PAPER ID-410925

Printed Page: 1 of 2
Subject Code: KCA303

Roll No: □□□□□□□□□□□□□

MCA
(SEM III) THEORY EXAMINATION 2021-22
COMPUTER NETWORK

Time: 3 Hours ***Total Marks: 100***

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief. 2 x 10 = 20

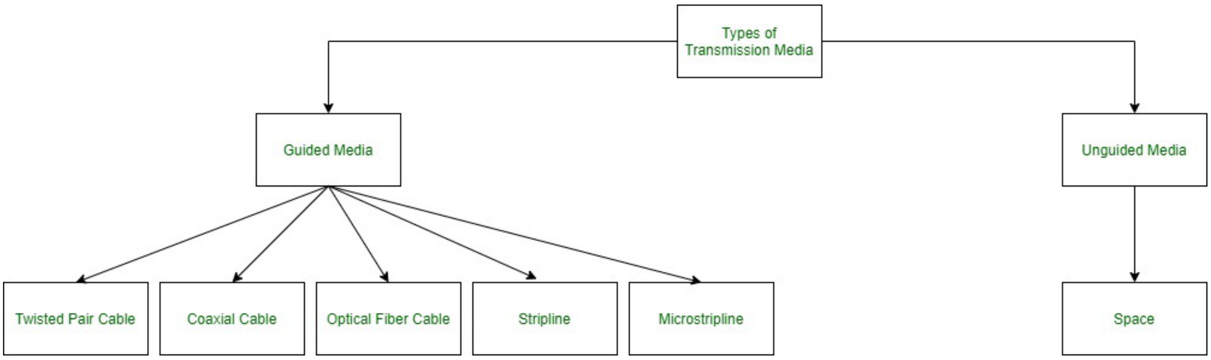
<table>
<tr><th>Q. No.</th><th></th></tr>
<tr><td><b>A</b></td><td><b>Question: Describe Data Communication.</b>
<b>Answer:</b> Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media.</td></tr>
<tr><td><b>B</b></td><td><b>Question: Differentiate between serial communication and parallel communication.</b>
<b>Answer:</b> The comparison between serial communication and parallel communication are as follows:
<table>
<tr><th>Basis for Comparison</th><th>Serial Communication</th><th>Parallel Communication</th></tr>
<tr><td><b>Data transmission speed</b></td><td>Slow</td><td>Comparatively fast</td></tr>
<tr><td><b>Number of communication link used</b></td><td>Single</td><td>Multiple</td></tr>
<tr><td><b>Number of transmitted bit/clock cycle</b></td><td>only one bit.</td><td>n number of link will carry n bits.</td></tr>
<tr><td><b>Cost</b></td><td>Low</td><td>High</td></tr>
<tr><td><b>Crosstalk</b></td><td>Not present</td><td>Present</td></tr>
<tr><td><b>System Up-gradation</b></td><td>Easy</td><td>Quite difficult</td></tr>
<tr><td><b>Mode of transmission</b></td><td>Full duplex</td><td>Half duplex</td></tr>
<tr><td><b>Suitable for</b></td><td>Long distance</td><td>Short distance</td></tr>
<tr><td><b>High frequency operation</b></td><td>More efficient</td><td>Less efficient</td></tr>
</table></td></tr>
<tr><td><b>C</b></td><td><b>Question: Discuss about Protocol.</b></td></tr>
</table>

	Answer: A communication protocol is a system of rules that allows two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods.
D	**Question: How would you formulate shanon's theorem** **Answer:** For error free communication, Shannon's Theorem is related with the rate of information transmission over a communication channel, The form communication channel cares all the features and component arty the transmission system which introduce noise or limit the band width. $C=B\ log_2\ (1+S/N)\ b/s$ Where B → Bandwidth of the channel, S/N →Signal to noise ratio and C → Shannon capacity of the channel in bps.
e	**Question: what is purpose of hamming code?** **Answer:** Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. It is technique developed by R.W. Hamming for error correction.
f	**Question: How would you formula efficiency of standard ethernet?** **Answer:** Efficiency of standard ethernet can be calculated as: Efficiency of Ethernet = 1 / (1 + 6.44a) where a = Tp / Tt. Where, Tt - transmission time Tp - propagation time
g	**Question: Discuss about Fragmentation.** **Answer:** Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held in a frame i.e., its Maximum Transmission Unit (MTU). The network layer divides the datagram received from the transport layer into fragments so that data flow is not disrupted.
h	**Question: What are responsibilities of transport layer?** **Answer:** The responsibilities of transport layer are: ✓ End-to-end delivery ✓ Addressing ✓ Reliable delivery ✓ Flow control ✓ Multiplexing
i	**Question: what do you mean by piggybacking?** **Answer:** Piggybacking is a method of attaching acknowledgment to the outgoing data packet.
j	**Question: Illustrate about socket?**

	Answer: Sockets allow communication between two different processes on the same or different machines. To be more precise, it's a way to talk to other computers using standard Unix file descriptors.

SECTION B

2. Attempt any *three* of the following:

Q. No.	
a	**Question: Explain the duties of each layer in TCP/IP model.** **Answer:**
b	**Question: What is transmission Media? Describe in detail about guided and unguided transmission media.** **Answer:** In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e., it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:  Types of Transmission Media Guided Media Unguided Media Twisted Pair Cable Coaxial Cable Optical Fiber Cable Stripline Microstripline Space **1. Guided Media:** It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links. Features: • High Speed • Secure • Used for comparatively shorter distances There are 3 major types of Guided Media: **(i) Twisted Pair Cable –** It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

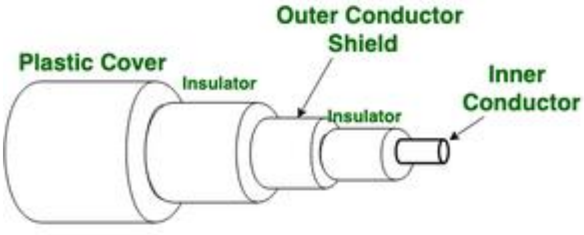
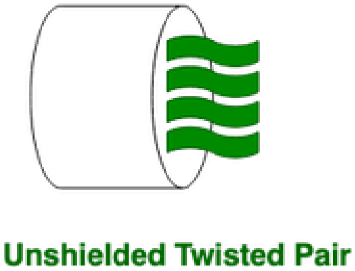


Figure of Coaxial Cable



- **Unshielded Twisted Pair (UTP):**

UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

⇢ Least expensive

⇢ Easy to install

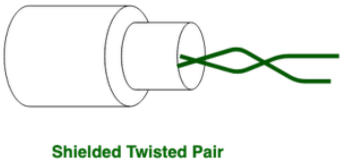
⇢ High-speed capacity

⇢ Susceptible to external interference

⇢ Lower capacity and performance in comparison to STP

⇢ Short distance transmission due to attenuation

- **Shielded Twisted Pair (STP):** This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Advantages:

⇢ Better performance at a higher data rate in comparison to UTP

⇢ Eliminates crosstalk

⇢ Comparatively faster

⇢ Comparatively difficult to install and manufacture

⇢ More expensive

⇢ Bulky

(ii) Coaxial Cable: It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode (dedicated cable bandwidth) and Broadband mode (cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

(iii) Optical Fiber Cable –

It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

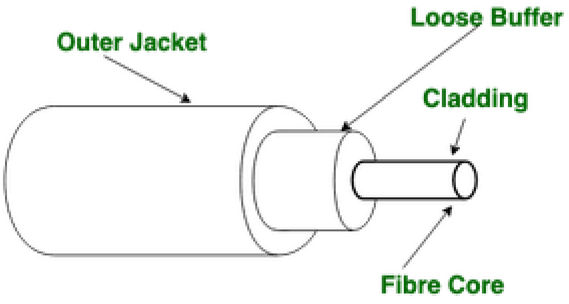


Figure of Optical Fibre Cable

The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost

2. Unguided Media:

It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

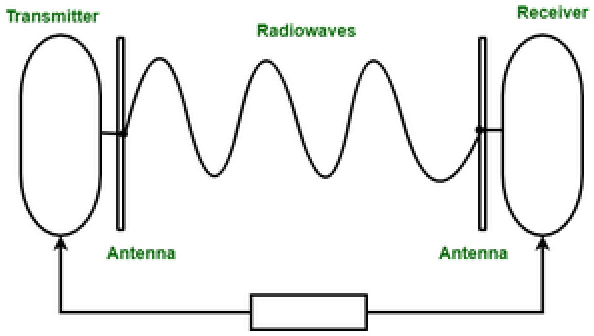
Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 types of Signals transmitted through unguided media:

(i) Radio waves –

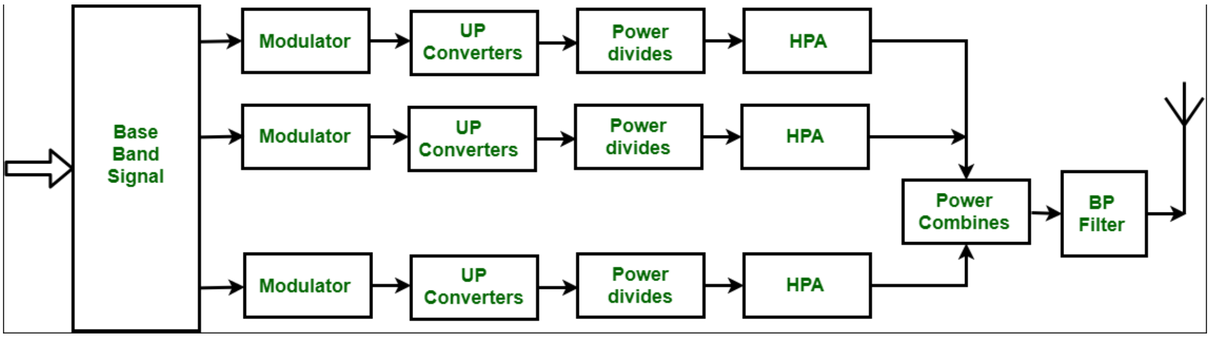
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.



Further Categorized as (i) Terrestrial and (ii) Satellite.

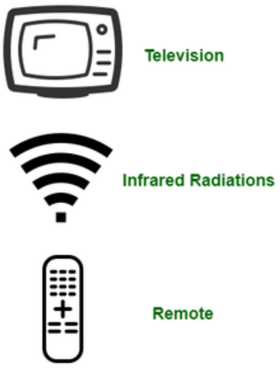
(ii) Microwaves –

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.



(iii) Infrared –

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.



c **Question: what are unicast, Multicast and broadcast addresses? Define. Type of the following destination addresses:**

a. 4A: 30:10:21: 10:1A

b. 47:20:1B:2E:08:EE

c. FF: FF: FF: FF: FF: FF

Answer: Three types of Ethernet addresses exist:

- **unicast addresses** – represents a single LAN interface. A unicast frame will be sent to a specific device, not to a group of devices on the LAN.
- **multicast addresses** – represents a group of devices in a LAN. A frame sent to a multicast address will be forwarded to a group of devices on the LAN.
- **broadcast addresses** – represents all device on the LAN. Frames sent to a broadcast address will be delivered to all devices on the LAN.

a. This is a unicast address because A in binary is 1010 (even).
b. This is a multicast address because 7 in binary is 0111 (odd).
c. This is a broadcast address because all digits are Fs in hexadecimal.

d **Question: Explain any two protocols Stop and wait, Go back in selective repeat.**

Answer: The protocols are discussed as follows:

- ✓ **Stop and Wait protocol:** Stop and Wait protocol is a protocol for flow control mechanism. In this protocol, sender sends one frame at a time and waits for acknowledgment from the receiver. Once acknowledged, sender sends another frame to the receiver. If acknowledgment is not received, then frame/packet is retransmitted.
- ✓ **Go-Back N protocol:** Go Back N is also a protocol for flow control mechanism. In this protocol, sender sends n frames at a time and wait for cumulative acknowledgment. If acknowledgment is not received, then entire frames are retransmitted again.
- ✓ **Selective Repeat protocol:** It is also a protocol for flow control mechanism. In this protocol, sender sends n frames at a time and wait for acknowledgment of packets received in particular order. If acknowledgment is not received, then lost packets are transmitted again which is based on receiver acknowledgment. Receiver maintains a buffer of lost packets.

Following are some of the important differences between Stop and Wait protocol and Sliding Window protocol.

Sr. No.	Key	Stop and Wait protocol	Go Back N protocol	Selective Repeat protocol
1	Sender window size	In Stop and Wait protocol, Sender window size is 1.	In Go Back N protocol, Sender window size is N.	In Selective Repeat protocol, Sender window size is N.

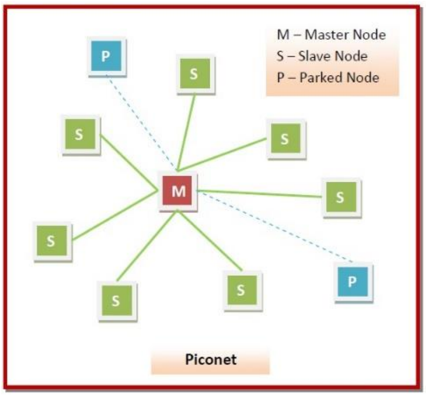
2	Receiver Window size	In Stop and Wait protocol, Receiver window size is 1.	In Go Back N protocol, Receiver window size is 1.	In Selective Repeat protocol, Receiver window size is N.
3	Minimum Sequence Number	In Stop and Wait protocol, Minimum Sequence Number is 2.	In Go Back N protocol, Minimum Sequence Number is N+1 where N is number of packets sent.	In Selective Repeat protocol, Minimum Sequence Number is 2N where N is number of packets sent.
4	Efficiency	In Stop and Wait protocol, Efficiency formular is 1/(1+2*a) where a is ratio of propagation delay vs transmission delay.	In Go Back N protocol, Efficiency formular is N/(1+2*a) where a is ratio of propagation delay vs transmission delay and N is number of packets sent.	In Selective Repeat protocol, Efficiency formular is N/(1+2*a) where a is ratio of propagation delay vs transmission delay and N is number of packets sent.
5	Acknowledgement Type	In Stop and Wait protocol, Acknowledgement type is individual.	In Go Back N protocol, Acknowledgement type is cumulative.	In Selective Repeat protocol, Acknowledgement type is individual.
6	Supported Order	In Stop and Wait protocol, no specific order is needed at receiver end.	In Go Back N protocol, in-order delivery only is accepted at receiver end.	In Selective Repeat protocol, out-of-order deliveries also can be accepted at receiver end.

7	Retransmissions	In Stop and Wait protocol, in case of packet drop, number of re-transmition is 1.	In Go Back N protocol, in case of packet drop, numbers of re-transmition are N.	In Selective Repeat protocol, in case of packet drop, number of re-transmition is 1.

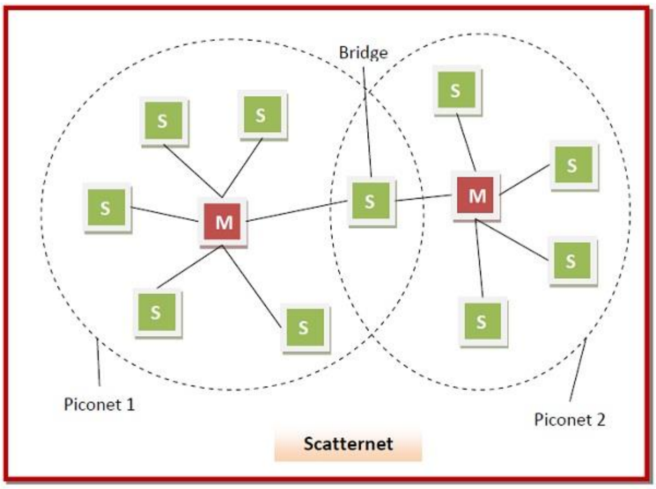
e **Question: Explain Bluetooth architecture with the help of neat diagram.**

Answer: Bluetooth is a network technology that connects mobile devices wirelessly over a short range to form a personal area network (PAN). They use short-wavelength, ultra-high frequency (UHF) radio waves within the range 2.400 to 2.485 GHz, instead of RS-232 data cables of wired PANs. There are two types of Bluetooth networks:

- ➢ Piconets
- ➢ Scatternets



Piconets: Piconets are small Bluetooth networks, formed by at most 8 stations, one of which is the master node and the rest slave nodes (maximum of 7 slaves). Master node is the primary station that manages the small network. The slave stations are secondary stations that are synchronized with the primary station. Communication can take place between a master node and a slave node in either one-to-one or one-to-many manner. However, no direct communication takes place between slaves. Each station, whether master or slave, is associated with a 48-bit fixed device address.



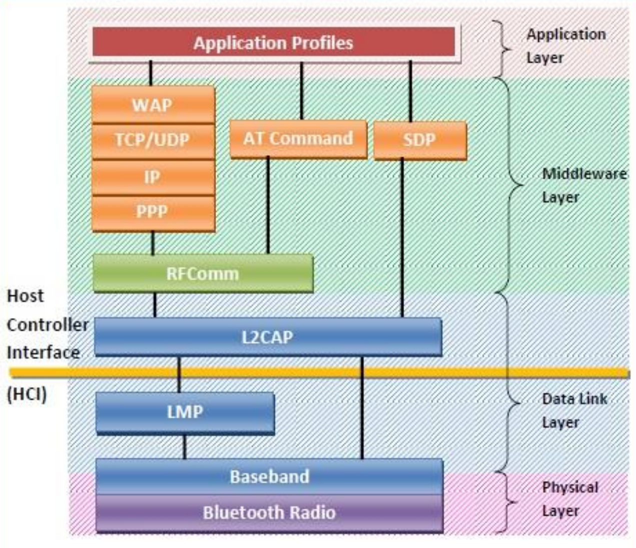
Besides the seven active slaves, there can be up to 255 numbers of parked nodes. These are in a low power state for energy conservation. The only work that they can do is respond to a beacon frame for activation from the master node.

Scatter Net: A scatternet is an interconnected collection of two or more piconets. They are formed when a node in a piconet, whether a master or a slave, acts as a slave in another piconet. This node is called the bridge between the two piconets, which connects the individual piconets to form the scatternet.

Bluetooth network technology connects mobile devices wirelessly over a short-range to form a personal area network (PAN). The Bluetooth architecture has its own independent model with a stack of protocols, instead of following the standard OSI model or TCP/IP model.

The protocols in the Bluetooth standard can be loosely grouped into the physical layer, data link layer, middleware layer, and application layer as shown in the following diagram −

Protocols in the Bluetooth Protocol Architecture



Bluetooth Protocol Architecture

- **Physical Layer** − This includes Bluetooth radio and Baseband (also in the data link layer.
    - **Radio** − This is a physical layer equivalent protocol that lays down the physical structure and specifications for transmission of radio waves. It defines air interface, frequency bands, frequency hopping specifications, and modulation techniques.
    - **Baseband** − This protocol takes the services of radio protocol. It defines the addressing scheme, packet frame format, timing, and power control algorithms.
- **Data Link Layer** − This includes Baseband, Link Manager Protocol (LMP), and Logical Link Control and Adaptation Protocol (L2CAP).
    - **Link Manager Protocol (LMP)** − LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.
    - **Logical Link Control and Adaptation Protocol (L2CAP)** − L2CAP provides adaption between upper layer frame and baseband layer frame format. L2CAP provides support for both connection oriented as well as connectionless services.
- **Middleware Layer** − This includes Radio Frequency Communications (RFComm) protocol, adopted protocols, SDP, and AT commands.
    - **RFComm** − It is short for Radio Frontend Component. It provides a serial interface with WAP.

- **Adopted Protocols** − These are the protocols that are adopted from standard models. The commonly adopted protocols used in Bluetooth are Point-to-Point Protocol (PPP), Internet Protocol (IP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Wireless Application Protocol (WAP).
- **Service Discovery Protocol (SDP)**− SDP takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices.
- **AT Commands** − ATtention command set.

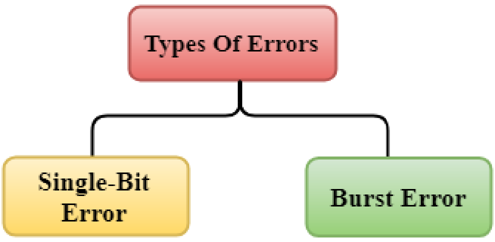
- **Applications Layer** − This includes the application profiles that allow the user to interact with the Bluetooth applications.

SECTION C

3. Attempt any *one* part of the following:

Q. No.	
A	**Question: discuss about error detection methods. Describe anyone technique used for error detection with suitable example.**

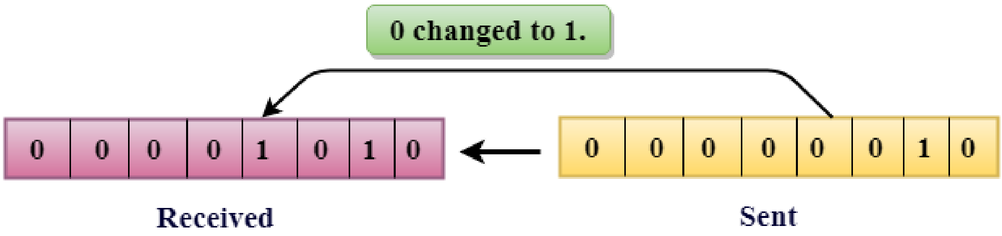
Answer: When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.



Types of Errors: Errors can be classified into two categories:

- ✓ Single-Bit Error
- ✓ Burst Error

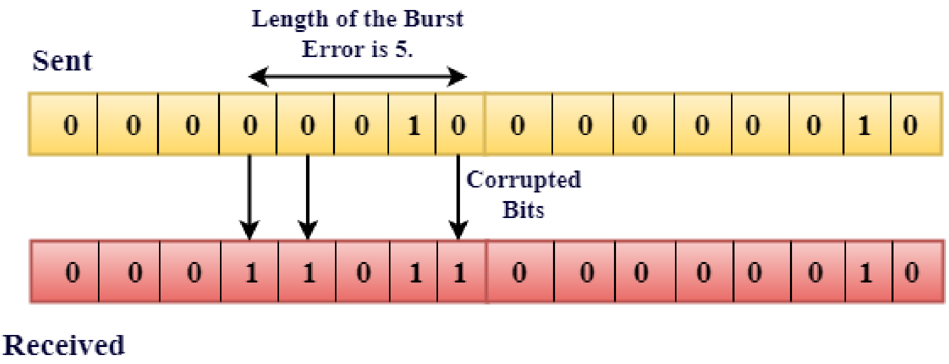
Single-Bit Error: The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



In the above figure, the message which is sent is corrupted as single bit, i.e., 0 bit is changed to 1.

Single-Bit Error: It does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1s and for a single-bit error to occurred, a noise must be more than 1s. Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wires is noisy, then single bit is corrupted per byte.

Burst Error: The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error. The Burst Error is determined from the first corrupted bit to the last corrupted bit.



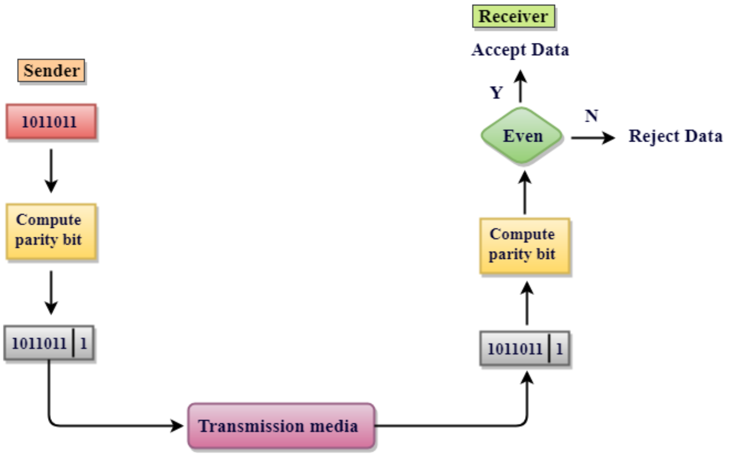
The duration of noise in Burst Error is more than the duration of noise in Single-Bit. Burst Errors are most likely to occur in Serial Data Transmission. The number of affected bits depends on the duration of the noise and data rate.

Error Detecting Techniques:

The most popular Error Detecting Techniques are:

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

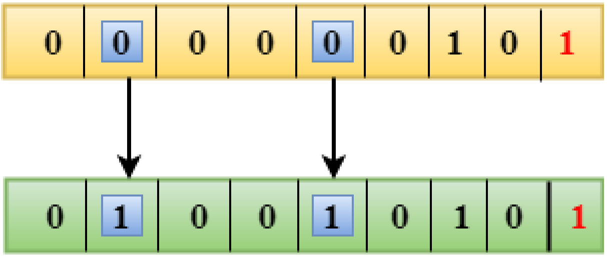
Single Parity Check: Single Parity checking: It is the simple mechanism and inexpensive to detect the errors. In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits. If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit. At the receiving end, the parity bit is calculated from the received data bits and



compared with the received parity bit. This technique generates the total number of 1s even, so it is known as even-parity checking.

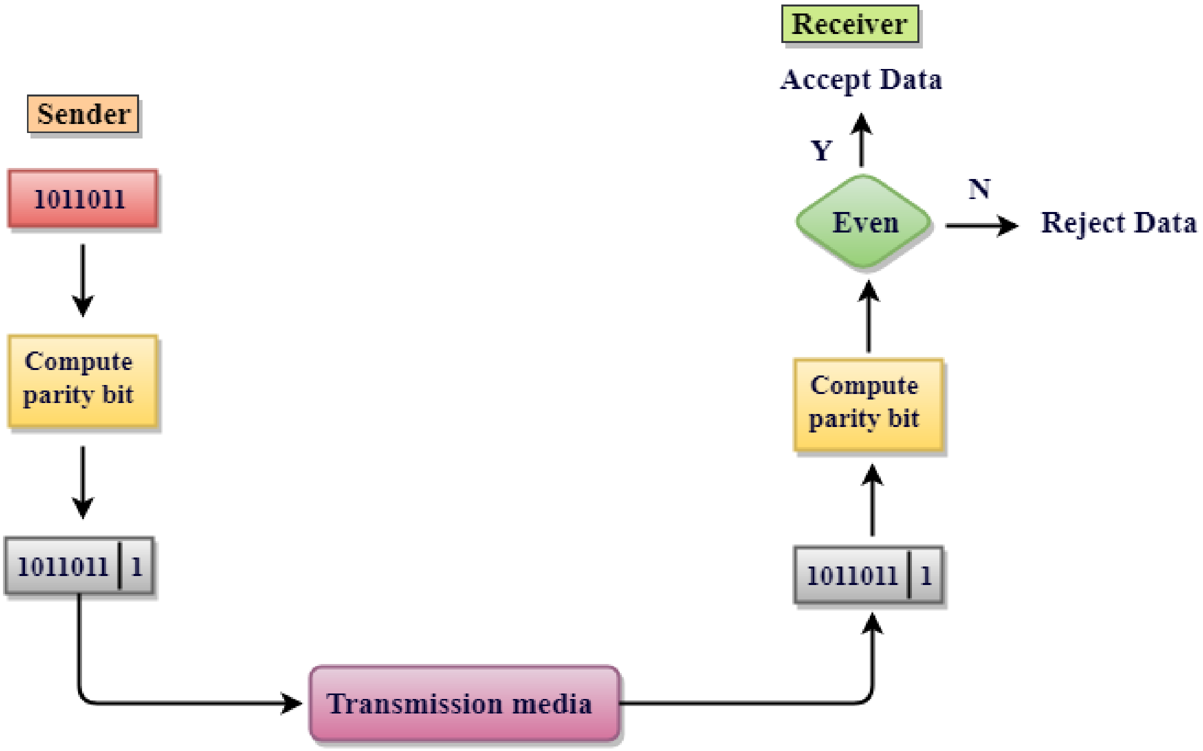
Drawbacks Of Single Parity Checking

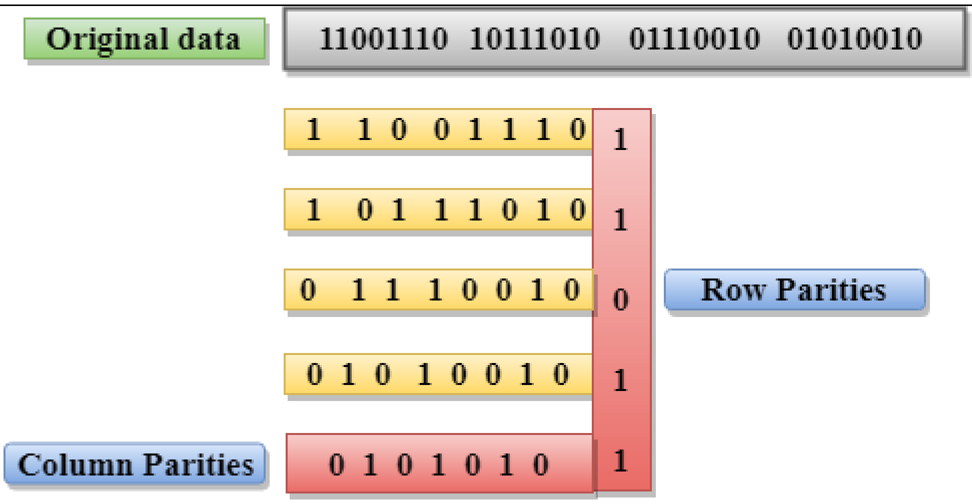
- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.





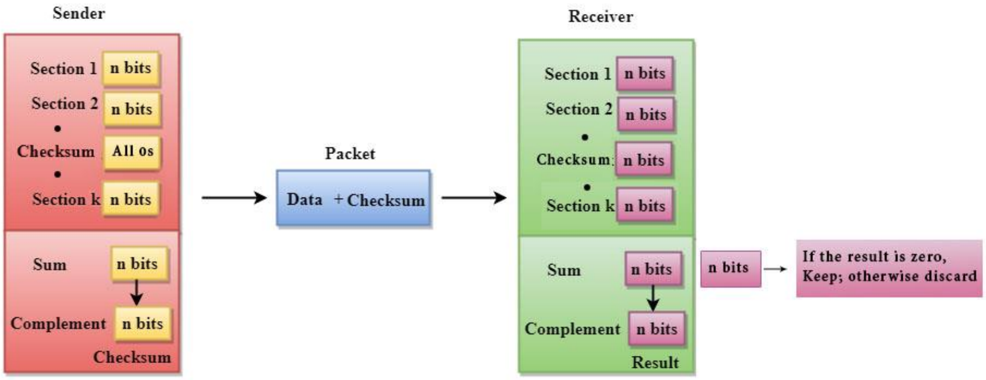
Drawbacks Of 2D Parity Check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

Checksum: A Checksum is an error detection technique based on the concept of redundancy.

It is divided into two parts:

Checksum Generator: A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network. Suppose L is the total sum of the data segments, then the checksum would be L.



The Sender follows the given steps:

1. The block unit is divided into k sections, and each of n bits.
2. All the k sections are added together by using one's complement to get the sum.
3. The sum is complemented, and it becomes the checksum field.
4. The original data and checksum field are sent across the network.

Checksum Checker

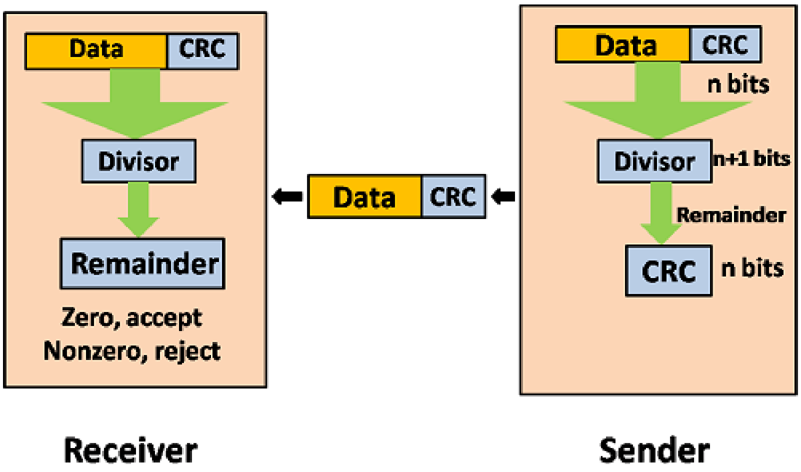
A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

- The Receiver follows the given steps:
- The block unit is divided into k sections and each of n bits.
- All the k sections are added together by using one's complement algorithm to get the sum.
- The sum is complemented.
- If the result of the sum is zero, then the data is accepted otherwise the data is discarded.

Cyclic Redundancy Check (CRC): CRC is a redundancy error technique used to determine the error. Following are the steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.
- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.
- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

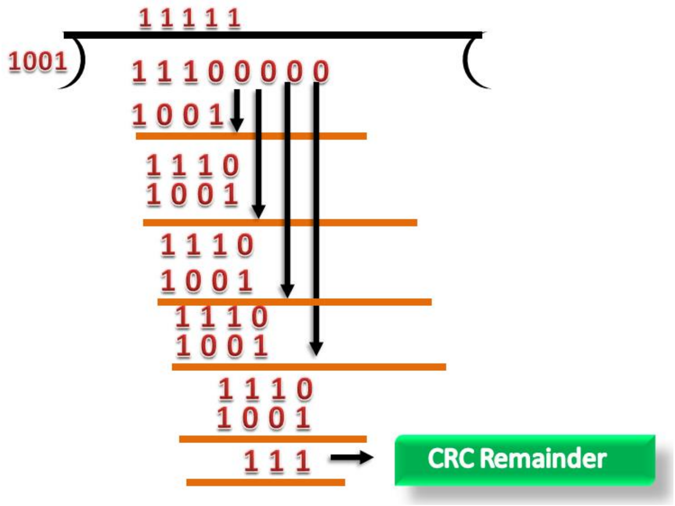


If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.

Let's understand this concept through an example. Suppose the original data is 11100 and divisor is 1001.

CRC Generator

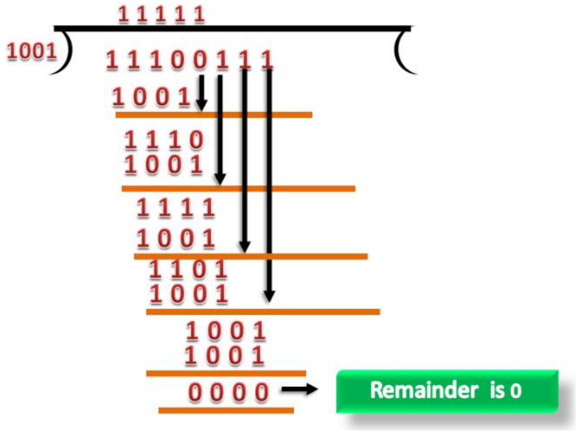
- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.



- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.

CRC Checker

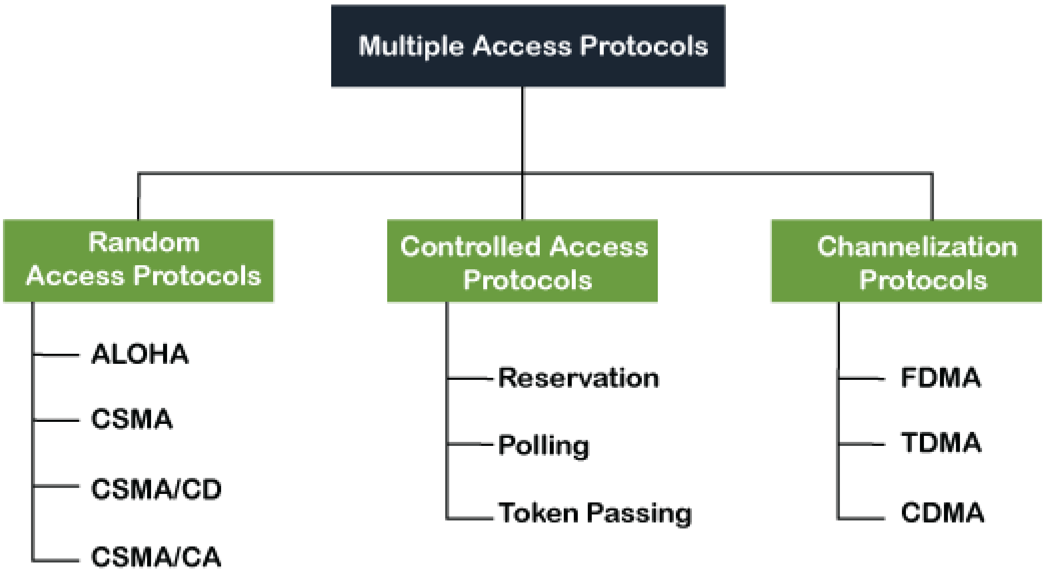
- The functionality of the CRC checker is similar to the CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



b **Question: Briefly explain about multiple access protocol.**

Answer: When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels. For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

Following are the types of multiple access protocol that is subdivided into the different process as:



A. Random Access Protocol: In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

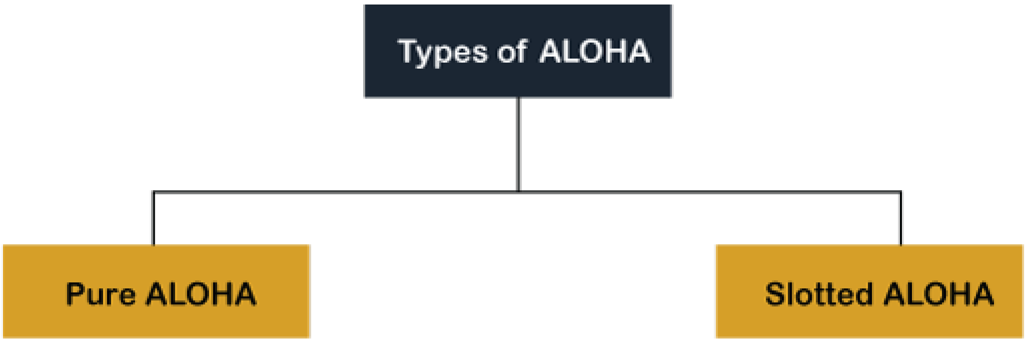
Following are the different methods of random-access protocols for broadcasting frames on the channel.

- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA Random Access Protocol: It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

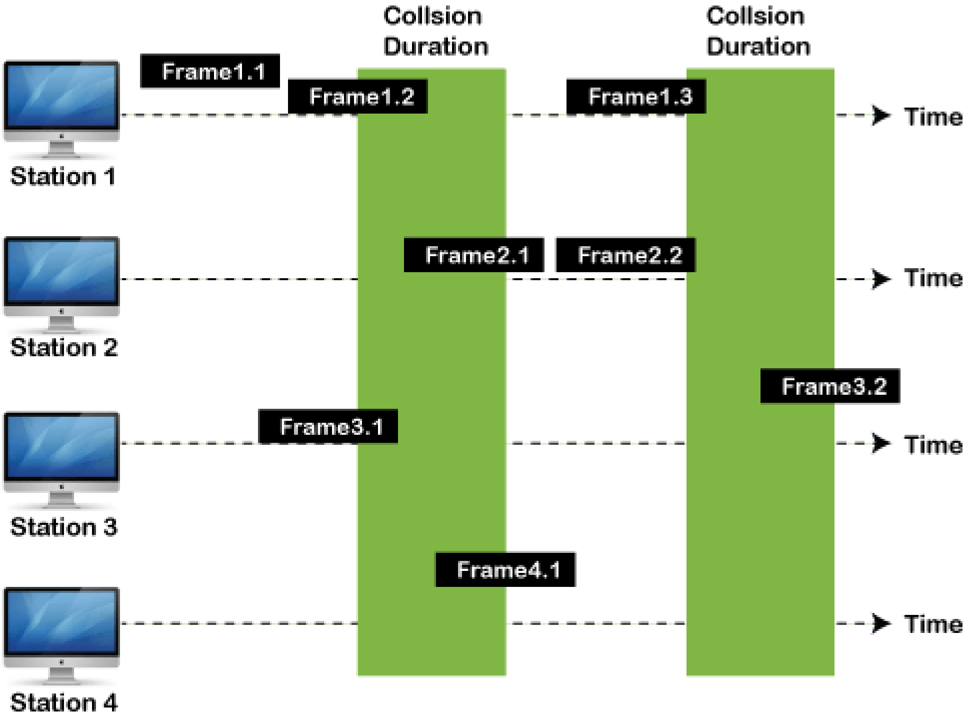
Aloha Rules

1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



Pure Aloha: Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.

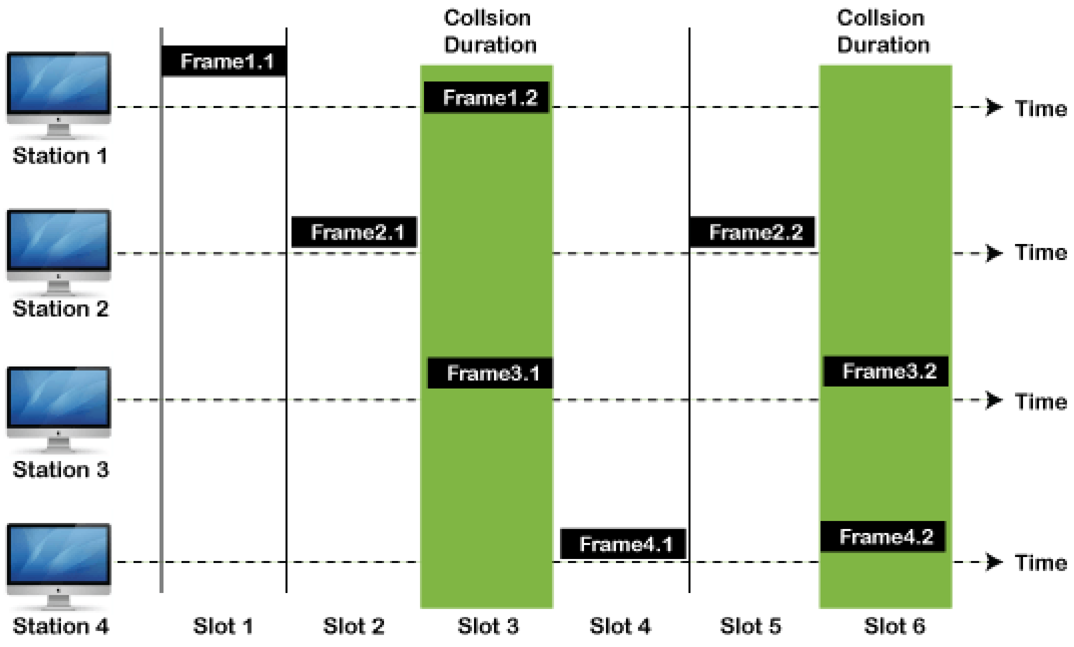


Frames in Pure ALOHA

As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha: The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

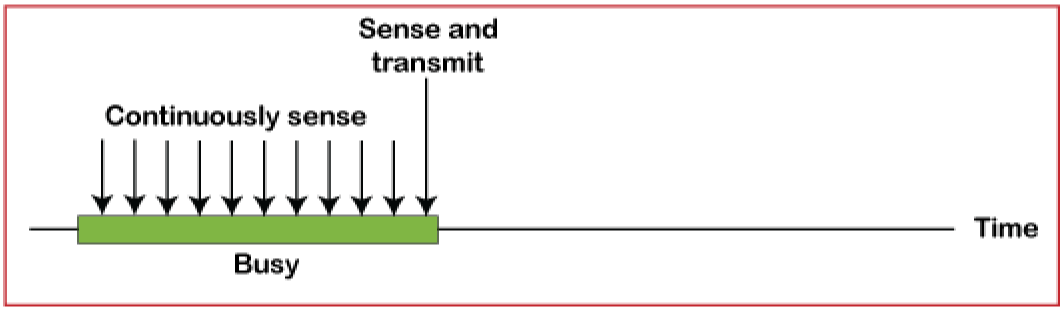
CSMA Access Modes

1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

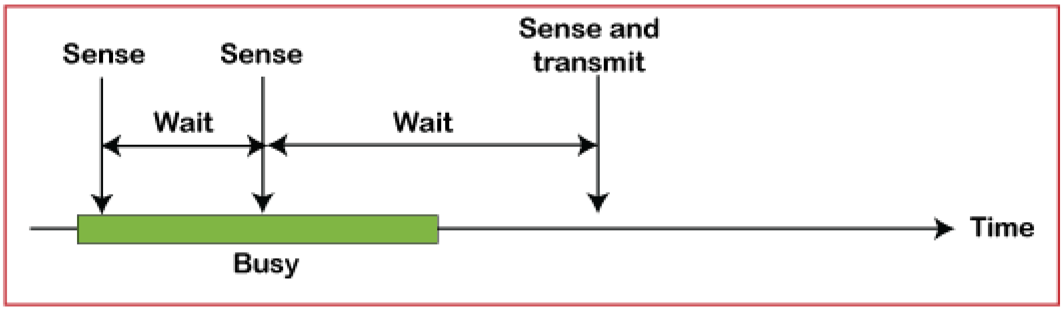
Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

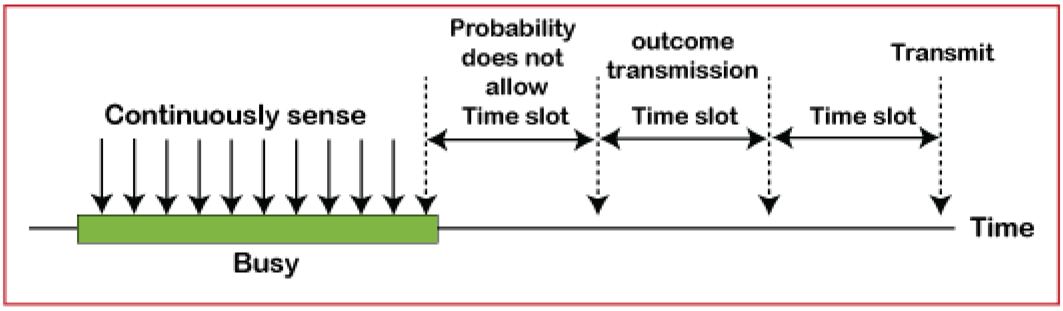
0- Persistent: It is an 0-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent



b. Nonpersistent



c. p-persistent

- **CSMA/ CD:** It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.
- **CSMA/ CA:** It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

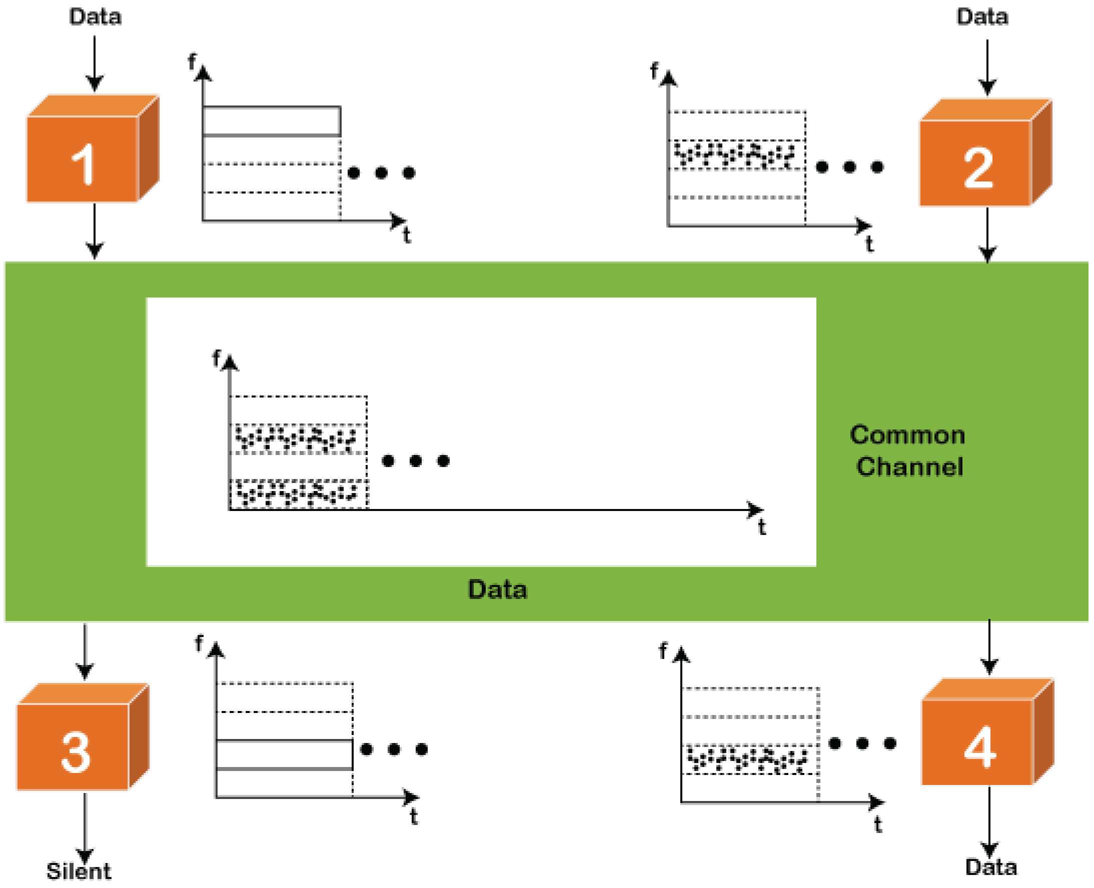
B. Controlled Access Protocol: It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

C. Channelization Protocols: It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

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

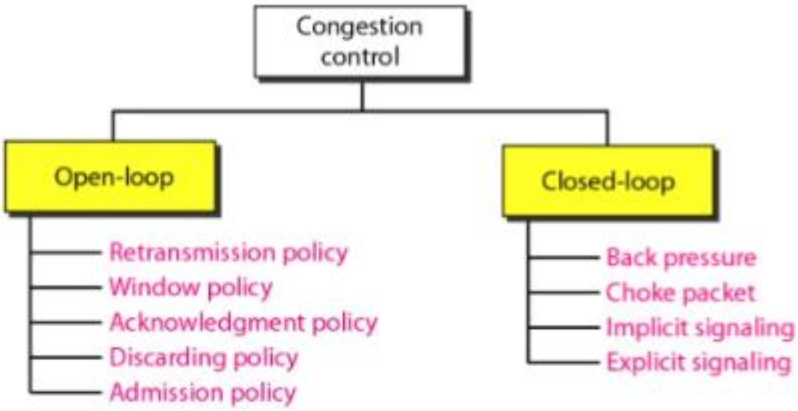
FDMA: It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



TDMA: Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

CDMA: The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to

	a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.

Q. No.	
a	**Question: What is meant by congestion control? What are the techniques involved in eliminating it?** **Answer:** Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network (i.e. the number of packets sent to the network) is greater than the capacity of the network (i.e. the number of packets a network can handle.). Network congestion occurs in case of traffic overloading. Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:  Congestion control Open-loop Closed-loop Retransmission policy Window policy Acknowledgment policy Discarding policy Admission policy Back pressure Choke packet Implicit signaling Explicit signaling **Open Loop Congestion Control:** Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination. Policies adopted by open loop congestion control 1. **Retransmission Policy:** It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network. To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

2. **Window Policy:** The type of window at the sender side may also affect the congestion. Several packets in the Go-back-n window are resent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and making it worse. Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.
3. Discarding Policy: A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive package and also able to maintain the quality of a message. In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.
4. Acknowledgment Policy: Since acknowledgement are also the part of the load in network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment. The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send a acknowledgment only if it has to sent a packet or a timer expires.
5. Admission Policy: In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

Closed Loop Congestion Control: Closed loop congestion control technique is used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. Backpressure: Backpressure is a technique in which a congested node stop receiving packet from upstream node. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.

   In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and informs the source to slow down.

2. Choke Packet Technique: Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitor its resources and the utilization at each of its output lines. whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.

   Implicit Signaling: In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

3. **Explicit Signaling:** In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet technique.
   Explicit signaling can occur in either forward or backward direction.
   - **Forward Signaling:** In forward signaling signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.
   - **Backward Signaling:** In backward signaling signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

b **Question: What do you mean by IP address? Explain IP addressing method.**

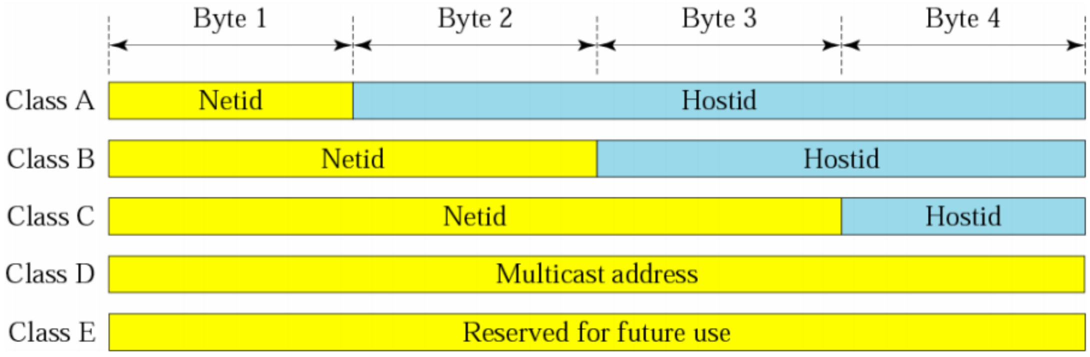
Answer: Every machine on a network has a unique identifier. Just as you would address a letter to send in the mail, computers use the unique identifier to send data to specific computers on a network. Most networks today, including all computers on the Internet, use the TCP/IP protocol as the standard for how to communicate on the network. In the TCP/IP protocol, the unique identifier for a computer is called its IP address. There are two standards for IP addresses: IP Version 4 (IPv4) and IP Version 6 (IPv6). All computers with IP addresses have an IPv4 address, and many are starting to use the new IPv6 address system as well. Here's what these two address types mean:

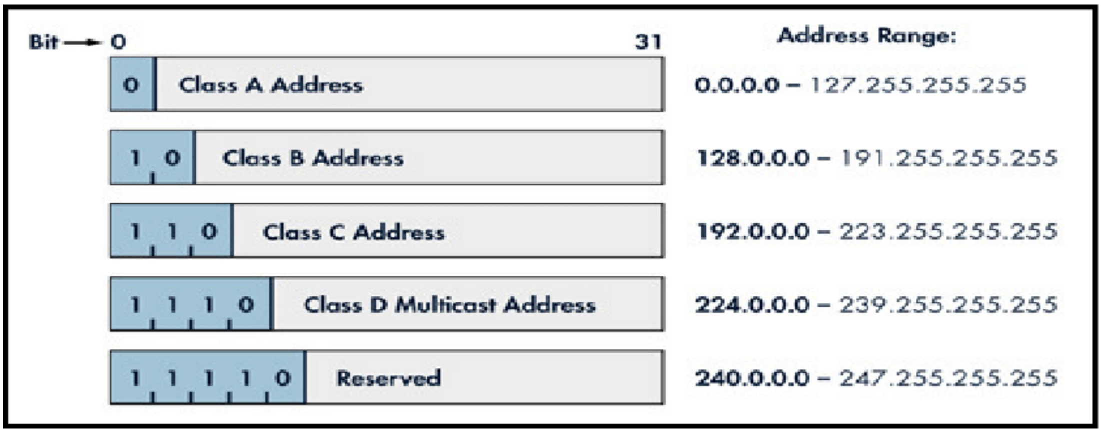
IPv4 uses 32 binary bits to create a single unique address on the network. An IPv4 address is expressed by four numbers separated by dots. Each number is the decimal (base-10) representation for an eight-digit binary (base-2) number, also called an octet. For example: 216.27.61.137

IPv6 uses 128 binary bits to create a single unique address on the network. An IPv6 address is expressed by eight groups of hexadecimal (base-16) numbers separated by colons, as in 2001:cdba:0000:0000:0000:0000:3257:9652. Groups of numbers that contain all zeros are often omitted to save space, leaving a colon separator to mark the gap (as in 2001:cdba::3257:9652).

Each IPv4 address is divided into two parts:

- Network ID
- Host ID





Q. No.	
a	**Question: The contents of UTP header in hexadecimal format is.** **a. What is the source port number?**

b. What is the destination port number?

c. What is the total length of the user datagram?

d. What is the length of the data?

Answer:

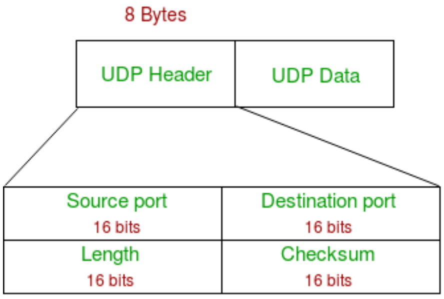
b **Question: Explain any two protocols in the TCP/IP protocol suite.**

a. UDP

b. TCP

Answer: The protocols are discussed as follows:

a. UDP: User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer. Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency. Here, UDP comes into picture. For the realtime services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also save bandwidth. User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.



UDP Header: UDP header is 8-bytes fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary header information and remaining part consist of data. UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or process.

- ✓ **Source Port:** Source Port is 2 Byte long field used to identify port number of source.
- ✓ **Destination Port:** It is 2 Byte long field, used to identify the port of destined packet.

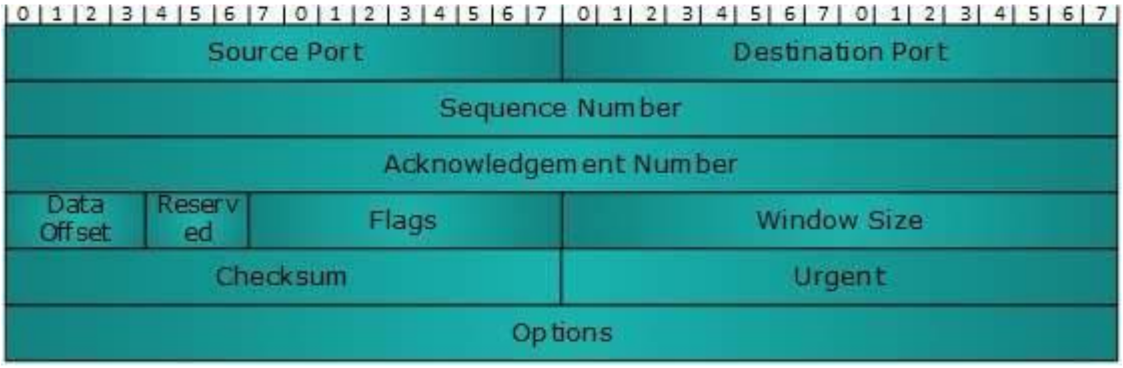
- ✓ **Length:** Length is the length of UDP including header and the data. It is 16-bits field.
- ✓ **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one’s complement of the one’s complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

b. **TCP:** The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet. The features of TCP are as follows:

- ✓ TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- ✓ TCP ensures that the data reaches intended destination in the same order it was sent.
- ✓ TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- ✓ TCP provides error-checking and recovery mechanism.
- ✓ TCP provides end-to-end communication.
- ✓ TCP provides flow control and quality of service.
- ✓ TCP operates in Client/Server point-to-point mode.
- ✓ TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

The frame format of TCP is as follows:

a) **Header:** The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
  - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
  - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
  - **ECE** -It has two meanings:
    - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
    - If SYN bit is set to 1, ECE means that the device is ECT capable.
  - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
  - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
  - **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
  - **RST** - Reset flag has the following features:
    - It is used to refuse an incoming connection.
    - It is used to reject a segment.
    - It is used to restart a connection.
  - **SYN** - This flag is used to set up a connection between hosts.

    - **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.
- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

Q. No.

a

Question: explain any two.

a. **URL**
b. **Cookies**
c. **API**
d. **NVT**

Answer:

a. **URL** stands for Uniform Resource Locator. It is the address of a resource, which can be a specific webpage or a file, on the internet. It is also known as web address when it is used with http. It was created in 1994 by Tim Berners-Lee. URL is a specific character string that is used to access data from the World Wide Web. It is a type of URI (Uniform Resource Identifier). Every URL contains the following information:

- The scheme name or protocol.
- A colon, two slashes.
- A host, normally called a domain name but sometimes as a literal IP address.
- A colon followed by a port number.

- Full path of the resource.

The URL of a web page is displayed above on the page in the address bar. A typical URL looks like this: http://www.javatpoint.com/full-form

The above URL contains:

- **protocol**: http
- **host or domain**: www.javatpoint.com
- **Path of the resource**: /full-form

A URL can be entered manually by typing it in the address bar of your web browser. If the URL does not contain a valid server, a browser may display a "Server not found" error and if the path in the URL is incorrect, the browser may display a "404 error". A URL does not contain spaces and uses forward slashes to represent different directories. So, dashes and underscores are used separate the words of a web address

b. Cookies are files, generally from the visited webpages, which are stored on a user's computer. They hold a small amount of data, specific to a particular client and website, and can be accessed either by the web server or the client computer which can be usernames, password, session token, etc.

This allows the server to deliver a page personalized to a particular user, or the page itself can contain some script which is aware of the data in the cookie and so is able to carry information from one visit to that website.

Types of Cookies

There are three different types of cookies −

- **Session Cookies** − These are mainly used by online shops and allows you to keep items in your basket when shopping online. These cookies expire after a specific time or when the browser is closed.
- **Permanent Cookies** − These remain in operation, even when you have closed the browser. They remember your login details and password so you don’t have to type them in every time you use the site. It is recommended that you delete these type of cookies after a specific time.
- **Third-Party Cookies** − These are installed by third parties for collecting certain information. For example: Google Maps.

C. API: API stands for application program interface. A programmer writing an application program can make a request to the Operating System using API (using graphical user interface or command interface). It is a set of routines, protocols and tools for building software and applications. It may be any type of system like a web-based system, operating-system or a database System.

D. The Network Virtual Terminal (NVT): It is a representation of a basic terminal and provides a standard that the computers on either end of a Telnet connection are assumed to follow. It defines how data and commands are sent across the network. Thus, NVT allows interoperability between Telnet and a variety of heterogeneous computers and operating systems. It consists of a virtual keyboard that generates user-specified characters and a printer that displays specific characters. Clients and servers can map their local devices to the characteristics and handling conventions of an NVT and can assume that other servers and clients are doing the same.

b

Question: Define network management. Explain five areas of network management.

Answer: A network management system (NMS) refers to a collection of applications that enable network components to be monitored and controlled. In general, network management systems have the same basic architecture. The architecture consists of two key elements: a managing device, called a management station, or a manager and the managed devices, called management agents or simply an agent. A management station serves as the interface between the human network manager and the network management system. It is also the platform for management applications to perform management functions through interactions with the management agents. The management agent responds to the requests from the management station and also provides the management station with unsolicited information. Five areas of network management are:

✓ **Performance Management:**

To quantify, measure, report, analyze, and control the performance (e.g, utilization and throughput) of different network components are the main goal of performance management. These components include individual devices (e.g, links, routers, and hosts) as well as the end-to-end abstraction such as a path through the network. Protocol standard such as the Simple Network Management Protocol (SNMP) play a central role in Internet performance management.

✓ **Fault Management:**

The goal of fault management is to log, detect, and respond to fault condition int the network. The difference between fault management and performance management is blurred.

The fault management is used to manage immediate handling of the failures like link failure, host failure, or router hardware problem, these problems are also known as a transient network failure. With the help of performance management, the SNMP protocol plays a major part in fault management.

- ✓ **Configuration Management:**

  Tracking of the devices that are on the managed network and the hardware and software configurations are allowed by Configuration management.

- ✓ **Accounting Management:**

  To specify, log, and control user and device access to network resources are allowed by Accounting management. usage quotas, usage-based charging, and the allocation of resource-access privileges all fall under accounting management.

- ✓ **Security Management:**

  The goal of security management is to control access to network resource according to some well-defined policy. The key distribution centres are a component of network management.

  The use of firewalls to monitor and control external access point to one’s network is another crucial component.