COMPUTER NETWORKS

OVERVIEW OF DATA COMMUNICATION AND NETWORKING

Multiple Choice Type Questions

1. If a signal changes instantaneously, its frequency is [WBUT 2010]
a) 0 b) finite c) infinite d) none of these
Answer: (c)

2. A digital signal has eight levels. How many bits are needed per level? [WBUT 2010]
a) 0 b) 4 c) 3 d) none of these
Answer: (c)

3. The value of SNR_{dB} for a noiseless channel is [WBUT 2010]
a) 0 b) finite c) infinite d) none of these
Answer: (c)

4. Total bandwidth required for AM is [WBUT 2010, 2012]
a) 0 b) 2(1+d) B c) 2B d) none of these
Answer: (c)

5. In ..... we make the highest input data rate the dominant data rate and then add dummy bits to the input lines with lower rates. [WBUT 2010]
a) multiplexing b) interleafing c) pulse stuffing d) none of these
Answer: (a)

6. An example of full duplex transmission is [WBUT 2012]
a) Telephone channel b) Satellite channel
c) Broadcast radio d) none of these
Answer: (a)

7. Repeaters function in the ..... layer. [WBUT 2013]
a) physical b) data link c) network d) transport
Answer: (a)

8. Process to Process delivery is the function of ..... layer. [WBUT 2013]
a) transport b) network c) physical d) none of these
Answer: (a)

9. In Ethernet when Manchester encoding is used, the bit rate is [WBUT 2014]
a) Half the baud rates b) Twice the baud rate
c) Same as the baud rate d) None of these
Answer: (a)

10. Match with suitable option [WBUT 2014]

LIST – I

(A) Node-to-Node delivery (B) Reassembly of data packets

(C) Bit representation (D) Encryption

LIST – II

(1) Physical Layer (2) Application Layer

(3) Data Link Layer (4) Transport Layer

a) A – 4, B – 3, C – 1, D – 2 b) A – 3, B – 4, C – 1; D – 2

c) A – 2, B – 3, C – 4, D – 1 d) A – 4, B – 4, C – 3, D – 3

Answer: (b)

11. Which transmission is highly susceptible to noise interference? [WBUT 2015]

a) ASK b) FSK c) PSK b) QAM

Answer: (a)

12. Phase transition for each bit is used is [WBUT 2016]

a) NRZ encoding b) Manchester encoding

c) Carrier modulation d) Amplitude modulation

Answer: (b)

13. In an optical fibre, the inner core is ..... the cladding. [WBUT 2017]

a) denser than b) less dense than

c) the same density as d) another name for

Answer: (a)

14. A bridge has access to the ..... address of a station on the same network. [WBUT 2017]

a) Physical (MAC) b) Network

c) Service access point d) all of these

Answer: (a)

15. Which of the following is not a guided medium? [WBUT 2019]

a) Twisted-pair b) Fibre optic

c) Air d) Coaxial cable

Answer: (c)

16. Which multiplexing technique involves signals composed of light beams? [WBUT 2019]

a) FDM b) TDM c) WDM d) None of these

Answer: (c)

Short Answer Type Questions

1. a) What is the major disadvantage in using NRZ encoding? How does RZ encoding attempt to solve the problem? [WBUT 2006, 2012]

b) We want to digitize human voice (frequencies ranging from 0 to 4000 kHz). What is the bit rate, assuming 8 bits per sample? [WBUT 2006, 2015]

Answer:

a) The main problem with NRZ encoding occurs when the sender and receiver clocks are not synchronized. The receiver does not know when one bit has ended and the next nbit is starting. One solution is the **return-to-zero (RZ)** scheme, which uses three values: positive, negative, and zero. In RZ, the signal changes not between bits but during the bit.

b) Sampling rate = 4000*2 = 8000 sample/sec
Bit rate = Sampling rate * nos. of bit per sample
= 8000*8 = 64000 bit per sec = 64 kbps

2. a) What is the purpose of multiplexing? FDM is for analog signals, TDM is for digital signals. Explain why. [WBUT 2008, 2014]

b) What Should be the link capacity to multiplex 3 input signals each of 300 bits per sec speed using 2 bits/sec framing rate? [WBUT 2008, 2014]

Answer:

a) Multiplexing is needed so that the available channel can be used efficiently and also to save costs. There is too much to know about multiplexing, here is just a short overview. One thing that one has to know is multiple access.

Time-domain concept

With respect to time, a signal can be either continuous or discrete. In a continuous signal, the signal intensity varies smoothly over a period of time, i.e., there are no breaks in the signal, e.g., human speech. The familiar sine wave (y = sin(x)) is an example of a continuous signal. On the other hand, in a discrete signal, the signal intensity is maintained at a constant level for some period of time and then changes to another constant level, e.g., binary 1 and 0.

Frequency-domain concept

Practically speaking, an electromagnetic signal is made up of many frequencies, for example, the human speech uses a frequency range between 20 Hz – 200,000 Hz. This frequency range is called as the spectrum of the signal.

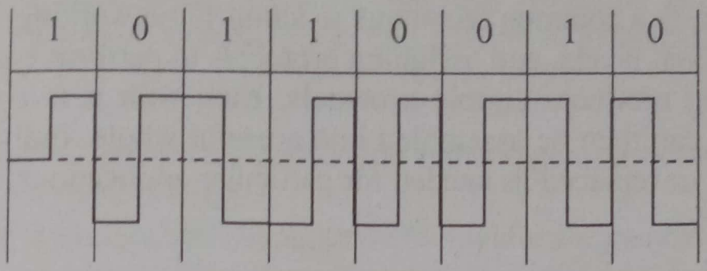
b) 3 input signals, each of 300 bps + 2bps framing rate means no. of bits arrives per second = (300 + 2) * 3 = 906 bps.
Therefore, Link Capacity = 906bps

3. a) Sketch the waveform for the bit stream 10110010 in differential Manchester encoding format. [WBUT 2008, 2012, 2013]

b) A binary signal is sent over a 8 kHz channel whose signal to noise ratio is 20 dB. What is the maximum achievable rate? Define signaling rate. [WBUT 2008]

Answer:

a)



b) Bandwidth $B = 8KHz = 2^{13}Hz$

$S/N = 20db = 100$

$C = B\log_2(1+S/N) = 2^{13} \log_2(1+100) = 6.5 \times 2^{13}$

4. a) What is the purpose of providing two separate protocols UDP and TCP in the transport layer of TCP/ IP architecture?

b) Physical address operates in a local domain whereas logical address has a global domain. Explain, Define bandwidth of a media. **[WBUT 2008, 2014]**

Answer:

a) TCP is a connection oriented protocol. So it offers a reliable transmission of data. But UDP is connectionless protocol. Which produce an unreliable service but it is faster than connection oriented protocol.

b) i) A Physical address is a 48-bit flat address burned into the ROM of the NIC card which is a Layer1 device of the OSI model. This is divided into 24-bit vendor code and 24-bit serial address. This is unique for each system and cannot be changed.

A Logical address is a 32- bit address assigned to each system in a network. This works in Layer-3 of OSI Model. This would be generally the IP address.

ii) Physical address also called MAC address. It is present on Network interface cad. It won't change.

Logical addressing is used when a packet passes n/w boundary.

Band Width:

Bandwidth (computing) or digital bandwidth: a rate of data transfer, throughput or bit rate, measured in bits per second.

Bandwidth (signal processing) or analog bandwidth: a measure of the width of a range of frequencies, measured in hertz.

5. Explain the utility of layered network architecture. Compare ISO-OSI and TCP/IP models. **[WBUT 2008, 2010, 2011]**

OR,

Write down the similarities and differences between OSI and TCP/IP model. **[WBUT 2013]**

OR,

Explain the utility of layered network architecture. **[WBUT 2014]**

OR,

Compare and contrast between OSI and TCP layered models. **[WBUT 2018]**

Answer:

1. Protocol layering is a common technique to simplify networking designs by dividing them into functional layers, and assigning protocols to perform each layer's task.
2. Protocol layering produces simple protocols, each with a few well defined tasks. These protocols can then be assembled into a useful whole. Individual protocols can also be removed or replaced as needed for particular applications.

Similarities

The main similarities between the two models include the following:

They share similar architecture. Both of the models share a similar architecture. This can be illustrated by the fact that both of them are constructed with layers.

They share a common application layer. Both of the models share a common "application layer". However in practice this layer includes different services depending upon each model.

Both models have comparable transport and network layers. This can be illustrated by the fact that whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.

Differences:

Both, TCP/IP model and OSI model, work in very similar fashions. But they do have very subtle differences.

OSI Model	TCP/IP Model
1. More of reference model created by ARPA. There are no real implementations.	1. Implemented by almost all equipments used in the context of Internet/Intranet – computers, routers, cell-phones, etc.
2. Defines seven layers.	2. Defines four layers (Application, Transport, Network and Data-Link) with an abstract physical layer.
3. No clear distinction specified with respect to connection-less and connection-oriented scenarios.	3. Clearly defined connectionless (UDP) and connection-oriented (TCP) Transport layers.
4. Have Session layer and Presentation layer with defined semantics.	4. Transport layer "links-up" with the physical layer directly.

6. What are the disadvantages in using NRZ encoding? How does RZ encoding attempt to solve the problem? **[WBUT 2010]**

Answer:

The main problem with NRZ encoding occurs when the sender and receiver clocks are not synchronized. The receiver does not know when one bit has ended and the next nbit is starting. One solution is the **return-to-zero (RZ)** scheme, which uses three values: positive, negative, and zero. In RZ, the signal changes not between bits but during the bit.

7. What is the purpose of Guard bands? In FDM, suppose there are three signal sources each having bandwidth 300 MHz. Find the minimum bandwidth of the path if 10MHz. Find the minimum bandwidth of the path if 10 MHz guard bands are used. **[WBUT 2010]**

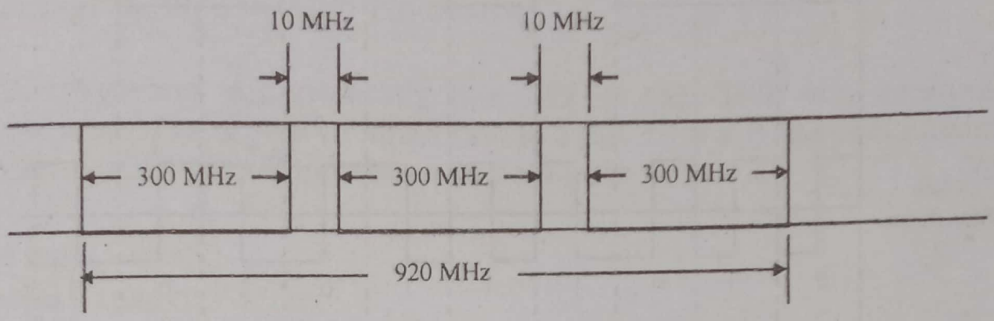
Answer:

In radio, a guard band is an unused part of the radio spectrum between radio bands, for the purpose of preventing interference.

It is a narrow frequency range used to separate two wider frequency ranges to ensure that both can transmit simultaneously without interfering each other. It is used in frequency division multiplexing.

With 3 signals, there are minimum 2 guard bands.

So minimum band width $= 3 \times 300 + 2 \times 10 = 920$ MHz.



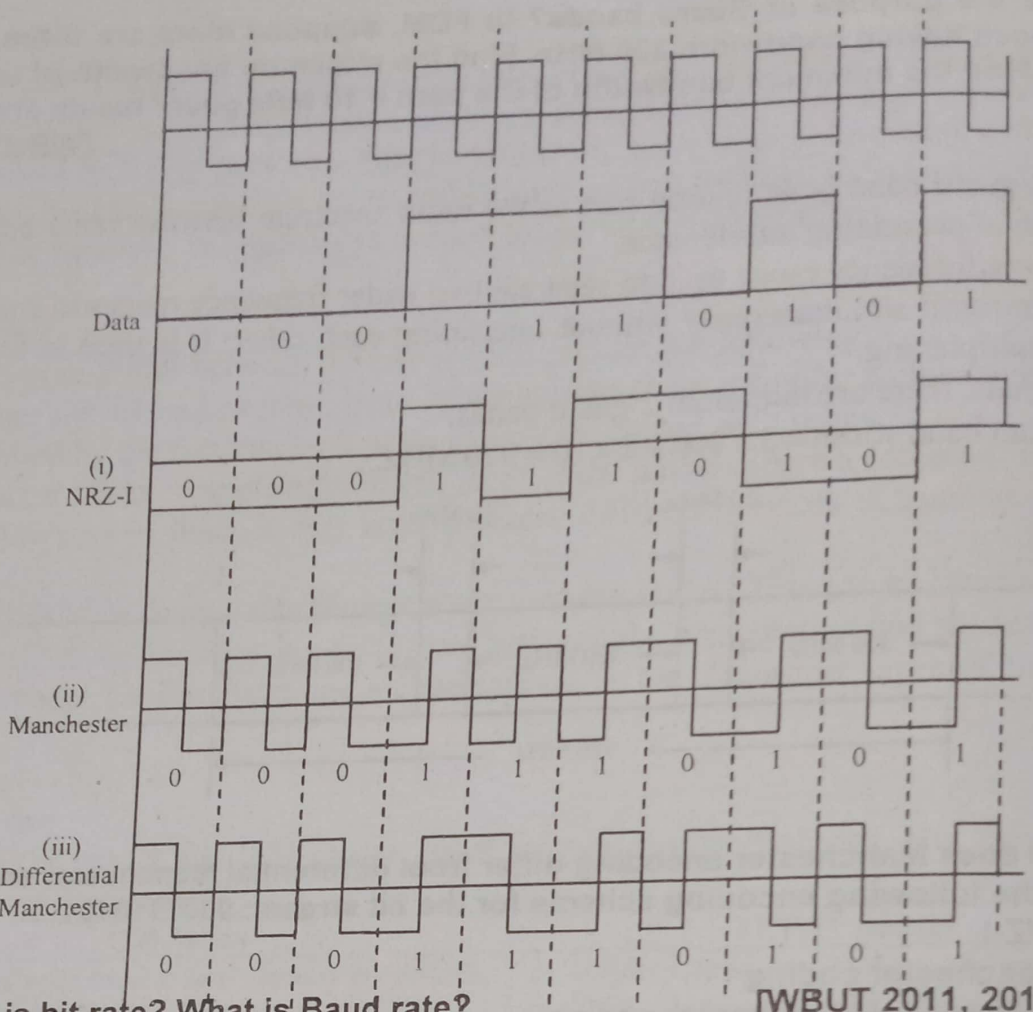
8. a) How does Manchester encoding differ from differential Manchester encoding?
b) Draw the following encoding scheme for the bit stream: 0001110101
(i) NRZ-I
(ii) Manchester coding
(iii) Differential Manchester coding. **[WBUT 2011]**

Answer:

a) Manchester code is a form of data communications line code in which each bit of data is signified by at least one transition. Manchester encoding is therefore considered to be self-clocking, which means that accurate synchronisation of a data stream is possible. Each bit is transmitted over a predefined time period.

On the other hand, Differential Manchester encoding is a method of encoding data in which data and clock signals are combined to form a single self-synchronizing data stream. It is a differential encoding, using the presence or absence of transitions to indicate logical value.

b)



9. a) What is bit rate? What is Baud rate? **[WBUT 2011, 2013, 2016]**

Answer:

Bit rate is the number of data bits transmitted per second.

Baud is a measure of the "signaling rate" which is the number of changes to the transmission media per second in a modulated signal. For example, 250 baud means that 250 signals are transmitted in one second.

Each signaling event transmitted can carry one or more bits (for example, 8 bits in 256-QAM modulation) of information. If baud rate is 250 and each signal carries 4 bits of information then in each second 1000 bits are transmitted. Thus, bit rate is 1000 bit/s.

b) An analog signal carries 4 bit in each signal unit. If 1000 signal units are sent per second, find the baud rate and bit rate. **[WBUT 2011, 2013, 2016]**

Answer:

There are 1000 signal units are sent per second.

And each signal carries 4 bits, as we know

Bit rate = No. of bits per second = 4×1000 bit/sec. = 4000 bit/sec. = 4 kbps.

where, **Baud rate** = No. of signal units per second = 1000 bits/sec. = 1kbps.

10. Differentiate between datagram and virtual circuit packet switching schemes. **[WBUT 2012]**

Answer:

- **Datagram packet switching** introduces the idea of cutting data on a flow into packets which are transmitted over a network without any resource being allocated. If no data is available at the sender at some point during a communication, then no packet is transmitted over the network and no resources are wasted.
  In this scheme each packet is processed individually by a router, all packets sent by a host to another host are not guaranteed to use the same physical links.
- **Virtual circuit packet switching** (VC-switching) is a packet switching technique which merges datagram packet switching and circuit switching to extract both of their advantages. VC **switching is a variation of datagram packet switching where packets flow on so-called logical circuits for which** no physical resources like frequencies or time slots are allocated.

11. a) A telephone line normally has BW of (300-3300 Hz) assigned for data communication. The signal to noise rate is 3162. Find the channel capacity.
b) Compare virtual circuit network and datagram network. **[WBUT 2014]**

Answer:

a) $C = B \log_2 (1+SNR)$
C= Channel Capacity
B= Bandwidth (Hz)
SNR = Signal to noise ratio
For this channel the capacity is calculated as
$C = B*\log_2(1 + SNR) = 3000*\log_2(1 + 3162) = 3000*\log_2(3163)$
$C = 3000*11.62 = 34860$ bps

b)

Virtual Circuit	Datagram
Host to host address is needed in link setup only	Host to host address is always needed in sending the datagram (Embedded in the datagram itself)
Errors are handled by subnetwork. Host will receive the packets in correct sequence.	Error checking is required by host to resemble the packet and find out the missing packets.
Messages passed in order to the network.	messages may be out of order in the communication sub-network
Connection setup is initially required prior to sending data	Connection setup is not required
Network component failure in path may affect the result	Is a flexible foundation to support a range of higher level protocols which can provide for additional network services
Less overhead in addressing embedded in the packet	Overhead in addressing
Example is X.25 Level 3	Example is Internet Protocol of (TCP/IP)

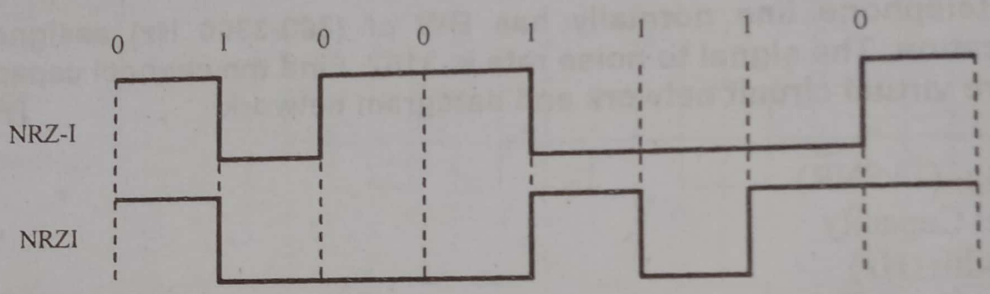
12. a) A signal has four data levels with a pulse duration of 1ms. Calculate the pulse rate and bit rate of the signal.
b) What do you mean by line coding? For a signal represented by 01001110 draw the patterns using the schemes: NRZ –L & NRZ-I. **[WBUT 2015]**

Answer:

a) Pulse Rate = $1/10^{-3} = 1000$ pulses/s
Bit Rate = Pulse Rate × $\log_2 L = 1000 \times \log_2 4 = 2000$ bps

b) 1st part:
Line coding consists of representing the digital signal to be transported, by a waveform that is optimally tuned for the specific properties of the physical channel (and of the receiving equipment).

2nd Part:



13. Discuss about various transmission impairments. **[WBUT 2015]**

Answer:

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

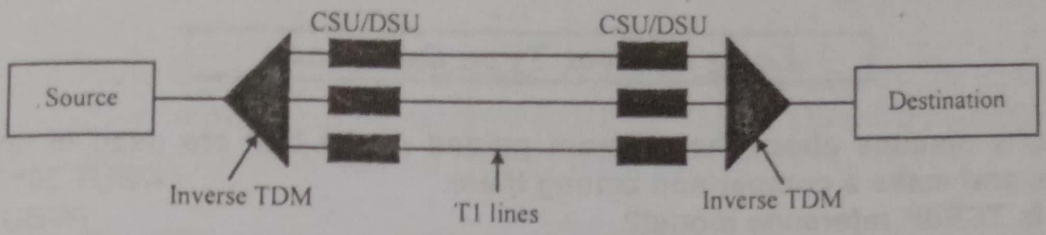
Attenuation is a telecommunications term that refers to a reduction in signal strength commonly occurring while transmitting analog or digital signals over long distances. Attenuation is historically measured in dB but it can also be measured in terms of voltage.

Noise is unwanted electrical or electromagnetic energy that degrades the quality of signals and data. Noise occurs in digital and analog systems, and can affect files and communications of all types, including text, programs, images, audio, and telemetry.

14. What is inverse TDM? **[WBUT 2015]**

Answer:

There is another technique which is known as inverse TDM which is also used in data communication today. This is opposite of the multiplexing technique. In the previous case what was done was the individual inputs of lesser bandwidth then we are combining to form a composite signal of higher bandwidth. Here it is opposite. Here we are receiving signal of higher bandwidth then it is divided into a number of channels of smaller bandwidth and at the other end opposite operation is done.



15. Define baseband and broadband transmission. What is the application of TDM switching? What is multiplexing? **[WBUT 2019]**

Answer:

Baseband: Electronic data prior to any modification. It refers to analog or digital data before they are merged with other signals (multiplexed) or intermixed into a carrier wave (modulated).

Broadband: A type of data transmission in which a single medium (wire) can carry several channels at once, cable TV, for example. In contrast, baseband transmission allows only one signal at a time.

Time Division Multiplexing (TDM) Switching is a type of digital multiplexing where two or more channels are derived from a selected frequency spectrum.

There are some apparent key benefits to using Time Division Multiplexing Switching as opposed to one of the other multiplexing switching techniques, such as:

TDM switching enables service providers to use both their legacy services and the new services simultaneously.

TDM can reduce costs by enabling service providers to move to Signalling System 7 (SS7).

TDM switching can positively impact investment and cost for service providers.

Multiplexing is sending multiple signals or streams of information on a carrier at the same time in the form of a single, complex signal and then recovering the separate signals at the receiving end.

16. a) Find the bandwidth for a QPSK signal transmitting at 2kbps. The transmission is in full duplex mode.

b) A digital signalling system is required to operate at 9600 bps. If a signal element encodes 16 bit word, what is the minimum bandwidth required for this channel? **[WBUT 2019]**

Answer:

a) Each signal element in QPSK carries 4 bits. Hence, band rate is $\frac{2\text{ kbps}}{4} = 500$ bps.

b) A digital signalling system is required to operate at 9600 bps.

Signal element encodes 16 bit word.

$\therefore$ Required bandwidth $= \frac{9600}{16} = 600$ Hz

Long Answer Type Questions

1. a) briefly discuss about the different guided media that are used in computer networks and make a comparison among them. **[WBUT 2012, 2019]**
b) What is TCP/IP reference model? **[WBUT 2012]**

Answer:

a) There are four basic types of Guided Media:

- Open Wire
- Twisted Pair
- Coaxial Cable
- Optical Fiber

Open Wire: Open Wire is traditionally used to describe the electrical wire strung along power poles. There is a single wire strung between poles. No shielding or protection from noise interference is used. This media is susceptible to a large degree of noise and interference and consequently not acceptable for data transmission except for short distances under 20 ft.

Twisted Pair: The wires in Twisted Pair cabling are twisted together in pairs. Each pair would consist of a wire used for the positive data signal and a wire used for the negative data signal. Any noise that appears on one wire of the pair would occur on the other wire. Because the wires are opposite polarities, they are 180 degrees out of phase and the noise appearing on the wires cancels itself out. Twisted Pair cables are most effectively used in systems that use a balanced line method of transmission.
The degree of reduction in noise interference is determined specifically by the number of turns per foot. Increasing the number of turns per foot reduces the noise interference.
To further improve noise rejection, a foil or wire braid shield is woven around the twisted pairs.

Coaxial Cable: Coaxial Cable consists of two conductors. The inner conductor is held inside an insulator with the other conductor woven around it providing a shield. An insulating protective coating called a jacket covers the outer conductor. The outer shield protects the inner conductor from outside electrical signals. The distance between the outer conductor (shield) and inner conductor plus the type of material used for insulating the inner conductor determine the cable properties or impedance. Typical impedances for coaxial cables are 75 ohms for Cable TV, 50 ohms for Ethernet Thinnet and Thicknet. The excellent control of the impedance characteristics of the cable allows higher data rates to be transferred than Twisted Pair cable.

Optical Fibre: Optical Fibre consists of thin glass fibres that can carry information at frequencies in the visible light spectrum and beyond. The typical optical fibre consists of a very narrow strand of glass called the Core. Around the Core is a concentric layer of glass called the Cladding. A typical Core diameter is 62.5 microns (1 micron = 10-6

meters). Typically Cladding has a diameter of 125 microns. Coating the cladding is a protective coating consisting of plastic, it is called the Jacket. Data is transmitted as light waves which undergo continuous total internal reflection.

The cost of optical fibre is a trade-off between capacity and cost. At higher transmission capacity, it is cheaper than copper. At lower transmission capacity, it is more expensive.

Topic	Twisted Pair	Co-Axial Cable	Optical Fiber
Number of Cable	One pair of cables are required	Single cable is required	Single Cable is required
Medium	Electrical medium is used	Electrical medium is used	Illumination medium is used
Noise	Noise immunity is low	Noise immunity is moderate.	Noise immunity is high
Speed	Communication speed is low, nearly 4 Mbps	Communication speed is moderate, nearly 500 Mbps	Communication speed is high, nearly 2 Gbps
Bandwidth	Low Bandwidth, 3 MHz	Comparatively high bandwidth, 350MHz	Very High bandwidth, 2 GHz
Distance	Cover small distance, 2 to 10 km	Cover small distance, 1 to 10 km	Cover large distance, 10 to 100km
Usage	Used in LAN, T1 Lines	Used in Cable TV, Ethernet Channel	Used in WAN,MAN etc.

b) TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

TCP/IP Model
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI Model
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Layer 1: Network Access Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
   - Delivering IP packets
   - Performing routing
   - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
   - TCP (Transmission Control Protocol): It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
   - UDP (User-Datagram Protocol): It is an unreliable connection-less protocol that does not want TCPs, sequencing and flow control. E.g.: One-shot request-reply kind of service.

2. a) Describe the following encoding techniques with suitable diagrams:
i) QPSK ii) QAM iii) FSK
b) Discuss the advantages of fibre optic cable. **[WBUT 2013]**

Answer:

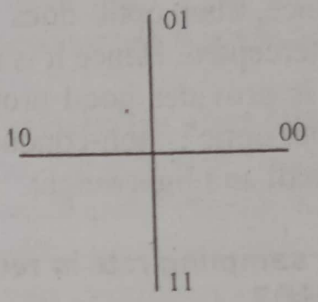
a) i) QPSK:

To increase the data rate and minimize error, advanced technique over ASK and FSK used is phase shift keying.

Phase of the carrier is varied to represent 1/0 while the peak multitude and frequency remains constant.

QPSK uses phase shift of $\frac{\pi}{2}$, 4 different signals generated each represents 2 bits. (00, 01, 10, 11).

Signal	Binary data	Phase
$A\cos(2\pi f_c t)$	00	0°
$A\cos\left(2\pi f_c t+\frac{\pi}{2}\right)$	01	90°
$A\cos(2\pi f_c t+\pi)$	10	180°
$A\cos\left(2\pi f_c t+\frac{3\pi}{2}\right)$	11	270°



ii) QAM:

It is a method is a method of combining two amplitudes – modulated (AM) signals into a single channel, thereby doubling the effective bandwidth.

In a QAM signal, there are two carriers, each having the same frequency but differing in phase by $\frac{\pi}{2}$ (In phase (I) and Quadrature phase (Q) signal). If one signal is represented by sine-waves the other can be represented by cos-wave.

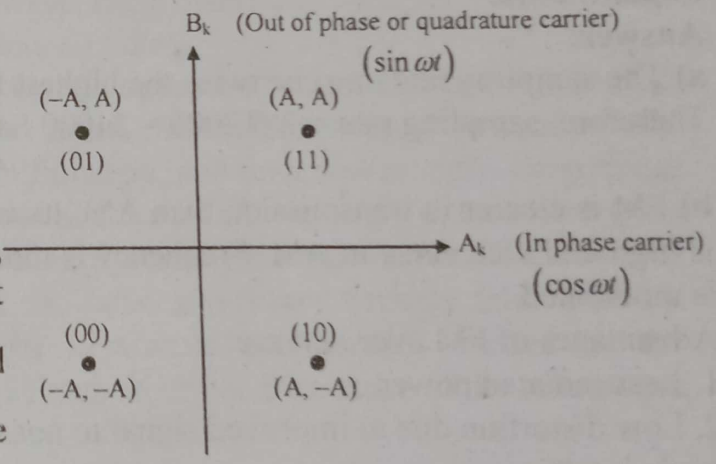


Fig: 1 Constellation diagram

They are used in digital data and in wireless communication

- Various types of QAM may be used like 16 QAM, 32 QAM, 64 QAM, 128 QAM, 256 QAM.
- It carries more bits per symbol and hence it is a higher order form of modulation. 16 AM → 4 bits per symbol → 1/4 bit rate $= 2^4$ data levels.
- At the transmitter the composite signal is sent $A_k \cos(2\pi f_c t) + B_k \sin(2\pi f_c t)$

iii) FSK:

Frequency-shift keying is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier wave. The two binary states, logic 0 (low) and 1 (high), are each represented by an analog waveform. FSK was the main way of communication in early days of analog telephone communication. But in modern world BFSK has been replaced by many new modulation techniques for higher-performances.

b) ***Advantages of fiber optic cable are***

i) Supports high speed communication over long distances without use of repeaters.
ii) As the technology uses total internal reflection, hence loss of signal and data involved is minimum.
iii) Since fiber optic does not radiate electromagnetic energy, emission cannot be intercepted. Hence it is a good choice for carrying secure data.
iv) It is provides good protection against electronic surges, as the material used in fiber optic is non-conductive.
v) Small and lightweight.

3. a) What sampling rate is required for a signal with bandwidth of 10,000 Hz (2,000 to 12,000 Hz)?
b) State the advantages of FM over AM.
c) What is transmission impairment? Discuss various types of transmission impairments. **[WBUT 2017]**

Answer:

a) The sampling rate must be twice the highest frequency in the signal.
Therefore, sampling rate = 2×12000 = 24000 Samples/s.

b) FM is clearer in transmission than AM. Its wavelength is short whereas the frequency is high and vice versa in AM. Frequency is modulated in FM whereas in AM, amplitude is modulated.

Advantages of FM over AM are:

1. Less radiated power.
2. Low distortion due to improved signal to noise ratio (about 25dB) with respect to man-made interference.
3. Smaller geographical interference between neighboring stations.
4. Well defined service areas for given transmitter power.

c) 1st Part: Transmission impairment is a property of a transmission medium which causes the signal to be degraded, reduced in amplitude, distorted or contaminated. Impairment can introduce errors into digital signals. Examples of transmission impairments are attenuation, delay distortion, and several sources of noise including, interference, thermal noise, impulse noise, and inter-modulation noise.

2nd Part: ***Refer to Question No. 13 of Short Answer Type Questions.***

4. Write short notes on the following:
a) Microwave transmission [WBUT 2010]
b) FDM [WBUT 2015]
c) Twisted Pair Cables [WBUT 2015]
d) LAN Topologies [WBUT 2018]

Answer:

a) Microwave transmission:

Microwave transmission refers to the technology of transmitting information by the use of the radio waves whose wavelengths are conveniently measured in small numbers of centimeters, by using various electronic technologies. These are called microwaves. This part of the radio spectrum ranges across frequencies of roughly 1.0 gigahertz (GHz) to 30 GHz. Also by using the formula $\lambda = c/f$, these correspond to wavelengths from 30 centimeters down to 1.0 cm. [In the above equation, the Greek letter λ (lambda) is the wavelength in meters; c is the speed of light in meters per second; and f is the frequency in hertz (Hz).]

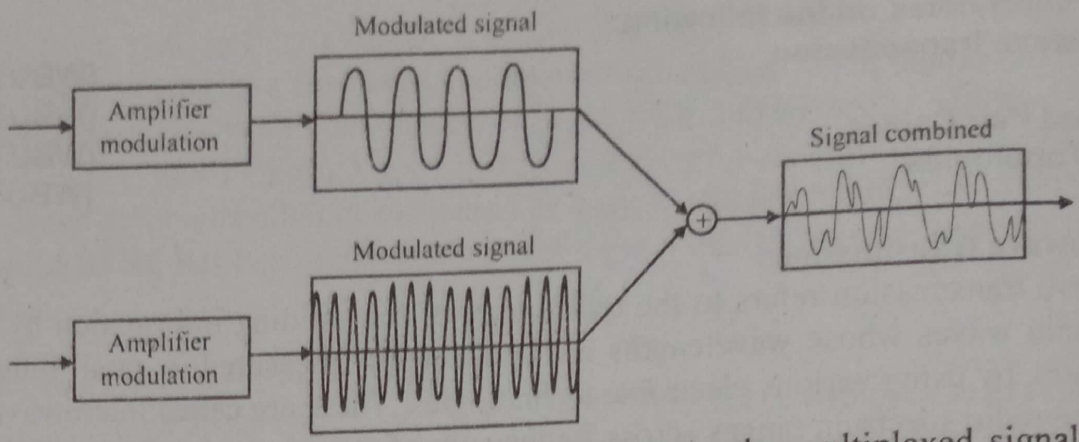
In the microwave frequency band, antennas are usually of convenient sizes and shapes, and also the use of metal waveguides for carrying the radio power works well. Furthermore, with the use of the modern solid-state electronics and traveling wave tube technologies that have been developed since the early 1960s, the electronics used by microwave radio transmission have been readily used by expert electronics engineers.

Microwave radio transmission is commonly used by communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

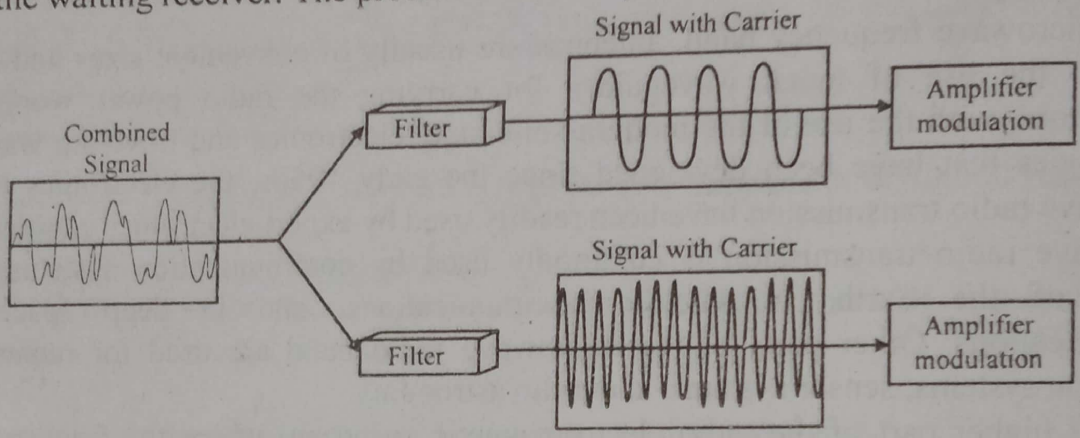
The next higher part of the radio electromagnetic spectrum, where the frequencies are above 30 GHz and below 100 GHz, are called "millimeter waves" because their wavelengths are conveniently measured in millimeters, and their wavelengths range from 10 mm down to 3.0 mm. Radio waves in this band are usually strongly attenuated by the Earthly atmosphere and particles contained in it, especially during wet weather. Also, in wide band of frequencies around 60 GHz, the radio waves are strongly attenuated by molecular oxygen in the atmosphere. The electronic technologies needed in the millimeter wave band are also much more difficult to utilize than those of the microwave band.

b) FDM:

In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. The carrier frequencies have to be different enough to accommodate the modulation and demodulation signals. The following figure illustrates the FDM multiplexing process. The multiplexing process starts by applying amplitude modulation into each signal by using different carrier frequencies as/I and/j. Then both signals are combined.



In demultiplexing process, we use filters to decompose the multiplexed signal into its constituent component signals. Then each signal is passed to an amplitude demodulation process to separate the carrier signal from the message signal. Then, the message signal is sent to the waiting receiver. The process of demultiplexing is shown in the figure.



c) Twisted Pair Cables:

A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures.

The wires in Twisted Pair cabling are twisted together in pairs. Each pair would consist of a wire used for the positive data signal and a wire used for the negative data signal. Any noise that appears on one wire of the pair would occur on the other wire. Because the wires are opposite polarities, they are 180 degrees out of phase and the noise appearing on the wires cancels itself out. Twisted Pair cables are most effectively used in systems that use a balanced line method of transmission.

The degree of reduction in noise interference is determined specifically by the number of turns per foot. Increasing the number of turns per foot reduces the noise interference.

To further improve noise rejection, a foil or wire braid shield is woven around the twisted pairs.

d) LAN Topologies:

LAN physical topology defines the geographical arrangement of networking devices. Topologies are driven fundamentally by two network connection types:

A point-to-point connection is a direct link between two devices. For example, when you attach your computer to a printer, you have created a point-to-point link. In networking

terms, most of the today's point-to-point connections are associated with modems and PSTN (Public Switched Telephone Network) communications because only two devices share point-to-point connections, it defeats the purpose of a shared network.
A multipoint connection, on the other hand, is a link between three or more devices. Historically, multipoint connections were used to attach central CPUs to distributed dumb terminals.
In today's LAN environments, multipoint connections link many network devices in various configurations.

The major topologies of LAN are:

1. Bus Topology
2. Ring Topology
3. Star Topology
4. Mesh Topology
5. Cellular Topology
6. Hybrid Topology

Bus Topology

The physical bus topology is the simplest and most widely used of the network designs. It consists of one continuous length of cabling (trunk) and a terminating resistor (terminator) at each end. The data communications message travels along the bus in both directions until it is picked up by a workstation or server NIC.
If the message is missed or not recognized, it reaches the end of the cabling and dissipates at the terminator. All nodes in the bus topology have equal access to the trunk – no discriminating here. This is accomplished using short drop cables or direct T-connectors.
This design is easy to install because the backbone trunk traverses the LAN as one cable segment. This minimizes the amount of transmission media required. Also, the number of devices and length of the trunk can be easily expanded.

Advantages of Bus Topology:

1. It uses established standards and it is relatively easy to install.
2. Requires fewer media than other topologies.

Disadvantages of Bus Topology:

1. The bus networks are difficult to reconfigure, especially when the acceptable number of connections or maximum distances have been reached.
2. They are also difficult to troubleshoot because everything happens on a single media segment. This can have dangerous consequences because any break in the cabling brings the network to its knees.

Ring Topology

As its name implies, the physical ring topology is a circular loop of point-to-point links. Each device connects directly or indirectly to the ring through an interface device or drop cable. Messages travel around the ring from node to node in very organized manner. Each workstation checks the messages for a matching destination address.

If the address doesn't match, the node simply regenerates the message and sends it on its way. If the address matches, the node accepts the message and sends a reply to the originating sender. Initially, ring topologies are moderately simple to install; however, they require more media than bus systems because the loop must be closed.
Once your ring has been installed, it's a bit more difficult to reconfigure. Ring segments must be divided or replaced every time they're changed. Moreover, any break in the loop can affect all devices on the network.

Advantages of Ring Topology:

1. They are very easy to troubleshoot because each device incorporates a repeater.
2. A special internal feature called becoming, allows the troubled workstation to identify themselves quickly.

Disadvantages of Ring Topology:

1. It is considerably difficult to install and reconfigure ring topology.
2. Media failure on unidirectional or single loop causes complete network failure.

Star Topology

The Physical star topology uses a central controlling hub with dedicated legs pointing in all directions – like points of a star. Each network devices has a dedicated point-to-point link to the central hub. This strategy prevents troublesome collisions and keeps the line of communication open and free of traffic.
Star topologies are somewhat difficult to install because each device gets its own dedicated segment. Obviously, they require a great deal of cabling. This design provides an excellent platform for reconfiguration and troubleshooting.
Changes to the network are as simple as plugging another segment into the hub. In addition, a break in the LAN is easy to isolate and doesn't affect the rest of the network.

Advantages of Star Topology:

1. Relatively easy to configure.
2. Easy to troubleshoot.
3. Media faults are automatically isolated to the failed segment.

Disadvantages of Star Topology:

1. Requires more cable than most topologies.
2. Moderately difficult to install.'

Mesh Topology

The mesh topology is the only true point-to-point design. It uses a dedicated link between every device on the network. This design is not very practical because of its excessive waste of transmission media. This topology is difficult to install and reconfigure.
Moreover, as the number of devices increases geometrically, the speed of communication also become slow. ATM (Asynchronous Transfer Mode) and switched Hubs are the example of high-speed Mesh implementation.

Advantages of Mesh Topology:

1. Easy to troubleshoot because each link is independent of all others.

2. You can easily identify faults and isolate the affected links. Because of the high number of redundant paths, multiple links can fail before the failure affects any network device.

Disadvantages of Mesh Topology:

1. It is difficult to install and reconfigure especially as the number of devices increases.

Cellular Topology

A cellular topology combines wireless point-to-point and multipoint designs to divide a geographic area into cells. Each cell represents the portion of the total network area in which a specific connection operates. Devices within the cell communicate with a central station or hub. Hubs are then interconnected to route data between cells.

The cellular topology relies on the location of wireless media hubs. Cellular networks exhibit interesting characteristics since this topology do not depend on cables. Troubleshooting is easy because each hub interacts independently with each device. A cellular installation depends on the accessibility hub locations.

Advantages of Cellular Topology:

1. It is relatively easy to install.
2. It does not require media reconfiguration when adding or removing users.
3. Fault isolation and troubleshooting is fairly simple.

Disadvantages of Cellular Topology:

1. All devices using a particular hub are affected by a hub failure.

Hybrid Topology

By modifying or combining some of the characteristics of the 'pure' network topologies, a more useful result may be obtained. These combinations are called hybrid topologies.

PHYSICAL LEVEL

Multiple Choice Type Questions

1. The total number of link required to connect *n* devices using Mesh Topology is [WBUT 2007, 2011]

a) 2^n b) $n(n+1)/2$ c) $n(n-1)/2$ d) n^2

Answer: (c)

2. Circuit switching takes place at the ..... layer. [WBUT 2010, 2012]

a) transport b) data link c) physical d) none of these

Answer: (c)

3. For a 4-bit sliding window, sequence number range is [WBUT 2013]

a) 1 to 16 b) 0 to 7 c) 0 to 15 d) 8 to 15

Answer: (c)

4. Which layer converts bit into electromagnetic signals? [WBUT 2016]

a) Physical b) Network c) Transport d) Session

Answer: (a)

5. The total number of links required to connect '*n*' devices using Mesh Topology is [WBUT 2018]

a) 2^n b) $n(n+1)/2$ c) $n(n-1)/2$ d) n^2

Answer: (c)

6. In Go-Back-N ARQ, the size of the receiver window will be [WBUT 2019]

a) 2^n b) 1 c) 2^{n-1} d) 0

Answer: (b)

Short Answer Type Questions

1. Differentiate circuit switching and packet switching.

[WBUT 2008, 2010, 2011, 2012, 2013]

OR,

Compare circuit switching with packet switching. [WBUT 2017]

Answer:

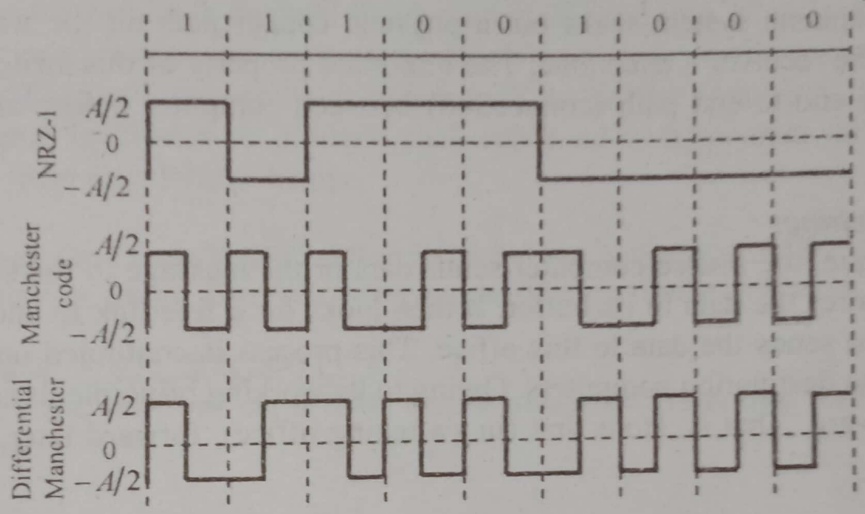
Circuit switching	Packet switching
Circuit switching establishes fixed bandwidth circuit/channel between nodes and terminals before the users may communicate	Packet switching is a communication in which packet are routed between node over data links shared with other traffic. In each network node, packets are queued in buffered, resulting in variable delay.

2. For following situations state which type of network architecture is appropriate
i) No. of users 50
ii) Data and resources need to be restricted
iii) No. network administrator required
iv) all users with equal priority. **[WBUT 2014]**

Answer:
i) Bus or Ring topology
ii) Mesh topology
iii) Mesh topology
iv) Bus or Ring topology

3. Find NRZ-I, Manchester and Differential Manchester encoding for the binary data 111001000. **[WBUT 2017]**

Answer:



4. Compare Mesh and Star Topology. **[WBUT 2017]**

Answer:

Mesh topology	Star topology
In this type of topology, every node has a dedicated point to point link to every other node in the network. This means each link carries traffic only between the two nodes it connects. No traffic problem as there are dedicated links. Robust as failure of one link does not affect the entire system. Security as data travels along a dedicated line. The hardware is expansive as there is dedicated link for any two nodes and each device should have (n-1) I/O ports	Star topology is less expensive than a mesh topology as there are no dedicated links between nodes and each device needs only one link and one I/O ports to connect it to any number of nodes. Entire network collapse if central controller fails. Security is less. Star topology is less expensive than a mesh topology as there are no dedicated links between nodes and each device needs only one link and one I/O ports to connect it to any number of nodes

5. Explain message switching with a proper diagram. **[WBUT 2019]**

Answer:

Refer to Question No. 1 of Long Answer Type Questions.

Long Answer Type Questions

1. Distinguish among the working principles of circuit switching, message switching and packet switching techniques. [WBUT 2010, 2012]

Answer:

Different types of switching techniques are employed to provide communication between two computers. These are: Circuit switching, message switching and packet switching.

Circuit Switching:

In this technique, first the complete physical connection between two computers is established and then data are transmitted from the source computer to the destination computer. That is, when a computer places a telephone call, the switching equipment within the telephone system seeks out a physical copper path all the way from sender telephone to the receiver's telephone. The important property of this switching technique is to setup an end-to-end path (connection) between computer before any data can be sent.

Message Switching:

In this technique, the source computer sends data or the message to the switching office first, which stores the data in its buffer. It then looks for a free link to another switching office and then sends the data to this office. This process is continued until the data are delivered to the destination computers. Owing to its working principle, it is also known as store and forward. That is, store first (in switching office), forward later, one jump at a time.

Packet Switching:

With message switching, there is no limit on block size, in contrast, packet switching places a tight upper limit on block size. A fixed size of packet which can be transmitted across the network is specified. Another point of its difference from message switching is that data packets are stored on the disk in message switching whereas in packet switching, all the packets of fixed size are stored in main memory. This improves the performance as the access time (time taken to access a data packet) is reduced, thus, the throughput (measure of performance) of the network is improved.

2. What is a multiplexer? Discuss one analog multiplexing technique. [WBUT 2013]

Answer:

1st Part:

Multiplexer is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A multiplexer of 2^n inputs has n select lines, which are used to select which input line to send to the output. Multiplexers are mainly used to increase the amount of data that can be sent over the network within a certain amount of time and bandwidth.

2nd Part:

Analog Multiplexing Technique: At the source end, for each frequency channel, an electronic oscillator generates a carrier signal at a single frequency that carries information, which has higher frequency than the baseband signal. The carrier signal and the baseband signal are applied to a modulator circuit. The modulator alters some aspect of the carrier signal, such as its amplitude, frequency, or phase, with the baseband signal, "piggybacking" the data onto the carrier. Multiple modulated sub-bands at different frequencies are sent through the transmission medium, such as a RF, cable, or optical fiber, on this main carrier. The information from the modulated signal is carried in the sidebands each side of the carrier frequency. This band of frequencies is called the passband of the channel. As long as the sub-band frequencies of the channel are spaced far enough apart, so they do not overlap, the sub-bands will not interfere with each another. Thus the available channel bandwidth is divided into "slots" or sub-bands, each of which can carry a separate or parallel modulated signal. At the destination end of the RF, cable, or fiber, a local oscillator mixes with the carrier frequency, and the resulting baseband signal is filtered to produce each sub-band to a separate output, or a single serial output from parallel sub-bands.

3. a) How does Go-Back-N ARQ differ from Selective Repeat ARQ?
b) A computer is using the following sequence numbers. What is the size of the window?
0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, ...
c) What does the number on a NAK frame mean for Selective Repeat ARQ? Give one example. **[WBUT 2018]**

Answer:

a) Comparison Chart

BASIS FOR COMPARISON	GO-BACK-N	SELECTIVE REPEAT
Basic	Retransmits all the frames that sent after the frame which suspects to be damaged or lost.	Retransmits only those frames that are suspected to lost or damaged.
Bandwidth Utilization	If error rate is high, it wastes a lot of bandwidth.	Comparatively less bandwidth is wasted in retransmitting.
Complexity	Less complicated.	More complex as it require to apply extra logic and sorting and storage, at sender and receiver.
Window size	N-1	<= (N+1)/2
Sorting	Sorting is neither required at sender side nor at receiver side.	Receiver must be able to sort as it has to maintain the sequence of the frames.
Storing	Receiver do not store the frames received after the damaged frame until the damaged frame is retransmitted.	Receiver stores the frames received after the damaged frame in the buffer until the damaged frame is replaced.

BASIS FOR COMPARISON	GO-BACK-N	SELECTIVE REPEAT
Searching	No searching of frame is required neither on sender side nor on receiver	The sender must be able to search and select only the requested frame.
ACK Numbers	NAK number refer to the next expected frame number.	NAK number refer to the frame lost.
Use	It more often used.	It is less in practice because of its complexity.

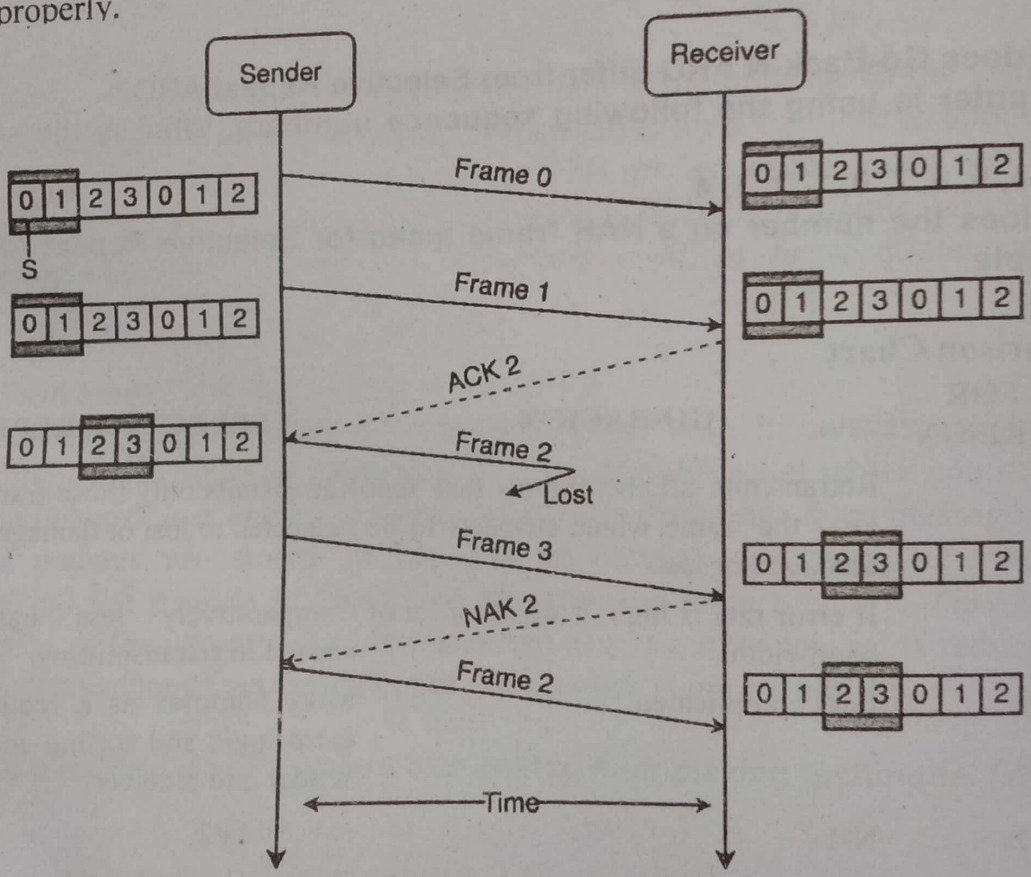
b) Sequence Number is:

0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4.....

$\therefore\ 2^{m-1} = 2^7$

As, window size $< 2^{m-1}$ (Ans.)

c) For selective repeat ARQ, NAK frame means upto that sequence no the frames are received properly.



$\therefore$ It means the frame 2 is not received and that frame is again sent to the receiver. So, NAK implies the lost frame number, which will be resent selectively.

4. Write short note on Virtual Circuit Switching. [WBUT 2018]

OR,

Write short note on Virtual Circuit. [WBUT 2019]

Answer:

Virtual circuit switching is a **packet switching** methodology whereby a path is established between the source and the final destination through which all the packets will be routed during a call. This path is called a virtual circuit because to the user, the connection appears to be a dedicated physical circuit. However, other communications may also be sharing the parts of the same path.

Before the data transfer begins, the source and destination identify a suitable path for the virtual circuit. All intermediate nodes between the two points put an entry of the routing in their routing table for the call. Additional parameters, such as the maximum packet size, are also exchanged between the source and the destination during call setup. The virtual circuit is cleared after the data transfer is completed.

Virtual circuit packet switching is connection orientated. This is in contrast to **datagram switching**, which is a connection less packet switching methodology.

Advantages of virtual circuit switching are:

- Packets are delivered in order, since they all take the same route;
- The overhead in the packets is smaller, since there is no need for each packet to contain the full address;
- The connection is more reliable, network resources are allocated at call setup so that even during times of congestion, provided that a call has been setup, the subsequent packets should get through;
- Billing is easier, since billing records need only be generated per call and not per packet.

Disadvantages of a virtual circuit switched network are:

- The switching equipment needs to be more powerful, since each switch needs to store details of all the calls that are passing through it and to allocate capacity for any traffic that each call could generate;
- Resilience to the loss of a trunk is more difficult, since if there is a failure all the calls must be dynamically reestablished over a different route.

Examples of virtual circuit switching are **X.25** and **Frame Relay**.

DATA LINK LAYER

Multiple Choice Type Questions

[WBUT 2008, 2017]

1. The Hamming code is used for
   a) Error Detection
   b) Error correction
   c) Error encapsulation
   d) (a) and (b) both

Answer: (d)

2. For a 4 bit sliding window the sequence number can range from [WBUT 2008, 2012]
   a) 1 to16
   b) 0 to 7
   c) 0 to 15
   d) 8 to 15

Answer: (c)

3. The hamming distance d(000, 011) is [WBUT 2010]
   a) 0
   b) 1
   c) 2
   d) none of these

Answer: (c)

4. In selective repeat sliding window protocol, the receiver window size is [WBUT 2011]
   a) greater than one
   b) one
   c) two
   d) none of these

Answer: (a)

5. In HDLC inserts a 0 bit after *five* consecutive 1bits in the message data. [WBUT 2011]

6. The Hamming code is used for [WBUT 2011]
   a) error detection
   b) error correction
   c) error encapsulation
   d) both (a) and (b)

Answer: (d)

7. Which channel access method is used in Ethernet network? [WBUT 2011, 2012]
   a) CSMA/CD
   b) Token bus
   c) Token ring
   d) all of those

Answer: (a)

8. Pure ALOHA has a maximum efficiency of [WBUT 2011]
   a) 18%
   b) 37%
   c) 10%
   d) none of these

Answer: (b)

9. The ..... layer handles the creation of data frames. [WBUT 2012]
   a) Data link
   b) Network
   c) Transport
   d) Physical

Answer: (a)

10. Which detection method can detect a single bit error? [WBUT 2012]
a) CRC
b) two dimensional parity checks
c) simple parity check
d) previous all
Answer: (d)

11. If the dataword is 111111, the divisor is 1010, the remainder is 110, the CRC codeword is [WBUT 2013]
a) 1111111010 b) 111111110 c) 1010110 d) 1101010
Answer: (b)

12. In ..... ARQ, if a NAK is received, only the specified damaged or lost frame is transmitted. [WBUT 2013]
a) Go-Back-N
b) Selective Repeat
c) Stop-and-Wait
d) all of these
Answer: (b)

13. ..... is a collision free technique. [WBUT 2013]
a) Token Passing b) CSMA c) ALOHA d) CSMA/CD
Answer: (a)

14. HDLC protocols insert a 0 bit after ..... consecutive 1 bits in the message data. [WBUT 2013]
a) 5 b) 7 c) 4 d) 8
Answer: (a)

15. Which channel access method is used in IEEE 802.5 network? [WBUT 2013]
a) CSMA/CD b) token bus c) token ring d) all of these
Answer: (c)

16. How much of channel output of slotted ALOHA will be in comparison to pure ALOHA? [WBUT 2013]
a) same b) double c) three times d) none of these
Answer: (b)

17. Error detection and correction at the data link level is achieved by [WBUT 2014]
a) bit stuffing
b) cyclic redundancy codes
c) Hamming codes
d) Equalization
Answer: (c)

18. Match the following list: Sequence number is 5 bits [WBUT 2014]

	Protocol		W_S, W_R
(A)	Stop-N-Wait ARQ	(1)	31, 1
(B)	Go-Back-N ARQ	(2)	16, 16
(C)	Selective repeat ARQ	(3)	1, 1

W_S : Sender Window Size

W_R : Receiver Window size

a) A-3, B-1, C-2
b) A-1, B-3, C-2
c) A-2, B-1, C-3
d) A-3, B-2, C-1
Answer: (a)

[WBUT 2015]

19. Error Control activity is performed by
a) Data link layer b) Network layer c) Transport layer d) Session layer

Answer: (a)

[WBUT 2015]

20. HDLC is a
a) bit oriented protocol b) byte oriented protocol
c) both a) and b) d) can't say

Answer: (a)

[WBUT 2015]

21. Pick the odd one out from the following
a) 2D Parity Check b) CRC c) Hamming Code d) Checksum

Answer: (b)

22. Which of the following transmission media is not readily suitable to CSMA operation? [WBUT 2016]
a) Radio b) Twisted pair c) Fibre optic d) Coaxial

Answer: (a)

[WBUT 2017]

23. Sliding window protocol is used for
a) error control b) session control
c) flow control d) concurrency control

Answer: (c)

24. Which the following is an inter-domain routing protocol? [WBUT 2017]
a) RIP b) OSPF c) BGP d) Both (a) & (b)

Answer: (c)

25. HDLC (High-Level Data Link Control) is a [WBUT 2018]
a) bit oriented protocol b) byte oriented protocol
c) both (a) and (b) d) None of these

Answer: (a)

26. At which layer circuit switching takes place? [WBUT 2018]
a) IP b) ARP c) ICMP d) DHCP

Answer: (b)

27. For a system using TCP, the sender window size is determined by the window size of [WBUT 2019]
a) Receiver b) Congestion c) both (a) and (b) d) none of these

Answer: (c)

Short Answer Type Questions

1. A 10 bit data bit block 0111010111 is to sent using hamming code for error detection and correction. Show how the receiver corrects an error that occurs in 6th bit position form right. [WBUT 2008, 2011, 2014, 2016]

Answer:

First step (blank parity positions): _ _ 0 _ 1 1 1 _ 0 1 0 1 1 1

P1 = Parity(011001) = 1
P2 = Parity(011101) = 0
P4 = Parity(111111) = 0
P8 = Parity(010111) = 0
Hence sent word: 1 0 0 0 1 1 1 0 0 1 0 1 1 1
The sixth bit from right, i.e., the one underlined above is received erroneously.
So, received word: 1 0 0 0 1 1 1 0 1 1 0 1 1 1
At receiver:
P1 = Parity(1011101) = 1
P2 = Parity(0011101) = 0
P4 = Parity(0111111) = 0
P8 = Parity(0110111) = 1
Now: P4 : P3 : P2 : P1 = 1001 = 9Decimal.
So, the 9-th bit from left is erroneous, which is the underlined bit.

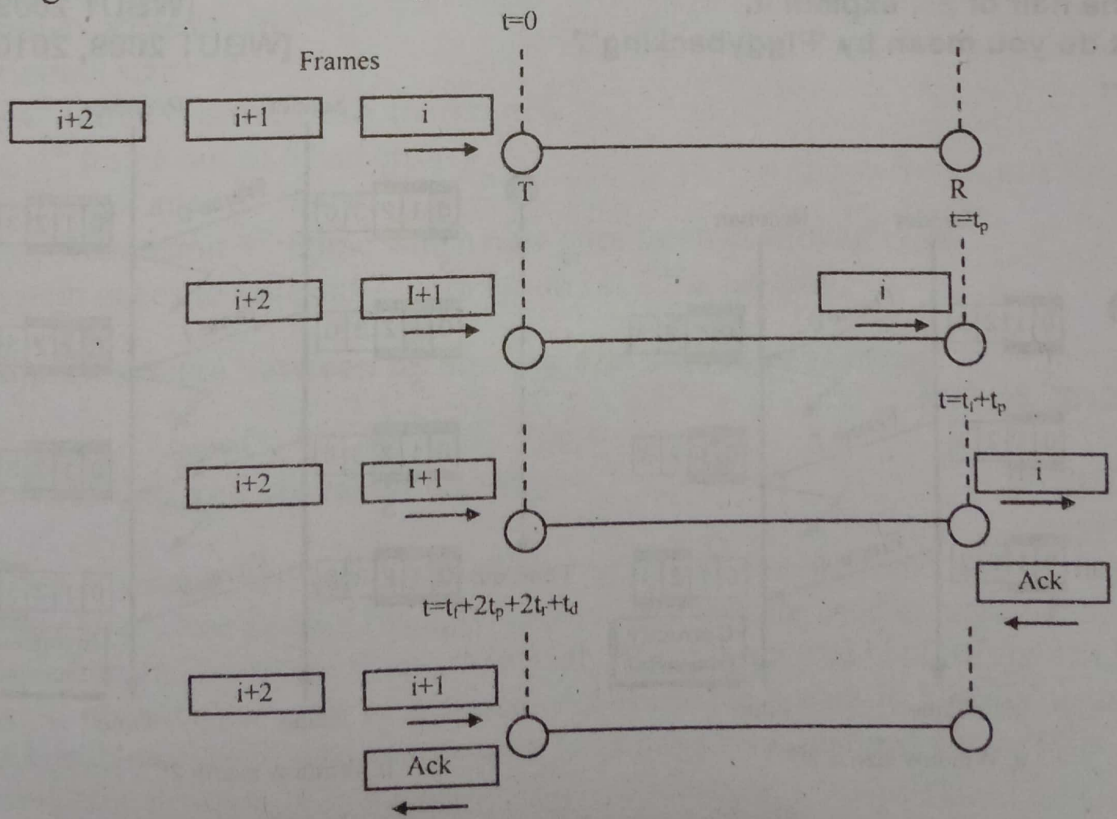
2. If a = propagation delay/ transmission delay and P is the Probability of frame error then prove that channel utilization in the case of stop and wait ARQ protocol is (1-p) / (1+2a). Assume negligible sender, receiver processing time, transmission time and acknowledgement time. **[WBUT 2008]**

OR,

What is working operation of stop and wait ARQ for Lost Acknowledgement. **[WBUT 2014]**

Answer:

The stop-and-wait protocol is the simplest and the least expensive technique for link-overflow control. The idea behind this protocol is that the transmitter waits for an acknowledgement after transmitting one frame.



In the following figure, we assume two consecutive frames i and i + 1. Frame i is ready to enter the link and is transmitted at t = 0. Let t_f be the time required to enter all the bits of a frame and t_p the propagation time of the frame between the transmitter (T) and the receiver (R). It takes as long as $t = t_f + t_p$ to transmit a frame. At the arrival of a frame i, the receiver processes the frame for as long as tr and generates an acknowledgment. For the same reason, the acknowledgment packet takes t = ta + tp to be received by the transmitter if ta is assumed to be the time required to enter all the bits of an acknowledgment frame, and it takes tr for processing it at the receiver. Therefore, the total time to transmit a frame, including acknowledgment processes,

$$t = t_f + 2t_p + 2t_r + t_a.$$

Note here that with this technique, the receiver can stop or slow down the flow of data by withholding or delaying acknowledgment. Practically, t_r and t_a are negligible compared to other components of the equation. Thus, this equation can be approximated as

$$t \approx t_f + 2t_p.$$

In this equation, t_f =l /r, where l is the length of frame in bits; r is the data rate; and t_p = d/Ï..., where d is the length of transmission line, and Ï... is speed of transmission. For wireless and wired transmissions, Ï... = 3 x 108 m/s where except for fiber-optic links, Ï...2.2 × 108 m/s, owing to the fact that light travels zigzag over links, and thus overall speed is lower. Therefore, the link efficiency is defined as

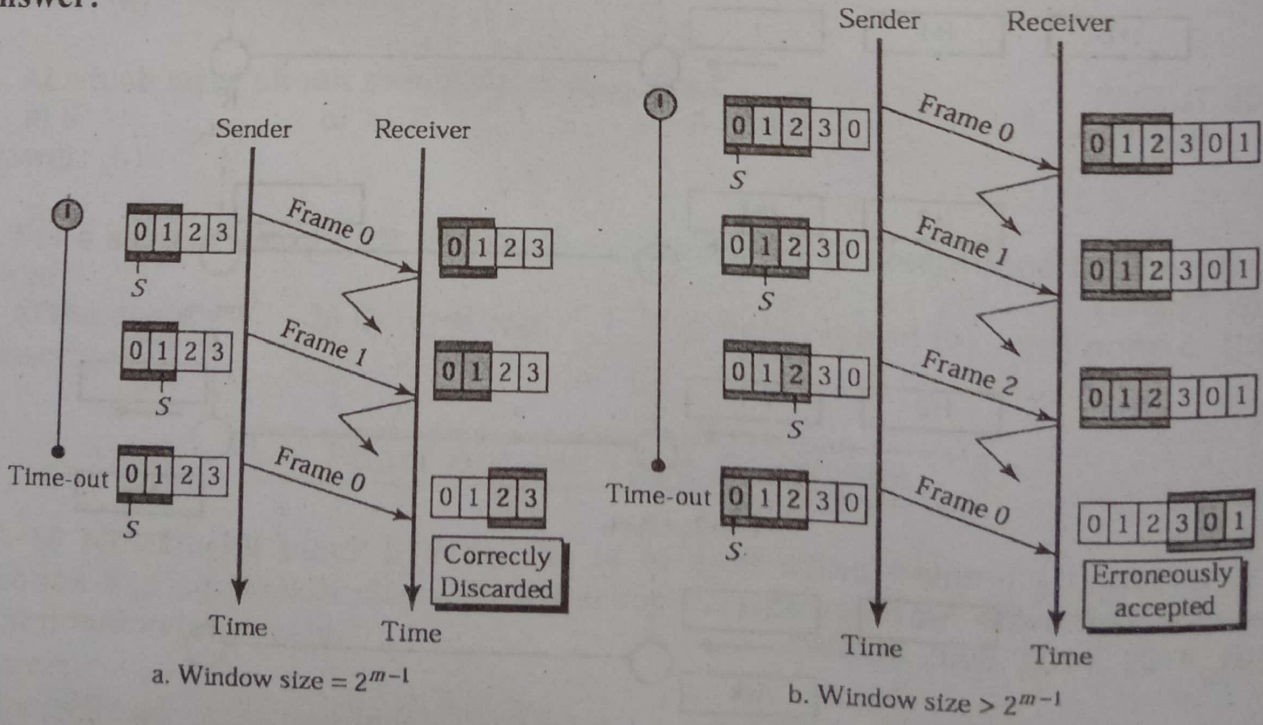
$$E_\ell = \frac{t_f}{t} = \frac{1}{1 + 2\left(\frac{t_p}{t_f}\right)}.$$

3. a) In Selective Reject ARQ the size of the sender and receiver window must be at most one half of 2^m, explain it. **[WBUT 2009, 2010]**

b) What do you mean by 'Piggybacking'? **[WBUT 2009, 2010, 2013]**

Answer:

a)



a. Window size = 2^{m-1}

b. Window size > 2^{m-1}

Size of the sender and receiver windows must be at most one-half of 2 m. If m = 2, window size should be 2 ^m /2 = 2. Fig compares a window size of 2 with a window size of 3. Window size is 3 and all ACKs are lost, sender sends duplicate of frame 0, window of the receiver expect to receive frame 0 (part of the window), so accepts frame 0, as the 1st frame of the next cycle – an error.

b) Piggybacking is a bi-directional data transmission technique in the network layer (OSI model). It makes the most of the sent data frames from receiver to emitter, adding the confirmation that the data frame sent by the sender was received successfully (ACK acknowledge). This practically means, that instead of sending an acknowledgement in an individual frame it is piggy-backed on the data frame.

4. Suppose a system uses Stop and Wait protocol with propagation delay 20 ms. If the frame size is 160 bits and band width is 4kbps then calculate channel utilization or efficiency. **[WBUT 2011, 2016]**

Answer:

At a transmission rate of 4bits/ms, 160 bits takes 20ms+20ms = 40 ms. So, after transmitting a 160 bits frame in 160/4=160ms, the sending system has to wait another 40ms to get the ACK. Thus it takes 20+20=80ms for a frame of which transmission happens for 40 ms.

So, efficiency = 40/80 = 50% for round trip propagation delay.

5. Suppose a system uses Go Back N protocol with window size 3. If a sender wants to transmit 6 frames and every 4th frame is error then calculate how many number of extra frames to be transmitted to the receiver. **[WBUT 2011]**

Answer:

Given: Frames 40 send = 6

N = window size = 3.

Every 4th frame is erroneously transmitted.

Hence, 4th frame out of 6 had error.

NAK received after 6th frame.

Action – Retransmit 4th frame which now goes through without error.

So, System needs to transmit 1 extra frame i.e. 7 frames total.

6. Write the difference between bit stuffing and character stuffing. **[WBUT 2012, 2013]**

OR,

What is bit stuffing and character stuffing? **[WBUT 2018]**

Answer:

Both bit and character stuffing are used to distinguish the start and end of frames. In character stuffing, some special (usually three) characters are used to mark the beginning and end of frames. In bit-stuffing, a special flag pattern "01111110" is send at the beginning to indicate the start of a frame. All subsequent data is literally treated as a stream of bits. However, if five consecutive '1'-s have been pumped out, a '0' is ignored by the receiver.

7. Discuss the IEEE 802.5 protocol. Draw the lower two layers of the IEEE 802.5 protocol. [WBUT 2012]

Answer:

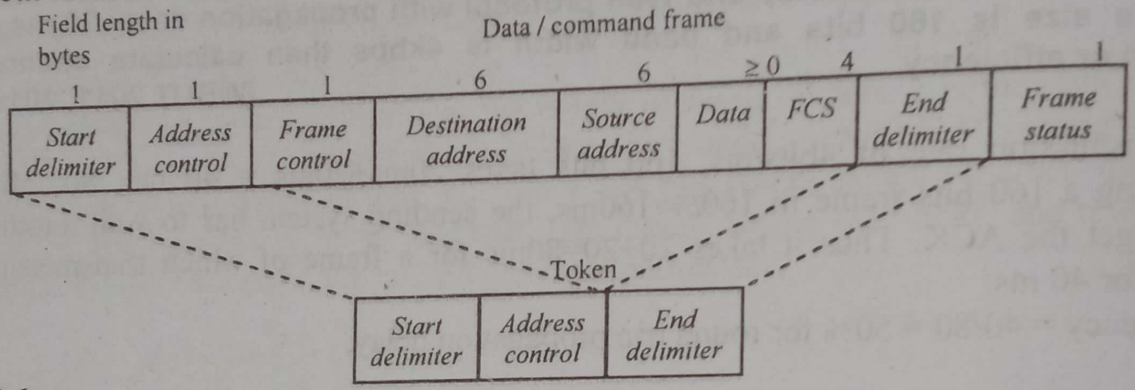
Token Ring and IEEE 802.5 support two basic frame types

- Tokens
- Data/command frames.

Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter.

Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols.

Both formats are shown in Figure below.



Tokens:

Start delimiter: Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

Access-control byte: Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

End delimiter: Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame

Data/command frames have the same three fields as Token Frames, plus several others:

Start delimiter: Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

Access-control byte: Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

Frame-control bytes: Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.

Destination and source addresses: Consists of two 6-byte address fields that identify the destination and source station addresses.

Data: Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.

Frame-check sequence (FCS): Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.

End Delimiter: Signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Frame Status: Is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

8. a) Suppose a sender is using sliding window protocol of window size 15. What will be the window status for the following occurrence? Sender has sent packets 0 to 11 and has received NAK 6.

b) "In Selective-Repeat ARQ, sender window size $> 2^{m-1}$." Is it correct? Justify.

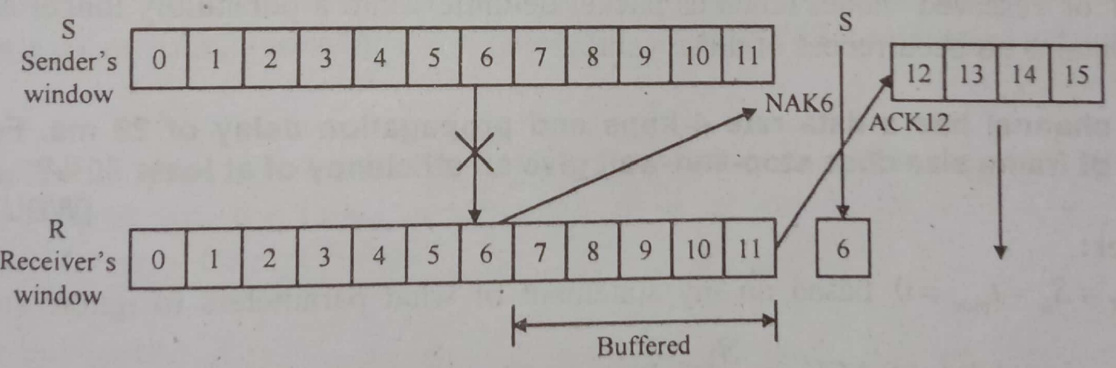
[WBUT 2013]

Answer:

a) Window size of sender is 15.

Sender(S) has sent 0 – 11 packets and received NAK6

- ✓ NAK is used by receiver to indicate there is error no frames received and sender must resend frame 6.
- ✓ After frame 6, from 7 to 15 are buffered in receiver (R).
- ✓ After resending frame 6 by S, the R can now send ACK 12 – expecting rest of frames (12 – 15)



b) The size of the sending and receiving windows must be equal and half the maximum sequence number (assuming that sequence numbers are numbered from 0 to n–1) to avoid miscommunication in all cases of packets being dropped. To understand this, consider the case when all ACKs are destroyed. If the receiving window is larger than half the maximum sequence number, some, possibly even all, of the packages that are resent after timeouts are duplicates that are not recognized as such. The sender moves its window for every packet that is acknowledged.

9. Discuss about data transparency and bit stuffing in case of HDLC? [WBUT 2015]

Answer:
In the frame format of HDLC flag fields delimit the frame at both ends with the unique pattern 01111110. A single flag may be used as the closing flag for one frame and the opening flag for the next. On both sides of the user-network interface, receivers are continuously hunting for the flag sequence to synchronize on the start of a frame. While receiving a frame, a station continues to hunt for that sequence to determine the end of the frame. Since the pattern 01111110 may appear in the frame as well, a procedure know bit stuffing is used. After detecting a starting flag, the receiver monitors the bit stream. When a pattern of five 1s appears, the sixth bit is examined. If this bit is 0, it is deleted. If the sixth bit is a 1 and the seventh bit is a 0, the combination is accepted as a flag. If the sixth and seventh bits are both 1, the sender is indicating an abort condition. With the use of bit stuffing, arbitrary bit patterns can be inserted into the data field of the frame. This property is known as data transparency.

10. What is bit stuffing and byte stuffing? [WBUT 2016]

Answer:
Bit stuffing is the mechanism of inserting one or more non-information bits into a message to be transmitted, to break up the message sequence, for synchronization purpose. This is called bit-oriented framing.
Bit stuffing is a mechanism to convert a message formed of a sequence of bytes that may contain reserved values such as frame delimiter into another byte sequence that does not contain the reserved values. This is also called character-oriented framing.

Byte stuffing is a process that transforms a sequence of data bytes that may contain 'illegal' or 'reserved' values (such as packet delimiter) into a potentially longer sequence that contains no occurrences of those values.

11. A channel has a data rate 4 kbps and propagation delay of 20 ms. For what range of frame size does stop-and-wait give an efficiency of at least 50%? [WBUT 2016]

Answer:
Set $S_0 = S_a = t_{proc} = 0$ based on my statement of what parameters to ignore (note that transmission delay of ACK is $\frac{S_a}{r}$). Plug in the values of $r = 4\,\text{kbps}$, $t_{prop} = 20\,\text{ms}$, and transmission efficiency is 50%. Find S_f. This works out to be 160 bits.

$$0.5 = \frac{1}{1 + \frac{(2 \times 20\,\text{ms}) \times 4\,\text{kbps}}{S_f}}$$

or, $S_f = 160$ bits.

12. What is polling?

Answer: **[WBUT 2018]**

Polling is the process where the computer or controlling device waits for an external device to check for its readiness or state, often with low-level hardware. For example, when a printer is connected via a parallel port, the computer waits until the printer has received the next character.

Algorithm

Polling can be described in the following steps:

Host actions:

1. The host repeatedly reads the busy bit of the controller until it becomes clear.
2. When clear, the host writes in the command register and writes a byte into the data-out register.
3. The host sets the command-ready bit (set to 1).

Controller actions:

1. When the controller senses command-ready bit is set, it sets busy bit.
2. The controller reads the command register and since write bit is set, it performs necessary I/O operations on the device. If the read bit is set to one instead of write bit, data from device is loaded into data-in register, which is further read by the host.
3. The controller clears the command-ready bit once everything is over, it clears error bit to show successful operation and reset busy bit (0).

13. Why acknowledgement is numbered in stop and wait protocol? Discuss the situation when unnumbered acknowledgements can create confusion in the sender and receiver end. **[WBUT 2019]**

Answer:

Refer to Question No. 3 of Long Answer Type Questions.

14. Compare Repeater, Router, Bridge and Gateway functionally as well as coverage of various layers for operational aspect in OSI/ISO reference model. **[WBUT 2019]**

Answer:

In order for computers from different manufacturers to communicate with each other by a reference model, which is called the OSI seven layer network model.

The seven layers of OSI model are –

i) Physical layer
ii) Data link layer
iii) Network layer
iv) Transport layer
v) Session layer
vi) Presentation layer
vii) Application layer

Repeater, Router, Bridges operate at the lowest three layers of the OSI network model i.e. the physical layer, data link layer and Network layer.

- Hubs and Repeater works at the first or physical layer. It just repeats the message to all the ports.
- Routers are on the third layer i.e. Network layer. They are used to connects network together. The internet consists of many interconnected routers. Using a network protocol, like TCP/IP, a router can intelligently move data from one network to another.
- Bridges operate at data link layer or second layer.

Long Answer Type Questions

1. Applying CRC algorithm, determine the checksum and the transmitted frame for the frame 11010111 and for the generator polynominal $x^3 + x^2 + 1$.
[WBUT 2006, 2011, 2016, 2018]

Answer:
Frame: 11010111

Generator G(x) of degree 3, $x^3 + x^2 + 1$: 1101
T(x) is the frame with 3 attached 0-bits: 11010111**000**
Divide T(x) by G(x) by using XOR,

$$1101 \,|\, 11010111000 \,|\, 1000010$$

$$\begin{array}{r} 1101 \\ \hline 0000 \end{array}$$

$$\begin{array}{r} 01110 \\ \underline{1101} \\ 000110 \rightarrow \text{Remainder} \end{array}$$

The remainder R(x) = 110. The Transferred frame: 11010111 **110**

2. What is the minimum window size required for selective-repeat ARQ protocol and how?
[WBUT 2010, 2018]

Answer:
The size of the sending and receiving windows must be equal and half the maximum sequence number (assuming that sequence numbers are numbered from 0 to n–1) to avoid miscommunication in all cases of packets being dropped. To understand this, consider the case when all ACKs are destroyed.
If the receiving window is larger than half the maximum sequence number, some, possibly even all, of the packages that are resent after timeouts are duplicates that are not recognized as such. The sender moves its window for every packet that is acknowledged.

3. Why acknowledgement is numbered in stop and wait protocol? Discuss a situation when unnumbered acknowledgements can create confusion in the sender and receiver end.
[WBUT 2012]

Answer:

The frame/ACK number field in Stop and Wait protocol is used in the receiver to distinguish between a new frame and a frame received earlier.

Suppose frames of succeeding packets are framed with frame numbers 0, 1, 0, 1, and so on (i.e., 0 and 1 repeating alternately).

The receiver keeps a local copy of the frame number that it expects to receive. If the arriving frame has a different frame number, it is silently discarded. On other cases, the receiver sets the ACK frame's frame-number with the received frames frame number and alters its expected frame number appropriately (0 to 1 or 1 to 0, as the case may be).

At the sender side, the last-sent frame is considered delivered correctly only if its frame number matches that of an ACK frame received.

Suppose frames and ACK-s are not numbered and a frame is sent and arrives error free on the receiver. It is delivered to the network layer and an unnumbered ACK is sent. Suppose the ACK itself gets corrupted on its way. The sender never gets the ACK and by the Stop and Wait algorithm, when the timer fires, it re-sends the frame. The receiver may receive this frame error-free. Since it has no inkling that the ACK it had sent earlier got lost, it will accept the frame and deliver the packet. In essence, the packet gets delivered twice and hence the sequence assumption is clearly broken.

4. a) Given a 10 bit sequence 1010011110 and a divisor of 1011. Find the CRC. **[WBUT 2012, 2013]**

OR,

Generate the CRC code for the data word of 1010011110. The divisor is 1011. **[WBUT 2018]**

b) What is the advantage of two dimensional parity over simple parity? Explain with suitable example. **[WBUT 2012]**

Answer:

a) Since divisor is 1101, we append from 0-s to the data and divide.

```
          100100011
       ____________
1011 | 1010 011110 0000
       1011
       ----
         1011
         1011
         ----
           1100
           1011
           ----
            1110
            1011
            ----
             1010
             1011
             ----
Remainder →  0010
```

∴ Data with CRC is 1010 0111 1000 10

b) Two dimensional parity check increases the likelihood of detecting burst errors. It can detect upto three burst errors that occurs anywhere in the table, whereas one-dimensional parity can detect upto one error in a block.

Example: Suppose we want to send four 5-bit words arranged in a table and the data are 10111, 00100, 11001, 01100

10111	0
00100	1
11001	1
01100	0
00110	0

So, the sent bit pattern is 10111 0 00 1001 110011 011000 001100

Suppose the three 0-s as shown is box get received as 1-s. In one-dimensional parity, the double error in the second word will not get detected. However, in one example, the last parity word will easily detect the errors.

5. a) Prove that $2^r \geq m+r+1$, where m is the no. of data bits and r is the no. of redundancy bits required to correct the error.
b) How does a single bit error differ from a burst error? **[WBUT 2013]**

Answer:

a) In Hamming code, r parity bits must indicate all possible error positions plus one case for no error. Since there are total m+r bits and r parity bits indicate r th power of 2, we get $2^r \geq m+r+1$.

b)

Single bit error	Burst bit error
1. It means only one bit of data unit is changed during transmission T_X 1 0 1 1 R_X 1 1 1 1	1. Multiple bits in single data units (two or more) are changed. Length of error is measured from first changed bit to last bit. T_X 1 0 1 1 R_X 0 1 1 1
2. Single bit errors can happen in parallel transmission – where all the data bits are transmitted using separate wires.	2. Burst errors are likely to occur in a serial transmission.
3. Can be detected by Hamming code or Block code.	3. Detected by Convolution codes.

6. a) The address 43:7B:6C:DE:10:00 has been shown as the source address in an Ethernet frame. The receiver has discarded the frame. Why?
b) What is transparent bridge? How does a repeater extend the length of a LAN?

Answer: **[WBUT 2014]**

a) The first byte in binary is 0100001. The least significant bit is 1. This means the pattern defines a multicast address. A multicast address can be a destination address, but

not a source address. Therefore the receiver knows there is an error and discards the packet.

b) Transparent bridges are bridges that connect more than one network segments with other bridges and take routing decisions.

A repeater is a networking component that extends a network by boosting the signal so that it can travel farther along the cabling. Digital signals travelling on cables weaken with distance—a phenomenon known as attenuation. A repeater is a form of digital amplifier that works at the physical layer (layer 1) of the Open Systems Interconnection (OSI) reference model for networking to regenerate (amplify) the signal so that it can travel farther. Repeaters also perform other functions such as filtering out noise caused by electromagnetic interference (EMI), reshaping the signal, and correcting timing to remove signal jitter so that the signal can travel farther. Repeaters can also be used to join dissimilar media such as unshielded twisted-pair (UTP) cabling and thinnet, but they cannot be used to join dissimilar network architectures such as Ethernet and Token Ring. Repeaters are an inexpensive way to extend a network.

7. a) What do you mean by Forward Error Correction (FEC)? Discuss in detail.
b) The code 11110101101 was received. Using the Hamming Code method find out what was the original code sent.
c) In case of stop –and –Wait ARQ, with the help of suitable diagrams discuss the operations performed on the following situations:
i) Lost or damaged frame
ii) Lost Acknowledgement
iii) Delayed Acknowledgement.

[WBUT 2015]

Answer:

a) Forward error correction (FEC) is a digital signal processing technique used to enhance data reliability. It does this by introducing redundant data, called error correcting code, prior to data transmission or storage. FEC provides the receiver with the ability to correct errors without a reverse channel to request the retransmission of data. The first FEC code, called a Hamming code, was introduced in the early 1950s. It is a method adopted to obtain error control in data transmission where the transmitter sends redundant data. Only a portion of the data without apparent errors is recognized by the receiver. This allows broadcasting data to be sent to multiple destinations from a single source. Forward error coding is also known as channel coding.

b) Received code is 11110101101. We perform the parity check for even.

Hamming code	P_1	P_2	m_1	P_3	m_2	m_3	m_4	P_4	m_5	m_6	m_7	Even parity check
Bit positions	1	2	3	4	5	6	7	8	9	10	11	
Received hamming code	1	1	1	1	0	1	0	1	1	10	1	
First parity check	1		1		0		0		1		1	Pass
Second parity check		1	1			1	0			0	1	Pass
Third parity check				1	0	1	0					Pass
Fourth parity check								1	1	0	1	fail 8

Fourth parity check is failed for even parity. There is error in 8th position bit. The received value for 8th position bit is 1. So we can change it to 0.
The original code was = 111101010101

c) i) As the figure below shows, from sender to receiver, frame 1 is lost, but sender is still expecting the ACK 0 back. After timer time out, frame 1 sends again.

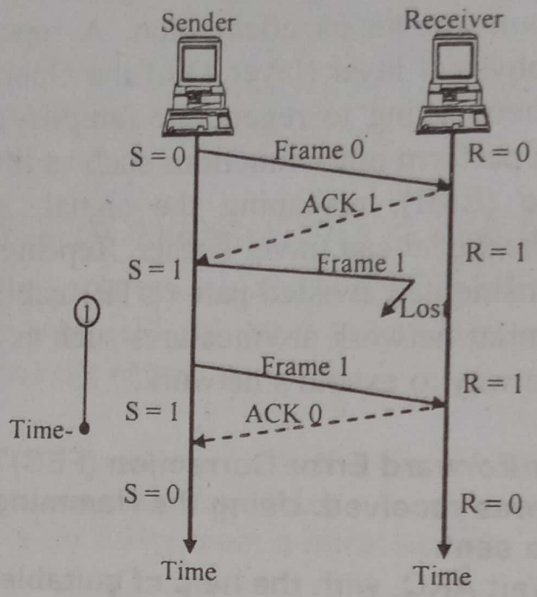


Fig: Stop-and-wait ARQ lost frame

ii) As the figure below shows, when ACK 0 sends back to sender, this frame has lost. So after time out, frame 1 sends again. Receiver side is excepting for frame 0, so frame 1 is discarded.

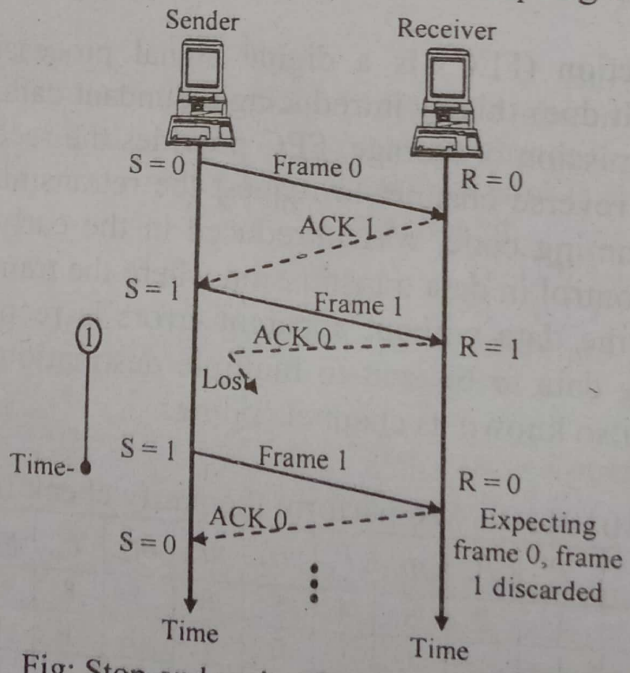


Fig: Stop-and-wait ARQ lost ACK[] [1]

iii) Frame 0 sends to receiver, ACK 1 sends back to Sender, but the transmission has delayed. After time out, sender sends frame 0 again; receiver is excepting frame 1. Therefore, the frame 0 is discarded, ACK 1 is discarded. Frame 1 sends again.

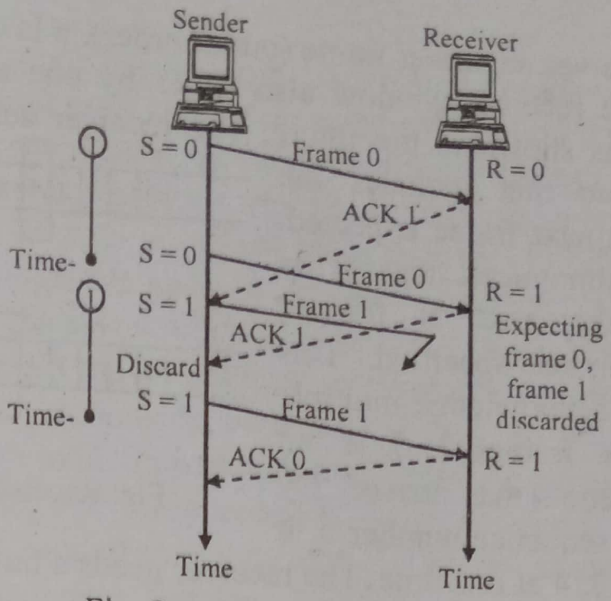


Fig: Stop-and-wait ARQ delayed

8. Discuss the concept of sliding window in detail with the help of an example. How does HDLC perform flow control? **[WBUT 2015]**

Answer:

1st Part: Sliding window algorithm is a method of flow control for network data transfers. TCP, the Internet's stream transfer protocol, uses a sliding window algorithm. A sliding window algorithm places a buffer between the application program and the network data flow. For TCP, the buffer is typically in the operating system kernel, but this is more of an implementation detail than a hard-and-fast requirement.

Data received from the network is stored in the buffer, from where the application can read at its own pace. As the application reads data, buffer space is freed up to accept more input from the network. The window is the amount of data that can be "read ahead" - the size of the buffer, less the amount of valid data stored in it. Window announcements are used to inform the remote host of the current window size.

Sender sliding Window: At any instant, the sender is permitted to send frames with sequence numbers in a certain range (the sending window) as shown in Figure below.

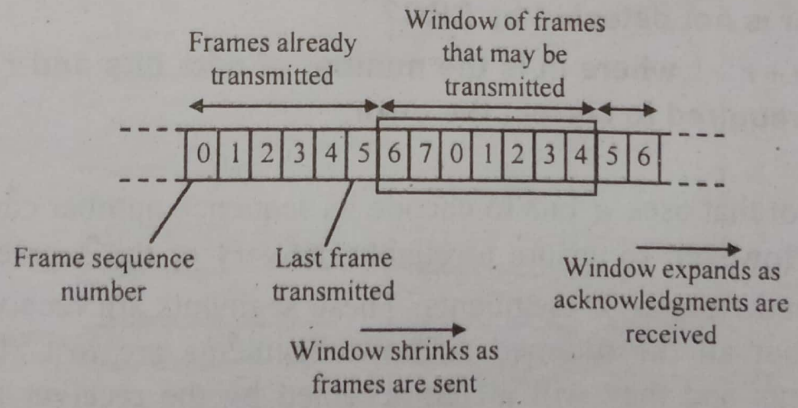


Fig: Sender's window

Receiver sliding Window: The receiver always maintains a window of size 1 as shown in Figure below. It looks for a specific frame (frame 4 as shown in the figure) to arrive in

a specific order. If it receives any other frame (out of order), it is discarded and it needs to be resent. However, the receiver window also slides by one as the specific frame is received and accepted as shown in the figure. The receiver acknowledges a frame by sending an ACK frame that includes the sequence number of the next frame expected. This also explicitly announces that it is prepared to receive the next N frames, beginning with the number specified. This scheme can be used to acknowledge multiple frames. It could receive frames 2, 3, 4 but withhold ACK until frame 4 has arrived. By returning an ACK with sequence number 5, it acknowledges frames 2, 3, 4 at one time. The receiver needs a buffer of size 1.

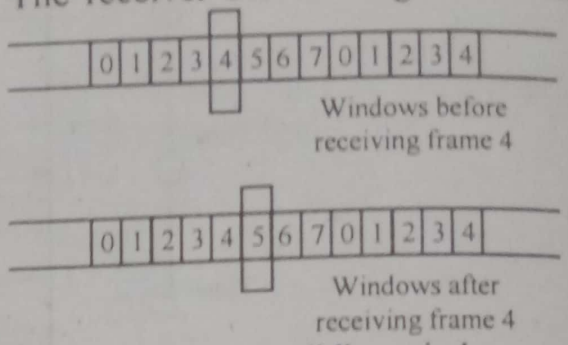


Fig: Receiver sliding window

2nd Part:

Short for High-level Data Link Control, a transmission protocol used at the data link layer (layer 2) of the OSI seven layer model for data communications. The HDLC protocol embeds information in a data frame that allows devices to control data flow and correct errors. HDLC is an ISO standard developed from the Synchronous Data Link Control (SDLC) standard proposed by IBM in the 1970's.

For any HDLC communications session, one station is designated primary and the other secondary. A session can use one of the following connection modes, which determine how the primary and secondary stations interact.

- **Normal unbalanced:** The secondary station responds only to the primary station.
- **Asynchronous:** The secondary station can initiate a message.
- **Asynchronous balanced:** Both stations send and receive over its part of a duplex line. This mode is used for X.25 packet-switching networks.

9. a) Why window size of the Go-Back-N protocol is $2^n - 1$, where n is the number of bits requited to identify the sequence number of the data frame?

b) What type of error is not detected by CRC?

c) Prove that $2^r \geq m + r + 1$, where m is the number of data bits and *r* is the number of redundancy bits required to correct the error. **[WBUT 2016]**

Answer:

a) A transport protocol that uses n bits to encode its sequence number can send up to 2^n different segments. However, to ensure a reliable delivery of the segments, go-back-n and assume that a sender sends 2^n segments. These segments are received in-sequence by the destination, but all the returned acknowledgements are lost. The sender will retransmit all segments and they will all be accepted by the receiver and delivered a second time to the user. It is easy to see that this problem can be avoided if the maximum size of the sending window is $2^n - 1$ segments.

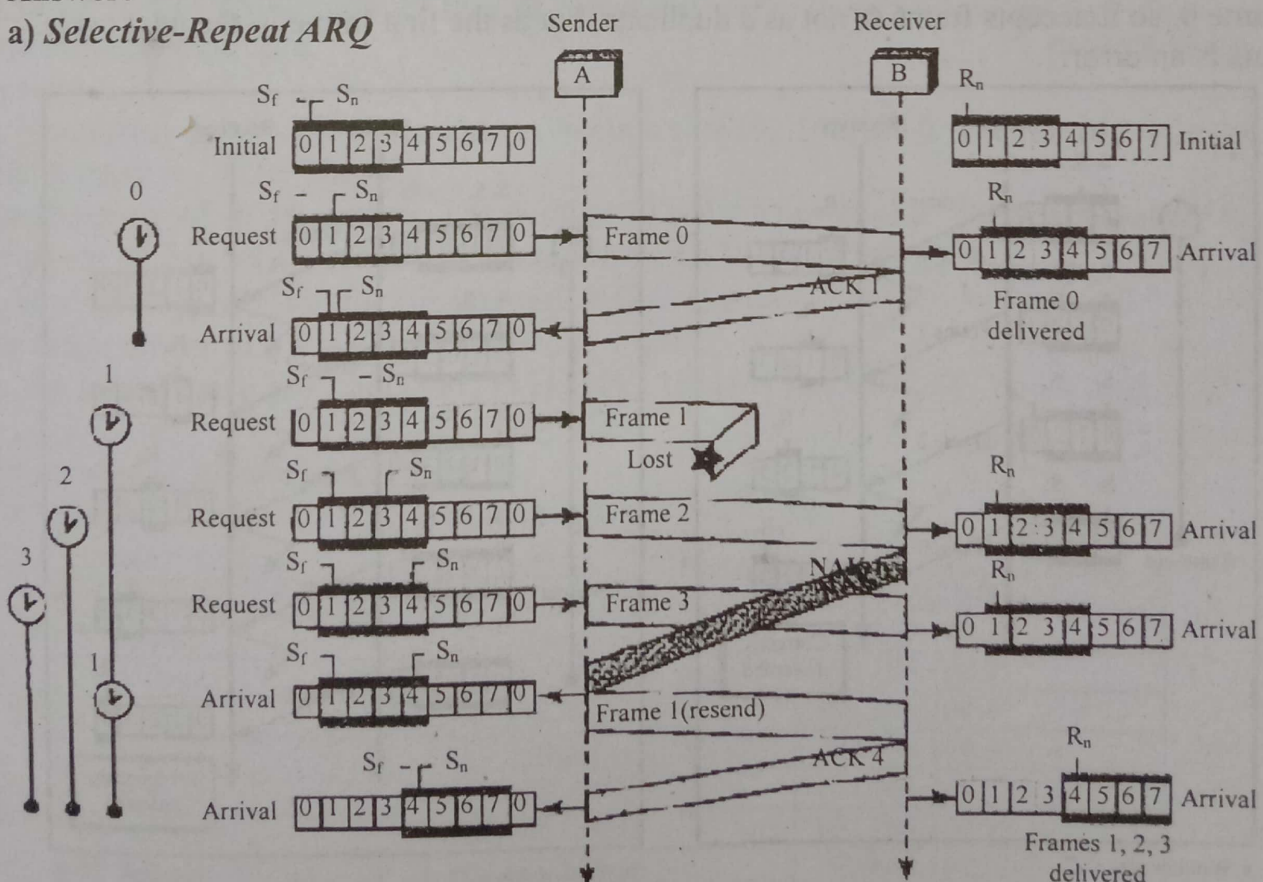
b) n-bit CRC will not detect burst errors that are of length greater than n.

c) Concept of error-correction can be easily understood by examining the simplest case of single-bit errors. Single-bit error can be detected by addition of a parity bit (VRC) with the data, which needed to be send. A single additional bit can detect error, but it's not sufficient enough to correct that error too. For correcting an error one has to know the exact position of error, i.e. exactly which bit is in error (to locate the invalid bits). For example, to correct a single-bit error in an ASCII character, the error correction must determine which one of the seven bits is in error. To this, we have to add some additional redundant bits. To calculate the numbers of redundant bits (r) required to correct m data bits, let us find out the relationship between the two. So we have (m+r) as the total number of bits, which are to be transmitted; then r must be able to indicate at least m+r+1 different values. Of these, one value means no error, and remaining m+r values indicate error location of error in each of m+r locations. So, m+r+1 states must be distinguishable by r bits, and r bits can indicates 2^r states. Hence, 2^r must be greater than m+r+1.
$2^r >= m+r+1$ The value of r must be determined by putting in the value of m in the relation. For example, if m is 7, then the smallest value of r that satisfies the above relation is 4. So the total bits, which are to be transmitted is 11 bits (m+r = 7+4 =11).

10. a) How selective-repeat ARQ will work for lost frame?
b) In Go-Back-N ARQ show why the window size should be < 2m.
c) Applying CRC algorithm determine the transmitted frame 10101000 where the generator polynomial is $x^3 + x + 1$.
d) Compare bit stuffing with byte stuffing with an example. **[WBUT 2017]**

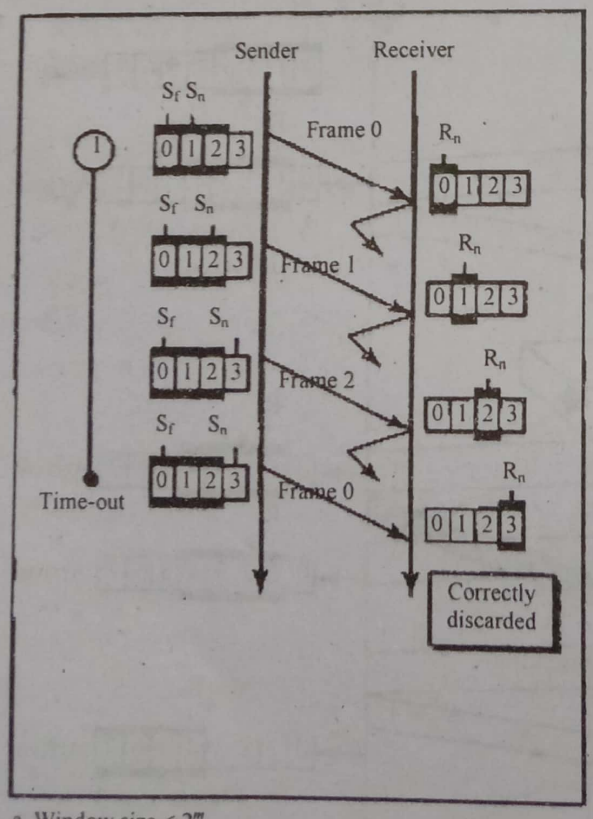
Answer:

a) ***Selective-Repeat ARQ***

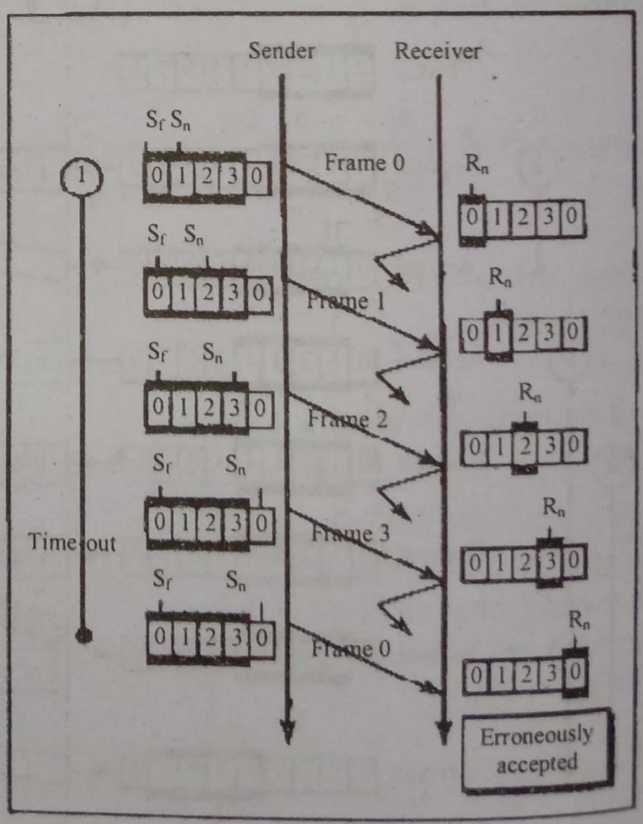


Here, each frame sent or resent needs a timer, which means that the timers need to be numbered (0, 1, 2 and 3). The timer for frame 0 starts at the first request, but stops when the ACK for this frame arrives. The timer for frame 1 starts at the second request, restarts when a NAK arrives, and finally stops when the last ACK arrives. The other two timers start when the corresponding frames are sent and stop at the last arrival event.
At the receiver site, the acceptance of a frame and its delivery to the network layer need to be distinguished. At the second arrival, frame 2 arrives and is stored and marked, but it cannot be delivered because frame 1 is missing. At the next arrival, frame 3 arrives and is marked and stored, but still none of the frames can be delivered. Only at the last arrival, when finally a copy of frame 1 arrives, can frame 1, 2, and 3 be delivered to the network layer. There are two conditions for the delivery of frames to the network layer: First, a set of consecutive frames must have arrived. Second, the set starts from the beginning of the window. After the first arrival, there was only one frame and it started from the beginning of the window. After the last arrival, there are three frames and the first one starts from the beginning of the window.

b) In a Go-Back-N ARQ, the size of the send window must be less than 2m. As an example, we choose m = 2, which means the size of the window can be 2m – 1, or 3. The figure below compares a window size of 3 against a window size of 4. If the size of the window is 3 (less than 22) and all three acknowledgements are lost, the frame 0 timer expires and all three frames are resent. The receiver is now expecting frame 3, not frame 0, so the duplicate frame is correctly discarded. On the other hand, if the size of the window is 4 (equal to 22) and all acknowledgements are lost, the sender will send a duplicate of frame 0. However, this time the window of the receiver expects to receive frame 0, so it accepts frame 0, not as a duplicate, but as the first frame in the next cycle. This is an error.



a. Window size < 2^m



b. Window size = 2^m

c) x^3+x+1 gives the binary divisor 1011.

$$
\begin{array}{r}
x^3\ x^2\ x^1\ x^0 \\
1\ \ 0\ \ 1\ \ 1 \\
1011\overline{)10101000000}\ (1001110 \\
\underline{1011} \\
1100 \\
\underline{1011} \\
1110 \\
\underline{1011} \\
1010 \\
\underline{1011} \\
100 \text{ — remainder}
\end{array}
$$

∴ The transmitted frame will be 10101000100.

d) *Refer to Question No. 10 of Short Answer Type Questions.*

11. a) A company is granted the site with the address 192.168.100.0. The company needs 10 subnets. Design the subnets (which include subnet mask number of subnets, number of hosts in each subnet, first and last address of each subnet).
b) What is the advantage of two dimensional parity over simple parity? Explain with suitable example. **[WBUT 2019]**

Answer:

a) A company granted to a site address in class C = 192.168.100.0. The no. of 1's in the default mask is 24 (for class C)

The company needs 10 subnets. The number 10 is not a power of 2. The next number i.e., the power of 2 is 16(2^4). Hence, we need 4 more 1's in the subnet mask.

∴ Total number of 1's in the subnet mask is (24+4) = 28

The total number of 0's is (32 – 28) = 4

So, the subnet mask is – 11111111. 11111111 . 11111111 . 11110000

255 . 255 . 255 . 240

The number of subnets is = 2^4 = 16

The number of addresses (hosts) in each subnet is = 2^4 = 16

The 1st and last address of each subnet is as follows:

Subnet No.	First Address	Last
1st Subnet	192.168.100.0	192.168.100.15
2nd Subnet	192.168.100.16	192.168.100.31
3rd Subnet	192.168.100.32	192.168.100.47
4th Subnet	192.168.100.48	192.168.100.63
5th Subnet	192.168.100.64	192.168.100.79
6th Subnet	192.168.100.80	192.168.100.95
7th Subnet	192.168.100.96	192.168.100.111

Subnet No.	First Address	Last
8th Subnet	192.168.100.112	192.168.100.127
9th Subnet	192.168.100.128	192.168.100.143
10th Subnet	192.168.100.144	192.168.100.159

b) *Refer to Question No. 4 (b) of Long Answer Type Questions.*

12. Write a short note on Traditional Ethernet. **[WBUT 2015]**

Answer:

Local-area networks have been well-served by Ethernet for 40 years. It works just fine within the framework of a traditional, physical network architecture. However, this technology is beginning to show its age – and its limitations – thanks to the emergence of virtualization and cloud computing.

Traditional Ethernet is beginning to give way to Ethernet fabric, a younger, smarter upstart that promises to provide the performance, scalability, flexibility and manageability required to take full advantage of today's virtualized data centers. Ethernet fabric simplifies the switching architecture to improve traffic flow and bandwidth efficiency in virtual environments, where applications are expected to be deployed in minutes instead of months.

The problems with traditional Ethernet are, ethernet uses Spanning Tree Protocol to route traffic "north-south," or up and down the tree, between switches on a single, predefined path. Server virtualization requires "east-west" traffic between multiple servers, making traditional Ethernet prone to latency. Because there is only one active path between switches, bandwidth inefficiencies of 50 percent or more are common in traditional Ethernet environments. This bottleneck becomes more pronounced in a virtualized data center, where network traffic is highly concentrated.

A classic Ethernet network also utilizes static network policies, each configured to an individual physical switch port. A virtual machine and its applications tend to move from server to server on different switch ports, while the static network policy remains attached to its original port. To prevent downtime, configurations must be manually adjusted, which negates the agility and on-demand nature of virtualization.

Traditional Ethernet supports data transfers at the rate of 10 megabits per second (Mbps). As the performance needs of networks increased over time, the industry created additional Ethernet specifications for Fast Ethernet and Gigabit Ethernet. Fast Ethernet extends traditional Ethernet performance up to 100 Mbps and Gigabit Ethernet up to 1000 Mbps speeds. Although products aren't yet available to the average consumer, 10 Gigabit Ethernet (10,000 Mbps) also exist and are used on some business networks and onInternet2.

MEDIUM ACCESS SUB LAYER

Multiple Choice Type Questions

1. How much channel throughput of slotted ALOHA will be in comparison to pure Aloha? [WBUT 2008, 2012]
   a) Same b) Double c) Three times d) None of these
   Answer: (b)

2. PPP is a ..... oriented protocol. [WBUT 2010]
   a) phase b) bit c) byte d) none of these.
   Answer: (c)

3. Token passing is a technique applied in [WBUT 2015]
   a) Data link layer b) Transport layer
   c) Physical layer d) Presentation layer
   Answer: (a)

4. Base-FL is a version of [WBUT 2015]
   a) Ethernet b) Token Bus c) Token Ring d) Wireless LAN
   Answer: (a)

5. Which of the following could not be an Ethernet unicast destination? [WBUT 2019]
   a) 43-7B-6C-DE-10-00 b) 44-AA-C1-23-45-32
   c) 46-56-21-1A-DE-F4 d) 48-32-21-21-4D-34
   Answer: (a)

Short Answer Type Questions

1. Why bit stuffing is needed in HDLC frame? [WBUT 2006, 2010]

Answer:

Bit stuffing is the insertion of one or more bits into a transmission unit as a way to provide signaling information to a receiver. The receiver knows how to detect and remove or disregard the stuffed bits.

For example, the timing or bit rate of T-carrier system signals is constantly synchronized between any terminal device and an adjacent repeater or between any two repeaters. The synchronization is achieved by detecting the transition in polarity for 1 bits in the data stream. (T-1 signaling uses bipolar signaling, where each successive bit with a value of 1 is represented by voltage with a reverse polarity from the previous bit. Bits with a value of 0 are represented by a no-voltage time slot). If more than 15 bits in a row are sent with a 0 value, this "lull" in 1 bits that the system depends on for synchronization may be long enough for two end points to become out of synchronization. To handle this situation (the sequence of more than 150 bits), the signal is "stuffed" with a short, unique bit pattern

(which includes some 1 bits) that is recognized as a synchronization pattern. The receiving end removes the stuffed bits and restores the bit stream to its original sequence. In another example of bit stuffing, a standard HDLC packet begins and ends with 01111110. To make sure this sequence doesn't appear again before the end of the packet, a 0 is inserted after every five consecutive 1s.
Bit stuffing is defined by some to include bit padding, which is the addition of bits to a transmission to make the transmission unit conform to a standard size, but is distinct from bit robbing, a type of in-band signaling.

2. Analyze the performance of pure ALOHA. How does slotted ALOHA improve performance over pure ALOHA. In both the cases find the expression for average delay and throughput. Compare the performance of pure ALOHA with slotted ALOHA. **[WBUT 2007]**

OR,

Find the expressions for average delay and throughput for both pure ALOHA and slotted ALOHA. Compare their performances as well. **[WBUT 2011, 2013]**

OR,

Derive the expression of throughput for ALOHA. **[WBUT 2014]**

OR,

Discuss in detail about the mechanism of multiple access provided by pure ALOHA. Why the efficiency of slotted ALOHA gets doubled compared to pure ALOHA? Explain. **[WBUT 2015]**

OR,

Explain ALOHA and Slotted ALOHA. Compare between them. **[WBUT 2017]**

Answer:

Suppose the stations generate frames following a Poisson distribution of mean S frames per second. Also, the probability of k transmissions attempts per time frame is a Poisson distribution with mean G per frame time, i.e.

$\mathbf{P(k) = Gk\ e^{-G}/k!}$

Thus, $\mathbf{P(No\ frames\ generated\ in\ frame\ duration) = e^{-G}}$

Now, throughput = G * P(transmission is successful)

Hence, $\mathbf{S = GP(0)}$

Collision happens if another frame is generated during twice the time duration of a frame.

This is $\mathbf{P(0) = e^{-2G}}$

Solving for S we get

$\mathbf{S = Ge^{-2G}}$

Maximum throughput occurs at G = 0.5, where $\mathbf{S = 1/2e = 0.184}$

In slotted ALOHA, we need to check for collision only within duration of frame because no new frame can start within that time (collision can happen at the beginning only). This gives us:

$\mathbf{S = Ge^{-2G}}$

Where maximum $\mathbf{S = 1/e = 0.368}$

Comparison:

a) Pure Aloha is a Continuous time system whereas Slotted Aloha is discrete time system.

b) Pure ALOHA doesn't check whether the channel is busy before transmission. Slotted ALOHA send the data at the beginning of timeslot.

c) Pure aloha not divided in to time .Slotted aloha divided in to time.

3. What are the basic differences between Pure ALOHA and Slotted ALOHA? Draw the flowchart of CSMA/CD protocol. **[WBUT 2009]**

OR,

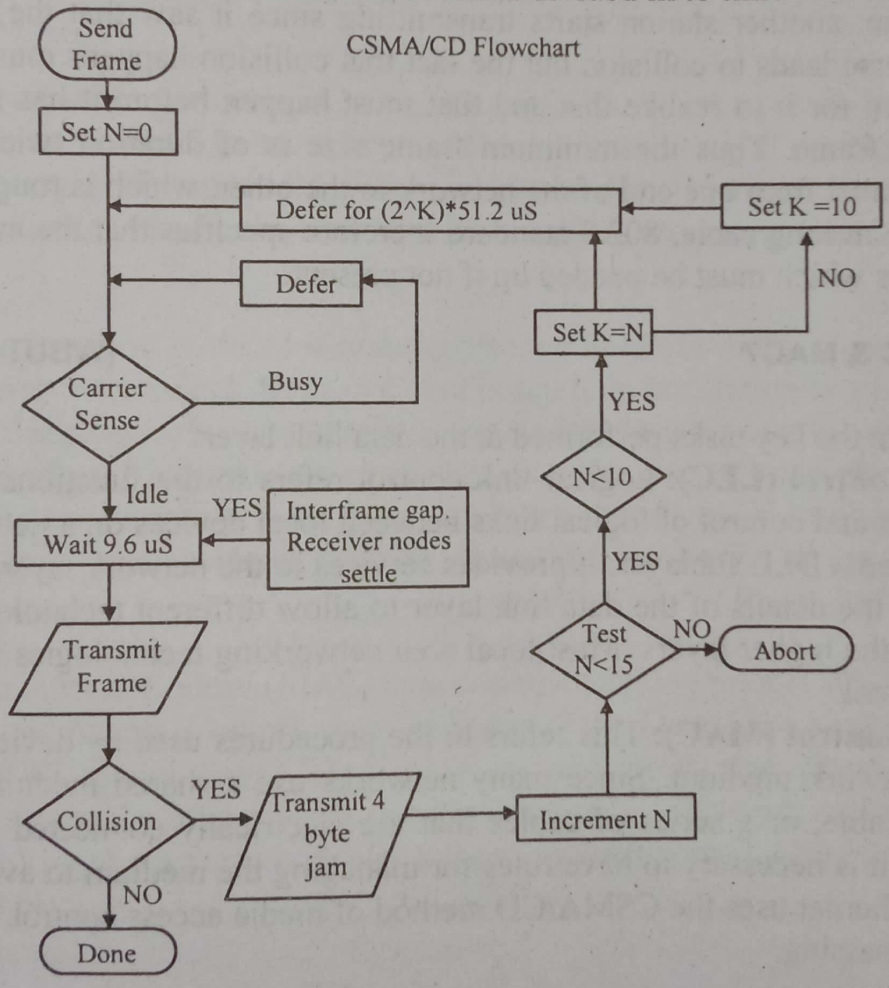
What are the differences between pure ALOHA & slotted ALOHA? **[WBUT 2014]**

Answer:

1) Pure Aloha is a Continuous time system whereas Slotted Aloha is discrete time system.

2) Pure ALOHA doesn't check whether the channel is busy before transmission. Slotted ALOHA send the data at the beginning of timeslot.

3) Pure aloha not divided in to time. Slotted aloha divided in to time



4. Describe 802.3 header format. Why padding is required? **[WBUT 2012, 2019]**

Answer:

Ethernet traffic is transported in units of a frame, where each frame has a definite beginning and end. The form of the frame is in the figure below.

Preamble	Dest Addr	Src Addr	Type	Data	CRC

- **The Preamble Field** (8 bytes, 64 bits) is used for synchronization. The first seven bytes contain the bit pattern 10101010 and the eighth contain the pattern 10101011.
- **Destination Address** specifies the Ethernet address of the destination station, 48-bits
- **Source Address** specifies Ethernet address of the source station, 48-bits
- **Type** field specifies the type of data encapsulated, e.g. IP, ARP, RARP, etc, 16-bits.
- **Data Field** carries 46-1500 bytes of data. If data length is lower than 46 bytes, it must be padded to 46 bytes.
- **CRC** or Cyclical Redundancy Check, used for error detection

The reason why there is an upper limit to the length of the data field, is fairly obvious --- so that each station gets a fair chance with the channel. The lower limit, and the reason for padding in case that limit is not met, is as follows:

Suppose a station at one extreme of sends a very short frame. Before this frame reaches the other extreme, another station starts transmitting since it saw that the channel was free. This of course leads to collision but the fact that collision happens must travel back to the first station for it to realize that and that must happen before it has finished with transmitting the frame. Thus the minimum frame size is of duration twice the time a signal takes to travel from one end of the network to the other, which is roughly 5 micro-seconds on a 1 Km long cable. 802.3 standard therefore specifies that the minimum data length is 46 bytes which must be padded up if not present.

5. What are LLC & MAC? **[WBUT 2016, 2019]**

Answer:

The following are the key tasks performed at the data link layer:

Logical Link Control (LLC): Logical link control refers to the functions required for the establishment and control of logical links between local devices on a network. This is usually considered a DLL sublayer; it provides services to the network layer above it and hides the rest of the details of the data link layer to allow different technologies to work seamlessly with the higher layers. Most local area networking technologies use the IEEE 802.2 LLC protocol.

Media Access Control (MAC): This refers to the procedures used by devices to control access to the network medium. Since many networks use a shared medium (such as a single network cable, or a series of cables that are electrically connected into a single virtual medium) it is necessary to have rules for managing the medium to avoid conflicts. ***For example:*** Ethernet uses the CSMA/CD method of media access control, while Token Ring uses token passing.

Long Answer Type Questions

1. a) What do you mean by channel utilization? **[WBUT 2008]**

b) Discuss and differentiate persistent CSMA and non- persistent CSMA? **[WBUT 2008, 2013]**

c) Why are medium access control techniques required?

List three popular medium access control techniques. [WBUT 2008, 2011, 2012, 2018]

d) A 1 km 10 Mbps CSMA/ CD LAN has a propagation speed of 200 m/μ sec. Data frames are 256 bits long including 32 bits of header, checksum and other overhead. The first bit slot after a successful transition is reserved for the receiver to capture the channel to send a 32 bit acknowledge frame. What is the affective data rate excluding overhead assuming there is no collusion. [WBUT 2008]

Answer:

a) Channel utilization means channel throughput.

In communication networks, throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

b) Protocols in which station listens for a carrier and act accordingly are called as carrier sense protocols.

The first carrier sense protocols is 1-persistant CSMA. When a station has data to send, it first listens to the channel to see if anyone else is transmitting. If the channel is busy, the station waits until it becomes idle. When the station detects an idle channel, it transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again.

A second carrier sense protocol is non-persistent CSMA. In this protocol, before sending a station senses the channel. If no one else is sending, the station begins doing so itself. However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. Instead, it waits a random period of time and then repeats the algorithm. Intuitively, this algorithm should lead to better channel utilization and longer delays then 1-persistent CSMA.

c) The Media Access Control (MAC) data communication protocol sub-layer, also known as the Medium Access Control, is a sublayer of the Data Link Layer specified in the seven-layer OSI model (layer 2). It provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multi-point network, typically a local area network (LAN) or metropolitan area network (MAN).

CSMA
CSMA/CD
CSMA/CA

d) Round trip propagation time $= \frac{1000\,\text{mtr} \times 2}{200} = 10\ \text{m/}\mu\text{sec.}$

Transmission can be divided into 6 stages.

i) Sender size cable T_1 = round trip propagation time $= 10\ \mu\text{sec.}$

ii) Data frame transmission, $T_2 = \frac{256}{10}\ \text{Mbps} = 25.6\ \text{Mbps.}$

iii) Delay for last bit to reach the end, $T_3 = \frac{1000\,\text{mtr}}{200\,\text{mtr/}\mu\text{sec}} = 5\mu\text{sec}$

iv) Acknowledgement frame transmission, $T_5 = 32\,\text{bit}/10\text{Mbps} = 3.2\ \mu\text{sec.}$

v) Delay for last bit to reach end

$T_6 = T_3 = 5\ \mu\text{sec.}$

$\therefore \quad T = T_1 + T_2 + T_3 + T_4 + T_5 + T_6 = 10 + 25.6 + 5 + 10 + 3.2 + 5 = 58.5\ \mu\text{sec.}$

Effective data rate $= \frac{(256 - 32)\,\text{bit}}{58.8\ \mu\text{sec}} = 3.8\ \text{Mbps.}$

2. a) Explain CDMA technique with a suitable example.
b) How is CSMA a clear improvement over ALOHA? How is it further improved by implementing CSMA/CD?
c) Suppose in a CSMA/CD LAN, the maximum end to end propagation delay is 25.6 μsecond. If the LAN is operating in 100Mbps, then what will be the minimum frame length (in bytes) of the LAN? **[WBUT 2010]**

Answer:

a) In cellular service there are two main competing network technologies: Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA).

One of the basic concepts in data communication is the idea of allowing several transmitters to send information simultaneously over a single communication channel. This allows several users to share a band of frequencies (see bandwidth). This concept is called multiplexing. CDMA employs spread-spectrum technology and a special coding scheme (where each transmitter is assigned a code) to allow multiple users to be multiplexed over the same physical channel. By contrast, time division multiple access (TDMA) divides access by time, while frequency-division multiple access (FDMA) divides it by frequency. CDMA is a form of spread-spectrum signaling, since the modulated coded signal has a much higher data bandwidth than the data being communicated.

b) In both slotted and pure ALOHA, a node's decision to transmit is made independently of the activity of the other nodes attached to the broadcast channel. In particular, a node neither pays attention to whether another node happens to be transmitting when it begins to transmit, nor stops transmitting if another node begins to interfere with its transmission.

Listen before speaking: If someone else is speaking, wait until they are done. To the channel before transmitting if a frame from another node is currently being transmitted into the channel, a node then waits ("backs off") a random amount of time and then again senses the channel. If the channel is sensed to be idle, the node then begins frame transmission. Otherwise, the node waits another random amount of time and repeats this process.

In CSMA, the "listen before speaking" principle is employed. A node listens to the channel before transmitting. If a frame from another node is currently being transmitted, a node "backs off" for some (random) time before sensing if the channel has become idle and so on.

In CSMA/CD, additionally "collision-detection" is employed. A node additionally checks whether a frame put on the channel "collides" with another frame transmitted by another channel. In such a case the node again "backs off" and repeats listening before speaking.

c) RTT = 51.2 μsecond

Minimum frame length = (100 Mbps * 51.2 μs) = 5120 bits = 640 octets.

3. a) Differentiate between FHSS and DSSS spread spectrum. [WBUT 2010]

b) Discuss the 802.11 protocol. Draw the lower two layers of the IEEE 802.11 protocol. What are the functions of DCF and PCF?

c) What is the difference between bit oriented and byte oriented protocols?

Answer:

a) FHSS (Frequency-hopping spread spectrum) is typically used by wireless mobile devices such as blue tooth and wireless phones. The transmission distance of FHSS is shorter and not very reliable. DSSS is used by wireless immobile devices. The transmission speed of DSSS is faster than FHSS and is more reliable.

b) The original 802.11 standard had two variations both offering the same speeds but differing in the RF spread spectrum used. One of the 802.11 used FHSS. This 802.11 variant used the 2.4 GHz radio frequency band and operated with a 1 or 2 Mbps data rate. Since this original standard, wireless implementations have favored DSSS.

The second 802.11 variation used DSSS and specified a 2 Mbps-peak data rate with optional fallback to 1 Mbps in very noisy environments. 802.11, 802.11b and 802.11g use the DSSS spread spectrum, this means that the underlying modulation scheme is very similar between each standard, enabling all DSSS systems to coexist with 2, 11 and 54 Mbps 802.11 standards. Because of the underlying differences between 802.11a and the 802.11b/g, they are not compatible.

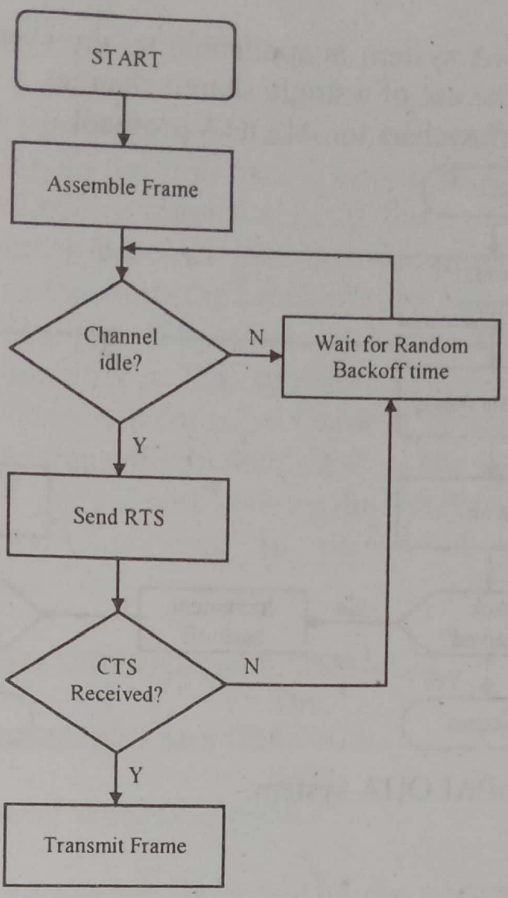
Distributed coordination function (DCF) is the fundamental MAC technique of the IEEE 802.11 based WLAN standard. DCF employs a CSMA/CA with Binary exponential backoff algorithm.

DCF requires a station wishing to transmit to listen for the channel status for a DIFS interval. If the channel is found bust during the DIFS interval, the station defers its transmission. In a network where a number of stations contend for the wireless medium. If multiple stations sense the channel busy and defer their access, they will also virtually

simultaneously find that the channel is released and then try to seize the channel. As a result, collisions may occur. In order to avoid such collisions, DCF also specifies random backoff, which forces a station to defer its access to the channel for an extra period.
Point coordination function (PCF) is a Media Access Control (MAC) technique used in IEEE 802.11 based WLANs. It resides in a point coordinator also known as Access Point (AP), to coordinate the communication within the network. The AP waits for PIFS duration rather than DIFS duration to grasp the channel. PIFS is less than DIFS duration and hence the point coordinator always has the priority to access the channel.
The PCF is located directly above the Distributed Coordination Function (DCF), in the IEEE 802.11 MAC Architecture. Channel access in PCF mode is centralized and hence the point coordinator sends CF-Poll frame to the PCF capable station to permit it to transmit a frame. In case the polled stations does not have any frames to send, then it must transmit null frame.

c) In bit oriented Protocol, a flag is used to frame the bits sent. Simply put, you have a flag (01111110) and the required bits are sent after the flag and you end the transmission again with a flag. Using this method you can send any number of bits of any length. Another important fact is the zero insertion method used. Say for example, you want to send the bit string 01111110. You cannot do this because it will be interpreted as a flag. However, by adding a zero after 5 consecutive 1's as a standard, this bit stream can be send. The transmitter sends the string as 011111010 and the receiver removes the zero after 5 consecutive 1's and stores the data as 01111110.
In byte oriented protocol (character oriented protocol) the receiver considers 8 bits at a time and figures out the relevant character. This system is used when communicating with printers and keyboards which use ASCII characters exclusively. (All the ASCII characters can be covered by 8 bits (256 characters). The main disadvantage of COP is that you cannot send 9 or 10 bits, arbitrary bits. Furthermore, in COP there are special characters – channel control characters, e.g. SYN character which is used to synchronize the receiver and the transmitter. These characters cannot be transferred as data. They will be misread as control characters.

4. a) Discuss CSMA/CA with the help of a flowchart. **[WBUT 2012, 2019]**
b) Why is CSMA/CD not implemented in WLAN? **[WBUT 2012, 2019]**
Answer:
a) When station receives data to transmit, it converts it into frames of appropriates size. Then it waits to see if the channel is idle and backs of for a random time if not idle. When the channel becomes idle, the station transmits a special sequence called "Request to Send" (RTS) to the receiver and awaits for a short while for the receiver in turn to send the special "Clear to Send" (CTS) sequence. Only upon receiving a CTS does the station transmits frames. Or else, it again backs off.



The flow chart for CSMA/CA is given above.

b) In Wireless LAN, a transmitter never gets to know whether its data got corrupted while on way. That is, it never can detect collision. Hence, CSMA/CD, which is based on collision detection, is based on collision detection, is not used in WLAN.

5. a) What are random access & controlled access? **[WBUT 2014]**

Answer:

In controlled access methods, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. Three popular controlled-access methods: reservation, polling, and token passing.

In random access methods, there is no access control (as there is in controlled access methods) and there is no predefined channels (as in channelization). Each station can transmit when it desires. This liberty may create collision.

b) Describe ALOHA with flowchart. **[WBUT 2014]**

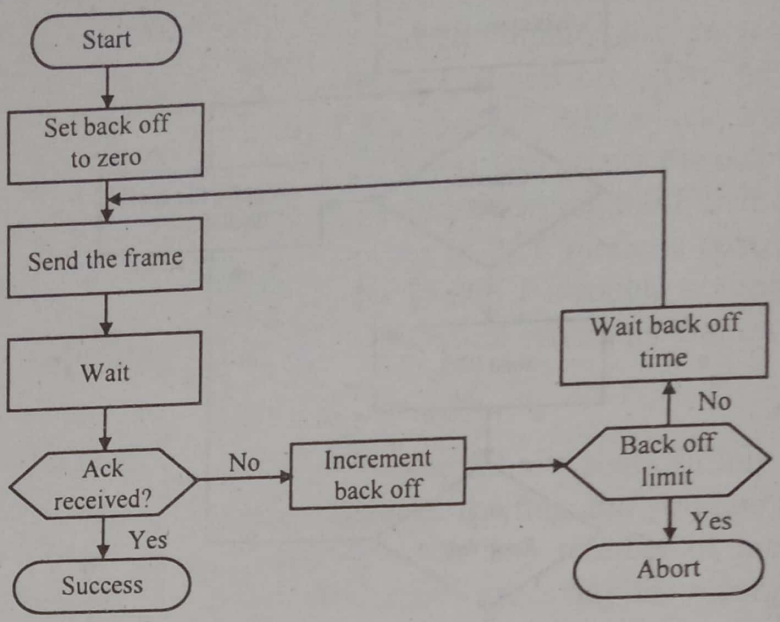
Answer:

ALOHA

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.
Figure below shows the flowchart for ALOHA protocol.



There are two versions of ALOHA system.
1. Pure ALOHA
2. Slotted ALOHA

c) What are non-persistence, l-persistence & p-persistence strategies? **[WBUT 2014]**

OR,

Discuss about the various persistence strategies provided by CSMA. [WBUT 2015]

Answer:

1-persistent

1-persistent CSMA is an aggressive transmission algorithm. When the sender (station) is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits the message (a frame) unconditionally (i.e. with probability=1). In case of a collision, the sender waits for a random period of time and attempts to transmit again unconditionally (i.e. with probability=1). 1-persistent CSMA is used in CSMA/CD systems including Ethernet.

Non-persistent

Non persistent CSMA is a non aggressive transmission algorithm. When the sender (station) is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it waits for a random period of time (during which it does not sense the transmission medium) before repeating the whole logic cycle (which started with sensing the transmission medium for idle or busy) again. This approach reduces collision, results in overall higher medium throughput but with a penalty of longer initial delay compared to 1–persistent.

P-persistent

This is an approach between 1-persistent and non-persistent CSMA access modes. When the sender (station) is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits a frame with probability *p*. If the sender chooses not to transmit (the probability of this event is *1-p*), the sender waits until the next available time slot. If the transmission medium is still not busy, it transmits again with the same probability *p*. This probabilistic hold-off repeats until the frame is finally transmitted or when the medium is found to become busy again (i.e. some other sender has already started transmitting their data). In the latter case the sender repeats the whole logic cycle (which started with sensing the transmission medium for idle or busy) again. p-persistent CSMA is used in CSMA/CA systems including Wi-Fi and other packet radio systems.

d) Compare and contrast CSMA/CA with CSMA/CD. **[WBUT 2014, 2016]**

OR,

Differentiate between CSMA/CD and CSMA/CA. **[WBUT 2018]**

OR,

How does CSMA/CD differ from CSMA/CA? **[WBUT 2018]**

Answer:

Carrier Sense Multiple Access or CSMA is a Media Access Control (MAC) protocol that is used to control the flow of data in a transmission media so that packets do not get lost and data integrity is maintained. There are two modifications to CSMA, the CSMA CD (Collision Detection) and *CSMA CA (Collision Avoidance)*, each having its own strengths.

CSMA operates by sensing the state of the medium in order to prevent or recover from a collision. A collision happens when two transmitters transmit at the same time. The data gets scrambled, and the receivers would not be able to discern one from the other thereby causing the information to get lost. The lost information needs to be resent so that the receiver will get it.

CSMA CD operates by detecting the occurrence of a collision. Once a collision is detected, CSMA CD immediately terminates the transmission so that the transmitter does not have to waste a lot of time in continuing. The last information can be retransmitted. In comparison, CSMA CA does not deal with the recovery after a collision. What it does is to check whether the medium is in use. If it is busy, then the transmitter waits until it is idle before it starts transmitting. This effectively minimizes the possibility of collisions and makes more efficient use of the medium.

Another difference between CSMA CD and CSMA CA is where they are typically used. CSMA CD is used mostly in wired installations because it is possible to detect whether a collision has occurred. With wireless installations, it is not possible for the transmitter to detect whether a collision has occurred or not. That is why wireless installations often use CSMA CA instead of CSMA CD.

6. a) Discuss in detail about the connection establishment procedure performed by LCP with the help of various LCP packets.
b) Explain in detail the state transition diagram of PPP.
c) Discuss the mechanism for authentication provided by Challenge Handshake Authentication Protocol. **[WBUT 2015]**

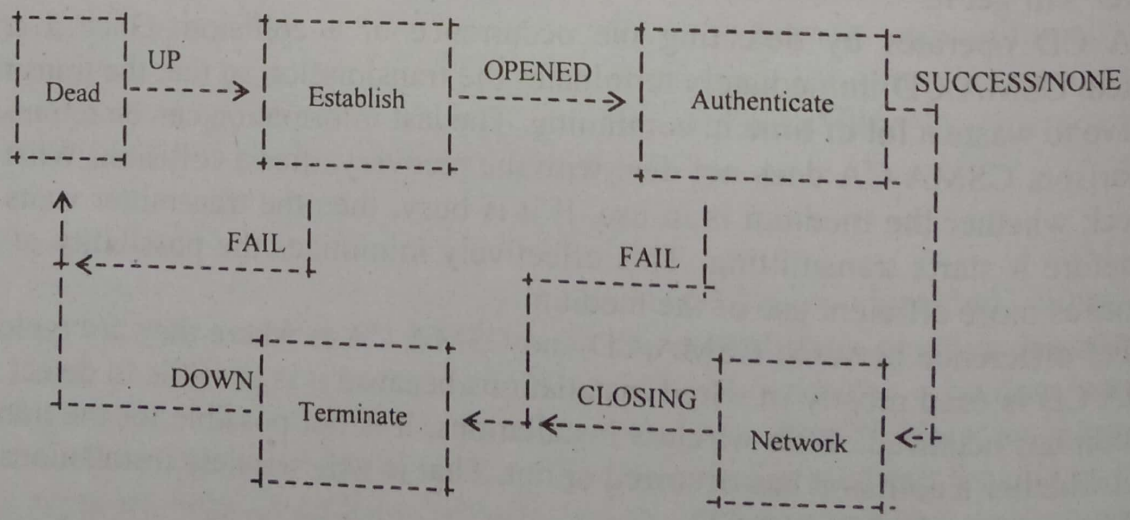
Answer:

a) In the Link Establishment phase, the system initiating the connection transmits an LCP Configure Request message to the destination containing the options it would like to enable, such as the use of specific authentication, link-quality monitoring, and network-layer protocols (if any), and whether the systems should modify standard features, such as the size of the FCS field or a different MRU value. If the receiving system can support all the specified options, it replies a Configure Ack message containing the same option values, and this phase of the connection process is completed.

If the receiving system recognizes the options in the request message, but cannot support the values for those options supplied by the sender (such as if the system supports authentication, but not with the protocol the sender has specified), it replies with a Configure Nak message containing the options with values it cannot support. With these options, the replying system supplies all the values it does support and also may include other options it would like to see enabled. Using this information, the connecting system generates another Configure Request message containing options it knows are supported, to which the receiver replies with a Configure Ack message.

If the receiving system fails to recognize any of the options in the request, it replies with a Configure Reject message containing only the unrecognized options. The sender then generates a new Configure Request message that does not contain the rejected options and the procedure continues as previously outlined. Eventually, the systems perform a successful request/acknowledgement exchange and the connection process moves on to the next phase.

b) In the process of configuring, maintaining and terminating the point-to-point link, the PPP link goes through several distinct phases which are specified in the following simplified state diagram:



Not all transitions are specified in this diagram. The following semantics MUST be followed.

Link Dead (physical-layer not ready): The link necessarily begins and ends with this phase. When an external event (such as carrier detection or network administrator configuration) indicates that the physical-layer is ready to be used, PPP will proceed to the Link Establishment phase. During this phase, the LCP automaton will be in the Initial or Starting states. The transition to the Link Establishment phase will signal an Up event to the LCP automaton.

Link Establishment Phase: The Link Control Protocol (LCP) is used to establish the connection through an exchange of Configure packets. This exchange is complete, and the LCP Opened state entered, once a Configure-Ack packet has been both sent and received.

Authentication Phase: On some links it may be desirable to require a peer to authenticate itself before allowing network-layer protocol packets to be exchanged. By default, authentication is not mandatory. If an implementation desires that the peer authenticate with some specific authentication protocol, then it MUST request the use of that authentication protocol during Link Establishment phase.

Link Termination phase: PPP can terminate the link at any time. This might happen because of the loss of carrier, authentication failure, link quality failure, the expiration of an idle-period timer, or the administrative closing of the link.

LCP is used to close the link through an exchange of Terminate packets. When the link is closing, PPP informs the network-layer protocols so that they may take appropriate action.

Network-Layer Protocol Phase: Once PPP has finished the previous phases, each network-layer protocol (such as IP, IPX, or AppleTalk) MUST be separately configured by the appropriate Network Control Protocol (NCP).

c) CHAP (Challenge-Handshake Authentication Protocol) is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP). Here's how CHAP works:

1. After the link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained by using a one-way hash function.
2. The server checks the response by comparing it its own calculation of the expected hash value.
3. If the values match, the authentication is acknowledged; otherwise the connection is usually terminated.

At any time, the server can request the connected party to send a new challenge message. Because CHAP identifiers are changed frequently and because authentication can be requested by the server at any time, CHAP provides more security than PAP. RFC1334 defines both CHAP and PAP.

7. a) Derive the expression of the efficiency of pure ALOHA.
b) Compare performance of pure ALOHA with slotted ALOHA. **[WBUT 2018]**

Answer:

a) *Refer to Question No. 2(1st part) of Short Answer Type Questions.*

b) *Refer to Question No. 3 of Short Answer Type Questions.*

8. Write short notes on the following: [WBUT 2006, 2011]

a) IEEE 802.11 [WBUT 2010, 2019]
b) FDDI [WBUT 2012]
c) CSMA/CD [WBUT 2015]
d) CDMA [WBUT 2019]
e) HDLC [WBUT 2019]
f) CSMA [WBUT 2019]
g) Virtual Private Network (VPN)

Answer:

a) IEEE 802.11:

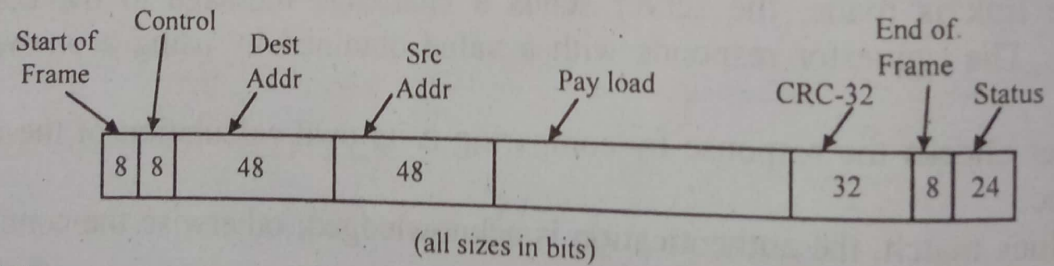
Refer to Question No. 3 (b) (1st Part) of Long Answer Type Questions.

b) FDDI:

FDDI (Fiber-Distributed Data Interface) is a standard for data transmission on fiber optic lines in that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users.

An FDDI network contains two token rings, one for possible backup in case the primary ring fails. The primary ring offers up to 100 Mbps capacity. If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 miles).

FDDI is a product of American National Standards Committee X3-T9 and conforms to the open system interconnect (OSI) model of functional layering. It can be used to interconnect LANs using other protocols. FDDI-II is a version of FDDI that adds the capability to add circuit-switched service to the network so that voice signals can also be handled. Work is underway to connect FDDI networks to the developing Synchronous Optical Network.



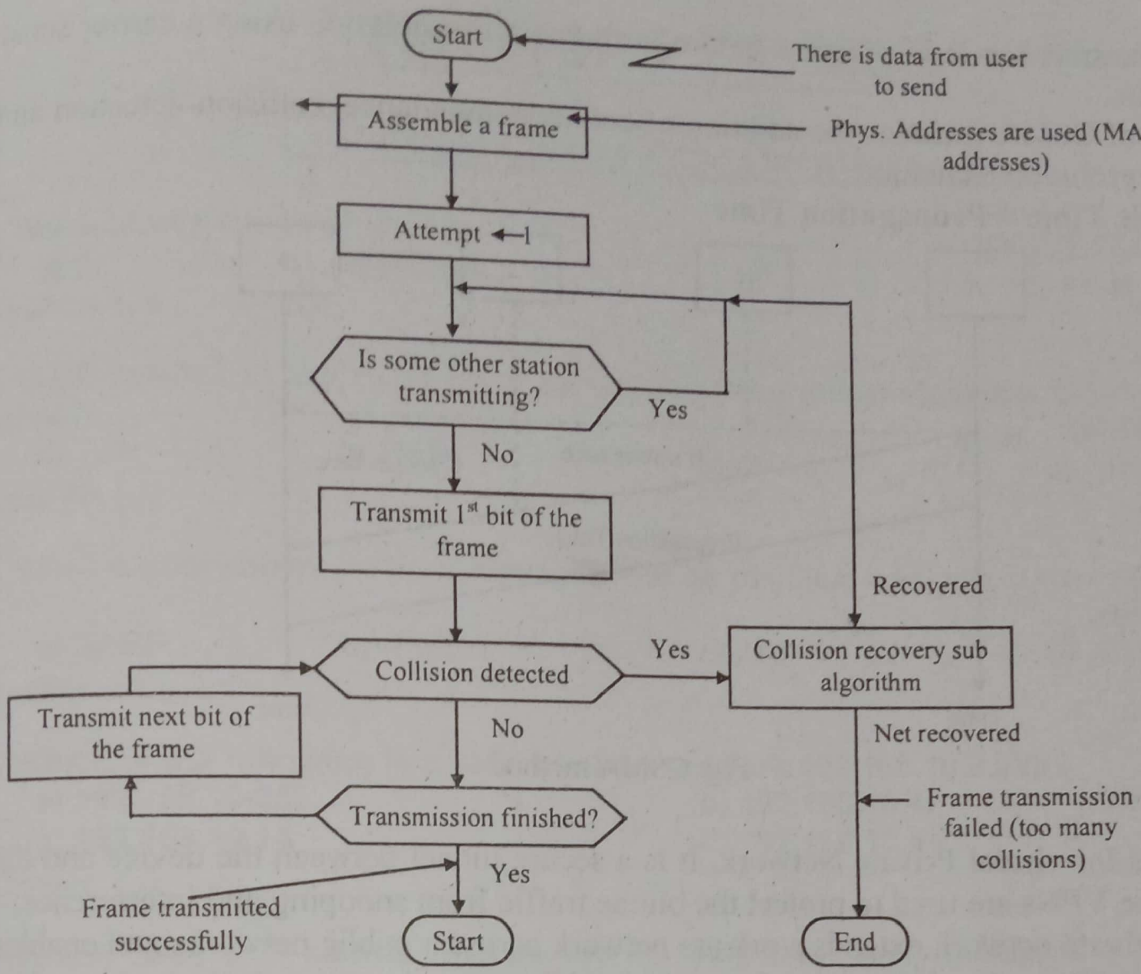
(all sizes in bits)

c) CSMA/CD:

CSMA/CD is a modification of pure Carrier sense multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus reducing the probability of a second collision on retry.

A jam signal is sent which will cause all transmitters to back off by random intervals, reducing the probability of a collision when the first retry is attempted.

CSMA/CD is a layer 2 access method, not a protocol of the OSI model.



d) CDMA: ***Refer to Question No. 2(a) of Long Answer Type Questions.***

e) HDLC:

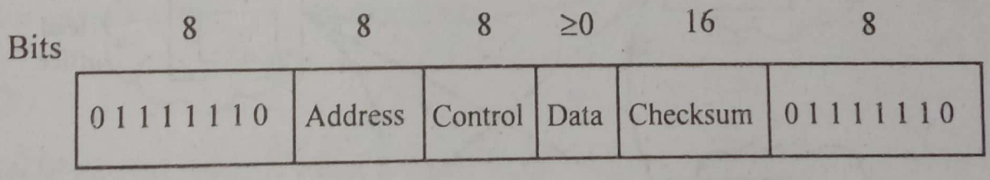


Fig: Frame format for bit-oriented protocols

The HDLC frame has a starting flag byte (7EH) followed by an 8-bit Address to identify a terminal in a multi-terminal line. The 8-bit control field is used for sequence numbers, acknowledgements etc. The data field is arbitrarily long. After the data is a 16-bit CRC field based on CRC-CCITT generator polynomial. The frame ends with a flag byte. There are three kinds of frames – Information, Supervisory and Unnumbered.

f) CSMA:

CSMA stands for carrier sense multiple access. It is a media access protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as electromagnetic spectrum. A transmitter attempts to determine whether

another transmission is in progress before initiating a transmission using a carrier sense mechanism.
Variation of CSMA includes the addition of collision–avoidance, collision-detection and collision-resolution technique.

Vulnerable Time = Propagation Time

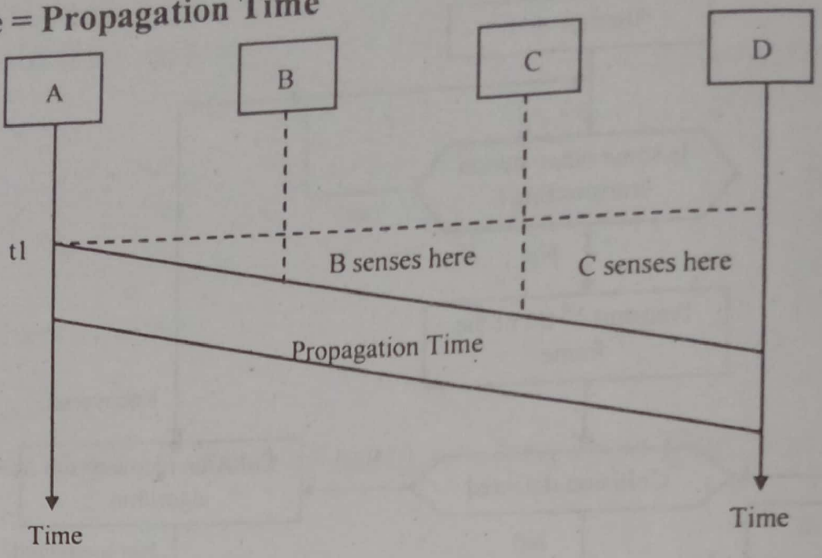
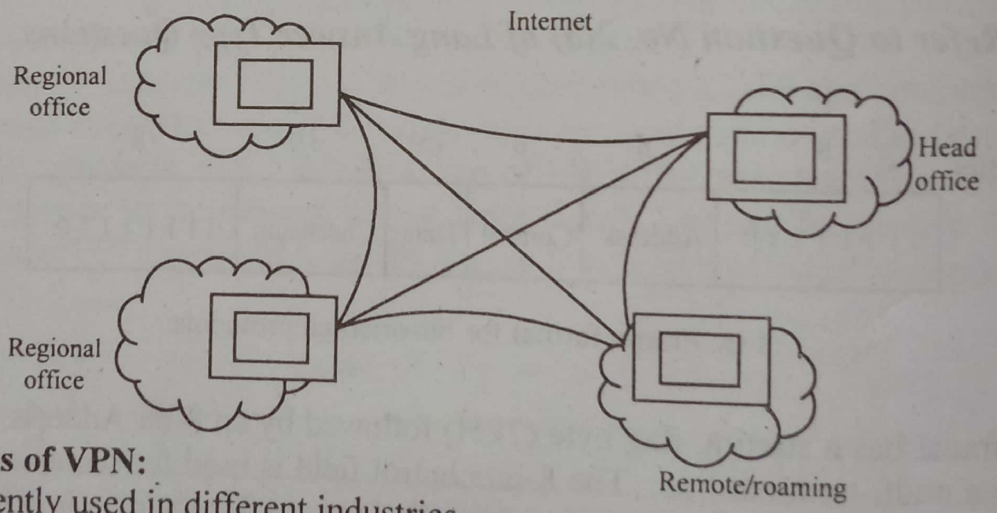


Fig: CSMA method

g) VPN:

VPN stands for virtual Private Network. It is a secure tunnel between the device and the internet. The VPNs are used to protect the online traffic from snooping and interference. A virtual private network extends a private network across a public networks and enables user to send and receive data across shared and public networks.



Applications of VPN:

i) It is efficiently used in different industries.
ii) VPN security model provides confidentiality, authenticity and integrity.
iii) It allows only authenticated remote access using tunneling protocols and encryption Technique.

NETWORK LAYER

Multiple Choice Type Questions

1. The address space of IPv4 is [WBUT 2011, 2012]
a) 0 b) infinite c) 2^{32} d) none of these
Answer: (c)

2. ICMP resides at the same layer as which of the following protocols mentioned below? [WBUT 2011]
a) TCP b) UDP c) IP d) ARP
Answer: (d)

3. When a host knows its IP address but not its physical address, it can use [WBUT 2011]
a) RARP b) ICMP c) ARP d) IGMP
Answer: (c)

4. Which of the following is a valid host for network 192.168.10.32/28? [WBUT 2011]
a) 192.168.10.39 b) 192.168.10.47
c) 192.168.10.14 d) 192.168.10.54
Answer: (a)

5. Which class of IP address is reserved for multicast communication? [WBUT 2012, 2013]
a) Class *A* b) Class *B* c) Class *C* d) Class *D*
Answer: (d)

6. IPv6 addresses are _____ bytes long. [WBUT 2014]
a) 6 b) 16 c) 32 d) 128
Answer: (b)

7. Let in an IPv4 datagram, total length is 461 bytes and length of data is 433 bytes. What is the header size in bytes [WBUT 2014]
a) 28 b) 894 c) 36 d) 27
Answer: (a)

8. IP address in the B class is given by [WBUT 2014]
a) 125.123.123.2 b) 192.023.21.54 c) 191.128.32.56 d) 10.14.12.34
Answer: (c)

9. Given IP address is 180.25.21.172 and the subnet mask 255.255.192.0, then what is the subnet address? [WBUT 2014]
a) 180.25.21.0 b) 180.25.0.0 c) 180.25.8.0 d) 180.0.0.0
Answer: (b)

10. Which of the following is an interior routing protocol? [WBUT 2014]
a) RIP b) OSPF c) BGP d) both (a) & (b)
Answer: (d)

11. IPV6 address is having a length of [WBUT 2015]
a) 16 bit b) 32 bit c) 64 bit d) 128 bit
Answer: (d)

12. The protocol that maps a physical (MAC) address to the corresponding logical address is [WBUT 2015]
a) ARP b) RARP c) ICMP d) IMAP4
Answer: (b)

13. Which of the following protocol is based on the concept of Link State Routing? [WBUT 2015]
a) RIP b) OSPF c) BGP d) DVMRP
Answer: (b)

14. The subnet mask 255.255.255.192 [WBUT 2016, 2017]
a) extends the network portion to 16 bits
b) extends the network portion to 26 bits
c) extends the network portion to 36 bits
d) has no effect on the network portion of an IP address
Answer: (b)

15. Router solicitation and advertisement message is used by [WBUT 2016]
a) IP b) ARP c) ICMP d) DHCP
Answer: (c)

16. If source is using IPV6 and destination is using IPV4, which type of address needs to be used? [WBUT 2016]
a) Loopback b) Mapped c) Compatible d) None of these
Answer: (b)

17. In the string 219.46.123.107, what is the network address of the host we are looking for? [WBUT 2017]
a) 219.46.123.0 b) 107.123.0.0 c) 107.123.46.0 d) 107.0.0.0
Answer: (a)

18. Which of the following protocols is a network layer protocol? [WBUT 2017]
a) FTP b) ARP c) UDP d) Telnet
Answer: (b)

19. If subnet mask is 255.255.252.0, then many subnets are available? [WBUT 2018]
a) 2 b) 18 c) 4 d) 24
Answer: (b)

20. Router solicitation and advertisement message is used by [WBUT 2018]
a) IP b) ARP c) ICMP d) DHCP
Answer: (c)

21. When host knowns its IP address but not its physical address, it can use [WBUT 2018]
a) RARP b) ARP c) ICMP d) IGMP
Answer: (b)

22. Which class of IP address is reserved for multicast communication? [WBUT 2018]
a) Class A b) Class B c) Class C d) Class D
Answer: (d)

23. Which of the following is not a silent program in www? [WBUT 2019]
a) FTP b) SMTP c) HTTP d) HTML
Answer: (d)

24. The ..... socket is used with a protocol that directly uses the services of IP. [WBUT 2019]
a) Stream b) Datagram c) Raw d) Remote
Answer: (c)

25. Which of the following is not a part of the UDP user datagram header? [WBUT 2019]
a) Length of header b) Source port number
c) Checksum d) Destination port number
Answer: (a)

26. ..... address uniquely identifies a running application program. [WBUT 2019]
a) IP address b) Host c) NIC d) Socket
Answer: (d)

27. Router *B* receives an update from router *A* that indicates Net-1 is two hops away. The next update from *A* says Net-1 is five hops away. What value is entered in *B*'s routing table for Net-1? [WBUT 2019]
a) 2 b) 3 c) 5 d) 7
Answer: (b)

Short Answer Type Questions

1. Explain Link State Routing. [WBUT 2007, 2013]

Answer:

A Link-state routing is a concept used in routing of packet-switched networks in computer communications. Link-state routing works by having the routers tell every router on the network about its closest neighbors. The entire routing table is not

distributed from any router, only the part of the table containing its neighbors. The following are some key characters of the Link-state routing concept:
The neighbor information is gathered continuously.
The neighbor information list is then broadcasted to every router that can answer to this protocol, a process known as flooding, which means that it sends the information to all of its neighbors who in turn send it to all of their neighbors and so on. Soon, all routers on the network have this information.
The neighbor information is flooded whenever there is a (routing-significant) change in the network.
As every router knows everything about the network by structuring the information from other routers, it can calculate the best path to any host on any destination network.
Some of the link-state routing protocols are the OSPF, IS-is and EIGRP.

Advantages:

LinkState Routing protocols provide greater flexibility and sophistication than the Distance Vector routing protocols. They reduce overall broadcast traffic and make better decisions about routing by taking characteristics such as bandwidth, delay, reliability, and load into consideration, instead of basing their decisions solely on distance or hop count.

2. What are the different types of addresses contained in a packet flowing in the internet?
Explain each one of them with respect to their usefulness. **[WBUT 2010]**

Answer:

When a client on the internal network contacts a machine on the Internet, it sends out IP packets destined for that machine. These packets contain all the addressing information necessary to get them to their destination. NAT is concerned with these pieces of information:

Source IP address (for example, 192.168.1.35)
Source TCP or UDP port (for example, 2132)

When the packets pass through the NAT gateway they will be modified so that they appear to be coming from the NAT gateway itself. The NAT gateway will record the changes it makes in its state table so that it can a) reverse the changes on return packets and b) ensure that return packets are passed through the firewall and are not blocked. For example, the following changes might be made:
Source IP: replaced with the external address of the gateway (for example, 24.5.0.5)
Source port: replaced with a randomly chosen, unused port on the gateway (for example, 53136)
Neither the internal machine nor the internet host is aware of these translation steps. To the internal machine, the NAT system is simply an internet gateway. To the internet host, the packets appear to come directly from the NAT system; it is completely unaware that the internal workstation even exists.
When the internet host replies to the internal machine's packets, they will be addressed to the NAT gateway's external IP (24.5.0.5) at the translation port (53136). The NAT gateway will then search the state table to determine if the reply packets match an already established connection. A unique match will be found based on the IP/port combination

which tells PF the packets belong to a connection initiated by the internal machine 192.168.1.35. PF will then make the opposite changes it made to the outgoing packets and forward the reply packets on to the internal machine.
Translation of ICMP packets happens in a similar fashion but without the source port modification.

3. a) Find the netid and the hostid of the following IP addresses. [WBUT 2011, 2013]
(i) 19.34.21.5
(ii) 220.34.8.9

b) A network has subnet mask 255.255.255.224
Determine the maximum or number of Host in this network. Also determine the broadcast address of this network.

Answer:

a)

Network Address	Class	Host bits	Network-id	Host-id
(i) 19.34.21.5	A	34.21.5	19	34.21.5
(ii) 220.34.8.9	C	9	220.34.8	9

b) Number of Hosts = 12. Here in the Broadcast address, host=11111.So, the broadcast address is 255.255.255.255

4. Compare IPv4 and IPv6. [WBUT 2011]

Answer:
IPV6 is 128 bit. Whereas IPV4 is only 32 bit. Though IPV4 is in use presently but the IP addresses come to an end means they cannot cope up with the increasing demand. Here 2^32 addresses can be gives. But in IPV6, as there are 128 bit 2^128 bit addresses can be given to the users. There is no chance of short coming of IP's. The ratio of total number of IP addresses to the surface area of the earth is very large means within unit surface area so many computers can't be placed.

5. What is Gateways? Differentiate between hub and switch? [WBUT 2012]

Answer:
A Gateway is a network node that is equipped to interface with another network that possibly uses different protocols. Gateways are therefore protocol converters that may operate at any layer.
Hubs and switches are networking equipments that inter-connect several hosts. They differ in the way that they pass on network traffic that they receive. A hub repeats everything it receives on all other ports. A switch on the other hand makes a short analysis of the packet received and tries to repeat it only on an appropriate port. For Ethernet, a hub does not isolate collision domain. Switches on the other hand isolate collision domain and hence permit a larger number of hosts to operate smoothly with low collision levels.

6. What is intranet? Differentiate between IP address and MAC address. [WBUT 2013]

Answer:

1st Part:

A collection of hosts or nodes that uses standard protocol to communicate among themselves but is restricted from outside access is **Intranet.**

2nd Part:

Difference between IP and MAC address is as follows:

IP	MAC
1. Uses 32 bits for IPV4 and 128 bits for IPV6.	1. Uses 48 bits.
2. Also called logical or network layer address.	2. Also known as physical/NIC address or burned-in address.
3. Recognized by routers.	3. Recognized by switch.
4. Uses concept of subnet masking to differentiate between network and host ID.	4. No concept of subnet masking.

7. N routers are to be connected in a point-to-point subnet. Between each pair of routers, the designers may put a high-speed line, a medium-speed, a low-speed line, or no line. If it takes t unit of computer time to generate and inspect each topology, how long will it take to inspect all of them? [WBUT 2014]

Answer:

There are $P = C_N^2$ possible lines between N routers. Each line has 4 possible cases. So total number of topology is 4^P.

We will take $(4^P \times t)$ unit time to inspect all of them.

8. a) What is the purpose of the "Time to live" field in the IP header?

b) If the IP header is 28 bytes long, what will be the value of the "HLEN" field (in Binary)?

c) Write the advantages of ICMP over the IPV4. [WBUT 2014, 2018]

Answer:

a) An 8-bit time to live (TTL) field helps prevent datagrams from persisting (e.g. going in circles) on an internetwork. Historically the TTL field limited a datagram's lifetime in seconds, but has come to be a hop count field. Each packet switch (or router) that a datagram crosses decrements the TTL field by one. When the TTL field hits zero, the packet is no longer forwarded by a packet switch and is discarded. Typically, an ICMP message (specifically the time exceeded) is sent back to the sender that it has been discarded. The reception of these ICMP messages is at the heart of how traceroute works.

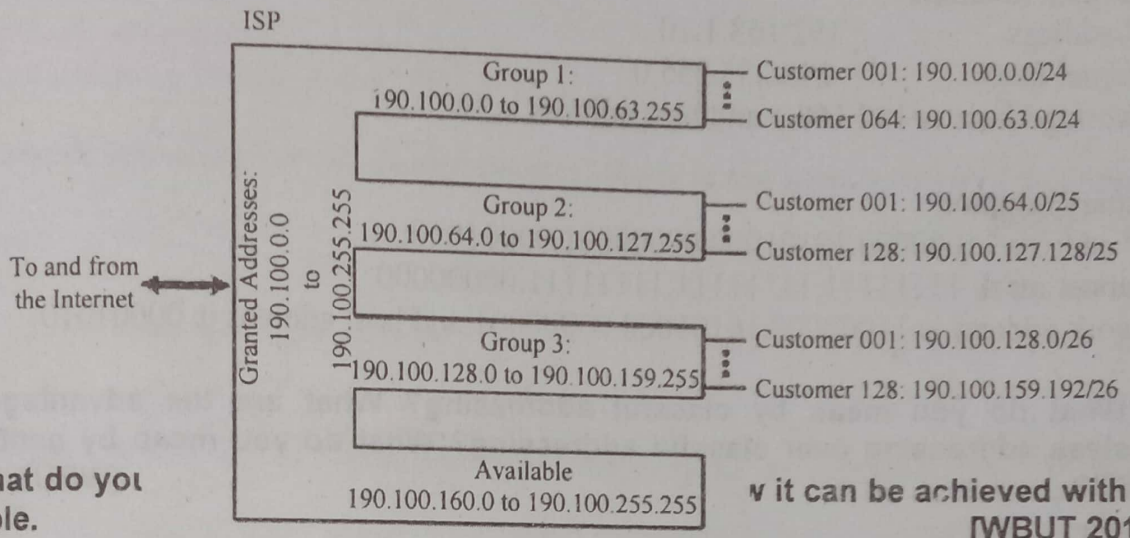
b) Value of the HLEN is 28/4=7 (in decimal) = 0111 (in binary)

c) Computer networks provide unlimited uses for today's society. A network administrator's responsibility consists of always being able to track a problem when it happens on the network. To perform their jobs effectively, they rely on a vast amount of tools and expertise. One such tool is ICMP protocol. This protocol is integrated with IP protocol, which is the basic makeup of a network and allows requests to be sent out and information to be sent back to the administrator.

9. An ISP is granted a block of address starting with 190.100.0.0/16. The ISP needs to distribute these addresses to three groups of customers as follows:
a) The 1st group has 64 customers; each needs 256 addresses.
b) The 2nd group has 128 customers; each needs 128 addresses.
c) The 3rd group has 128 customers; each needs 64 addresses.
Design the subblocks and give the slash notation for each subblock. [WBUT 2015]

Answer:

Figure below shows the situation



10. What do you **v it can be achieved with an example.** **[WBUT 2016]**

Answer:

1st part:

With the advent of subnetting, one can no longer rely on the definition of the IP address classes to determine the network ID in the IP address. A new value is needed to define which part of the IP address is the network ID and which part is the host ID regardless of whether class-based or subnetted network IDs are being used.

RFC 950 defines the use of a subnet mask (also referred to as an address mask) as a 32-bit value that is used to distinguish the network ID from the host ID in an arbitrary IP address. The bits of the subnet mask are defined as follows:

- All bits that correspond to the network ID are set to 1.
- All bits that correspond to the host ID are set to 0.

Each host on a TCP/IP network requires a subnet mask even on a single segment network. Either a default subnet mask, which is used when using class-based network IDs, or a custom subnet mask, which is used when subnetting or supernetting, is configured on each TCP/IP node.

2nd part:

Subnet mask is a 32 bits long address used to distinguish between network address and host address in IP address. Subnet mask is always used with IP address. Subnet mask has only one purpose, to identify which part of an IP address is network address and which part is host address.

For example how will we figure out network partition and host partition from IP address 192.168.1.10 ? Here we need subnet mask to get details about network address and host address.

- In decimal notation subnet mask value 1 to 255 represent network address and value 0 [Zero] represent host address.
- In binary notation subnet mask ON bit [1] represent network address while OFF bit[0] represent host address.

In decimal notation

IP address	192.168.1.10
Subnet mask	255.255.255.0

Network address is 192.168.1 and host address is 10.

In binary notation

IP address 11000000.10101000.00000001.00001010
Subnet mask 11111111.11111111.11111111.00000000

Network address is 11000000.10101000.00000001 and host address is 00001010

11. What do you mean by classful addressing? What are the advantages of classless addressing over classful addressing? What do you mean by netID and hostID? **[WBUT 2016]**

Answer:

1st part:

In classful addressing, the network portion ends on one of the separating dots in the address (on an octet boundary). Classful addressing divides an IP address into the Network and Host portions along octet boundaries. In the classful addressing system all the IP addresses that are available are divided into the five classes A,B,C,D and E, in which class A,B and C address are frequently used because class D is for Multicast and is rarely used and class E is reserved and is not currently used.

2nd part:

Classless notation is preferred over classful addressing because of its inherent advantages. First, classless notation results in the efficient use of IP addresses. This is not the case in classful addresses, where Class C addresses are too small for a moderate-sized network and Class B is too large. Since most networks opt for the Class B address, this leads to the huge wastage of a precious public resource. Second, classless addressing facilitates address summarization (i.e., ability to represent a group of addresses through a single address), thereby resulting in lesser routing traffic and smaller routing table size.

3rd part:

In classful addressing, an IP address of class A, B and C is divided into two parts : netid and hostid.

The netid and hostid are of varying lengths, depending on the class of the address.

Netid: The part of an IP address that identifies the network.

Hostid: The part of an IP address that identifies a host in a network.

Class A: One byte netid three bytes host id
Class B: Two bytes netid Two bytes host id
Class C: Three bytes netid One byte host id
Example:
IP address: 84.42.58.11
Binary Notation: 01010100 00101010 00111010 00001011
It is a class A IP address.
The network address /netid is 84.0.0.0
The host addresses /hostid is 0.42.58.11

12. Draw various fields in IP packet header. What is the significance of total length field? [WBUT 2019]

Answer:

1st Part:

An IP packet consists of two sections:
header
data.
The header consists of 13 fields and, of which, only 12 are required. The 13th field is optional.

+	Bits 0 - 3	4 - 7	8 - 15	16 - 18	19	20 - 31
0	Version	Header length	Type of Service (now DiffServ and ECN)	Total Length		
32	Identification			Flags	Evil Bit	Fragment Offset
64	Time to Live		Protocol	Header Checksum		
96	Source Address					
128	Destination Address					
160	Options					
160/192+	Data					

Version

The first header field in an IP packet is the 4-bit version field. For IPv4, this has a value of 4 (hence the name IPv4).

Internet Header Length (IHL)

The second field is a 4-bit Internet Header Length (IHL) telling the number of 32-bit words in the header. Since an IPv4 header may contain a variable number of options, this field specifies the size of the header (this also coincides with the offset to the data). The minimum header size is 20 bytes, so the minimum value for this field is 5 (5×4 = 20 bytes). Being a 4-bit field the maximum length is 15 words or 60 bytes.

Type of Service (ToS)
bits 0-2: precedence
bit 3: 0 = Normal Delay, 1 = Low Delay
bit 4: 0 = Normal Throughput, 1 = High Throughput
bit 5: 0 = Normal Reliability, 1 = High Reliability
bits 6-7: Reserved for future use
This field is now used for DiffServ and ECN. The original intention was for a sending host to specify a preference for how the datagram would be handled as it made its way through an internetwork. For instance, one host could set its IPv4 datagrams' ToS field value to prefer low delay, while another might prefer high reliability. In practice, the ToS field has not been widely implemented. However, a great deal of experimental, research and deployment work has focused on how to make use of these eight bits. These bits have been redefined, most recently through DiffServ working group in the IETF and the Explicit Congestion Notification codepoints. New technologies are emerging that require real-time data streaming and therefore will make use of the ToS field. An example is Voice over IP (VoIP) that is used for interactive data voice exchange.

Total Length
This field defines the entire datagram size, including header and data, in bytes. The minimum-length datagram is 20 bytes (20 bytes header + 0 bytes data) and the maximum is 65,535 — the maximum value of a 16-bit word. The minimum size datagram that any host is **required** to be able to handle is 576 bytes, but most modern hosts handle much larger packets.

Identification
This field is an identification field and is primarily used for uniquely identifying fragments of an original IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to datagrams in order to help trace back datagrams with spoofed source addresses.
Flags
A 3-bit field follows and is used to control or identify fragments. They are (in order, from high order to low order):
Reserved, must be zero
Don't Fragment (DF)
More Fragments (MF)
If the DF flag is set and fragmentation is required to route the packet then the packet will be dropped. This can be used when sending packets to a host that does not have sufficient resources to handle fragmentation.
When a packet is fragmented all fragments have the MF flag set except the last fragment, which does not have the MF flag set. The MF flag is also not set on packets that are not fragmented — clearly an unfragmented packet can be considered the last fragment.

Fragment Offset

The fragment offset field is 13-bits long and allows a receiver to determine the place of a particular fragment in the original IP datagram, measured in units of 8-byte blocks. This method allows a maximum offset of 65,528 ((2^13 - 1)*8 which would exceed the maximum IP packet length of 65,535 with the header length counted with it.

Time to Live (TTL)

An 8-bit time to live (TTL) field helps prevent datagrams from persisting (e.g. going in circles) on an internetwork. Historically the TTL field limited a datagram's lifetime in seconds, but has come to be a hop count field. Each packet switch (or router) that a datagram crosses decrements the TTL field by one. When the TTL field hits zero, the packet is no longer forwarded by a packet switch and is discarded. Typically, an ICMP message (specifically the time exceeded) is sent back to the sender that it has been discarded. The reception of these ICMP messages is at the heart of how traceroute works.

Protocol

This field defines the protocol used in the data portion of the IP datagram.

Header Checksum

The 16-bit checksum field is used for error-checking of the header. At each hop, the checksum of the header must be compared to the value of this field. If a header checksum is found to be mismatched, then the packet is discarded. Note that errors in the data field are up to the encapsulated protocol to handle — indeed, both UDP and TCP have checksum fields.

Source address

An IP address is a group of 4 8-bit octets for a total of 32 bits. The value for this field is determined by taking the binary value of each octet and concatenating them together to make a single 32-bit value.

Destination address

Identical to the source address field but indicates the receiver of the packet.

Options

Additional header fields (called options) may follow the destination address field, but these are not often used. Note that the value in the IHL field must include enough extra 32-bit words to hold all the options (plus any padding needed to ensure that the header contains an integral number of 32-bit words). The list of options may be terminated with an EOL (End of Options List) option; this is only necessary if the end of the options would not otherwise coincide with the end of the header.

2nd Part:

Significance of total length field:

It specifies the length of the entire IP packet, including both the header and data segments in bytes.

13. a) What are the basic differences between Router and Gateway?
b) Distinguish between the two terms 'internet' and 'intranet'? **[WBUT 2019]**

Answer:

a) Router

Network device that forwards packets from one network to another. Based on internal routing tables, routers read each incoming packet and decide how to forward it.
Routers work at the network layer (layer 3) of the protocol.

Gateway

Device that converts one protocol or format to another. A network gateway converts packets from one protocol to another. The gateway functions as an entry/exit point to the network. An earlier name for router.
GATEWAY work at the network layer (layer 4) of the protocol.

b) The Internet is a network of LAN-s that uses the IP protocol at the network layer and covers the entire world. The Intranet is similar, i.e., it is also a network of networks driven by the IP protocol. However, all the networks of the Intranet belong to the same organization.

Long Answer Type Questions

1. a) What is the purpose of subnetting? **[WBUT 2006, 2011]**
b) State the advantages of IPV_6 over IPV_4. **[WBUT 2006, 2013, 2016]**

Answer:

a) The main purpose of subnetting is to help relieve network congestion. Congestion used to be a bigger problem than it is today because it was more common for networks to use hubs than switches. When nodes on a network are connected through a hub, the entire network acts as a single collision domain. What this means is that if one PC sends a packet to another PC, every PC on the entire network sees the packet. Each machine looks at the packet header, but ignores the packet if it isn't the intended recipient.

b) Following are some of the advantage of IPv6 over IPv4:

1. **Larger Address Space:** address filed in IPv6 is 128 bits long while the address filed of IPv4 is only 32 bits in length. IPv6 offers very large, i.e.296 address space as compared to IPv4.
2. **Better header format:** the header of IPv6 has been designed in a way to speed-up the routing process. In header of IPv6 options are separated from the base header. Options are inserted into base header only when required by the upper-layer data.
3. **Provision for extension:** IPv6 has been designed in a way that a protocol can be extended easily to meet the requirements of emerging technologies or new applications.
4. **Resource Allocation support in IPv6:** IPv6 provides a mechanism called Flow Label for resource allocation. Flow label enables source to send request for the

special handling of a packet. This mechanism is really helpful in real-time audio and video transmission.

5. **Security Features:** to ensure confidentiality and packet's integrity encryption and authentication options are included in IPv6.

2. Differentiate static routing with dynamic routing. Explain various fields of a typical routing table. **[WBUT 2008, 2012]**

Answer:

static routing	dynamic routing
Static routing is when you statically configure a router to send traffic for particular destinations in preconfigured directions	Dynamic routing is when you use a routing protocol such as OSPF, ISIS, EIGRP, and/or BGP to figure out what paths traffic should take.

The routing table consists of at least three information fields:
the network id: i.e. the destination network id
cost: i.e. the cost or metric of the path through which the packet is to be sent
next hop: The next hop, or gateway, is the address of the next station to which the packet is to be sent on the way to its final destination
Depending on the application and implementation, it can also contain additional values that refine path selection:
Flag: quality of service associated with the route. For example, the U flag indicates that an IP route is up.
links to filtering criteria/access lists associated with the route
interface: such as eth0 for the first Ethernet card, eth1 for the second Ethernet card, etc.

3. Differentiate between connected-oriented and connectionless services implemented by the network layer. **[WBUT 2010]**

OR,

Differentiate between connection-oriented and connectionless services implemented by the network layer. **[WBUT 2016]**

Answer:

Connection-oriented: Requires a session connection (analogous to a phone call) be established before any data can be sent. This method is often called a "reliable" network service. It can guarantee that data will arrive in the same order. Connection-oriented services set up virtual links between end systems through a network. Note that the packet on the left is assigned the virtual circuit number 01. As it moves through the network, routers quickly send it through virtual circuit 01.

Connectionless: Does not require a session connection between sender and receiver. The sender simply starts sending packets (called datagrams) to the destination. This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers. Neither system must maintain state information for the systems that they send transmission to or receive transmission from. A connectionless network provides minimal services.

4. Distinguish between a router and a bridge. What do you mean by transparent bridge? **[WBUT 2010]**

Answer:

1st Part:

1) Routers are more intelligent than bridges in the sense that if runs an algorithm that depends on the contents of a packet. For example, and IP router runs the routing algorithm based on the destination IP address of the packet.
2) Routers can operate on interfaces that lead to identical media types but bridges are meant to interconnect different kinds of media. For example we can have a router connecting Ethernet LANs. A bridge on the other hand can connect an Ethernet LAN with a Token-ring LAN (for example).
3) Routers allow hosts that aren't practically on the same logical network to be able to communicate with each other, while bridges can only connect networks that are logically the same.
4) Routers operate at the layer 3 (network layer) of the OSI model, while bridges are only at the layer 2 (Data link layer).

2nd Part:

Transparent bridges are devices which connects more than one network segments with other bridges to make all routing decisions. A transparent bridge is essentially used to learn the MAC addresses of all nodes and their associated port, to filter incoming frames whose destination MAC addresses are located on the same incoming port, and to forward incoming frames to the destination MAC through their associated port.

5. Explain link state routing.

Answer: **[WBUT 2010]**

A Link-state routing is a concept used in routing of packet-switched networks in computer communications. Link-state routing works by having the routers tell every router on the network about its closest neighbors. The entire routing table is not distributed from any router, only the part of the table containing its neighbors. The following are some key characters of the Link-state routing concept:

- The neighbor information is gathered continuously.
- The neighbor information list is then broadcasted to every router that can answer to this protocol, a process known as flooding, which means that it sends the information to all of its neighbors who in turn send it to all of their neighbors and so on. Soon, all routers on the network have this information.
- The neighbor information is flooded whenever there is a (routing-significant) change in the network. As every router knows everything about the network by structuring the information from other routers, it can calculate the best path to any host on any destination network.

Some of the link-state routing protocols are the OSPF, IS-is and EIGRP. Novell's NLSP (NetWare Link State Protocol) is also a link-state routing protocol, which only supports IPX.

LinkState Routing protocols provide greater flexibility and sophistication than the Distance Vector routing protocols. They reduce overall broadcast traffic and make better decisions about routing by taking characteristics such as bandwidth, delay, reliability, and load into consideration, instead of basing their decisions solely on distance or hop count.

6. a) Write brief notes on distance vector routing protocol. What is the primary difference between RIP and BGP? What is the value of infinity in case of RIP?
[WBUT 2010]

b) What do you mean by an Autonomous System (AS)? What is the difference between Intra-AS and Inter-AS routings? Give an example of each routing protocol.
[WBUT 2010, 2012]

c) What do you mean by count-to-infinity problem? How is the problem partially overcome by the technique Split Horizon with Poisson reverse method?
[WBUT 2010]

Answer:

a) In computer communication theory relating to packet-switched networks, a distance-vector routing protocol is one of the two major classes of routing protocols, the other major class being the link-state protocol. A distance-vector routing protocol uses the Bellman-Ford algorithm to calculate paths.

A distance-vector routing protocol requires that a router informs its neighbors of topology changes periodically and in some cases, when a change is detected in the topology of a network. Compared to link-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity and message overhead.

Distance Vector means that Routers are advertised as vector of distance and direction. 'Direction' is represented by next hop address and exit interface, whereas 'Distance' uses metrics such as hop count.

Routers using distance vector protocol do not have knowledge of the entire path to a destination. Instead DV uses two methods:

Direction in which or interface to which a packet should be forwarded.

Distance from its destination.

Rip is a distance-vector based routing protocol meant to work with smaller IP base networks. RIP uses UDP for propagating routing information.

BGP is designed to work across large networks, usually belonging to one or group of ISP-s. Such group, known as Autonomous Segments (AS-s). BGP is a protocol for routing between AS-s. BGP uses TCP for propagating routing information.

The value of infinity in case of RIP is 16 hops.

b) On the Internet, an autonomous system (AS) is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

Networks within an autonomous system communicate routing information to each other using an Interior Gateway Protocol (IGP) like RIP, OSPF, etc. An autonomous system shares routing information with other autonomous systems using the Border Gateway Protocol (BGP).

Intra-Autonomous System	Inter-Autonomous System
An intra-AS routing protocol is used to configure and maintain the routing tables within an autonomous system (AS).	An inter-autonomous system routing protocol provides routing between autonomous systems (that is, administrative domains).
Intra-AS routing protocols are also known as interior gateway protocols RIP: Routing Information Protocol	The Border Gateway Protocol (BGP)

c) The core of the count-to-infinity problem is that if A tells B that it has a path somewhere, there is no way for B to know if the path has B as a part of it. To see the problem clearly, imaging a subnet connected like as A-B-C-D-E-F and let the metric between the routers be "number of jumps". Now suppose that A goes down (out of order). In the vector-update-process B notices that the route to A, which was distance 1, is down – B does not receive the vector update from A. The problem is, B also gets an update from C and C is still not aware of the fact that A is down – so it tells B that A is only two jumps from C (C to B to A), which is false. This slowly propagates through the network until it reaches infinity (in which case the algorithm corrects itself, due to the "Relax property" of Bellman Ford).

According to the split-horizon rule, node A does not advertise its route for C (namely A to B to C) back to B. On the surface, this seems redundant since B will never route via node A because the route costs more than the direct route from B to C. However, if the link between B and C goes down and B had received a route from A, B could end up using that route via A. A would send the packet right back to B, creating a loop. With the split-horizon rule in place, this particular loop scenario cannot happen, improving convergence time in complex, highly-redundant environments.

7. a) Distinguish between adapting routing and fixed routing? [WBUT 2011]
b) Differentiate between Link State and Distance Vector routing algorithms.

Answer:

a) Adaptive routing (i.e. dynamic routing) that adjusts automatically to network topology or traffic changes. It describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change.

People using a transport system can display adaptive routing. For example, if a local railway station is closed, people can alight from a train at a different station and use another method, such as a bus, to reach their destination.

The term is commonly used in data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so long as other path choices are available. There are several protocols used to achieve this: RIP, OSPF, IS-IS, etc.

Systems that do not implement adaptive routing are described as using static routing, where routes through a network are described by fixed paths (statically). A change, such a loss of a node, or loss of a connection between nodes, is not compensated for. This means that anything that wishes to take an affected path will either have to wait for the failure to be repaired before restarting its journey, or will have to fail to reach its destination and give up the journey.

b) Distance vector routing protocol, like RIP, the routing table is forwarded by each router to neighboring routers. Here, the routers don't know the topology, i.e., how other routers are interconnected.

Link state routing protocol, like OSPF, routers first exchange information about connections within the network and build a topology table. Then each router calculate the best route to each destination by using Dijkstra's algorithm.

8. a) Distinguish between gateway and bridge. What is transparent bridge? **[WBUT 2012]**

Answer:

1st Part:

A bridge is used for connecting two or more networks that have similar topology and technology. It is a device that transfers data without regard to its format. For example, wireless APs with routers can bridge between an Ethernet LAN and WLAN.

To connect networks of different topology or technology, gateways are used. A gateway can be a software or hardware or a combination of both. An office LAN may be connected to the Internet Service Provider's WAN using a gateway.

2nd Part:

Transparent bridges are bridges that connect more than one network segments with other bridges and take routing decisions.

b) What is distance vector routing protocol? What is the difference between RIP and EGP? **[WBUT 2012]**

Answer:

1st Part: ***Refer to Question No. 6 (a)(1st Part) of Long Answer Type Questions.***

2nd Part:

EGP is a currently obsolete exterior gateway protocol. RIP on the other hand is one of the earliest internal gateway protocol used in the Internet.

9. a) State the differences between IPV4 and IPV6. [WBUT 2012]

OR,

Compare IPv4 and IPv6. [WBUT 2018]

b) Describe any shortest path algorithm. [WBUT 2012]

c) Differentiate between ARP and RARP. [WBUT 2012, 2013]

Answer:

a)

IPV4	IPV6
Addresses are 32 bits (4 bytes) in length. So, maximum 232 addresses possible.	Addresses are 128 bits (16 bytes) in length. So, maximum 2128 addresses are possible.
Dotted Number notation, e.g., 192.168.10.160	Hexadecimal number notation, e.g., 32FE:4201:39A6:0000:0000:0000:1234:ABCD
IPSec is optional and should be supported externally	IPSec support is not optional
Header does not identify packet flow for QoS handling by routers	Header contains Flow Label field, which Identifies packet flow for QoS handling by router.
Both routers and the sending host fragment packets.	Routers do not support packet fragmentation. Sending host fragments packets.
Header includes a checksum.	Header does not include a checksum.
Header includes options.	Optional data is supported as extension headers.
ARP uses broadcast ARP request to resolve IP to MAC/Hardware address.	Multicast Neighbour Solicitation messages resolve IP addresses to MAC addresses.
Broadcast addresses are used to send traffic to all nodes on a subnet.	IPv6 uses a link-local scope all-nodes multicast address.
Configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

b) Let the node at which we are starting be called the initial node. Let the distance of node Y be the distance from the initial node to Y. Dijkstra's shortest path algorithm will assign some initial distance values and will try to improve them step by step.

1. Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes.
2. Mark all nodes unvisited. Set the initial node as current. Create a set of the unvisited nodes called the unvisited set consisting of all the nodes except the initial node.
3. For the current node, consider all of its unvisited neighbours and calculate their tentative distances. For example, if the current node A is marked with a distance of 6 and the edge connecting it with a neighbour B has length 2, then the distance to B (through A) will be 6+2=8. If this distance is less than the previously recorded tentative distance of B, then overwrite that distance. Even though a neighbour has been examined, it is not marked as "visited" at this time and it remains in the unvisited set.

4. When we are done considering all of the neighbours of the current node, mark the current node as visited and remove it from the unvisited set. A visited node will never be checked again.
5. If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the unvisited set is infinity (when planning a complete traversal), then stop. The algorithm has finished.
6. Select the unvisited node that is marked with the smallest tentative distance and set it as the new "current node" then go back to step 3.

c) ARM basically asks the question — "What is the MAC address of the host in the current network that has a given IP address?" Every host in a LAN uses ARP at some point of time.
RARP asks the reverse question — "What is the IP address that is associated with a given MAC address?" RARP is used mostly by diskless devices to know its own IP address.

10. a) Assume a layered networking architecture. The packet structure in this architecture, as seen at the lowest (physical) layer, is as follows:

AICTE Header	WBUT Header	INSTITUTE Header	STUDENT data

Sketch the layered protocol model that applies to the given architecture (i.e., packet) by labeling each layer in the figure below with the appropriate layer name. Your choices are AICTE, WBUT, INSTITUTE and STUDENT data.

---------- Layer
---------- Layer
---------- Layer
---------- Layer

[WBUT 2014]

Answer:

STUDENT Layer				Student Data
INSTITUTE Layer			Institute Header	Student Data
WBUT Layer		WBUT Header	Institute Header	Student Data
AICTE Layer	AICTE Header	WBUT Header	Institute Header	Student Data

b) In a packet switched network, packets are routed from source to destination along a single path having two intermediate nodes. If messages size is 24 bytes and each packet contains a header of 3 bytes, then find the optimum packet size.
[WBUT 2014]

Answer:

Packet size	Data in packets	Packet require to transmit 24bytes of data	Total header overhead
4	4-3=1	24	24*3=72bytes
6	6-3=3	8	8*3=24bytes
7	7-3=4	6	6*3=18bytes
9	9-3=6	4	4*3=12bytes

So the optimum packet size is 9.

11. a) The following network (Figure 1) uses a distance vector routing protocol. Once the routes have stabilized, the distance vectors at different nodes are as following:

N1: (0,1,7,8,4) N2: (1,0,6,7,3) N3: (7,6,0,2,6)
N4: (8,7,2,0,4) N5: (4,3,6,4,0)

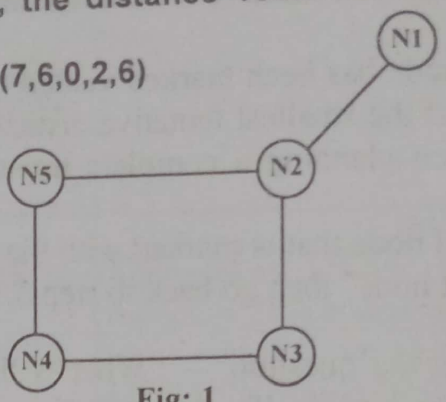


Fig: 1

(i) The cost of link N2-N3 reduces to 2 in both directions. After next round of updates, what will be the new distance vector at node, N3?
(ii) After the updates in the previous questions, the link N1-N2 goes down. N2 will reflect this change immediately in its distance vector as cost∞. After the next round of update, what will be the cost to N1 in distance vector of N3? [WBUT 2014]

Answer:

i) After next round of updates, the new distance vector at node, N3 the new distance vector will be (3,2,0,2,5)

ii) After link between N1-N2 goes down cost to N1 in distance vector of N3 will be ∞.

b) A router has the following RIP routing table: [WBUT 2014]

Net 1	4	B
Net 2	2	C
Net 3	1	F
Net 4	5	G

What would be the contents of the table if the router receives the following RIP message from Router C?

Net 1	2
Net 2	1
Net 3	3
Net 4	7

Answer:

The contents of the table will be

Net 1	3	C
Net 2	2	C
Net 3	1	F
Net 4	5	G

c) An organization is granted the block 211.17.180.124. The administrator wants to create 32 subnets.

i) Find the subnet mask.
ii) Find the number of addresses in each subnet.
iii) Find the first and last address in the first subnet.
iv) Find the first and last address in the last subnet. [WBUT 2014]

Answer:

i) To get 32 usable subnets the subnet mask is
1111 1111.1111 1111.1111 1111.1111 1100 or 255.255.255.252

ii) The usable number of address in each subnet is 2 . 01 and 10

iii) the first and last address in the first subnet is 255.255.255.5 and 255.255.255.6 respectively

iv) the first and last address in the last subnet is
1111 1111.1111 1111.1111 1111.1111 1001 or 255.255.255.249 and 255.255.255.250 respectively

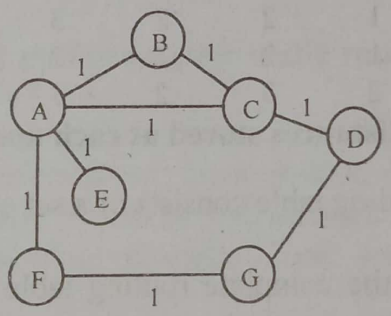
12. Explain Distance Vector Routing with a suitable example. [WBUT 2015, 2017]

Answer:

In Distance Vector Routing each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.

1. The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.
2. A link that is down is assigned an infinite cost.

Example



Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	-	1	1	-
B	1	0	1	-	-	-	-
C	1	1	0	1	-	-	-
D	-	-	1	0	-	-	1
E	1	-	-	-	0	-	-
F	1	-	-	-	-	0	1
G	-	-	-	1	-	1	0

Table 1: Initial distances stored at each node (global view)

We can represent each node's knowledge about the distances to all other nodes as a table like the one given in Table 1.

Each node only knows the information in one row of the table.

1. Every node sends a message to its directly connected neighbors containing its personal list of distance. (for example, A sends its information to its neighbors B,C,E, and F.)

2. If any of the recipients of the information from A find that A is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through A. (node B learns from A that node E can be reached at a cost of 1; B also knows it can reach A at a cost of 1, so it adds these to get the cost of reaching E by means of A. B records that it can reach E at a cost of 2 by going through A.)
3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.
4. In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table. (for example, B knows that it was A who said " I can reach E in one hop" and so B puts an entry in its table that says " To reach E, use the link to A.)

Information	Distance to Reach Node						
Stored at Node	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Table 2: final distances stored at each node (global view)

In practice, each node's forwarding table consists of a set of triples of the form: (Destination, Cost, NextHop).

For example, Table 3 shows the complete routing table maintained at node B for the network in figure1.

Destination	Cost	NextHop
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A

Table 3: Routing table maintained at node B

13. a) What is CIDR notation? What is its significance in case of classless addressing? **[WBUT 2015]**

Answer:

CIDR (Classless Inter-Domain Routing, sometimes called supernetting) is a way to allow more flexible allocation of Internet Protocol (IP) addresses than was possible with the original system of IP address classes. As a result, the number of available Internet addresses was greatly increased, which along with widespread use of network address translation (NAT), has significantly extended the useful life of IPv4.

b) What do you mean by a private address? What is NAT? [WBUT 2015]

Answer:

1st Part:

An IP address is considered private if the IP number falls within one of the IP address ranges reserved for private uses by Internet standards groups. These private IP address ranges exist:

10.0.0.0 through 10.255.255.255
169.254.0.0 through 169.254.255.255 (APIPA only)
172.16.0.0 through 172.31.255.255
192.168.0.0 through 192.168.255.255

Private IP addresses are typically used on local networks including home, school and business LANs including airports and hotels.

Devices with private IP addresses cannot connect directly to the Internet.

2nd Part:

Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

14. Why is dynamic routing preferred over static routing algorithm in the network, which changes continuously? [WBUT 2016]

Answer:

Dynamic routing: This is preferred over static routing in mid and large-sized networks. Dynamic routes are routes discovered by the network routing protocols and adjusted automatically for traffic or topology changes. There are two types of dynamic routing protocols:

Distance-vector protocols such as routing information protocol (RIP) and interior gateway routing protocol (IGRP)

Link-state protocols such as open shortest path first (OSPF) and intermediate system to intermediate system (IS-IS).

The use of static routes for multicast RPF suffers from the same drawbacks as using static routes for unicast routing. Network topology is constantly changing. Dynamic routing protocols automatically adapt to such changes, but static routes require human intervention when topology changes occur. Thus the use of dynamic routing protocols to populate the multicast RPF table is preferred over static routing.

15. a) A class B network on the internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts per subnet? [WBUT 2016]

Answer:

- For a class-B network, the upper 16-bits form the network address and the lower 16-bits are the subnet and host fields.

- Of the lower 16-bits, the most significant 4-bits are: 1111. This leaves 12-bits for the host number, so 4096 host addresses exist. Address 0 and 1 are special, so the maximum number of host is 4094.

b) An ISP has a block of 1024 addresses. It needs to divide the address among 1024 customers. Does it need subnetting? Justify. [WBUT 2016]

Answer:

No. Because when we perform subnetting, some IP addresses will be unusable as they will be assigned for network and broadcast addresses.

If we have one IP per customer, then we do not need smaller subnets.

There will only be 1022 addresses usable. The first and the last address of the block will be the network and the broadcast address.

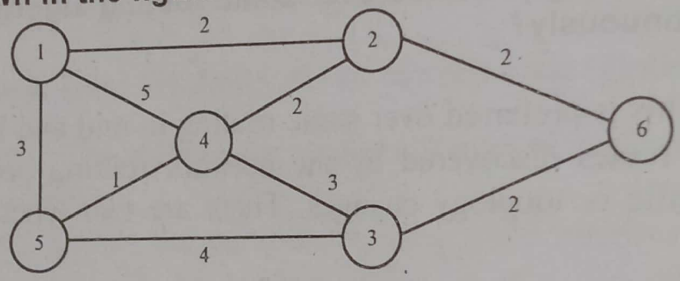
16. a) Describe the fields of an IP Datagram.

b) An IP network 192.168.130.0 is using the subnet mask 255.255.255.224. Determine the number of subnet of hosts in each subnet and from what subnet the following hosts belong to:

192.168.130.10 192.168.130.93

192.168.130.222 192.168.130.250

c) Apply Dijkstra's algorithm to find the shortest path from node 4 to node 6 of the network graph shown in the figure below: [WBUT 2017]



Answer:

a) ***Refer to Question No. 12 (1st part) of Short Answer Type Questions.***

b) For finding the number of subnets and the number of hosts in each subnet, we need to know the number of masked and unmasked bits in the subnet mask, which can be found as follows:

Given subnet mask = 255.255.255.224

The binary equivalent of host ID byte (that is, 24) is 11100000. Here, three bits are 1s while five bits are 0s. Thus, the number of masked bits (m) is 3 and the number of unmasked bits (n) is 5. Now, the number of subnets and the number of hosts in each subnet can be determined as follows:

Number of subnets = $2^m = 2^3 = 8$

Number of hosts in each subnet = $2^n - 2 = 2^5 - 2 = 30$

Thus, there are eight subnets in the network with each subnet comprising 30 hosts. As the given IP network is 192.168.130.0, the range of IP addresses assigned to each subnet can be given as follows:

Range of 1st subnet: 192.168.130.0 – 192.168.130.31

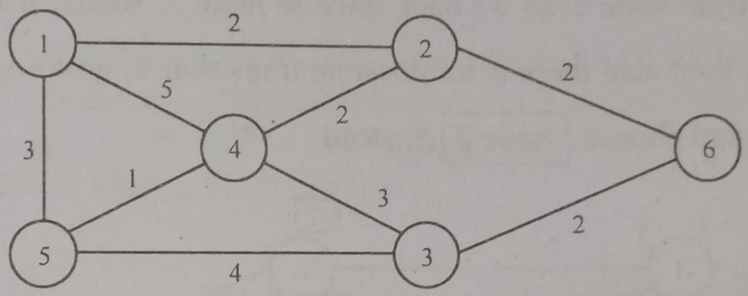
Range of 2nd subnet: 192.168.130.32 – 192.168.130.63

Range of 3rd subnet: 192.168.130.64 – 192.168.130.95
Range of 4th subnet: 192.168.130.96 – 192.168.130.127
Range of 5th subnet: 192.168.130.128 – 192.168.130.159
Range of 6th subnet: 192.168.130.160 – 192.168.130.191
Range of 7th subnet: 192.168.130.192 – 192.168.130.223
Range of 8th subnet: 192.168.130.224 – 192.168.130.255

The first and last address of each range cannot be assigned to hosts. For example, in the first subnet, the address 192.168.130.0 and 192.168.130.31 cannot be used for the hosts.

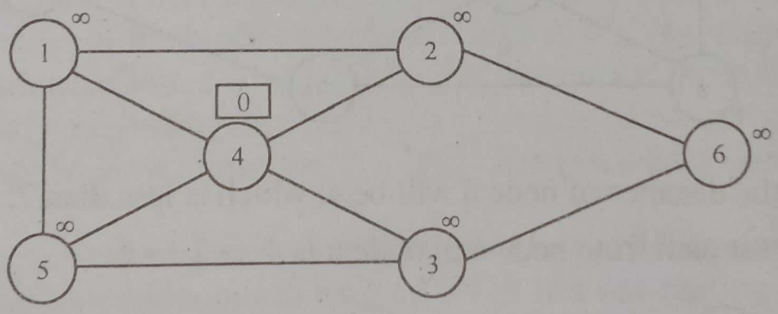
Therefore, 192.168.130.10 belongs to the first subnet.
192.168.130.93 belongs to the 3rd subnet.
192.168.130.222 belongs to the 7th subnet and,
192.168.130.250 belongs to the 8th subnet.

c)



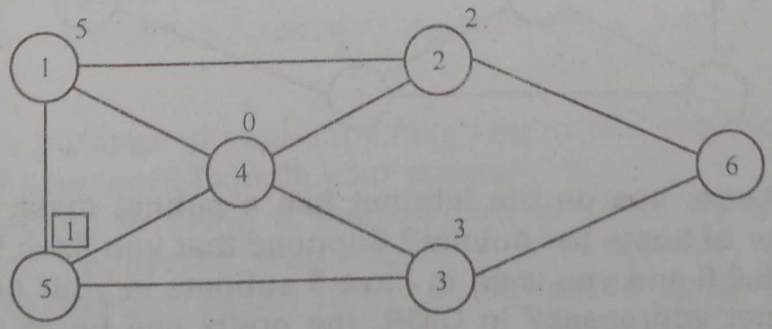
In the above, 4 is the root node initiated to 0 and other are set to ∞.

Step 1:



Step 2:

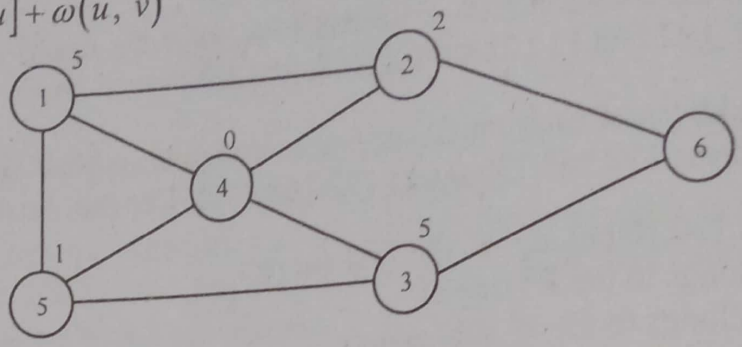
As, node 4 is connected to 1, 2, 3 and 5, so it visits the adjacent nodes.



Step 3:

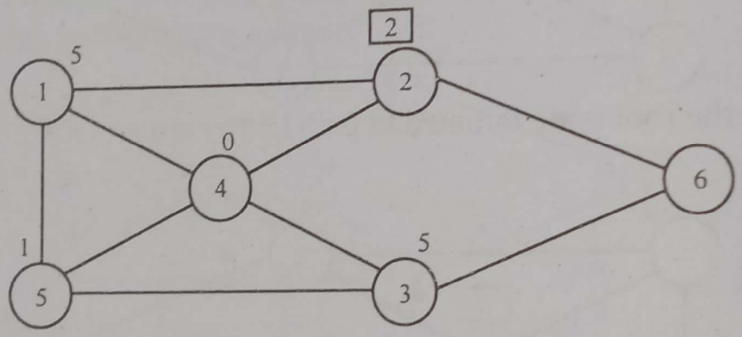
Taking, node 5, proceed such that if $d[u]+\omega(u+v)<d[v]$. Then,

$$d[v]=d[u]+\omega(u,\ v)$$



Step 4:

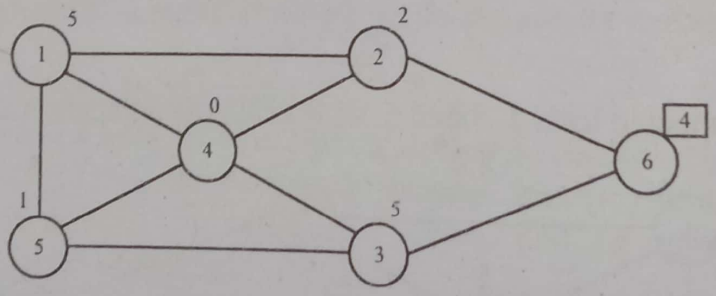
Now, if we take node 3, then the distance of node 6 will be 7. Since, there is no other transition possible from node 3, so we back track to node 5. Again, from node 5, if we consider node 1, then also there is no possible transition to go to node 6. So, we back track to node 4, and choose node 2 instead.



Step 5:

Taking, node 2, the distance of node 6 will be 4, which is less than 7.

Therefore, the shortest path from node 4 to node 6 is $4 \rightarrow 2 \rightarrow 6$.



17. A Class-B network has on the Internet has a subnet mask of 255.255.240.0. What is the number of hosts per subnet? Suppose that you have been assigned an IP address 132.128.0.0 and you wish to have 9 subnets in your organization. What could be the subnet addresses? In CIDR, the prefix can be of any length unlike fixed 8, 16 or 24 in Classful addressing for Class A, B or C respectively. What is its use?

[WBUT 2018]

Answer:

1st part:

Netmask:	255.	255.	255.	255
Binary:	11111111	11111111	11111111	11111111
Netmask length	8	16	24	32

A commonly used netmask is a 24-bit netmask as seen below.

Netmask:	255.	255.	255.	0
Binary:	11111111	11111111	11111111	00000000
Netmask length	8	16	24	--

255.255.240.0
maximum hosts :-total number of bits for host = (4+8) = 12
So no. of hosts = (2^12-2) = 4096–2 = 4094

2nd part:

The Network is clearly of Class-B. Hence, there can be about 2^{16} hosts in total. But we need 500 hosts per sub-network. The nearest power of 2 greater than or equal to 9 is $16 = 2^4$. Hence, we can create $2^{16}/2^4 = 2^{12} = 4096$ sub-networks.
We will use the sub-net mask 255.255.254.0.

3rd Part:

To illustrate the problems with the class system, consider that one of the most commonly used classes was Class B. An organization that needed more than 254 host machines would often get a Class B license, even though it would have far fewer than 65,534 hosts. This resulted in most of the block of addresses allocated going unused. The inflexibility of the class system accelerated IPv4 address pool exhaustion. With IPv6, addresses grow to 128 bits, greatly expanding the number of possible addresses on the Internet. The transition to IPv6 is slow, however, so IPv4 address exhaustion continues to be a significant issue.
CIDR reduced the problem of wasted address space by providing a new and more flexible way to specify network addresses in routers. CIDR lets one routing table entry represent an aggregation of networks that exist in the forward path that don't need to be specified on that particular gateway. This is much like how the public telephone system uses area codes to channel calls toward a certain part of the network. This aggregation of networks in a single address is sometimes referred to as a *supernet*.

18. a) What is the purpose of sequence numbers in TCP segment? Why is padding required for TCP segment? Explain your answer. [WBUT 2019]
b) A TCP connection is using a window size of 10000 bytes and the previous acknowledgement number was 22,001. It receives a segment with acknowledgement number 24,001. Draw a diagram to show the situation of the window before and after. [WBUT 2019]

Answer:

a) 1st Part:

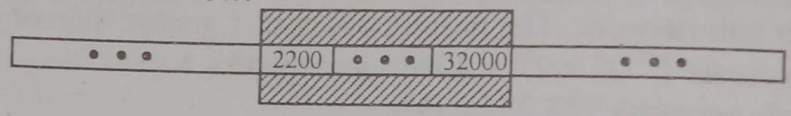
Purpose of sequence number in TCP segment:

A TCP connection is a method of transmitting two byte streams, one stream in each direction. To map the unordered, unreliable bytes in IP packets to the ordered bytes in this stream, each byte in each stream is identified by a sequence number. The TCP header contains the sequence number of the first byte in this segment. TCP packets can contain an acknowledgements, which is the sequence number of the next byte the sender expects to receive. The sequence number field is 32 bits. This implies each byte stream can be upto 2^{32} bytes.

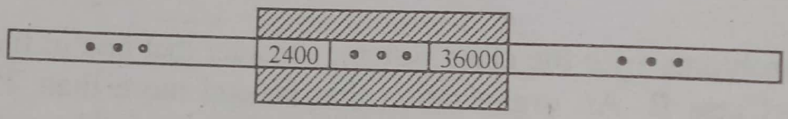
2nd Part:

The TCP header padding is required to used for the TCP header ends data begins on a 32 bit boundary. This padding is composed of zeros. This padding field must only be sent in the initial connection request.

b) The diagram is shown in below:



a. Sliding window before



b. Sliding window after

19. Write short notes on the following:

a) RIP [WBUT 2010, 2016]
b) NAT [WBUT 2011]
c) IPv6 [WBUT 2011, 2019]
d) OSPF [WBUT 2016]
e) BGP [WBUT 2016]
f) ARP packet format [WBUT 2016]
g) ICMP [WBUT 2017]
h) IP Data gram [WBUT 2018]
i) IP Addressing [WBUT 2018]

Answer:

a) RIP:

RIP is a dynamic, distance vector routing protocol based around the Berkely BSD application routed and was developed for smaller IP based networks. RIP uses UDP port 520 for route updates. RIP calculates the best route based on hop count. Like all distance vector routing protocols, RIP takes some time to converge. While RIP requires less CPU power and RAM than some other routing protocols, RIP does have some limitations:

Metric: Hop Count

Since RIP calculates the best route to a destination based solely on how many hops it is to the destination network, RIP tends to be inefficient in network using more than one LAN

protocol, such as Fast Ethernet and serial or Token Ring. This is because RIP prefers paths with the shortest hop count. The path with the shortest hop count might be over the slowest link in the network.

Hop Count Limit

RIP cannot handle more than 15 hops. Anything more than 15 hops away is considered unreachable by RIP. This fact is used by RIP to prevent routing loops.

Classful Routing Only

RIP is a classful routing protocol. RIP cannot handle classless routing. RIP v1 advertises all networks it knows as classful networks, so it is impossible to subnet a network properly via VLSM if you are running RIP v1, which

However, it must be pointed out that RIP is the only routing protocol that all routing devices and software support, so in a mixed equipment environment, RIP may be your only option for dynamic routing. This is changing with the widespread use of OSPF.

The routing-update timer controls the time between routing updates. Default is usually 30 seconds, plus a small random delay to prevent all RIP routers from sending updates simultaneously.

The route-timeout timer controls when a route is no longer available. The default is usually 180 seconds. If a router has not seen the route in an update during this specified interval, it is dropped from the router's announcements. The route is maintained long enough for the router to advertise the route as down (hop count of 16).

b) NAT:

The Internet has grown larger than anyone ever imagined it could be. Although the exact size is unknown, the current estimate is that there are about 100 million hosts and over 350 million users actively on the Internet. In fact, the rate of growth has been such that the Internet is effectively doubling in size each year. NAT allows an Internet Protocol (IP) network to maintain public IP addresses separately from private IP addresses. NAT is a popular technology for Internet connection sharing. It is also sometimes used in server load balancing applications on corporate networks.

In it's most common configuration, NAT maps all of the private IP addresses on a home network to the single IP address supplied by an Internet Service Provider (ISP). This allows computers on the home LAN to share a single Internet connection. Additionally, it enhances home network security by limiting the access of external computers into the home IP network space.

NAT works by snooping both incoming and outgoing IP datagrams. As needed, it modifies the source or destination address in the IP header (and the affected checksums) to reflect the configured address mapping. NAT technically supports either fixed or dynamic mappings of one or more internal and external IP addresses.

NAT functionality is usually found on routers and other gateway devices at the network boundary. NAT can also be implemented entirely in software. Microsoft's Internet Connection Sharing (ICS), for example, adds NAT support to the Windows operating system.

By itself, NAT does not provide all the features of a true firewall, but it is often used on servers that feature other firewall and antivirus support. NAT was designed originally to conserve public Internet address space. Internet RFC 1631 contains the basic NAT specification.

c) IPv6:

IP Version 6 (IPv6) is the newest version of IP. IPv6 is fairly well defined but is not yet widely deployed. The main differences between IPv6 and the current widely-deployed version of IP (which is IPv4) are:

- IPv6 uses larger addresses (128 bits instead of 32 bits in IPv4) and so can support many more devices on the network.
- IPv6 includes features like authentication and multicasting that had been bolted on to IPv4 in a piecemeal fashion over the years.

The main improvement brought by **IPv6** (Internet Protocol version 6) is the increase in the number of addresses available for networked devices, allowing, for example, each mobile phone and mobile electronic device to have its own address. IPv4 supports 2^{32} (about 4.3 billion) addresses, which is inadequate for giving even one address to every living person, let alone supporting embedded and portable devices. IPv6, however, supports 2^{128} addresses; this is approximately 5×10^{28} addresses for *each* of the roughly 6.5 billion people alive today. With such a large address space available, IPv6 nodes can have as many universally scoped addresses as they need, and network address translation is not required.

d) OSPF:

The OSPF routing protocol has largely replaced the older Routing Information Protocol (RIP) in corporate networks. Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information. Unlike RIP, which requires routers to send the entire routing table to neighbors every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place. When routes change -- sometimes due to equipment failure -- the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.

Rather than simply counting the number of router hops between hosts on a network, as RIP does, OSPF bases its path choices on "link states" that take into account additional network information, including IT-assigned cost metrics that give some paths higher assigned costs. For example, a satellite link may be assigned higher cost than a wireless WAN link, which in turn may be assigned higher cost than a metro Ethernet link.

Features and advantage of OSPF

- It supports both IPv4 and IPv6 routed protocols.
- It supports load balancing with equal cost routes for same destination.
- Since it is based on open standards, it will run on most routers.
- It provides a loop free topology using SPF algorithm.

- It is a classless protocol.
- It supports VLSM and route summarization.
- It supports unlimited hop counts.
- It scales enterprise size network easily with area concept.
- It supports trigger updates for fast convergence.

Just like other routing protocols, OSPF also has its negatives.

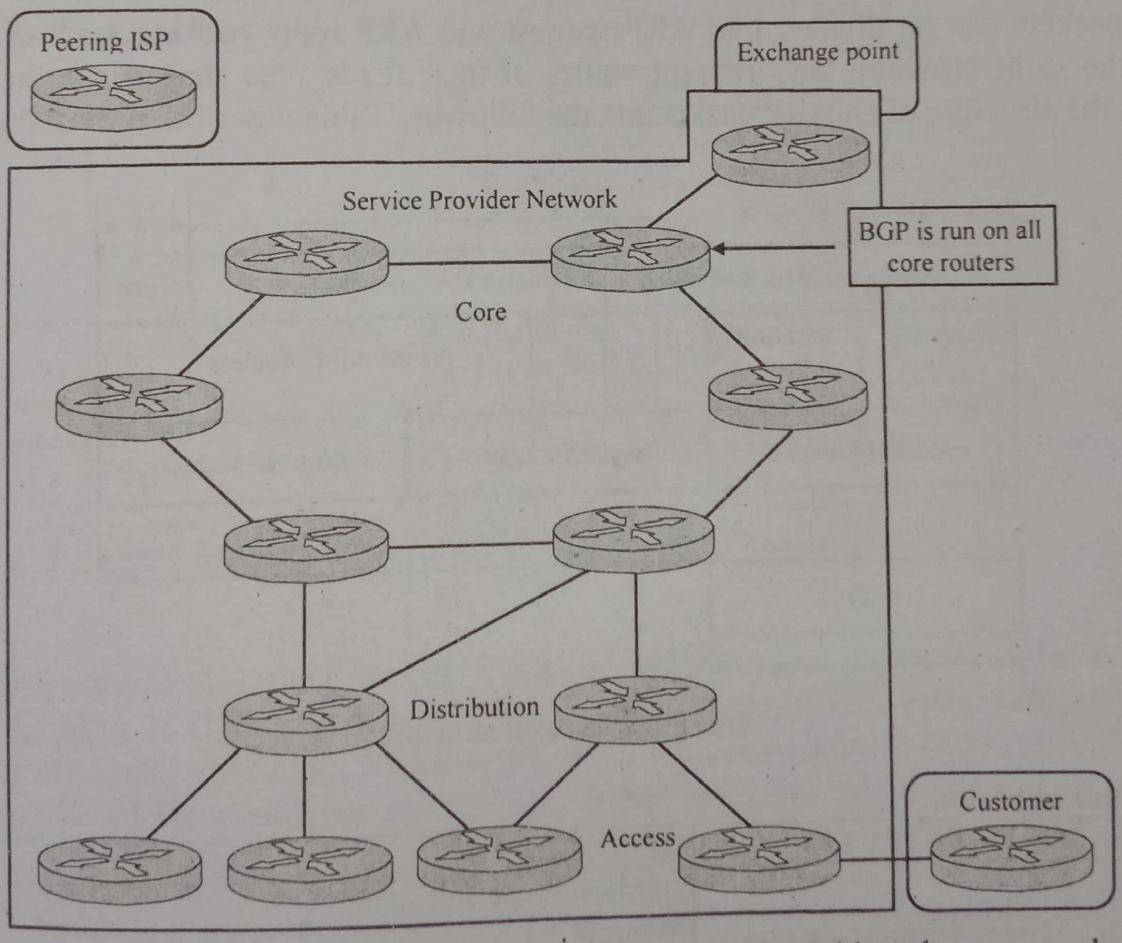
Disadvantage of OSPF

- It requires extra CPU process to run SPF algorithm.
- It requires more RAM to store adjacency topology.
- It is more complex to setup and hard to troubleshoot.

This tutorial is the first part of our article "OSPF Routing Protocol Explained with examples". You can read other parts of this article here.

e) BGP:

BGP (Border Gateway Protocol) is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers. BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider.



BGP offers network stability that guarantees routers can quickly adapt to send packets through another reconnection if one internet path goes down. BGP makes routing decisions based on paths, rules or network policies configured by a network

administrator. Each BGP router maintains a standard routing table used to direct packets in transit. This table is used in conjunction with a separate routing table, known as the routing information base (RIB), which is a data table stored on a server on the BGP router. The RIB contains route information both from directly connected external peers, as well as internal peers, and continually updates the routing table as changes occur. BGP is based on TCP/IP and uses client-server topology to communicate routing information, with the client-server initiating a BGP session by sending a request to the server. BGP sends updated router table information only when something changes -- and even then, it sends only the affected information. BGP has no automatic discovery mechanism, which means connections between peers have to be set up manually, with peer addresses programmed in at both ends.

BGP makes best-path decisions based on current reachability, hop counts and other path characteristics. In situations where multiple paths are available -- as within a major hosting facility -- BGP can be used to communicate an organization's own preferences in terms of what path traffic should follow in and out of its networks. BGP even has a mechanism for defining arbitrary tags, called communities, which can be used to control route advertisement behavior by mutual agreement among peers.

f) ARP packet format:

ARP packets can be divided into ARP request and ARP reply packets, both of which have the same structure but different values of their fields. The shaded area in Fig. 1 shows the structure of an ARP packet and the following Table describes the ARP packets fields.

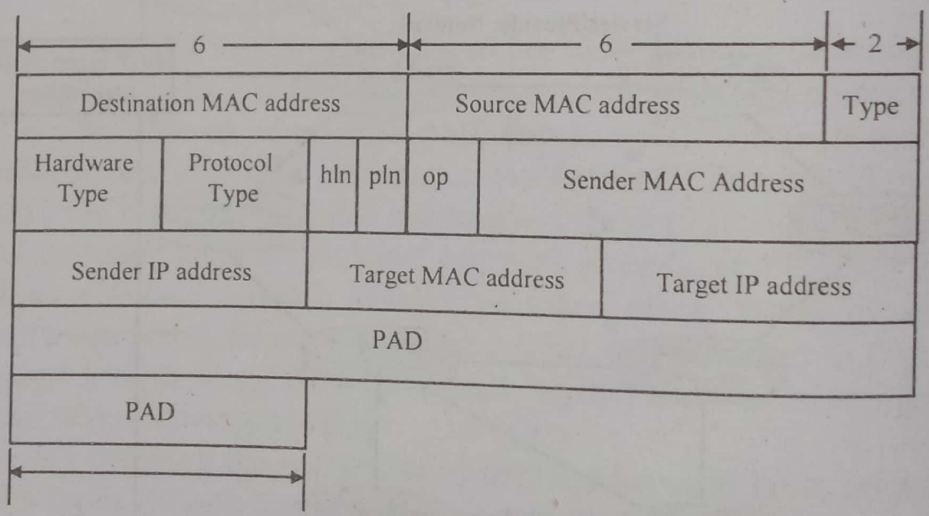


Fig: 1 ABP packet structure

ARP Packet Fields

FIELD NAME	SIZE (BYTE)	DESCRIPTION
HRD	2	Hardware type and value. Ethernet = 1 IEEE 802 networks = 6 ARCNET = 6 Frame Relay = 15

<table>
<tr><th>FIELD NAME</th><th>SIZE (BYTE)</th><th>DESCRIPTION</th></tr>
<tr><td></td><td></td><td>Asynchronous Transfer Mode (ATM) = 16
HDLC = 17
Fibre Channel = 18
Asynchronous Transfer Mode (ATM) = 19
Serial Line = 20</td></tr>
<tr><td>PRO</td><td>2</td><td>this is a compliment for the Hardware type field, specifying the type of layer being used in the messages. For IPv4, the value is 2048, which also corresponds to the Ether code for the Internet Protocol.</td></tr>
<tr><td>HLN</td><td>1</td><td>this is there to specify the length of the hardware relates addresses that are there in the message.</td></tr>
<tr><td>PLN</td><td>1</td><td>this specifies how long will the protocol address is going to be in the message.</td></tr>
<tr><td>OP</td><td>2</td><td>This field demonstrates the nature of the ARP message. The first two values (i.e. 0 and 1) are being used for regular ARP. other values are being defined have a look at the below-mentioned table –
<table>
<tr><th>OpCode</th><th>ARP Message Type</th></tr>
<tr><td>1</td><td>ARP Request</td></tr>
<tr><td>2</td><td>ARP Reply</td></tr>
<tr><td>3</td><td>RARP Request</td></tr>
<tr><td>4</td><td>RARP Reply</td></tr>
<tr><td>5</td><td>DRARP Request</td></tr>
<tr><td>6</td><td>DRARP Reply</td></tr>
<tr><td>7</td><td>DRARP Error</td></tr>
<tr><td>8</td><td>InARP Request</td></tr>
<tr><td>9</td><td>InARP Reply</td></tr>
</table></td></tr>
<tr><td>SHA</td><td>Equal to HLN field</td><td>Deals with the hardware address of the device that is sending the message</td></tr>
<tr><td>SPA</td><td>Equal to PLN field</td><td>The IP address of the device which is sending the message</td></tr>
<tr><td>THA</td><td>Equals to HLN field</td><td>The hardware address of the device which is receiving the message</td></tr>
<tr><td>TPA</td><td>Equals to PLN field</td><td>The IP address of the dev</td></tr>
</table>

g) ICMP:

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network.

- The ICMP header starts after the IPv4 header.
- All ICMP packets will have an 8 byte header and variable sized data section.
- The first 4 bytes of the header will be consistent. The first byte is for the ICMP type. The second byte is for the ICMP code. The third and fourth bytes are a checksum of the entire ICMP message.
- The contents of the remaining 4 bytes of the header will vary based on the ICMP type and code.

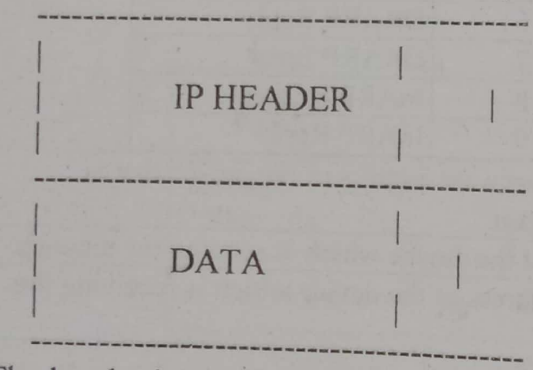
ICMP error messages contain a data section that includes the entire IP header plus the first 8 bytes of the packet that generated the error message. The ICMP datagram is then encapsulated in a new IP datagram.

its	0-7	8-15	16-23	24-31
0	Type	Code	Checksum	
32	Rest of Header			

- Type - ICMP type as specified below.
- Code - Subtype to the given type.
- Checksum - Error checking data. Calculated from the ICMP header + data, with value 0 for this field. The algorithm is the same as the header checksum for IPv4.
- Rest of Header - Eight byte field. Will vary based on the ICMP type and code.

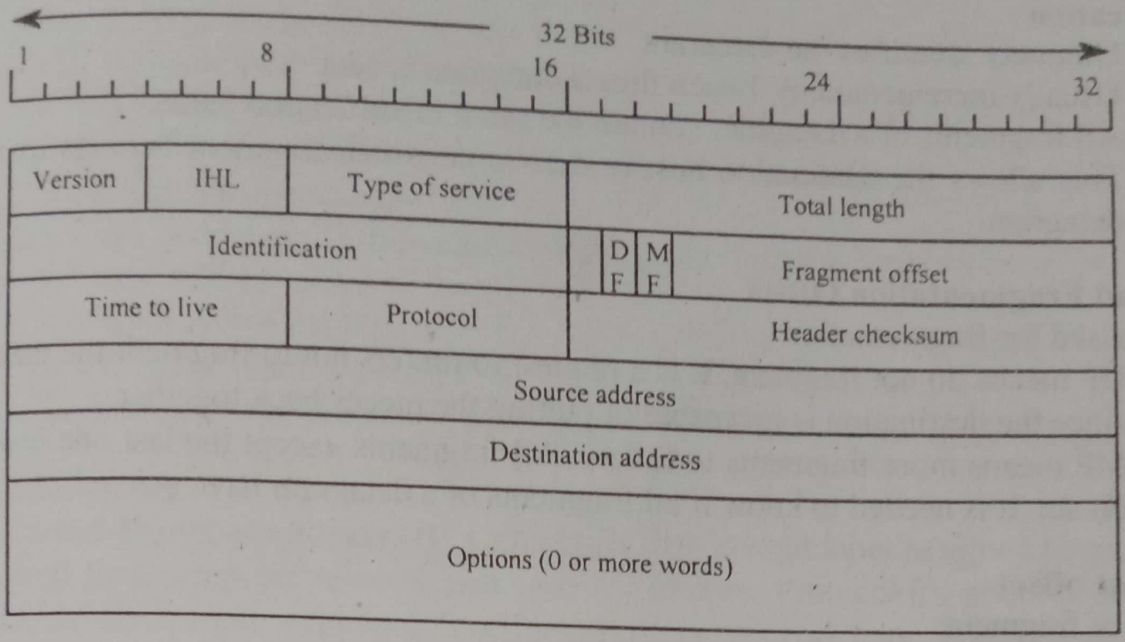
h) IP data gram:

An IP datagram consists of a header part and text part.



The header has a 20 bytes fixed part and a variable length optional part. It is transmitted in big endian order. (On little endian machines, software conversion is required).

The IP datagram header format



Version

- Which version of the protocol the datagram belongs to.
- The current version number is 4.
- Next version: 6

IHL

- The number of 32-bit words in the header
- Because this is 4 bits, the max header length is 15 words (i.e. 60 bytes)
- The header is at least 20 bytes, but options may make it bigger

Type of Service

- Contains a 3-bit precedence field (that is ignored today), 4 service bits, and 1 unused bit.
- The four service bits can be:
  - 1000 - minimize delay
  - 0100 - maximize throughput
  - 0010 - maximize reliability
  - 0001 - minimize monetary cost
- This is a "hint" of what characteristics of the physical layer to use
- The Type of Service is not supported in most implementations. However, some implementations have extra fields in the routing table to indicate delay, throughput, reliability, and monitary cost.

Total Length

- total length of the datagram in bytes.
- we know where the data starts by the header length
- we know the size of the data by computing "total length - header length"

Identification

- Uniquely identifies the datagram.
- Usually incremented by 1 each time a datagram is sent.
- All fragments of a datagram contain the same identification value.
- This allows the destination host to determine which fragment belongs to which datagram.

Flags and Fragmentation Offset

- Used for fragmentation
- DF means do not fragment. It is a request to routers not to fragment the datagram since the destination is incapable of putting the pieces back together.
- MF means more fragments to follow. All fragments except the last one have this bit set. It is needed to know if all fragments of a datagram have arrived.

Fragment offset

Number of fragment.

Time to Live

- Upper limit of routers
- usually set to 32 or 64.
- decremented by each router that processes the datagram,
- router discards the datagram when TTL reaches 0.

Protocol

- Tells IP where to send the datagram up to.
- 6 means TCP
- 17 means UDP

Header checksum

Only covers the header, not the data.

Source IP address

The sender

Destination IP address

The final destination

Options

- Optional data.
- Some examples include having the router put in a IP address of router and a time stamp so the final destination knows how long it took to get to each hop.

The source and destination in the IP header is the original source and the final destination! The physical layer addresses pass the datagram from router to router. So, while the physical layer addresses change from router to router, the source and destination IP addresses in the IP datagram remain constant!

The checksum

- How to compute a checksum?
  - Put a 0 in the checksum field.
  - Add each 16-bit value together.
  - Add in any carry
  - Inverse the bits and put that in the checksum field.
- To check the checksum:
  - Add each 16-bit value together (including the checksum).
  - Add in carry.
  - Inverse the bits.
  - The result must be 0.
- Remember, only the bits in the header are calculated in the IP checksum.

i) IP Addressing:

An **Internet Protocol address (IP address)** is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was developed in 1995, and standardized in December 1998. In July 2017, a final definition of the protocol was published. IPv6 deployment has been ongoing since the mid-2000s.

IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 in IPv4, and 2001:db8:0:1234:0:567:8:1 in IPv6. The size of the routing prefix of the address is designated in CIDR notation by suffixing the address with the number of significant bits, e.g., 192.168.1.15/24, which is equivalent to the historically used subnet mask 255.255.255.0.

The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIRs) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers. IPv4 addresses have been distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each. Each ISP or private network administrator assigns an IP address to each device connected to its network. Such assignments may be on a *static* (fixed or permanent) or *dynamic* basis, depending on its software and practices.

TRANSPORT LAYER

Multiple Choice Type Questions

1. Flow control is the responsibilities of the [WBUT 2011]
a) Data link layer b) Transport layer c) Both of these d) none of these
Answer: (c)

2. UDP is [WBUT 2014, 2016]
a) connection-oriented b) connection-less
c) both (a) and (b) d) none of these
Answer: (b)

3. Which of the following is a technique to improve Quality of Service? [WBUT 2015]
a) Traffic Shaping b) Resource Reservation
c) Admission Control d) All of the above
Answer: (d)

4. Exponential increase is used in [WBUT 2016]
a) Slow start b) Congestion avoidance
c) Congestion detection d) none of these
Answer: (a)

5. Port number is [WBUT 2016]
a) process number b) computer physical address
c) both (a) and (b) d) none of these
Answer: (a)

6. The two parameters used for measuring the performance of a network are [WBUT 2017]
a) throughput & delay b) power & delay
c) power and throughput d) throughput & buffer size
Answer: (a)

7. Connection establishment involves a ..... way handshake in TCP. [WBUT 2017]
a) one b) two c) three d) four
Answer: (c)

8. Connection establishment in TCP involves a _____ handshake. [WBUT 2018]
a) one-way b) two-way c) three-way d) None of these
Answer: (c)

9. Port number in packet indicates [WBUT 2018]
   a) LAN card port number in a computer
   b) Host identification number in network
   c) Unique number for a communication process
   d) PID number of a communicating process under OS

Answer: (d)

10. Segmentation is done in [WBUT 2018]
   a) physical layer
   b) data link layer
   c) network layer
   d) transport layer

Answer: (d)

11. Which of the following is a mandatory part of the IPv6 datagram? [WBUT 2019]
   a) Base header
   b) Extension header
   c) Data packet from upper layer
   d) none of these

Answer: (b)

12. What is a common authentication protocol used for digital signature? [WBUT 2019]
   a) Kerberos
   b) Digital signature
   c) PKI
   d) None of these

Answer: (a)

Short Answer Type Questions

1. Explain Leaky bucket algorithm for congestion control. [WBUT 2007, 2012]

Answer:

The leaky bucket is an algorithm used in packet switched computer networks and telecommunications networks to check that data transmissions conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). The leaky bucket algorithm is also used in leaky bucket counters, e.g. to detect when the average or peak rate of random or stochastic events or stochastic processes exceed defined limits.

The Leaky Bucket Algorithm is based on an analogy of a bucket .that has a hole in the bottom through which any water it contains will leak away at a constant rate, until or unless it is empty. Water can be added intermittently, i.e. in bursts, but if too much is added at once, or it is added at too high an average rate, the water will exceed the capacity of the bucket, which will overflow.

There are actually two different methods of applying this analogy described in the literature .These give what appear to be two different algorithms, both of which are referred to as the leaky bucket algorithm. This has resulted in confusion about what the leaky bucket algorithm is and what its properties are.

In one version, the analogue of the bucket is a counter or variable, separate from the flow of traffic, and is used only to check that traffic conforms to the limits, i.e. the analogue of the water is brought to the bucket by the traffic and added to it so that the level of water

in the bucket indicates conformance to the rate and burstiness limits. This version is referred to here as the leaky bucket as a meter. In the second version, the traffic passes through a queue that is the analogue of the bucket, i.e. the traffic is the analogue of the water passing through the bucket. This version is referred to here as the leaky bucket as a queue. The leaky bucket as a meter is equivalent to (a mirror image of) the token bucket algorithm, and given the same parameters will see the same traffic as conforming or nonconforming. The leaky bucket as a queue can be seen as a special case of the leaky bucket as a meter.

2. Besides bandwidth and latency, which other parameters are needed to give a good characterization of QoS offered by a network used for digitized voice traffic? **[WBUT 2007, 2009]**

OR,

Describe Quality of Service (QoS). **[WBUT 2017]**

Answer:

QoS (Quality of Service) refers to a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. Elements of network performance within the scope of QoS often include availability (uptime), bandwidth (throughput), latency (delay), and error rate.

QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications. A network monitoring system must typically be deployed as part of QoS, to insure that networks are performing at the desired level.

QoS is especially important for the new generation of Internet applications such as VoIP, video-on-demand and other consumer services. Some core networking technologies like Ethernet were not designed to support prioritized traffic or guaranteed performance levels, making it much more difficult to implement QoS solutions across the Internet.

3. Explain in detail. What is admission control? **[WBUT 2015]**

Answer:

Admission Control is a validation process in communication systems where a check is performed before a connection is established to see if current resources are sufficient for the proposed connection.

In order for an admission control scheme to be successful in practice, it needs to fulfill several requirements:

- Robustness: An admission control scheme must ensure that the requested QoS is provided and is robust with respect to traffic heterogeneity, time-scale fluctuations (long-range dependency), as well as to heavy offered traffic loads.
- Resource utilization: The secondary goal for admission control is to maximize resource utilization, subject to the QoS constraints for the admitted flows.
- Implementation: The cost of deploying an admission control scheme must be smaller than its benefits. In addition, the traffic characteristics required by the scheme should be easily obtained from the traffic sources and the network and, also, the scheme should scale well with the number of flows.

4. Compare Leaky Bucket Algorithm with Token Bucket Algorithm. [WBUT 2017]

Answer:

Comparison of Leaky Bucket Algorithm with Token Bucket Algorithm:

a. Leaky bucket is token independent whereas Token bucket is dependent.
b. In case of leaky bucket, if bucket is full, packet or data is discarded. But in case of token bucket, if bucket is full then token are discarded but not the packet.
c. In leaky bucket, packets are transmitted continuously whereas in token bucket, packets can be transmitted only when there are enough tokens.
d. Leaky bucket sends the packet at constant rate. But token bucket allows large bursts to be sent at faster rate after that constant rate.
e. Leaky bucket does not save token but token bucket saves token to send large bursts.

Long Answer Type Questions

1. a) What is congestion? Why do congestion occur? Explain Leaky bucket algorithm for congestion control. [WBUT 2011, 2018]

b) State the basic differences between TCP and UDP. [WBUT 2011, 2018, 2019]

OR,

Compare TCP with UDP. [WBUT 2017]

Answer:

a) Network congestion is the situation in which an increase in data transmissions results in a proportionately smaller increase, or even a reduction, in throughput.

Throughput is the amount of data that passes through the network per unit of time, such as the number of packets per second. Packets are the fundamental unit of data transmission on the Internet and all other TCP/IP (transmission control protocol/Internet protocol) networks, including most LANs (local area networks).

Congestion results from applications sending more data than the network devices (e.g., routers and switches) can accommodate, thus causing the buffers on such devices to fill up and possibly overflow. A buffer is a portion of a device's memory that is set aside as a temporary holding place for data that is being sent to or received from another device. This can result in delayed or lost packets, thus causing applications to retransmit the data, thereby adding more traffic and further increasing the congestion.

The leaky bucket is an algorithm used in packet switched computer networks and telecommunications networks to check that data transmissions conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). The leaky bucket algorithm is also used in leaky bucket counters, e.g. to detect when the average or peak rate of random or stochastic events or stochastic processes exceed defined limits.

The Leaky Bucket Algorithm is based on an analogy of a bucket .that has a hole in the bottom through which any water it contains will leak away at a constant rate, until or unless it is empty. Water can be added intermittently, i.e. in bursts, but if too much is added at once, or it is added at too high an average rate, the water will exceed the capacity of the bucket, which will overflow.

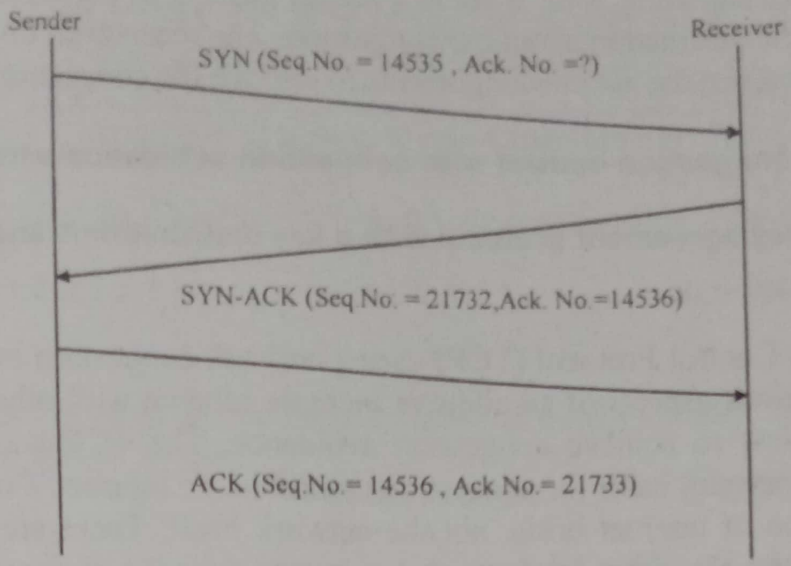
There are actually two different methods of applying this analogy described in the literature. These give what appear to be two different algorithms, both of which are referred to as the leaky bucket algorithm. This has resulted in confusion about what the leaky bucket algorithm is and what its properties are.
In one version, the analogue of the bucket is a counter or variable, separate from the flow of traffic, and is used only to check that traffic conforms to the limits, i.e. the analogue of the water is brought to the bucket by the traffic and added to it so that the level of water in the bucket indicates conformance to the rate and burstiness limits. This version is referred to here as the leaky bucket as a meter. In the second version, the traffic passes through a queue that is the analogue of the bucket, i.e. the traffic is the analogue of the water passing through the bucket. This version is referred to here as the leaky bucket as a queue. The leaky bucket as a meter is equivalent to (a mirror image of) the token bucket algorithm, and given the same parameters will see the same traffic as conforming or nonconforming. The leaky bucket as a queue can be seen as a special case of the leaky bucket as a meter.

b)

TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
TCP is a connection-oriented protocol, a connection can be made from client to server, and from then on any data can be sent along that connection.	A simpler message-based connectionless protocol. With UDP you send messages (packets) across the network in chunks.
Reliable - when you send a message along a TCP socket, you know it will get there unless the connection fails completely. If it gets lost along the way, the server will re-request the lost part. This means complete integrity, things don't get corrupted.	**Unreliable** - When you send a message, you don't know if it'll get there, it could get lost on the way.
Ordered - if you send two messages along a connection, one after the other, you know the first message will get there first. You don't have to worry about data arriving in the wrong order.	**Not ordered** - If you send two messages out, you don't know what order they'll arrive in.
Heavyweight - when the low level parts of the TCP "stream" arrive in the wrong order, resend requests have to be sent, and all the out of sequence parts have to be put back together, so requires a bit of work to piece together.	**Lightweight** - No ordering of messages, no tracking connections, etc. It's just fire and forget! This means it's a lot quicker, and the network card / OS have to do very little work to translate the data back from the packets.

2. A Host S opens a TCP connection using an initial sequence number (ISN) of 14,535. Other party R opens the connection with an ISN of 21,732. Show the three TCP segments during the connection establishment. **[WBUT 2014]**

Answer:



3. Discuss the methods of closed loop congestion control. **[WBUT 2017]**

Answer:

Closed loop congestion control mechanisms try to remove the congestion after it happens. The various methods used for closed loop congestion control are:

Backpressure: Backpressure is a node-to-node congestion control that starts with a node and propagates in the opposite direction of data flow. This technique can be applied only to virtual circuit networks. In such virtual circuit each node knows the upstream node from which a data flow is coming. In this method of congestion control, the congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node on nodes to become congested, and they, in turn, reject data from their upstream node or nodes.

Choke Packet: In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion. Here, congested node does not inform its upstream node about the congestion as in backpressure method but it sends a warning directly to the source station i.e. the intermediate nodes through which the packet has traveled are not warned.

Implicit Signaling: In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. Therefore the delay in receiving an acknowledgment is interpreted as congestion in the network. On sensing this congestion, the source slows down. This type of congestion control policy is used by TCP.

Explicit Signaling: In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion. Explicit signaling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signaling method, the signal is included in the packets that carry data. It can occur in either the forward direction or the backward direction. In backward signaling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slow

down. In forward signaling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion. The receiver in this case uses policies such as slowing down the acknowledgements to remove the congestion.

4. a) Compare congestion control with congestion avoidance with example in each case.
b) Compare a key agreement protocol with a key distribution/transport protocol. **[WBUT 2019]**

Answer:
a) Transmission Control Protocol (TCP) uses a network congestion avoidance algorithm that includes various aspects of an additive increase scheme with other schemes such as congestion window to achieve congestion avoidance. The TCP congestion avoidance algorithm is the primary basis for congestion control in the Internet. Congestion control is largely a function of internet hosts, not the network itself. There are several variations and versions of the algorithm implemented in protocol stacks of operating systems, that connect to the internet.
TCP uses a congestion window and a congestion policy that avoid congestion. Only receiver can dictate the sender's window size. In congestion avoidance there are many phase to operate. In these phase, the threshold value is incremented by 1.

b) A key agreement protocol is a protocol where two or more parties can agree on key in such a way that both influence the outcome. If these precludes undesired third parties form forcing a key choice on the agreeing parties. Protocols that are useful also and it does not reveal to any eaves dropping party what key has been agreed upon. It avoids some of the key distribution problems associated with such systems.
Protocols where both parties influence the final derived key are the only way to implement perfect forward secrecy.

5. Write short note on QoS in Transport Layer. **[WBUT 2010, 2012]**
Answer:
Refer to Question No. 2 of Short Answer Type Questions

APPLICATION LAYER

Multiple Choice Type Questions

1. All objects managed by SNMP are given an object identifier. The object identifier always starts with [WBUT 2010]

a) 0 b) 1.3.2.6.1.1 c) 1.3.6.1.2.1 d) none of these

Answer: (c)

2. If user *A* wants to send a message to user *B* confidentially, the plain text is encrypted with the public key of [WBUT 2011]

a) *A* b) *B* c) the network d) Either *A* or *B*

Answer: (b)

3. (A) DNS (i) Name service
(B) FTP (ii) File sharing
(C) NFS (iii) File transfer
(D) SMTP (iv) Mail service

Which of the following is the correct match? [WBUT 2011]

	A	B	C	D
a)	(iv)	(iii)	(ii)	(i)
b)	(i)	(ii)	(iii)	(iv)
c)	(i)	(iii)	(ii)	(iv)
d)	(ii)	(iv)	(iii)	(i)

Answer: (c)

4. Remote login is a function performed by [WBUT 2015]

a) Physical layer b) Network layer
c) Presentation layer d) Application layer

Answer: (d)

5. A _____ certifies the binding between a public key and its owner. [WBUT 2015]

a) KDC b) CA c) TLS d) Firewall

Answer: (b)

6. The packet of information at the application layer is called [WBUT 2018]

a) packet b) message c) segment d) frame

Answer: (b)

7. Which of the following is an application layer service? [WBUT 2018]

a) FTP b) Remote login c) Mail service d) All of these

Answer: (d)

Short Answer Type Questions

1. What do you understand by data privacy? How can authentication, integrity and non-repudiation be implemented by the digital signature technique? **[WBUT 2007, 2009, 2011, 2013]**

Answer:

Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data.

Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.

Authenticity, integrity, non-repudiation can be explained by digital signature and digital certificate.

A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.

Digital certificates - To implement public key encryption on a large scale, such as a secure Web server might need, requires a different approach. This is where digital certificates come in. A digital certificate is essentially a bit of information that says the Web server is trusted by an independent source known as a Certificate Authority. The Certificate Authority acts as the middleman that both computers trust. It confirms that each computer is in fact who they say they are and then provides the public keys of each computer to the other.

2. How are iterative query resolution and recursive query resolution different from each other in the context of DNS? Explain with example. **[WBUT 2011]**

Answer:

Basically a recursive query means the client machine sends the query to a DNS server for resolution, and the DNS server will resolve the query based either on a zone that has been configured locally (in its Forward Lookup Zones or Reverse Lookup Zones), or from a Stub zone, Root Hints, General Forwarder or Conditional Forwarder.

Therefore, in summary, a **recursive** name queries are generally made by a DNS client to a DNS server, or by a DNS server that is configured to pass unresolved name queries that it does not host the zone, to another DNS server, whether through a Stub, Conditional or General Forwarder.

Iterative queries is a request from a client that tells the DNS server that the client expects the best answer the DNS server can provide immediately, without contacting other DNS servers, whether it has the zone configured or not. The process then relies on the client to continue the process possibly by using a referral where the DNS server supplying the client NS or A records of a DNS server that is closer to the namespace which may possibly provide the answer. However we don't see that with the normal sense of the word, 'query,' when a client sends a request to a DNS server, which we are more familiar with. For the most part, the DNS resolver service on Windows clients are basically 'stub

resolvers' that rely on a recursive-enabled DNS server to resolve queries it is not aware of. Of course you can create resolver scripts to perform an iterative query.
However, with a recursion request from a client to a DNS server, which as I mentioned above, is what we normally think of using the term 'query,' the DNS server will do its best to resolve it, either by using Stubs, Conditional or General Forwarder, or Root Hints, which is essentially an iterative query to the Root Hints to devolve the namespace from the TLD backwards (such as from "com" to the second level name, etc), or a query to a Forwarder, if configured with a Forwarder, which is essentially a recursion request because technically it's not an iterative request, even though the server repeats (iterates or re-iterates) when trying to find the answer.

3. a) Differentiate between symmetric and asymmetric key cryptography. **[WBUT 2015]**

Answer:
Symmetric cryptography uses the same secret (private) key to encrypt and decrypt its data whereas asymmetric uses both a public and private key. Symmetric requires that the secret key be known by the party encrypting the data and the party decrypting the data. Asymmetric allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be decoded by the person having the private key. This eliminates the need of having to give someone the secret key (as with symmetric encryption) and risk having it compromised.
The issue with asymmetric is that it is about 1000 times slower than symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use strong a stronger key than symmetric.

b) What do you mean by Key Distribution Centre (KDC). **[WBUT 2015]**

Answer:
In cryptography, KDC, or a key distribution center is part of a cryptosystem intended to reduce the risks inherent in exchanging keys. KDC-s often operate in systems within which some users may have permission to use certain services at some times and not at others.
A typical operation with a KDC involves a request from a user to use some service. The KDC will use cryptographic techniques to authenticate requesting users as themselves. It will also check whether an individual user has the right to access to the service requested. If the authenticated user meets all prescribed conditions, the KDC can issue a ticket permitting access.
KDCs mostly operate with symmetric encryption. In most (but not all) cases the KDC shares a key with each of all the other parties. The KDC produces a ticket based on a server key. The client receives the ticket and submits it to the appropriate server. The server can verify the submitted ticket and grant access to the user submitting it.
Security systems using KDCs include Kerberos.

Benefits

- Easier key distribution
- Scalability

Drawbacks

- A KDC can become a single point of failure
- Everybody must trust the KDC

4. Why do we need a DNS system? What is inverse domain? **[WBUT 2017]**

Answer:

1st Part:

The Domain Name System or Domain Name Server (DNS) is a system that stores information associated with domain names in a distributed database on networks, such as the Internet. DNS associates many types of information with domain names, but most importantly, it provides the IP address associated with the domain name. DNS is an essential component of contemporary Internet use.

DNS is useful for several reasons. Most well known, the DNS makes it possible to attach hard-to-remember IP addresses (such as 207.142.131.206) to easy-to-remember domain names (such as "microsoft.com"). Humans take advantage of this when they recite URLs and e-mail addresses. Less recognized, the domain name system makes it possible for people to assign authoritative names, without needing to communicate with a central registrar each time.

2nd Part:

Inverse domain is used to map an address to a name.

For instance, if a server receives a request from a client and this server has only the IP addresses of the clients in its list then the server needs to find out if this client is on its authorized client list.

In order to determine if the client is on the authorized client list, server asks its resolver to query to the DNS server to map an address to name.

And this type of queries are called inverse query (pointer query -PTR).

Long Answer Type Questions

1. a) Explain the SMTP and FTP in brief. **[WBUT 2006, 2007, 2009]**

b) What do you understand by data security? Explain the various aspects of security with the help of public and private key.

Answer:

a) *SMTP*

SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred. SMTP uses TCP port 25. SMTP started becoming widely used in the early 1980s and gradually replaced UUCP which was better suited to handle e-mail transfers between Unix machines that were intermittently connected. SMTP works best when both the sending and receiving machines are connected to the network all the time.

Sendmail was one of the first (if not the first) mail transfer agents to implement SMTP. Today, there are several programs that implement SMTP as a client or a server, for example, *exim, Postfix, qmail*, and *Microsoft Exchange Server*.
This protocol started out as purely ASCII and did not deal well with binary files. Later, standards such as MIME were developed to encode binary files for transfer through SMTP.
SMTP is a "**push**" protocol that does not allow one to "**pull**" messages from a remote server on demand. To do this a mail client must use **POP3** or **IMAP**.

FTP or **File Transfer Protocol** is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. There are two computers involved in an FTP transfer --- a server and a client. The **FTP server**, running FTP server software, listens on the network for connection requests from other computers. The client computer, running FTP client software, initiates a connection to the server. Once connected, the client can do a number of file manipulation operations such as uploading files to the server, download files from the server, rename or delete files on the server and so on. Any computer connected to a TCP/IP based network can manipulate files on another computer on that network regardless of which operating systems are involved (if the computers permit FTP access). There are many existing FTP client and server programs, and many of these are free.
FTP is commonly run on two ports, 20 and 21, and runs exclusively over TCP. The FTP server listens on port 21 for incoming connection from FTP clients. A connection on this port forms the control stream, on which commands are passed to the FTP server. For the actual file transfer to take place, a different connection is required. Depending on the transfer mode, the client (active mode) or the server (passive mode) can listen for the incoming data connection. Before file transfer begins, the client and server also negotiate the port of the data connection. In case of active connections (where the server connects to the client to transfer data), the server binds on port 20 before connecting to the client. For passive connections, there is no such restriction.
While data is being transferred via the data stream, the control stream sits idle. This can cause problems with large data transfers through firewalls which time out sessions after lengthy periods of idleness. While the file may well be successfully transferred, the control session can be disconnected by the firewall, causing an error to be generated.
Many sites that run FTP servers enable so-called "anonymous ftp". Under this arrangement, users do not need an account on the server. The user name for anonymous access is typically 'anonymous' or 'ftp'. This account does not need a password. Although users are commonly asked to send their email addresses as their passwords for authentication, usually there is trivial or no verification.
While transferring data over the network, two modes can be used

- ASCII mode
- Binary mode

The two types differ in the way they send the data. When a file is sent using an ASCII-type transfer, the individual letters, numbers and characters are sent using their ASCII character codes. The receiving machine saves these in a text file in the appropriate format

(for example, a Unix machine saves it in a Unix format, a Macintosh saves it in a Mac format). Hence if an ASCII transfer is used it can be assumed plain text is sent, which is stored by the receiving computer in its own format.
Sending a file in binary mode is different. The sending machine sends each file bit for bit and as such the recipient stores the bitstream as it receives it.
By default, most FTP clients use ASCII mode. Some clients try to determine the required transfer-mode by inspecting the file's name or contents.

b) Data security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data.
Public key encryption is considered very secure because it does not require a secret shared key between the sender and receiver. Other encryption technologies that use a single shared key to both encrypt and decrypt data rely on both parties deciding on a key ahead of time without other parties finding out what that key is. However, the fact that it must be shared between both parties opens the door to third parties intercepting the key. This type of encryption technology is called symmetric encryption, while public key encryption is known as asymmetric encryption.
A "key" is simply a small bit of text code that triggers the associated algorithm to encode or decode text. In public key encryption, a key pair is generated using an encryption program and the pair is associated with a name or email address. The public key can then be made public by posting it to a key server, a computer that hosts a database of public keys. Alternately, the public key can be discriminately shared by emailing it to friends and associates. Those that possess your public key can use it to encrypt messages to you. Upon receiving the encrypted message, your private key will decrypt it.
Secret-key encryption uses one key, the secret key, that is used to both encrypt and decrypt messages. This is also called symmetric encryption. The term "private key" is often used inappropriately to refer to the secret key. Refer to "Secret-Key Cryptography.

2. a) What are the differences between Symmetric key cryptography and Asymmetric key cryptography?
b) Explain RSA algorithm with an example. **[WBUT 2014]**
Answer:
a) Symmetric Encryption uses a single secret key that needs to be shared among the people who needs to receive the message while Asymmetric encryption uses a pair of public key, and a private key to encrypt and decrypt messages when communicating.

- Symmetric Encryption is an age old technique while Asymmetric Encryption is relatively new.
- Asymmetric Encryption was introduced to complement the inherent problem of the need to share the key in symmetric encryption model eliminating the need to share the key by using a pair of public-private keys.

b) In cryptography, RSA is an algorithm for public-key encryption. The algorithm was described in 1977 by Ron Rivest, Adi Shamir and Len Adleman at MIT; the letters RSA

are the initials of their surnames. RSA involves two keys: public key and private key. The public key is known to everyone and is used to encrypt messages.
The following are steps to generate a public key and a private key:
Choose two large prime numbers p and q such that $p \neq q$, randomly and independently of each other.
Compute $n = pq$.
Compute $\phi(n) = (p-1)(q-1)$.
Choose an integer e such that $1 < e < \phi(n)$ which is coprime to $\phi(n)$
Compute d such that $de \equiv 1 \pmod{\phi(n)}$.

Encrypting messages

Suppose Bob wishes to send a message M to Alice. He turns M into a number $m < n$, using some previously agreed-upon reversible protocol. Bob now has m, and knows n and e, which Alice has announced. He then computes the ciphertext c corresponding to m:

$c = m^e \mod n$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

Decrypting messages

Alice receives c from Bob, and knows her private key d. She can recover m from c by the following procedure: $m = c^d \pmod{n}$

Given m, she can recover the original message M. The decryption procedure works because $c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}$.

Now, since $ed \equiv 1 \pmod{p\text{-}1}$ and $ed \equiv 1 \pmod{q\text{-}1}$, Fermat's little theorem yields

$m^{ed} \equiv m \pmod{p}$ and $m^{ed} \equiv m \pmod{q}$

Since p and q are distinct prime numbers, applying the Chinese remainder theorem to these two congruences yields

$m^{ed} \equiv m \pmod{pq}$

Thus, $c^d \equiv m \pmod{n}$.

Example:

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and n are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

3. Write short notes on the following: [WBUT 2006, 2007]

a) RSA Algorithm [WBUT 2007]
b) Telnet [WBUT 2009, 2012, 2017]
c) DNS [WBUT 2011, 2015]
d) Firewall [WBUT 2011]
e) VLAN [WBUT 2012, 2017]
f) FTP [WBUT 2012]
g) SMTP [WBUT 2016, 2017]
h) Cryptography [WBUT 2016]
i) Digital Signature [WBUT 2017]
j) DQDB [WBUT 2017]
k) HTTP

Answer:

a) RSA Algorithm: *Refer to Question No. 2(b) of Long Answer Type Questions.*

b) Telnet:

Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

A Telnet command request looks like this (the computer name is made-up):

telnet the.libraryat.whatis.edu

The result of this request would be an invitation to log on with a userid and a prompt for a password. If accepted, you would be logged on like any user who used this computer every day.

Telnet is most likely to be used by program developers and anyone who has a need to use specific applications or data located at a particular host computer.

c) DNS:

The **Domain Name System** or **Domain Name Server (DNS)** is a system that stores information associated with **domain names** in a distributed database on networks, such as the Internet. DNS associates many types of information with domain names, but most importantly, it provides the IP address associated with the domain name. DNS is an essential component of contemporary Internet use.

DNS is useful for several reasons. Most well known, the DNS makes it possible to attach hard-to-remember IP addresses (such as 207.142.131.206) to easy-to-remember domain names (such as "microsoft.com") Humans take advantage of this when they recite URLs and e-mail addresses. Less recognized, the domain name system makes it possible for people to assign authoritative names, without needing to communicate with a central registrar each time.

Domain names are arranged in a tree, and cut into zones, which are served by **nameservers**.

The domain name space is a tree of domain names. Each node or leaf in the tree is associated with **resource records**, which hold the information associated with the domain name. The tree is divided into **zones**. A zone is a collection of connected nodes that are authoritatively served by an **authoritative DNS nameserver**. A single nameserver can host several zones.

Adomain name usually consists of two or more parts (technically *labels*), separated by dots. For example *microsoft.com*.

The rightmost label conveys the **top-level domain** (for example, the address *mail.yahoo.com* has the top-level domain *com*).

Each label to the left specifies a subdivision or **subdomain** of the domain above it. Note that "subdomain" expresses relative dependence, not absolute dependence. For example, *yahoo.com* comprises a subdomain of the domain, *com* and *mail.yahoo.com* is a subdomain of the domain *yahoo.com*. In theory, this subdivision can go down to 127 levels deep, and each label can contain up to 63 characters, as long as the whole domain name does not exceed a total length of 255 characters. But in practice some domain registries have shorter limits than that.

A domain name that has one or more associated IP addresses is called a **hostname**. For example, the *yahoo.com* and *mail.yahoo.com* domains are both hostnames, but the *com* domain is not.

d) Firewall:

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- ***Packet filter:*** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- ***Application gateway:*** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- ***Circuit-level gateway:*** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- ***Proxy server:*** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

e) VLAN:
Virtual LAN (VLAN) refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization.
There are the following types of Virtual LANs:
Port-Based VLAN: each physical switch port is configured with an access list specifying membership in a set of VLANs.
MAC-based VLAN: a switch is configured with an access list mapping individual MAC addresses to VLAN membership.
Protocol-based VLAN: a switch is configured with a list of mapping layer 3 protocol types to VLAN membership - thereby filtering IP traffic from nearby end-stations using a particular protocol such as IPX.
ATM VLAN - using LAN Emulation (LANE) protocol to map Ethernet packets into ATM cells and deliver them to their destination by converting an Ethernet MAC address into an ATM address.

f) FTP: ***Refer to Question No. 1(a) of Long Answer Type Questions.***

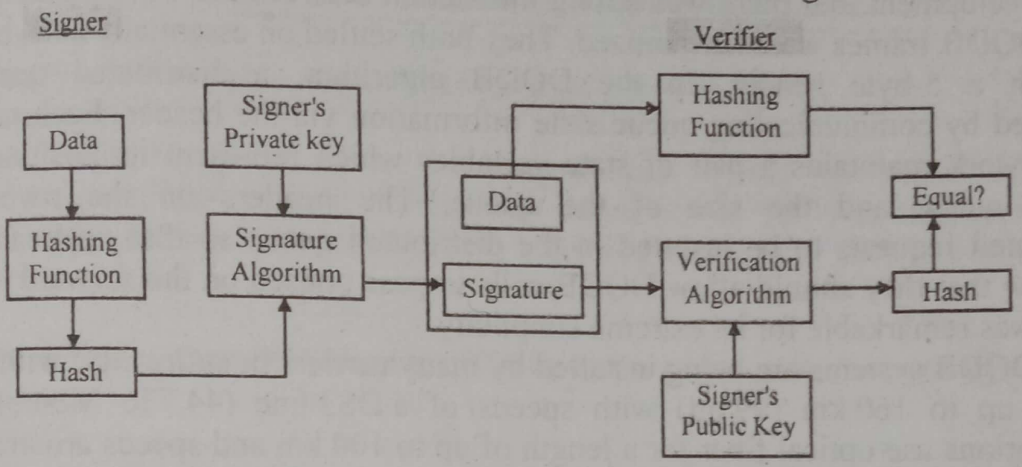
g) SMTP: ***Refer to Question No. 1(a) of Long Answer Type Questions.***

h) Cryptography:
Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.
Modern cryptography concerns itself with the following four objectives:

1) Confidentiality (the information cannot be understood by anyone for whom it was unintended)
2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4) Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

i) Digital Signature:
Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.
Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.
In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.
As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration:



The following points explain the entire process in detail –

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

j) DQDB:

In telecommunication, a distributed queue dual bus network (DQDB) is a distributed multi-access network that supports integrated communications using a dual bus and distributed queuing, provides access to local or metropolitan area networks, and supports connectionless data transfer, connection-oriented data transfer, and isochronous communications, such as voice communications.

The DQDB may be thought of as two token rings, one carrying data in each direction around the ring. This improves reliability which is important in MAN, where repairs may take longer than in a LAN and Wi-Fi because the damage may be inaccessible.

The DQDB standard IEEE 802.6 was developed while ATM (Broadband ISDN) was still in early development, but there was strong interaction between the two standards. ATM cells and DQDB frames were harmonized. They both settled on essentially a 48-byte data frame with a 5-byte header. In the DQDB algorithm, a distributed queue was implemented by communicating queue state information via the header. Each node in a DQDB network maintains a pair of state variables which represent its position in the distributed queue and the size of the queue. The headers on the reverse bus communicated requests to be inserted in the distributed queue so that upstream nodes would know that they should allow DQDB cells to pass unused on the forward bus. The algorithm was remarkable for its extreme simplicity.

Currently DQDB systems are being installed by many carriers in entire city; with lengths that reach up to 160 km (99 mi) with speeds of a DS3 line (44.736 Mbit/s). Other implementations use optical fiber for a length of up to 100 km and speeds around 150 M bit/s.

k) HTTP:

Short for Hyper Text Transfer Protocol, HTTP is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when we enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.

Errors on the Internet can be quite frustrating — especially if we do not know the difference between a 404 error and a 502 error. These error messages, also called HTTP status codes are response codes given by Web servers and help identify the cause of the problem.

For example, "404 File Not Found" is a common HTTP status code. It means the Web server cannot find the file you requested. The file -- the webpage or other document we try to load in our Web browser -- has either been moved or deleted, or you entered the wrong URL or document name.

MODERN TOPICS

Multiple Choice Type Questions

1. Blue-tooth uses ..... To communicate between two devices. [WBUT 2007]
   a) Radiowave b) Microwave c) Infrared
   d) none of these, a separate technology exists

Answer: (a)

Short Answer Type Questions

1. Why is coaxial cable superior to twisted pair cable? [WBUT 2013]

Answer:

Coaxial cable is less prone to interference than twisted pair cable. In long distance transmission coaxial cable is preferred as signal loss is less. The interference is although reduced by twisting cable pairs but the shielding technology provides more reliability in data transmission.

2. Write down the advantages of fibre-optic cable over twisted pair and coaxial cable. [WBUT 2016]

Answer:

Advantages of optical fiber over twisted-pair and co -axial cable are: i) They are light-weighted ii) They are immune to noise iii) They suffer low power loss

Long Answer Type Questions

1. Write short notes on the following:

a) ISDN [WBUT 2006, 2007, 2011]
b) Wi-Max technology [WBUT 2010]
c) Distributed system [WBUT 2010]
d) Satellite transmission [WBUT 2012]

Answer:

a) ISDN:

Integrated Services Digital Network (ISDN) is a type of circuit switched telephone network system, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher speeds than available with analog systems. More broadly, **ISDN** is a set of protocols for establishing and breaking circuit switched connections, and for advanced call features for the user. In a videoconference, ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group (room) videoconferencing systems.

Configurations

In ISDN, there are two types of channels, *B* (for "Bearer") and *D* (for "Delta"). *B channels* are used for data (which may include voice), and *D channels* are intended for signalling and control (but can also be used for data).

There are two kinds of access to ISDN. **Basic rate interface (BRI)** — also **Basic rate access (BRA)** — consists of two B channels, each with bandwidth of 64 kbit/s, and one D channel with a bandwidth of 16 kbit/s. Together these three channels can be designated as 2B+D. **Primary rate interface (PRI)** — also **Primary rate access (PRA)** — contains a greater number of B channels and a D channel with a bandwidth of 64 kbit/s.

b) Wi-Max technology:

WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunications protocol that provides fixed and fully mobile Internet access. The current WiMAX revision provides up to 40 Mbit/s. with the IEEE 802.16m update expected to offer up to 1 Gbit/s fixed speeds. The name "WiMAX" was created by the WiMAX Forum, which was formed in June 2001 to promote conformity and interoperability of the standard. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL".

WiMAX refers to interoperable implementations of the IEEE 802.16 wireless-networks standard (ratified by the WiMAX Forum), in similarity with Wi-Fi, which refers to interoperable implementations of the IEEE 802.11 Wireless LAN standard (ratified by the Wi-Fi Alliance). The WiMAX Forum certification allows vendors to sell their equipment as WiMAX (Fixed or Mobile) certified, thus ensuring a level of interoperability with other certified products, as long as they fit the same profile.

The IEEE 802.16 standard forms the basis of 'WiMAX' and is sometimes referred to colloquially as "WiMAX", "Fixed WiMAX", "Mobile WiMAX", "802.16d" and "802.16e". Clarification of the formal names are as follow:

802.16-2004 is also known as 802.16d, which refers to the working party that has developed that standard. It is sometimes referred to as "Fixed WiMAX", since it has no support for mobility.

802.16e-2005, often abbreviated to 802.16e, is an amendment to 802.16-2004. It introduced support for mobility, among other things and is therefore also known as "Mobile WiMAX".

Mobile WiMAX is the WiMAX incarnation that has the most commercial interest to date and is being actively deployed in many countries. Mobile WiMAX is also the basis of future revisions of WiMAX. As such, references to and comparisons with "WiMAX" in this Wikipedia article mean "Mobile WiMAX".

The bandwidth and range of WiMAX make it suitable for the following potential applications:

Providing portable mobile broadband connectivity across cities and countries through a variety of devices. Providing a wireless alternative to cable and DSL for "last mile" broadband access.

Providing data, telecommunications (VoIP) and IPTV services (triple play).

Providing a source of Internet connectivity as part of a business continuity plan.

c) Distributed System:

Distributed computing is a field of computer science that studies distributed systems. A distributed system consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common goal. A computer program that runs in a distributed system is called a

distributed program, and distributed programming is the process of writing such programs.

Distributed computing also refers to the use of distributed systems to solve computational problems. In distributed computing, a problem is divided into many tasks, each of which is solved by one computer.

There are two main reasons for using distributed systems and distributed computing. First, the very nature of the application may require the use of a communication network that connects several computers. For example, data is produced in one physical location and it is needed in another location.

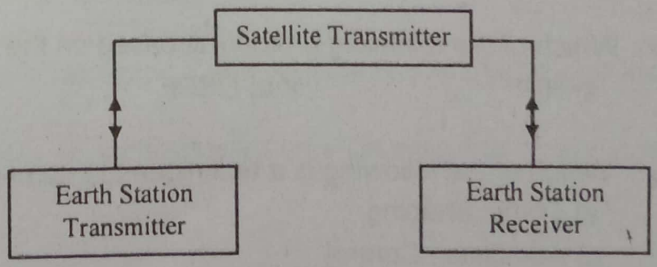
Second, there are many cases in which the use of a single computer would be possible in principle, but the use of a distributed system is beneficial for practical reasons. For example, it may be more cost-efficient to obtain the desired level of performance by using a cluster of several low-end computers, in comparison with a single high-end computer. A distributed system can be more reliable than a non-distributed system, as there is no single point of failure. Moreover, a distributed system may be easier to expand and manage than a monolithic uniprocessor system.

Examples of distributed systems and applications of distributed computing include the following:

- Telecommunication networks.
- Telephone networks and cellular networks.
- Computer networks such as the Internet.
- Wireless sensor networks.
- Routing algorithms.
- Network applications.
- World Wide Web and peer-to-peer networks.
- Massively multiplayer online games and virtual reality communities.
- Distributed databases and distributed database management systems.
- Network file systems.
- Distributed information processing systems such as banking systems and airline reservation systems.

d) Satellite transmission:

In Satellite transmission, signal transferring between the sender and receiver is done with the help of satellite. In this process, the signal which is basically a beam of modulated microwaves is sent towards the satellite. Then the satellite amplifies the signal and sent it back to the receiver's antenna present on the earth's surface. So, all the signal transferring is happening in space. Thus this type of communication is known as space communication.



Two satellites which are commonly used in satellite communication are Active and passive satellites.

QUESTION 2015

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for any ten of the following:

i) Remote login is a function performed by
a) Physical layer b) Network layer c) Presentation layer ✓d) Application layer

ii) Error Control activity is performed by
✓a) Data link layer b) Network layer c) Transport layer d) Session layer

iii) Which transmission is highly susceptible to noise interference?
✓a) ASK b) FSK c) PSK b) QAM

iv) Pick the odd one out from the following
a) 2D Parity Check ✓b) CRC c) Hamming Code d) Checksum

v) HDLC is a
✓ a) bit oriented protocol b) byte oriented protocol
c) both (a) and (b) d) can't say

vi) Token passing is a technique applied in
✓a) Data link layer b) Transport layer c) Physical layer d) Presentation layer

vii) 10 Base-FL is a version of
✓a) Ethernet b) Token Bus c) Token Ring d) Wireless LAN

viii) IPV6 address is having a length of
a) 16 bit b) 32 bit c) 64 bit ✓d) 128 bit

ix) The protocol that maps a physical (MAC) address to the corresponding logical address is
a) ARP ✓b) RARP c) ICMP d) IMAP4

x) Which of the following protocol is based on the concept of Link State Routing?
a) RIP ✓b) OSPF c) BGP d) DVMRP

xi) Which of the following is a technique to improve Quality of Service?
a) Traffic Shaping b) Resource Reservation
c) Admission Control ✓d) All of these

xii) A _____ certifies the binding between a public key and its owner.
a) KDC ✓b) CA c) TLS d) Firewall

Group – B
(Short Answer Type Questions)

2. a) A signal has four data levels with a pulse duration of 1ms. Calculate the pulse rate and bit rate of the signal.
b) What do you mean by line coding? For a signal represented by 01001110 draw the patterns using the schemes: NRZ –L & NRZ-I.
See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 12(a) & (b).

3. a) We want to digitize the human voice. What is the bit rate, assuming 8 bits per sample?
b) Discuss about various transmission impairments.
a) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 1(b).
b) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 13.

4. a) What is inverse TDM?
b) Discuss about data transparency and bit stuffing in case of HDLC?
a) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 14.
b) See Topic: DATA LINK LAYER, Short Answer Type Question No. 9.

5. An ISP is granted a block of address starting with 190.100.0.0/16. The ISP needs to distribute these addresses to three groups of customers as follows:
a) The 1st group has 64 customers; each needs 256 addresses.
b) The 2nd group has 128 customers; each needs 128 addresses.
c) The 3rd group has 128 customers; each needs 64 addresses.
Design the sub blocks and give the slash notation for each sub block.
See Topic: NETWORK LAYER, Short Answer Type Question No. 9.

6. a) Differentiate between symmetric and asymmetric key cryptography.
b) What do you mean by Key Distribution Centre (KDC).
See Topic: APPLICATION LAYER, Short Answer Type Question No. 3(a) & (b).

Group – C
(Long Answer Type Questions)

7. a) What do you mean by Forward Error Correction (FEC)? Discuss in detail.
b) The code 11110101101 was received. Using the Hamming Code method find out what was the original code sent.
c) In case of stop–and–Wait ARQ, with the help of suitable diagrams discuss the operations performed on the following situations:
i) Lost or damaged frame
ii) Lost Acknowledgement
iii) Delayed Acknowledgement.
See Topic: DATA LINK LAYER, Long Answer Type Question No. 7.

8. a) Discuss in detail about the connection establishment procedure performed by LCP with the help of various LCP packets.
b) Explain in detail the state transition diagram of PPP.

c) Discuss the mechanism for authentication provided by Challenge Handshake Authentication Protocol.
d) Discuss the concept of sliding window in detail with the help of an example. How does HDLC perform flow control?

a), b) & c) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 6(a), (b) & (c).
d) See Topic: DATA LINK LAYER, Long Answer Type Question No. 8.

9. a) Discuss in detail about the mechanism of multiple access provided by pure ALOHA. Why the efficiency of slotted ALOHA gets doubled compared to pure ALOHA? Explain.
b) Discuss about the various persistence strategies provided by CSMA.
c) Explain Distance Vector Routing with a suitable example.

a) See Topic: MEDIUM ACCESS SUB LAYER, Short Answer Type Question No. 2.
b) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 5(c).
c) See Topic: NETWORK LAYER, Long Answer Type Question No. 12.

10. a) What is CIDR notation? What is its significance in case of classless addressing?
b) What do you mean by a private address? What is NAT?
c) What do you mean by flow characteristics? Explain in detail. What is admission control?

a) & b) See Topic: NETWORK LAYER, Long Answer Type Question No. 13(a) & (b).
c) 1st Part: Question is not clear.
2nd Part: See Topic: TRANSPORT LAYER, Short Answer Type Question No. 3.

11. Write short notes on the following:
a) FDM
b) Twisted Pair Cables
c) Traditional Ethernet
d) CDMA
e) Firewall

a) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 4(b).
b) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 4(c).
c) See Topic: DATA LINK LAYER, Long Answer Type Question No. 12.
d) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 8(d).
e) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(d).

QUESTION 2016

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for any ten of the following:

i) Which layer converts bit into electromagnetic signals?
✓a) Physical b) Network c) Transport d) Session

ii) Which of the following transmission media is not readily suitable to CSMA operation?
✓a) Radio b) Twisted pair c) Fibre optic d) Coaxial

iii) Phase transition for each bit is used is
a) NRZ encoding
c) Carrier modulation
✓b) Manchester encoding
d) Amplitude modulation

iv) The subnet mask 255.255.255.192
a) extends the network portion to 16 bits
✓b) extends the network portion to 26 bits
c) extends the network portion to 36 bits
d) has no effect on the network portion of an IP address

v) Router solicitation and advertisement message is used by
a) IP b) ARP ✓c) ICMP d) DHCP

vi) If source is using IPV6 and destination is using IPV4, which type of address needs to be used?
a) Loopback ✓b) Mapped c) Compatible d) None of these

vii) Which one of the following is a valid host for network 192.168.4.32/68?
a) 192.168.4.39 b) 192.168.4.50 c) 192.168.4.47 d) 192.168.4.31
Answer: Question is probably wrong

viii) Exponential increase is used in
✓a) Slow start
b) Congestion avoidance
c) Congestion detection
d) none of these

ix) UDP is
a) connection oriented
✓b) connection less
c) both (a) and (b)
d) none of these

x) Port number is
✓a) process number
b) computer physical address
c) both (a) and (b)
d) none of these

Group – B
(Short Answer Type Questions)

2. Suppose a system uses Stop and Wait protocol with propagation delay 20 ms. If the frame size is 160 bits and band-width is 4 kbps when calculate channel utilization of efficiency. What is bit stuffing and byte stuffing?
1st Part: See Topic: DATA LINK LAYER, Short Answer Type Question No. 4.
2nd Part: See Topic: DATA LINK LAYER, Short Answer Type Question No. 10.

3. Apply CRC algorithm, determine the checksum and the transmitted frame for the bit stream 11010111 and for the generator polynomial $x^3 + x^2 + 1$.
See Topic: DATA LINK LAYER, Long Answer Type Question No. 1.

4. Differentiate between CSMA/CD and CSMA/CA.
See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 5(d).

5. What do you mean by subnet masking? Explain how it can be achieved with an example.
See Topic: NETWORK LAYER, Short Answer Type Question No. 10.

6. What do you mean by classful addressing? What are the advantages of classless addressing over classful addressing? What do you mean by netID and hostID?
See Topic: NETWORK LAYER, Short Answer Type Question No. 11.

Group – C
(Long Answer Type Questions)

7. a) What are Bit rate and Baud rate? An analog signal carries 4 bits in each signal unit. If 1000 signal units are sent per second, find the Baud rate and Bit rate.
b) A channel has a data rate 4 kbps and propagation delay of 20 ms. For what range of frame size does stop-and-wait give an efficiency of at least 50%?
a) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 9(a) & (b).
b) See Topic: DATA LINK LAYER, Short Answer Type Question No. 11.

8. a) A 10 bit data bit block 0111010111 is to be sent using hamming code for error detection and correction. Show how the receiver corrects an error that occurs in 6^{th} bit position from right.
b) Differentiate between connection-oriented and connectionless services implemented by the network layer.
a) See Topic: DATA LINK LAYER, Short Answer Type Question No. 1.
b) See Topic: NETWORK LAYER, Long Answer Type Question No. 3.

9. a) Why is dynamic routing preferred over static routing algorithm in the network, which changes continuously? What are LLC & MAC?
b) Why window size of the Go-Back-N protocol is $2^n - 1$, where n is the number of bits requited to identify the sequence number of the data frame?
c) What type of error is not detected by CRC?
d) Prove that $2^r \geq m + r + 1$, where m is the number of data bits and r is the number of redundancy bits required to correct the error.
a) 1st part: See Topic: NETWORK LAYER, Long Answer Type Question No. 14.
2nd part: See Topic: MEDIUM ACCESS SUB LAYER, Short Answer Type Question No. 5.
b), c) & d) See Topic: DATA LINK LAYER, Long Answer Type Question No. 9(a), (b) & (c).

10. a) Write down the advantages of fibre-optic cable over twisted pair and coaxial cable.
b) State the advantage of IPV6 over IPV4.
c) A class B network on the internet has a subnet mask of 255.255.240.0. What is the maximum number of hosts per subnet?
d) Write a short note on Cryptography.
e) An ISP has a block of 1024 addresses. It needs to divide the address among 1024 customers. Does it need subnetting? Justify.
a) See Topic: MODERN TOPICS, Short Answer Type Question No. 2.
b) See Topic: NETWORK LAYER, Long Answer Type Question No. 1(b).
c) & e) See Topic: NETWORK LAYER, Long Answer Type Question No. 15(a) & (b).
d) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(h).

11. Write the short notes any three of the following:
    a) RIP
    b) OSPF
    c) BGP
    d) Digital Signature
    e) ARP packet format

a) See Topic: NETWORK LAYER, Long Answer Type Question No. 19(a).
b) See Topic: NETWORK LAYER, Long Answer Type Question No. 19(d).
c) See Topic: NETWORK LAYER, Long Answer Type Question No. 19(e).
d) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(i).
e) See Topic: NETWORK LAYER, Long Answer Type Question No. 19(f).

QUESTION 2017

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for the following:

i) In an optical fibre, the inner core is …… the cladding.
    ✓a) denser than
    b) less dense than
    c) the same density as
    d) another name for

ii) In the string 219.46.123.107, what is the network address of the host we are looking for?
    ✓a) 219.46.123.0
    b) 107.123.0.0
    c) 107.123.46.0
    d) 107.0.0.0

iii) The two parameters used for measuring the performance of a network are
    ✓a) throughput & delay
    b) power & delay
    c) power and throughput
    d) throughput & buffer size

iv) Sliding window protocol is used for
    a) error control
    b) session control
    ✓c) flow control
    d) concurrency control

v) Which of the following protocols is a network layer protocol?
    a) FTP
    ✓b) ARP
    c) UDP
    d) Telnet

vi) The subnet mask 255.255.255.192 extends the network portion to
    a) 16 bits
    b) 24 bits
    ✓c) 26 bits
    d) 32 bits

vii) A bridge has access to the …… address of a station on the same network.
    ✓a) Physical (MAC)
    b) Network
    c) Service access point
    d) all of these

viii) Hamming code is a method of
    a) error detection
    b) error-correction
    c) error-encapsulation
    ✓d) both (a) & (b)

ix) Connection establishment involves a ..... -way handshake in TCP.
a) one b) two ✓c) three d) four

x) Which the following is an inter-domain routing protocol?
a) RIP b) OSPF ✓c) BGP d) Both (a) & (b)

Group – B
(Short Answer Type Questions)

2. Compare Mesh and Star Topology.
See Topic: PHYSICAL LEVEL, Short Answer Type Question No. 4.

3. Explain ALOHA and Slotted ALOHA. Compare between them.
See Topic: MEDIUM ACCESS SUB LAYER, Short Answer Type Question No. 2.

4. Explain Distance Vector Routing with an example.
See Topic: NETWORK LAYER, Long Answer Type Question No. 12.

5. Compare Leaky Bucket Algorithm with Token Bucket Algorithm.
See Topic: TRANSPORT LAYER, Short Answer Type Question No. 4.

6. Why do we need a DNS system? What is inverse domain?
See Topic: APPLICATION LAYER, Short Answer Type Question No. 4.

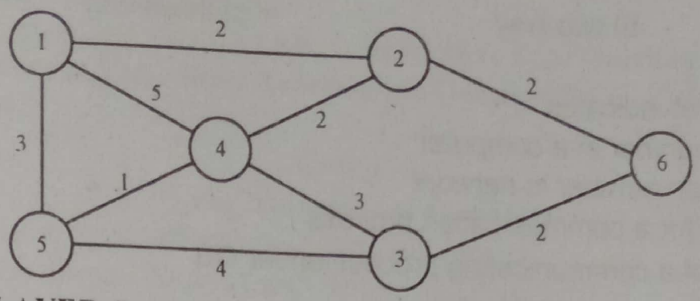
Group – C
(Long Answer Type Questions)

7. a) Find NRZ-I, Manchester and Differential Manchester encoding for the binary data 111001000.
b) What sampling rate is required for a signal with bandwidth of 10,000 Hz (2,000 to 12,000 Hz)?
c) State the advantages of FM over AM.
d) What is transmission impairment? Discuss various types of transmission impairments.
a) See Topic: PHYSICAL LEVEL, Short Answer Type Question No. 3.
b), c) & d) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 3.

8. a) How selective-repeat ARQ will work for lost frame?
b) In Go-Back-N ARQ show why the window size should be < 2m.
c) Applying CRC algorithm determine the transmitted frame 10101000 where the generator polynomial is $x^3 + x + 1$.
d) Compare bit stuffing with byte stuffing with an example.
See Topic: DATA LINK LAYER, Long Answer Type Question No. 10.

9. a) Describe the fields of an IP Datagram.
b) An IP network 192.168.130.0 is using the subnet mask 255.255.255.224. Determine the number of subnet of hosts in each subnet and from what subnet the following hosts belong to:
192.168.130.10 192.168.130.93
192.168.130.222 192.168.130.250

c) Apply Dijkstra's algorithm to find the shortest path from node 4 to node 6 of the network graph shown in the figure below:



See Topic: NETWORK LAYER, Long Answer Type Question No. 16.

10. a) Compare TCP with UDP.
b) Describe Quality of Service (QoS).
c) Discuss the methods of closed loop congestion control.
d) Compare circuit switching with packet switching.

a) See Topic: TRANSPORT LAYER, Long Answer Type Question No. 1(b).
b) See Topic: TRANSPORT LAYER, Short Answer Type Question No. 2.
c) See Topic: TRANSPORT LAYER, Long Answer Type Question No. 3.
d) See Topic: PHYSICAL LEVEL, Short Answer Type Question No. 1.

11. Write the short notes any three of the following:
a) DQDB
b) FTP
c) Cryptography
d) DNS
e) ICMP
f) HTTP

a) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(j).
b) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(f).
c) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(h).
d) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(c).
e) See Topic: NETWORK LAYER, Long Answer Type Question No. 19(g).
f) See Topic: APPLICATION LAYER, Long Answer Type Question No. 3(k).

QUESTION 2018

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for any *ten* of the following:

i) The packet of information at the application layer is called

a) packet ✓b) message c) segment d) frame

ii) HDLC (High-Level Data Link Control) is a

✓a) bit oriented protocol b) byte oriented protocol
c) both (a) and (b) d) None of these

iii) If subnet mask is 255.255.252.0, then many subnets are available?

a) 2 ✓b) 18 c) 4 d) 24

iv) Connection establishment in TCP involves a _____ handshake.
a) one-way b) two-way ✓c) three-way d) None of these

v) Port number in packet indicates
a) LAN card port number in a computer
b) Host identification number in network
c) Unique number for a communication process
✓d) PID number of a communicating process under OS

vi) Router solicitation and advertisement message is used by
a) IP b) ARP ✓c) ICMP d) DHCP

vii) At which layer circuit switching takes place?
a) IP ✓b) ARP c) ICMP d) DHCP

viii) The total number of links required to connect 'n' devices using Mesh Topology is
a) 2^n b) $n(n+1)/2$ ✓c) $n(n-1)/2$ d) n^2

ix) Which of the following is an application layer service?
a) FTP b) Remote login c) Mail service ✓d) All of these

x) When host knowns its IP address but not its physical address, it can use
a) RARP ✓b) ARP c) ICMP d) IGMP

xi) Segmentation is done in
a) physical layer b) data link layer c) network layer ✓d) transport layer

xii) Which class of IP address is reserved for multicast communication?
a) Class A b) Class B c) Class C ✓d) Class D

Group – B
(Short Answer Type Questions)

2. Compare and contrast between OSI and TCP layered models.
See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 5(OR).

3. Differentiate between CSMA/CD and CSMA/CA.
See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 5(d).

4. Generate the CRC code for the data word of 1010011110. The divisor is 1011.
See Topic: DATA LINK LAYER, Long Answer Type Question No. 4(a).

5. a) What is the purpose of the TTL (Time to live) field in the IP header?
b) If the IP header is 28 bytes long, what will be the value of the 'HLEN' field (in binary)?
c) Write the advantage of ICMP over the IPv 4.
See Topic: NETWORK LAYER, Short Answer Type Question No. 8.

6. a) Why is medium access control technique required?
b) What is bit stuffing and character stuffing?

a) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 1.c).
b) See Topic: DATA LINK LAYER, Short Answer Type Question No. 6.

Group – C
(Long Answer Type Questions)

7. a) Derive the expression of the efficiency of pure ALOHA.
b) Compare performance of pure ALOHA with slotted ALOHA.
c) What is the minimum window size required for selective repeat ARQ protocol and how?
d) What is polling?
e) How does CSMA/CD differ from CSMA/CA?

a) & b) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 7.
c) See Topic: DATA LINK LAYER, Long Answer Type Question No. 2.
d) See Topic: DATA LINK LAYER, Short Answer Type Question No. 12.
e) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 5 (d).

8. a) How does Go-Back-N ARQ differ from Selective Repeat ARQ?
b) A computer is using the following sequence numbers. What is the size of the window?
0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, ...
c) What does the number on a NAK frame mean for Selective Repeat ARQ? Give one example.
d) Apply CRC algorithm, to determine the checksum and the transmitted frame for the frame 11010111 and for the generator polynomial $x^3 + x^2 + 1$.

a), b) & c) See Topic: PHYSICAL LEVEL, Long Answer Type Question No. 3.
d) See Topic: DATA LINK LAYER, Long Answer Type Question No. 1.

9. A Class-B network has on the Internet has a subnet mask of 255.255.240.0. What is the number of hosts per subnet? Suppose that you have been assigned an IP address 132.128.0.0 and you wish to have 9 subnets in your organization. What could be the subnet addresses? In CIDR, the prefix can be of any length unlike fixed 8, 16 or 24 in Classful addressing for Class A, B or C respectively. What is its use?

See Topic: NETWORK LAYER, Long Answer Type Question No. 17.

10. a) What is congestion?
b) Why does congestion occur?
c) Explain Leaky Bucket algorithm for congestion control.
d) State the basic difference between TCP and UDP.
e) Compare IPv4 and IPv6.

a), b), c) & d) See Topic: TRANSPORT LAYER, Long Answer Type Question No. 1 (a) & (b).
e) See Topic: NETWORK LAYER, Long Answer Type Question No. 9(a).

11. Write short notes on any three of the following:
    a) IP Data gram
    b) Virtual Circuit Switching
    c) LAN Topologies
    d) IP Addressing

a) See Topic: NETWORK LAYER, Long Answer Type Question No. 19(h).
b) See Topic: PHYSICAL LEVEL, Long Answer Type Question No. 4.
c) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 4(d).
d) See Topic: NETWORK LAYER, Long Answer Type Question No. 19(i).

QUESTION 2019

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternatives for any *ten* of the following:

i) Which of the following is not a silent program in www?
a) FTP b) SMTP c) HTTP ✓d) HTML

ii) For a system using TCP, the sender window size is determined by the window size of
a) Receiver b) Congestion ✓c) both (a) and (b) d) none of these

iii) The ..... socket is used with a protocol that directly uses the services of IP.
a) Stream b) Datagram ✓c) Raw d) Remote

iv) Which of the following is not a part of the UDP user datagram header?
✓a) Length of header b) Source port number
c) Checksum d) Destination port number

v) ..... address uniquely identifies a running application program.
a) IP address b) Host c) NIC ✓d) Socket

vi) Router *B* receives an update from router *A* that indicates Net-1 is two hops away. The next update from *A* says Net-1 is five hops away. What value is entered in *B*'s routing table for Net-1?
a) 2 ✓b) 3 c) 5 d) 7

vii) Which of the following is a mandatory part of the IPv6 datagram?
a) Base header ✓b) Extension header
c) Data packet from upper layer d) none of these

viii) Which of the following could not be an Ethernet unicast destination?
✓a) 43-7B-6C-DE-10-00 b) 44-AA-C1-23-45-32
c) 46-56-21-1A-DE-F4 d) 48-32-21-21-4D-34

ix) In Go-Back-N ARQ, the size of the receiver window will be
a) 2^n ✓b) 1 c) 2^{n-1} d) 0

x) Which of the following is not a guided medium?
a) Twisted-pair b) Fibre optic ✓c) Air d) Coaxial cable

xi) Which multiplexing technique involves signals composed of light beams?
a) FDM b) TDM ✓c) WDM d) None of these

xii) What is a common authentication protocol used for digital signature?
✓a) Kerberos b) Digital signature c) PKI d) None of these

Group – B
(Short Answer Type Questions)

2. Draw various fields in IP packet header. What is the significance of total length field?
See Topic: NETWORK LAYER, Short Answer Type Question No. 12.

3. Define baseband and broadband transmission. What is the application of TDM switching? What is multiplexing?
See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 15.

4. a) What are the basic differences between Router and Gateway?
b) Distinguish between the two terms 'internet' and 'intranet'?
See Topic: NETWORK LAYER, Short Answer Type Question No. 13.

5. Explain message switching with a proper diagram.
See Topic: PHYSICAL LEVEL, Short Answer Type Question No. 5.

6. a) Find the bandwidth for a QPSK signal transmitting at 2kbps. The transmission is in full duplex mode.
b) A digital signalling system is required to operate at 9600 bps. If a signal element encodes 16 bit word, what is the minimum bandwidth required for this channel?
See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Short Answer Type Question No. 16.

Group – C
(Long Answer Type Questions)

7. a) A company is granted the site with the address 192.168.100.0. The company needs 10 subnets. Design the subnets (which include subnet mask number of subnets, number of hosts in each subnet, first and last address of each subnet).
b) What is the advantage of two dimensional parity over simple parity? Explain with suitable example.
c) Briefly discuss different guided media that are used in computer networks and make a comparison among them.
d) What are LLC & MAC?
a) See Topic: DATA LINK LAYER, Long Answer Type Question No. 11(a).
b) See Topic: DATA LINK LAYER, Long Answer Type Question No. 11(b).
c) See Topic: OVERVIEW OF DATA COMMUNICATION AND NETWORKING, Long Answer Type Question No. 1 (a).
d) See Topic: MEDIUM ACCESS SUB LAYER, Short Answer Type Question No. 5.

8. a) Discuss CSMA/CA with the help of a flowchart.
b) Why is CSMA/CD not implemented in WLAN?

c) Why acknowledgement is numbered in stop and wait protocol? Discuss the situation when unnumbered acknowledgements can create confusion in the sender and receiver end.
d) Describe 802.3 header formats. Why is padding required?

a) & b) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 4(a) & (b).
c) See Topic: DATA LINK LAYER, Short Answer Type Question No. 13.
d) See Topic: MEDIUM ACCESS SUB LAYER, Short Answer Type Question No. 4.

9. a) Compare Repeater, Router, Bridge and Gateway functionally as well as coverage of various layers for operational aspect in OSI/ISO reference model.
b) Compare congestion control with congestion avoidance with example in each case.
c) Compare a key agreement protocol with a key distribution/transport protocol.

a) See Topic: DATA LINK LAYER, Short Answer Type Question No. 14.
b) & c) See Topic: TRANSPORT LAYER, Long Answer Type Question No. 4(a) & (b).

10. a) What is the purpose of sequence numbers in TCP segment? Why is padding required for TCP segment? Explain your answer.
b) A TCP connection is using a window size of 10000 bytes and the previous acknowledgement number was 22,001. It receives a segment with acknowledgement number 24,001. Draw a diagram to show the situation of the window before and after.
c) State the basic difference between TCP and UDP.

a) See Topic: NETWORK LAYER, Long Answer Type Question No. 18(a).
b) See Topic: NETWORK LAYER, Long Answer Type Question No. 18(b).
c) See Topic: TRANSPORT LAYER, Long Answer Type Question No. 1(b).

11. Write short notes on any *three* of the following:
    a) FDDI
    b) HDLC
    c) Virtual Circuit
    d) IPv6
    e) CSMA
    f) Virtual Private Network (VPN)

a) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 8(b).
b) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 8(e).
c) See Topic: PHYSICAL LEVEL, Long Answer Type Question No. 4.
d) See Topic: NETWORK LAYER, Long Answer Type Question No. 19(c).
e) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 8(f).
f) See Topic: MEDIUM ACCESS SUB LAYER, Long Answer Type Question No. 8(g).