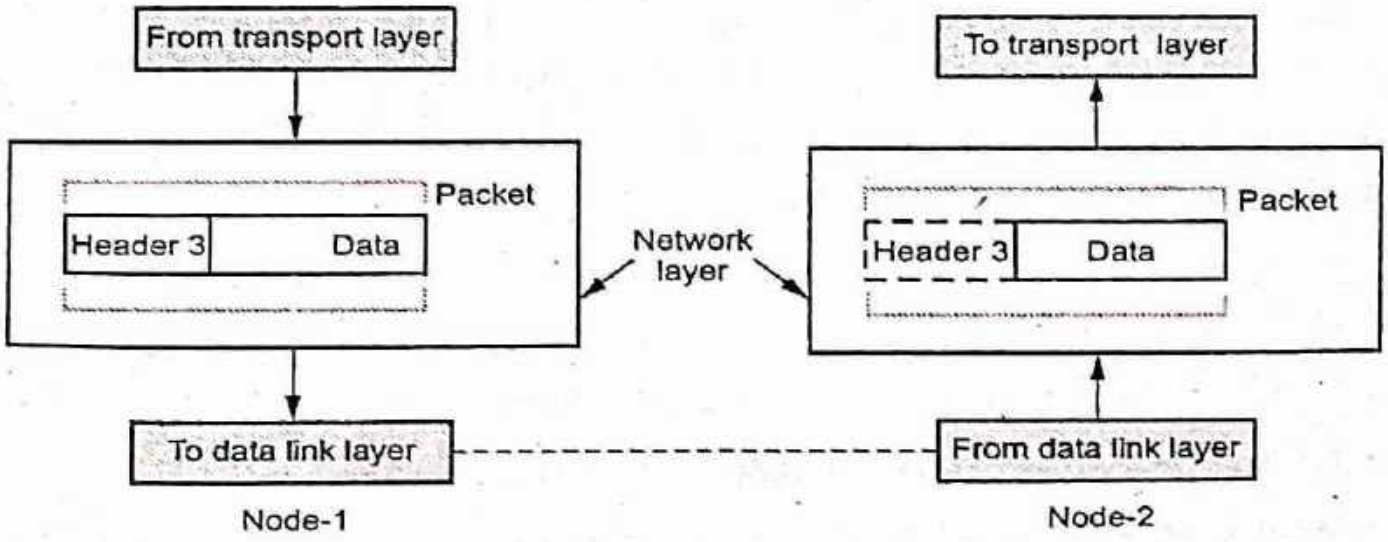


Fig. Q.16.4 Network layer

Functions of network layer

1. **Logical addressing :** Data link layer implements physical addressing. When a packet passes network boundary, an addressing system is needed to distinguish source and destination, network layer performs these function. The network layer adds a header to the packet of upper layer includes the logical addresses of sender and receiver.
2. **Routing :** Network layer route or switch the packets to its final destination in an internetwork.

Q.17 Draw and explain TCP/IP protocol suite.

☞ [SPPU : May-18, Marks 6]

Ans. : • The internet architecture, which is also sometimes called the TCP/IP architecture after its two main protocols.

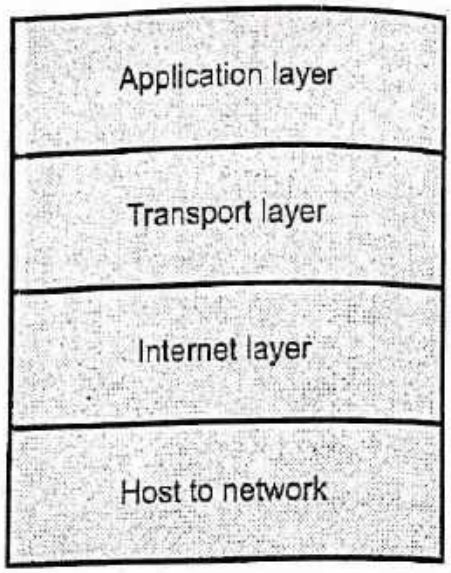


Fig. Q.17.1 TCP/IP reference model

- TCP/IP stands for Transmission Control Protocol / Internet Protocol.
- The TCP/IP reference model is a set of protocols that allow communication across multiple diverse networks.
- TCP/IP is normally considered to be a four layer system. Layers of TCP/IP are Application layer, Transport layer, Internet layer, Host to network layer.
- Host to network layer is also called physical and data link layer.
- The application layer in TCP/IP can be equated with the combination of session, presentation, application layer of the OSI reference model.
- Fig. Q.17.1 shows TCP/IP reference model.
- TCP/IP defines two protocol at transport layer : TCP and UDP.
- **User Datagram Protocol (UDP)** is connectionless protocol.
- UDP is used for application that requires quick but necessarily reliable delivery.

- Internet layer also called **network layer.** Internet layer handles communication from one machine to the other. Routing of packet takes place in internet layer.
- TCP/IP does not define any specific protocol in host to network layer. This layer is responsible for accpeting and transmitting IP datagrams. This layer normally includes the device driver in the operating system.
- Detailed function of each layer is given below.
  1. **Application layer :** Application layer includes all process and services that use the transport layer to deliver data. The most widely known application protocols are : TELNET, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). TELNET is the Network Terminal Protocol, which provides remote login over the network. FTP is used for interactive file transfer. SMTP delivers the electronic mail.
  2. **Transport layer :** Application programs send data to the transport layer protocols TCP and UDP. An application is designed to choose either TCP or UDP based on the services it needs.
- The transport layer provides peer entities on the source and destination hosts to carry on a conversation. Both ends protocol is defined in this layer.
- TCP is reliable connection oriented protocol that allows a byte stream originating on one computer to be delivered without error or any other computer in the internet.
- It converts the incoming byte stream into discrete message and passes each one onto the internet layer. At the destination side, the receiving TCP reassembles the received data or messages into the output format.
- TCP also handles flow control. It synchronizes between fast sender and slow receiver. UDP is a connectionless protocol. Sometimes this type of protocol is used for prompt delivery. The relation of the protocols is shown in the Fig. Q.17.2.

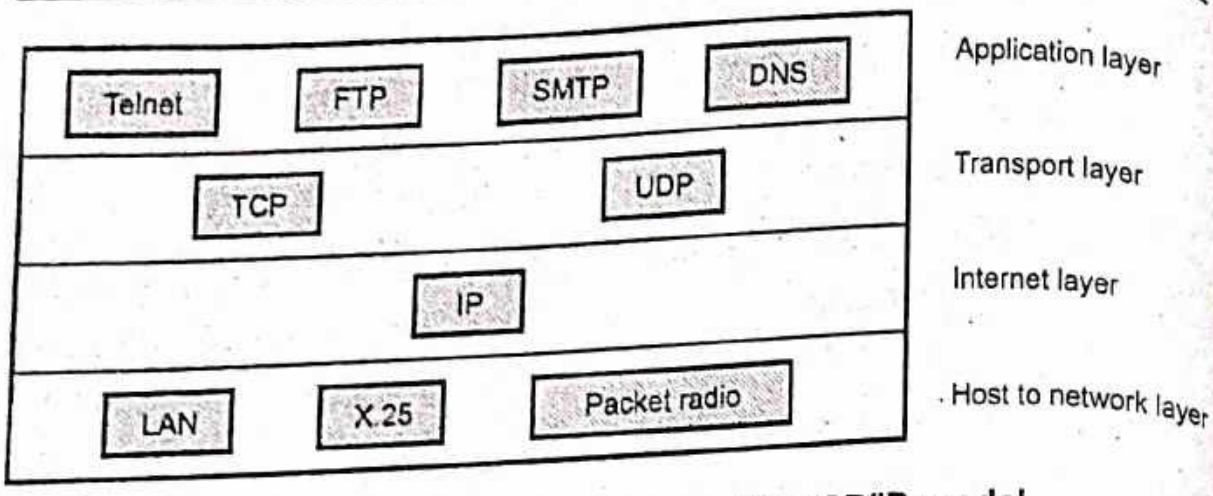


Fig. Q.17.2 Relation of protocol in TCP/IP model

3. **Internet layer :** The Internet network level protocol (IP, ARP, ICMP) handle machine to machine communications.

- These protocols provide for transmission and reception of transport requests and handle network level control. The TCP/IP internet layer moves data from one host to another; even if the hosts are on different networks. The primary protocol used to move data is the Internet Protocol (IP), which provides the following services :

a. **Addressing :** Determining the route to deliver data to the destination host.

b. **Fragmentation :** Breaking the messages into pieces if an intervening network cannot handle a large message.

- It provides a connectionless method of delivering data from one host to another. It does not guarantee delivery and does not provide sequencing of datagrams. It attaches a header to datagram that includes source address and the destination address, both of which are unique internet addresses.

4. **Host to network :** This layer is also called network interface layer. This layer is same as **physical and data link layer** of **OSI model. Host to network layer cannot define any protocol.** It is responsible for accpeting and transmitting IP datagrams. This layer may consist of a device driver in the operating system and the corresponding network interface card in the machine.

1.11 : Addressing

Q.18 Explain with examples different addressing schemes used in TCP/IP.

☞ [SPPU : May-17, Dec.-18, 19, Marks 6]

Ans. : • An Internet employing TCP/IP protocols uses four levels of addresses :

1. Physical (Link) addresses
2. Logical (IP) addresses
3. Port addresses
4. Specific addresses

• Each address type is related to a specific layer in TCP/IP architecture. Fig. Q.18.1. shows the relationship of layers and addresses in TCP/IP.

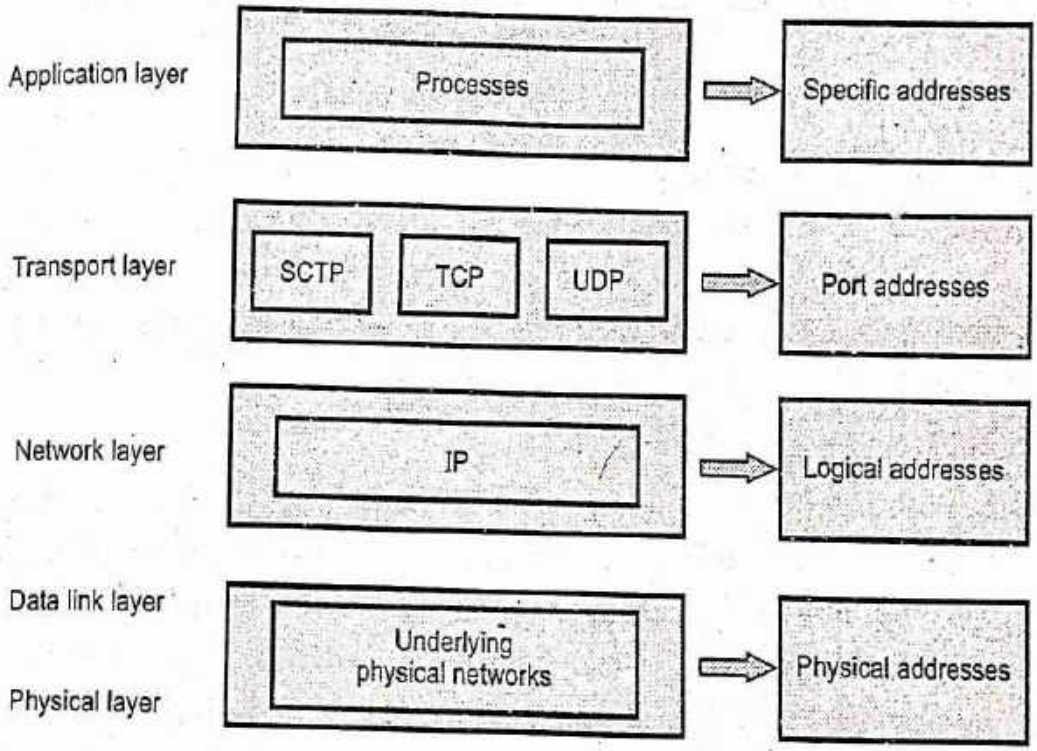


Fig. Q.18.1 TCP/IP layers and associated addresses

Physical addresses

• The physical address is the lowest level address and is also referred as link address. The physical address of a node is defined by its LAN or WAN. The physical address is included in the frame by the data link layer.

• The size and format of physical addresses vary depending on the network. It has authority over the network. At data link layer the frame contains physical (link) addresses in the header. The data link layer at

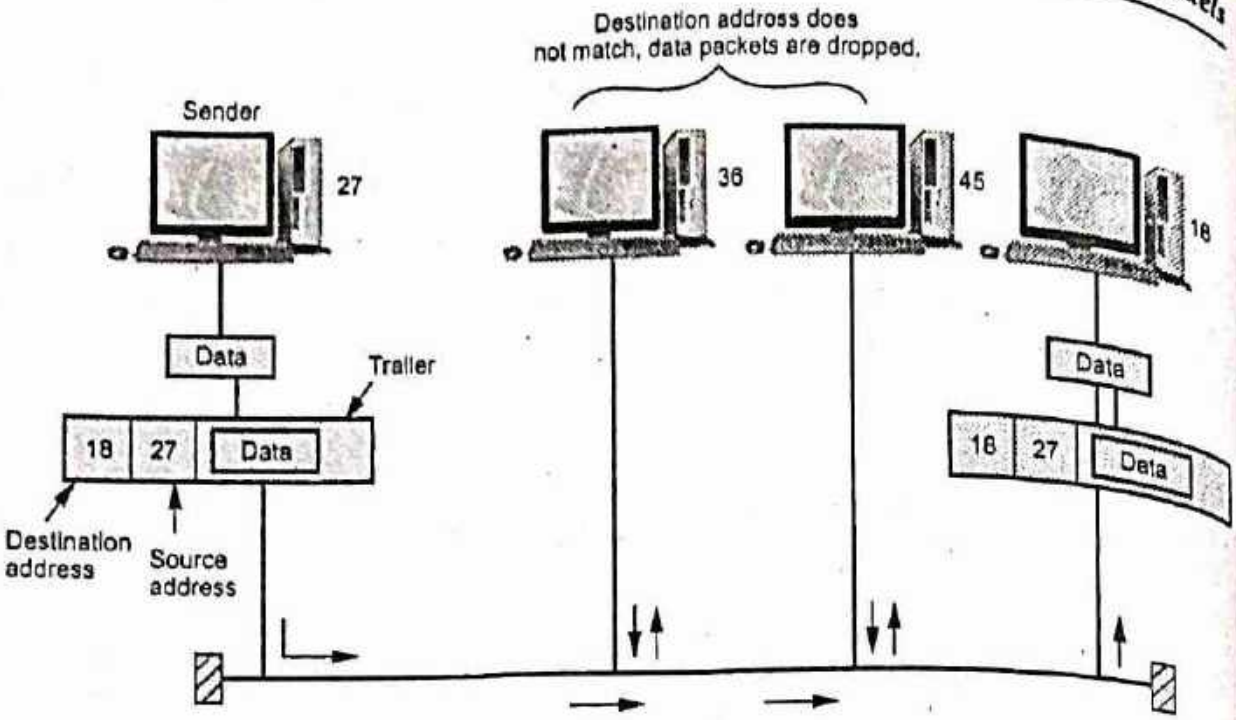


Fig. Q.18.2 Physical addresses

sender receives data from upper layer, encapsulates the data in a frame, adds an header and trailer. Only the station having matched address with destination address accepts the frames. The frame is checked, the header and trailer are dropped and data is decapsulated and delivered to upper layer.

Logical addresses

- Logical addresses are independent of underlying physical networks. Since different networks can have different address formats hence a universal address system is required which can identify each host uniquely irrespective of underlying physical networks. Logical addresses are necessary for universal communications. It is a 32-bit address which uniquely defines host connected to Internet.
- The physical addresses changes from hop to hop, but the logical address usually remains the same.

Port addresses

- The IP address and physical address are necessary for data to travel from source to destination. But a communication process involves TELNET and FTP which requires addresses. In TCP/IP architecture, the

label assigned to a process is called port address. In TCP/IP the port address is of 16-bit.

Specific addresses

- Specific addresses are designed by users for some applications. For example, evilaas@in.com and the Universal Resource Locator (URL), www.vtubooks.com. The first example defines the recipient of e-mail and second example is used to find a document on the world wide web.
- The specific addresses gets changed to corresponding port and logical addresses by the station or host who sends it.

END...

Unit II

2 Error Detection, Correction and Data Link Control

2.1 : Data Link Layer

Q.1 Explain services provided to network layer.

Ans. : • The primary responsibility of data link layer is to provide services to the network layer. The principle service is transferring data from the network layer on the source machine to the network layer on the destination machine.

- The two data link layer communicates with each other by data link control protocol.
- Following are the important services provided by data link layer to the network layer.
  1) Unacknowledged connectionless service.
  2) Acknowledged connectionless service.
  3) Acknowledged connection-oriented service.

1) Unacknowledged connectionless service : As the name suggests, it is unacknowledged form of transmission. Here the source machine sends the data to the destination machine without any acknowledgement. For this, no connection is either established or released. If the data is lost due to noise or interference, the lost data is not even recovered by the layer.

2) Acknowledged connectionless service : In acknowledged connectionless service each data frame is acknowledged by the destination machine. If any data frame is lost or not arrived in time the same can be transmitted again. In this service no connection are used.

3) Acknowledged connection service : Acknowledged connection service establishes a connection prior to data transmission. Each frame is numbered before transmission and corresponding acknowledgement is also received. The transmission is carried out in distinct phases.

2.2 : Error Detection and Correction

Q.2 Explain types of errors ?

Ans. : Two general types of errors can occur

1. Single bit error 2. Burst error

1. Single bit error

- It means that only 1 bit of a given data unit is changed from 1 to 0 or from 0 to 1. A single bit error is an isolated error condition that alters one bit but does not affect nearby bits.
- A single bit error can occur in the presence of white noise, when a slight random deterioration of the signal to noise ratio is sufficient to confuse the receiver's decision of a single bit. Single bit errors are the least likely type of error in serial data transmission.

2. Burst error

- The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.
- Burst errors are more common and more difficult to deal with errors. Burst errors can be caused by impulse noise. Note that the effects of burst errors are greater at higher data rates.

2.3 : Linear Block Codes

Q.3 Explain linear block coding, error detection and error correction.

Ans. : • In block coding, message is divided into blocks. Each block size is K bits and called as **datawords**. Redundant bits (r) is add to each block to make the length $n = K + r$. The resulting n-bit blocks are called **codewords**.

- With K bits, combination of 2^K datawords are possibe and with n bits, 2^n codewords combination are possible. The block coding process is

one-to-one; the same dataword is always encoded as the same codeword.

- Fig. Q.3.1 shows the datawords and codewords in block coding.

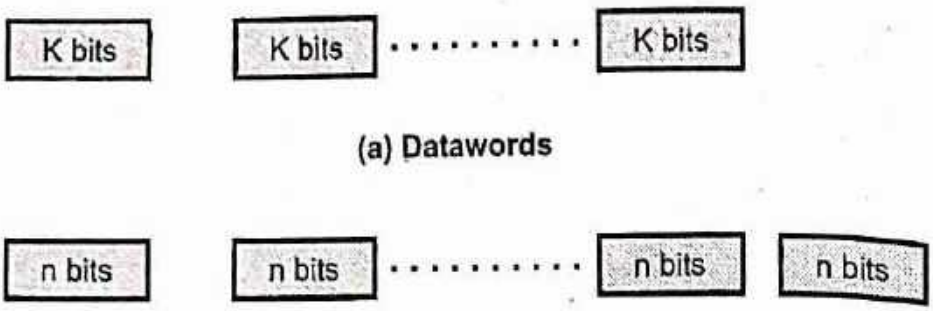


Fig. Q.3.1 Datawords and codewords

Error Detection

- Following steps are used for detecting errors in the block coding.
  1. The receiver has a list of valid codewords.
  2. The original codeword has changed to an invalid one.
- Fig. Q.3.2 shows the role of block coding in error detection.

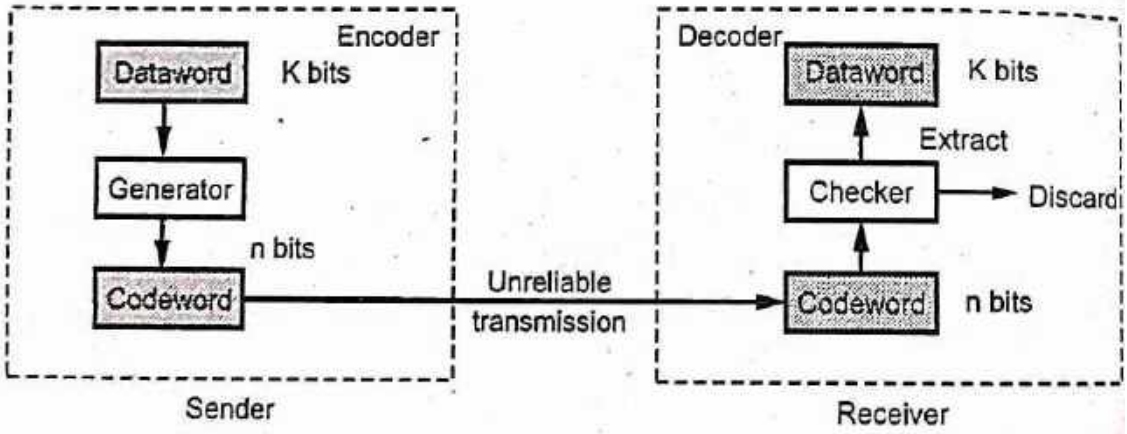


Fig. Q.3.2 Error detection process

- The sender creates codewords out of datawords by using a generator that applies the rules and procedures of encoding. Each codeword send to the receiver may change during transmission.
- If the received codeword is the same as one of valid codewords, the word is accepted; the corresponding dataword is extracted for use. If the received codeword is not valid, it is discarded.

- If the codeword is corrupted during transmission but the received word still matches a valid codeword, the error remains undetected.
- Block coding can detect only single errors. Two or more errors may remain undetected.

Error Correction

- Fig. Q.3.3 shows the error correction process. Error correction is much more difficult than error detection.

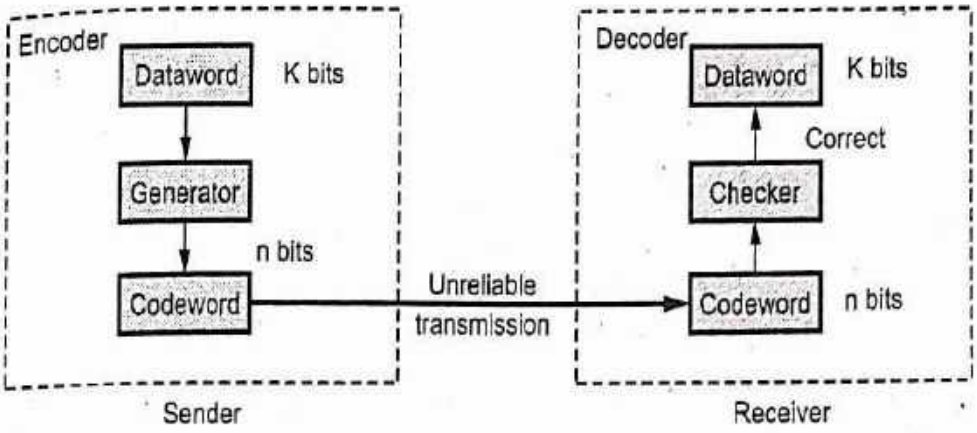


Fig. Q.3.3 Error correction in block coding

- In error correction, the receiver needs to find the original codeword sent. More number of redundant bits are required for error correction than for error detection.

Q.4 Explain hamming distance.

Ans. : • Hamming bits are inserted into the message at the random locations. Hamming code is a single error correcting code. It is most complex from the stand point of creating and interpreting the error bits. Let us consider a frame which consists of m data bits and r check bits. The total length of message is then n = m + r. An n-bit unit containing data and checkbits is often referred to as an **n-bit codeword.**

- If 10001001 and 10110001 are two codewords, then the corresponding bits differ in these two codewords is 3 bits. The number of bit positions in which two codewords differ is called the **Hamming distance**
- If two codewords are a hamming distance d apart, it will require d single bit errors to convert one into the other. Determining the

placement and binary value of the hamming bits can be implemented using hardware, but it is often more practical to implement them using software.

- The number of bits in the message are counted and used to determine the number of hamming bits to be used. The equation is used to count the number of hamming bits.

$$2^H \geq M + H + 1 \quad \text{... (Q.4.1)}$$

where M = Number of bits in a message

H = Hamming bits

- After calculating the number of hamming bits, the actual placement of the bits into the message is performed.
- Hamming code works as follows : Supose that frame consists of eight bits say $m_1\ m_2\ m_3\ m_4\ m_5\ m_6\ m_7\ m_8$. If n parity checks are used, there are 2^n possible combinations of failures and successes.
- If we use 4-bit parity checks, then there are 16 possible combinations of parity successes and failures. Total 12 bits are sent which contain 8-bit original message and 4-bit parity bits. The four parity is inserted into the frame.
- Four parity bits are $P_1\ P_2\ P_3$ and P_4. Let us consider following.

Data bit $m_1\ m_2\ m_3\ m_4\ m_5\ m_6\ m_7\ m_8$

Hamming code	P_1	P_2	m_1	P_3	m_2	m_3	m_4	P_4	m_5	m_6	m_7	m_8
	1	2	3	4	5	6	7	8	9	10	11	12

- The parity bits are inserted into the message. Position of the parity bit is calculated as follows. Create a 4 bit binary number $b_4\ b_3\ b_2$ and b_1 where

$b_i = 0$ if the parity check for P_i succeeds

$b_i = 1$ otherwise

for i = 1, 2, 3 or 4.

1) The parity bit P_1 is inserted at bit position 1 for even parity for bit positions 1, 3, 5, 7, 9, 10. In these bit positions it contains even number of 0s or 1s.

2) The parity bit P_2 is inserted at bit position 2, for even parity for bit positions 2, 3, 6, 7, 10, 11.

3) The parity bit P_3 is inserted at bit position 4, for even parity of the bit positions 4, 5, 6, 7, 12.

4) The parity bit P_4 is inserted at bit position 8 for even parity of the bit positions 8, 9, 10, 11, 12.

- For inserting the parity bit even or odd parity can be used. Each parity bit is determined by the data bits it checks. When a receiver gets a transmitted frame, it performs each of the parity checks.
- The combination of failures and successes then determines whether there was no error or in which position an error occurred. Once the receiver knows where the error occurred, it changes the bit value in that position and the error is corrected.

Minimum hamming distance (d_{min})

- The minimum hamming distance is the smallest hamming distance between all possible pairs in a set of words.
- To find the value of d_{min}, we find the hamming distances between all words and select the smallest one.

2.4 : Cyclic Codes

Q.5 What is meant by parity check ? Explain two-dimensional parity check method in detail. ☞ [SPPU : Dec.-18, Marks 6]

Ans. : • The simplest error detection scheme is to append a parity bit to the end of a block of data. Parity checking will detect any single bit error.

- The parity bit is transmitted with the data bits and the receiver checks the parity. If the receiver finds an odd number of 1 bits, an error has occurred.
- Suppose two bits change during transmission. If they were both 0, they change to 1. Two extra 1s still make the total number of 1 bits even. Similarly, if they were both 1 they both change to 0 and there are two

fewer 1 bits, but still an even number. If they were opposite values and both change, they are still opposite. This time the number of 1 bits remains the same. This means that the parity checks do not detect double bit errors.

- In general, if an odd number of bits change, parity checking will detect the error. If an even number of bits change, parity checking will not detect the error.
- Fig. Q.5.1 shows encoder and decoder for parity check.

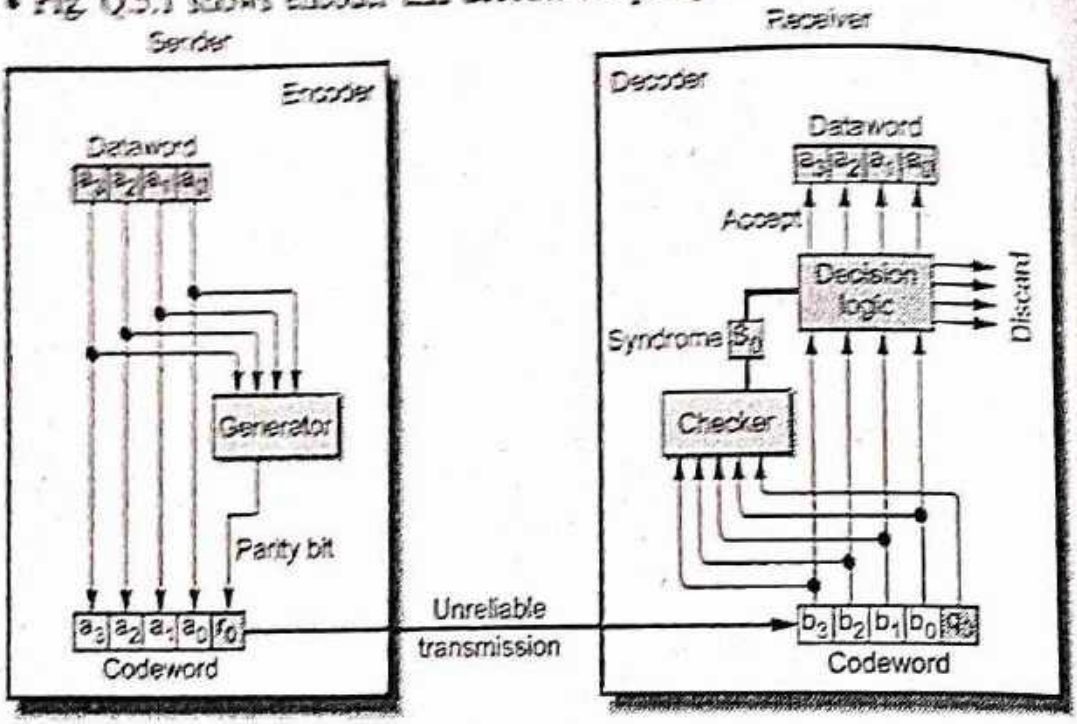


Fig. Q.5.1 Encoder and decoder for parity check

Q.6 Generate the CRC code for message 1101010101. Given generator polynomial

$g(x) = x^4 + x^2 + 1$ ☞ **[SPPU : May-17, Dec.-17, 18, 19, Marks 6]**

Ans. : For polynomial division $T(X)/G(X)$

where $T(X) = 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1$

$$\left(x^9 + x^8 + x^6 + x^4 + x^2 + 1\right)$$

$$G(X) = x^4 + x^2 + 1 = 1\ 0\ 1\ 0\ 1$$

Polynomial division is done from an algebra.

Rules for addition and subtraction.

1. Addition

$0 + 0 = 0$

$1 + 0 = 1$

$0 + 1 = 1$

$1 + 1 = 0$

2. Subtraction

$0 - 0 = 0$

$1 - 0 = 1$

$0 - 1 = 1$

$1 - 1 = 0$

The steps are as follows :

Step 1 : Append 0 to the end of the string T(X).

The degree of polynomial $G(X) = x^4 + x^2 + 1 = 4$.

So we append 4 zeros to string $T(X)$.

The string becomes

1 1 0 1 0 1 0 1 0 1 0 0 0 0

Step 2 : Divide $B(X)$ by $G(X)$. After appending 0s to $T(X)$ it becomes $B(X)$. (Actually it is new $T(X)$ divided by $G(X)$).

```
          1110001110
      ____________
10101) 11010101010000
       11010
       10101
        011111
        10101
        010100
        10101
        000011010
             10101
             011110
             10101
             010110
             10101
             000110        ← Remainder
```

$$\begin{array}{r} 10011001\,0000 \\ \leftarrow \quad\quad 0110 \\ \hline 10011001\,0110 \end{array} \Leftarrow \text{Codeword}$$

Q.7 Explain CRC generator and CRC checker with suitable example. [SPPU : May-19, Marks 6]

Ans. : • Parity method detects only odd numbers of errors. To overcome this weakness polynomial codes error detection method is used. Polynomial codes involve generating check bits in the form of a cyclic redundancy code (CRC). Therefore polynomial also called cyclic redundancy codes (CRCs).

- The theory of polynomial code is derived from a branch of mathematics called algebra theory. The theory of CRC checksums is developed by using algebra and polynomials. These polynomials are equations which have the form of powers of X :

$$X^N + X^{N-1} + \ldots + X^2 + X^1 + X^0$$

- Polynomial codes are used with frame transmission schemes. A single set of check digits is generated for each frame transmitted, based on the contents of the frame and is appended by the transmitter to the tail of the frame. The receiver then performs a similar computation on a complete frame and check digits. If no errors have been induced, a known result should always be obtained, if a different answer is found, this indicates an error. Consider an example for binary, the polynomial for binary 10011001 is

$$X^7 + X^4 + X^3 + X^0 \left(X^0 = 1\right)$$

- The polynomial which represents the data bits is called the message polynomial, usually shown as G(X). There is a second polynomial, called the generator polynomial P(X). G(X) and P(X) both having same

format. Combine two polynomials P(X) and G(X) to produce the CRC checksum polynomial F(X) calculating CRC error as follows :

a) Multiply the G(X) by X^{n-k}, where $n-k$ is the number of bits in the CRC checksum.

b) Divide the resulting product $X^{n-k}[G(X)]$ by the generator polynomial P(X).

c) Add the remainder C(X) to the product to give the F(X), which is representated as $X^{n-k}[G(X)]+C(X)$.

d) The division is performed in binary without carrying or borrowing. In this case, the remainder is always 1 bit less than the divisor. The remainder is the CRC and the divisor is the generator polynomial.

Working of CRC

- Let's now describe how CRC works. Suppose we want to send the bit string **1101011** and the generator polynominal is $G(x) = x^4 + x^3 + 1$

Step 1 : Append 0s to the end of the string. The number of 0s is the same the degree of the generator polynominal G(x) (in this case, 4). Thus the string becomes 11010110000.

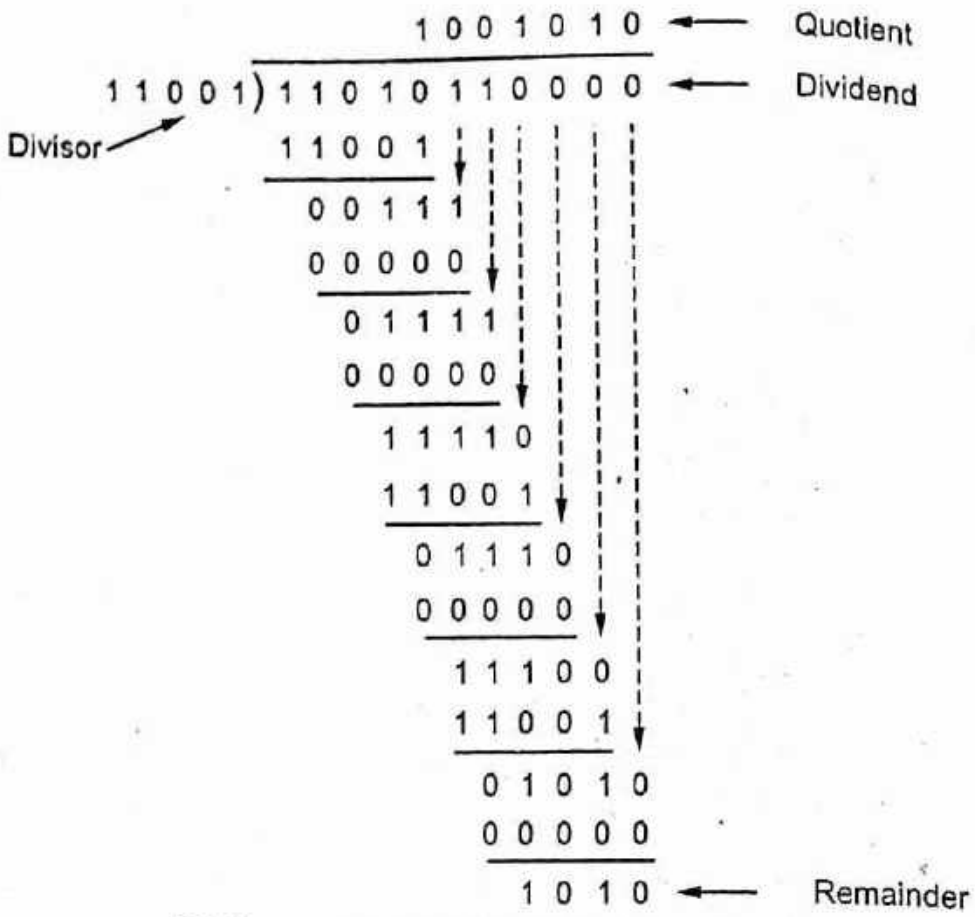
Step 2 : Divide B(x) by G(x). We can write this algebraically as,

$$\frac{B(x)}{G(x)} = Q(x) + \frac{R(x)}{G(x)}$$

where Q(x) represent the quotient.

$$G(x) = x^4 + x^3 + 1 = 11001$$

String = 1101011 = After appending 11010110000



$B(x) = 1101011000$ bit string B

$R(x) = 1010$ bit string R

$T(x) = 11010111010$ bit string T

Step 3 : Define T(x) = B(x) – R(x). In this case,

Note that the string T is actually the same as string B with the appended 0s replaced by R. The sender transmit the string T.

Q.8 Information to be transmitted is 110011 and the generator polynomial is represented as $g(x) = 11001$. Do a CRC check.

Ans. : Append by 4 bit 0 because coefficient of g(x) is 4.

The binary equivalent of d(x) = 1 1 0 0 1 1 0 0 0 0

```
          100001
      ------------
11001 ) 1100110000
        11001
        -----
        11001
        -----
        0000010000
             11001
             -----
             01001        ← Remainder
```

Remainder is added to d(x) to give f(x) i.e.

1 1 0 0 1 1 0 0 0 0 + 0 1 0 0 1 = 1 1 0 0 1 1 1 0 0 1 ← f(x)

f(x) is transmitted.

2.5 : Framing

Q.9 What is mean by framing ? Explain character oriented protocol.

Ans. : • Framing in the data link layer separates a message from one source to a destination or from other messages to other destinations by adding a sender address and a destination address.

- To service the network layer, data link layer uses the service provided to it by the physical layer.
- Physical layer accepts the raw bit stream and delivers it to the destination. This bit stream may contain error i.e. number of bits received may not be equal to number of bits transmitted.
- The data link layer breaks the stream into discrete frames and computes the checksum for each frame.
- At the destination the checksum is recomputed.
- The breaking of bit stream by inserting spaces or time gaps is called framing. Since it is difficult and risky to count on timing and mark the start and end of each frame.

Fixed-size framing

- Frames can be of fixed or variable size. In fixed size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.
- ATM is the example of fixed size framing.

Variable Size Framing

- In variable size framing, end of the frame and the beginning of the next frame is defined.
- Two methods are used for this purposes.

  1. Character oriented 2. Bit oriented

2.6 : Flow Control

Q.10 Explain flow control.

Ans. : • When the sender is running on fast machine or lightly loaded machine and receiver is on slow or heavily loaded machine. Then the transmitter will transmit frames faster than the receiver can accept them.

- Even if the transmission is error free at a certain point the receiver will simply not be able to handle the frames as they arrive and will start to lose some.
- To prevent this, flow control mechanism is incorporated which includes a feedback mechanism requesting transmitter a retransmission of incorrect message block.
- The most common retransmission technique is known as Automatic-Repeat -Request.
- Error control in Data Link Layer (DLL) is based on Automatic Repeat Request (ARQ) i.e. retransmission of data in three cases.

  1. Damaged frames 2. Lost frames 3. Lost acknowledgements.

2.7 : Noiseless Channels

Q.11 Explain simplex stop and wait protocol.

Ans. : • Protocols in which the sender sends one frame and then waits for an acknowledgement before proceeding are called **stop-and-wait.**

- The communication channel is still assumed to be error free however and the data traffic is still complex.
- **Main problem :** How to prevent the sender from flooding the receiver with the data faster than the latter is able to process it.
- It is also assumed that there is no automatic buffering and queueing done within the receiver's hardware. The sender never transmit new frame until old one has been fetched by *from_physical_layer*.
- In some situations, delay is inserted by sender in the above protocol to slow it down sufficiently to keep from swamping the receiver.
- A more general solution to this dilemma is to have the receiver provide feedback (ACK) to the sender. After having passed a packet to its network layer, the receiver sends a little dummy frame back to the sender which, in effect, gives the sender permission to transmit the next frame.
- After having sent a frame, the sender is required by the protocol to bide its time until the little dummy (i.e., acknowledgement) frame arrives.
- Using feedback from the receiver to let the sender know when it may send more data is an example of the flow control.
- The simplest retransmission protocol is stop-and-wait. Transmitter (station A) sends a frame over the communication line and then waits for a positive or negative acknowledgement from the receiver (station B).
- If no errors occurred in the transmission, station B sends a positive acknowledgement (ACK) to station A.
- The transmitter can now start to send the next frame. If frame is received at station B with errors, then a negative acknowledgement

(NAK) is sent to station A. In this case station A must retransmit the old packet in a new frame.

- There is also the possibility that information frames and/or ACKs can be lost. To account for this, the sender is equipped with a timer. If no recognizable acknowledgement is received when the timer expires at the end of time out interval t_{out}, then the same frame is sent again.
- Fig. Q.11.1 shows the design of stop and wait protocol.

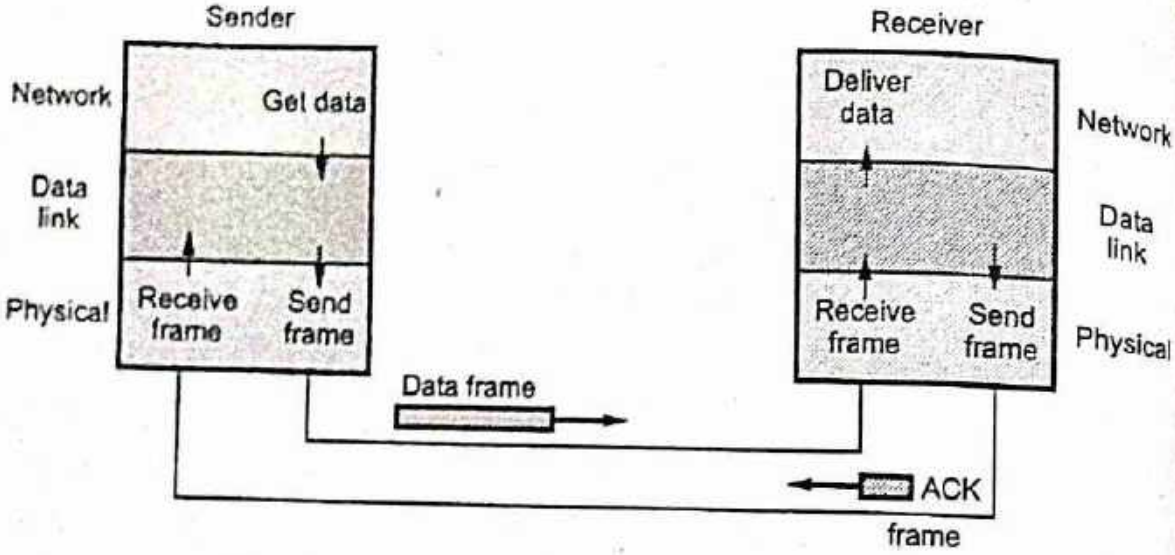


Fig. Q.11.1 Design of stop and wait protocol

- Protocols in which the sender sends one frame and then waits for an acknowledgement before process are called **stop and wait.**
- **Algorithm for sender**

```
void sender (void)
{
    frame s;
    packet buffer;
    event_type event;
while(true){
    from_network_layer(&buffer);
    s.info=buffer;
    to_physical_layer(&s);
    wait_for_event(&event);
```

```
}
}
```

- Fig. Q.11.2 shows the flow diagram.

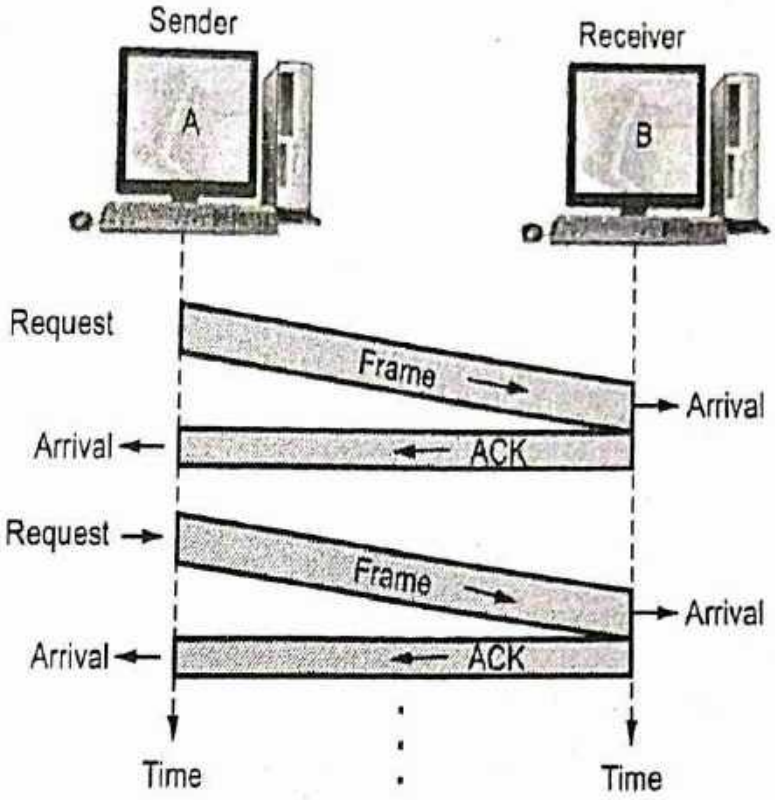


Fig. Q.11.2 Flow diagram for stop and wait

- **Algorithm for receiver side**

```
void receiver(void)
{
    frame r,s;
    event_type event;
while(true){

wait_for_event (&event);
from_physical_layer(&r);
to_network_layer(&r.info);
to_physical_layer(&s);
}
}
```

- **Major drawback of stop-and-wait flow control :**
  1) Only one frame can be in transmission at a time.
  2) This leads to inefficiency if propagation delay is much longer than the transmission delay.

2.8 : Noisy Channels

Q.12 Explain in detail go-back-N and selective repeat ARQ system.

☞ [SPPU : May-17,18, Dec.-17, Marks 6]

OR Explain in working mechanism of go-back-N and selective repeat ARQ system.

☞ [SPPU : Dec.-19, Marks 7]

Ans. : Go-Back-N ARQ Protocol

- Go-Back-N uses the sliding window flow control protocol. If no errors occur the operations are identical to sliding window.
- A station may send multiple frames as allowed by the window size.
- Receiver sends a NAK i if frame i is in error. After that, the receiver discards all incoming frames until the frame in error was correctly retransmitted.
- If sender receives a NAK i it will retransmit frame I and all packets i+1, i+2,... which have been sent, but not been acknowledged.
- The need for a large window on the sending side occurs whenever the product of bandwidth x round-trip-delay is large. If the bandwidth is high, even for a moderate delay, the sender will exhaust its window quickly unless it has a large window.
- If the delay is high, the sender will exhaust its window even for a moderate bandwidth. The product of these two factors basically tells what the capacity of the pipe is and the sender needs the ability to fill it without stopping in order to operate at peak efficiency. This technique is known as **pipelining.**
- As in Stop-and-Wait protocol senders has to wait for every ACK then next frame is transmitted. But in Go-Back-N ARQ W frames can be

transmitted without waiting for ACK. A copy of each transmitted frame is maintained until the respective ACK is received.

Additional features of Go-Back-N ARQ

1) Sequence numbers : Sequence numbers of transmitted frame are maintained in the header of each frame. If k is the number of bits for sequence number, then the numbering can range from 0 to $2^k - 1$ e.g. for $k = 3$. Sequence numbers are 0 to 7 $\left(2^3 - 1\right)$.

2) Sender sliding window : Window is a set of frames in buffer waiting for acknowledgment. This window keeps on sliding in forward direction. The window size is fixed. As the ACK is received, the respective frame goes out of window and new frame to sent come into window. Fig. Q.12.1 illustrates sliding of window for window size = 7. (See Fig. Q.12.1 on next page)

3) Receiver sliding window : In the receiver side the size of the window is always one. The receiver is expecting to arrive frames in specific sequence. Any other frame received which is out of order is discarded. The receiver slides over after receiving the expected frame. Fig. Q.12.2 shows receiver sliding window.

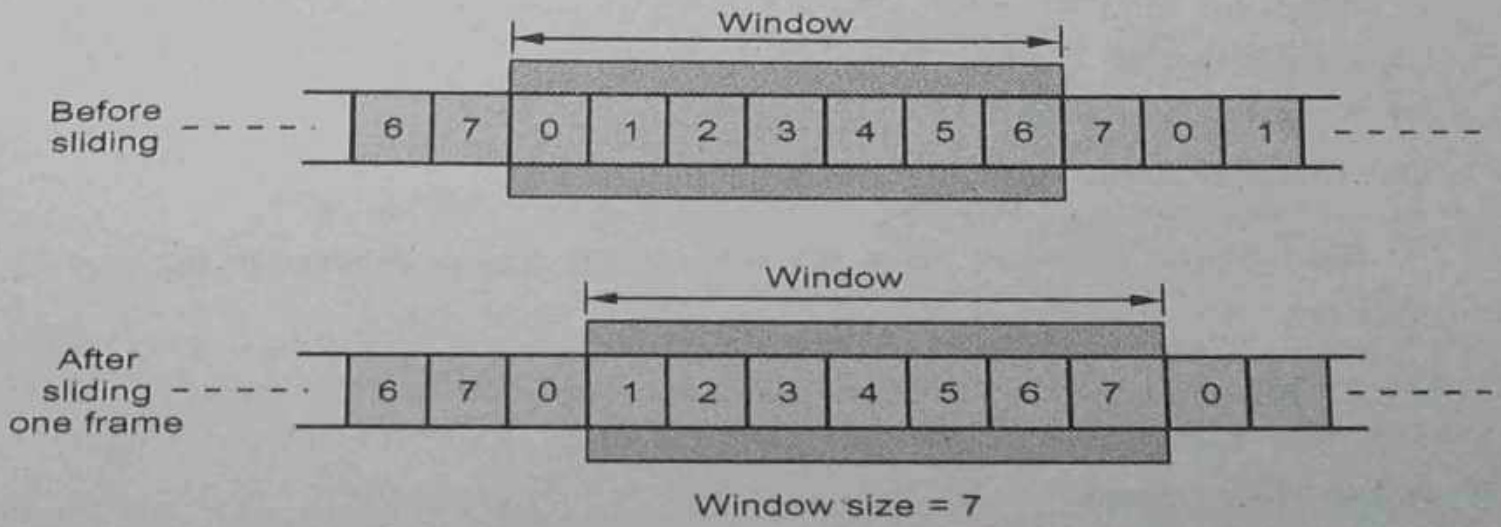


Fig. Q.12.1 Sender sliding window

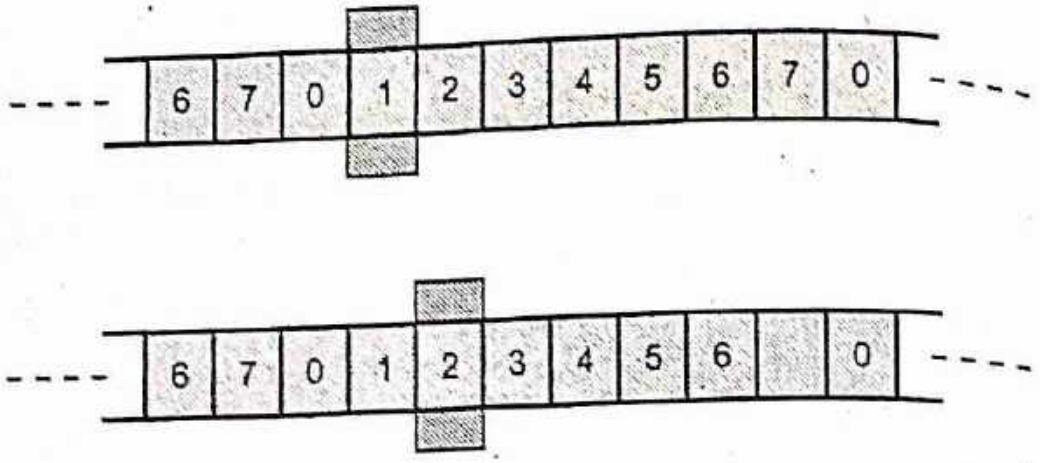


Fig. Q.12.2 Receiver sliding window

4) Control variables :

a) Sender variables

- The sender deals with three different variables.

  $S \rightarrow$ Sequence number of recently sent frame.

  $S_F \rightarrow$ Sequence number of first frame in window.

  $S_L \rightarrow$ Sequence number of last frame in window.

  $\therefore$ Window size $W = S_L - S_F + 1$

  e.g. in previous feature, $W = 7 - 0 + 1 = 8$

b) Receiver variable

- The receiver deals with one variable only.

  $R \rightarrow$ Sequence number of frame expected

  If the number matches, then the frame is accepted otherwise not.

5) Timers

- The sender has a timer for each transmitted frame. The receiver don have any timer.

6) Acknowledgment

- The receiver responds for frames arriving safely by positiv acknowledgments. For damaged or lost frames receiver does not repl the sender has to retransmit it when timer of that frame elapsed.
- The receiver may acknowledge once for several frames.

7) Resending of frames

- If the timer for any frame expires, the sender has to resend that frame and the subsequent frames also, hence the protocol is called Go-Back-N ARQ.

Operation

a) Normal operation

- The sender sends frames and update the control variables i.e. S_F, S, S_L and receiver updates variable R. Fig. Q.12.3 shows normal operation.

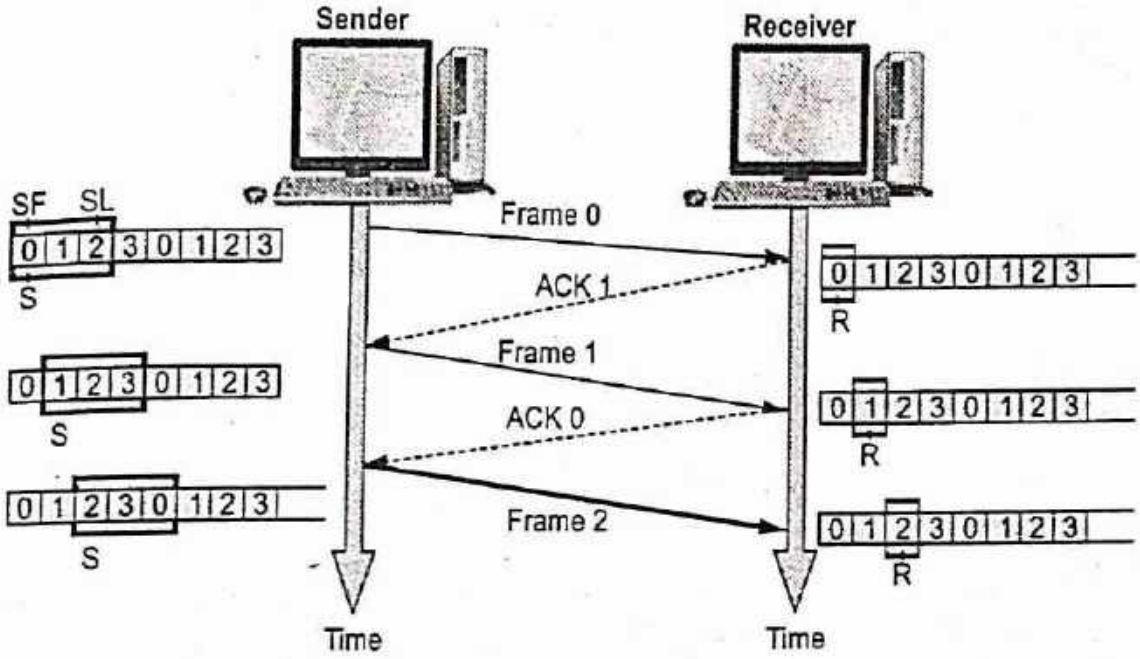


Fig. Q.12.3 Go-Back-N ARQ, normal operation

b) Damaged or lost frame

- Suppose frame 2 is damaged or lost and if receiver receives frame 3, it will be discarded since it is expecting frame 2. Sender retransmits frame 2 and frame 3. Fig. Q.12.4 shows this process.

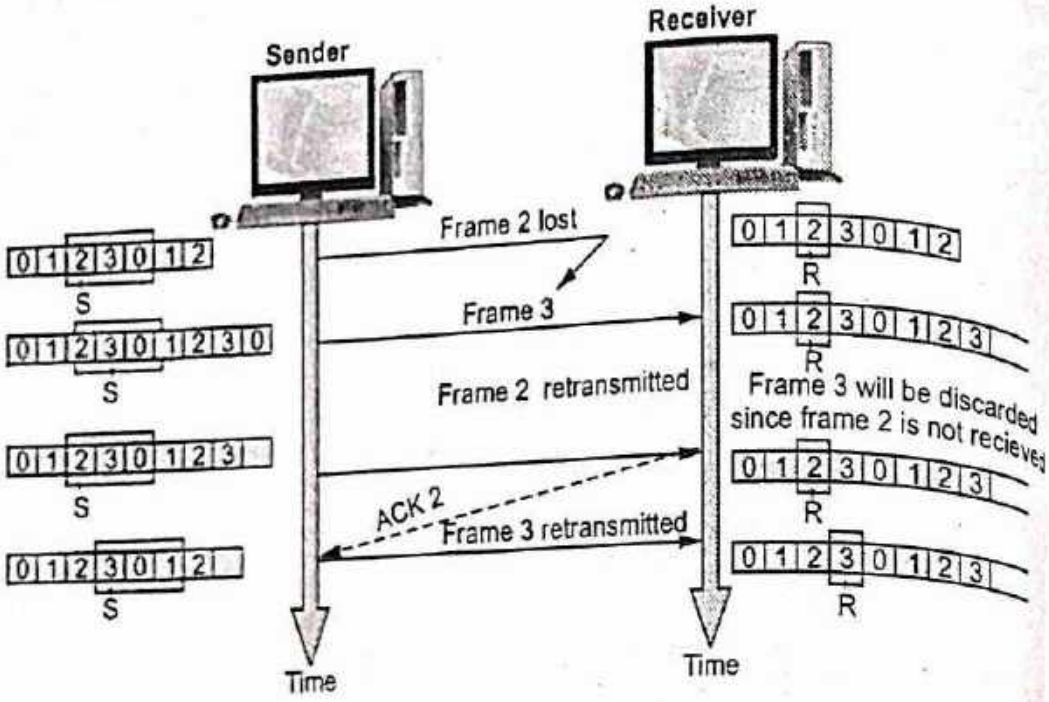


Fig. Q.12.4

Selective Repeat ARQ Protocol

- Selective repeat ARQ retransmitts only the damaged or lost frames instead of sending multiple frames. The selective retransmission increases the efficiency of transmission and is more suitable for noisy channel. The circuit complexities at the receiver side increases.
- The size of sender window is one half of 2^k. The receiver window size is of same length as that of sender. The receiver window includes the set of expected frames. The boundaries of receiver windows are defined by R_F and R_L. Fig. Q.12.5 shows the sender and receiver windows.

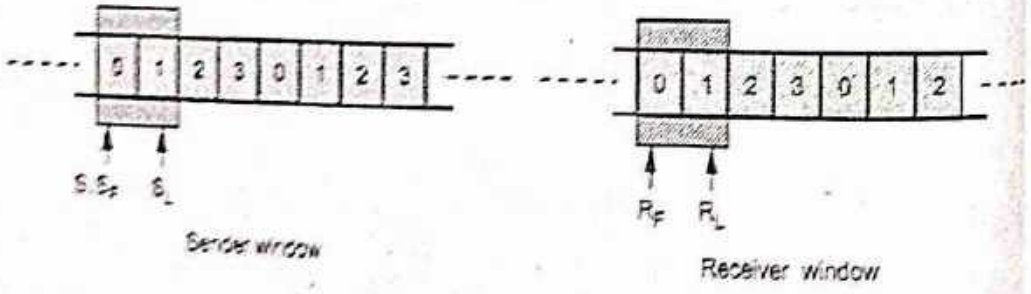


Fig. Q.12.5 Selective repeat windows

- Negative acknowledgement (NAK) is used for lost or damaged frames.

Operation

- In sequential transmission of frame 0, 1, 2, 3, suppose frame 2 is lost and the next frame 3 is already received then receiver sends NAK 2 frame to sender. Then sender retransmits frame 2 only. Fig. Q.12.6 shows operation of selective repeat ARQ.

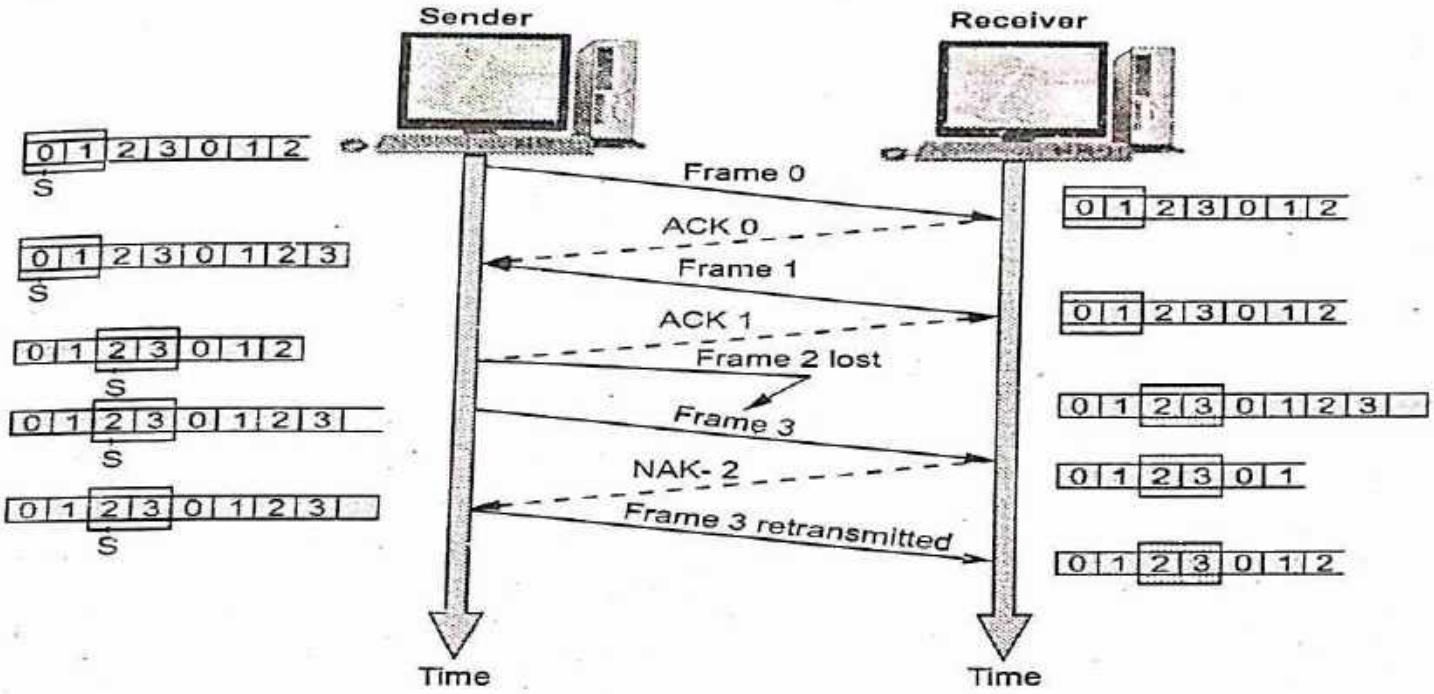


Fig. Q.12.6 Selective repeat ARQ

Advantage :

1) Fewer retransmissions.

Disadvantages :

1) More complexity at sender and receiver.
2) Each frame must be acknowledged individually (no cumulative acknowledgements).
3) Receiver may receive frames out of sequence.

Q.13 Give difference between go-back-n and selective repeat.

Ans. :

Sr. No.	Go-Back-N	Selective repeat
1.	Go-back-N requires all retransmission of the succeeding frame along with the lost or damaged frame.	In selective repeat, only the specific damaged or lost frame is retransmitted.
2.	Sender does not require any logic to select the specific frame for retransmission.	Extra logic is required for searching and retransmission of specific frame.
3.	Receiver do not required any sort of storage and sorting mechanism.	The complexity of sorting and storage mechanism is required by the receiver.
4.	It is not expensive.	It is expensive.

END...

Unit III

3 Multi-Access Mechanism and Ethernet Standards

3.1 : Random Access Techniques : CSMA, CSMA/CD, CSMA/CA

Q.1 Explain in brief ALOHA, slotted ALOHA mentioning efficiency advantages in each case. ☞ [SPPU : Dec.-18, Marks 6]

Ans. : • The ALOHA protocol was developed at the university of Hawaii in the early 1970s. ALOHA was developed for packet radio networks. However, it is applicable to any shared transmission medium.

- In a system when multiple users try to send messages to other stations through a common broadcast channel random access or contention techniques are used.
- Random access means there is no definite or scheduled time for any station to transmit. This scheme is simplest possible and it is asynchronous. It is asynchronous because there is no co-ordination among users.
- The basic idea of ALOHA system is applicable to any system in which unco-ordinated users are competing for the use of a single shared channel.
- When a station send data, another station may attempt to do so at the same time. The data from the two station collide and become garbled. If two signals collided, so be it. Each station would simply wait a random time and try again.

Slotted ALOHA

- In slotted ALOHA, the channel time is divided into time slots and the stations are allowed to transmit at specific instance of time. These time slots are exactly equal to the packet transmission time. All users are

then synchronized to these time slots, so that whenever a user generates a packet it must synchronize exactly with the next possible channel slot. Consequently the wasted time due to collisions can be reduced to packet time or vulnerable period is reduced to half.

- Transmission attempts for four network user and random retransmission delays for colliding packets in slotted ALOHA is shown in Fig. Q.1.1

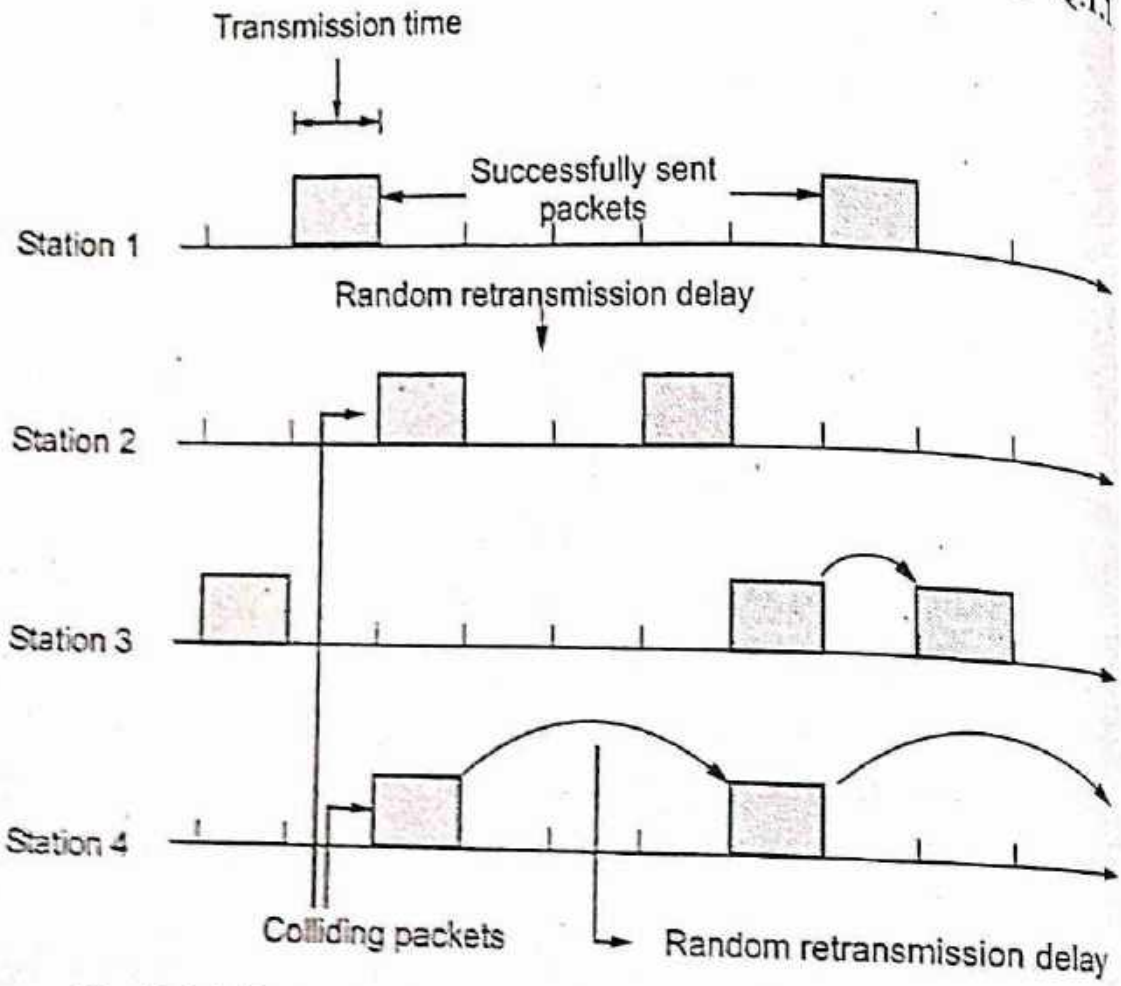


Fig. Q.1.1 Transmission attempts and random retransmission delays for colliding packets in slotted ALOHA

Assumptions :

1. All frames are of same size.
2. Time is divided into equal sized slots, a slot equals the time to transmit one frame.
3. Nodes start to transmit frames only at beginning of slots.
4. Nodes are synchronized.
5. If two or more nodes transmit in a slot, all nodes detects collision before the slot ends.

Throughput of slotted ALOHA channel

- In slotted ALOHA, the packets arrive in a synchronized fashion. The probability of single transmission during a slot time is,

$$p_o = e^{-G} \quad \text{... (Q.1.1)}$$

Also

$$S = G \cdot e^{-G} \quad \text{... (Q.1.2)}$$

The maximum throughput occurs at G = 1,

i.e. $$S = \frac{1}{e} = 0.368$$

which is twice that of pure ALOHA. This means that the best channel utilization that can be achieved is around 37 %.

- The relation between the offered traffic and the throughput is shown in Fig. Q.1.2.

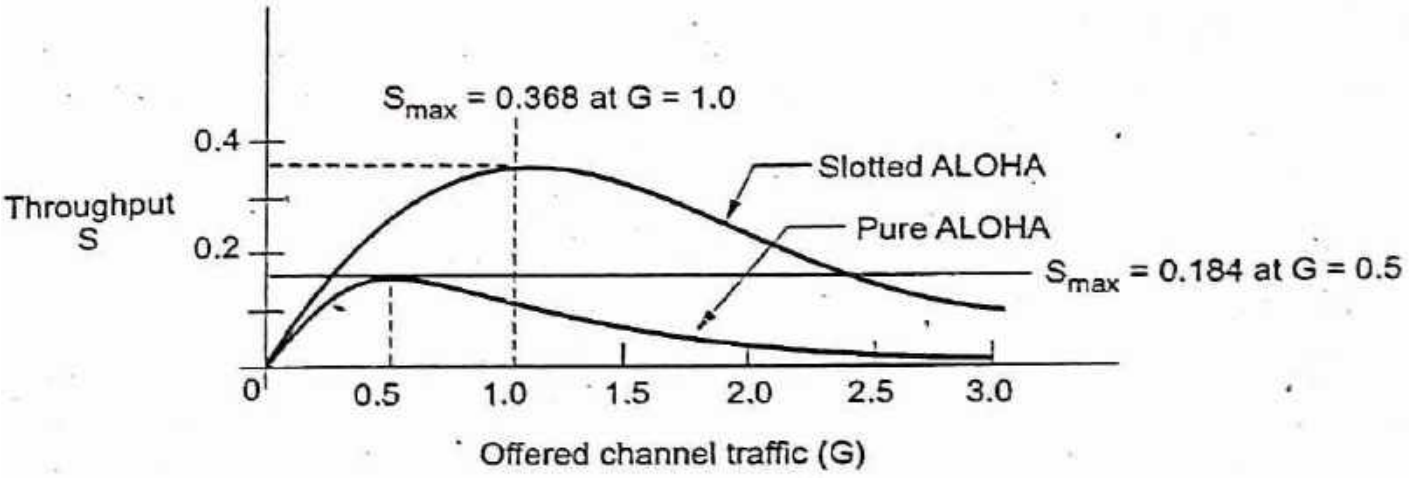


Fig. Q.1.2 Comparison of the throughput as a function of offered load for pure and slotted ALOHA

Pros and Cons of slotted ALOHA

Pros

1. Single active node can continuously transmit at full rate of channel.
2. Highly decentralized, each node independently decides when to retransmit.
3. Simple to implement.

Cons

1. Collisions waste slots.
2. Idle slots.

Q.2 Discuss CSMA/CD random access technique. How collision avoidance achieved in the same ? ☞ **[SPPU : Dec.-17, May-18, 19, Marks 6]**

Ans. : • In both CSMA and ALOHA schemes, collisions involve entire frame transmissions. If a station can determine whether a collision is taking place, then the amount of wasted bandwidth can be reduced by aborting the transmission when a collision is detected. The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) use this approach.

- CSMA/CD is the most commonly used protocol for LANs. CSMA/CD specifications were developed jointly by Digital Equipment Corporation (DEC), Intel and Xerox. This network is called as Ethernet. The IEEE 802.3 CSMA/CD standard for LAN is based on Ethernet specification.
- The basic protocol is that, a station with a message to send must monitor the channel to see if any other station is sending. If another station is sending, the second station must wait or defer, until the sending station has finished. Then it may send its message. If no station was sending at the time that it first listened, the station may send its message immediately. The term "carrier sense" indicates this "listening before transmitting" behaviour.
- If two or more stations have messages to send at the same time and they are separated by significant distances on the bus/channel, each may begin transmitting at roughly the same time without being aware of the other station. The signals from each station will superimpose on the channel and is garbled beyond the decoding ability of the receiving station. This is termed as "collision".
- A protocol is required for transmitting station to monitor the channel while sending each of its messages and to detect such "collisions".
- When a collision has been detected, each of sending stations must cease transmitting, wait for a random length of time, and then try again. Because of quick termination of transmission time and bandwidth is

saved. Therefore CSMA/CD is more efficient than ALOHA, slotted ALOHA and CSMA.

- CSMA/CD networks work best on a bus, multipoint topology with bursty asynchronous transmission. All stations are attached to one path and monitor the signal on the channel through transreceiver attached to the cable.
- CSMA/CD has totally decentralized control and is based on contention access.
- Fig. Q.2.1 illustrates this technique. Station A and station D are the extreme ends of a bus structure.

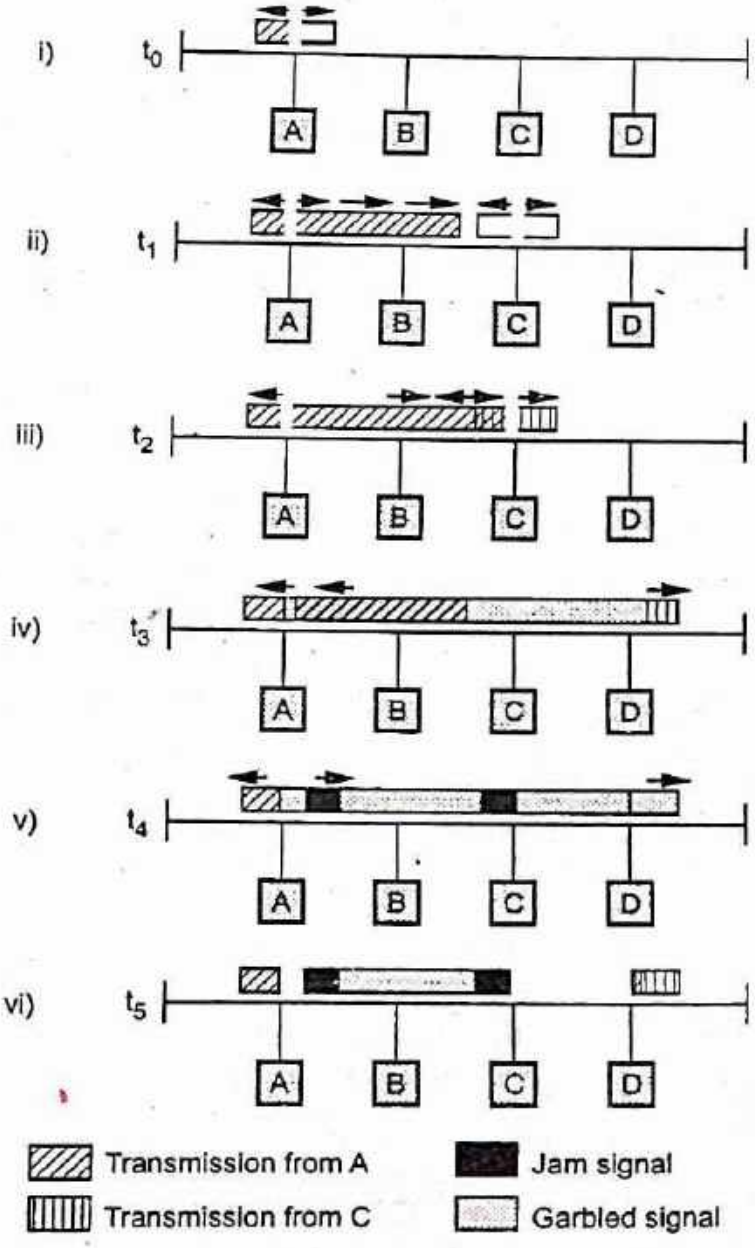


Fig. Q.2.1 CSMA/CD operation

i) Station A listens channel starts transmitting a packet addressing D.

ii) Station B and C are ready for transmission. B senses a transmission on channel so defers. C is unaware of transmission and begins its own transmission.

iii) Station A's transmission reaches C. C detects collision and ceases transmission. Sends jam signal.

iv) Effect of collision propagates back to A, A stops its transmission.

v) A sends jam signal.

vi) No station is transmitting but there are still signals on the bus.

- CSMA/CD supports both baseband and broadband system. CSMA/CD offers four options in terms of bit rate, signaling method and maximum electrical cable segment length. These are,

  1) 10BASE5 2) 10BASE2 3) 10BROAD36 4) 1BASE5

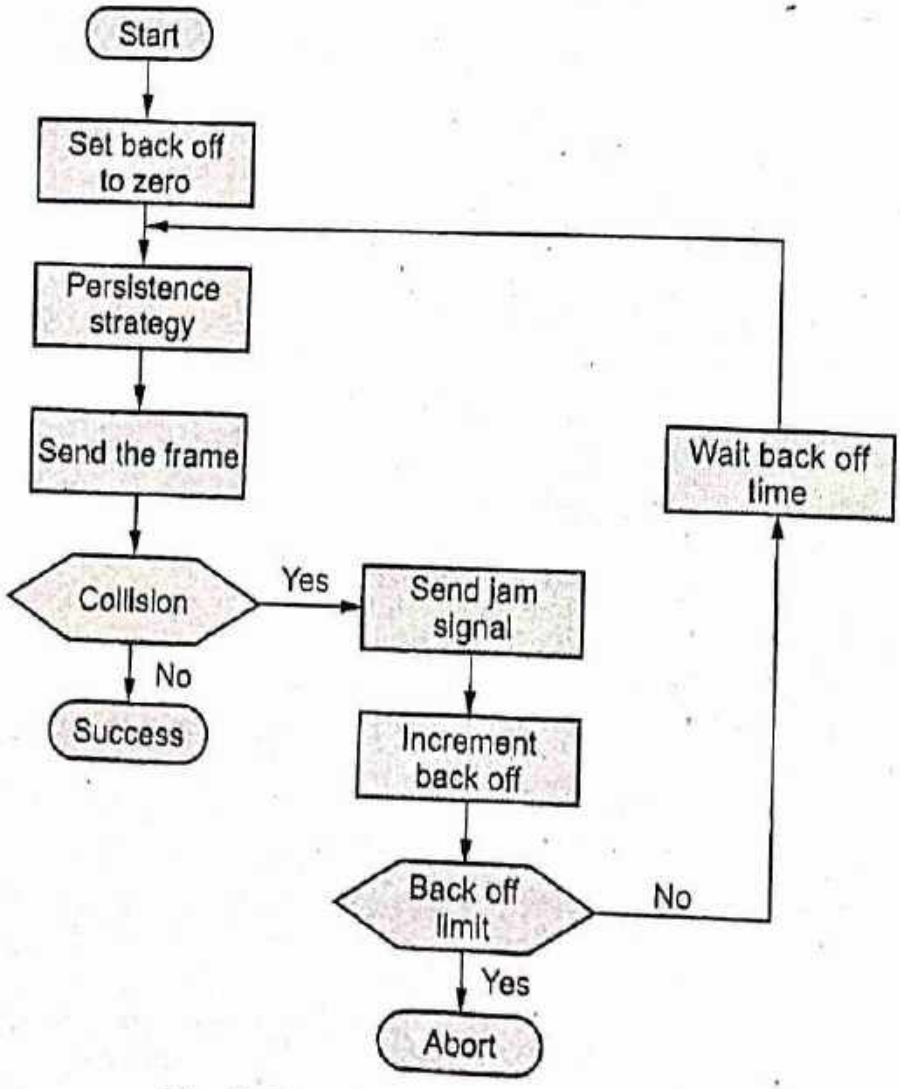


Fig. Q.2.2 Flowchart for CSMA/CD

- The numeric field in the beginning indicates the bit rate in Mbps, the middle term indicates type of signaling system i.e. baseband or broadband, the numeric field in the end indicates the electrical cable segment length in X 100 metres.
- Manchester signal code is used at the baseband level of transmission. In broadband transmission, Differential Phase Shift Keying (DPSK) is used to convert the Manchester encoded signal into analogue form.
- Fig. Q.2.2 shows the flowchart for CSMA/CD procedure.

CSMA/CD throughput

- The throughput of CSMA/CD is greater than that of pure or slotted ALOHA.
- For 1-persistent method, the maximum throughput is around 50 % when G = 1.
- For non-persistent method, the maximum throughput can go upto 90 % when G is between 3 and 8.

Q.3 Discuss CSMA/CA random access technique. How collision avoidance is achieved in this technique ?

☞ [SPPU : May-17, Dec.-18, Marks 6]

Ans. : • Wireless networks cannot use CSMA/CD in the MAC sublayer, since this requires the ability to receive and transmit at the same time - hence the use of CSMA/CA.

- In a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection. We need to avoid collision on wireless networks because they cannot be detected. So CSMA/CA was invented for this network.
- Collisions are avoided by using three methods.
  a. Inter-frame space b. Contention window c. Acknowledgments
- Fig. Q.3.1 shows the all three method of CSMA/CA.

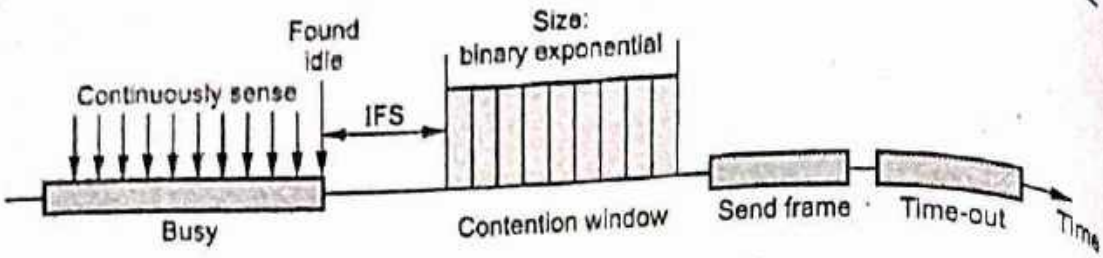


Fig. Q.3.1 CSMA/CA methods

Inter-frame space

- Collisions are avoided by deferring transmission even if the channel is found idle.
- When an idle channel is found, the station does not send immediately. It waits for a period of time called the Inter-Frame Space (IFS).
- In CSMA/CA, the IFS can also be used to define the priority of a station of a frame. A station that is assigned shorter IFS has a higher priority.

Contention window

- Contention windows are an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time.
- Station set one slot for the first time and then double each time the station cannot detect an idle channel after the IFS time.
- In this method, the station needs to sense the channel after each time slot.
- If the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle.
- This method gives the priority to the station with the longest waiting time.

Acknowledgments

- The data may be corrupted during the transmission. The positive acknowledgment and the time out can help guarantee that the receiver has received the frame.
- Fig. Q.3.2 shows the flowchart for CSMA/CA.

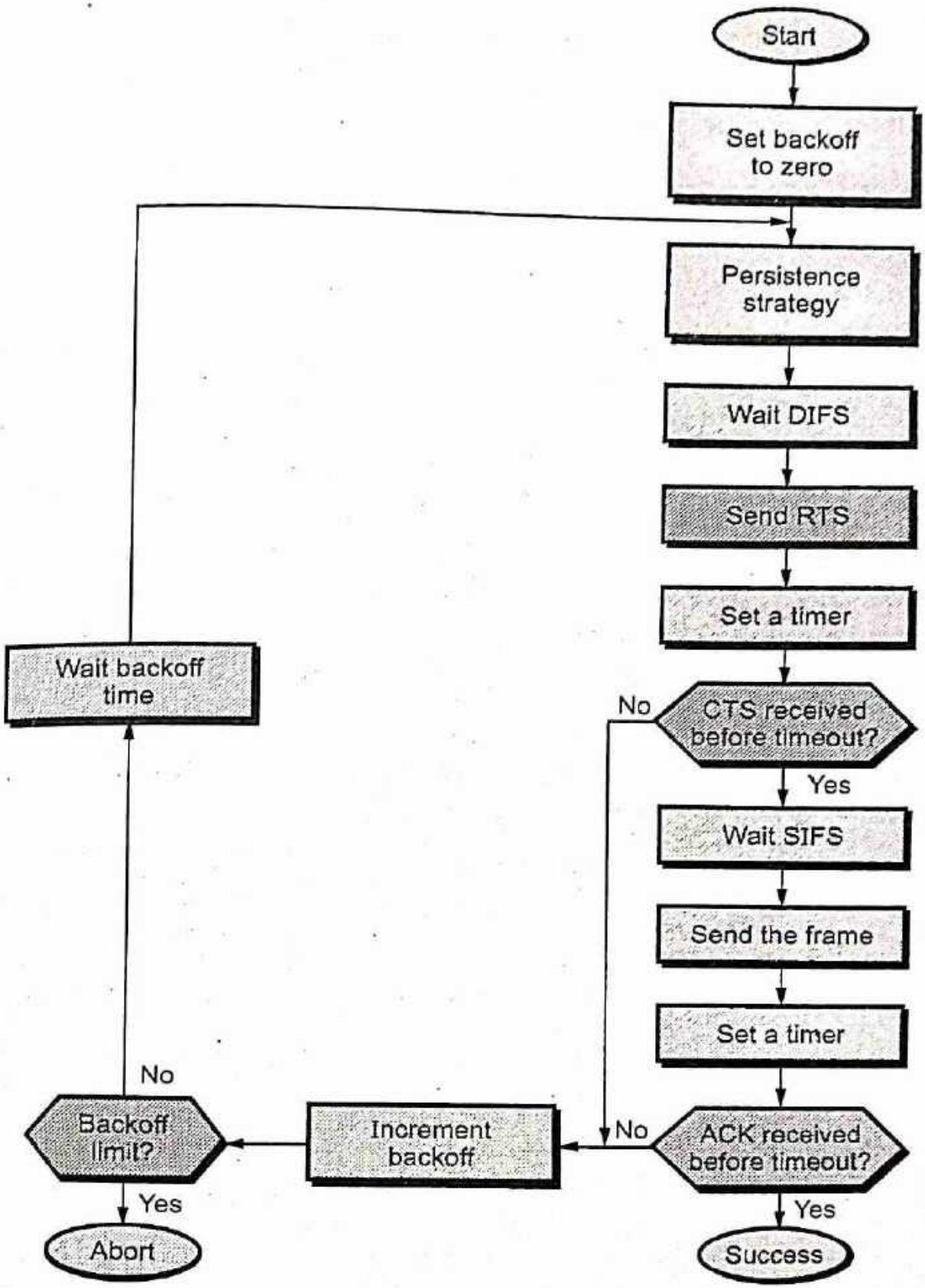


Fig. Q.3.2 Flowchart for CSMA/CA

Hidden Node Problem

- In the case of wireless network it is possible that A is sending a message to B, but C is out of its range and hence while "listening" on the network it will find the network to be free and might try to send packets to B at the same time as A. So, there will be a collision at B.
- The problem can be looked upon as if A and C are hidden from each other. Hence it is called the "hidden node problem".
- Fig. Q.3.3 shows node A is transmitting.

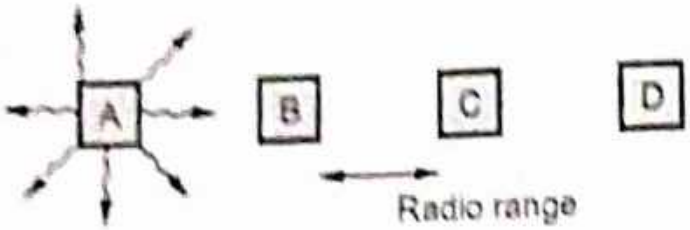


Fig. Q.3.3 A transmitting

Exposed Node Problem

- If C is transmitting a message to D and B wants to transmit a message to A, B will find the network to be busy as B hears C transmitting. Even if B would have transmitted to A, it would not have been a problem at A or D.
- CSMA/CD would not allow it to transmit message to A, while the two transmissions could have gone in parallel.
- Fig. Q.3.4 shows node B is transmitting.

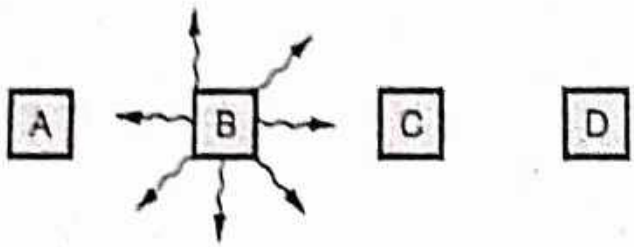


Fig. Q.3.4 B transmitting

Q.4 Explain CSMA / CA / and CSMA / CD random access technique with suitable diagram / flowchart. Also comment on efficiency of each. ☞ **[SPPU : June-22, Marks 8]**

Ans. : Refer Q.2 and Q.3.

3.2 : Controlled Access Techniques : Reservation, Polling, Token Passing

Q.5 Explain the various controlled access methods.

☞ [SPPU : Dec.-17, Marks 6]

Ans. :

1. In this, the stations consult one another to find which station has the right to send.
2. A station cannot send unless it has been authorized by other stations.
3. Controlled access methods are :
   i. Reservation ii. Polling iii. Token passing.

I. Reservation

1. Before sending data, station needs to make a reservation.
   Fig. Q.5.1 shows the reservation access method.

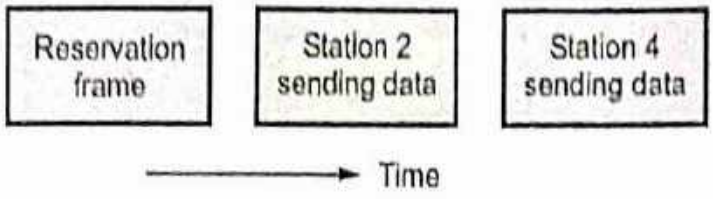


Fig. Q.5.1 Reservation access method

2. Number of reservation are equal to number of stations.
3. Each station have their own minislot in the reservation frame.
4. When station needs to send a data frame, it makes a reservation in its own minislot.
5. The stations that have made reservations can send their data frames after the reservation frame.
6. In the first slot, only station 1, 3 and 4 have made reservation.

II. Polling

1. Polling works with topology.
2. One device is designed as primary station and other devices are secondary station.
3. Link control is done by primary device.
4. All data exchange take place through primary device.
5. Primary device decides, which device is allowed to use the channel at a given time.

6. If primary device wants to receive data, it asks the secondaries if they have anything to send, this function is called **polling.**
7. Select mode and poll mode are the two functions of polling.
8. In polling, primary device receive the data.
9. In select mode, primary device sends data to secondary device.

Fig. Q.5.2 shows the select mode.

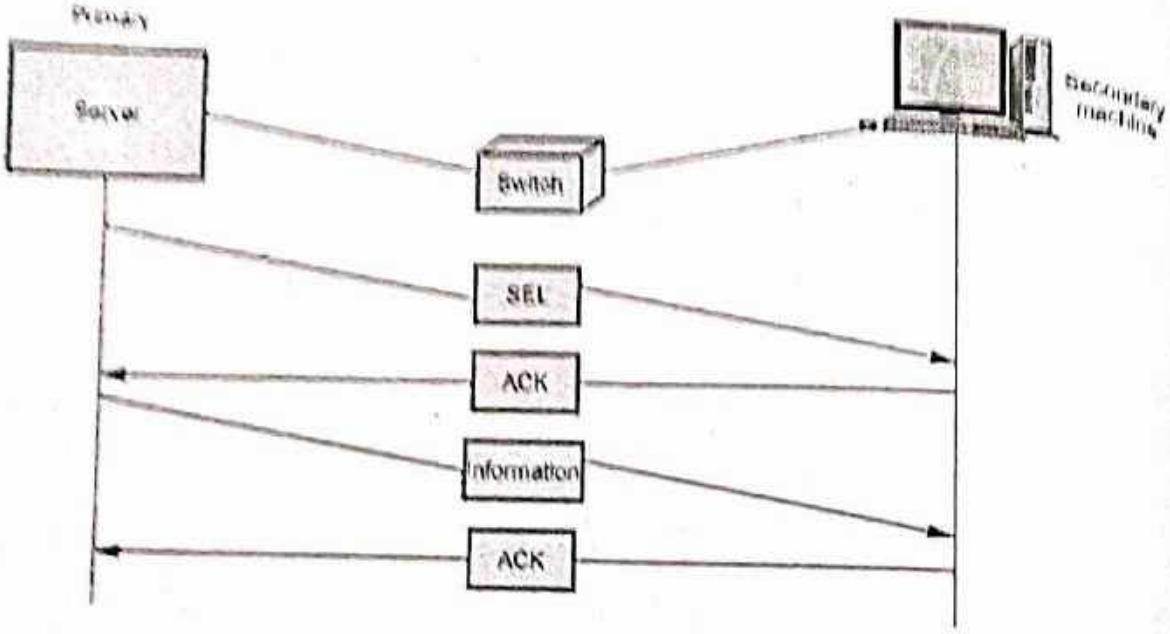


Fig. Q.5.2 Select mode

10. Link is available if primary device is not sending or receiving any data.
11. Before sending data, the primary creates and transmits a select (SEL) frame.
12. SEL frame includes address of the intended secondary device.

Fig. Q.5.3 shows the poll method. (Refer Fig. Q.5.3 on next page)

III. Token Passing

1. A station is allowed to send data when it receives a token (special frame).
2. Ring topology is used for connecting devices.
3. Each station has a predecessor and a successor.
4. Frames are coming from predecessor and going to the successor.
5. Token is circulates around the ring.

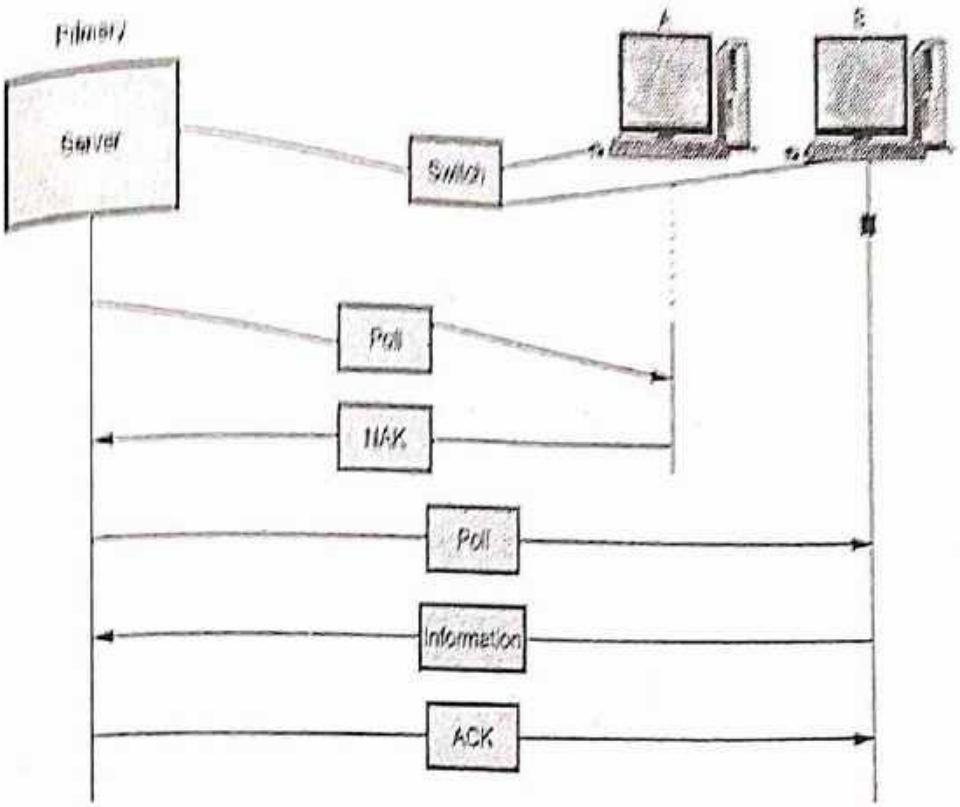


Fig. Q.5.3 Polling method

6. The station captures the token if they want to send data.

   Fig. Q.5.4 shows token passing network.

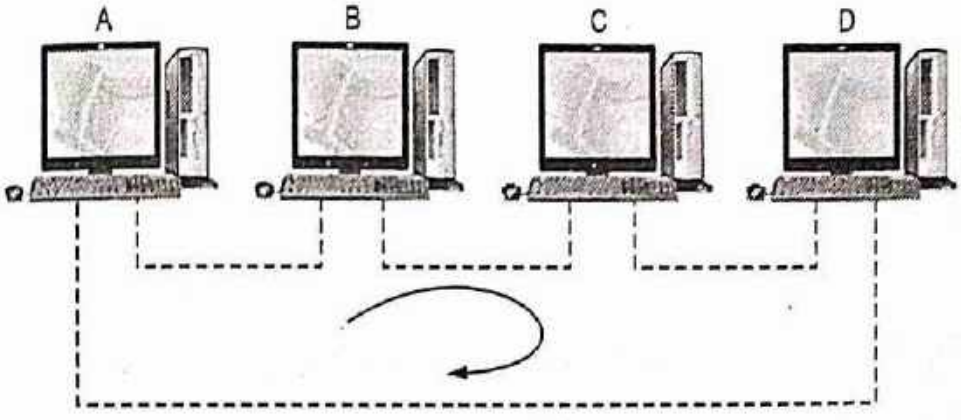


Fig. Q.5.4 Token passing network

7. Flowchart for token passing procedure is shown in Fig. Q.5.5. (See Fig. Q.5.5 on next page)

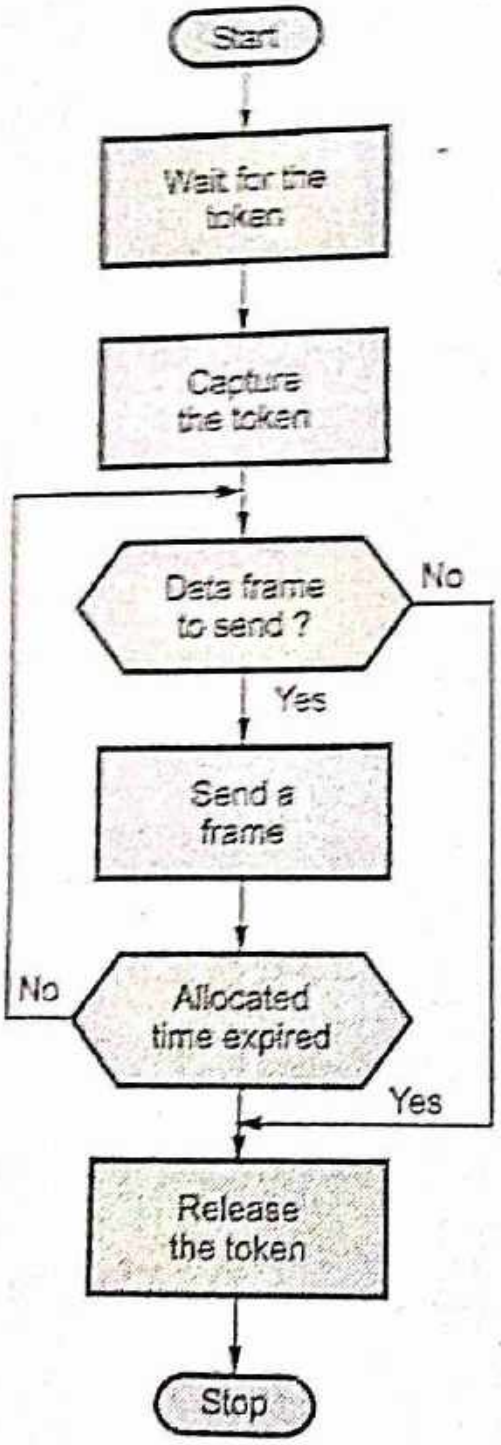


Fig. Q.5.5 Flowchart for token passing

3.3 : Channelization : FDMA, TDMA, CDMA

Q.6 Explain FDMA, TDMA and CDMA in detail.

☞ [SPPU : May-17, Marks 6]

Or Compare FDMA, CDMA, TDMA. ☞ [SPPU : Dec.-17, Marks 6]

Or Explain TDMA and CDMA with neat diagram.

☞ [SPPU : May-18, Dec.-19, Marks 6]

Or Write a note on channelization techniques (Any Two)
i) FDMA ii) TDMA iii) CDMA ☞ [SPPU : June-22, Marks 8]

Ans. : • Channelization is the multiple access method. Multiple access is the technique of sharing or dividing channel (transmission medium) for number of stations sharing it.

• Three most commonly used multiple access methods are -

1. Frequency Division Multiple Access (FDMA)
2. Time Division Multiple Access (TDMA)
3. Code Division Multiple Access (CDMA)

i) FDMA

• In FDMA the available bandwidth is divided into M number of smaller frequency bands called **sub bands**. Each station transmits its information continuously on an assigned sub band. To reduce the co-channel interference, guard band between two sub bands is provided.

If W = Available BW of channel

R = Data rate of channel

M = Number of stations

Then the transmit rate of each station is $\frac{R}{M}$ bits/sec.

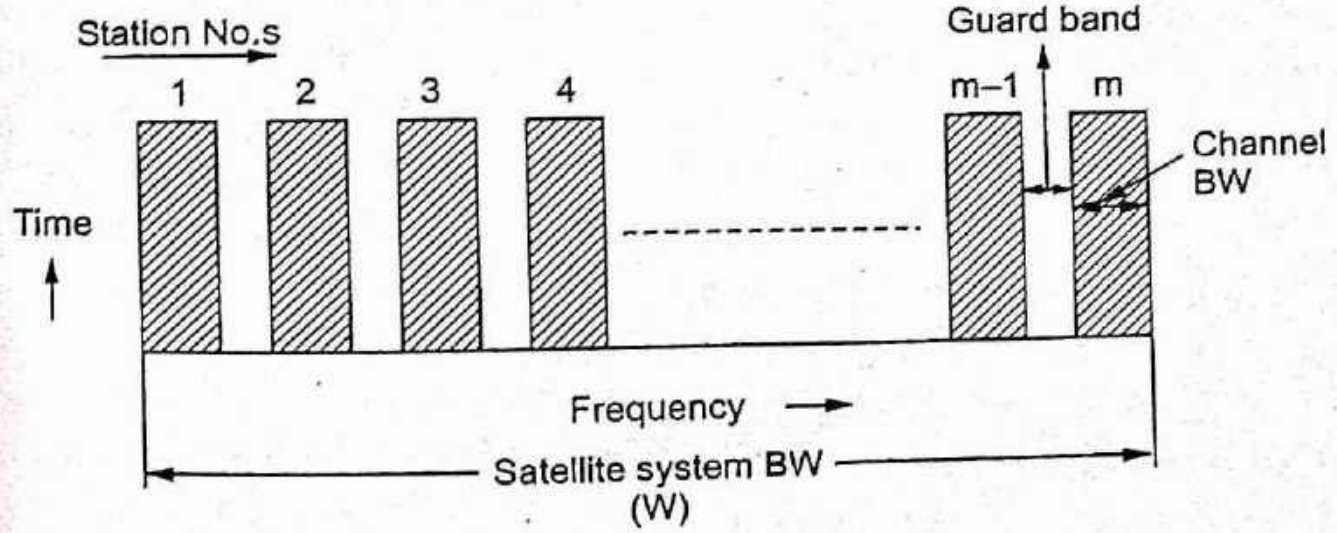


Fig. Q.6.1 FDMA

- FDMA transmissions are separated in frequency domain i.e. total available transponder bandwidth is shared by stations. Fig. Q.6.1 shows how FDMA stations use a fixed portion of frequency band all the time.
- FDMA is not suited for bursty traffic conditions because of inefficient use of transmission resources.

ii) TDMA

- TDMA is a method of time-division multiplexing of digitally modulated carriers. In TDMA, each station transmits digitally modulated carriers during a preassigned time slots, making use of the entire transmission channel during its transmission. The stations are synchronized such that only one carrier is present on the channel at any given time. Thus avoiding collisions of stations. Sufficient guard bands are also provided to ensure collision avoidance.
- Each station spends most of the time accumulating packets and preparing them for transmission in a burst during the assigned time slot. The average bit rate of each channel is same because time slot available is same for each station.
- Fig. Q.6.2 shows how TDMA stations use a fixed portion of time slot in the frequency band.

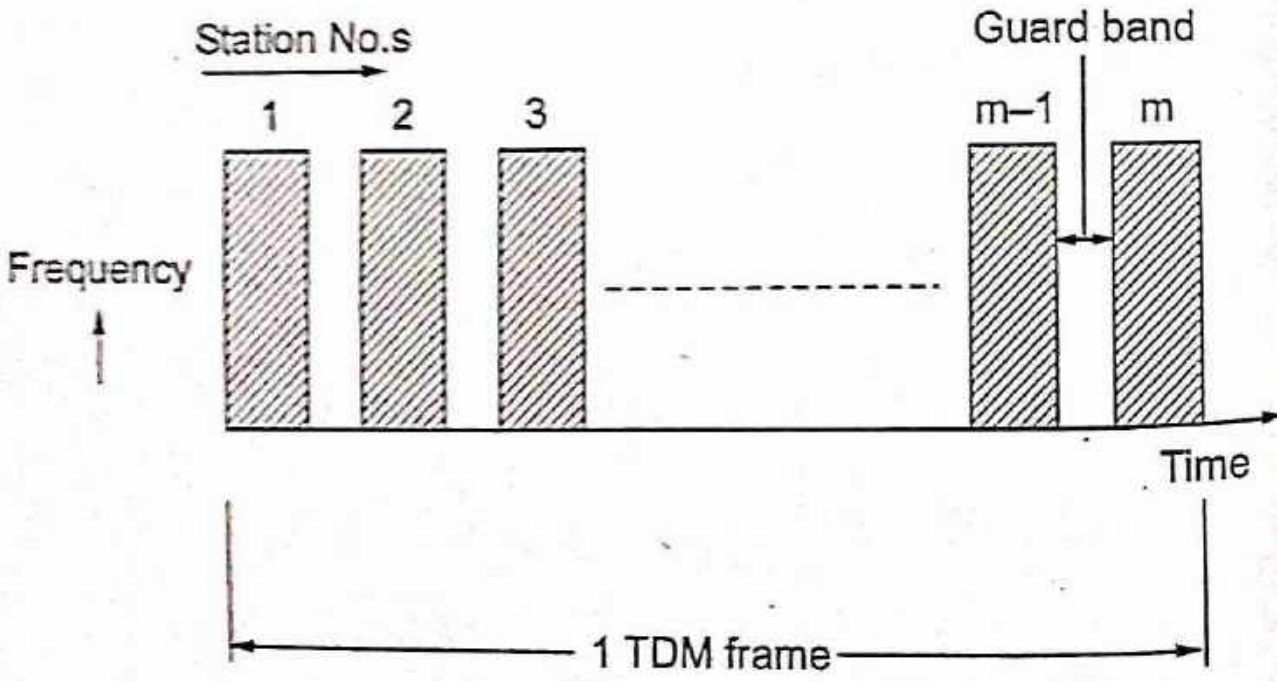


Fig. Q.6.2 TDMA

Advantages of TDMA :

1. At a given time only one carrier is present on the channel hence intermodulation distortion is eliminated.
2. TDMA transmission is separated in time domain. Processing of signal in time domain is easier.
3. TDMA is most efficient method of transmission because of efficient use of transmission resources.
4. TDMA can accomodate a wider range of bit rates by allowing a station to be allocated several slots. Thus TDMA is more flexible than FDMA.

Disadvantages of TDMA :

1. Precise synchronization between stations is required. Transmission of every station must occur during exact time slot.
2. Bit and frame timings must be maintained by TDMA.

iii. CDMA

- In CDMA each station transmitter may transmit whenever it requires and can use entire bandwidth i.e. there are no restrictions on time and bandwidth. CDMA is also called as **spread spectrum multiple access** because transmission can spread throughout the bandwidth. Each station is assigned a unique binary code, this code is called as **chip code**. Each station and transmission is identified by its chip code. The receiver uses

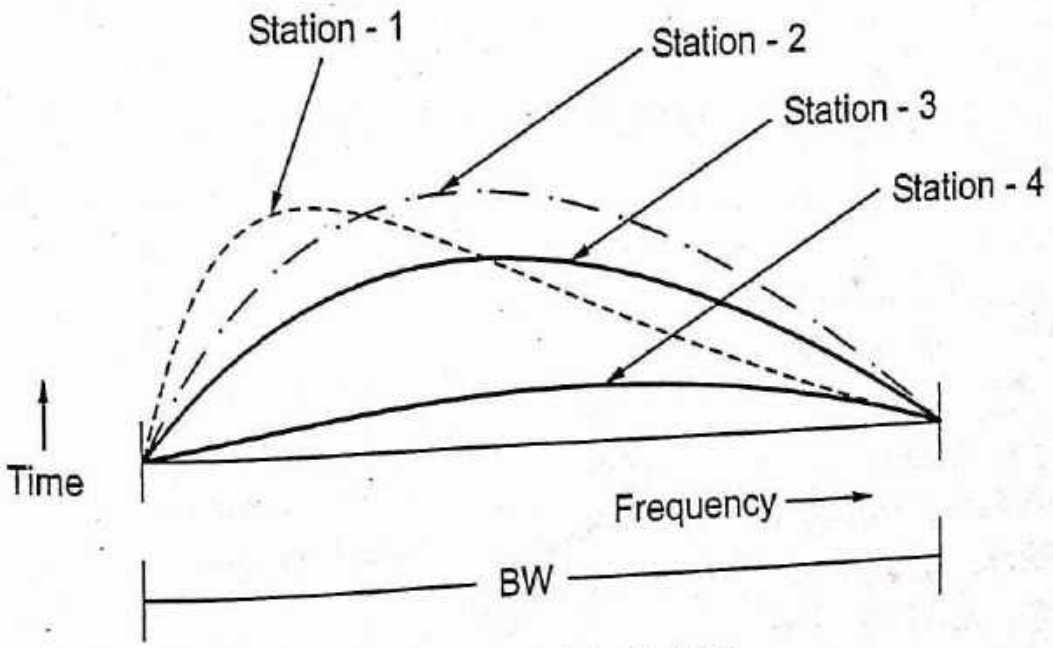


Fig. Q.6.3 CDMA technique

chip code to recover the signal from desired station. Fig. Q.6.3 shows conceptual view of CDMA technique.

Applications of CDMA :

1. CDMA is used for wireless systems with fixed base station and many mobile station at varying distance from it.
2. CDMA is used in satellite systems so that many signals can use a transponder; making it more efficient.
3. CDMA is used in digital cellular telephone services because it permits more users to occupy a given band.
4. Wideband CDMA (W-CDMA) is used for digital cell phone systems to accommodate voice transmission alongwith high speed data, FAX and internet communication.
5. CDMA is ideally suited for military application because of immunity to noise.

Advantages of CDMA :

1. Each station can use the entire bandwidth at any time.
2. High immunity for interference or jamming.

Disadvantages of CDMA :

1. The overall performance degrades with increase in number of users.
2. Time synchronization of stations is required.

3.4 : Ethernet : IEEE Standards - IEEE 802.3

Q.7 Explain the frame format for IEEE 802.3.

☞ [SPPU : May-17, Dec.-17, Marks 7]

Or Draw and explain each field of MAC frame format of IEEE 802.3.

☞ [SPPU : May-19, Dec.-19, Marks 6]

Ans. : • Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.

• The frame format of the MAC is shown in Fig. Q.7.1.

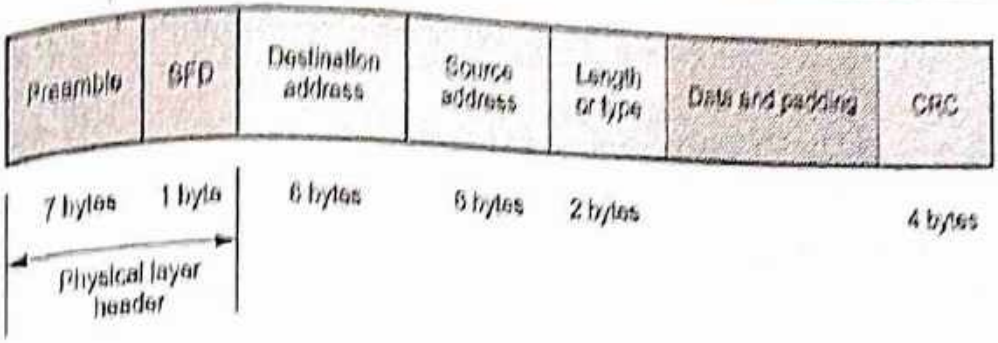


Fig. Q.7.1 802.3 Frame format

1. **Preamble** : A 7-byte pattern of alternating 0s and 1s used by the receiver to establish bit synchronization. Each frame contains the bit pattern 10101010. The pattern provides only an alert and a timing pulse. The preamble is actually added at the physical layer and is not part of the frame.
2. **Start Frame Delimiter (SFD)** : The sequence 10101011, which indicates the actual start of the frame and enables the receiver to locate the first bit of the rest of the frame.
3. **Destination Address (DA)** : The DA field is 6 bytes and specifies the station for which the frame is intended. It may be a unique physical address, a group address or a global address.
4. **Source Address (SA)** : The SA field is also 6 bytes and contains the physical address of the sender of the packet.
5. **Length or Type** : Length of LLC data field in octets, or Ethernet Type field, depending on whether the frame conforms to the IEEE 802.3 standard or earlier Ethernet specification. In either case, the maximum frame size, excluding preamble and SFD, is 1518 bytes.
6. **Data** : Data unit supplied by LLC. It is a minimum of 46 bytes and a maximum of 1500 bytes.
7. **CRC** : This field contains error detection information.

Q.8 Explain the following physical layer implementation in standard Ethernet :

i) 10Base5 ii) 10BaseT iii) 10BaseF

with respect to media, maximum length and line encoding.

☞ **[SPPU : Dec.-18, Marks 6]**

Ans. : • CSMA/CD offers various options in terms of transmission medium, signalling technique, data rate and maximum electrical cable segment length.

• Table Q.8.1 summarizes these options defined for the IEEE 802.3 medium.

Sr. No.	Medium options	Transmission medium	Signaling technique	Data rate (Mbps)	Maximum segment length (m)
1.	10BASE5	Coaxial cable (50 ohm)	Baseband (Manchester)	10	500
2.	10BASE2	Coaxial cable (50 ohm)	Baseband (Manchester)	10	185
3.	1BASE5	Unshielded twisted pair	Baseband (Manchester)	1	250
4.	10BASET	Unshielded twisted pair	Baseband (Manchester)	10	100
5.	10BROAD36	Co-axial cable (75 ohm)	Broad band (DPSK)	10	3600
6.	10BASEF	Fiber optics	Baseband	10	2000

Table Q.8.1 IEEE 802.3 medium options

1) **10BASE5 :** It is popularly called as **thick ethernet**. The notation 10BASE5 means that it operates at 10 Mbps, uses baseband signaling and can support segment upto 500 metres. The length of the network can be extended using repeaters. The standard allows a maximum of four repeaters in the path between any two stations, extending the effective length of the network to 2.5 km.

Application : 10BASE5 is generally used as low cost alternative for fiber optic media for use as a backbone segment with in a single building. Its extended length, higher attached device count and better noise resistance make 10BASE5 well suited for use as a network trunk for one or more floors in a building. However the high cost of connecting each device makes 10BASE5 too expensive for most LAN installations a single break or bad connection in the cable can bring the entire network down.

2) **10BASE2 :** It is popularly called as chepearnet or thin ethernet. It uses thin co-axial cable. The thinner cable results in significantly cheaper cost, at the penalty of fewer stations and shorter length. Therefore 10BASE2 is limited to a maximum of 30 network devices per unrepeated network segment with a minimum distance of 0.5 m. And segment length is reduced to 185 metres.

Application : For small budget conscious installations, 10BASE2 is the most economical topology such as UNIX work stations.

The disadvantages of 10BASE2 is that any break in the cable or poor connection will bring the entire network down and repeaters are required if more than 30 devices are connected to the network or the cable length exceeds 185 m.

3) **1BASE5 :** It is also known as star LAN. It specifies operation at 1 Mbps, using a passive star topology.

Application : This options is substantially lower in cost than either of coaxial cable options. This options could be appropriate for a departmental-level LAN.

4) **10BASET :** 10BASET is 10 MHz ethernet running over UTP cable. It also uses passive star topology. The maximum cable segment allowed is 100 - 150 metres. There is no minimum distance requirements between devices, such devices cannot be connected serially but in star wired. Maximum 1024 stations can be connected to network.

Application : 10BASET is the most flexible topology for LAN's and is generally the best choice for network installations. 10BASET hubs or multi-hub concentraters, are typically installed in a central locations to the user community. The signalling technology is very reliable even in somewhat noisy environments it automatically shutdown the offending parts without affecting the rest of the network. Cabling is cheaper and requires less skill to install. Maintenance is easy.

The disadvantages are the hardware required is more expensive and maximum cable run from hub is 100-150 metre.

5) **10BROAD36 :** It is a 10 Mbps broadband option. It provides support to more stations over greater distances than the baseband versions. The maximum cable run is restricted to 3600 m in two segments of 1800 m from the head end. Other services such as TV or voice can also be integrated on the same cable using FDM.

6) **10BASEF :** 10BASEF is 10 Mbps running over fiber optic cabling. The maximum cable length depends on signaling technology and

medium used but can go upto 2 km unrepeated segment. It is star wired so there is no minimum distance requirement between devices.

Application : 10BASEF is the only recommended topologies for inter-building links. However they need not be limited to this role, it can also run to desktop. It has excellent noise immunity.

- The disadvantage is, it is very expensive due to the cost of connectors and terminators.

3.5 : IEEE 802.4

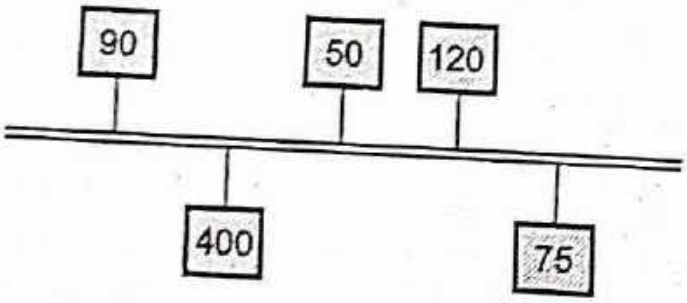
Q.9 Write short note on IEEE 802.4 (Token Bus).

☞ [SPPU : Dec.-18, Marks 4]

Ans. : • IEEE 802.4 describes a token bus LAN standards.

- In token passing method stations, connected on a bus are arranged in a logical ring. When the logical ring is initiated, the highest numbered station may send the first frame. After this it passes permission to its immediate neighbour by sending a special control frame called a token.

Physical topology



Logical sequence of token passing

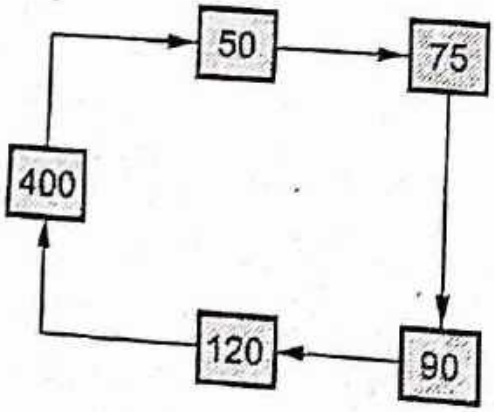
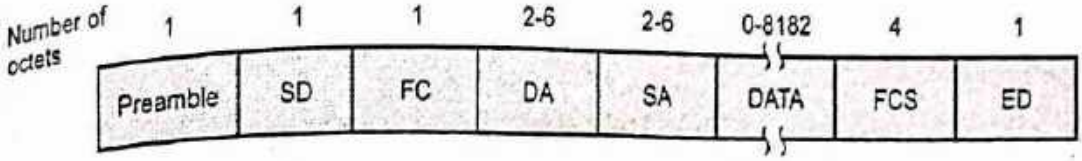


Fig. Q.9.1 Token passing sequence in a bus

The token propagates around the logical ring, with only the token holder being permitted to transmit frames. Since only one station at a time holds the token, collisions do not occur.

- There is no relation between the physical location of the station on the bus and its logical sequence number. Fig. Q.9.1 illustrates the operation of token bus.
- The token bus frame format is shown in Fig. Q.9.2. It consists of following fields.



Preamble : Bit synchronization
SD : Frame start delimiter
FC : Frame control
DA : Destination address
SA : Source address
DATA : Data field
FCS : Frame check sequence
ED : End delimiter

Fig. Q.9.2 802.4 frame format

- **Preamble :** The preamble is an at least one octet-long pattern to establish bit synchronization.
- **Start Delimiter (SD) :** It is a one octet-long unique bit pattern which marks the start of the frame.
- **Frame Control (FC) :** The frame control field is used to distinguish data frames from control frames. For data frame, it carries the frames priority. The frame control field indicates the type of the frame data frame or control frame.
- **Destination Address (DA) :** The destination address field is 2 or 6 octets long.
- **Source Address (SA) :** The source address field is also 2 or 6 octets long.

- **Frame Check Sequence (FCS) :** Frame check sequence is 4 octets long and contains CRC code. It is used to detect transmission errors on DA, SA, FC and data fields.
- **End Delimiter (ED) :** It is a unique bit pattern which marks the end of frame. It is one octet long.
- The total length of the frame is 8191 octets.

802.4 Performance :

- For token ring, the slightly higher delay compared to CSMA/CD bus occurs. For higher transmission loads the token ring performs well.

3.6 : IEEE 802.5

Q.10 Write short note on IEEE 802.5 (Token Ring).

☞ [SPPU : Dec.-18, Marks 3]

Ans. : • In a token ring a special bit pattern, called the **token**, circulates around the ring whenever all stations are idle.

- When a station transmits, it breaks the ring and inserts its own frame with destination and source addresses.

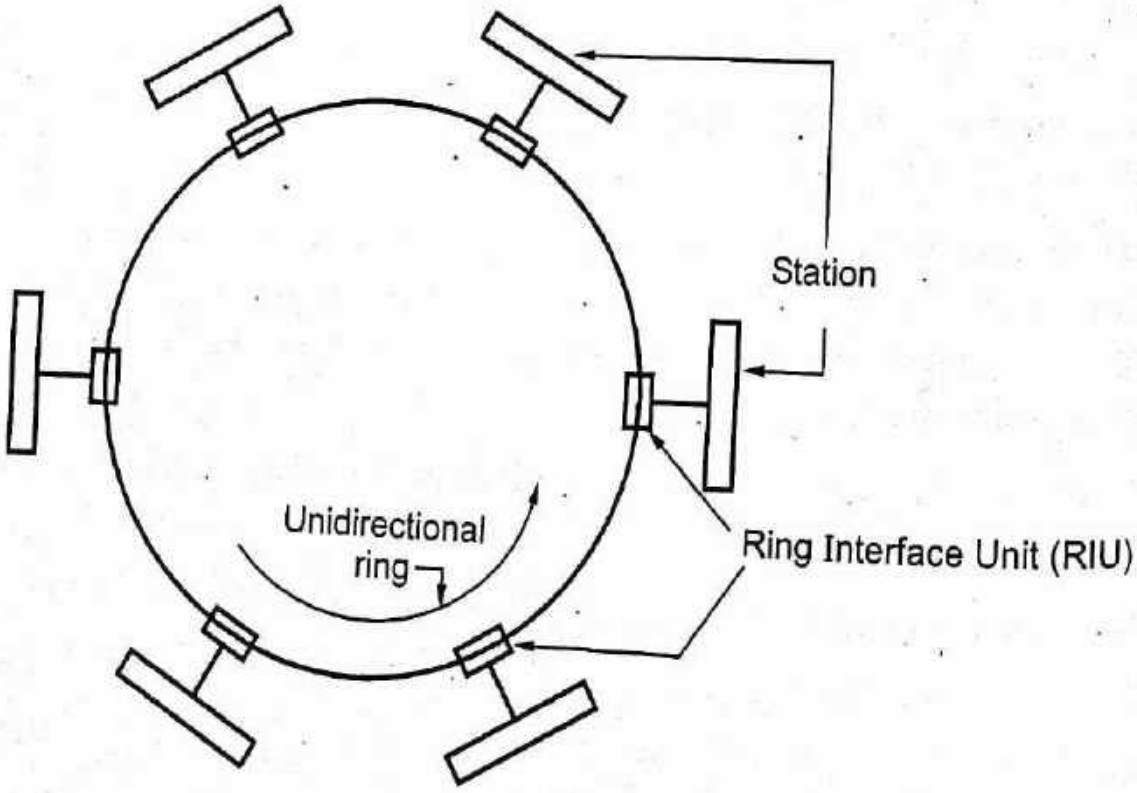


Fig. Q.10.1 A ring network

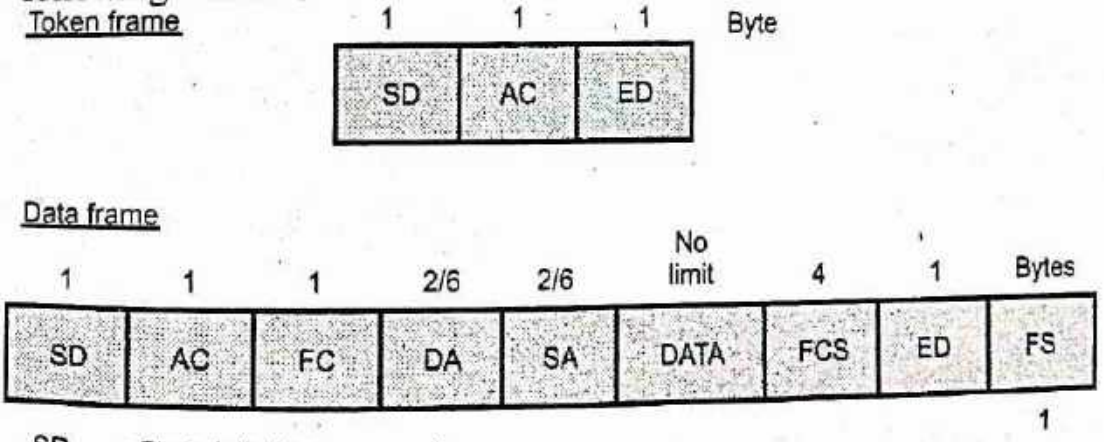
- When the frame eventually returns to the originating station after completing the round, the station removes the frame and closes the ring. Because there is only one token, only one station can transmit at a given instant, thus solving the channel access problem. .
- Fig. Q.10.1 shows token ring arrangement.
- Each station is connected to the ring through a Ring Interface Unit (RIU). The sequence of token is determined by the physical locations of the stations on the ring.

IEEE 802.5 cable standards :

- The token ring standard IEEE 802.5 specifies two types of transmission medium discussed below.
  1) **Shielded Twisted Pair (STP) :** It uses differential Manchester signaling technique. Data rate is 4 or 16 Mbps. Maximum number of repeaters allowed is 250.
  2) **Unshielded Twisted Pair (UTP) :** It uses differential Manchester signaling technique. Data rate is 4 Mbps, maximum number of repeaters allowed is 250.

IEEE 802.5 Frame Format

- The IEEE 802.5 token protocol is shown in Fig. Q.10.2. It consists of following fields.



SD : Start delimiter
AC : Access control
FC : Frame control
DA : Destination address
SA : Source address
DATA : Data field
FCS : Frame check sequence
ED : End delimiter
FS : Frame status

Fig. Q.10.2 Formats of IEEE 802.5 frames

- **Start Delimiter (SD) :** Start delimiter field marks the beginning of the frame. It is one octet long unique bit pattern.
- **Access Control (AC) :** It is a one octet long field containing priority bits (P), token bit (T), monitoring bit (M), and reservation bits (R).
- **Frame Control (FC) :** It is one octet long field and indicates the type of frame data frame or control frame. It also distinguishes the control frames.
- **Destination Address (DA) :** The destination address field is 2 or 6 octets long.
- **Source Address (SA) :** The source address field is also 2 or 6 octets long.
- **Data Field :** It can have 0 or more octets. There is no maximum size but the frame transmission time is limited by the token holder timer.
- **Frame Check Sequence (FCS) :** The frame check sequence is 4 octets long and contains the CRC code. It checks on DA, SA, FC and data fields.
- **End Delimiter (ED) :** It is one octet long and contains a unique bit pattern marking the end of a token or data frame.
- **Frame Status (FS) :** This field is one octet long and contains a unique bit pattern marking the end of a token or data frame.

Token Ring Performance :

- When traffic is light, the token will spend most of its time idly circulating around the ring. When traffic is heavy, there is a queue at each station. The network efficiency can approach 100 % under conditions of heavy load.

Q.11 Compare IEEE 802.3, IEEE 802.4, IEEE 802.5 in a tabular format.

☞ [SPPU : June-22, Marks 9]

Ans. :

Sr. No.	802.3	802.4	802.5
1.	Size of the frame format is 1572 bytes.	Size of the frame format is 8202 bytes.	Variable size
2.	Size of the data field is 0 to 1500 bytes.	Size of the data field is 0 to 8182 bytes.	No limit
3.	No priorities.	It supports priorities.	Priorities are possible.
4.	Non deterministic.	More deterministic than 802.3.	Deterministic
5.	Minimum frame required is 64 bytes.	It can handle short minimum frames.	It supports short frames.
6.	Efficiency decreases when speed increases and collision affects the throughput.	Throughput and efficiency at high load are excellent.	Throughput and efficiency at high load are excellent.
7.	Modems are not required.	Modems are required.	Modems are required.
8.	Protocol is simple.	Protocol is extremely complex.	Protocol is moderately complex.

3.7 : IEEE 802.6

Q.12 Explain IEEE 802.6.

Ans. : The IEEE 802.6 standard describes a MAN (Metropolitan Area Network) standard called DQDB (Distributed Queue Dual Bus).

- Fig. Q.12.1 shows architecture of the DQDB metropolitan area network.

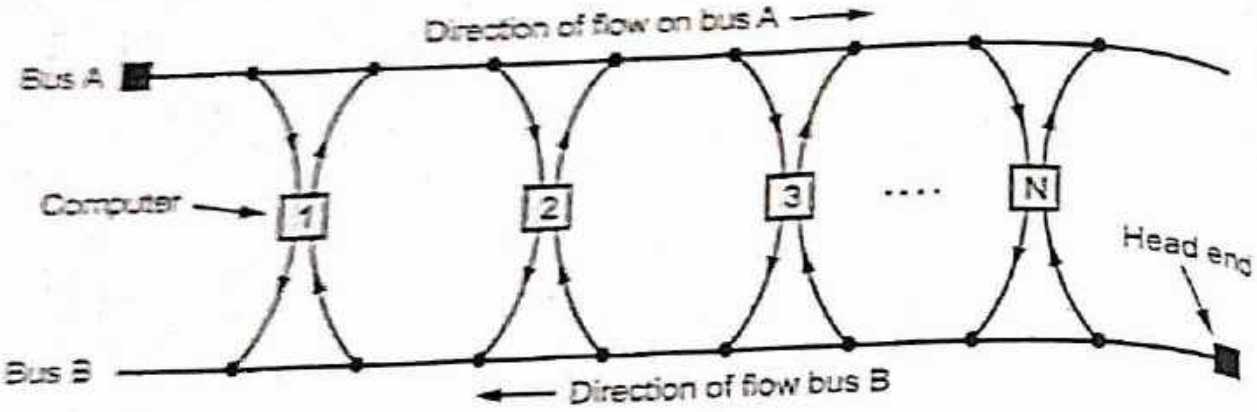


Fig. Q.12.1 Architecture of the DQDB metropolitan area network

- The network is defined as a high-speed shared medium access protocol for use over a dual, counter-flowing, unidirectional bus networks. The use of paired bus provides a failure tolerant configuration.
- DQDB is able to carry data, voice, and video transmissions, with bandwidth being allocated using time slots on the bus.
- It can cover an entire city, upto 160 km at a rate of 44.736 Mbps.
- Basic rule : If you want to send some thing to one of your right hand neighbours, use upper bus A; otherwise, lower bus B.
- Direction of flow on a bus points to down stream. Fixed-size 53-byte cells with 44-byte payload are used, similar to ATM.
- Stream of cells flows down on a bus. Each cell has a busy(B) bit and request (R) bit. If a cell is occupied, its B bit is 1. You make a request by setting a cell's R bit to 1.

3.8 : Fast Ethernet

Q.13 Discuss Fast Ethernet technology in brief. State its specification.

☞ [SPPU : May-17, Marks 6]

Or Explain following physical layer implementation in Fast Ethernet:
i) 100BaseTX ii) 100BaseFX iii) 100BaseT4
with respect to media, maximum length and line encoding.

☞ [SPPU : May-19, Marks 6]

Or Compare 100BASE-TX, 100BASE-FX, 100BASE-T4.

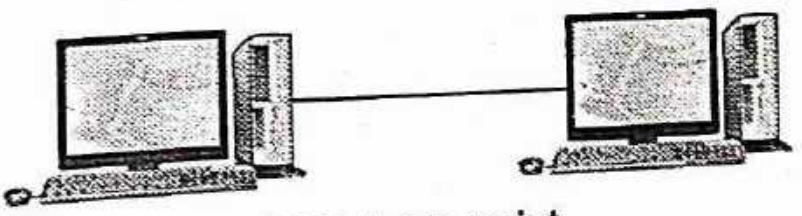
☞ [SPPU : Dec.-17, Marks 7]

Ans. : • Fast ethernet is backward compatible with standard ethernet. The goals of fast ethernet can be :

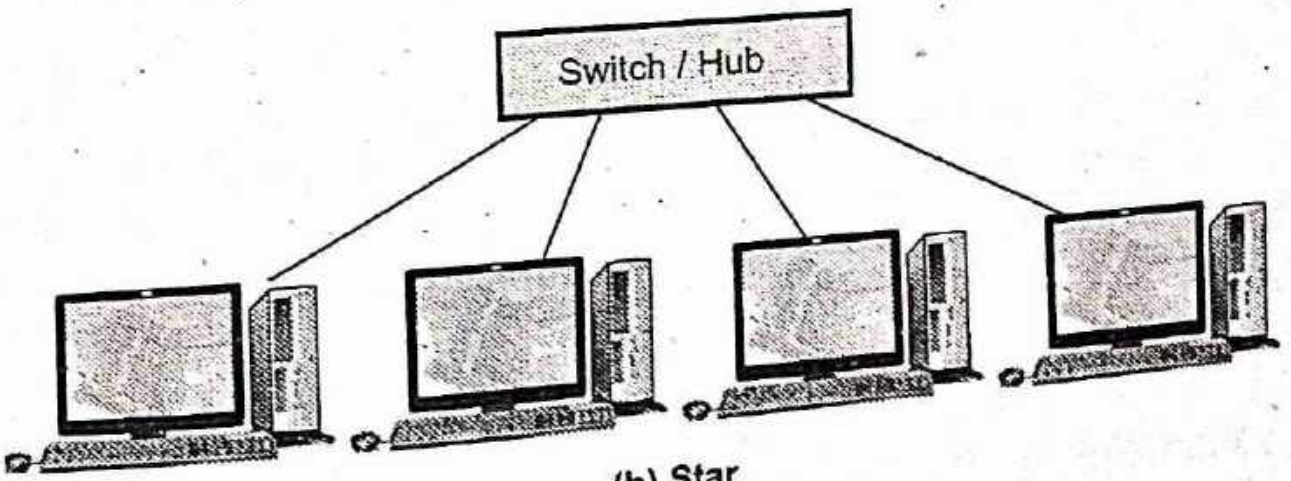
1. Upgrade the data rate to 100 Mbps.
2. Keep the same 48-bit address.
3. Keep the same frame format.
4. Make it compatible with standard ethernet.
5. Keep the same minimum and maximum frame length.

- Fast ethernet refers to a set of specifications developed by the IEEE 802.3 committee to provide a low cost, ethernet compatible LAN operating at 100 Mbps. A traditional ethernet is half duplex : A station can either transmit or receive a frame, but it cannot do both simultaneously.
- Fast ethernet supports the full duplex with full duplex operation, a station can transmit and receive simultaneously. In fact, there is no collisions and the CSMA/CD algorithm is no longer needed.

Topology



(a) Point-to-point



(b) Star

Fig. Q.13.1 Fast ethernet topology

- Fast ethernet is designed to connect two or more stations together. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center. It is shown in the Fig. Q.13.1.

Summary sheet of fast ethernet

Parameters	100BASE-TX		100BASE-FX	100BASE-T4
Transmission medium	STP	Cat 5 UTP	Fiber	Cat 3, 4, 5 UTP
Number of wires	4	4	2	4
Data rate	100 Mbps	100 Mbps	100 Mbps	100 Mbps
Maximum segment length	100 m	100 m	100 m	100 m
Network span	200 m	200 m	400 m	200 m
Line coding	MLT-3	MLT-3	4B5B	8B/6T/NRZ

3.9 : Gigabit Ethernet

Q.14 Explain Gigabit ethernet.

Ans. : • Goals of gigabit ethernet

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with standard or fast ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.

- It support the two different modes of operations.

i) Full duplex ii) Half duplex.

- In full duplex mode, there is a central switch connected to all computers or other switches. Each switch has buffers for each input port

in which data are stored until they are transmitted. There is no collisions in this mode. This means that CSMA/CD is not used.

- Gigabit ethernet can also be used in half duplex mode. In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. The half duplex approach uses CSMA/CD. For shared medium hub operation, there are two enhancements to the basic CSMA/CD scheme.

1. **Carrier extension :** It defines the minimum length of a frame as 512 bytes.
2. **Frame bursting :** It allows for multiple short frames to be transmitted consecutively, up to a limit, without relinquishing control for CSMA/CD between frames.

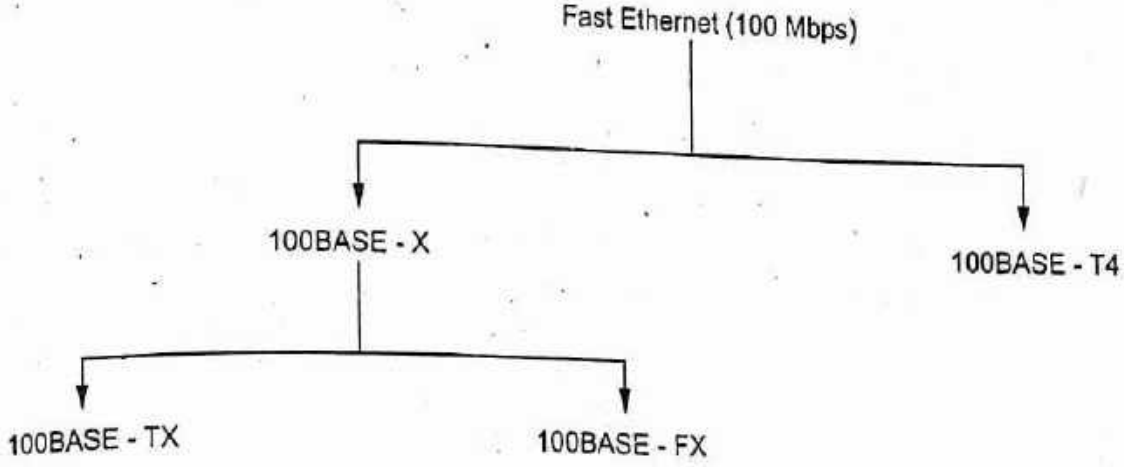


Fig. Q.14.1

Transmission Media

Summary sheet of gigabit ethernet

Parameters	1000Base-SX	100Base-LX	100Base-CX	1000Base-T
Transmission medium	Fiber short wave	Fiber long wave	STP	Cat 5 UTP
Number of wires	2	2	2	4

Maximum segment length	550 m	500 m	25 m	100 m
Line coding	NRZ	NRZ	NRZ	4D-PAM5

Topology

- Gigabit ethernet is designed to connect two or more stations. If there are only two stations, thsey can be connected point-to-point. Fig. Q.14.2 shows the point-to-point connection.

Fig. Q.14.2 Point-to-point

- Three or more stations need to be connected in a star topology with a hub or a switch at the center. This is shown in Fig. Q.14.3.

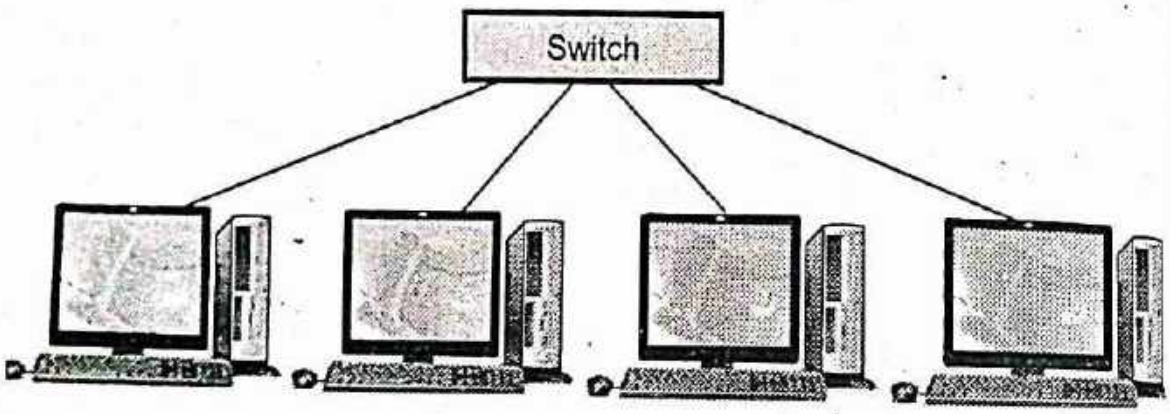


Fig. Q.14.3 Star

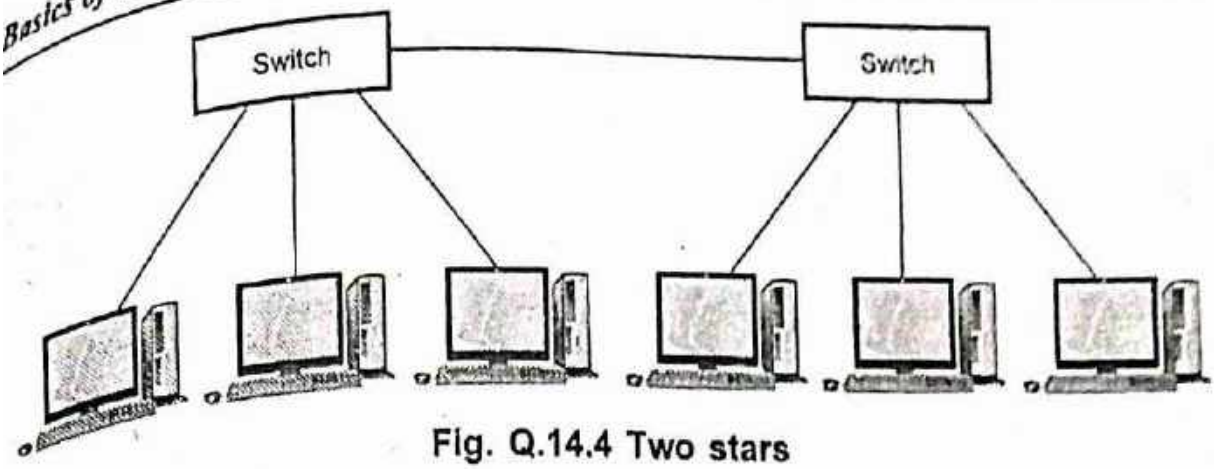


Fig. Q.14.4 Two stars

Q.15 Write a note on :

i) Standard ethernet [Refer Q.7]

ii) Fast etherenet [Refer Q.13]

iii) Gigabit ethernet [Refer Q.14]

☞ **[SPPU : June-22, Marks 9]**

END...

Unit IV

4 Network Layer : Services and Addressing

4.1 : Network Layer Services

Q.1 Explain network layer services with example.

☞ [SPPU : May-19, Marks 4]

Ans. : • Main Task of the network layer is to move packets from the source host to the destination host.

- It transport packet from sending to receiving hosts via internet. Network layer protocols exist in every host and route. In order to provide this service, the transport layer relies on the services of the network layer, which provides a communication service between hosts. In particular, the network layer moves transport-layer segments from one host to another.
- At the sending host, the transport-layer segment is passed to the network layer. It is then the job of the network layer to get the segment to the destination host and pass the segment up the protocol stack to the transport layer.
- Three important functions of network layer :
  1. **Path determination :** Route taken by packets from source to destination. Routing algorithms is used for this.
  2. **Switching :** Move packets from router's input to appropriate router output.
  3. **Call setup :** Some network architectures require router call setup along path before data flows.
- The basic function of network layer is to provide an end-to-end communications capability to the transport layer which lies above it.

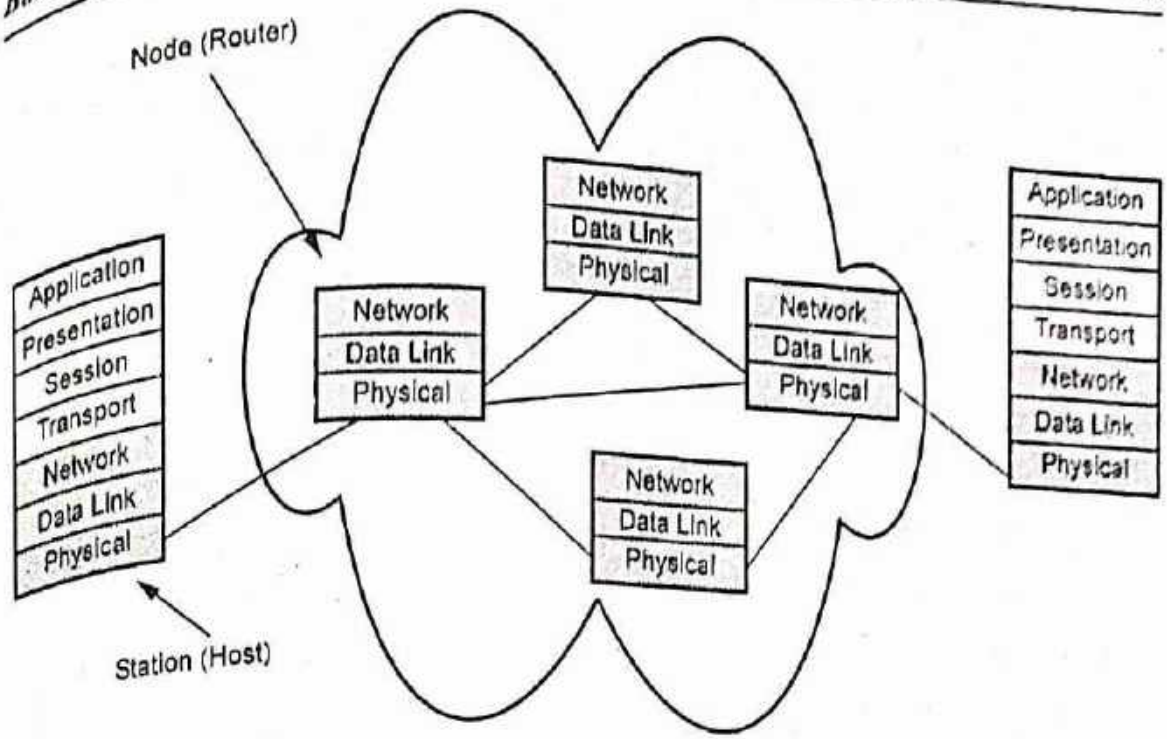


Fig. Q.1.1

Network layer is the lowest layer that deals with end-to-end transmission.

- To achieve the goal, the network layer must know about the topology of the communication subnet i.e. set of all routers and choose appropriate path through it. Network layer also takes care of loading of the chosen root.
- The network layer protocols are concerned with the exchange of packets of information between transport layer entities. A packet is a group of bits that includes data bits plus source and destination addresses. The service provided by the network layer to the transport layer is called network service.
- The functions carried out by a layer are different from its services. Functions are those activities which are carried out by a layer in order to provide the services. The network layer functions are carried out by adding a header to every Network Service Data Unit (NSDU) forming Network Protocol Data Unit (NPDU).

- The header contains all the information necessary for carrying out functions.
  1) It keeps track which MAC (Media Access Control), the unique number that each network card has address to send i.e. decides which system receives the information.
  2) It makes routing of data through network from source to destination.
  3) Virtual circuits are established in this layer.
  4) It translates logical network address into physical machine address.
  5) It breaks large packets into smaller so that it will be accepted by the frame of data link layer.
  6) Flow control of packetized information and congestion avoidance is concern of protocol.
  7) It determines the Quality Of Service (QOS) parameter.

4.2 : IPv4 Addresses

Q.2 What is classless addressing ? Explain.

☞ [SPPU : Dec.-15 (End Sem.) Marks 4]

Ans. : The IP address structure is divided into five address classes : Class A, Class B, Class C, Class D and Class E, identified by the most significant bits of the addresses.

- Fig. Q.2.1 shows the five classes of IP addresses.
- Class D addresses are used for multicast services that allow a host to send information to a group of hosts simultaneously. Class E addresses are reserved for future use.
- Class A addresses were designed for large organizations with a large number of attached hosts or routers.
- Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers.
- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size.

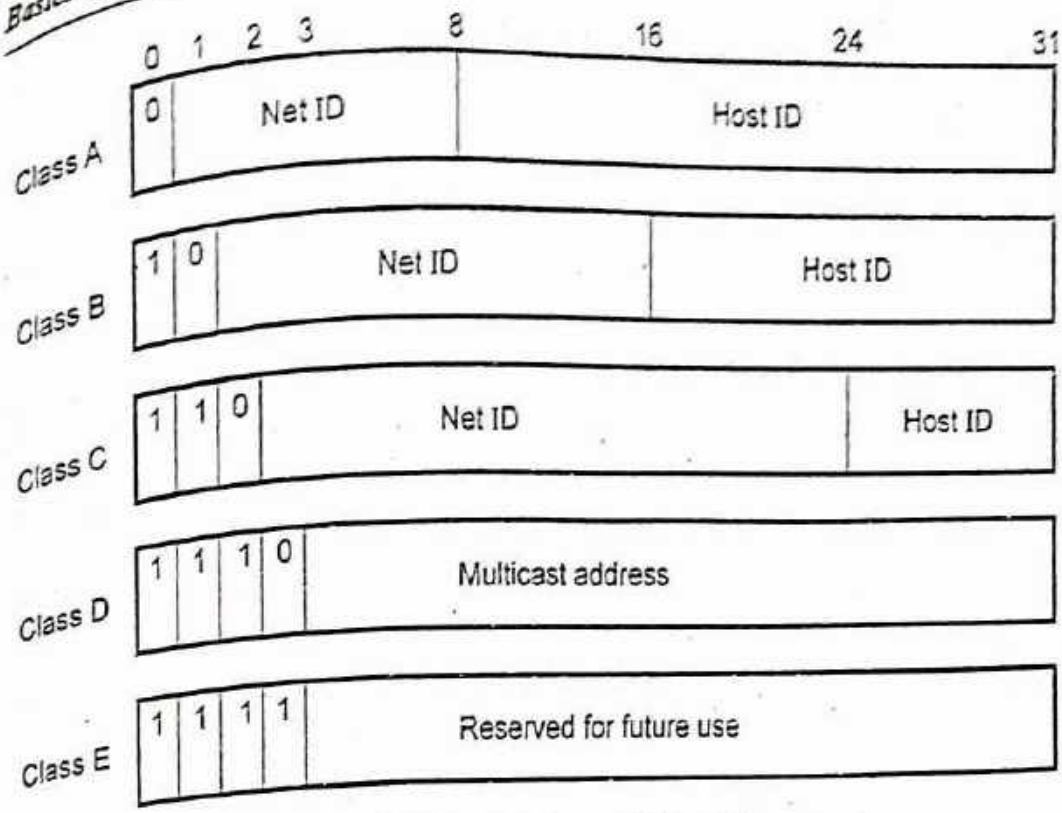


Fig. Q.2.1 Five classes of IP addresses

Class	Number of blocks	Block size
A	128	16777216
B	16384	65536
C	2097152	256
D	1	268435456
E	1	268435456

- In a class A network, the first byte is assigned to the network address and the remaining three bytes used for the node addresses. The class A format is

  Network.Node.Node.Node

  For example : 14.28.101.120 in this IP address 14 is the network address and 28.101.120 is the node address.

- In class B network, the first two bytes are assigned to the network address and the remaining two bytes are used for node addresses. The format is

  Network.Network.Node.Node

  For example : 150.51.30.40 in this IP address network address is 150.51 and node address is 30.40.

- In class C network, the first three bytes are assigned to network address and only one byte is used for node address. The format is

  Network.Network.Network.Node

  For example : 200.20.42.120 in this example 200.20.42 is the network address and 120 is the node address.

Q.3 Draw and explain IPv4 header format. List out special IP addresses and private IP addresses. ☞ [SPPU : June-22, Marks 8]

Or Draw and explain IPv4 header format.

☞ [SPPU : May-16, End Sem, Marks 6]

Ans. : • Packets in the IPv4 layer are called datagrams. A datagram is a variable length packet consisting of two parts : Header and data.

• Fig. Q.3.1 shows IPv4 header format

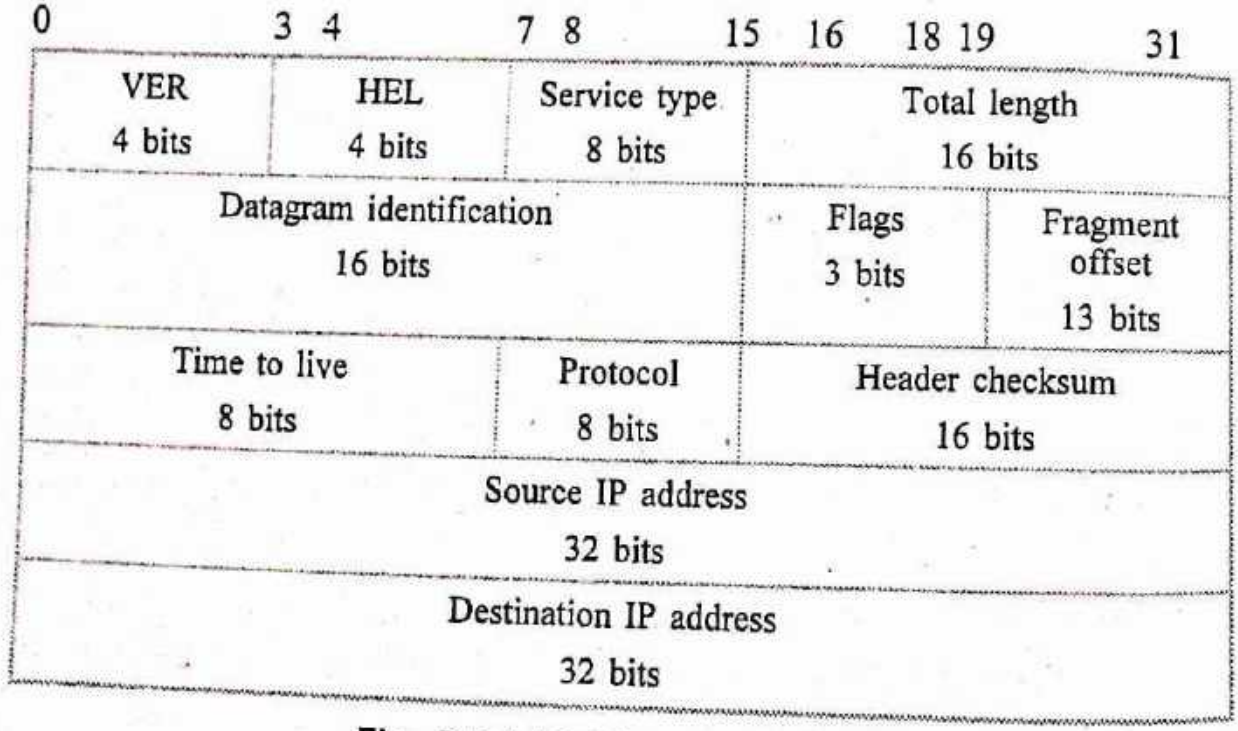


Fig. Q.3.1 IPv4 header format

1. **VER** is the field that contains the IP protocol version. The current version is 4.5 is an experimental version. 6 is the version for IPv6.
2. **HLEN** is the length of the IP header in multiples of 32 bits without the data field.The minimum value for a correct header is 5 (i.e. 20 bytes), the maximum value is 15 (i.e., 60 bytes).
3. **Service type** The service type is an indication of the quality of service requested for this IP datagram. It contains the following information.

Precedence	Types of service	R

Precedence specifies the nature / priority :

000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash override
101	Critical
110	Internetwork control
111	Internetwork control

TOS specifies the type of service value :

TOS bits	Description
1000	Minimize delay
0100	Maximum throughout
0010	Maximize reliability

0001	Minimize monetary cose
0000	Normal service

The last bit is reserved for future use.

4. **Total length** specifies the total length of the datagram, header and data, in octets.
5. **Identification** is a unique number assigned by the sender used with fragmentation.
6. **Flags** contain control flags :
   a. The first bit is reserved and must be zero;
   b. The 2nd bit is DF (Do not Fragment), 0 means allow fragmentation;
   c. The third is MF (More Fragments), 0 means that this is the last fragment.
7. **Fragment offset** is used to reassemble the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted) contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.
8. **TTL** (Time To Live) specifies the time (in seconds) the datagram is allowed to travel. In practice, this is used as a hop counter to detect routing loops.
9. **Protocol number** indicates the higher level protocol to which IP should deliver the data in this datagram. E.g., ICMP = 1; TCP = 6; UDP = 17.
10. **Header checksum** is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.
11. **Source/Destination IP addresses** are the 32-bit source/destination IP addresses.
12. **IP options** is a variable-length field (there may be zero or more options) used for control or debugging and measurement. For instance :
    a. The **loose source routing** option provide a means for the source of an IP datagram to supply explicit routing information;
    b. The **timestamp** option tell the routers along the route to put timestamps in the option data.

13. Padding is used to ensure that the IP header ends on a 32 bit boundary. The padding is zero.

Q.4 For a given class C network 195.168.65.0, Design the equal subnets in such a way that each subnet has at least 50 nodes.

☞ [SPPU : May-13, Marks 6]

Ans. : For class-C IP address, 2-bit is used for subnet. Each subnet has atleast 60 nodes, so calculate subnet mask.

$2^2 - 2 = 2$ subnet

∴ Subnet mask is 255.255.255.11000000

255.255.255.192 subnet mask

Calculate the subnet

255.255.255.01000000

255.255.255.64 First subnet

255.255.255.10000000

255.255.255.128 Second subnet

1st subnet = 255.255.255.64

2nd subnet = 255.255.255.128

Q.5 What is NAT ? Explain operation of NAT with suitable example.

☞ [SPPU : Oct-16 (In Sem.), Marks 5]

Or Explain the operation of NAT with suitable example.

☞ [SPPU : May-13, Dec-13, Marks 4]

Ans. : • Within the company, every machine has a unique address of the form 10.X.Y.Z. When a packet leaves the company premises, it passes through the NAT box that convert the internal IP source address 10.0.0.1.

- NAT box is often combined in a single device with a firewall. It is also possible to integrate the NAT box into the company router.
- Whenever an outgoing packet enters the NAT box, the 10.X.Y.Z. SA is replaced by the company true IP address. In, addition, TCP source port field is replaced by an index into the NAT box 65536 entry translation table. This table entry contains the original IP address and original

source port. Finally both the IP and TCP header checksums are recomputed and inserted into the packet.

- Fig. Q.5.1 shows the placement of NAT box.

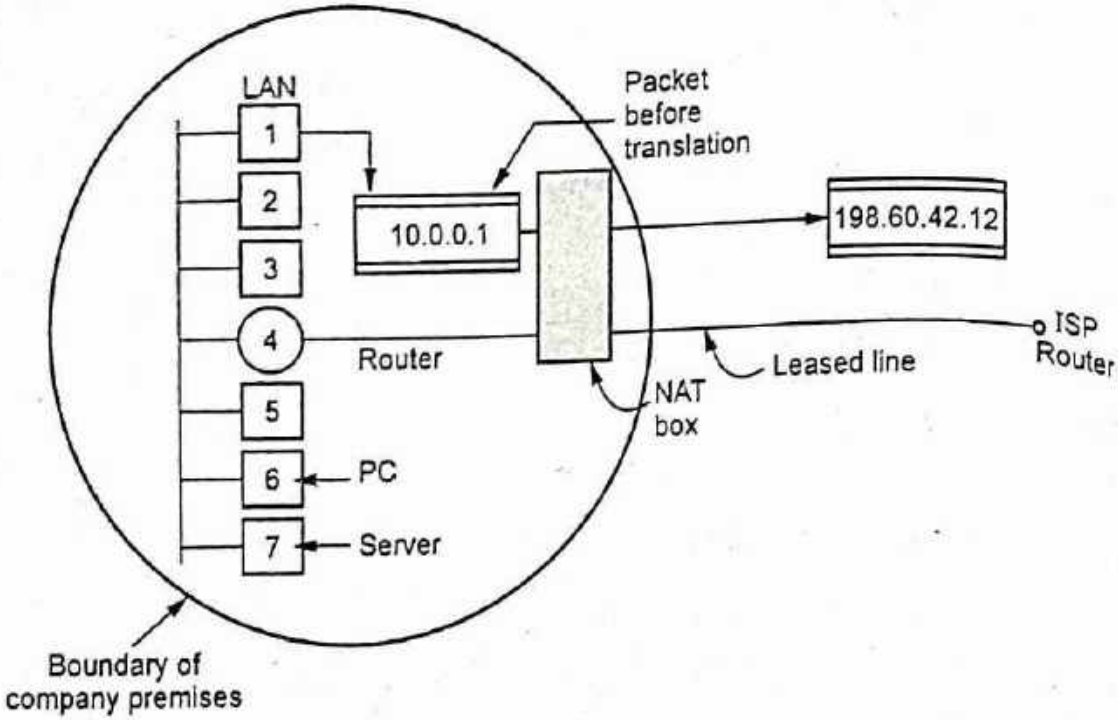


Fig. Q.5.1 NAT

- When process want to establish a TCP connection with a remote process, it attached itself to an unused TCP port on its own machine. This is called a source port and tells the TCP code where to send incoming packets belonging to this connection.
- The process also supplies a destination port to tell who to give the packet to on the remote side.

Q.6 Explain subnetting a network.

Ans. : • If a organization is large or if its computers are geographically dispersed, it makes good sense to divide network into smaller ones, connected together by routers. The benefits for doing things this way include.

1. Reduced network traffic
2. Optimized network performance
3. Simplified network management
4. Facilities spanning large geographical distances.

- If Network Information Center (NIC) assign only one network address to an organization which having multiple network, that organization has a problem. A single network address can be used to refer to multiple physical networks.
- An organization can request individual network address for each one of its physical networks. If these were granted, there wouldn't be enough to go around for everyone.
- Another problem is, if each router on the internet needed to know about each existing physical network, routing tables would be impossibly huge. This is physical overhead on the router. To solve this type of problem, the subnet addressing method is used.
- To allow a single network address to span multiple physical networks is called **subnet addressing** or **subnet routing** or **subnetting**. Subnetting is a required part of IP addressing.
- To understand subnet addressing, consider the next example. Consider the site has a single class B IP network address assigned to it, but the organization has two or more physical networks.

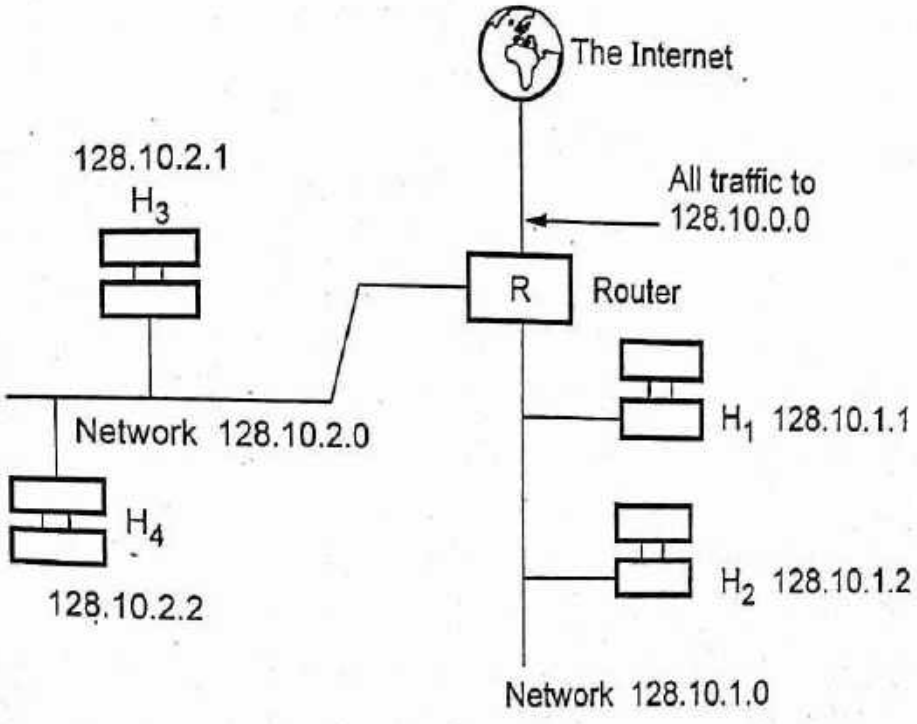


Fig. Q.6.1 Multiple network

- Only local routers know that there are multiple physical networks and how to route traffic among them.
- In the example, the organization is using the single class B network address for two networks. For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the subnet address. This is accomplished by assigning each machine a subnet mask.
- The network administrator creates a 32-bit subnet mask comprised of ones and zeros. The ones in the subnet mask represent the positions that refer to the network or subnet addresses.
- The zeros represent the positions that refer to the host part of the address. Class B address format is Net.Net.Node.Node. The third byte, normally assigned as part of the host address is now used to represent the subnet address. Hence, these bit positions are represented with ones in the subnet mask.
- The fourth byte is the only part in example that represents the unique host address.

Subnet mask code

1 = Positions representing network or subnet addresses.

0 = Positions representing the host address.

Subnet mask format

1111 1111 1111 1111 1111 1111 0000 0000

Network address positions *Subnet positions* *Host positions*

- The subnet mask can also be denoted using the decimal equivalents of the binary patterns. The default subnet masks for the different classes of networks are as below in Table Q.6.1.

Class	Format	Defult subnet mask
A	Net.Node.Node.Node	255.0.0.0
B	Net.Net.Node.Node	255.255.0.0
C	Net.Net.Net.Node	255.255.255.0

Table Q.6.1 Default subnet mask of IP address

Masking

- A process that extracts the address of the physical network from an IP address is called Masking. If we done the subnetting, then masking extracts the subnetwork address from an IP address.
- To find the subnetwork address, two method are used. There are boundary level masking and non-boundary level masking, we take one by one.
- In boundary level masking, two masking numbers are consider (i.e. 0 or 255). In non-boundary level masking other value of masking is used Apart from 0 and 255.

A. Rules for boundary level masking

1. In this mask number is either 0 or 255.
2. If the mask number is 255 in the mask IP address, then the IP address is repeated in subnetwork address.
3. If the mask number is 0 (zero) in the mask IP address, then the 0 is repeated in subnetwork address.

B. Rules for non-boundary level masking

1. In this mask numbers are not 0 or 255 mask number is greater than 0 or less than 255.
2. If the mask number is 255 in the mask IP address, then the original IP address (byte) is repeated in subnetwork address.
3. If the mask number is 0 in the mask IP address, then the 0 is repeated in the subnetwork address.

4. For any other mask numbers, bit-wise AND operator is used. Bit-wise ANDing is done in between mask number (byte) and IP address (byte).

- The first address in the block is used to identify the organization to rest of the Internet. This address is called the **network address.**

1. How many subnets ?

- Number of subnet is calculated as follows :

Number of subnet = 2^x

where x is the number of masked bits or the 1s (ones).

- For example 11100000, the number of 1s gives us 2^3 subnets. In this example there are 8 subnets.

2. How many host per subnet ?

Number of host per subnet = 2^y - 2

Where y is the number of unmasked bits or the 0s (zeros).

- For example 11100000, the number of 0s gives us $2^5 - 2$ hosts. In this example there are 30 hosts per subnet. You need to subtract 2 for subnet address and the broadcast address.

3. What are the valid subnets ?

For valid subnet = 256 – Subnet mask = Block size. An example would be 256 – 224 = 32. The block size of a 224 mask is always 32.

Start counting at zero in block of 32 until you reach the subnet mask value and these are your subnets. 0, 32, 64, 96, 128, 160, 192, 224.

4. What is the broadcast address for each subnet ?

- Our subnets are 0, 32, 64, 96, 128, 160, 192, 224, the broadcast address is always the number right before the next subnet. For example, the subnet 0 has a broadcast address of 31 because next subnet is 32. the subnet 32 has a broadcast address of 63 because next subnet is 64.

5. What are the valid hosts ?

- Valid hosts are the numbers between the subnets, omitting the all 0s and all 1s. For example, if 32 is the subnet number and 63 is the

broadcast address, then 32 to 63 is the valid host range. It is always between the subnet address and the broadcast address.

Q.7 What is subnetting ? A company is granted a site address 172.16.10.33/19 design the subnets and answer following questions :
i) How many subnets does the chosen subnet mask produce ?
ii) How many valid hosts per subnet are available ?
iii) What are the valid subnets ?
iv) What's the broadcast address of each subnet ?
v) What are the valid hosts in each subnet ?

☞ [SPPU : June-22, Marks 8]

Ans. : Subnetting : Refer Q.6.

Subnet mask : 255.255.224.0

Network Address : 172.16.0.0

Broadcast address : 172.16.31.255

Host IP range : 172.16.0.1 to 172.16.31.254

Valid number of hosts : 8192

Number of usable host : 8190

Q.8 Explain supernetting.

Ans. :

- Although class A and B addresses are almost depleted, class C addresses are still available. In super netting, an organization can combine several class C blocks to create a larger range of addresses.
- Several networks are combined to create a super network. For example : Organization needs 1000 address can be granted 4 contiguous class C blocks to create one super network.
- Supernet is a block of contiguous sub-networks addressed as a single subnet in the larger network. Supernets always have a subnet mask that is smaller than the masks of the component networks.
- The size of routing tables has been rapidly increasing during the expansion of the Internet. Supernetting is the process of aggregating routes to multiple smaller networks, thus saving storage space in the

routing table and simplifying routing decisions. Routing advertisements to neighboring gateways are reduced.

- An organization has been allocating a block of class C address in 2^n with contiguous address space. It archive by using bits which belongs to the network address as hosts bits.
- An organization with 4 class C

  193.0.32.0 , 193.0.33.0 , 193.0.34.0 , 193.0.35.0

11111111 11111111 11111100 00000000 mask 255.255.252.0

11000001 00000000 00100000 00000000 net 193.0.32.0

11000001 00000000 00100001 00000000 net 193.0.33.0

11000001 00000000 00100010 00000000 net 193.0.34.0

11000001 00000000 00100011 00000000 net 193.0.35.0

11000001 00000000 00100000 00000000

- Bit wise AND results 193.0.32.0 : 11000001 00000000 00100000 00000000
- This organization's network has changed from 4 net to a single net with 1,022 hosts.
- Supernetting requires the use of routing protocols that support Classless Inter-Domain Routing (CIDR). Interior Gateway Routing Protocol, Exterior Gateway Protocol and version 1 of the Routing Information Protocol (RIPv1) are based on classful addressing, and therefore cannot transmit subnet mask information.

Q.9 List the network layer services and define subnetting, supernetting, classful addressing, classless addressing.

☞ **[SPPU : June-22, Marks 9]**

Ans. : Refer Q.1,2,6 and 8.

4.3 : Delivery and Forwarding of IP Packet

Q.10 Explain delivery and forwarding IP packets.

Ans. : • Forwarding refers to the way a packet is delivered to the next node. It requires a host or router to have a routing table.

- Forwarding refers to the router local action of transferring a datagram from an input link interface to the appropriate output link interface.
- When host has a packet to send, it looks at routing table to find the route to the final destination.

Types of forwarding techniques

1. Next hop versus route method.
2. Network specific versus host specific method.
3. Default method.

1) Next hop versus route method

- Fig. Q.10.1 shows network with routing table for this method. This method reduce the content of rounting table. Routing table stores only the address of the next hop.

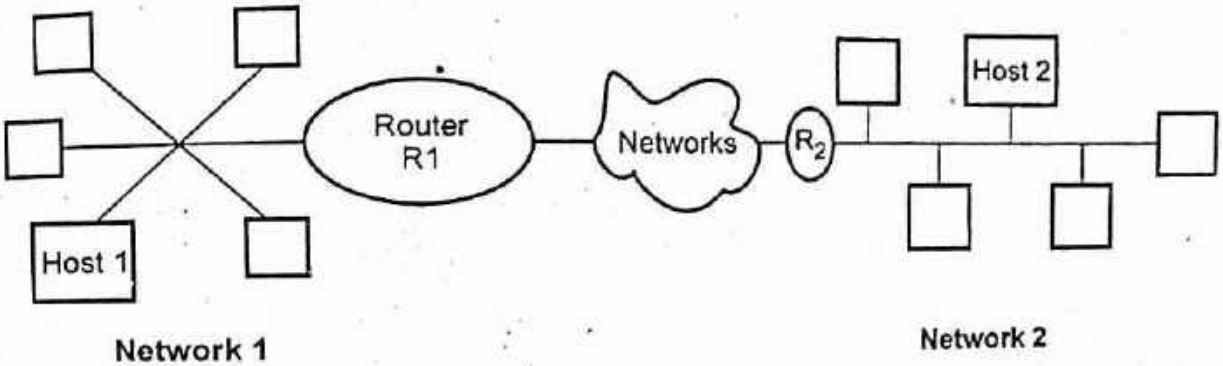


Fig. Q.10.1

Routing table for next hop

hkhdskjandm,

For host 1

Destination address	Next hop
Host 2	R1

For router R2

Destination Address	Next hop
Host 2	R2

For Router R2

Destination Address	Next hop
Host 2	-

2) Network specific versus host specific method

- It simplify the searching process and also reduce the routing table size.
- Routing table contains only the address of the destination network.
- It provides good security.

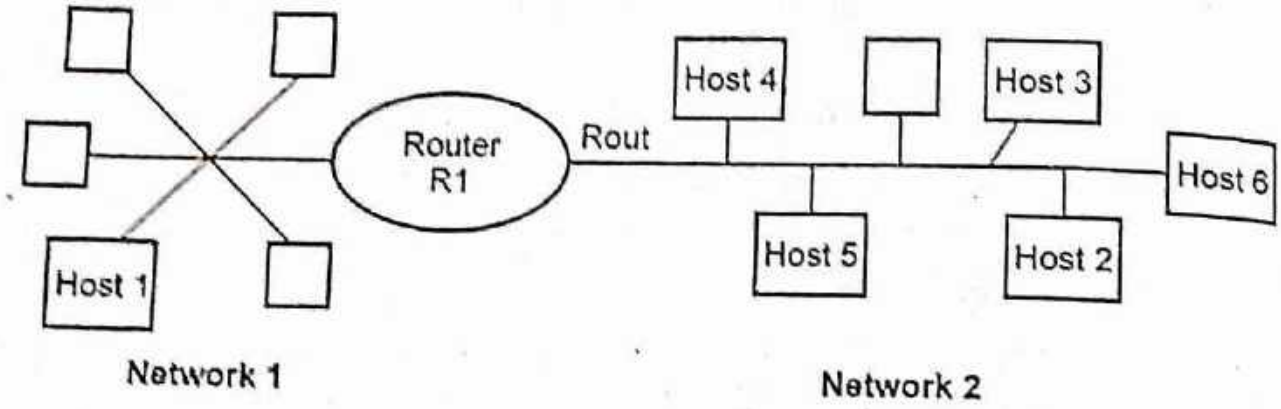


Fig. Q.10.2

Routing table for host 1

Destination address	Next hop
Network 2	R1

3) Default method

- Host is connected with more than one routers.
- A router is assigned to receive all packets with no match in the routing table.
- Default router is used for communication with outside world.

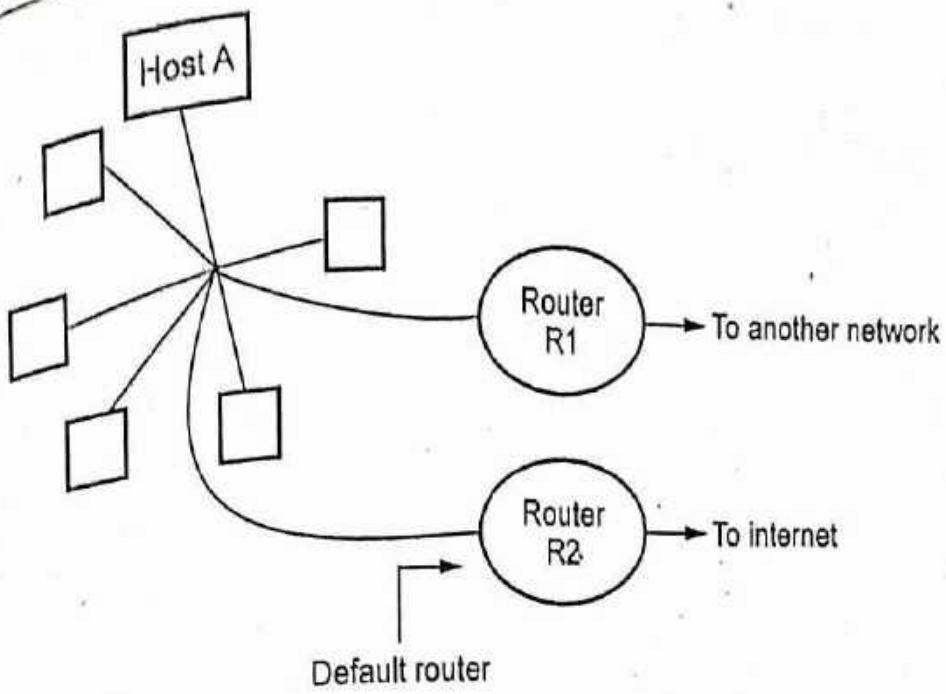


Fig. Q.10.3

4.4 : IPv6

Q.11 What is the need of IPv6 ? Explain types of IPv6 address.

☞ [SPPU : June-22, Marks 9]

Ans. : IPv6 allows three types of addresses.

1) Unicast 2) Anycast 3) Multicast

1) Unicast

An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

2) Anycast

An identifier for a set of interfaces. A packet sent to an anycast address is delivered to one of the interfaces identified by the address.

3) Multicast

An identifier for a set of interfaces. A packet sent to a multicast address is delivered to all interfaces identified by that address.

- Following Table Q.11.1 shows the current allocation of addresses based on the format prefix.
- The first field of any IPv6 address is the variable-length format prefix, which identifies various categories of addresses.

Allocation space	Prefix (binary)	Fraction of address space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP allocation	0000 001	1/128
Reserved for IPX allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Unassigned	001	1/8
Provider-Based Unicast Address	010	1/8
Unassigned	011	1/8
Reserved for Geographic-Based Unicast Addresses	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16

Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link Local Use Addresses	1111 1110 10	1/1024
Site Local Use addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

Table Q.11.1 Address allocation

Q.12 Draw neatly IPv6 header format.

☞ [SPPU : Aug.-15, In Sem., Marks 6]

Ans. : • The IPv6 packet is shown in Fig. Q.12.1. Each packet is composed of a mandatory base header followed by the payload. The payload consists of two parts : Optional and data

• Fig. Q.12.2 shows the IPv6 datagram header format.

1. **Versions :** This 4 bits field defines the version number of the IP. The value is 6 for IPv6.
2. **Priority :** The 4 bits priority field defines the priority of the packet with respect to traffic congestion.
3. **Flow label :** It is 24 bits field that is designed to provide special handling for a particular flow of data.
4. **Payload length :** The 16 bits payload length field defines the length of the IP datagram excluding the base header.
5. **Next header :** It is an 8 bits field defining the header that follows the base header in the datagram.
6. **Hop limit :** This 8 bits hop limit field serves the same purpose as the TTL field in IPv4.
7. **Source address :** The source address field is a 128 bits internet address that identifies the original.

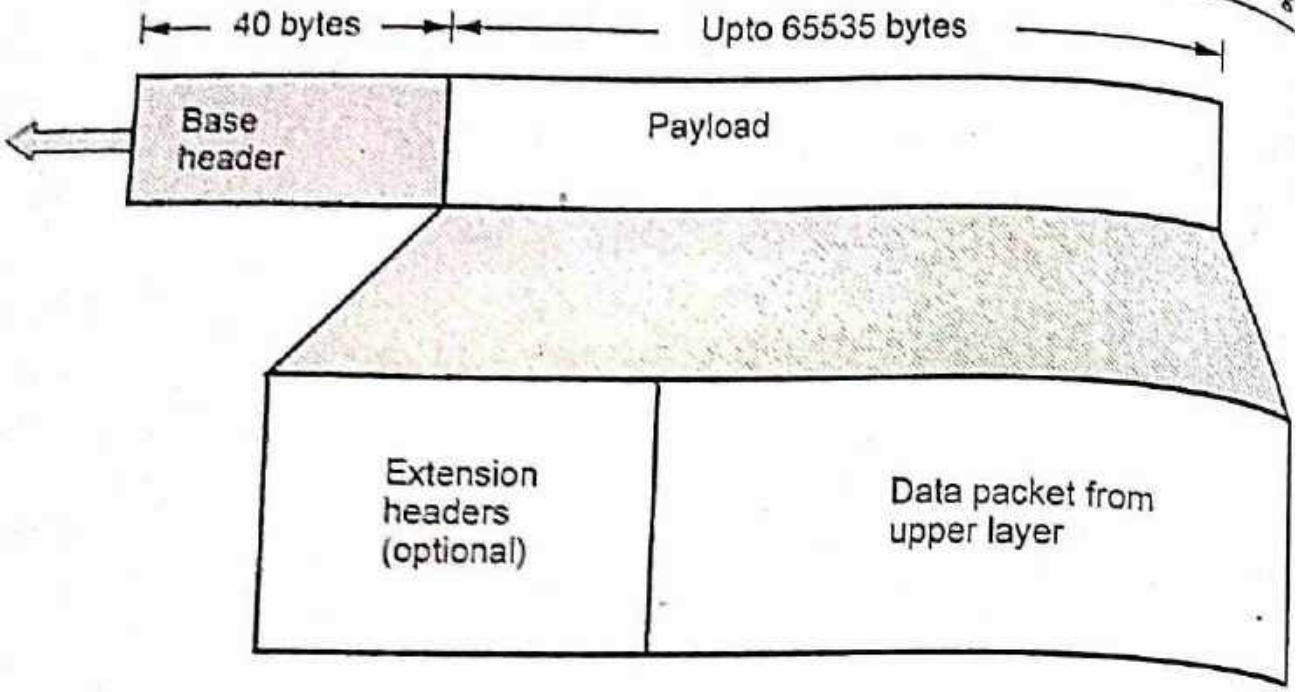
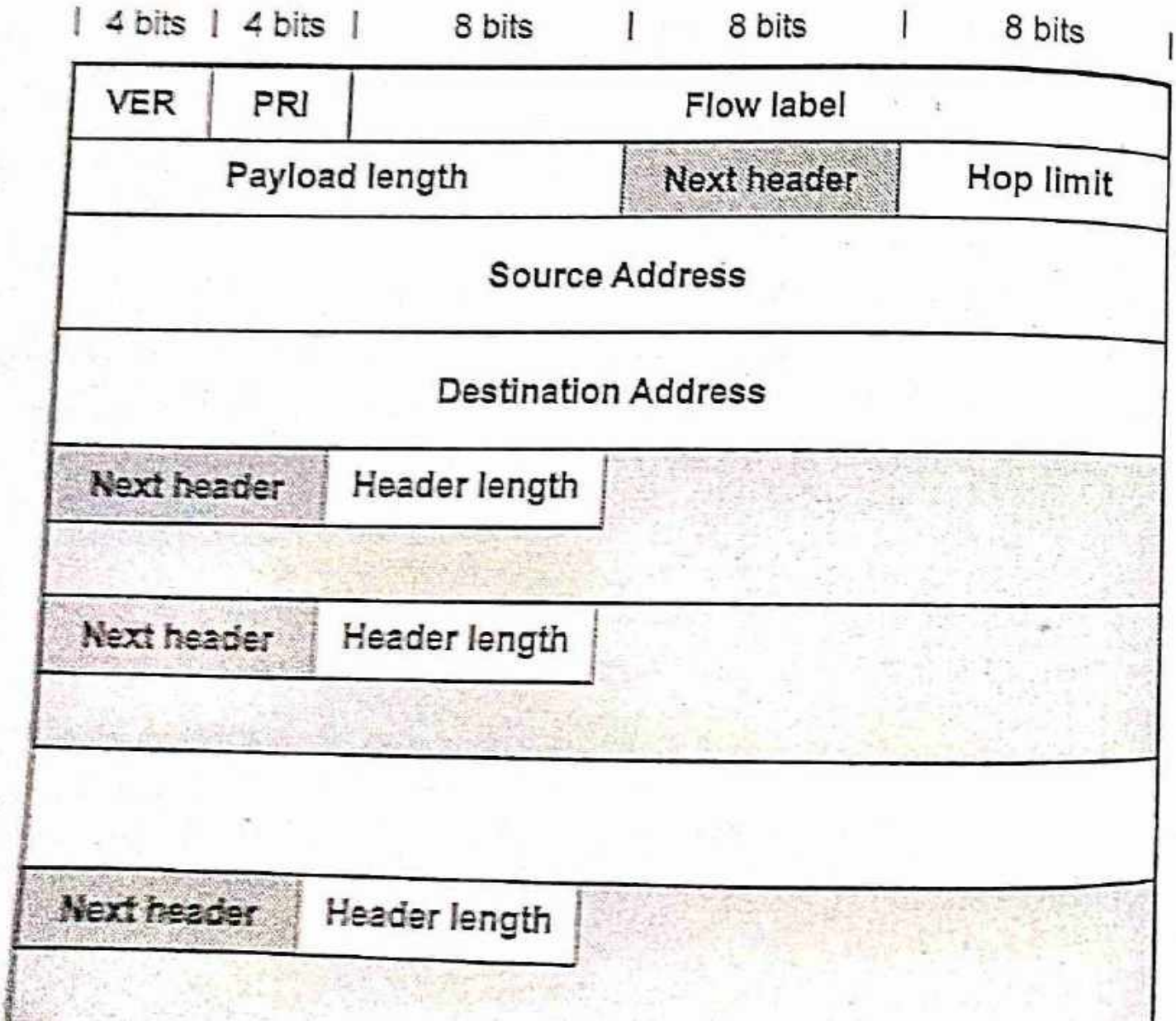


Fig. Q.12.1 IPv6 datagram header of payload



8. **Destination address** : It is 128 bits Internet address that usually identifies the final destination of the datagram.

- Next header codes for IPv6

Code	Next header
0	Hop by hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null
60	Destination option

Priority

- The priority field defines the priority of each packet with respect to other packets from the same source. IPv6 divides traffic into two broad categories
  1. Congestion controlled
  2. Noncongestion controlled
- If a source adapts itself to traffic slowdown when there is congestion, the traffic is referred to as congestion controlled traffic. Congestion controlled data are assigned priorities from 0 to 7.

Priority	Meaning
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

- A priority of 0 is the lowest; a priority of 7 is the highest.
- Noncongestion controlled traffic refers to a type of traffic that excepts minimum delay. Discarding of packets is not desirable. Retransmission in most cases is impossible. Real time audio and video are examples of this type of traffic.
- Priority numbers from 8 to 15 are assigned to noncongestion controlled traffic.

4.5 : Transition from IPv4 to IPv6

Q.13 Explain Dual stack and tuneling.

Ans. : • All the host must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.

- Fig. Q.13.1 shows the dual stack.
- To determine which version to use when sending a packet to destination, the source host queries the DNS. If the DNS returns an

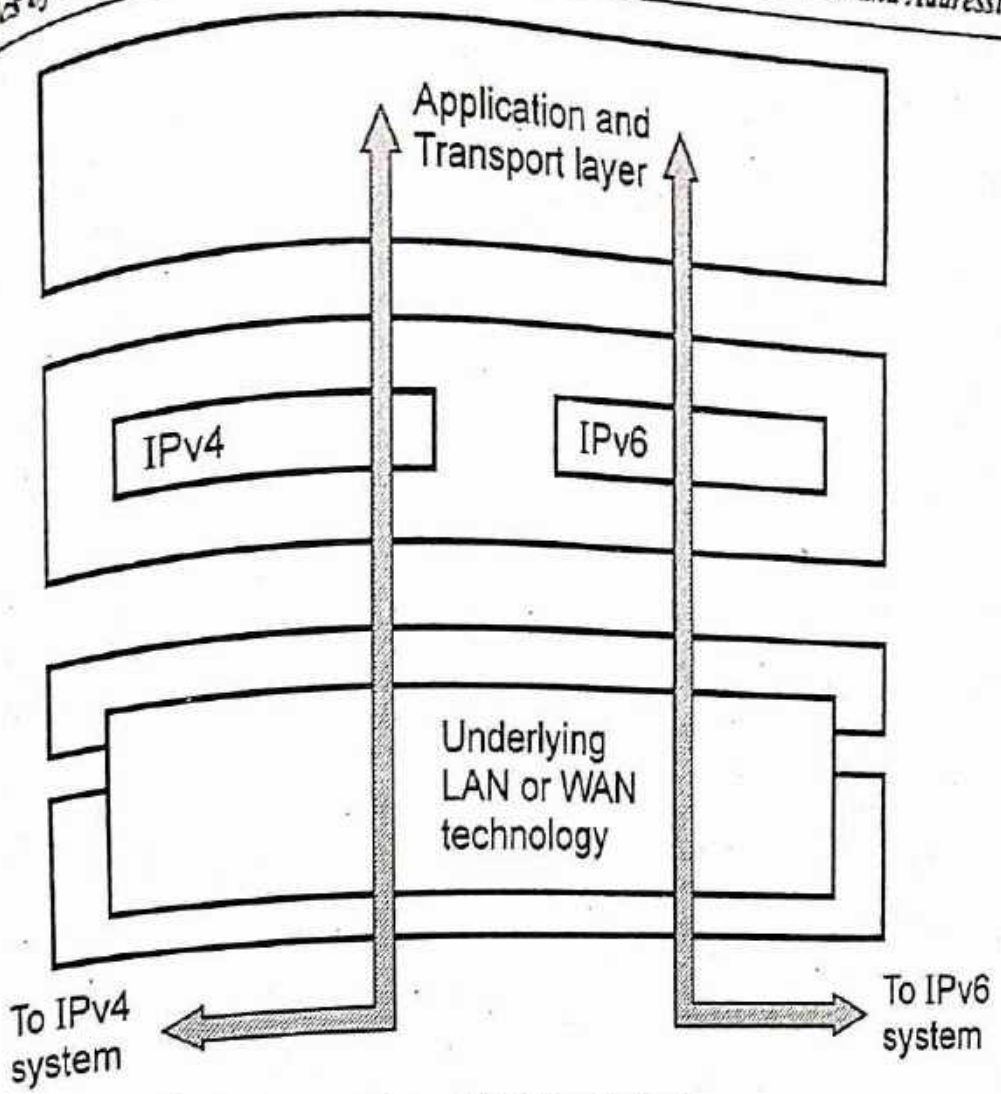


Fig. Q.13.1 Dual stack

IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

Tunneling

- When two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. The IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.
- Fig. Q.13.2 shows the tunneling.

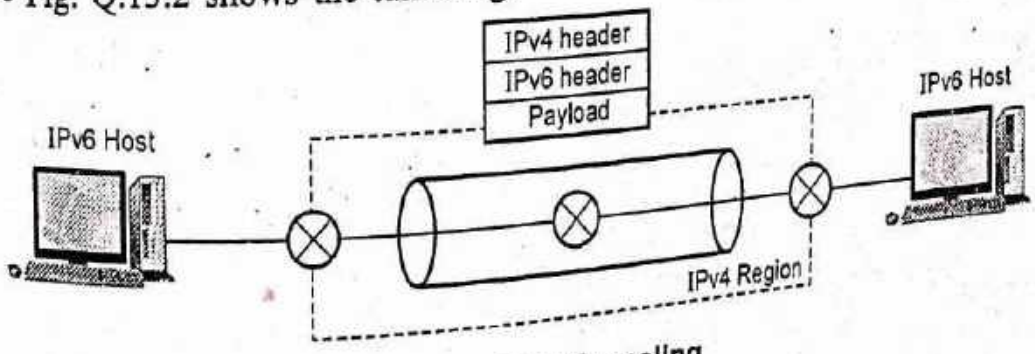


Fig. Q.13.2 Tunneling

Header Translation

- Header translation is used when some of the system uses IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6.
- Fig. Q.13.3 shows the header translation.

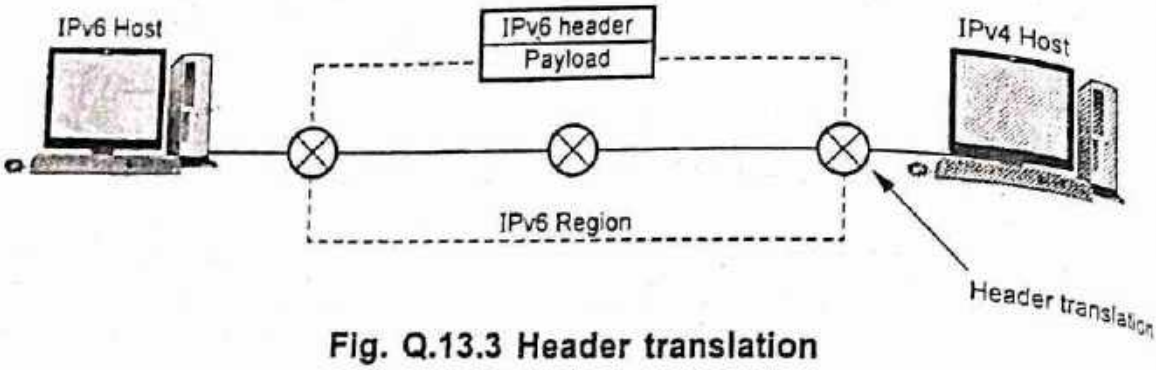


Fig. Q.13.3 Header translation

- The header format must be totally changed through header translation. The header of the IPv6 parket is converted to IPv4 header.

Q.14 1.Differentiate between IPv4 and IPv6.

☞ [SPPU : Dec.-15, End Sem, Marks 4]

Or Compare between IPv4 and IPv6.

☞ [SPPU : April-18, In Sem, Marks 6]

Ans. :

Sr. No.	IPv4	IPv6
1.	Header size is 32 bits.	Header size is 128 bits.
2.	It cannot support autoconfiguration	Supprots autoconfiguration
3.	Cannot support real time application.	Supports real time application.
4.	No security at network layer.	Provides security at network layer.
5.	Throughput and delay is more.	Throughput and delay is less.

END...

Unit V

5 Network Layer : Routing Protocols

5.1 : Routing

Q.1 Explain routing. State properties of routing algorithm. Classify routing algorithm.

Or Explain following routing
i) Static routing ii) Dynamic routing iii) Default routing.

☞ [SPPU : Jun-22, Marks 9]

Ans. : • A host or a router has a routing table with an entry for each destination, or a combination of destinations, to route IP packets. Routing table can be either static or dynamic.

- A static routing table contains information entered manually. The administrator enters the route for each destination into the table.
- Dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPE or BGP.
- The main function of the network layer is to route packets from source to destination. To accomplish this a route through the network must be selected, generally more than one route is possible.
- The selection of route is generally based on some performance criteria. The simplest criteria is to choose shortest root through the network.
- The shortest root means a route that passes through the least number of nodes. This shortest root selection results in least number of hops per packet. A routing algorithm is designed to perform this task. The routing algorithm is a part of network layer software.

Properties of routing algorithm

- Certain properties which are desirable in a routing algorithm are - Correctness, simplicity, robustness, stability, fairness, optimality and efficiency.

1. **Correctness** and simplicity are self-explanatory.
2. **Robustness** means the ability to cope with changes in the topology and traffic without requiring all jobs in hosts to be aborted and network to be rebooted everytime.
3. **Stability** refers to equilibrium state of algorithm. It is the technique that react to changing conditions such as congestions. Under any conditions the network must not react too slow or experience unstable swings from one extreme to another.
4. Some performance criteria may favour the exchange of data packets between nearby stations and discourage the exchange between distant stations. Some compromise is needed between fairness and optimality.

Routing algorithm classification

- Routing algorithm can be classified in several ways. Based on their responsiveness it can be classified into two types -

1. Static (non-adaptive) Routing Algorithms.
2. Dynamic (adaptive) Routing Algorithms.

1. Static (non-adaptive) routing algorithms

- In static routing the network topology determines the initial paths. The precalculated paths are then loaded to the routing table and are fixed for a longer period.
- Static routing is suitable for small networks. Static routing becomes **cumber some** for bigger networks.
- The disadvantage of static routing is its inability to respond quickly to network failure.

2. Dynamic (Adaptive) routing algorithms

- Dynamic routing algorithms change their routing decision if there is change in topology, traffic. Each router continuously checks the network status by communicating with neighbours.

- Thus a change in network topology is eventually propagated to all the routers. Based on this information gathered, each router computes the suitable path to the destination.
- The disadvantage of dynamic routing is its complexity in the router.

Routing tables

- Once the routing decision is made, this information is to be stored in routing table so that the router knows how to forward a packet.
- In virtual circuit packet switching, the routing table contains each incoming packet number and outgoing packet number and output port to which the packet is to forward.
- In datagram networks, routing table contains the next hop to which to forward the packet, based on the destination address.

Q.2 Differentiate between static & dynamic routing.

Ans. :

Sr. No.	Static routing (Non adaptive)	Dynamic routing (Adaptive)
1.	Static routing manually sets up the optimal paths between the source and the destination computers.	Dynamic routing uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers.
2.	The routers that use the static routing algorithm do not have any controlling mechanism if any faults in the routing paths.	The dynamic routing algorithms are used in the dynamic routers and these routers can sense a faulty router in the network.
3.	These routers do not sense the faulty computers encountered while finding the path between two computers or routers in a network.	The dynamic router eliminates the faulty router and finds out another possible optimal path from the source to the destination.
4.	The static routing is suitable for very small networks and they cannot be used in large networks	Dynamic routing is used for larger networks.

5.	The static routing is the simplest way of routing the data packets from a source to a destination in a network.	The dynamic routing uses complex algorithms for routing the data packets.
6.	The static routing has the advantage that it requires minimal memory.	Dynamic routers have quite a few memory overheads, depending on the routing algorithms used.
7.	The network administrator finds out the optimal path and makes the changes in the routing table in the case of static routing.	In the dynamic routing algorithm, the algorithm and the protocol is responsible for routing the packets and making the changes accordingly in the routing table.

5.2 : Routing Algorithm

Q.3 Explain distance vector routing algorithms with example.

☞ [SPPU : April-18, In-Sem, Marks 4]

Ans. : • Distance vector routing algorithm is the dynamic routing algorithm. It was designed mainly for small network topologies. Distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford** routing algorithm and the **Ford-Fulkerson** algorithm.

- The term distance vector derives from the fact that the protocol includes its routing updates with a vector of distances, or hop counts.
- In this algorithm, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet. This entry contains two parts :
  a. The preferred outgoing line to use for that destination.
  b. An estimate of the time or distance to that destination.
- The metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path, etc.
- Assume that delay is used as a metric and that the router knows the delay to each of its neighbours. All nodes exchange information only

with their neighbouring nodes. Nodes participating in the same local network are considered neighbouring nodes.

- Once every 'T' msec each router sends to each neighbor a list of its estimated delays to each destination. It also receives a similar list from each neighbor.
- By performing calculation for each neighbour, a router can find out which estimate seems the best and use that estimate and the corresponding line in its new routing table. Old routing table is not used in the calculation.
- Fig. Q.3.1 shows the subnet with 12 routers.

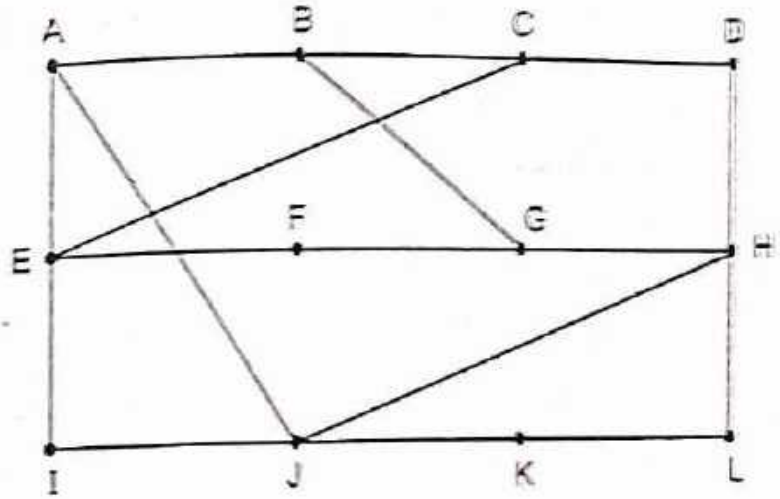


Fig. Q.3.1 Subnet

Routing table is shown below. (Refer table on next page)

Q.4 What are the problems in RIP ? How to overcome the problems ? Compare RIPv1 and RIPv2. ☞ [SPPU : Jun-22, Marks 9]

Ans. : • In RIP, routing updates are exchanged between neighbours approximately every 30 seconds using a so-called **RIP response message.** The response message sent by a router or host contains a list of upto 25 destination networks within an Autonomous System (AS). Response messages are also known as **RIP advertisements.**

- Fig. Q.4.1 shows a portion of an autonomous system.
- Forwarding table in router D before receiving advertisement from router A. For this example, the table indicates that to send a datagram from

To	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9

JA delay is 8 | JI delay is 10 | JH delay is 12 | JK delay is 6

Vectors received from J's four neighbors

New estimated delay from J

New estimated delay from J	Line
8	A
20	A
28	I
20	H
17	I
30	I
18	H
12	H
10	I
0	–
6	K
15	K

New routing table for J

router D to destination network W, the datagram should first be forwarded to neighbouring router A; the table also indicates that destination network W is two hops away along the shortest path.

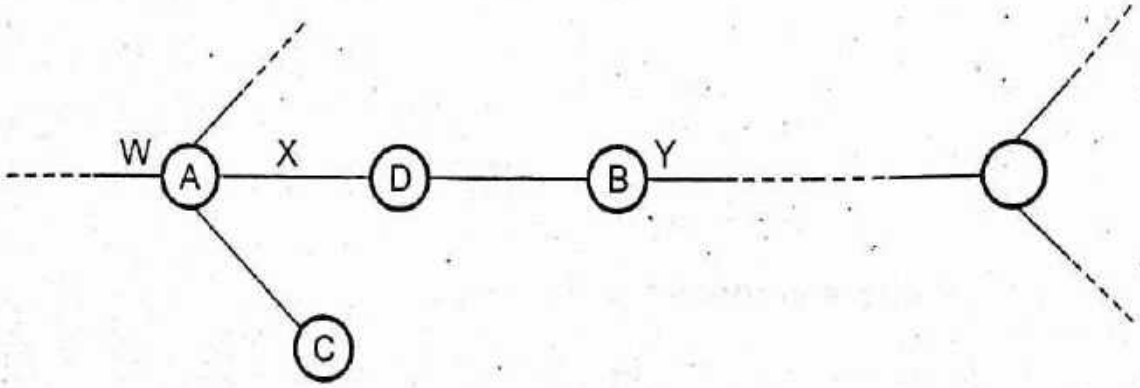


Fig. Q.4.1 Portion of AS

- The Table Q.4.1 also indicates that network Z is seven hops away via router B.

Destination network	Next router	Number of hops to destination
W	A	2
Y	B	2
Z	B	7
X	–	1
.....	.....	.....

Table Q.4.1 Forwarding table

- Now suppose that 30 seconds later, router D receives from router A the advertisement shown in Table Q.4.2.

Destination network	Next router	Number of hops to destination
Z	C	4
W	–	1
X	–	1
.....	.....	.....

Table Q.4.2 Advertisement from router A

- Note that the advertisement is nothing other than the forwarding table information from router A. This information indicates, in particular, that network Z is only four hops away from router A. Router D, upon receiving this advertisement, merges the advertisement with the old routing table.
- Router D learns that there is now a path through router A to network Z that is shorter than the path through router B. Thus, router D updates its forwarding table to account for the shorter shortest path, as shown in Table Q.4.3.

Destination network	Next router	Number of hops to destination
W	A	2
Y	B	2
Z	A	3
.....	.....	.....

Table Q.4.3 Forwarding Table

- RIP routers exchange advertisements approximately every 30 seconds. If a router does not hear from its neighbour atleast once every 180 seconds, that neighbour is considered to be no longer reachable; i.e. either the neighbour has died or the connecting link has gone down. When this happens, RIP modifies the local forwarding table and then propagates this information by sending advertisements to its neighbouring routers.
- A router can also request information about its neighbour's cost to a given destination using RIP's request message. Routers send RIP request and response messages to each other over UDP using port number 520.

RIP Message Format

- Fig. Q.4.2 shows the RIP message format.

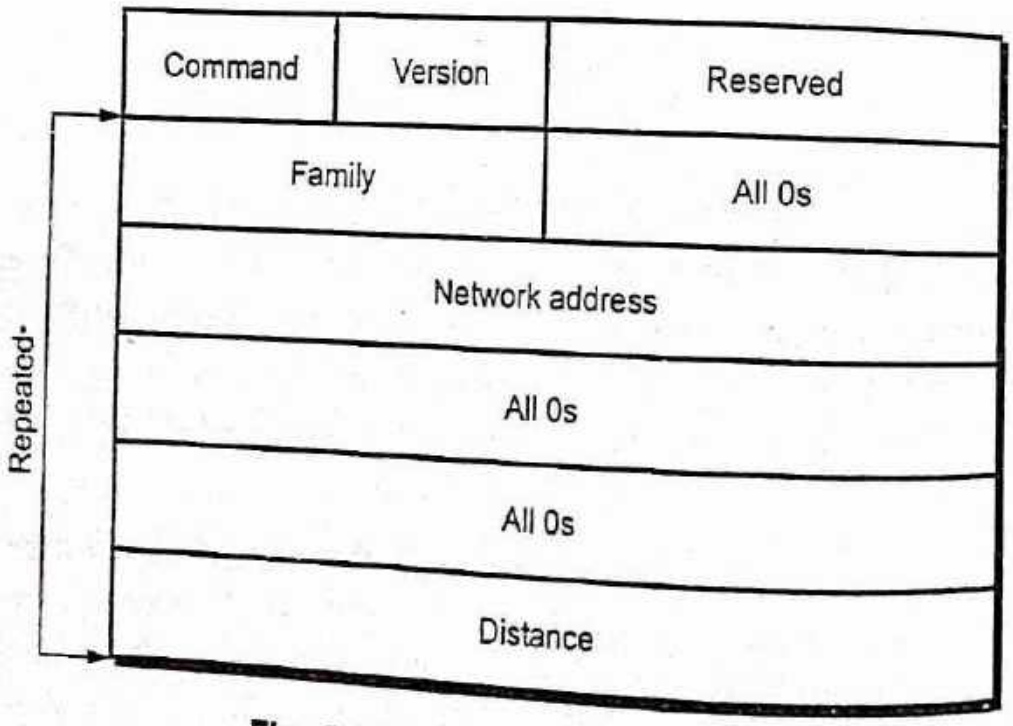


Fig. Q.4.2 RIP message format

1. **Command :** This is 8 bits field specifies the type of message : 1 for request and 2 for response.
2. **Version :** This is 8 bits field define the version.
3. **Family :** This 16 bits field defines the family of the protocol used. For TCP/IP the value is 2.
4. **Network address :** The address field defines the address of the destination network.
5. **Distance :** This 32 bits field defines the hop count from the advertising router to the destination network.

Request and Response

- RIP support two types of messages : Request and Response.

Request

- A request message is sent by a router that has just comp up or by a router that has some time out entries.

Response

- A response message can be either solicited or unsolicited.

1. Solicited response
   - Is sent only in answer to a request.
   - Containing information about the destination specified in the corresponding request.
2. Unsolicited response
   - Is sent periodically, every 30 seconds.
   - **Containing** information covering the whole routing table

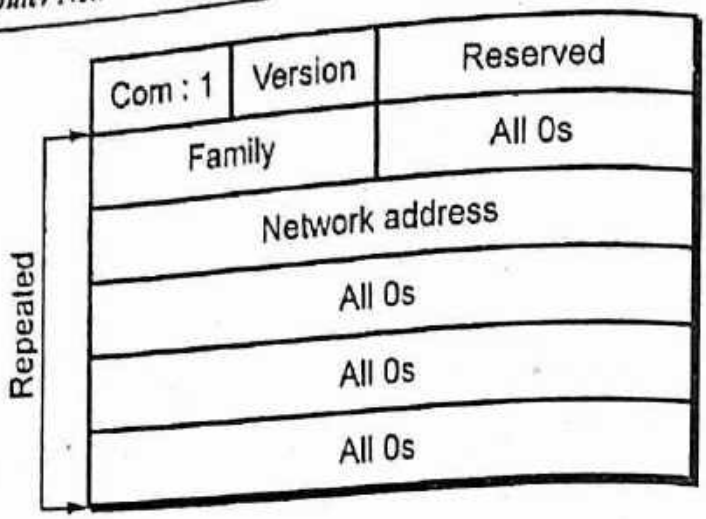
Fig. Q.4.3 shows the request message.

Timers in RIP

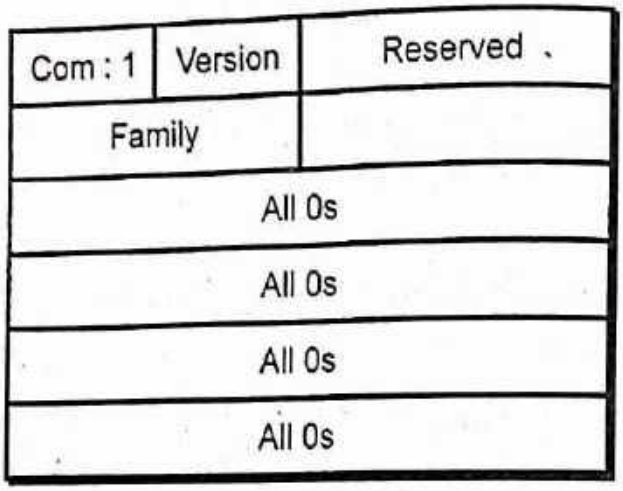
- RIP uses three timers to support its operation.

1. Periodic timer (25 - 35 sec)
2. Expiration (180 sec)
3. Garbage collection (120 sec).

1. **Periodic timer :** This type of timer controls the advertising of regular update messages. Each router has one periodic timer that is randomly set to a number between 25 to 35 seconds.



(a) Request for some



(b) Request for all

Fig. Q.4.3 Request message format

2. **Expiration timer :** The expiration timer governs the validity of a route. In normal situation, the new update for the route occurs every 30 seconds. But, if there is a problem on an internet and no update is received within the allotted 180 seconds, the route is considered expired and the hop count of the route is set to 16. Each router has its own expiration timer.
3. **Garbage collection timer :** When the information about a route becomes invalid, the router continues to advertise the route with a metric value of 16 and the garbage collection timer is set to 120 sec for that route. When the count reaches zero, the route is purged from the table.

RIPv2

- RIP version 2 was designed to overcome some of the shortcomings of version 1. Replaced fields in version 1 that were filled with 0s for the TCP/IP protocols with some new fields.

- **Advantages**

1. An AS can include several hundred routers with RIP-2 protocol.
2. Compatible upgrade of RIPv1 including subnet routing, authentication, CIDR aggregation, route tags and multicast transmission.
3. Subnet support : Uses more convenient partitioning using variable-length subnets
4. An end system can run RIP in passive mode to listen for routing information without supplying any.
5. Low requirement in memory and processing at the node .
6. RIP and RIP2 are for the IPv4 network while the RIPng is designed for the IPv6 network.

Fig. Q.4.4 shows the message format.

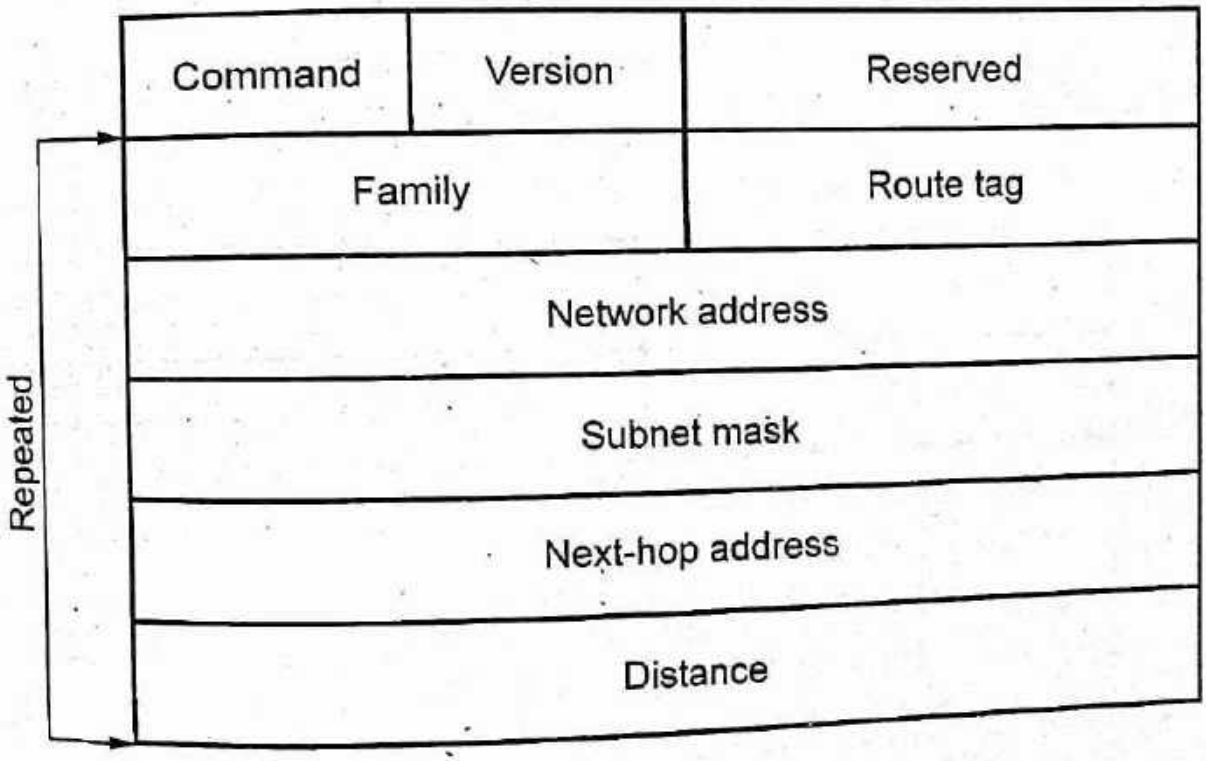


Fig. Q.4.4 Message format of RIPv2

1. **Command** - The command field is used to specify the purpose of the datagram.
2. **Version** - The RIP version number. The current version is 2.
3. **Identifier** - Indicates what type of address is specified in this particular entry.
4. **Route tag** - Attribute assigned to a route which must be preserved and readvertised with a route. The route tag provides a method of separating internal RIP routes from external RIP routes, which may have been imported from an EGP or another IGP.
5. **IP address** - The destination IP address.
6. **Subnet mask** - Value applied to the IP address to yield the non-host portion of the address. If zero, then no subnet mask has been included for this entry.
7. **Next hop** - Immediate next hop IP address to which packets to the destination specified by this route entry should be forwarded.
8. **Distance** - Represents the total cost of getting a datagram from the host to that destination.

Authentication

- Authentication is added to protect the message against unauthorized advertisement. No new field is added to the packet.
- To indicate that the entry is authentication information and not routing information, the value of FFFFH is entered in the family field.
- Fig. Q.4.5 shows the authentication.

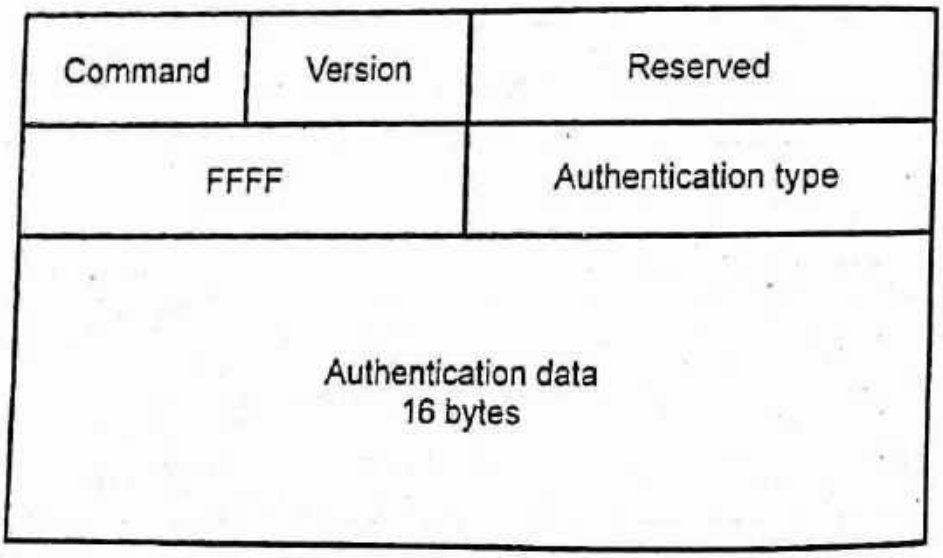


Fig. Q.4.5 Authentication

- Authentication type defines the protocol used for authentication.
- Authentication data is the actual data.

RIP2 - Disadvantages

1. RIP2 supports generic notion of authentication, but only "password" is defined so far. Still not very secure.
2. RIP2 packet size increases as the number of networks increases hence it is not suitable for large networks.
3. RIP2 generates more protocol traffic than OSPF, because it propagates routing information by periodically transmitting the entire routing table to neighbour routers.
4. RIP2 may be slow to adjust for link failures.

Advantages of RIP and Disadvantages of RIP version 1

Advantages of RIP

1. RIP is very useful in a small network, where it has very little overhead in terms of bandwidth used and configuration and management time.
2. Easy to implement than newer IGP's.
3. Many implementations are available in the RIP field.

Disadvantages of RIP1

1. Minimal amount of information for router to route the packet and also very large amount of unused space.
2. Subnet support : Supports subnet routes only within the subnet network.
3. Not secure; anyone can act as a router just by sending RIP1 messages.

RIP1 was developed for an AS that originally included less than a 100 routers.

Q.5 Compare between RIPv1 and RIPv2.

☞ [SPPU : April-18, In-Sem, Marks 4]

Ans. :

Sr. No.	RIPv1	RIPv2
1.	It is classful protocol.	It is classless protocol.

2.	There is no support for router authentication.	It support for authentication.
3.	It does not support variable length subnet mask.	It support variable length subnet mask.
4.	RIPv1 uses broadcasts for updates.	RIPv2 uses multicast for updates.
5.	It does not support variable length subnet mask.	It does not support variable length subnet mask.

Q.6 Explain Link State routing.

Ans. : • Link state routing is the second major class of intradomain routing protocol. It is **dynamic** type routing algorithm.

- The idea behind link state routing is simple and can be stated as five parts. Each router must do the following :

1. **Learning about the neighbors :** When a router is booted, it sends a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a reply telling who it is. When two or more routers are connected by a LAN, the LAN can be modeled as a node.
2. **Measuring line cost :** To determine the cost for a line, a router sends a special ECHO packet over the line that the other side is required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay. Should the load be taken into account when measuring the delay ?
3. **Building link state packets :** State packets may be built periodically, or when some significant event occurs, such as a line or neighbour going down or coming back up again.
4. **Distributing the link state packets :** The basic algorithm
   - Each state packet contains a sequence number that is incremented for each new packet sent.
   - Routers keep track of all the (source router, sequence) pairs they see.

- When a new link state packet comes in, it is checked against the list of packets already seen. If it is new, it is forwarded on all lines except the one it arrived on (i.e., flooding). If it is a duplicate, it is discarded. If a packet with a sequence number lower than the highest one seen so far ever arrives, it is rejected as being obsolete.

Problems with the basic algorithm :

1. The sequence numbers may wrap around, causing confusion. Solution : Using a 32-bit sequence number. With one packet per second, it would take 137 years to wrap around.
2. If a router ever crashes, it will lose track of its own sequence number. If it starts again at the sequence number 0, new packets will be rejected as obsolete/duplicate by other routers.
3. If a sequence number is ever corrupted and 65,540 is received instead of 4 (a 1-bit error), packets 5-65540 will be rejected as obsolete.

- The solution to router crashes and sequence number corruption is to associate an age with each state packet from any router and decrement the age once per second. When the age hits zero, the information from that router is discarded. Normally a new packet comes in every 10 seconds, so router information only times out when a router is down.

Some refinements to the basic algorithm make it more robust

- When a state packet comes in to a router for flooding, it is put in a holding area to wait a short while first.
- If another state packet from the same source comes in before it is transferred, their sequence numbers are compared.
- If they are equal, the duplicate is discarded.
- If they are different, the older one is thrown out. To guard against errors on the lines, all state packets are acknowledged.
- When a line goes idle, the holding area is scanned in round robin to select a packet or acknowledgement to send.

5. Computing the new routes : Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph. Then Dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations.

- Link state routing protocols use event driven updates rather than periodic updates. Link state routing is widely used in actual networks. OSPF protocol uses in a link state algorithm.
- Link state routing protocols are as follows :
  a. Open Shortest Path First (OSPF)
  b. Netware Link Services Protocol (NLSP).
  c. Apple's AURP.
  d. ISO's Intermediate System-Intemediate System (IS-IS).

Q.7 Explain with neat diagram OSPF routing protocol.

☞ [SPPU : May-18, Marks 6 Dec.-19, Marks 6]

Ans. : • OSPF is a link state routing protocol. OSPF is based on the distributed map concept all nodes have a copy of the network map, which is regularly updated. Each node contains a routing directory database.

- This database contains informations about the routers interfaces that are operable, as well as status information about adjacent routers. This information is periodically broadcast to all routers in the same domain.
- The OSPF computes the shortest path to the other routers. OSPF protocol is now widely used as the interior router protocol in TCP/IP networks. OSPF computes a route through the internet that incurs the least cost based on a user-configurable metric of cost.
- The user can configure the cost to express a function of delay, data rate, or other factors. OSPF is able to equalize loads over multiple equal cost paths.
- OSPF is classified as an Internal Gateway Protocol (IGP) because it support routing within one autonomous system only. The exchange of routing information between autonomous systems is the responsibility of another protocol an External Gateway Protocol (EGP). OSPF can support one or many networks.
- Following is the features of the OSPF.
  1. OSPF supports multiple circuit load balancing because it can store multiple routes to a destination.
  2. OSPF can converge very quickly to network topology change.

3. OSPF support multiple metrics.
4. OSPF is not susceptible to routing loops.
5. OSPF support for variable length subnetting by including the subnet mask in the routing message.

- OSPF introduces a two level hierarchy for improving scalability. It allows an AS to be partitioned into several groups called areas, that are interconnected by a central backbone area as shown in the Fig. Q.7.1.

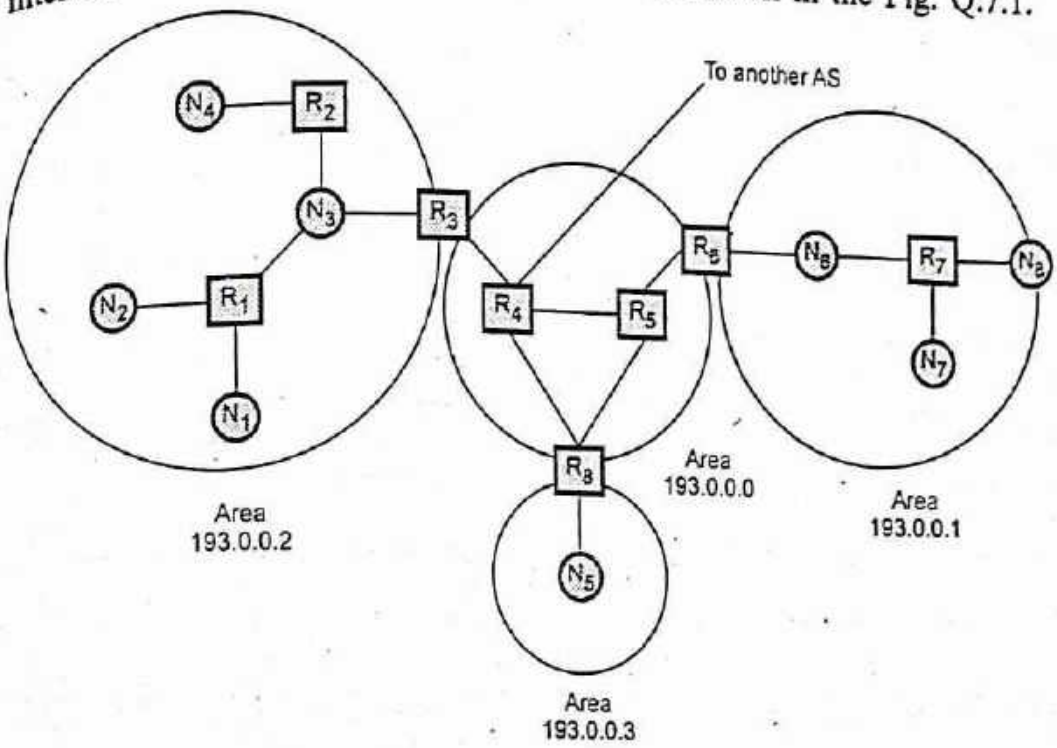


Fig. Q.7.1 OSPF areas

- An area is identified by a 32-bit number known as the area ID. The backbone area is identified with area ID 193.0.0.0. The information from other area is summarized by area border router that have connections to multiple areas.
- OSPF uses four types of routers.
  1. An internal router is a router with all its links connected to the networks within the same area.
  2. An area border router is a router that has its links connected to more than one area.
  3. A backbone router is a router that has its links connected to the backbone.

4. An Autonomous System Boundary Router (ASBR) is a router that has its links connected to another autonomous system.

- As shown in the Fig. Q.7.1 routers R_1, R_2 and R_7 are internal routers. Routers R_3, R_6, R_8 are area border routers. Routers R_3, R_4, R_5, R_6, R_8 are backbone routers. Router R_4 is an ASBR.
- A hello protocol allows neighbours to be discovered automatically. Two routers are said to be neighbours if they have an interface to a common network.
- The OSPF protocol runs directly over IP, using IP protocol 89. The header format for OSPF is shown in the Fig. Q.7.2.

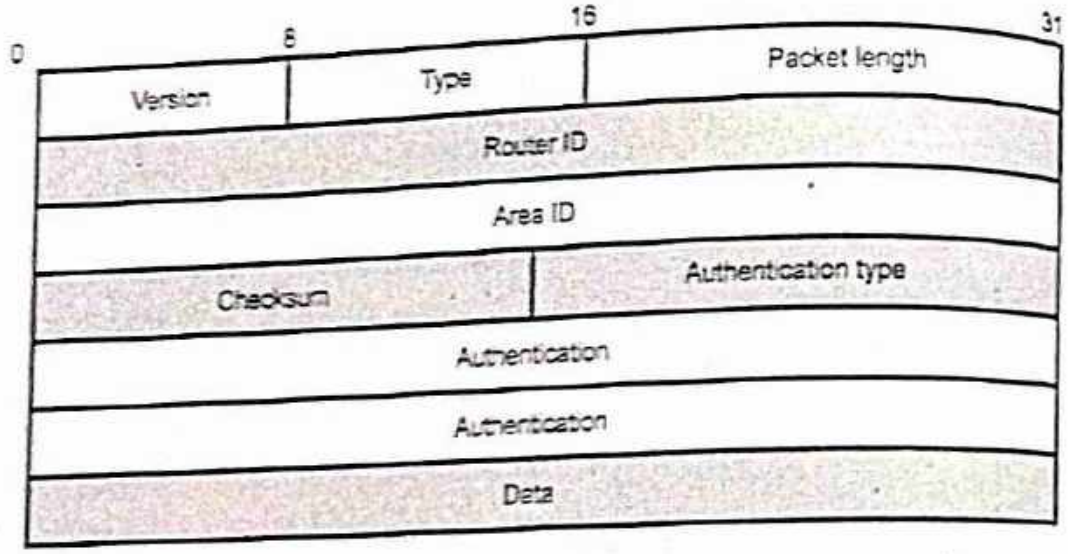


Fig. Q.7.2 OSPF common header

- OSPF header analysis is given below :
  1. **Version :** This field specifies the protocol version.
  2. **Type :** This field indicates messages as one of the following type.
     a. Hello
     b. Database description
     c. Link status
     d. Link status update
     e. Link status acknowledgement.
  3. **Packet length :** This field specifies the length of OSPF packet in bytes, including the OSPF header.
  4. **Router ID :** It identifies the sending router. This field is typically set to the IP address of one of its interfaces.

5. **Area ID** : This field identifies the area this packet belongs to (Transmitted).
6. **Checksum** : The checksum field is used to detect errors in the packet. The checksum is performed on the entire packet.
7. **Authentication type** : It identifies the authentication type that is used.
8. **Authentication** : This field includes a value from the authentication type.

- The OSPF operation consists of the following stages.

1. OSPF send the Hello messages for discovering the neighbours and designated routers are elected in multiaccess networks.
2. Adjacencies are established and link state databases are synchronized.
3. Link state advertisement are exchanged by adjacent routers to allow topological databases to be maintained and to advertise inter area and inter AS routes. The routers use the information in the database to generate routing tables.

OSPF Advantages

1. Low traffic overhead. OSPF is enconomical of network bandwidth on links between routers.
2. Fast convergence. OSPF routers flood updates to changes in the network around the internet, so that all routers quickly agree on the new topology after a failure.
3. Larger network metrics. This allows a network planner the freedom to assign costs for each path around the network, to give fine control over routing paths.
4. Area based topology. Large OSPF networks are organized as a set of areas linked by a backbone. Routing within each area is isolated to minimize cross area discovery traffic.
5. Route summaries. OSPF can minimize the routes propagated across an area boundary by collapsing several related sub-net routes into one. This reduces routing table sizes and increases the practical size of a network.
6. Support for complex address structures. OSPF allows variable size sub-netting within a network number and sub-nets of a network number to be physically disconnected. This reduces waste of address space and makes changing a network incrementally much easier.

7. Authentication. OSPF supports the use of passwords for dynamic discovery traffic, and checks that paths are operational in both directions. The main use for this is to prevent misconfigured routers from "poisoning" the routing tables throughout the internet.

OSPF Disadvantages

1. Memory overhead. OSPF uses a link state database to keep track of all routers and networks within each attached area. With a complex topology, this database can be much larger than the corresponding routing pool and may limit the maximum size of an area.
2. Processor overhead. During steady state operation the OSPF CPU usage is low, mainly due to the traffic between routers. However, when a topology change is detected, there is a large amount of processing required to support flodding of changes and recalculation of the routing table.
3. Configuration. OSPF can be complex to configure.

Q.8 Compare and contrast distance vector routing with link state routing. ☞ [SPPU : Dec.-18, Marks 4]

Ans. :

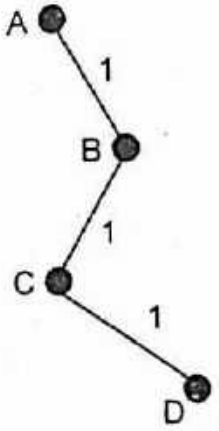
Sr. No.	Distance vector	Link state
1.	Bellman-ford algorithm used to calculate the shortest cost path.	Dijkstra's algorithm used to calculate link state cost.
2.	Sends message to their neighbors.	Sends message to every other node in the network.
3.	It is decentralized routing algorithm.	It is centralized global routing algorithm.
4.	Sends larger updates only to neighbouring routers.	Send small updates every where.
5.	Protocol example - RIP	Protocol example - OSPF and BGP.

6.	Require less CPU power and less memory space.	Require more CPU power and more memory space.
7.	Simple to implement and support.	Expensive to implement and support.

Q.9 Explain distance vector routing with count-to-infinity problem.

☞ [SPPU : April-19, Marks 4]

Ans. : • Fig. Q.9.1 shows an imagined network and denotes the distances from router A to every other router. Until now everything works fine.

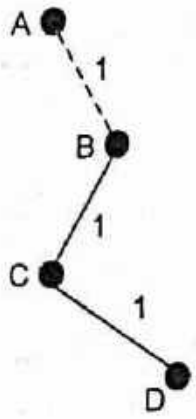


Routing table for A

B	C	D
1	2	3

Fig. Q.9.1

- Suppose that link (A, B) is broken. Router B observed it, but in his routing table he sees, that router C has a route to A with 2 hops. The problem is, that B does not know that C has router B as successor in his routing table on the route to A. That followed **count-to-infinity** problem. Router B actualizes his routing table and takes the router to A over router C.
- In Fig. Q.9.2, we can see the new distances to A. In router C's routing the route to A contains router B as next hop router, so if B has increased his costs to A, C is forced to do so. Router C increases his cost to A about B + 1 = 4.
- Now we see the conseuqence of the distributed Bellman-Ford protocal : Because router B takes the path over C to A, he reactualizes his routing table and so on.



B	C	D
3	2	3

B	C	D
3	4	3

B	C	D
5	4	5

Fig. Q.9.2

- There are several partial solutions to the count-to-infinity problem. The first one is to use some relatively small number as an approximation of infinity. For example, we might decide that the maximum number of hops to get across a certain network is never going to be more than 16 and so we could pick 16 as the value that represents infinity.
- This at least bounds the amount of time that it takes to count to infinity. Of course, it could also present a problem if our network grew to a point where some nodes were separated by more than 16 hops.
- One technique to improve the time to stabilize routing is called **split horizon**. Split horizon technique implies that routing information about some network stored in the routing table of a specific router is never sent to the router from which it was received.

Issues with the Distance Vector Routing

1. The primary drawback of this algorithm is its vulnerability to the 'Count-to-Infinity' problem. There have been proposed many partial solutions but none works under all circumstances.
2. Another drawback of this scheme is that it does not take into account Link Bandwidth.
3. Yet another problem with this algorithm is that it takes appreciably long time for convergence as the network-size grows.
4. A fallout of the Count-to-Infinity issue and slow convergence has been to limit the maximum number of hops to 15 which means more than 16-router subnets, it may not be appropriate routing algorithm.

Q.10 Understand and apply what is routing? Explain different types of routing algorithm. ☞ [SPPU : April-19, Marks 6]

Ans. : Refer Q.1, 3 & 5.

5.3 : EIGRP

Q.11 Explain EIGRP.

Ans. :

- Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance vector routing protocol based on the principles of the Interior Gateway Routing Protocol (IGRP).
- EIGRP is Cisco's IGP (Interior Gateway Protocol) that was made an "open standard" in 2013.
- EIGRP is an enhanced distance vector protocol, relying on the Diffused Update Algorithm (DUAL) to calculate the shortest path to a destination within a network.

Characteristics of EIGRP

- EIGRP has the following characteristics :
  1. Advanced operational efficiency
  2. Capabilities of both link state and distance vector
  3. A classless routing protocol
  4. Unique features including use of Reliable Transport Protocol (RTP), a diffusing update algorithm (DUAL), updates and updated information about neighbors
  5. Faster converging because it precalculates routes and does not broadcast hold-down timer packets before converging

Advantages of EIGRP

- Some of the many advantages of EIGRP are :
  1. Very low usage of network resources during normal operation; only hello packets are transmitted on a stable network.
  2. When a change occurs, only routing table changes are propagated, not the entire routing table; this reduces the load the routing protocol itself places on the network.
  3. Rapid convergence times for changes in the network topology (in some situations convergence can be almost instantaneous).

Q.12 Draw the router architecture. Explain the difference between RIP, EIGRP, OSPF in tabular format. ☞ [SPPU : June-22, Marks 9]

Ans. : A router is a networking device that allows separate individual networks of computers to connect with one another. Fig. Q.12.1 shows router architecture.

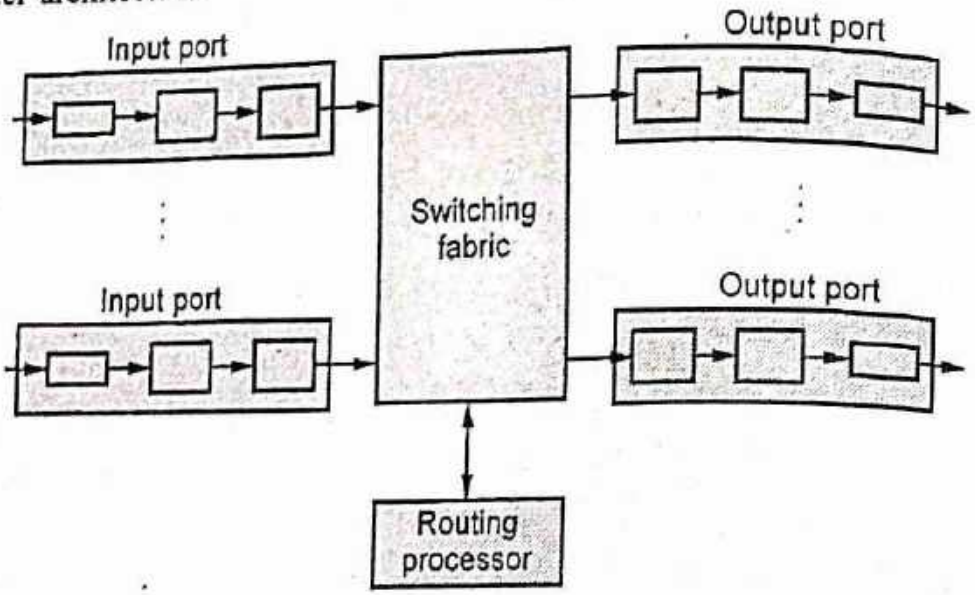


Fig. Q.12.1 Router architecture

- Router components are input port, output port, switching fabric and routing processor.
- Input port : It performs the physical layer functionality of terminating an incoming physical link to a router. It also performs the data link layer functionality and performs a lookup and forwarding function. Control packets are forwarded from the input port to the routing processor.
- Switching fabric : The switching fabric connects the router's input ports to its output ports.
- Output ports : An output port stores the datagrams that have been forwarded to it through the switching fabric and then transmits the datagrams on the outgoing link. The output port thus performs the reverse data link and physical layer functionality as the input port.

- Routing processor : The routing processor executes the routing protocols, maintains the routing tables and performs network management functions within the router.

Difference between RIP, EIGRP and OSPF :

RIP	EIGRP	OSPF
RIP is a distance vector protocol.	EIGRP is derived from Integrated Gateway Routing Protocol.	OSPF is a link state protocol.
It support maximum 15 routers in the network.	It supports maximum 255 routers in the network.	It supports unlimited router in the network.
Metrics used is hop.	Metrics used are bandwidth and delay, load and reliability.	Metrics used are bandwidth and delay.
It is basically use for smaller size organization.	It is basically use for medium to larger size organization in the network.	It is basically use for larger size organization in the network.
Admin cannot create a separate administrative boundary in the network.	Admin can create a separate administrative boundary in the network with the help of autonomous system number.	Admin can create a separate administrative boundary in the network through area number within the same area all of the routers are exchanging the route information from neighbour router in the network.

5.4 : Border Gateway Protocol (BGP)

Q.13 What is BGP ? What are the characteristics of BGP routing protocol ? What are the advantages and disadvantages of BGP routing protocol ? ☞ [SPPU : Jun-22, Marks 9]

Ans. : • The purpose of an exterior gateway protocol is to enable two different Autonomous System (AS) to exchange routing information so that IP traffic can flow across the autonomous system border. BGP was developed for use in conjunction with internets that employ the TCP/IP protocol suite. The BGP is an interdomain routing protocol that is used to exchange network reachability information among BGP routers (Also called BGP speakers). Each BGP speaker establishes a TCP connection with one or more BGP speakers (routers). Two routers are considered to be neighbours if they are attached to the same subnetwork. If the two routers are in different autonomous systems, they may wish to exchange routing information.

- BGP performs three functional procedures.
  1. Neighbour acquisition
  2. Neighbour reachability
  3. Network reachability
- Neighbour acquisition procedures used for exchanging the routing information between two routers in different Autonomous Systems (AS). To perform neighbour acquisition, one router sends an open message to another. If the target router accepts the request, it returns a keepalive message in response.
- Once a neighbour relationship is established, the neighbour reachability procedure is used to maintain the relationship. Both sides needs to be assured that the other side still exists and is still engaged in the neighbour relationship. For this purpose, both routers send .keepalive messages to each other. Both sides router maintains a database of the subnetworks that it can reach and the perferred route for reaching that subnetwork.
- If the database changes, router issues an update message that is broadcast to all other routers implementing BGP. By the broadcasting of these update message, all the BGP routers can build up and maintain routing information. BGP connections inside an autonomous system are called internal BGP (iBGP) and BGP connections between different autonomous systems are called external BGP (eBGP).

Fig. Q.13.1 shows the internal and external BGP.

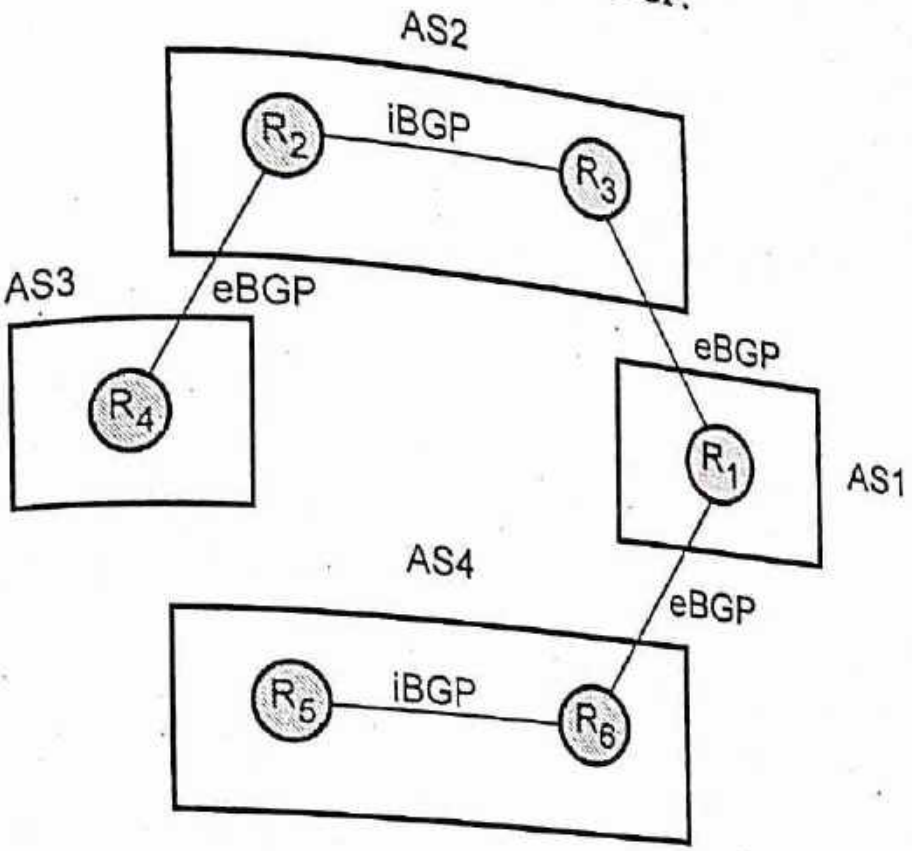


Fig. Q.13.1 Internal and external BGP

BGP messages : Header of the all BGP messages is fixed size that identifies the message type. Fig. Q.13.2 shows the BGP message header format.

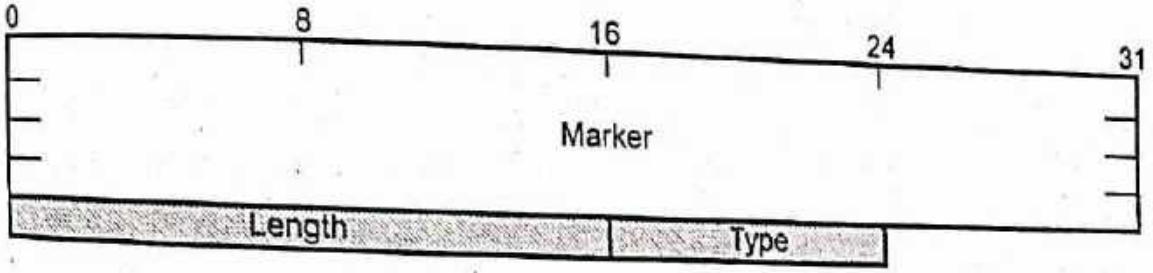


Fig. Q.13.2 BGP header format

1. **Marker :** Marker field is used for authentication. The sender may insert value in this field that would be used as part of an authentication mechanism to enable the recepient to verify the identity of the sender.
2. **Length :** This field indicates the total length of the message in octets, including the BGP header. Value of the length must be between 19 and 4096.

3. Type : Type field indicates type of message. BGP defines four message type.
   a) OPEN b) UPDATE c) NOTIFICATION d) KEEPALIVE

- Following Fig. Q.13.3 shows the four types of message formats.

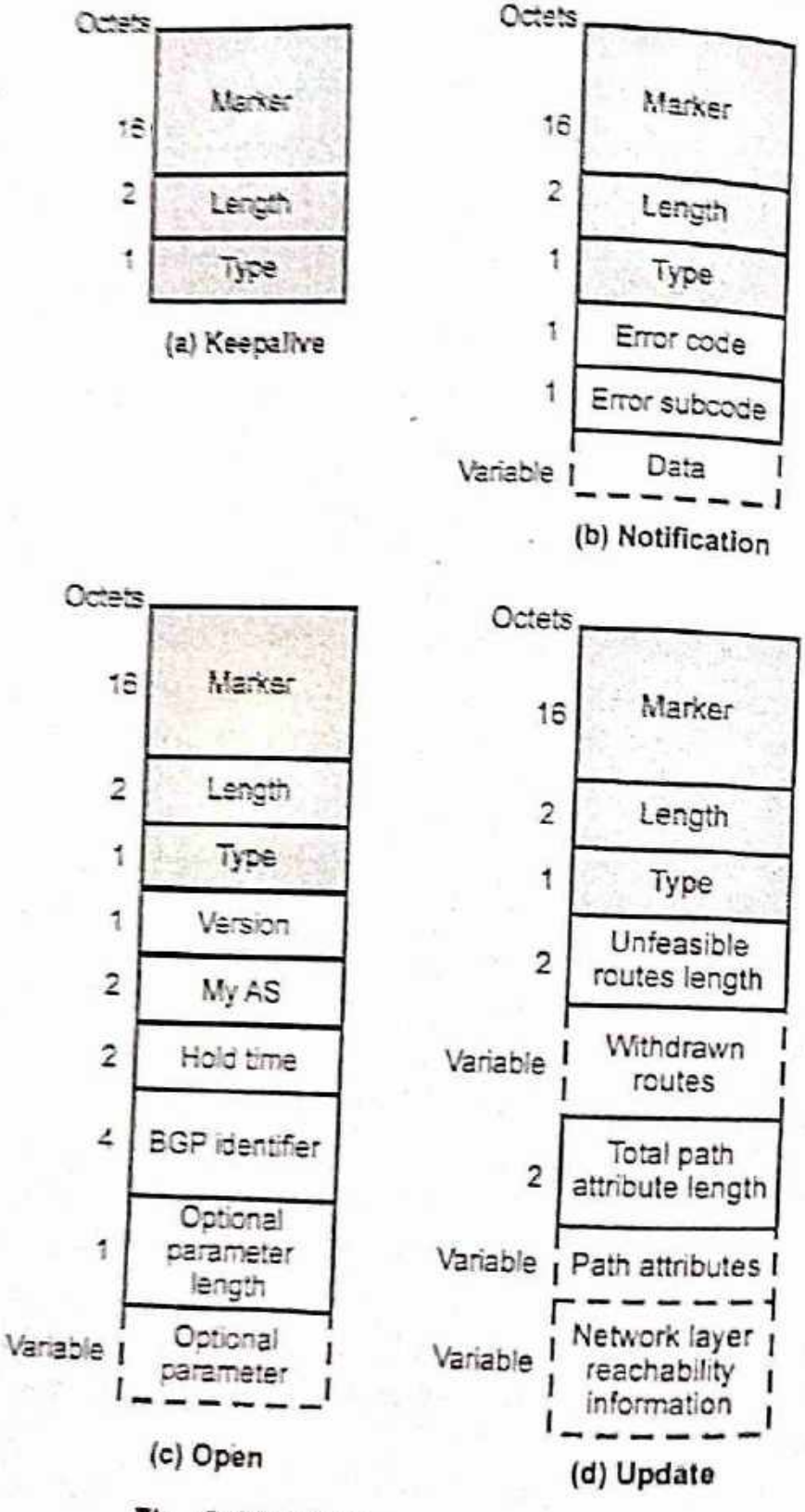


Fig. Q.13.3 BGP message format

- To acquire a neighbour, a router first opens a TCP connection to the neighbour router of interest. It then sends the open message. This message identifies the AS (Autonomous System) to which the sender belongs and provides the IP address of the router. It also includes a Hold time parameter. If the recipient is prepared to open a neighbour relationship, it calculate a value of Hold Timer that is the minimum of its Hold Time in the open message. This calculated value is the maximum number of seconds that may elapse between the receipt of successive keepalive and update message by the sender.
- The KEEPALIVE message is just the BGP header with the type field set to 4. The KEEPALIVE messages are exchanged often enough as to not cause the hold timer to expire. A recommended time between successive KEEPALIVE messages is one-third of the hold time interval. This value ensures that KEEPALIVE messages arrive at the receiving router almost always before the hold timer expires even if the transmission delay of a TCP is variable. If the hold time is zero, then KEEPALIVE messages will not be sent.
- When a BGP router detects an error, the router sends a NOTIFICATION message and then close the TCP connection. After the connection is established, BGP peers exchange routing information by using the UPDATE messages.
- The UPDATE messages may contain three pieces of information. Unfeasible routes, path attributes and network layer reachability information.
- An UPDATE message can advertise a single route and withdraw a list of route. An update message may contain one or both types of information. The UPDATE messages are used to construct a graph of Autonomous System (AS) connectivity. The withdrawn routes field provides a list of IP address prefixes for the routes that need to be withdrawn from BGP routing tables. The unfeasible routes length field indicates the total length of the withdrawn routes field in octates.
- An UPDATE message can withdraw multiple unfeasible routes from service. A BGP router uses Network Layer Reachability Information

(NLRI), the total path attributes length and the path attributes t
advertise a route. The NLRI field contains a list of IP address prefixe
that can be reached by the route.

Advantages of BGP

1. BGP is a very robust and scalable routing protocol.
2. CIDR is used by BGP to reduce the size of the Internet routing tables.
3. BGP easily solves the count-to-infinity problem.

Disadvantages of BGP

1. BGP is complex.
2. BGP routes to destination networks, rather than to specific hosts or routers.

END...

Unit VI

6 Transport Layer - Services and Protocols

6.1 : Transport Layer Duties and Functionalities

Q.1 Explain various transport layer services.

☞ [SPPU : May-17, End Sem, Marks 4]

Or Write a short note on quality of service parameter in transport layer.

☞ [SPPU : Dec.-19, Marks 4]

Ans. : • The transport protocol should provide to higher-level protocols. The transport entity that provides services to transport service users, which might be an application process. The hardware and software within the transport layer that does the work is called the transport entity. It can be in the operating system kernel, in a separate user process or on the network interface card. The relationship of the network, transport and application layers is shown in Fig. Q.1.1. (See Fig. Q.1.1 on next page)

- The following categories of service are useful for describing the transport service.

1. Type of service
2. Quality of service
3. Data transfer
4. User interface
5. Connection management
6. Expedited delivery
7. Status reporting
8. Security

1. Type of service :

- It provides two types of services connection-oriented and connectionless or datagram service. A connection-oriented service provides for the establishment, maintenance and termination of a logical connection between transport service users. The connection-oriented service generally implies that the service is reliable. The connection-oriented

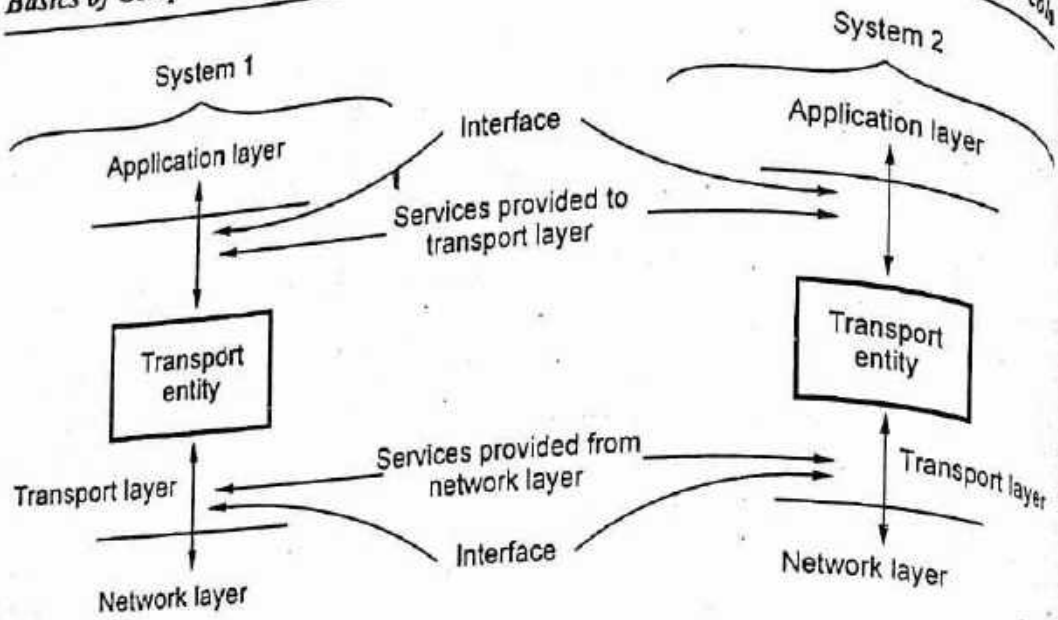


Fig. Q.1.1 Transport entity

service allows for connection-related features such as flow control, error control and sequenced delivery.

2. Quality of service :

- The transport protocol entity should allow the transport service user to specify the quality of transmission service to be provided. Following are the transport layer quality of service parameters
  - I) Error and loss levels
  - II) Desired average and maximum delay
  - III) Throughput
  - IV) Priority level
  - V) Resilience
- The error and loss level measures the number of lost or garbled messages as a fraction of the total sent.
- The desired average and maximum delay measures the time between a message being sent by the transport user on the source machine and its being received by the transport user on the destination machine. The throughput parameter measures the number of bytes of user data transferred per second, measured over some time interval.
- The priority level parameter provides a way for a transport user to indicate that some of its connection are more important than other ones.

The high priority connections get serviced before the low priority ones. Examples of applications that might request particular qualities of service are as follows :

a) A FTP might require high throughput.

b) A transaction protocol may require low delay.

c) An E-mail protocol may require multiple priority levels.

3. Data transfer :

- It transfers data between two transport entities. Both user data and control data must be transferred. Full duplex service must be provided. Half-duplex and simplex modes may also be offered.

4. User interface :

- There is not clear mechanism of the user interface to the transport protocol should be standardized.

5. Connection management :

- If connection-oriented service is provided, the transport entity is responsible for establishing and terminating connections. Symmetric connection procedure should be provided, which allows either TS user to initiate connection establishment.

6. Status reporting :

- It gives the following information.
  a) Addresses
  b) Performance characteristics of a connection
  c) Class of protocol in use
  d) Current timer values.

7. Security :

- The transport entity may provide a variety of security services. It provides encryption and decryption of data. The transport entity may be capable of routing through secure links or nodes if such a service is available from the transmission facility.

6.2 : Transmission Control Protocol (TCP)

Q.2 State and explain services provided by TCP.

☞ [SPPU : Oct.-16, In Sem, Marks 4]

Ans. : • TCP and UDP use the same network layer (IP), TCP provides totally different services. TCP provides a connection-oriented, reliable, byte stream service. There are exactly two end points communicating with each other on a TCP connection.

- TCP does not support multicasting and broadcasting. The application data is broken into what TCP considers the best sized chunks to send. The unit of information passed by TCP to IP is called a segment.
- When TCP sends a segment it maintains a timer, waiting for the other end to acknowledge reception of segment. If an acknowledgement isn't received in time, the segment is retransmitted.
- When TCP receives data from the other end of the connection, it sends an acknowledgement. TCP maintains a checksum on its header and data.
- TCP segments are transmitted as IP datagrams, and since IP datagrams can arrive out of order, TCP segments can arrive out of order. Since IP datagrams can get duplicated, a receiving TCP must discard duplicate data.
- TCP also provides flow control. Each end of a TCP connection has a finite amount of buffer space. A receiving TCP only allows the other end to send as much data as the receiver has buffers for. This prevents a fast host from taking all the buffers on a slower host.
- A TCP connection is a byte stream, not a message stream. A stream of 8-bit bytes is exchanged across the TCP connection between the two applications. There are no record markers automatically inserted by TCP. This is called a **byte stream service**.
- If the application on one end writes 20 bytes followed by a write of 40 bytes, followed by a write of 80 bytes, the application at the other end of the connection cannot tell what size the individual writes there. The

other end may read 140 bytes ones at a time or 140 bytes in two reads of 70 bytes at a time.

- TCP does not interpret the contents of the bytes at all. TCP has no idea if the data bytes being exchanged are binary data, ASCII character or any other.

Q.3 Explain TCP header format.

☞ [SPPU : Dec.-14, End Sem, Aug.-15, In Sem, Marks 4]

Or Explain TCP header format.

☞ [SPPU : May-19, Marks 4]

Ans. : The TCP data is encapsulated in an IP datagram as shown in the Fig. Q.3.1 (a).

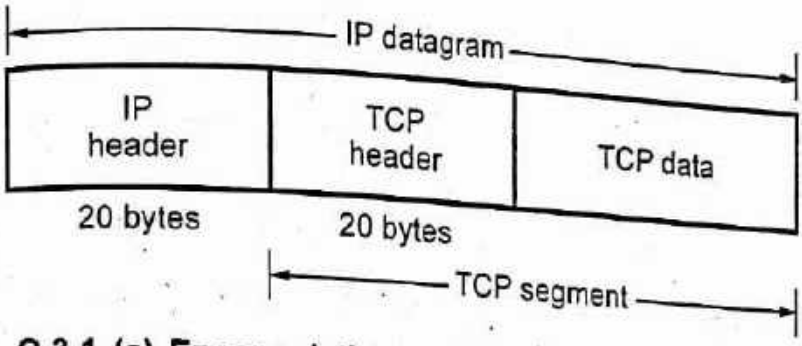


Fig. Q.3.1 (a) Encapsulation of TCP data in an IP datagram

- Fig. Q.3.1 (b) shows the format of the TCP header.
- Description of field in the TCP header as follows :

1. **Source port :** It specifies the application sending the segment. This is different from the IP address, which specifies an internet address.
2. **Destination port :** It identifies the receiving application port numbers below 256 are called well-known ports and have assigned to commonly used applications. For examples, port 23 corresponds to a Telnet function. Port 53 for DNS name server and port 21 assigned for FTP.
3. **Sequence number :** Each byte in the stream that TCP sends is numbered. The sequence number wraps back to 0 after $2^{32} - 1$.
4. **Acknowledgement number :** This field identifies the sequence number of the next data by the that the sender expects to receive if the ACK bit is set. If the ACK bit is not set, this field has no effect.

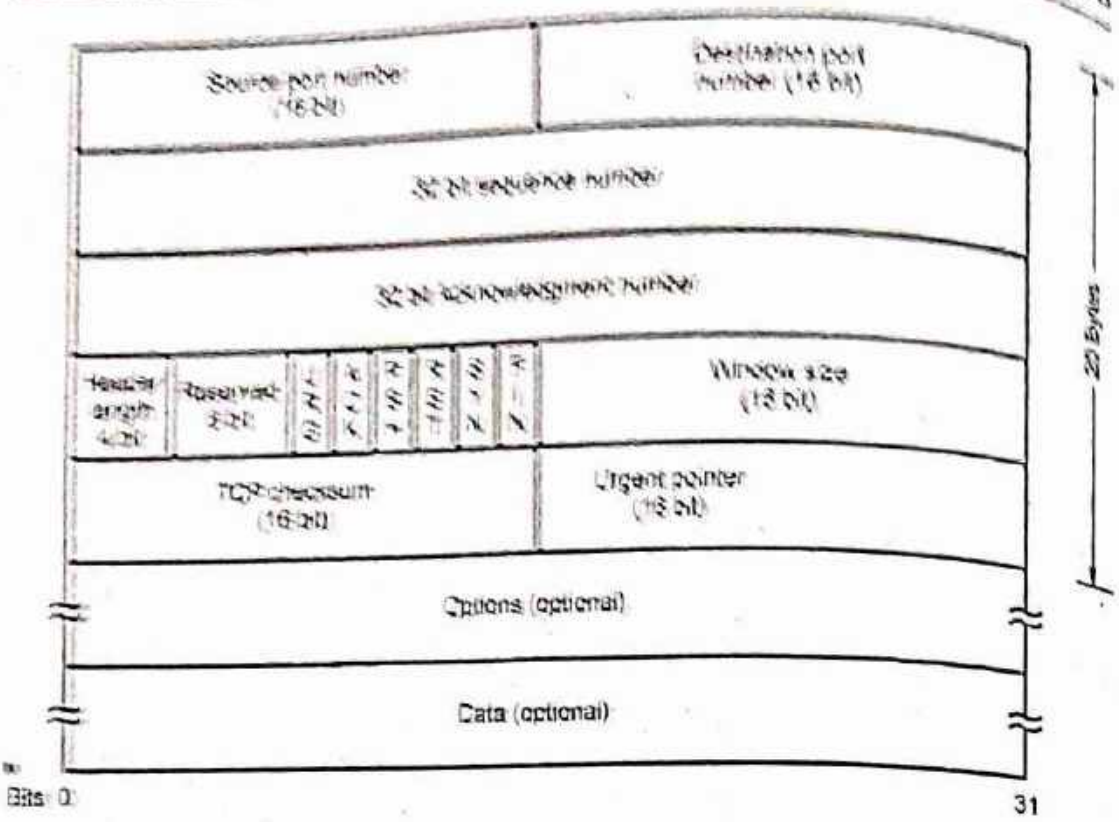


Fig. Q.3.1 (b) TCP header format

5. **Header length :** It specifies the length of the TCP header in 32-bit words. Because of option field, header length is used.
6. **Reserved :** This field is reserved for future use and must be set to 0 (zero).
7. TCP header contains six flag bits. One or more than one can be turned on at the same time. The function of each flag is as follows.
   a. **URG :** The Urgent pointer is valid if it set to 1.
   b. **ACK :** ACK bit is set to 1 to indicate that the acknowledgment number is valid.
   c. **PSH :** The receiver should pass this data to the application as soon as possible.
   d. **RST :** This flag is used to reset the connection. It is also used to reject an invalid segment.
   e. **SYN :** Synchronize sequence number to initiate a connection. The connection request has SYN = 1 and ACK = 0 to indicate that the piggyback acknowledgement field is not in use.
   f. **FIN :** The FIN bit is used to release a connection. It specifies that the sender is finished sending data.

8. **Window size :** It specifies the number of bytes the sender is willing to accept. This field can be used to control the flow of data and congestion.
9. **Checksum :** Used for transport layer error detection.
10. **Urgent pointer :** If the URG flag bit is set, the segment contains urgent data meaning the receiving TCP entity must deliver it to the higher layers immediately.
11. **Options :** Size of this field is variable options field may be used to provide other functions that are not covered by the header.
12. **Data :** Data field size is variable. It contains user data.

- TCP header normal size is 20 bytes, unless options are present. Each TCP segment contains the source and destination port number to identify the sending and receiving application.
- The port number alongwith 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 a **socket**.
- Sequence number is a 32-bit unsigned number. Sequence number identifies the byte in the stream of data from sending TCP to the receiving TCP that the first byte of data in this segment represents.
- When a new connection is being established, the SYN flag is turned on. The sequence number of the first byte of data sent by this host will be the ISN plus one because, the SYN flag consumes a sequence number.
- Every byte that is exchanged is numbered, the acknowledgement number contains the next sequence number that the sender of the acknowledgement excepts to receive. Therefore the sequence number plus 1 of the last successfully received byte of data. This field is valid only if the ACK flag is on.
- TCP provides full duplex service. Therefore, each end of a connection must contain a sequence number of the data flowing in each direction.
- TCP can be described as a sliding window protocol without selective or negative acknowledgements.

- The TCP header length tells how many 32-bit words are contained in the TCP header. This information is needed because the options field is of variable length with a 4-bit field, TCP is limited to a 60-byte header. Without options, the normal size is 20 bytes.
- TCP's flow control is handled using a variable size sliding window. This is the number of bytes, starting with the one specified by the acknowledgement number field, that the receiver is willing to accept.
- This is a 16-bit field, limiting the window to 65535 bytes.
- The checksum covers the TCP segment, the TCP header and the TCP data. Checksum field must be calculated and stored by the sender and then verified by the receiver.
- The urgent pointer is valid only if the URG flag is set. This pointer is a positive offset that must be added to the sequence number field of the segment to yield the sequence number of the last byte of urgent data. Option field is the maximum segment size option, called the Maximum Segment Size (MSS). MSS is the largest chunk of data that TCP will send to the other end.

Q.4 Explain the three-way handshake algorithm for TCP connection establishment. List the fields in TCP header that are not part of UDP header. Give the reasons of each missing field.

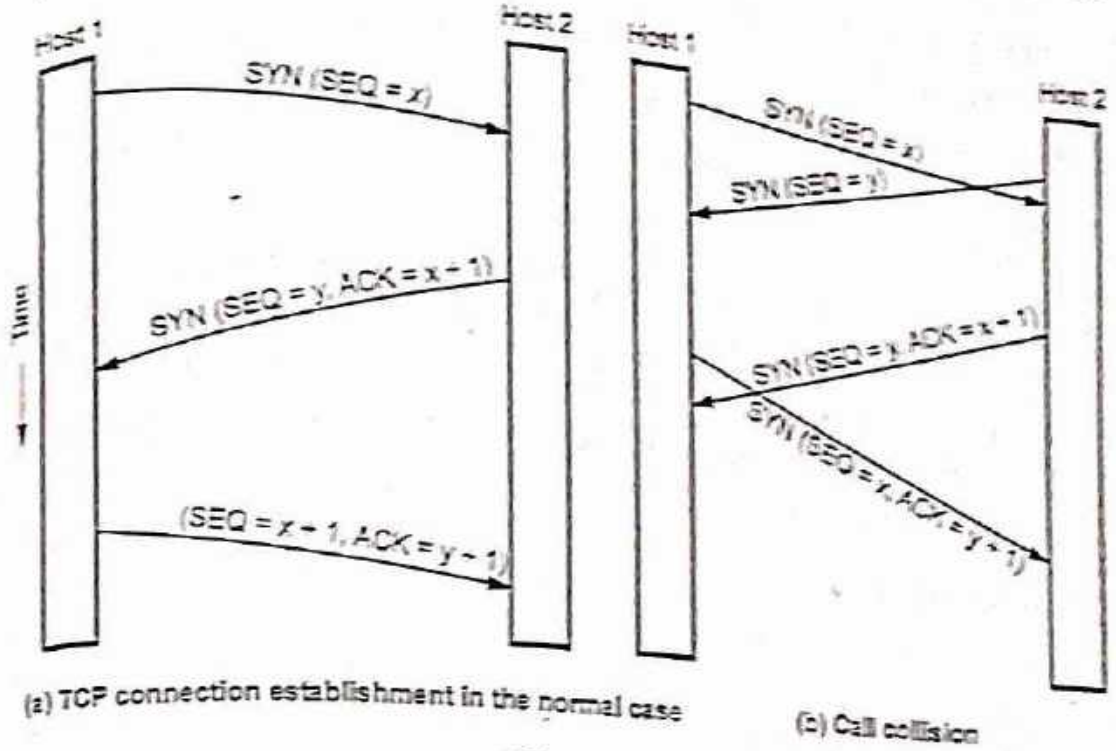
☞ [SPPU : June-22, Marks 9]

OR Explain the three way handshake algorithm for TCP connection establishment. ☞ [SPPU : May-19, April-18, In Sem, Marks 4]

Ans. : TCP Connection Establishment

- Connection establishment in a TCP session is initialized through a three-way handshake. To establish the connection, one side (server) passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, either specifying a specific source.
- Other side (client) executes a CONNECT primitive specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data.

• Fig. Q.4.1 shows the TCP connection establishment in the normal case and call collision.



(a) TCP connection establishment in the normal case (b) Call collision

Fig. Q.4.1

- A connection is established using a three-way handshake.
- The transmitter sends Connection Request (seq = x) to start a connection with transmitter message id x.
- The receiver replies Connection Accepted (seq = y, ACK = x+1), to acknowledge x and establish for its messages the identity y.
- Finally the transmitter confirms the connection with Connection Accepted (seq = x+1, ACK = y+1) to confirm its own identifier x and accept the receiver's identifier y.
- If the receiver wanted to reject x, it would send Reject(ACK = x).
- If the transmitter wanted to reject y it would send Reject(ACK = y).
- As part of the handshake the transmitter and receiver specify their MSS (Maximum Segment Size) that is the maximum size of a segment they can accept. A typical value for MSS is 1460.
- TCP connections are full duplex. The steps required establishing and release connections can be represented in a finite state machine.

Problem regarding 2-way handshake

- The only real problem with a 2-way handshake is that duplicate packets from a previous connection between the two nodes might still be floating on the network. After a SYN has been sent to the responder, it might receive a duplicate packet of a previous connection and it would regard it as a packet from the current connection which would be undesirable.
- Again spoofing is another issue of concern if a two way handshake is used. Suppose there is a node C which sends connection request to B saying that it is A. Now B sends an ACK to A which it rejects and asks B to close connection. Between these two events C can send a lot of packets which will be delivered to the application.

Three-way handshake

- The three-way handshake is the procedure used to establish a connection. This procedure normally is initiated by one TCP and responded to by another TCP.
- The three-way handshake involves the exchange of three messages between the client and the server.
- The procedure also works if two TCP simultaneously initiate the procedure. When simultaneous attempt occurs, each TCP receives a "SYN" segment which carries no acknowledgment after it has sent a "SYN". Of course, the arrival of an old duplicate "SYN" segment can potentially make it appear, to the recipient that a simultaneous connection initiation is in progress. Proper use of "reset" segments can disambiguate these cases.
- The three-way handshake reduces the possibility of false connections. It is the implementation of a trade-off between memory and messages to provide information for this checking.
- Fig. Q.4.2 shows the three way handshake scenario for establishing a connection.

Normal Operation

- Host 1 select a sequence number, 'x' and sends a CONNECTION REQUEST TPDU containing it to Host 2. Host 2 replies with an ACK TPDU acknowledging 'x' and announcing its own initial sequence number 'y'.
- Host 1 acknowledges Host 2's choice of an initial sequence number in the first data TPDU that it sends.
- This is shown in Fig. Q.4.2 (a).

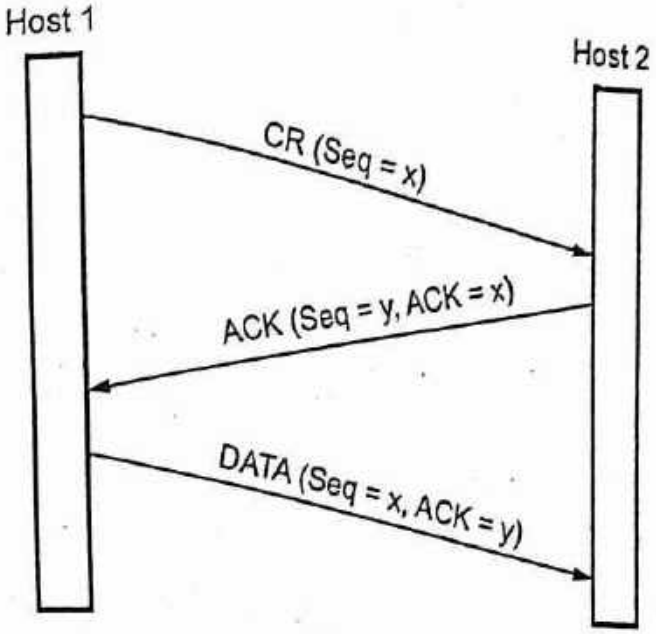


Fig. Q.4.2 (a) Normal operation

Old Duplicate

- The first TPDU is a delayed duplicate CONNECTION REQUEST from an old connection. This TPDU arrives at Host 2 without Host 1's knowledge.
- Host 2 sends ACK TPDU to Host 1 and ask for verification.
- When Host 1 rejects Host 2's attempt to establish a connection, Host 2 realizes that it was tricked by a delayed duplicate and abandons the connection.
- So, the delay duplicate does no damage.
- For this, refer Fig. Q.4.2 (b).

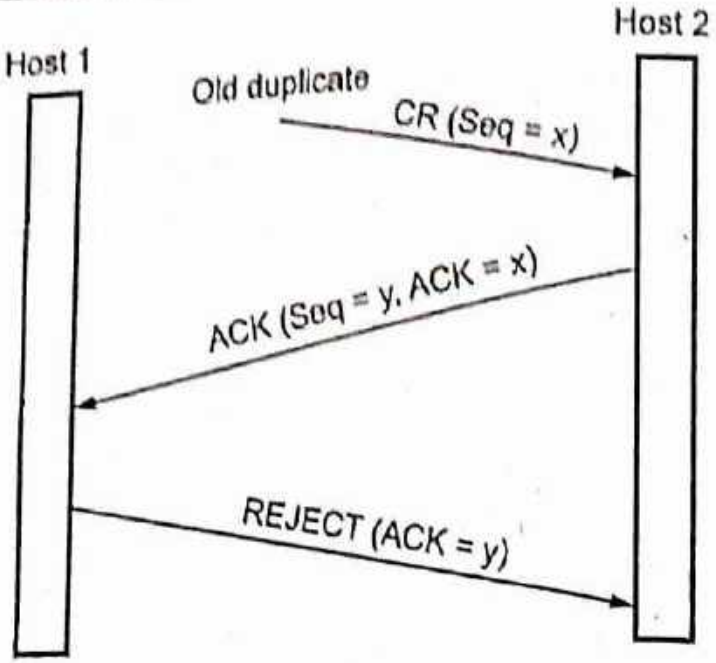


Fig. Q.4.2 (b) Old duplicate CR

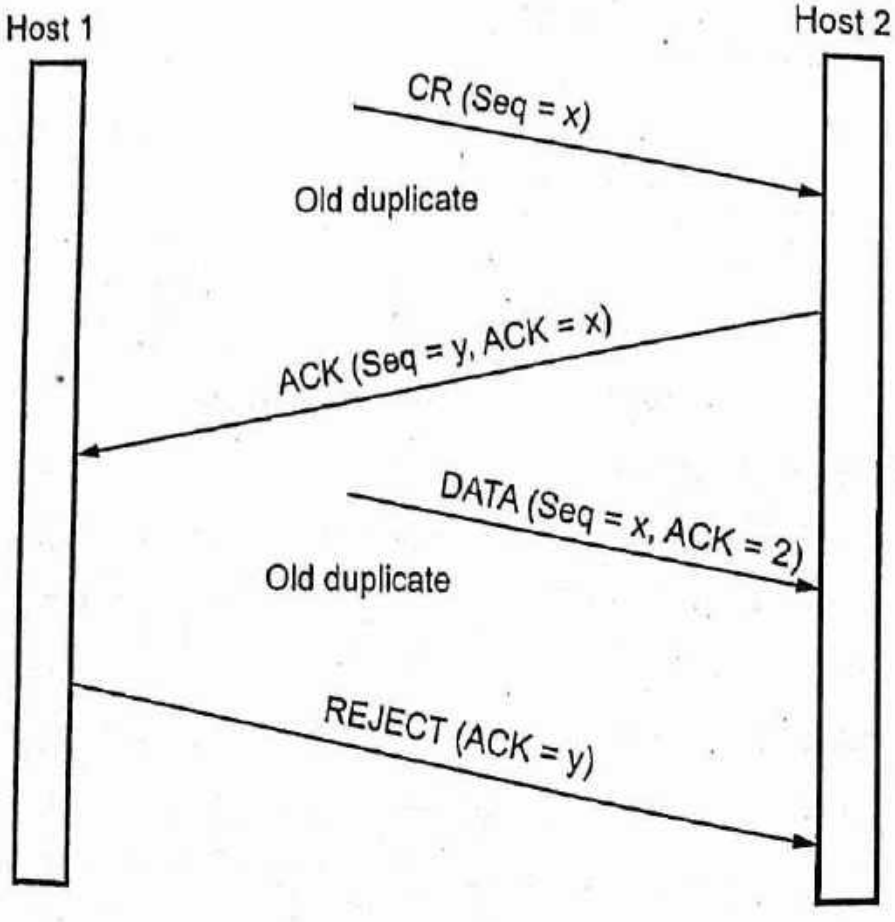


Fig. Q.4.2 (c) Duplicate CR and duplicate ACK

Fig. Q.4.2 Connection establishing using three-way handshake

Duplicate CR and Duplicate ACK

- When both a delayed CONNECTION REQUEST and an ACK are floating around in the subnet.
- Host 2 gets a delayed CONNECTION REQUEST and replies to it.
- When the second delayed TPDU arrives at Host 2, the fact that 'Z' has been acknowledged rather than 'y' tells Host 2 that this, too, is an old duplicate.

TCP Connection Release

- Any of the two parties involved in exchanging data can close the connection. When connection in one direction is terminated, the other party can continue sending data in the other direction.
- Four steps are required to close the connection in both direction. Fig. Q.4.3 shows four step connection termination.

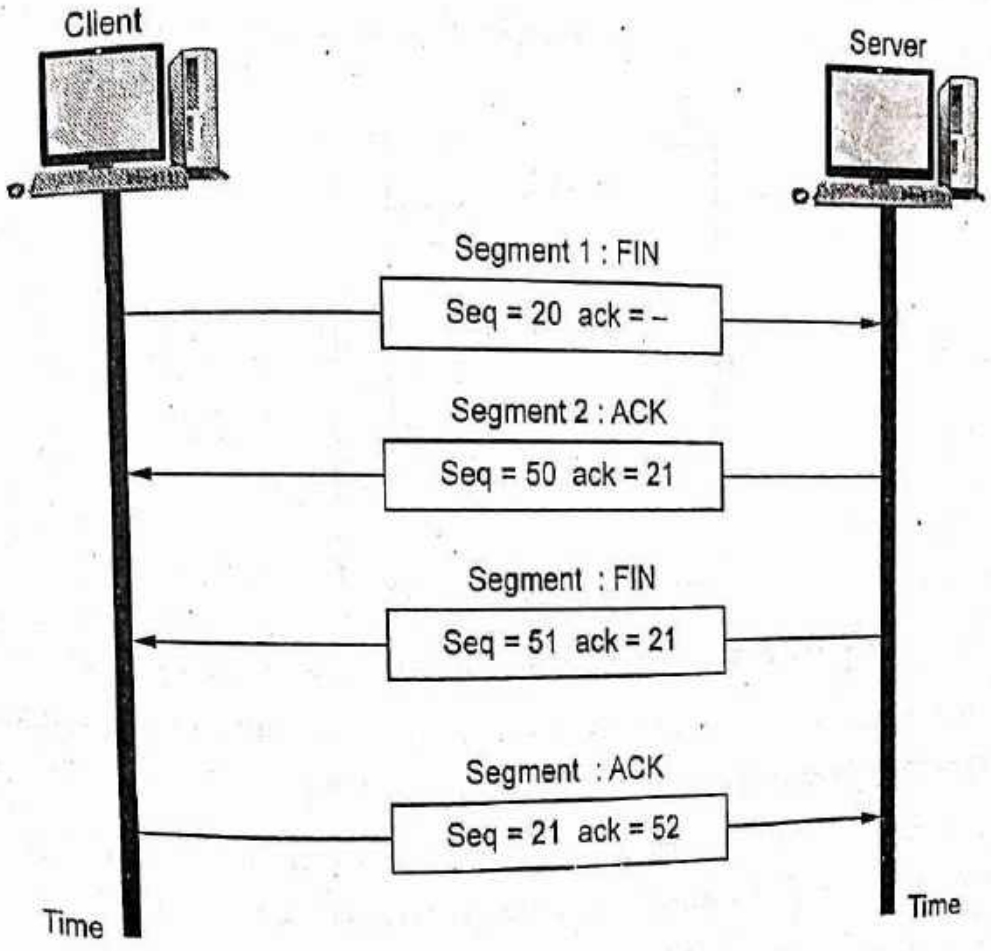


Fig. Q.4.3 Four steps connection termination

- Steps are as follows
  1. The client TCP sends the first segment, a FIN segment.
  2. The server TCP sends the second segment, an ACK segment, to confirm the receipt of the FIN segment from the client.
  3. The server TCP can continue sending data in the server client direction. When it does not have any more data to send, it sends the third segment.
  4. The client TCP sends the fourth segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server.
- Connection release is easier than connection establishing. Connection releases are of two types : Symmetric release and Asymmetric release.
- Asymmetric release is abrupt and may result in data loss. One way to avoid data loss is to use symmetric release, in which each direction is released independently of the other one.
- Fig. Q.4.4 shows the abrupt disconnection with loss of data.

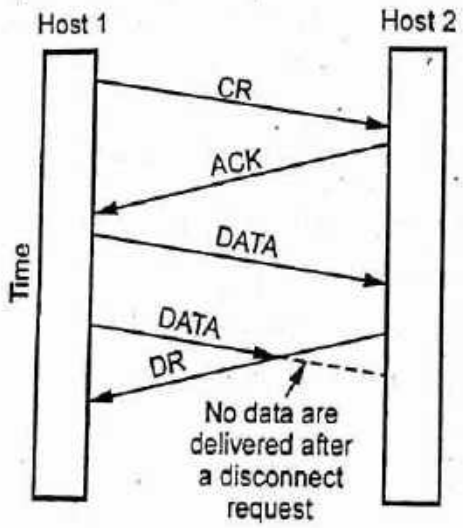


Fig. Q.4.4 Abrupt disconnection with loss of data

- After connection is established, Host 1 sends a TPDU that arrives properly at Host 2. Then Host 1 sends another TPDU.
- Unfortunately, Host 2 issues a DISCONNECT before the second TPDU arrives. The result is that the connection is released and data are lost.
- A more sophisticated release protocol is required to avoid data loss.

says:"I am done. Are you done too ?"

If responds: ''I am done too. Goodbye.''

This way does not always work.

- One way to avoid data loss is to use symmetric release, in which each direction is released independently of the other one.

Two army problem

- A white army is encamped in a valley.
- On both of the surrounding hillsides are blue armies.
- The white army is larger than either of the blue armies alone, but together they are larger than the white army.
- If either blue army attacks by itself, it will be defeated, but if the two blue armies attack simultaneously, they will be victorious.
- The communication medium between the two blue armies is to send messengers on foot down into the valley, where they might be captured and the message lost.
- Fig. Q.4.5 shows the two army problem.

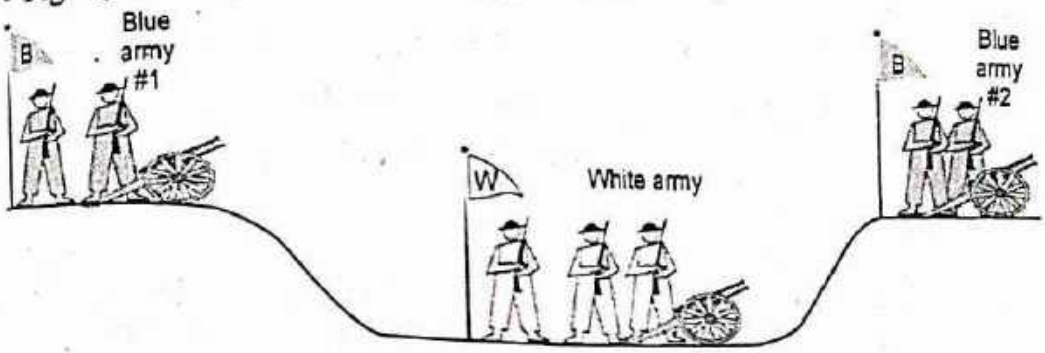


Fig. Q.4.5 Two army problem

- The question is, does a protocol exist that allows the blue armies to win ?
- The answer is there is **NO** such protocol exists.
- Just substitute ''disconnect'' for ''attack''. If neither side is prepared to disconnect until it is convinced that the other side is prepared to disconnect too, the disconnection will never happen.
- In practice, one is usually prepared to take more risks when releasing connections than attacking white armies, so the situation is not entirely hopeless.

- Fig. Q.4.6 shows four protocol scenarios for releasing a connection.

a) Normal case of three way handshake

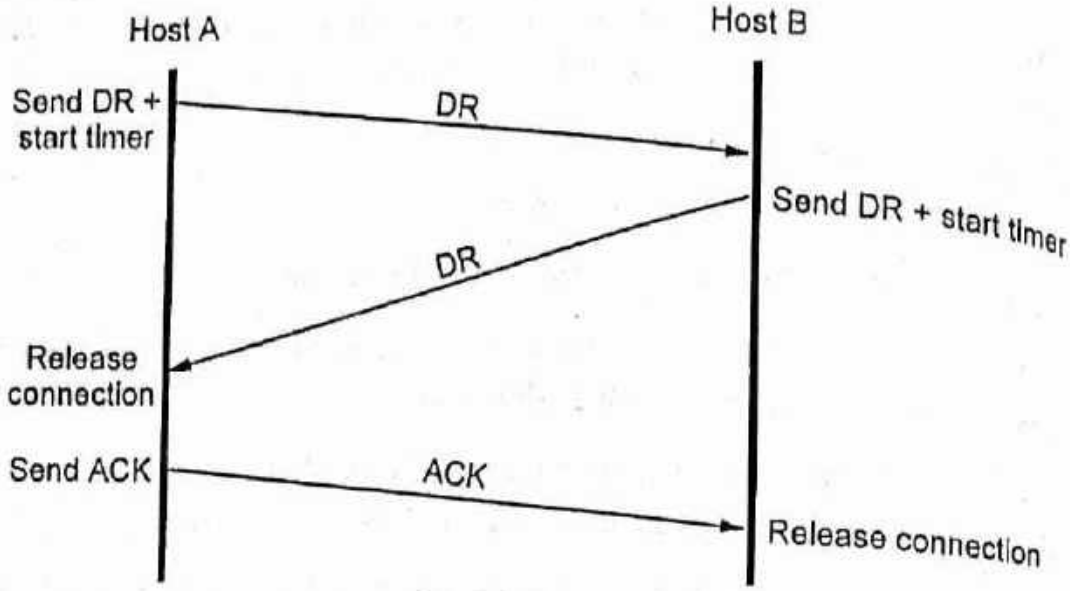


Fig. Q.4.6 (a) Releasing connection

- One of the user sends a DR (DISCONNECTION REQUEST) TPDU to initiate the connection release. When it arrives, the receipent sends back and DR TPDU and start a timer. When this DR arrives, the original sender sends back an ACK TPDU and releases the connection. Finally, when the ACK TPDU arrives, the receiver also releases the connection.

b) Final ACK lost

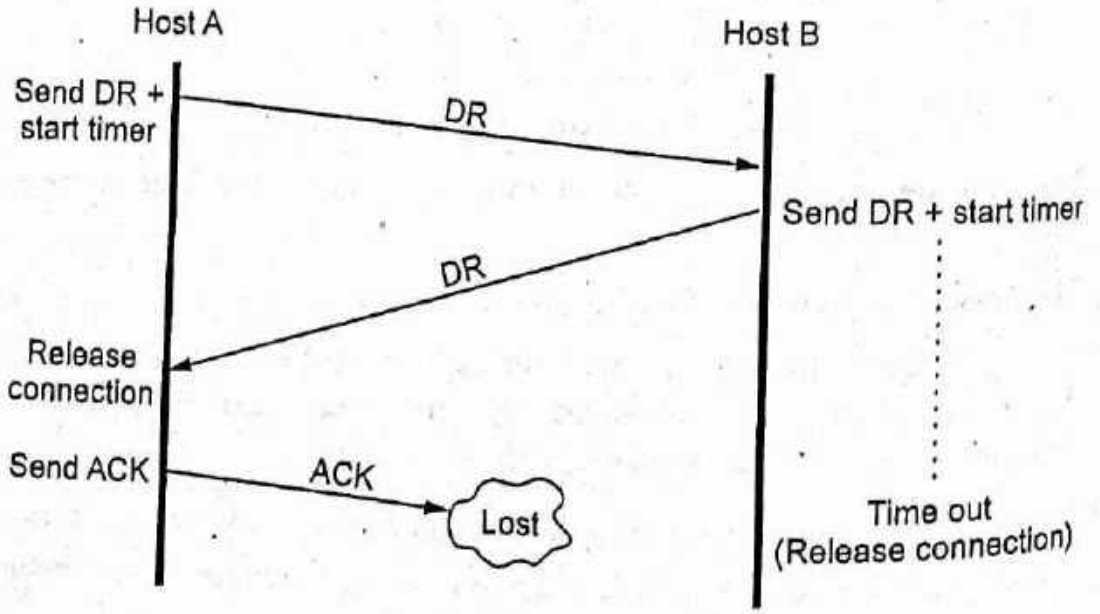


Fig. Q.4.6 (b) Releasing connection

- If the final ACK TPDU is lost, the situation is saved by the timer. When the timer expires, the connection is released anyway.

c) Response lost

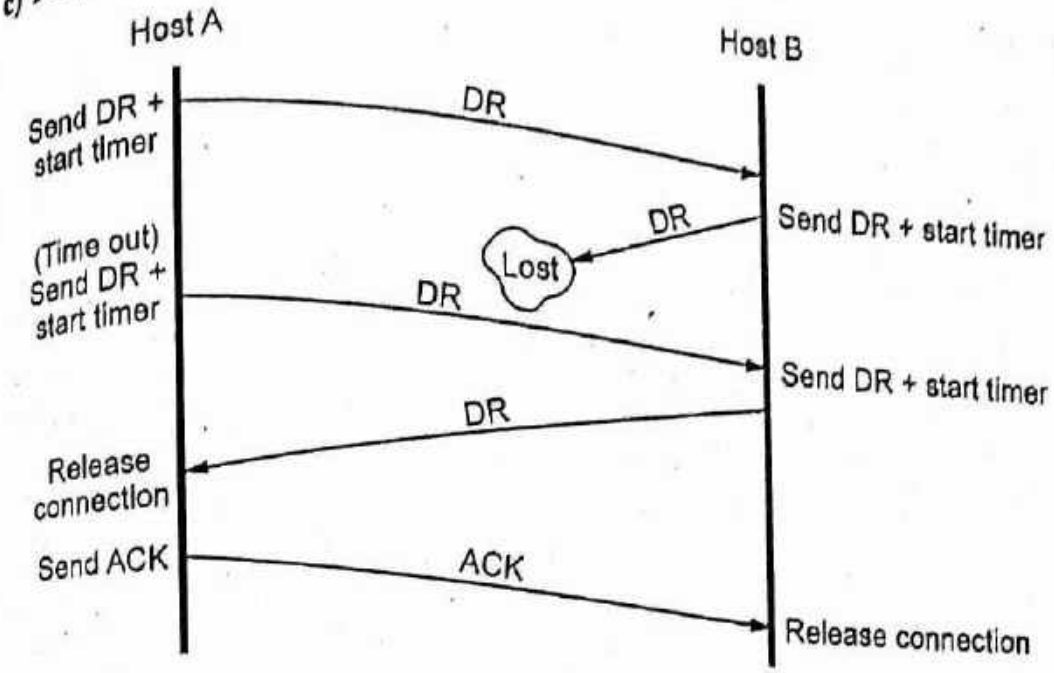


Fig. Q.4.6 (c) Releasing connection

- If the second DR lost then the user initiating the disconnection will not receive the expected response, will time out. The second time no TPDU are lost and all TPDUs are delivered correctly and on time.

d) Response lost and subsequent DR lost

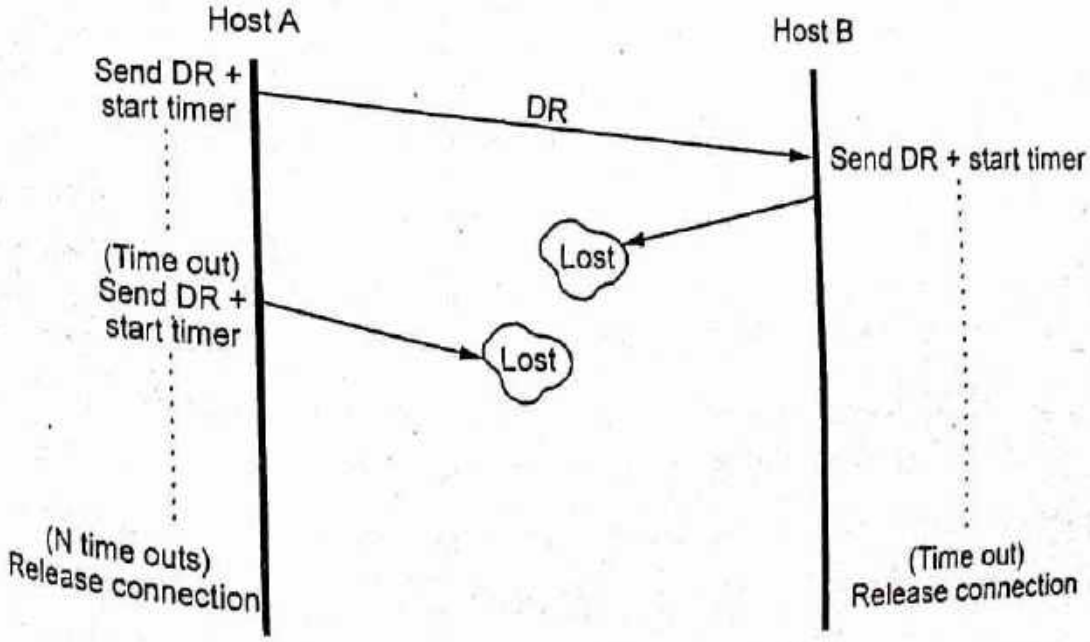


Fig. Q.4.6 (d) Releasing connection

Q.5 How Nagle algorithm helps in TCP transmission policy ? Explain the Clark's solution to overcome the silly window syndrome.

☞ [SPPU : April-18, In Sem, Marks 4, May-19, Marks 6]

Ans. : • Fig. Q.5.1 shows window management in TCP.

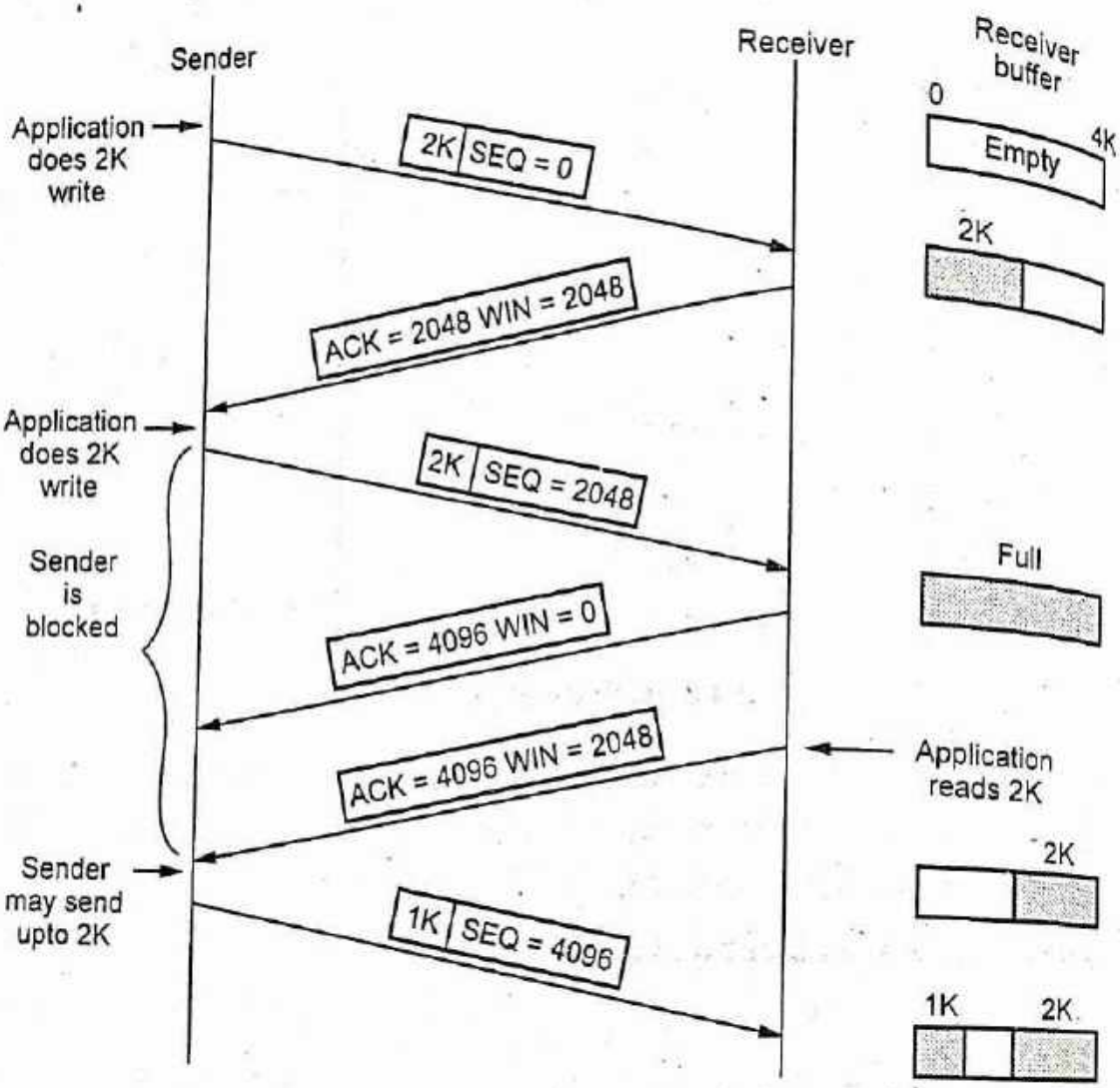


Fig. Q.5.1 Window management in TCP

- Let us assume that receiver buffer size is 4096-byte.
- If the sender transmits a 2048-byte segment that is correctly received, the receiver will acknowledge the segment.
- 2048 bytes of buffer space is only available and it will advertise a window of 2048 starting at the next byte expected.
- Again sender transmit one more 2048 bytes, which are acknowledged, but the advertised window size 0 (zero).

- Sender must stop until the application process has removed some data from the buffer.
- When the window is 0, the sender may not normally send segments because of two reasons :
  1. Urgent data may be sent.
  2. Sender may send a 1-byte segment to make the receiver reannounce the next byte excepted and window size.

Q.6 Explain different timers used in TCP.

☞ [SPPU : May-18, Dec.-18, Marks 4]

Or Why three timers are required in TCP timer management.

☞ [SPPU : Dec.-16, End Sem, Marks 6]

Ans. : • TCP manages four different timers for each connection.

a) A **retransmission timer** is used when excepting an acknowledgement from the other end.

b) A **persist timer** keeps window size information flowing even if the other end closes its receiver window.

c) A **keep alive timer** detects when the other end on an otherwise idle connection crashes.

d) A 2 **maximum segment lifetime** (2 MSL) timer measures the time a connection has been in the TIME_WAIT state.

- Fundamental to TCP timeout and retransmission is the measurement of the Round-Trip Time (RTT) experienced on a given connection. The TCP must measure the RTT between sending byte with a particular sequence number and receiving an acknowledgement that covers that sequence number. For each connection, TCP maintains a variable RTT, that is the best current estimate of the round-trip time to the destination. When a segment is sent, a timer is started, both to see how long the acknowledgement takes and to trigger a retransmission if it takes too long.
- If the acknowledgement get back before the timer expires, TCP measures how long the acknowledgement took i.e. M. The original TCP specification had TCP update a smoothed RTT estimator (R) using low-pass filter.

$$R \leftarrow \alpha R + (1-\alpha) M$$

where α is a smoothing factor with a recommended value 0.9. This smoothed RTT is updated every time when a new measurement is made. For given this smoothed estimator, which changes as the RTT changes, the retransmission timeout value (RTO) be set to

$$RTO = R\beta$$

where β = Delay variance factor with a recommended value 2.

- Unnecessary retransmission add to the network load, when the network is already loaded. Calculating the RTO based on both the mean and variance provide much better response to wide fluctuation in the round-trip time, than just calculating the RTO as a constant multiple of the mean. As described by Jacobson the mean deviation is a good approximation to the standard deviation, but easier to compute. This leads to the following equations that are applied to each RTT measurement M.

$$E_{rr} = M - A$$

$$A \leftarrow A + g E_{rr}$$

$$D \leftarrow D + h(|E_{rr}| - D)$$

$$RTO = A + 4D$$

where A = Smoothed RTT (estimator of average)

D = Smoothed mean deviation

E_{rr} = Difference between the measured value just obtained and the current RTT and estimator.

g = Gain

h = Gain of deviation

- Both A and D are used to calculate the next Retransmission Time Out (RTO). The gain (g) is for the average and is set to 0.125 and h is set to 0.25. The larger gain for the deviation makes the RTO go up faster when the RTT changes.

a) Karn's algorithm :

- A problem occurs when a packet is retransmitted. If the packet is retransmitted, a timeout occurs, the RTO is backed off. The packet is

retransmitted with the longer RTO and an acknowledgement is received. The received acknowledgement is whether the first transmission or the second. This is called the retransmission ambiguity problem.

- Karn's algorithm specify that when a timeout and retransmission occur, we cannot update the RTT estimator when the acknowledgement for the retransmitted data finally arrives. Since the data was retransmitted, and the exponential back off has been applied to the RTO, we reuse this backed off RTO for the next transmission. Do not calculate a new RTO until an acknowledgement is received for a segment that was not retransmitted.

Q.7 What is silly window syndrome ? How to overcome it ?

☞ [SPPU : April-18, In Sem, Marks 4]

Ans. :

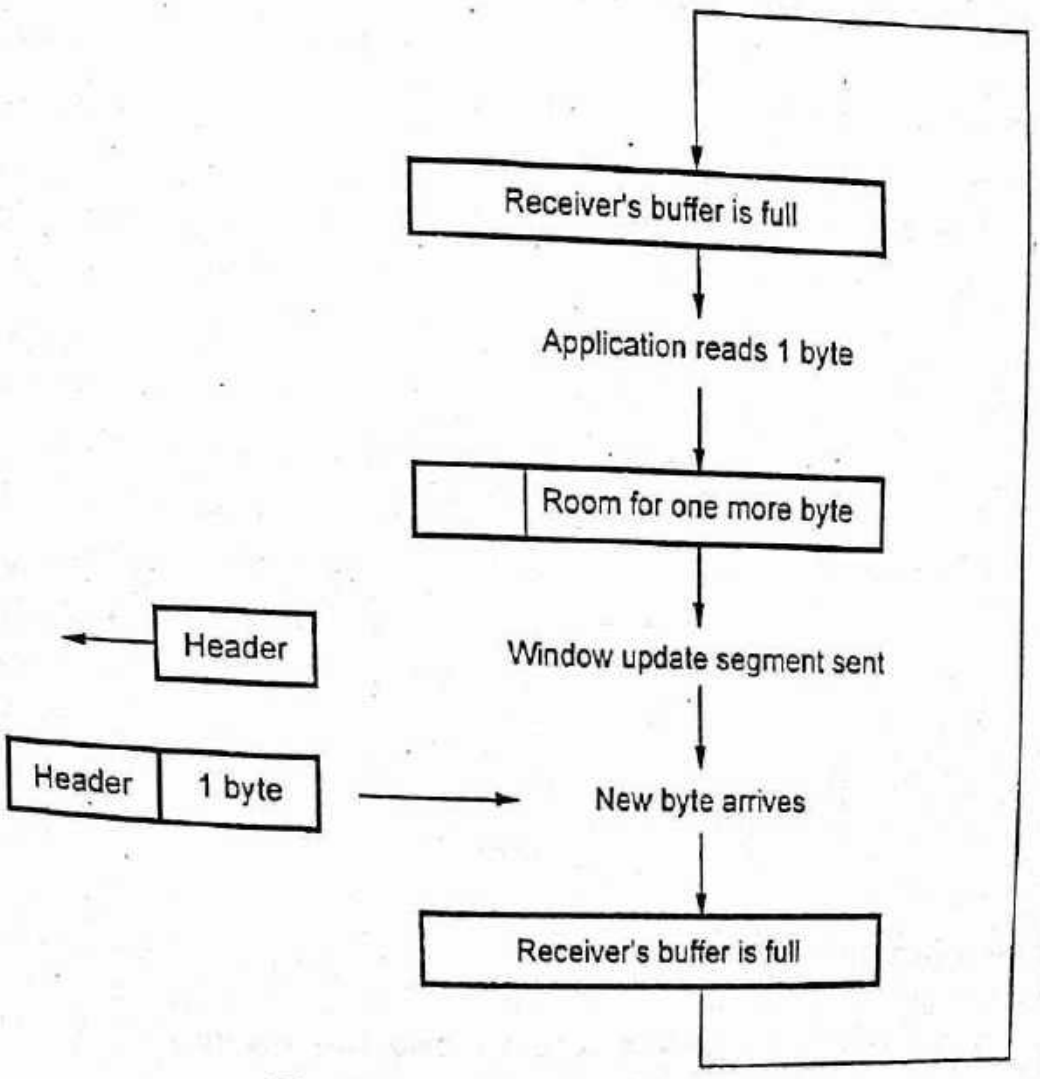


Fig. Q.7.1 Silly window syndrome

- When large block of data is passed from sender but the receiver reads data one byte at a time. Receiving side, the TCP buffer is full and the sender know the condition. The interactive application reads one character from the TCP stream.
- Receiving TCP tells to the sender to send the only 1 byte. Sender send 1 byte. Now buffer is full and receiver send acknowledgement the 1-byte segment and set the window 0. This operation is continuous. Fig. Q.7.1 shows these steps.
- Nagle algorithm and Clark's solution to the silly window syndrome are complementary. Clark solution is to prevent the receiver from sending a window update for 1 byte. Instead it is forced to wait until it has a decent amount of space available.

Q.8 Explain in detail how TCP provides flow control.

☞ [SPPU : May-17, End Sem, Marks 4]

Ans. : • TCP interactive data flow uses Rlogin application. In TCP/IP the each interactive keystroke normally generates a data packet. The keystrokes are sent from the client to the server 1 byte at a time. Rlogin has the remote system; each characters that the client type is displayed on the other side (server).

• Fig. Q.8.1 shows the flow of data.

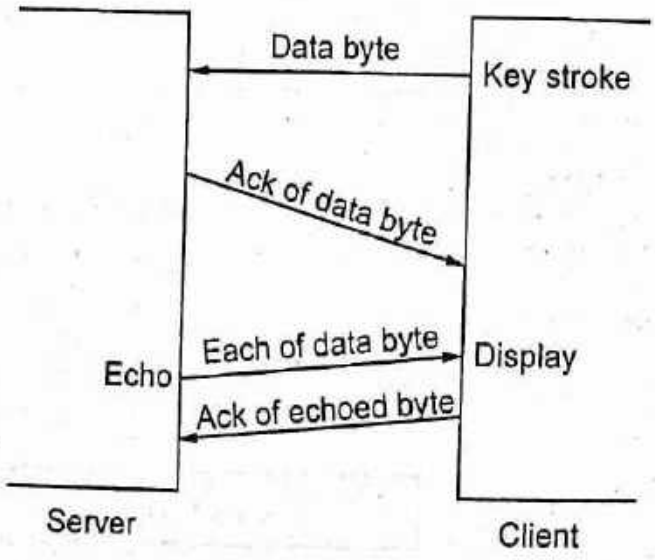


Fig. Q.8.1 Remote echo of interactive keystroke

- The TCP acknowledgements operates as follows.
- Line 1 sends the data byte with the sequence number 0. Line 2 ACKs this by setting the acknowledgement sequence number to 1, the sequence number of the last successfully received byte plus one. This is also called the sequence number of the next excepted byte.
- Line 2 also sends the data byte with a sequence number of 1 from the server to the client. This is ACKed by the client in line 3 by setting the acknowledgement sequence number to 2. Normally TCP does not send an ACK the instant it receives data. Instead, it delays the ACK, hoping to have data going in the same direction as the ACK, so the ACK can be sent alongwith the data. TCP will delay an ACK upto 200 ms to see if there is data to send with the ACK.

NAGLE Algorithm

- One byte at a time normally flows from the client to the server across a Rlogin connection. This generates 41-byte packet 20 bytes for the IP header and 20 bytes for TCP header and 1 byte of data. These small packets called as tinygrams. These tinygrams can add to congestion on WAN.
- Most LANs are not congested because tinygrams are not a problem on LANs. To solve the problem of congestion of WAN, the Nagle algorithm is used.
- The Nagle algorithm say that when TCP connection has outstanding data that has not yet been acknowledged, small segments cannot be sent until the outstanding data is acknowledged. Instead, small amounts of data are collected by TCP and sent in a single segment when the acknowledgement arrives.
- Nagle algorithm is self- clocking. The faster the ACKs come back, the faster the data is sent. But on a slow WAN, where it is desired to reduce the number of tinygrams, fewer segment are sent. Nagles algorithm is widely used by TCP implementations, but there are times when it is better to disable it. The example is the X window system server. Mouse movements must be delivered without delay to provide

real time feedback for interactive users doing certain operations for bulk data flow.

- TCP uses a different form of flow control called a sliding window protocol. This sliding window protocol working is same as Data link layer sliding window protocol.

6.3 : Congestion Control

Q.9 Explain choke packets and hop by hop choke packets.

☞ [SPPU : May-16, End Sem, Marks 6]

Ans. : • Closed loop control try to alleviate congestion after it happens.

End-to-End versus Hop-by-Hop

- In **end-to-end closed loop control**, the feedback information about state of the network is propagated back to the source that can regulate the packet flow rate. Fig. Q.9.1 shows end-to-end closed loop control.

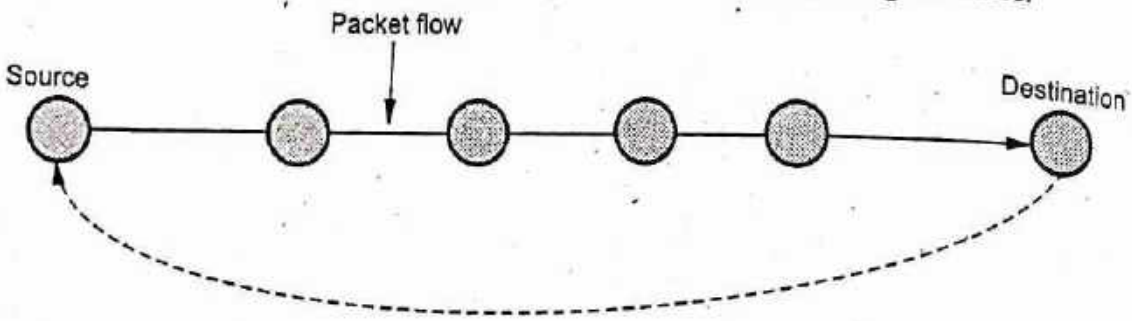


Fig. Q.9.1 End-to-end closed loop control

- The feedback information may be forwarded directly by a node that detects congestion, or it may be forwarded to the destination first which then relays the information to the source.
- With hop-by-hop closed loop control, the state of the network is propagated to the upstream node. Fig. Q.9.1 shows hop-by-hop control.
- When a node detects congestion on its outgoing link, it can tell its upstream neighbor to slow down its transmission rate.

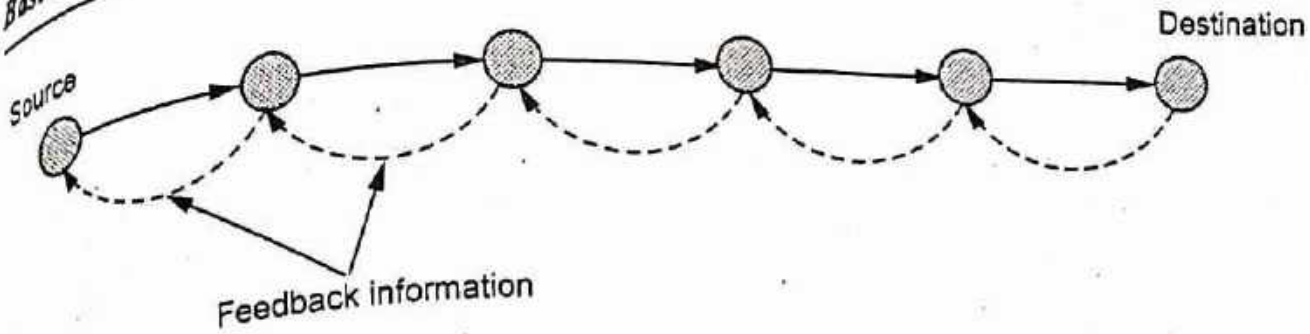
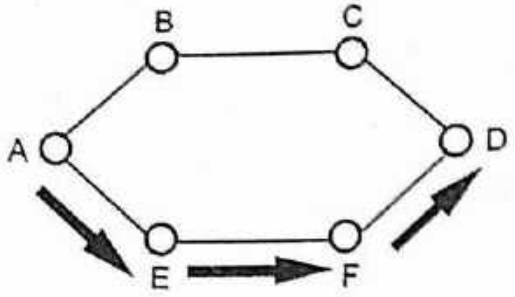


Fig. Q.9.2 Hop-by-hop loop control

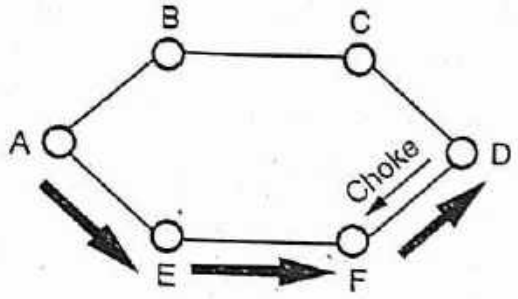
Choke Packets

- Another mechanism for congestion control is by using choke packets. This choke packet will have the effect of stopping or slowing down the rate of transmission from sources and hence limit the total number of packets in the networks. This approach requires additional traffic on the network during a period of congestion. This can be applicable to both virtual circuit and datagram subnets.
- When line utilization increases above some specific value called threshold, the line enters a 'alarming' situation. Each newly arriving packet is checked to see if its output line is in alarming state. If so, the router sends the said choke packet back to the source. This choke packet contains the destination address, so the source will not generate any more packets along the path.
- The traffic is reduced by adjusting parameters window size or leaky bucket output rate. Typically, the first choke packet causes the data rate to 50 % of its previous value the choke packet reduces the traffic to 25 % and so on.
- Congestion control using choke packets can be done by two ways. In first type the choke packet affects only source and in the second type the choke packet affects each hop it passes through. Fig. Q.9.3 shows choke packet that affects only the source.
- Fig. Q.9.3 shows a choke packet that affects each hop it passes through.
  a) A subnet with six nodes A, B, C, D, E and F is shown in Fig. Q.9.3 (a). Here the source node is A and destination node is D.

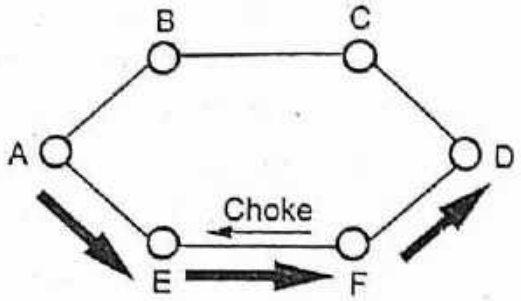


(a)

b) When link utilization increased above its threshold, destination node D starts sending choke packets towards source node A.



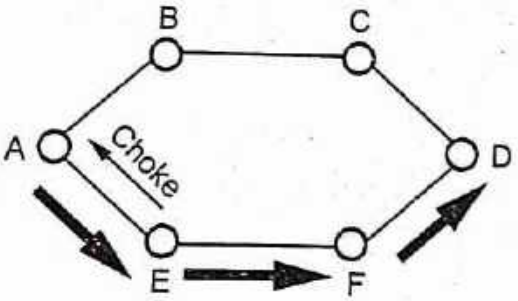
(b)



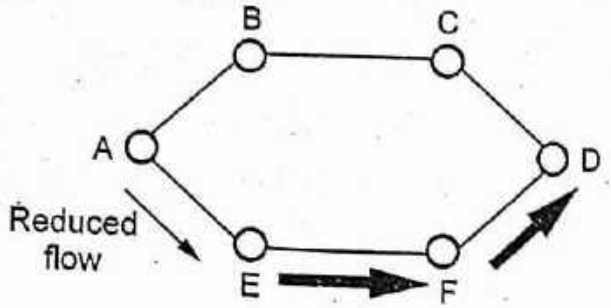
(c)

c) The choke packets travels through the shortest or same path as that of packets.

d) The choke packet reaches to the source node A.



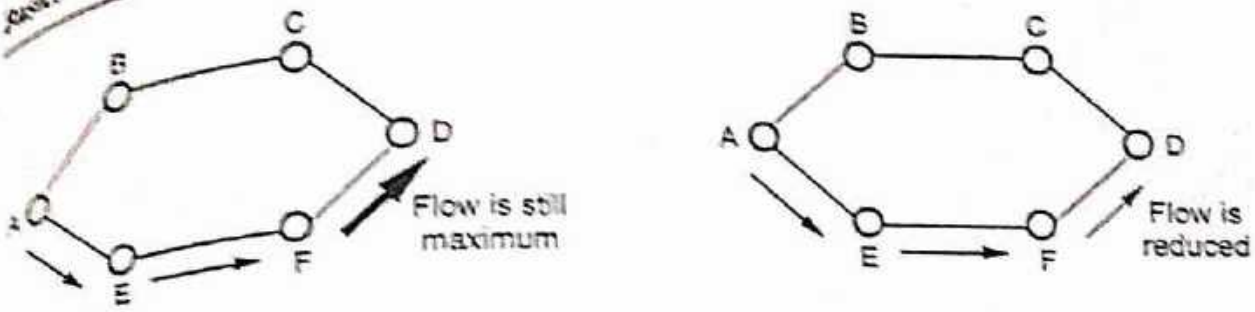
(d)



(e)

e) After receiving first chock packet source node A reduces its flow towards destination.

f) The reduced packet flow follows the same reversed path i.e. the path of choke packets through various nodes.

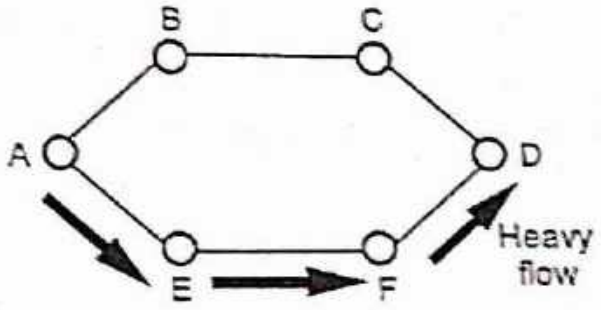


(f) (g)

Fig. Q.9.3 A choke packet that affects only the source

g) The reduced flow reaches to destination node D.

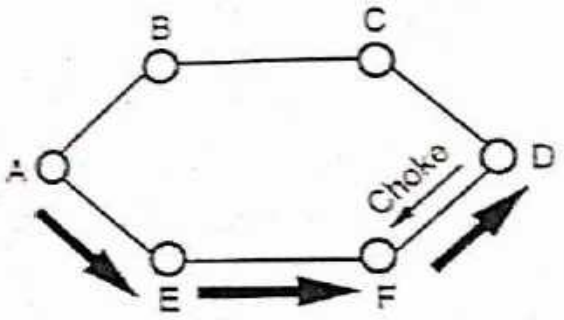
Fig. Q.9.4 shows a choke packet that affects each hop it passes through.



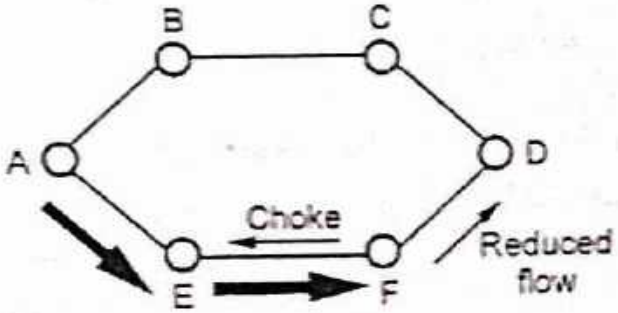
(a)

a) For the same subnet having nodes A, B, C, D, E and F source node and destination node D.

b) When link utilization increased above its threshold destination node D starts sending choke packets towards source node A.



(b)



(c)

c) The chock packets follows the exactly reversed path of traffic flowing packets. Here the chock packet reaches to node F. Immediately after reaching choke packet at node F, the traffic flow towards node D reduces.

d) As choke packet crosses node E, the traffic flow between nodes E, F, and F, D is reduced.

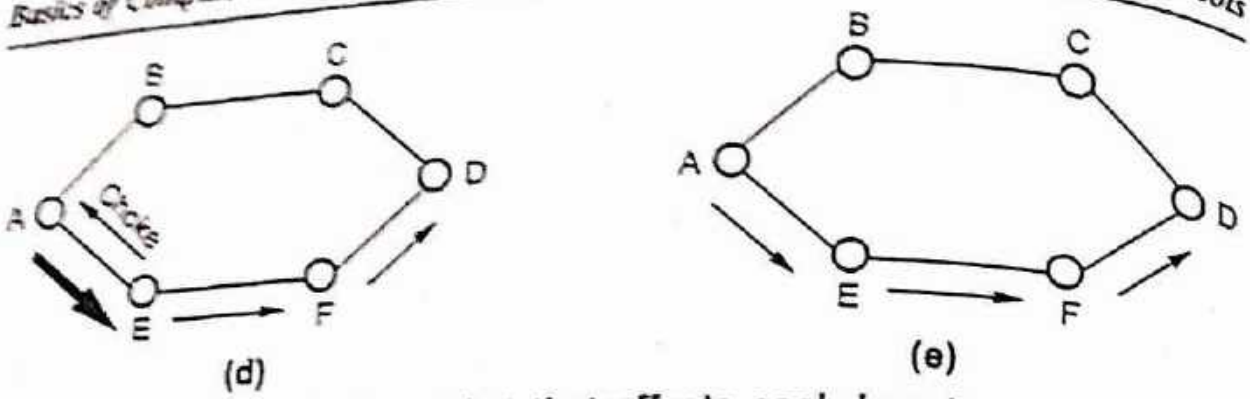


Fig. Q.9.4 A choke packet that affects each hop it passes

e) After reaching choke packet to source node A, the traffic flow between node A and node E and hence up to the destination node D is reduced.

Hop-by-hop choke packets

- Over long distances or at high speeds, the choke packets are not very effective.
- A more efficient way is to send choke packets hop-by-hop.
- A congested node would again generate a choke pocket, but each hop would be needed to reduce its transmission even before the choke packet arrives at the source.

Q.10 What is congestion control ? Explain leaky bucket and token bucket algorithm ?

☞ [SPPU : April-19, Marks 5]

Or What is the purpose of leaky bucket and token bucket algorithms ? Describe working of token bucket algorithm with reference to CBR, VBR and bursty traffic.

☞ [SPPU : Dec.-18, Marks 6, June-22, Marks 9]

Or Explain leaky bucket and token bucket algorithm.

☞ [SPPU : May-18, Marks 6]

Ans. : Congestion control : Congestion control is a process of maintaining the number of packets in a network below a certain level at which performance falls off. Congestion control makes sure that subnet is able to carry the offered traffic. So congestion control is different process than flow control.

Leaky Bucket Algorithm

Traffic shaping

- Traffic shaping is about regulating the average rate of data transmission.
- Traffic shaping smooths out the traffic on the server, rather than on the client side.
- Monitoring a traffic flow is called traffic policing. Agreeing to a traffic shape and policing it afterward are easier with virtual circuit subnets than with datagram subnets.
- Traffic shaping is an open loop method of congestion control.
- Two types of algorithm are used for traffic shaping.

1. Leaky bucket algorithm
2. Token bucket algorithm

Leaky bucket algorithm

- Leaky bucket i.e. a bucket with a small hole in the bottom is used to store the water. The outflow from hole is at constant rate and irrespective of rate of entering water. Once the bucket is full, any additional water entering it spills over the sides and is lost.
- The same idea can be applied to packets. This is similar to a single server queueing system with constant service time.
- Each host is connected to network with a finite internal queue. The host is allowed to put one packet per second on to the network. If a packet arrives at the queue when it is full, the packet is discarded. This mechanism turn an unregulated traffic of the host regulated traffic on the network. Thus bursty traffic is smoothen and chances of congestion is reduced. Fig. Q.10.1 illustrates this algorithm.
- A leaky bucket regulator allows to control the average rate, largest burst from a source. A leaky bucket regulator has both a packet bucket and a data buffer. Packets that arrive to the regulator that cannot be sent immediately are delayed in the data buffer.

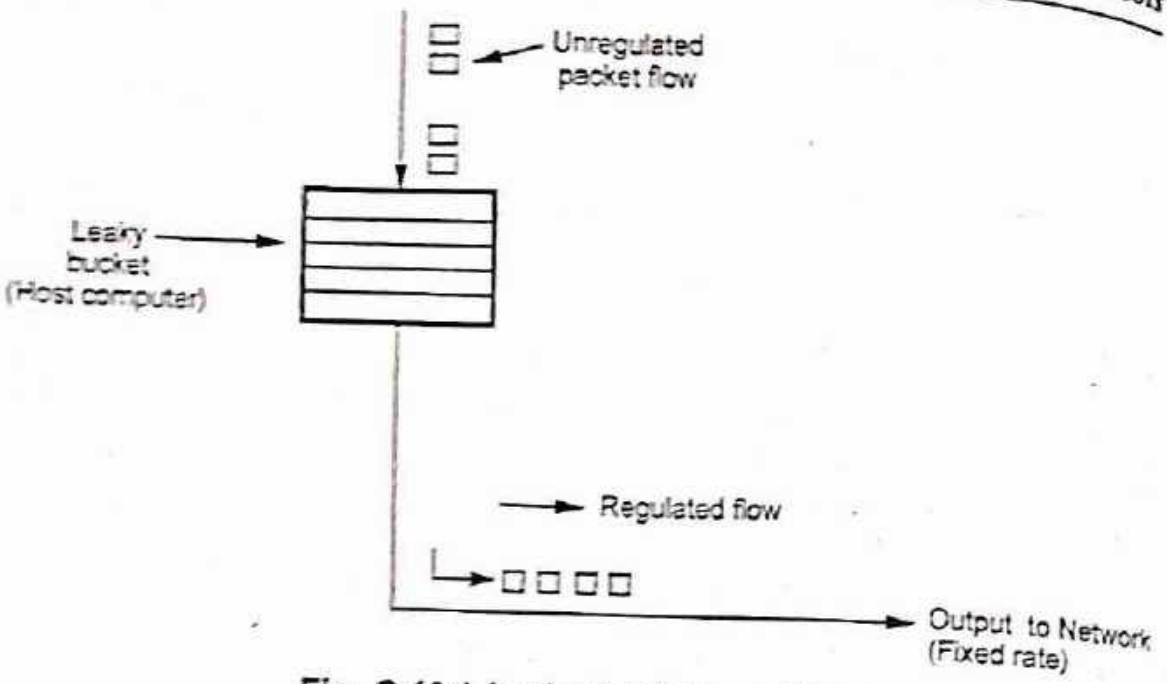


Fig. Q.10.1 Leaky bucket regulator

- The main drawback of leaky bucket algorithm is that its output pattern cannot be modified i.e. if the bursty traffic arrives the output should speed up, so that no packets will be lost.
- Fig. Q.10.2 (See Fig. Q.10.2 on next page) shows the leaky bucket algorithm that can be used to police the traffic flow.
- At the arrival of the first packet, the content of the bucket X is set to zero and the last conforming time is set to the arrival time of the first packet. The depth of the bucket is L+I where L typically depends on the traffic burstiness.

Token Bucket Algorithm

- Token bucket algorithm eliminates drawback of leaky bucket algorithm. In this, the leaky bucket holds tokens. These tokens are generated by a clock at the rate of one token for every ΔT sec. In token bucket bursts of upto n packets can be sent at once, which gives faster response to sudden bursts of input.
- The regulator collects tokens in a bucket, which fills-up at steady drip rate by packets. When a packet arrives at the regulator, the regulator sends the packet if the bucket has enough tokens. Otherwise, the packet waits either until the buckets has enough tokens. If the bucket is already fill of tokens, incoming tokens overflow and are not available to future

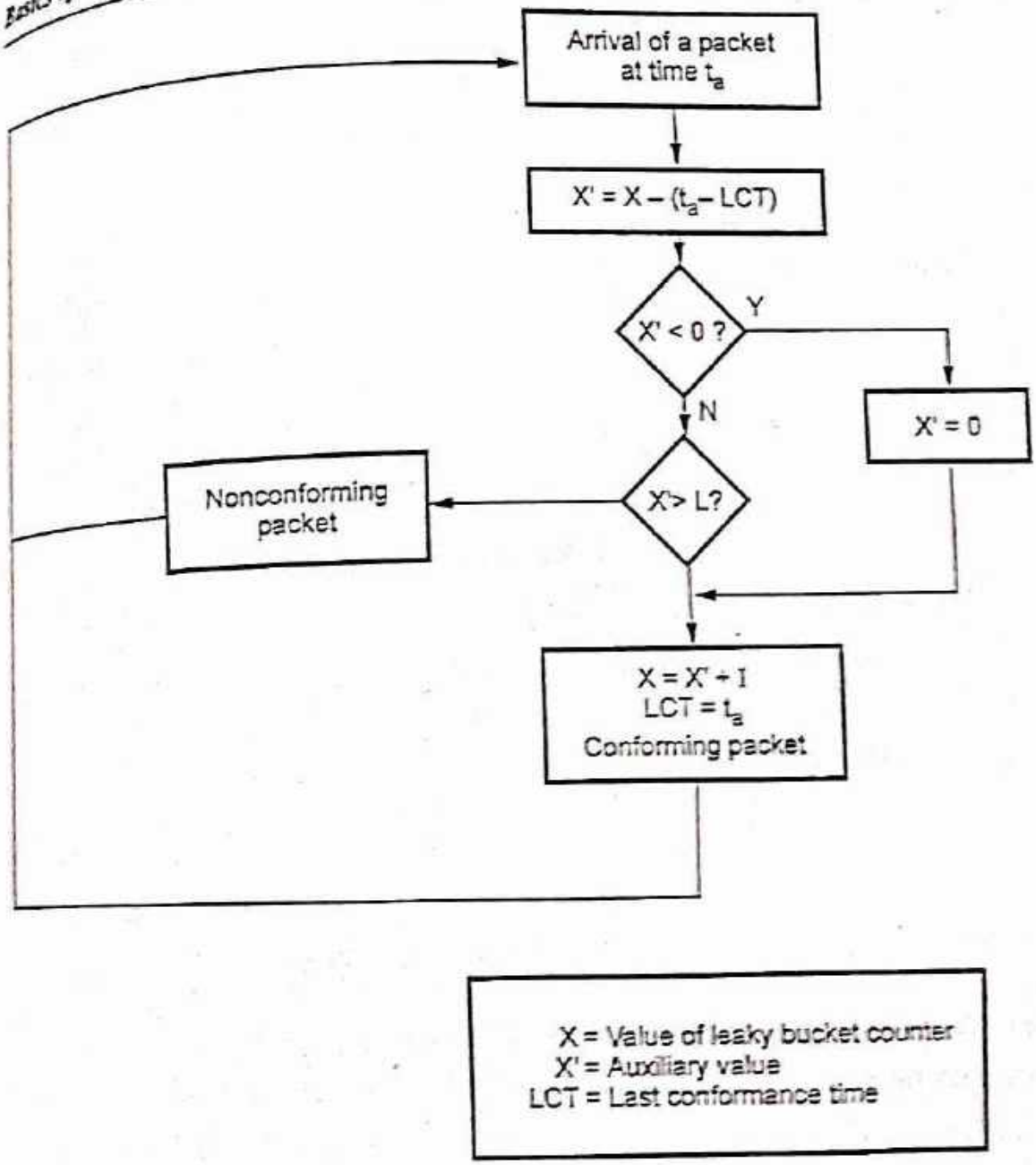


Fig. Q.10.2 Leaky bucket algorithm for policing

packets. Thus, at anytime, the largest burst a source can send into the network is roughly proportional to the size of the leaky bucket.

- The regulator delays a packet if does not have sufficient number of tokens for transmission. A counter keeps track of tokens, the counter is incremented by one every ΔT and decremented by one whenever a packet is sent. When the counter hits zero, no packets may be sent. Smoother traffic can be obtained by putting a leaky bucket after the token bucket.

• Fig. Q.10.3 illustrates token bucket regulator.

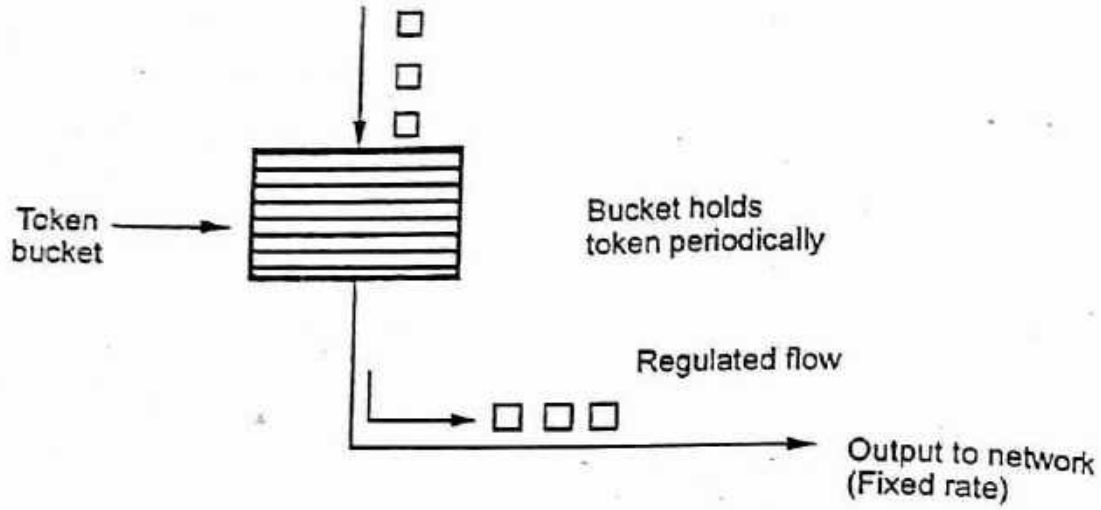


Fig. Q.10.3 Token bucket regulator

Let Token bucket capacity = C bytes

Token arrival rate = ρ bytes/sec

Maximum output rate = M bytes/sec

Then the maximum burst rate S,

$$S = \frac{C}{M-\rho}$$

6.4 : Quality of Service (QoS)

Q.11 Write a short note on quality of service parameters in transport layer. ☞ [SPPU : May-17,18, End Sem, Marks 4]

Ans. : • Quality of service (QoS) is an internetworking issue. QoS mainly defines flow characteristics and flow classes.

A] Flow Characteristics

• Four types of characteristics are attributed to a flow :

1. Bandwidth 2. Jitter 3. Delay 4. Reliability.

1. Bandwidth :

• Bandwidth is a characteristic of network. Bandwidth can be measured in hertz and in bits per seconds.

- **Bandwidth in Hertz :** Bandwidth in hertz refers to the range of frequencies in a composite signal or the range of frequencies that a transmission channel can pass.
- **Bandwidth in bps :** Bandwidth in bps refers to speed of bit transmission in a channel or link.

2. Jitter :

- Jitter is a parameter related to delay. Jitter is introduced since different packets of data encounter different delays. The data packets reaching at receiver at different times causing jitter.

3. Delay :

- Latency is also termed as delay. Latency is time required for a message to completely arrive at the destination from source. It has four components propagation time, transmission time, queuing time and processing delay.

4. Reliability :

- Loss of packet or acknowledgement is due to lack of reliability.

B] Flow Classes

- Based on the flow characteristics, we can classify flows into groups, with each group having similar levels of characteristics.

6.5 : User Datagram Protocol (UDP)

Q.12 List out key features of UDP protocol. Explain how flow control is different than congestion control in TCP ?

☞ [SPPU : June-22, Marks 9]

Or Draw and explain UDP header format.

☞ [SPPU : Oct.-14, In Sem, Marks 6]

Ans. :

- Fig. Q.12.1 (a) shows the encapsulation of a UDP datagram as an IP datagram.
- Fig. Q.12.1 (b) shows the format of the UDP header. The port number identify the sending process and the receiving process.

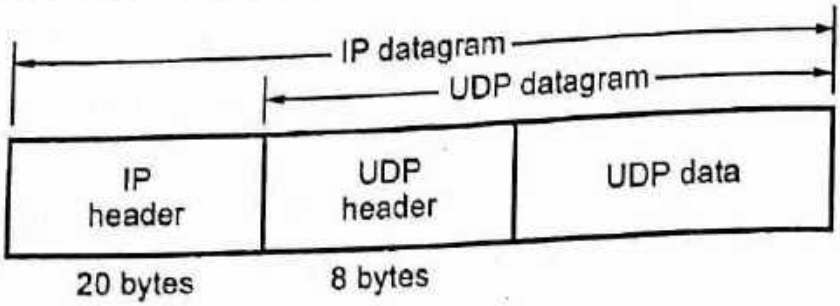


Fig. Q.12.1 (a) UDP encapsulation

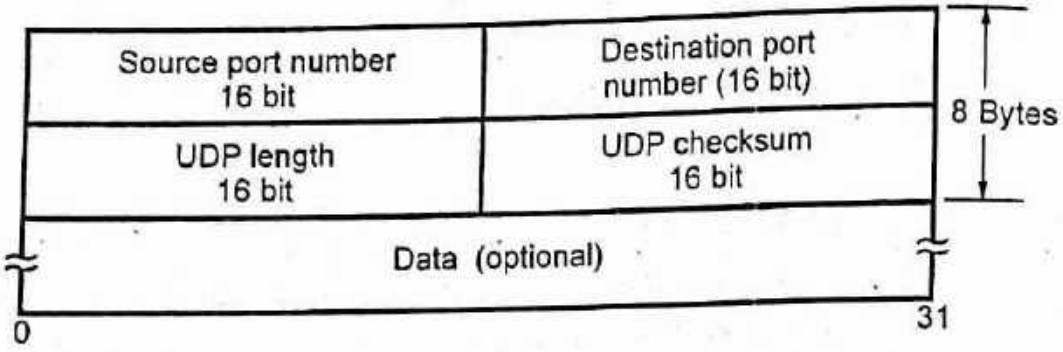


Fig. Q.12.1 (b) UDP header

- The UDP datagram contains a source port number and destination port number. Source port number identifies the port of the sending application process. The destination port number identifies the receiving process on the destination host machine.
- The UDP length field is the length of the UDP header and the UDP data in bytes. The minimum value for this field is 8 bytes.
- UDP checksum covers the UDP header and the UDP data. Both UDP and TCP include a 12 byte pseudo-header with the UDP datagram just for the checksum computation. This pseudo_header includes certain fields from the IP header. The purpose is to let UDP double check that the data has arrived at the correct destination.
- UDP checksum is end-to-end checksum. It is calculated by the sender, and then verified by receiver. It is designed to catch any modification of the UDP header or data anywhere between sender and receiver.
- Goal of the UDP checksum is to detect "errors" in transmitted segment. Function performed by sender and receiver is as follows :

Sender :

1. Treat segment contents as sequence of 16-bit integers
2. Checksum : addition (1's complement sum) of segment contents
3. Sender puts checksum value into UDP checksum field

Receiver :

1. Compute checksum of received segment
2. Check if computed checksum equals checksum field value : NO - error detected and YES - no error detected.

Why is there a UDP ?

1. No connection establishment (which can add delay)
2. Simple : no connection state at sender, receiver
3. Small segment header
4. No congestion control : UDP can blast away as fast as desired
5. Often used for streaming multimedia apps

6.6 : Socket

Q.13 What is socket ? Explain various socket primitives used in client server interaction.

☞ [SPPU : June-22, Marks 9, April-18,19, In Sem, Dec.-18, Marks 4]

Ans. : Socket : • Socket interface is a protocol independent interface to multiple transport layer primitives. In order to write applications which need to communicate with other applications.

- Socket is an abstraction that is provided to an application programmer to send or receive data to another process.
- Data can be sent to or received from another process running on the same machine or a different machine.
- It is like an endpoint of a connection. It exists on either side of connection and identified by IP Address and Port number.
- Sockets works with UNIX I/O services just like files, pipes and FIFO.
- API stands for Application Programming Interface. It is an interface to use the network. Socket API defines interface between application and transport layer.

- The API defines function calls to create, close, read and write to/from a socket.

Advantages of using socket interface

- Syntax of the API functions is independent of the protocol being used. Ex:- TCP/IP and UNIX domain protocols can be used by applications using a common set of functions.
- Gives way to better portability of applications across protocol suites.
- Hides the finer details of the protocols from application programs thereby yielding faster and bug free application development
- Sockets are referenced through socket descriptors which can be passed directly to UNIX system I/O calls. File I/O and socket I/O are exactly similar from the programmer perspective.

Sockets versus file I/O

- Working with sockets is very similar to working with files. The socket( ) and accept( ) functions both return handles (file descriptor) and reads and writes to the sockets requires the use of these handles (file descriptors).
- In Linux, sockets and file descriptors also share the same file descriptor table. That is, if you open a file and it returns a file descriptor with value say 8, and then immediately open a socket, you will be given a file descriptor with value 9 to reference that socket.
- Even though sockets and files share the same file descriptor table, they are still very different. Sockets have addresses associated with them whereas files do not; notice that this distinguishes sockets form pipes, since pipes do not have addresses with which they associate.
- You cannot randomly access a socket like you can a file with lseek( ). Sockets must be in the correct state to perform input or output.

Socket abstraction

- Socket is the basic abstraction for network communication in the socket API. Socket defines an endpoint of communication for a process.

- Operating system maintains information about the socket and its connection. Fig. Q.13.1 shows the socket and process.

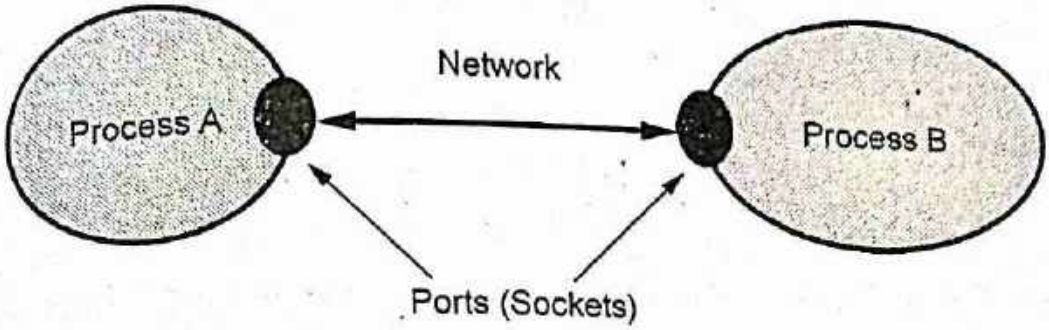


Fig. Q.13.1 Socket and process

Socket creation

int socket (int family, int type, int protocol);

Parameters :

1. family : AF_INET or PF_INET (These are the IP4 family)
2. type : SOCK_STREAM (for TCP) or SOCK_DGRAM (for UDP)
3. protocol : IPPROTO_TCP (for TCP) or IPPROTO_UDP (for UDP) or use 0

- If successful, socket ( ) returns a socket descriptor, which is an integer, and – 1 in the case of a failure.
- An example call :

```
if ((sd = socket(AF_INET, SOCK_DGRAM, 0) < 0)
{
        printf(socket() failed.);
        exit(1);
}
```

- Creating a socket is in some ways similar to opening a file. This function creates a file descriptor and returns it from the function call. You later use this file descriptor for reading, writing and using with other socket functions.

- Remember that the sockets API are generic. There must be a generic way to specify endpoint addresses. TCP/IP requires an IP address and port number for each endpoint address. Other protocol suites (families) may use other schemes.

TCP Socket

- In UNIX, whenever there is a need for IPC within the same machine, we use mechanism like signals or pipes. When we desire a communication between two applications possibly running on different machines, we need **sockets.**
- Sockets are treated as another entry in the UNIX open file table.
- Sockets provide an interface for programming networks at the transport layer.
- Network communication using Sockets is very much similar to performing file I/O. In fact, socket handle is treated like file handle.
- Socket-based communication is programming language independent.
- To the Kernel, a socket is an endpoint of communication. To an application, a socket is a file descriptor that lets the application read/write from/to the network.
- A server (program) runs on a specific computer and has a socket that is bound to a specific port. The server waits and listens to the socket for a client to make a connection request.
- To review, there are five significant steps that a program which uses TCP must take to establish and complete a connection. The server side would follow these steps :
  1. Create a socket.
  2. Listen for incoming connections from clients.
  3. Accept the client connection.
  4. Send and receive information.
  5. Close the socket when finished, terminating the conversation.

- In the case of the client, these steps are followed :

1. Create a socket.
2. Specify the address and service port of the server program.
3. Establish the connection with the server.
4. Send and receive information.
5. Close the socket when finished, terminating the conversation.

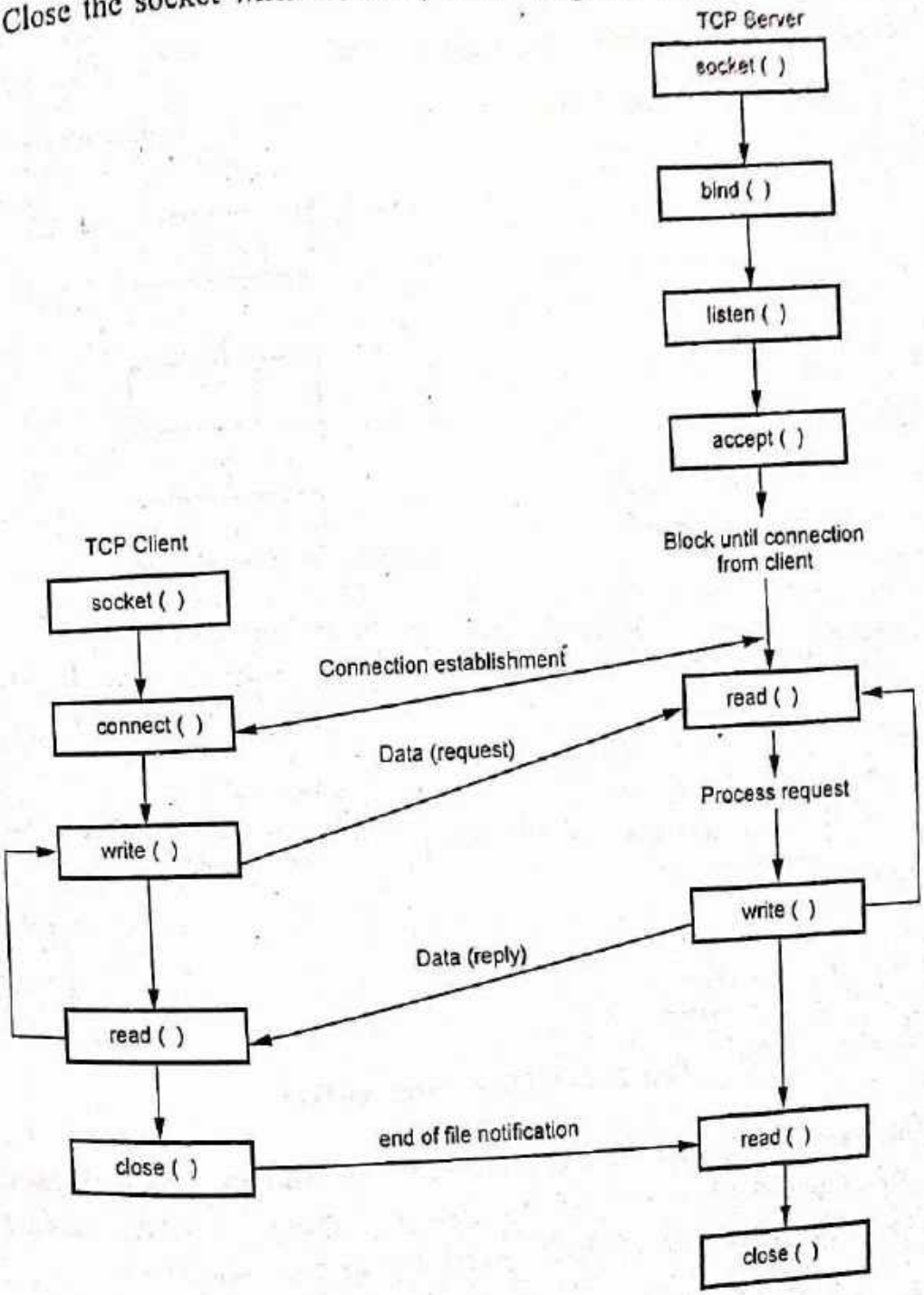


Fig. Q.13.2 Socket function for elementary TCP client server

- Only steps two and three are different, depending on if it's a client or server application.
- Fig. Q.13.2 shows a timeline of the typical scenario that takes place between a TCP client and server.

UDP Socket

- There are some instances when it makes to use UDP instead of TCP. Some popular applications built around UDP are DNS, NFS and SNMP.
- Fig. Q.13.3 shows the interaction between a UDP client and server.

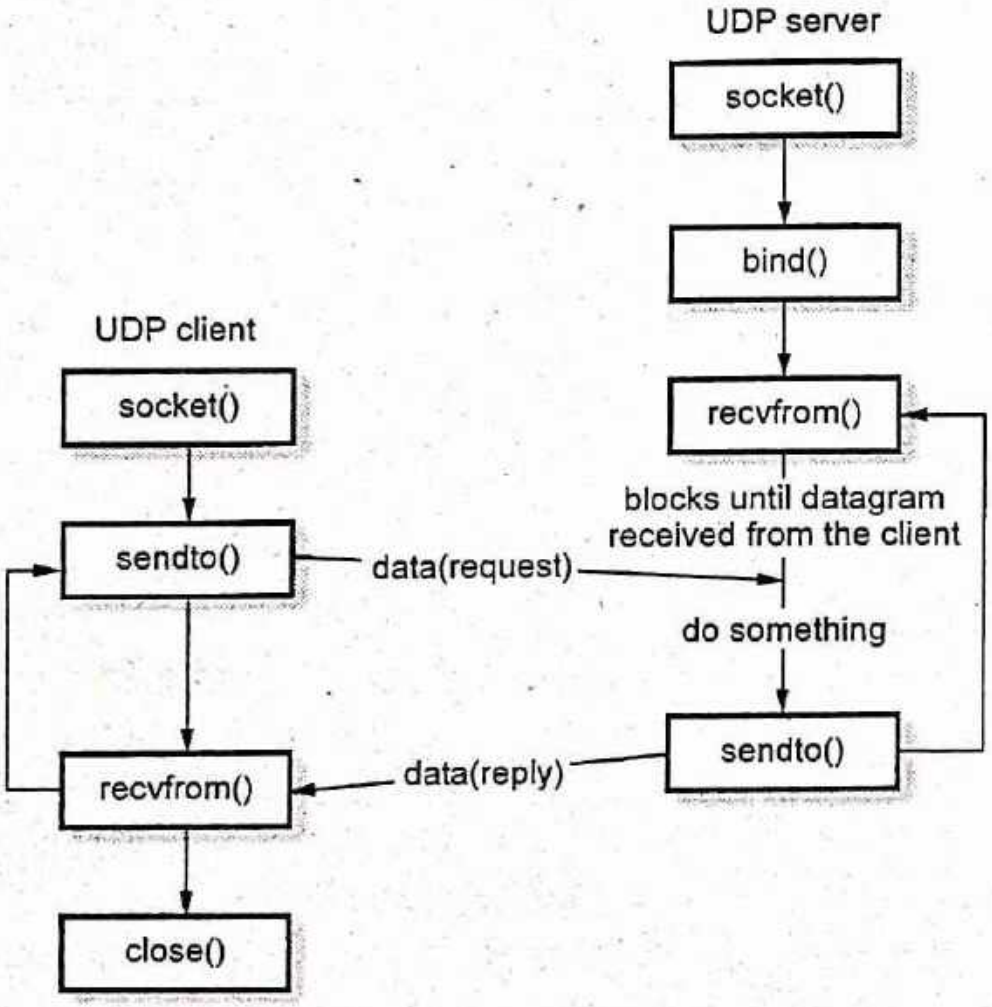


Fig. Q.13.3 UDP client-server

- Initially client does not establish a connection with the server. Instead, the client just sends a datagram to the server using the sendto function which requires the address of the destination as a parameter.

- Similarly, the server does not accept a connection from a client. Instead, the server just calls the recvfrom function, which waits until data arrives from some client.
- *recvfrom* returns the protocol address of the client, along with the datagram, so the server can send a response to the client.

Steps on the client side are as follows :

1. Create a socket using the socket( ) function;
2. Send and receive data by means of the recvfrom( ) and sendto( ) functions.

Steps on the server side are as follows :

1. Create a socket with the socket() function;
2. Bind the socket to an address using the bind( ) function;
3. Send and receive data by means of recvfrom( ) and sendto( ).

END...

JUNE - 2022 (END SEM) [5869] - 285 **Solved Paper**

Course 2019

Time : $2\frac{1}{2}$ Hours] **[Maximum Marks : 70**

Instructions to the candidates :

1) ***Neat diagrams must be drawn wherever necessary.***
2) ***Figures to the right side indicate full marks.***
3) ***Use of calculator is allowed.***
4) ***Assume suitable data if necessary.***

Q.1 a) *Write a note on channelization techniques (Any Two)*
i) FDMA ii) TDMA iii) CDMA.
(Refer Q.6 of Chapter - 3) **[8]**

b) *Compare IEEE 802.3, IEEE 802.4, IEEE 802.5 in a tabular format.* **(Refer Q.11 of Chapter - 3)** **[9]**

OR

Q.2 a) *Explain CSMA / CA and CSMA / CD random access technique with suitable diagram / flowchart. Also comment on efficiency of each.*
(Refer Q.4 of Chapter - 3) **[8]**

b) *Write a note on*
i) Standard ethernet ii) Fast ethernet iii) Gigabit ethernet
(Refer Q.15 of Chapter - 3) **[9]**

Q.3 a) *What is subnetting ? A company is granted a site address 172.16.10.33/19 design the subnets and answer following questions :*
i) How many subnets does the chosen subnet mask produce ?

ii) How many valid hosts per subnet are available ?
iii) What are the valid subnets ?
iv) What's the broadcast address of each subnet ?
v) What are the valid hosts in each subnet ?
(Refer Q.7 of Chapter - 4) [8]

b) *What is the need of IPv6 ? Explain types of IPv6 address.* **(Refer Q.11 of Chapter - 4)** [9]

OR

Q.4 a) *Draw and explain IPv4 header format. List out special IP addresses and private IP addresses.*
(Refer Q.3 of Chapter - 4) [8]

b) *List the network layer services and define subnetting, supernetting, classful addressing, classless addressing.*
(Refer Q.9 of Chapter - 4) [9]

Q.5 a) *What is BGP ? What are the characteristics of BGP routing protocol ? What are the advantages and disadvantages of BGP routing protocol ?*
(Refer Q.13 of Chapter - 5) [9]

b) *Draw the router architecture. Explain the difference between RIP, EIGRP, OSPF in tabular format.*
(Refer Q.12 of Chapter - 5) [9]

OR

Q.6 a) *What are the problems in RIP ? How to overcome the problems ? Compare RIPv1 and RIPv2.*
(Refer Q.4 of Chapter - 5) [9]

b) *Explain following routing.*
i) Static routing ii) Dynamic routing iii) Default routing.
(Refer Q.1 of Chapter - 5) [9]

Q.7 a) *What is the purpose of Leaky bucket and token bucket algorithms ? Describe working of Leaky bucket algorithm with reference to CBR, VBR and bursty traffic.*
(Refer Q.10 of Chapter - 6) [9]

b) *What is socket ? Explain various socket primitives used in client server interaction.* **(Refer Q.13 of Chapter - 6)** [9]

OR

Q.8 a) *Explain the three-way handshake algorithm for TCP connection establishment. List the fields in TCP header that are not part of UDP header. Give the reasons of each missing field.* **(Refer Q.4 of Chapter - 6)** [9]

b) *List out key features of UDP protocol. Explain how flow control is different than congestion control in TCP ?* **(Refer Q.12 of Chapter - 6)** [9]

END...