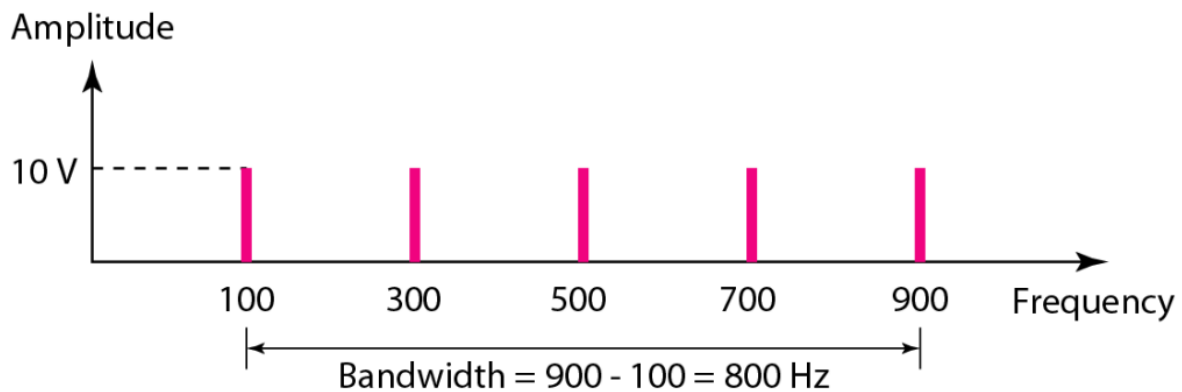


Module 1

A periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700 and 900 Hz. What is the bandwidth of the signal? Draw the spectrum assuming all components have a maximum amplitude of 10 volts. L

The bandwidth of a signal is the range of frequencies that it occupies. In the case of a periodic signal, it is the difference between the highest frequency component and the lowest frequency component.

In this case, the highest frequency component is 900 Hz and the lowest frequency component is 100 Hz. Therefore, the bandwidth of the signal is $900 \text{ Hz} - 100 \text{ Hz} = 800 \text{ Hz}$.



What is the need for Analog to Analog modulation? Describe all the possible modulation techniques?L

This modulation is generally needed when a bandpass channel is required. Bandpass is a range of frequencies which are transmitted through a bandpass filter which is a filter allowing specific frequencies to pass, preventing signals at unwanted frequencies.

What is the role of Network layer and Data Link layer in OSI Reference Model? Why IP in Network layer is purposely made connection less?L

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends

them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

IP is connectionless because it does not require a connection between hosts. It does not sequence, acknowledge, or control the flow of data between hosts. IP treats each datagram as a separate entity; it merely addresses the datagram and sends it out, hoping it reaches the destination.

A low-pass signal is sampled with a bandwidth of 400 kHz using 1024 levels of quantization.

a. Calculate the bit rate of the digitized signal.

Bit rate = sampling rate × number of bits per sample

Low pass signal: frequency between 0 – 200 KHz BW = 200 KHz

Sampling rate $\geq 2 \times f_{\text{highest}} = 2 \times 200 \text{ KHz} \geq 400,000 \text{ samples /s}$

$n_b = \log_2 1024 = 10 \text{ bits/sample};$

Bit rate = $400,000 \times 10 = 4 \text{ Mbps}$

b. Calculate the SNR_{dB} for this signal.

$\text{SNR}_{\text{dB}} = 6.02 n_b + 1.76 = 6.02 \times 10 + 1.76 = 61.96 \text{ dB}$

c. Calculate the PCM bandwidth of this signal.L

$\text{SNR}_{\text{dB}} = 6.02 n_b + 1.76 = 6.02 \times 10 + 1.76 = 61.96 \text{ dB}$

Match the following to one or more layers of the OSI model:

a. Reliable process-to-process message delivery **Transport Layer**

b. Route selection **Network Layer**

c. Defines frames **Data link Layer**

d. Provides user services such as e-mail and file transfer **Application Layer**

e. Transmission of bit stream across the physical medium **Physical Layer**

Show the Differential Manchester encoding for the bit pattern given below.

(i) 01001100

(ii) 10110011 M

(ans kiye ho to dm [Nehal Bhuyan](#) / [WhatsApp](#))

In a noiseless channel with a bandwidth of 9000 hz transmitting a signal with two signal levels. Calculate the bit rate? S

Consider a noiseless channel with a bandwidth of 9000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as Bit Rate $= 2 \times 9000 \times \log_2 2 = 18000 \text{ bps}$. (Bit Rate = $2 \times \text{bandwidth} \times \log_2 L$)

If the data link layer can detect errors between hops, why do you think we need another checking mechanism at the transport layer?

The errors between the nodes can be detected by the data link layer control, but the error at the node (between input port and output port) of the node cannot be detected by the data link layer.

Suppose a computer sends a packet at the transport layer to another computer somewhere on the Internet. There is no process with the destination port address running at the destination computer. What will happen? S

Most protocols issue a special error message that is sent back to the source in this case.

Define a DC component and its effect on digital transmission. S

When the voltage level in a digital signal is constant for a while, the spectrum creates very low frequencies, called DC components, which present problems for a system that cannot pass low frequencies.

A file contains 2 million bytes. How long does it take to download this file using a 56-Kbps channel? M

With a 56-Kbps channel, it takes $16,000,000/56,000 = 289 \text{ s} \approx 5 \text{ minutes}$. (Convert bytes to bits)

What is the need for Analog to Analog modulation? Describe all the possible modulation techniques? L

Analog to Analog Conversion (Modulation) - GeeksforGeeks (Link)

For 6 devices in a network, what is the number of cable links required for a mesh, ring and star topology? S

- | | |
|--|-----------------|
| • $n(n-1)/2$ cable links are required for mesh | $6(6-1)/2 = 15$ |
| • n for ring | 6 |
| • $n-1$ cable link for bus | 5 |
| • n cable link for star topology. | 6 |

A signal travels from point A to point B. At point A, the signal power is 200 W. At point B, the power is 170 W. What is the attenuation in decibels? M

For, $10 \log_{10} (200/170) = 0.7058085$

Similar qsn:

Attenuation in decibels = $10 \log_{10} \frac{P_t}{P_r}$ where P_t is the transmitted power and P_r is the received power.

In the given case attenuation in dB =

$$10 \log \frac{100}{90} = 10 (\log(10) - \log(9)) = 0.46 \text{ dB} \approx 0.5 \text{ dB}$$

Encode the given data word 101110101 using RZ, NRZ-L, NRZ-I, Manchester and differential Manchester schemes. L

(ans kiye ho to dm Nehal Bhuyan / [WhatsApp](#))

Show the Manchester encoding for the bit pattern given below.

(i) 01001100

(ii) 10110011 M

(ans kiye ho to dm Nehal Bhuyan / [WhatsApp](#))

Draw the OSI Model and explain the functions of different layers. L

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

7. Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

5. Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

4. Transport Layer

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

3. Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

2. Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

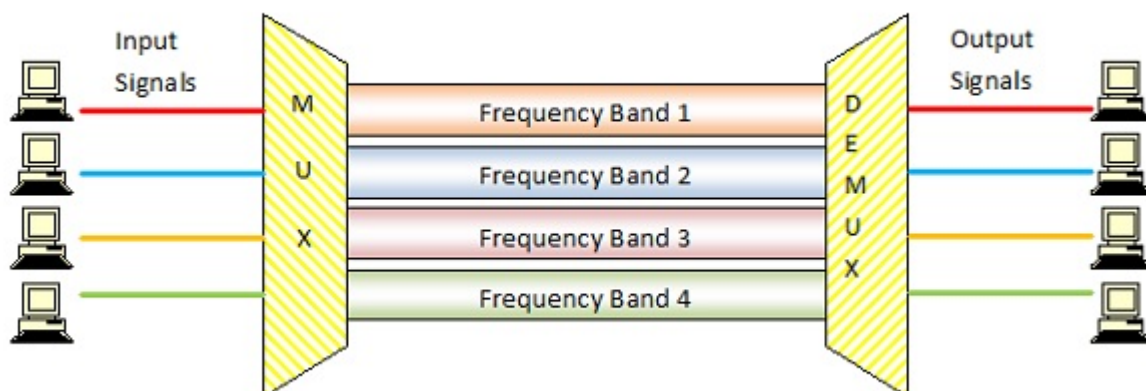
1. Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

State FDM with a neat diagram. M

In FDM, the total bandwidth is divided to a set of frequency bands that do not overlap. Each of these bands is a carrier of a different signal that is generated and modulated by one of the sending devices. The frequency bands are separated from one another by strips of unused frequencies called the guard bands, to prevent overlapping of signals.

The modulated signals are combined together using a multiplexer (MUX) in the sending end. The combined signal is transmitted over the communication channel, thus allowing multiple independent data streams to be transmitted simultaneously. At the receiving end, the individual signals are extracted from the combined signal by the process of demultiplexing (DEMUX).



Draw the encoded signal for the NRZ-L and NRZ-I Scheme of the following bits;
001101101 M

(ans kiye ho to dm [Nehal Bhuyan](#) / [WhatsApp](#))

What are the key elements of a protocol? S

The key elements of a protocol are syntax, semantics and timing.

Define distortion. S

Distortion means changes in the form or shape of the signal. This is generally seen in composite signals made up with different frequencies.

In a noiseless channel with a bandwidth of 6000 hz transmitting a signal with two signal levels. Calculate the bit rate? S

Consider a noiseless channel with a bandwidth of 6000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as Bit Rate = $2 \times 6000 \times \log_2 2 = 12000$ bps. (Bit Rate = $2 \times \text{bandwidth} \times \log_2 L$)

What is the difference between half-duplex and full-duplex transmission modes? S

A half-duplex transmission could be considered a one-way street between sender and receiver. Full-duplex, on the other hand, enables two-way traffic at the same time.

Explain different types of topology with their advantages and disadvantages. L

Advantages and disadvantages of topologies (Link)

Differentiate between TDM and FDM. M

Parameters	TDM	FDM
Full-Form	The term TDM is an acronym for Time Division Multiplexing.	The term FDM is an acronym for Frequency Division Multiplexing.
Basic	For all the signals it deals with, it shares the overall timescale. It means that it shares the time for available signals.	For all the signals it works with, it shares the overall frequency. It means that it shares the frequency for the available signals.
Types of Signals	It works with both- digital as well as analog signals.	It only deals with analog signals.
Circuitry	It consists of a very simple type of circuitry.	The circuitry, in this case, is comparatively more complex.
Wiring Used	The Chip or Wiring of TDM is comparatively much simpler.	FDM has a comparatively much more complex Chip or Wiring.
Conflict	This technique has very low conflict.	This technique has a comparatively higher conflict.
Input Required	The synchronization pulse is a prerequisite in the case of the TDM technique.	The guard band is a prerequisite in the case of the FDM technique.
Interference	The TDM technique has a very low or negligible interference.	The FDM technique has a very high level of interference.
Efficiency	This technique is way more efficient than FDM.	This technique is quite inefficient as compared to TDM.

Module 2

Given an account of the frame format of I-frame and S-frame in HDLC protocol, describing the function of each field. L

I-frame (Information frame) in HDLC has the following fields:

Flag: marks the beginning and end of the frame

Address: contains the device address

Control: contains the frame type and control information

Information: contains the data being sent

Frame Check Sequence (FCS): used for error detection

Flag: marks the end of the frame

S-frame (Supervisory frame) in HDLC has the following fields:

Flag: marks the beginning and end of the frame

Address: contains the device address

Control: contains the frame type and control information specific to S-frame like sequence numbers, Receiver ready/not ready etc

Information field is absent

Frame Check Sequence (FCS): used for error detection

Flag: marks the end of the frame

Difference between CSMA and CSMA/CD. M

S.NO	CSMA/CD	CSMA/CA
1.	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision.
2.	CSMA / CD is used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
3.	It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
4.	CSMA / CD resends the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5.	CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11 standard.
6.	It is more efficient than simple CSMA(Carrier Sense Multiple Access).	While it is similar to simple CSMA(Carrier Sense Multiple Access).

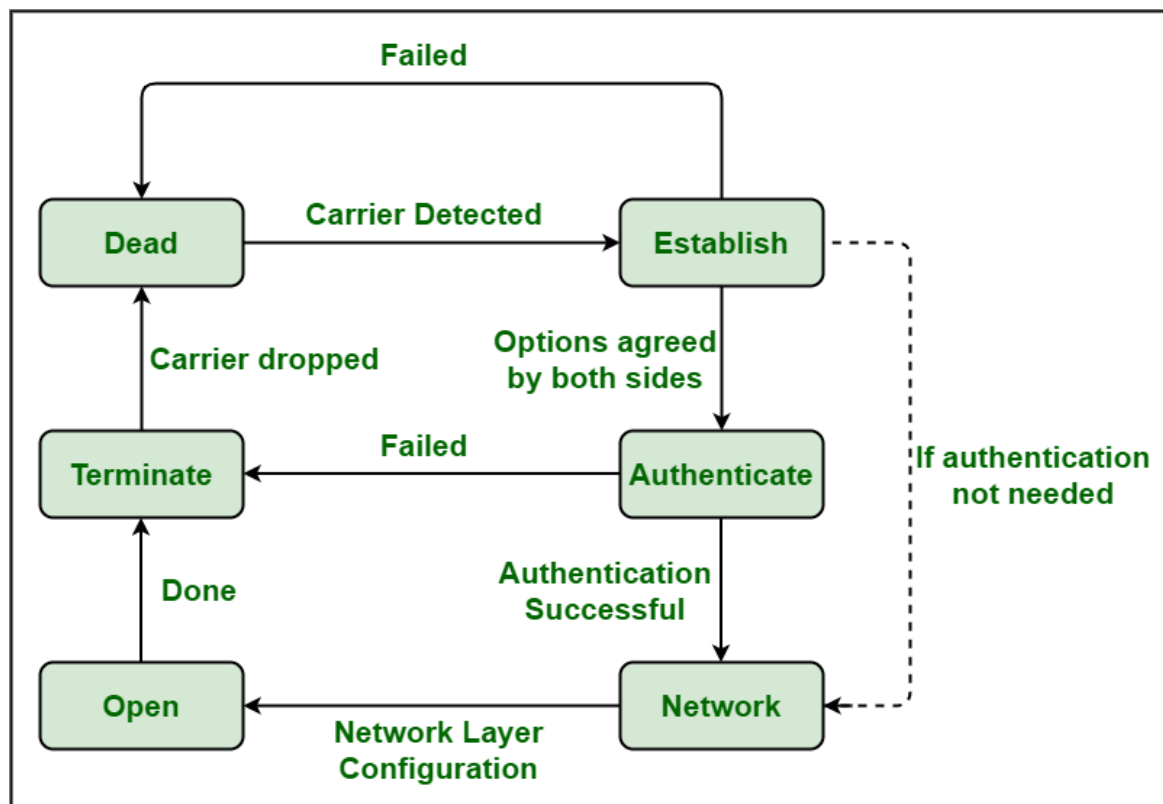
What is bit stuffing? Bit stuff the following data:

0001111101111110011 S

Bit stuffing is a technique that adds extra bits to data to prevent control characters confusion.

To bit stuff the data 0001111101111110011, add a 0 after every 5 consecutive 1s, resulting in 000111110111111010011.

Draw the phase transition diagram for PPP. Distinguish between PAP and CHAP. L



Transition Phases

Password Authentication Protocol

It is a two-step process to verify the identity of the client.

Authentication is only requested at the initial time of establishment of link or connection.

This protocol is less secured implementation as actual passwords are transmitted without any encryption code or pattern through the link.

In this, both the user name and passwords are transmitted through the link.

Unencrypted usernames and Passwords are usually transmitted in plain text.

It also allows point to point protocol to validate users i.e. to check and verify the users.

It does not provide protection and prevention from trial and error attacks.

It cannot do repeated midsession authentications.

Its usage has been decreased due to security issues.

In PAP, Authentication is done only at the caller side or client side.

Challenge Handshake Authentication Protocol

It is a three-step process of exchange of a shared secret.

Authentication is requested at the initial time of establishment of link or connection and can also be requested after the establishment of link or connection.

This protocol is highly secure in implementation as the actual password is never transmitted through the link.

In this, only the username is transmitted through the link.

Encrypted username and password are usually transmitted in this type of authentication.

It is a communication protocol that simply authenticates a user or a network host to an authentication entity.

It effectively provides protection and prevention from trial and error attacks.

It can also do repeated midsession authentications.

It is used by remote users, routers, and NASs simply to provide authentication before connectivity.

In CHAP, Authentication is done at both of the sides.

What do you mean by multiple accesses? Briefly discuss the operations of CSMA/CD and CSMA/CA random access methods. L

Multiple access refers to the ability of multiple devices to share a communication channel and access it simultaneously. In a multiple access network, a communication channel is shared by multiple devices, and the devices need a method to decide when to transmit and when to listen.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) and CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) are two different random access methods used in LANs.

CSMA/CD: In this method, devices listen to the channel before transmitting. If the channel is busy, the device waits for a random amount of time and then listens again. If the channel is still busy, the device waits again. If the channel is idle, the device can transmit. If a collision occurs, the devices involved in the collision sense the collision and stop transmitting, and the colliding devices wait for a random amount of time before trying to transmit again.

CSMA/CA: In this method, devices listen to the channel before transmitting. If the channel is busy, the device waits for a random amount of time and then listens again. If the channel is still busy, the device waits again. If the channel is idle, the device can transmit. If a collision occurs, the devices involved in the collision sense the collision and stop transmitting. Instead of waiting for a random amount of time before trying to transmit again like CSMA/CD, devices in CSMA/CA use a random back-off algorithm to decide when to try to transmit again.

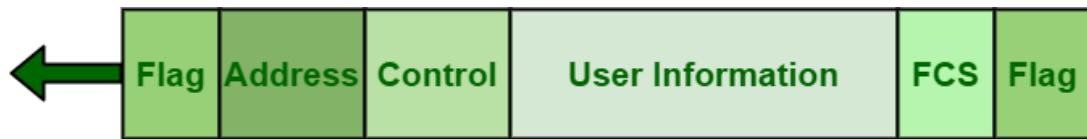
In summary, both CSMA/CD and CSMA/CA are multiple access methods where devices listen to a channel before transmitting, but CSMA/CD uses collision detection while CSMA/CA uses collision avoidance to handle the collision.

Define HDLC. Discuss about the different formats of HDLC frame with neat diagrams. L

High-Level Data Link Control (HDLC) generally provides flexibility to simply support all options that are possible in various data transfer modes and configurations. To provide flexibility, HDLC basically uses and explains three different types of frames. Type of frame is basically determined by the control field of the frame. Each type of frame generally serves as an envelope for transmission of various types of messages. These three different classes of frames used in HDLC are given below.

1. **I-frame** : I-frame stands for Information frames. This frame is generally used for transporting user data from the network layer. These frames actually carry actual data or information of the upper layer and some control information. This frame carries data along with both a send sequence number and an acknowledgment number. It can also be used to piggyback acknowledgement

information in case of ABM (Asynchronous Balanced Mode). The first bit of this frame of the control field is 0.



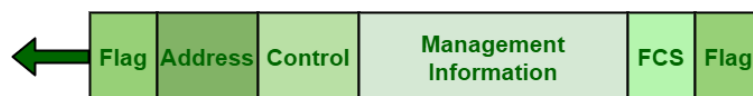
I-frame

2. **S-frame** : S-frame stands for Supervisory frames. These frames are basically required and essential for error control and flow control. They also provide control information. It contains or includes only an Acknowledgment number. First two bit of this frame of the control field is 10. S-frame does not have any information fields. This frame contains send and receive sequence numbers.



S-frame

3. **U-frame** : U-frame stands for Unnumbered frames. These frames are also required in various functions like link setup and disconnections. These frames basically support control purposes and are not sequenced. First, two-bit of this frame of the control field are 11. Some U-frame contain an information field depending on the type. These frames are also used for different miscellaneous purposes along with link management. U-frame is required for managing the link itself. This frame does not include any type of acknowledgment information i.e. in turn it includes or is contained in sequence number. These frames are generally reserved for system management.



U-frame

How TDM differs from FDM. What are the types of TDM? Explain each of them in detail. L

TDM (Time Division Multiplexing) and **FDM (Frequency Division Multiplexing)** are both multiplexing techniques that allow multiple signals to share a single communication channel. The main difference between them is the way they divide the channel into smaller units. TDM divides the channel into time slots, while FDM divides the channel into frequency bands. TDM assigns each device a specific time slot, while FDM assigns each device a specific frequency band. TDM is efficient and predictable but less flexible than FDM. FDM is more flexible but less efficient than TDM.

Synchronous TDM: In this type of TDM, the time slots are fixed and of equal length. Each device is assigned a specific time slot, and it can only transmit during its assigned time slot. The devices are synchronized with a common clock signal, and the time slots are repeated periodically. This type of TDM is typically used in digital networks such as T1 and E1.

Asynchronous TDM: In this type of TDM, the time slots are not fixed and may vary in length. Each device is assigned a time slot based on its data rate, and it can transmit whenever it has data to send. The devices are not synchronized with a common clock signal, and the time slots are not repeated periodically. This type of TDM is typically used in analog networks such as voice over telephone lines.

In variable-size framing, what are the ways there are to define the end of one frame and the beginning of the next frame? S

In variable-size framing, there are several ways to define the end of one frame and the beginning of the next frame, such as:

Using a special character or sequence of characters as a delimiter between frames.
Using a fixed number of idle bits or a predefined pattern of bits between frames.
Using a specific bit or field in the header of the frame to indicate the end of the frame.
Using the length field in the header of the frame to indicate the end of the frame.

What is the purpose of Virtual Circuit Identifier? S

The Virtual Circuit Identifier (VCI) is a unique identifier assigned to a virtual circuit that is used to identify it among other virtual circuits in a network. It is used by a switch or router to identify the specific virtual circuit to which a data packet belongs to and forward it to the correct destination.

Explain the mechanism of Stop and Wait ARQ for different operations and how selective Repeat ARQ differs from it. L

Stop-and-Wait ARQ is a type of Automatic Repeat Request (ARQ) error control method used to ensure reliable data transfer over a noisy communication channel. The mechanism of Stop-and-Wait ARQ is as follows:

- **Data transmission:** The sender sends a single frame of data at a time and waits for an acknowledgement (ACK) from the receiver.
- **Acknowledgement:** The receiver receives the frame and sends an ACK to the sender.
- **Timeout:** If the sender does not receive an ACK within a certain time period (timeout), it retransmits the same frame.
- **Frame acceptance:** If the receiver receives the same frame multiple times, it accepts only the first copy and discards the rest.

- **Frame error:** If the receiver detects an error in the received frame, it sends a negative acknowledgement (NAK) to the sender, and the sender retransmits the same frame.

The main difference between Stop-and-Wait ARQ and Selective Repeat ARQ is that in the later, the receiver can selectively retransmit lost or corrupted frames, and the sender retransmits only the lost or corrupted frames, not all the frames. This makes Selective Repeat ARQ more efficient than Stop-and-Wait ARQ.

Demonstrate the mechanism used in Go-Back –N ARQ for normal and damaged/lost frame operations. L

Go-Back-N ARQ is a type of Automatic Repeat Request (ARQ) error control method that is similar to selective repeat ARQ, but it allows the sender to transmit multiple frames before waiting for an acknowledgement (ACK) from the receiver. The mechanism of Go-Back-N ARQ is as follows:

1. **Data transmission:** The sender sends a certain number of frames (N) before waiting for an acknowledgement from the receiver. These frames are sequentially numbered and the sender keeps track of the highest acknowledged number, which is called the Next Expected Acknowledge (NEA).
2. **Acknowledgement:** The receiver receives the frames and sends an ACK for each successfully received frame. The ACK contains the number of the next expected frame.
3. **Frame acceptance:** If the receiver receives a duplicate frame, it discards it and sends an ACK for the previously acknowledged frame.
4. **Frame error:** If the receiver detects an error in a received frame, it discards it and sends a negative acknowledgement (NAK) for the frame number that contains the error.
5. **Lost frame:** If the receiver doesn't receive a frame, it sends a NAK for the next expected frame.
6. **Timeout:** If the sender doesn't receive an ACK or NAK within a certain time period (timeout), it retransmits all the frames starting from the frame number specified in the NAK or the NEA.

In case of lost frame or damaged frame, the sender retransmits the lost frame or the damaged frame after receiving a NAK for that frame. The sender also retransmits all the frames after the lost or damaged frame until the Next Expected Acknowledge (NEA) or the highest acknowledged number.

In summary, Go-Back-N ARQ allows the sender to transmit multiple frames before waiting for an acknowledgement, this makes it more efficient than Stop-and-Wait ARQ, but less efficient than Selective Repeat ARQ as it retransmits all frames after the lost or damaged frame.

List down different techniques of error detection. S

Different techniques of error detection include:

- Parity check
- Cyclic Redundancy Check (CRC)
- Checksum
- Hash functions
- Forward Error Correction (FEC)
- Hamming Code
- Error-Correcting Code (ECC)

What are the two main methods of error correction? S

The two main methods of error correction are:

- **Forward Error Correction (FEC):** It is a method where the sender adds redundant data to the original data, before transmitting it, so that the receiver can use this redundant data to detect and correct errors.
- **Automatic Repeat Request (ARQ):** It is a method where the receiver sends an acknowledgement (ACK) to the sender after receiving a frame of data, if the frame is received without errors. If the receiver detects an error in the received frame, it sends a negative acknowledgement (NAK) to the sender, so that the sender can retransmit the frame.

Differentiate between error detection and error correction. S

Error detection and error correction are both methods used to ensure the integrity of data during transmission over a noisy communication channel.

- **Error detection:** is a method used to detect errors that occur during data transmission. It does this by adding extra bits, called redundancy bits, to the data, which can be used to check whether errors have occurred or not.
- **Error correction:** is a method used to correct errors that occur during data transmission. It does this by using redundant information added to the data, called error-correcting code, to detect and correct errors in the data.

What are the responsibilities of the data link layer? S

The data link layer is responsible for providing reliable data transfer between devices on a single link. It provides error detection and correction, flow control, and media access control. In short, the data link layer ensures that data is transmitted correctly and reliably between devices on a local network.

Differentiate between circuit switching and packet switching. M

Difference Between Circuit Switching and Packet Switching	
Circuit Switching	Packet Switching
A circuit needs to be established to make sure that data transmission takes place.	Each packet containing the information that needs to be processed goes through the dynamic route.
A uniform path is followed throughout the session.	There is no uniform path that is followed end to end through the session.
It is ideal for voice communication, while also keeping the delay uniform.	It is used mainly for data transmission as the delay is not uniform.
Without a connection, it cannot exist, as the connection needs to be present on a physical layer.	A connection is not necessary, as it can exist without one too. It needs to be present on a network layer.
Data to be transmitted is processed at the source itself.	Data is processed and transmitted at the source as well as at each switching station.

What is the operation of CRC? Given a 10-bit sequence 1011001011 and a divisor of 1101, find the CRC. Verify your answer.

CRC (Cyclic Redundancy Check) is an error detection method that uses a mathematical algorithm to generate a checksum, called a CRC value, based on the data being transmitted. The receiver uses the same algorithm to calculate the CRC value of the received data and compares it to the transmitted CRC value. If the values match, the data is assumed to be error-free; otherwise, an error is detected.

Construct the Hamming code for the bit sequence 110011001. L

The Hamming Code is a type of error-correcting code that can detect and correct errors in a bit sequence. To construct the Hamming code for the bit sequence 110011001, the following steps are performed:

1. Find the number of redundant bits, r , needed to make the total number of bits, n , equal to $2^r - 1$.
In this case, we need to add 3 redundant bits to the 9 data bits.
2. Place the redundant bits in positions that correspond to powers of 2. This is called parity bit positioning. In this case, we will place the redundant bits in positions 1, 2 and 4.
3. Calculate the value of the redundant bits by applying the parity bit formula.
- 4.

The redundant bits are calculated as follows:

Parity bit 1: (1, 3, 5, 7, 9) = $1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 = 1$

Parity bit 2: (2, 3, 6, 7) = $1 \oplus 0 \oplus 0 \oplus 1 = 0$

Parity bit 4: (4, 5, 6, 7) = $0 \oplus 1 \oplus 0 \oplus 1 = 0$

The final Hamming code for the bit sequence 110011001 is 110110001, where the first, second and fourth positions are the redundant bits.

The receiver can check if a transmission error has occurred by comparing the received Hamming code and the calculated Hamming code. If they don't match, it can use the redundant bits to correct the error.

How fiber optic cable differs from coaxial cable? M

Sr. No.	Key	Optical Fibre	Coaxial Cable
1	Transmission Type	Optical Fibre transmits data/signals in the form of light.	The coaxial cable transmits data/signals in the form of electrical signals.
2	Material	Optical fibre is made using plastic and glass.	Coaxial cable is prepared using plastic and copper wires.
3	Efficiency	Optical fibre is highly efficient and signal loss is negligible.	Coaxial cable is less efficient.
4	Cost	Optical fibre is costly and its installation is quite expensive.	Coaxial cable is cheap and its installation is less expensive.
5	Weight	Optical fibre is quite light in weight.	Coaxial cable is very heavy as compared to an optical fibre.
6	Bandwidth	Optical fibre bandwidth is less than coaxial cable.	Coaxial cable provides high bandwidth.
7	Diameter	Optical fibre is having a smaller diameter.	Coaxial cable diameter is bigger than that of optical fibre.
8	Installation	The installation of Optical fibre is complex.	The installation of Coaxial cable is comparatively easy.

Differentiate among UTP and STP cable. M

Key	Unshielded Twisted Pair (UTP)	Shielded Twisted Pair (STP)
Full form	UTP stands for Unshielded Twisted Pair.	STP stands for Shielded Twisted Pair.
Grounding	Grounding cable is not required.	Grounding cable is required.
Data Transmission Rate	Data Transmission Rate is slower than STP.	Data Transmission Rate is very high.
Cost	UTP cables are cheaper.	STP cables are expensive.
Maintenance	Low maintenance cost in case of UTP.	High maintenance cost in case of STP.
Noise	Noise is high in UTP.	Noise is quite less in STP.
Crosstalk	Possibility of crosstalk is very high in UTP.	Possibility of crosstalk is quite low in STP.

Module 3

What is dotted decimal notation in IPv4? How many numbers of bytes are required to represent an address in dotted decimal notation? S

Dotted decimal notation is a human-readable representation of IPv4 addresses that separates the four octets of the IP address with a period. Each octet is represented by a decimal number between 0 and 255, and the IP address is written as four decimal numbers separated by periods.

Each number of bytes required to represent an address in dotted decimal notation is 4 bytes.

For a given IP address 192.168.1.0/26, L

- i. Find the subnet mask.
- ii. How many subnets will the subnet mask provide?
- iii. What is the block size for a subnet mask?
- iv. What are the valid subnets?
- v. How many valid hosts are available per subnet?
- vi. What is the broadcast address of each subnet?
- vii. What is the network address of each subnet?

For the given IP address 192.168.1.0/26,

- i. The subnet mask for this IP address is 255.255.255.192, which is derived from the number of bits in the subnet mask (26) and the subnet mask notation (CIDR notation)
- ii. With a subnet mask of 255.255.255.192, it will provide 64 subnets.
- iii. The block size for this subnet mask is 64.
- iv. Valid subnets are
192.168.1.0
192.168.1.64
192.168.1.128
192.168.1.192
- v. There are 62 valid hosts available per subnet
- vi. The broadcast address of each subnet is the last IP of the subnet block. For example, the broadcast address of subnet 192.168.1.0 is 192.168.1.63, the broadcast address of subnet 192.168.1.64 is 192.168.1.127 and so on.
- vii. The network address of each subnet is the first IP of the subnet block. For example, the network address of subnet 192.168.1.0 is 192.168.1.0, the network address of subnet 192.168.1.64 is 192.168.1.64 and so on.

Generate the shortest path tree for the given topology using the link-state routing protocol, taking E as the root node. (incomplete question)

▶ **Link State Routing in computer networks || Link state routing algorithm || Computer Net...**

▶ **3.6 Dijkstra Algorithm - Single Source Shortest Path - Greedy Method**

Distinguish between multicast and broadcast. S

Broadcast sends to all devices on a network, Multicast sends to a specific group of devices on a network.

Differentiate between Link state routing and Distance vector routing. L

Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkstra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

Why does RIP use UDP instead of TCP?

RIP (Routing Information Protocol) is a distance-vector routing protocol that is used to distribute routing information within a network. It uses UDP (User Datagram Protocol) instead of TCP (Transmission Control Protocol) for several reasons:

1. **Low overhead:** UDP is a connectionless, simple protocol that does not require the overhead of establishing and maintaining a connection, as is necessary with TCP. This makes it more efficient for applications that need to send a large number of small packets, such as routing protocols.

2. **Less delay:** Because UDP does not require the overhead of establishing and maintaining a connection, it incurs less delay than TCP. This is important for real-time applications like routing protocols, where delay can cause problems.
3. **No congestion control:** UDP does not provide any mechanism for congestion control, which makes it more suitable for routing protocols, where the goal is to quickly propagate routing information regardless of network congestion.
4. **Broadcasting:** UDP allows for broadcasting packets to all devices on a network, which makes it a good fit for routing protocols that need to send information to all routers in a network.

In summary, using UDP for RIP allows for more efficient, less delayed and faster communication, it also allows for broadcasting packets.

What is a mask in IPv4 addressing? What is a default mask in IPv4 addressing?

A mask in IPv4 addressing is a 32-bit value that is used to specify which portion of an IP address represents the network address and which portion represents the host address. The mask is typically represented in dotted decimal notation (e.g. 255.255.255.0) and is used in conjunction with an IP address to determine the network and host addresses.

A default mask is the mask value that is used when no mask is explicitly specified. The default mask is determined by the class of the IP address. The three classes of IP addresses (A, B, and C) have different default masks.

- Class A IP addresses have a default mask of 255.0.0.0, the first octet is used for the network address and the remaining three octets are used for the host address.
- Class B IP addresses have a default mask of 255.255.0.0, the first two octets are used for the network address and the remaining two octets are used for the host address.
- Class C IP addresses have a default mask of 255.255.255.0, the first three octets are used for the network address and the remaining octet is used for the host address.

It's worth noting that the default mask method of IP addressing is now considered as an obsolete method and replaced by CIDR (classless inter-domain routing) which allows for more flexible and fine-grained IP address allocation.

A block of addresses is granted to a small organization. If one of the addresses is **205.16.37.39/28**. Find the class, net-id, host-id, first address, last address and the number of addresses in the block. L

- The IP address is 205.16.37.39/28, which means it is a CIDR notation.
- The class of this IP address is Class C, which means the first three octets of the address (205.16.37) represent the network address, and the last octet (39) represents the host address.

- The net-id of this IP address is 205.16.37.32, the net-id is the network address of the IP block, and it is obtained by setting the host bits of the IP address to 0.
- The host-id of this IP address is 39, the host-id of the IP address is the last octet of the IP address which is represented by the host bits of the IP address
- The first address of the block is 205.16.37.32, it is the same as the net-id
- The last address of the block is 205.16.37.47, it is obtained by setting the host bits of the last IP address of the block to 1.
- The number of addresses in the block is 16, it is calculated by $2^{(32-28)} = 2^4 = 16$
- The block of addresses is a Class C block, the net-id is 205.16.37.32, the host-id is 39, the first address of the block is 205.16.37.32, the last address of the block is 205.16.37.47, and the block contains 16 addresses.

In a block of addresses, we know the IP address of one host is **182.44.82.16/26**. What is the first address (network address) and the last address in this block? M

The IP address is 182.44.82.16/26, which means it is a CIDR notation.

The network address (also known as the first address) of this block is 182.44.82.0, it is obtained by setting the host bits of the IP address to 0.

The last address of this block is 182.44.82.63, it is obtained by setting the host bits of the last IP address of the block to 1.

The total number of addresses in the block can be calculated by $2^{(32-26)} = 2^6 = 64$

It's worth noting that the address 182.44.82.16/26 belongs to the block, and it's the first host address in the block and it's not the network address, the network address also known as the first address is 182.44.82.0.

Write the following masks in slash notation (/n).

- 255.255.255.0
- 255.0.0.0
- 255.255.224.0 M

- The mask 255.255.255.0 can be written in slash notation as /24
- The mask 255.0.0.0 can be written in slash notation as /8
- The mask 255.255.224.0 can be written in slash notation as /19

In the slash notation, the number after the slash represents the number of 1's in the binary representation of the mask.

It's worth noting that, the mask 255.255.255.0 is a Class C mask, 255.0.0.0 is a Class A mask, and 255.255.224.0 is a Class B mask, they are all used in CIDR (classless inter-domain routing) which allows for more flexible and fine-grained IP address allocation.

Find the range of addresses in the following blocks.

- a. 123.56.77.32/29
- b. 200.17.21.128/27
- c. 17.34.16.0/23 M

- a. The IP address 123.56.77.32/29 is a CIDR notation, The net-id of this IP address is 123.56.77.32, and the range of addresses in this block is 123.56.77.32 - 123.56.77.39.
- b. The IP address 200.17.21.128/27 is a CIDR notation, The net-id of this IP address is 200.17.21.128, and the range of addresses in this block is 200.17.21.128 - 200.17.21.159
- c. The IP address 17.34.16.0/23 is a CIDR notation, The net-id of this IP address is 17.34.16.0, and the range of addresses in this block is 17.34.16.0 - 17.34.17.255

It's worth noting that the net-id is the first IP address of the block, and the last IP address is obtained by setting the host bits to 1. The total number of addresses in the block can be calculated by $2^{(32-n)}$ where n is the number of bits in the mask.

Given a fragmented datagram (in IPv4) with an offset of 120, how can you determine the first and last byte numbers? S

The first byte number is 960 ($120 * 8$) and the last byte number can be calculated as 66495 ($65535 + \text{first byte number}$) if it's the last fragment.

State protocol stack of PPP. M

PPP (Point-to-Point Protocol) is a protocol stack that is used to establish a point-to-point link between two devices, such as a router and a remote host. The protocol stack of PPP includes the following layers:

Physical Layer: This is the lowest layer of the PPP protocol stack and it is responsible for establishing and maintaining the physical link between the two devices.

Data Link Layer: This layer is responsible for providing reliable data transfer across the physical link. It includes the following sublayers:

- a. Link Control Protocol (LCP): This sublayer is responsible for establishing, configuring, and maintaining the PPP link.
- b. Authentication Protocol (AP): This sublayer is responsible for authenticating the devices at each end of the link.
- c. Link Quality Report (LQR): This sublayer is responsible for monitoring the link quality.

Network Layer: This layer is responsible for providing network-layer services to the PPP link. It includes the following sublayers:

- a. Internet Protocol Control Protocol (IPCP): This sublayer is responsible for configuring the IP address and other parameters for the PPP link.

b. IPv6 Control Protocol (IPv6CP): This sublayer is responsible for configuring the IPv6 address and other parameters for the PPP link.

Higher-layer protocols: PPP provides a mechanism for encapsulating higher-layer protocols such as IP, IPv6, IPX, AppleTalk, and others, to be transported over the PPP link.

In short, PPP protocol stack includes Physical, Data Link, Network, and Higher-layer protocols to establish and maintain a point-to-point link

What is the range of private IPs for class A and class B?

Private IPs for class A: 10.0.0.0 - 10.255.255.255

Private IPs for class B: 172.16.0.0 - 172.31.255.255

How can you find the first IP, last IP and number of nodes in a network, if the mask is given as a 32 bit IP sequence? S

To find the first IP, last IP, and number of nodes in a network, you need to know the IP address and mask, and perform bitwise AND operation between the IP address and the mask.

To find the number of nodes, you have to subtract the number of host bits from 32, then raise 2 to that power.

Find the class, net-id and host-id of the following IP address: 188.25.45.48 S

The IP address 188.25.45.48 is Class B, net-id is 188.25.0.0 and host-id is 0.0.45.48

Module 4

Briefly explain the "Three way handshaking" process in a TCP connection. L

The "Three-way Handshaking" process, also known as the "TCP Three-way handshake" is the process used to establish a reliable, connection-oriented session between two systems using TCP (Transmission Control Protocol). The process involves the exchange of three messages between the two systems, as follows:

1. The first message, called the "SYN" (Synchronize) message, is sent by the initiating system (the client) to the receiving system (the server). The SYN message contains a randomly generated initial sequence number, which will be used to number the bytes of data sent during the session.
2. The second message, called the "SYN-ACK" (Synchronize-Acknowledgment) message, is sent by the receiving system (the server) to the initiating system (the client). The SYN-ACK message contains the server's own randomly generated initial sequence number and an acknowledgment of the client's initial sequence number.
3. The third message, called the "ACK" (Acknowledgment) message, is sent by the initiating system (the client) to the receiving system (the server). The ACK message contains the client's own acknowledgment of the server's initial sequence number.

Once the three-way handshake is complete, a reliable, connection-oriented session is established between the two systems, and data can be exchanged using the agreed upon sequence numbers. The session will be closed with a similar process in which the closing party sends a message called FIN, the other party ACK's it and then the closing party ACKs the ACK.

The three-way handshake process is important to ensure that both systems are ready to communicate and that the connection is established in a reliable and secure manner.

The following is the content of a TCP header in hexadecimal format. L
04720017 00000001 00001000 400207FF 0000000F

- a. What is the source port number?
- b. What is the destination port number?
- c. What is the sequence number?
- d. What is the acknowledgement number?
- e. What is the length of the header?
- f. What is the type of the segment?
- g. What is the window size?

- a. The source port number is located in the first 2 bytes of the TCP header (04 72 in hexadecimal), which corresponds to a decimal value of 1170.

- b. The destination port number is located in the next 2 bytes of the TCP header (00 17 in hexadecimal), which corresponds to a decimal value of 23.
- c. The sequence number is located in the next 4 bytes of the TCP header (00 00 00 01 in hexadecimal), which corresponds to a decimal value of 1.
- d. The acknowledgment number is located in the next 4 bytes of the TCP header (00 00 00 08 in hexadecimal), which corresponds to a decimal value of 8.
- e. The length of the header can be calculated from the HLEN field (4 bits) in the fourth byte of the TCP header (40 in hexadecimal), which corresponds to a decimal value of 4. So, the length of the header is $4 \times 4 \text{ bytes} = 16 \text{ bytes}$.
- f. The type of the segment cannot be determined from the given information. The type of the segment is conveyed by the values of the flags and is determined by the combination of the 6 control bits (URG, ACK, PSH, RST, SYN, FIN) found in the flags field in the TCP header.
- g. The window size is located in the next 2 bytes of the TCP header (07 FF in hexadecimal), which corresponds to a decimal value of 2047.

What role does ICMP play for an IP packet? What are the various types of ICMP packets that are sent back to the sender?

ICMP (Internet Control Message Protocol) is a network protocol that is used to send error messages and operational information about network conditions. ICMP is typically used by IP (Internet Protocol) to provide feedback about the success or failure of an IP packet's journey through the network.

The role of ICMP for an IP packet is to provide a mechanism for the sender to receive information about the state of the network, such as whether a destination host is reachable or if a packet has been lost. ICMP messages are typically generated by network devices, such as routers, in response to errors or exceptional conditions that occur when processing an IP packet.

There are several types of ICMP packets that are sent back to the sender, including:

1. **Echo Request/Reply (ping):** This type of ICMP packet is used to test the reachability of a host and measure the round-trip time for packets to travel from the source host to the destination host and back.
2. **Destination Unreachable:** This type of ICMP packet is sent back to the sender when a destination host or network is unreachable. This can occur due to a variety of reasons, such as a network being down or a host being offline.
3. **Time Exceeded:** This type of ICMP packet is sent back to the sender when a packet has been discarded because it exceeded the maximum time allowed for it to traverse the network.

4. **Parameter Problem:** This type of ICMP packet is sent back to the sender when an error has been encountered in the header of an IP packet.
5. **Redirect:** This type of ICMP packet is sent back to the sender when a more efficient route for the packet's destination is available.
6. **Echo Request/Reply (ping) and Timestamp Request/Reply:** These types of ICMP packet are used to determine the round-trip time and to measure the clock offset between the sender and the destination.

Compare the TCP header and the UDP header. List the fields in the TCP header that are missing from the UDP header.

The UDP header typically includes the following fields:

- **Source port:** Identifies the source of the datagram
- **Destination port:** Identifies the destination of the datagram
- **Length:** Indicates the total length of the UDP header and data
- **Checksum:** Verifies the integrity of the header and data

The fields that are missing from the UDP header compared to the TCP header are:

- **Sequence number**
- **Acknowledgment number**
- **Data offset**
- **Flags**
- **Window**
- **Urgent pointer**
- **Options**

In short, the UDP header is simpler and shorter than the TCP header, it does not have the features of reliability, flow control, and error correction that TCP provides.

Differentiate among UDP and TCP.

Feature	TCP	UDP
Connection status	Requires an established connection to transmit data (connection should be closed once transmission is complete)	Connectionless protocol with no requirements for opening, maintaining, or terminating a connection
Data sequencing	Able to sequence	Unable to sequence
Guaranteed delivery	Can guarantee delivery of data to the destination router	Cannot guarantee delivery of data to the destination
Retransmission of data	Retransmission of lost packets is possible	No retransmission of lost packets
Error checking	Extensive error checking and acknowledgment of data	Basic error checking mechanism using checksums
Method of transfer	Data is read as a byte stream; messages are transmitted to segment boundaries	UDP packets with defined boundaries; sent individually and checked for integrity on arrival
Speed	Slower than UDP	Faster than TCP
Broadcasting	Does not support Broadcasting	Does support Broadcasting
Optimal use	Used by HTTPS, HTTP, SMTP, POP, FTP, etc	Video conferencing, streaming, DNS, VoIP, etc

The following is a dump of a UDP header in hexadecimal format.

0632000DOO ICE217

- What is the source port number?
- What is the destination port number?
- What is the total length of the user datagram?
- What is the length of the data?

- The source port number is located in the first 2 bytes of the UDP header (06 32 in hexadecimal), which corresponds to a decimal value of 1570.
- The destination port number is located in the next 2 bytes of the UDP header (00 0D in hexadecimal), which corresponds to a decimal value of 13.
- The total length of the user datagram is located in the next 2 bytes of the UDP header (OO in hexadecimal) which corresponds to a decimal value of OO. However, the given hexadecimal dump is not complete and it seems to be a typo, it doesn't have the correct format of a hexadecimal representation, thus it's impossible to extract the value of the total length.
- The length of the data can't be extracted from the provided hexadecimal dump since we don't have the total length of the user datagram and we can't calculate it by subtracting the length of the header from the total length of the user datagram.

In TCP, if the value of HLEN is 0111, how many bytes of option is included in the segment?
What is the significance of the "Sequence number" and "Acknowledgement number" field in a TCP segment?

In TCP (Transmission Control Protocol), the HLEN (Header Length) field is 4 bits long and it specifies the length of the TCP header in 32-bit words.

If the value of HLEN is 0111, it corresponds to a decimal value of 7. This means that the length of the TCP header is 7 32-bit words, or $7 \times 4 = 28$ bytes.

So, if the value of HLEN is 0111, the number of bytes of options included in the segment is 28 bytes - 20 bytes (the fixed size of the TCP header without options) = 8 bytes.

Sequence number

This 32 bit field defines the number assigned to the first byte of data contained in this segment.

As TCP is a stream transport protocol, to ensure connectivity, each byte to be transmitted is numbered.

The sequence number tells the destination which byte in this sequence is the first byte in the segment.

Acknowledgment number

This 32 bit field defines the byte number that the receiver of the segment is expecting to receive from the other party.

If the receiver of the segment has successfully received byte number x from the other party, it returns x+1 as the acknowledgment number. Acknowledgement and data can be piggybacked together.

Define a Socket? What role does it play in data delivery across multiple networks?

A socket is an endpoint for sending or receiving data across a computer network. It is a combination of an IP address and a port number, used to identify a specific process running on a host.

The role of sockets in data delivery across multiple networks is to act as a bridge between the application layer and the network layer. Sockets allow applications to send and receive data using a standard interface, regardless of the underlying network protocol. This means that an application can use the same socket code to communicate over different networks, such as TCP/IP or UDP.

Sockets also enable communication between different computers on a network, by providing a way to identify and address the endpoint of a connection. They enable the use of multiple networks such as IP and other protocols to be used together, to form a communication channel.

Module 5

Explain the architecture of the Domain Name System(DNS) to map the domain name to IP address using the recursive method. L

Mapping a name to an address or an address to a name is called name-address resolution.

Recursive Resolution:

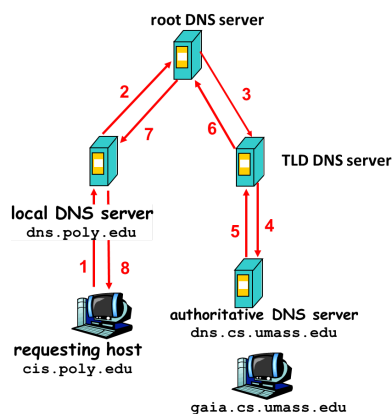
The resolver asks for a recursive answer from a DNS server.

The server must respond with the complete answer.

If it does not know the answer the server itself asks a parent server in the hierarchy.

If the parent does not know, the parent asks a higher level server in the hierarchy.

Eventually the resolver will be told the answer by the first DNS server the resolver contacted.



With the help of a diagram, explain the working of HTTP request and response from a Client-Server communication perspective. Why is HTTP a stateless protocol? L



HTTP (Hypertext Transfer Protocol) is a protocol that is used for communication between a server and a client. The following is a step-by-step overview of the process of communication between an HTTP client (such as a web browser) and an HTTP server (such as a website):

1. The client sends an HTTP request to the server. The request includes a method (such as GET or POST) and a URL (Uniform Resource Locator) that specifies the location of the resource it is requesting.
2. The server receives the request and processes it. It then sends an HTTP response message to the client.
3. The response message includes a status code (such as 200 for success or 404 for not found) and any data that is requested, such as HTML, XML, JSON, or plain text.
4. The client receives the response and processes the data. If the status code is 200, the client displays the requested information. If the status code is 404, the client shows an error message to the user.
5. The client and server can continue to exchange messages to complete the task.
6. Once the communication is complete, the client and server close their connections.

HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

Briefly explain the functions of FTP? What are the default port numbers used by FTP? M

It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, text files to be transferred between different kinds of computers. The end-user in the connection is known as localhost and the server which provides data is known as the remote host.

FTP utilizes two ports, a 'data' port and a 'command' port (also known as the control port). These are port 20 for the data port and port 21 for the 'command' port.

What is the difference between an active document and a dynamic document? M

A dynamic document is the product of a program run by a server as requested by a browser. An active document is the product of a program sent from the server to the client and run at the client site.

What is a proxy server and how is it related to HTTP? M

A proxy server lessens network traffic by rejecting unwanted requests, forwarding requests to balance and optimize server workload, and fulfilling requests by serving data from cache rather than unnecessarily contacting the true destination server. HTTP Server has proxy server capabilities built in.

What is an advantage of a hierarchical name space over a flat name space for a system the size of the Internet? S

When the name space is large, searching a name in a hierarchical structure (tree) is much faster than searching it in a flat structure (linear). The first can use a binary search; the second needs to use a sequential search.

What are the three FTP transmission modes? S

In FTP, there are three types of Transmission modes stream, block, and compressed.

Consider different activities related to email:

m1: Send an email from a email client to a email server

m2: Download an email from mailbox server to a email client

m3: Checking email in a web browser

What are the application-layer protocols used in each activity? S

m1 : SMTP m2 : POP m3 : HTTP


Sending an email will be done through user agent and message transfer agent by SMTP, downloading an email from mailbox is done through POP, checking email in a web browser is done through HTTP.

Identify the correct order in which the following actions take place in an interaction between a web browser and a web server.

- 1.The web browser requests a web page using HTTP.
- 2.The web browser establishes a TCP connection with the webserver.
- 3.The web server sends the requested web page using HTTP.
- 4.The web browser resolves the domain name using DNS.

4 → 2 → 1 → 3

[Important Numericals PDF](#) 

 cn numericals.pdf

Mod 1, 2 MidSem Important Questions

1. Different topologies and their advantages and disadvantages. Number of links required in each case if n number of devices are there.
2. Encode a given bit sequence using line coding techniques
3. like 1011110011 using NRZ-L, NRZ-I etc
4. OSI and TCP/IP reference model
5. Differentiate bit rate and baud rate.
6. Compare and contrast FDM, TDM.
7. STP, UTP, Coaxial cable, Fibre optic cable
8. Given a dataword and divisor find codewords using CRC.
9. List error detection methods.
10. Differentiate Packet switching and Circuit Switching
11. List the responsibilities of Data Link Layer
12. Define Virtual Circuit Identifier.
13. Describe all analog to analog conversion techniques.