Unit-1

1. Define computer networks. [2M]

A computer network is a collection of two or more computer systems that are linked together to share information and resources.

2. Explain Applications of computer network.

- E-mail: E-mail is the electronic way of exchanging messages between the two entities.
- E-commerce: E-commerce is the electronic method of buying or selling goods and services over the internet.
- E-governance: The role of computer networking in e-governance is sharing government services, information among the citizens and the government officials.
- Sharing of resources: The major uses of computer networking is the sharing of resources. The resources can be of two types; hardware and software. The hardware resources include printers, scanners, disk storage space etc, whereas the software resources include the application software running on the server.
- Banking: Banking sectors operated their function online with the help of a computer network. Every bank stores their customers account information in the database server.

3. Give two differences between point to point and multipoint connection.

Point to Point connection	Multipoint connection
Point to point connection means the channel is shared between two devices.	Multipoint Connection means the channel is shared among multiple devices.
In this connection, there is one transmitter and one receiver.	In this connection, there is one transmitter and many receivers.
The smallest distance is most important to reach the receiver.	The smallest distance is not important to reach the receiver.
It provides security and privacy because communication channel is not shared.	It does not provide security and privacy because communication channel is shared.

4. Explain classification of computer networks/ Explain Types of computer networks.[5m]

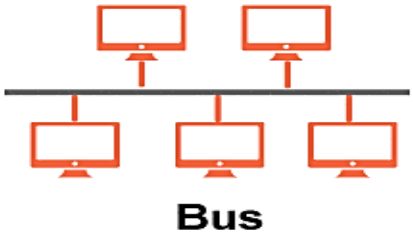
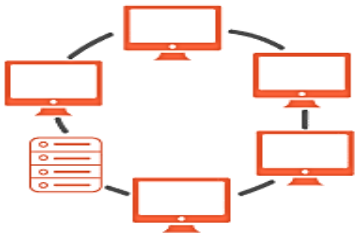
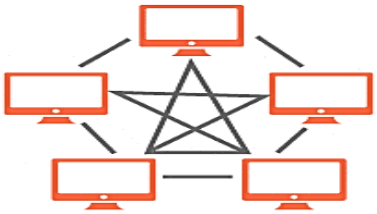
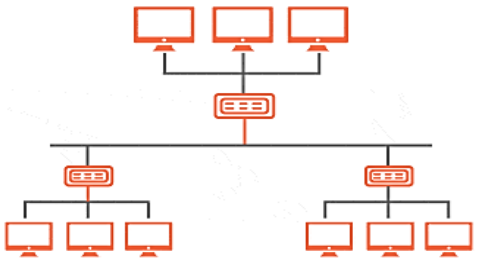
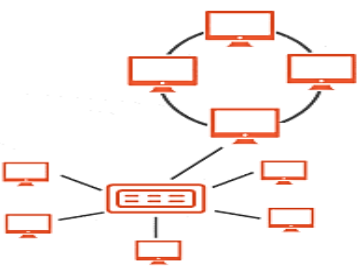
1.PAN: Personal Area Network

- It is a network that connects computers, mobile phones, tablets, printers, ETC. Placed at a limited distance.
- PAN covers an area of 30 feet
- It is used for connecting the computer devices of personal use.
- PAN can be wired or wireless connection.
- PAN has a various application.

2.LAN	3.MAN	4.WAN
LAN stands for local area network.	MAN stands for metropolitan area network.	WAN stands for wide area network.
Operates in small areas such as the same building or campus.	Operates in large areas such as a city.	Operates in larger areas such as country or continent.
LAN's ownership is private.	MAN's ownership can be private or public.	WAN also might not be owned by one organization.
The transmission speed of a LAN is high	The transmission speed of a MAN is average.	The transmission speed of a WAN is low.
There is less congestion in LAN.	There is more congestion in MAN.	There is more congestion than MAN in WAN.
LAN's design and maintenance are easy.	MAN's design and maintenance are difficult than LAN.	WAN's design and maintenance are also difficult than LAN as well MAN.
There is more fault tolerance.	There is less fault tolerance.	There is also less fault tolerance.

5. Explain Network Topologies.[5m/10m]

Topology: Topology defines the structure of the network how all the components are interconnected to each other.

1)Bus Topology: •In Bus Topology One long cable acts as a backbone to link all the devices in a network. •Devices share the same communication channel. •It is easy to install and Cost of the network is low. •It requires less Number of I/O ports. •Heavy network traffic can slow down the network. •Difficult to add new device and Difficult reconnection.	 Bus
2)Ring Topology: •Devices connected in a circular or ring arrangement. •Each device has exactly two neighbours for communication purposes. •Efficient data transmission. •Fault detection and isolation •Adding/removing of device disturb the network. •Failure of one device can affect the whole network. •Cost of cable is more.	 Ring
3)Star Topology: •Central hub or switch connects all devices in the network. •Each device has a dedicated link to the central hub. •Limited failure and Trouble shooting techniques is easy. •It is easy to modify and add new device. •If the central hub fails the whole network fails to operate. •Installation and Arrangement is difficult.	 Star
4)Mesh Topology: • Devices are interconnected, and each device may have a connection to every other device. • Fast Communication • Easier Reconfiguration • Complex installation and maintenance • Very Costly and Difficult to Management.	 Mesh
5)Tree Topology: •Tree Topology is combination of bus topology and star topology. •In Tree topology all the computers are connected with each other in hierarchical structure. •Support for broadband transmission. •Easily expandable and manageable. •Error detection. •Difficult troubleshooting •It is very costly •Failure in main cable will damage the overall network	 Tree
6)Hybrid Topology: •Hybrid topology is combination of two or more different topologies. •This topology is very flexible. •The size of network can be easily expanded by adding new device. •Its design is complex. •Costly hub and infrastructure.	 Hybrid

6.Define protocol. What are the key elements of a protocol. [2M]
A protocol is a set of rules which is used by computers to communicate with each other across a network.
key elements of a protocol: Syntax, Semantics, Timing.

7. Define network model. [2M]
A network model is a database model designed to represent objects and their relationships in a flexible manner.

8. Explain OSI reference model. [10M]
•The OSI (Open System Interconnection) model is a framework that explains how data travels between software applications on different computers through a physical connection.
•OSI consists of Seven layers, and each layer performs a particular network function:

1.Application Layer:
•An application layer serves as a window for users and application process to access network service.
•It handles issues such as network transparency, resource allocation, etc…

2.Presentation Layer:
•This layer is a part of OS that converts the data from one presentation format to another format.
•It acts as a data translator for a network.
•The presentation layer is also known as the syntax layer.

3. Session Layer:
•Session Layer Primarily responsible for handling the session between devices.
•The session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

4.Transport Layer:
•The main responsibility of the transport layer is transfer the data completely.
•It receives the data from the upper layer and converts them into smaller units known as segments.

5.Network Layer:
•The network layer groups the data frames into packets.
•It acts as network controller and manages the subnet traffic.
•It decides the which route data should take.

6.Data Link Layer:
•This layer is responsible for the error-free transfer of data frames.
•It defines the format of the data on the network.
•It provides an efficient communication between two or more devices.

7.Physical Layer:
•The main function of physical layer is transmit the individual bits from one device to another device.
•It is the lowest layer of the OSI model.
•It establishes, maintains and deactivates the physical connection.

9. Differentiate between OSI reference model and TCP/IP reference model.

OSI reference model	TCP/IP reference model.
OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
It has 7 layers.	It has 4 layers.
It is low in usage.	It is mostly used.
It is vertically approached.	It is horizontally approached.
Delivery of the package is guaranteed in OSI Model.	Delivery of the package is not guaranteed in TCP/IP Model.
Replacement of tools and changes can be done easily in this model.	Replacement of tools is not easy as in the OSI Model.
It is less reliable than TCP/IP Model.	It is more reliable than OSI Model.

10. Explain TCP/IP reference model.[5m/10m]

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a set of protocols that manage how data is transmitted over the internet.

TCP/IP consists 4 layers:

1. Application Layer:

•The topmost layer that interacts with end-user applications and network services.

•Application Layer contains protocols like TELNET, FTP, SMTP, HTTP etc.

2. Transport Layer:

• Manages end-to-end communication and data flow control between devices.

• This layer uses protocols like TCP and UDP to divide data into packets.

3. Internet Layer:

• Its job is inserting the packets into the subnet and allow them to travel independently.

• This layer uses the IP protocol.

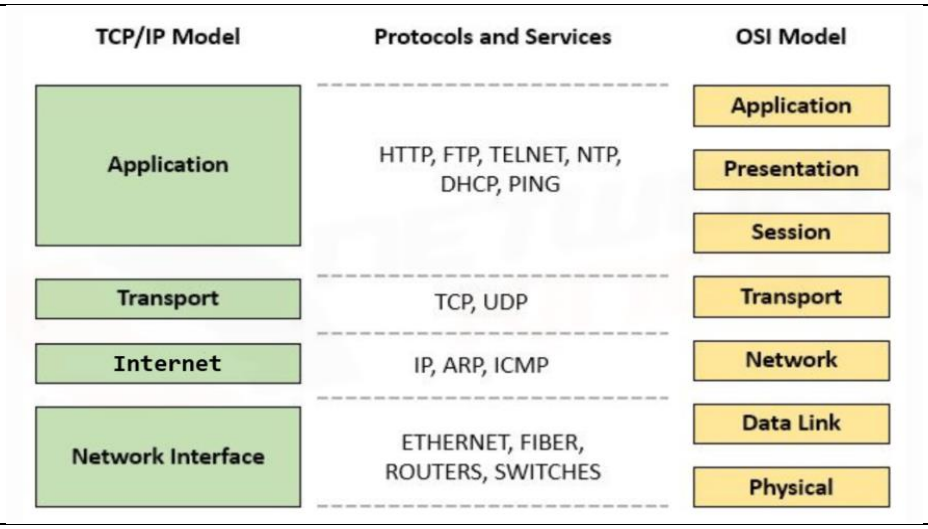
• Its job is delivering IP packets to destination.

4. Network Interface Layer:

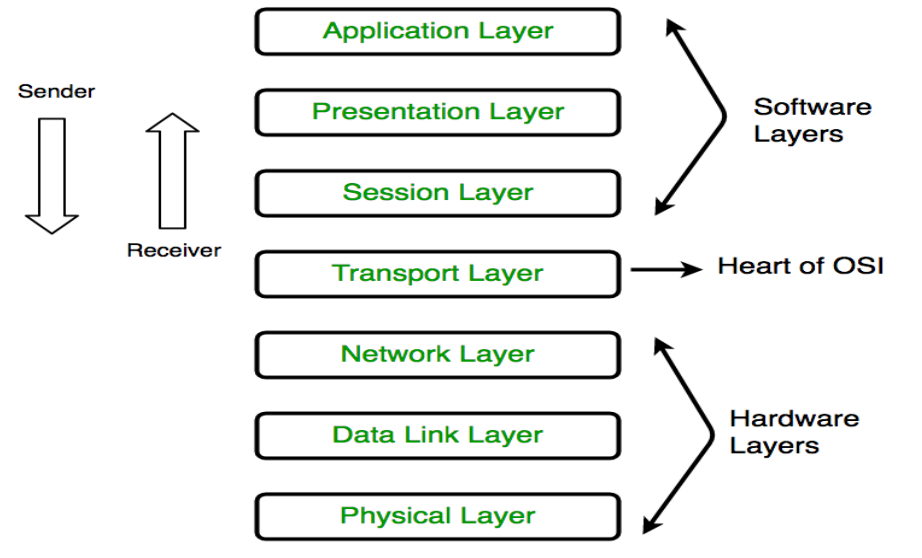
• Network layer is also called physical and data link layer.

• This layer does not define any specific protocol.

• It is responsible for accepting and transmitting IP packets.



TCP/IP Diagram
Q.no- 10 [5m/10m]



OSI Diagram
Q.no- 08 [10m]

Unit-2

1. Explain different types of guided transmission media.

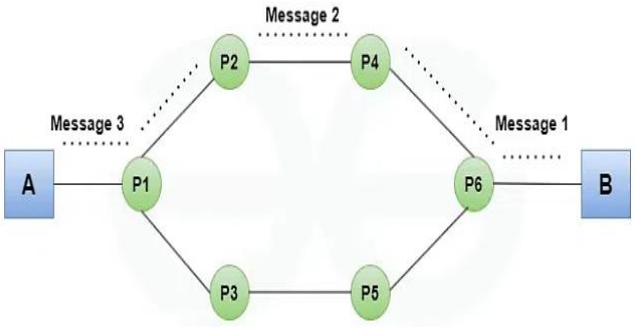
1.Twisted Pair Cable: • Twisted pair contains of two insulated copper wires twisted together • It Reduces electromagnetic interference (EMI) • It is used in telephone lines and LANs. • There are two types of twisted pair: UTP and STP • UTP (Unshielded twisted pair): It contain Two insulated copper wires twisted together. • STP (Shielded twisted pair): Same as UTP but has additional shielding to reduce electromagnetic interference.	
2.Co-axial cable: • Co-axial contains Inner copper wire surrounded by insulation, metallic shield, and outer insulating layer. • It has High bandwidth and long-distance transmission • It is used in cable TV and broadband internet • It is less expensive as compared to fibre optic cables.	
3. Fiber Optic Cable: • Fiber optic cable is made of glass or plastic and transmits signals in the form of light. • It has High-speed and long-distance transmission • Used in telecommunications and data centres • Fibre cables are more secure than other cables.	

2. Explain different types of unguided transmission media.

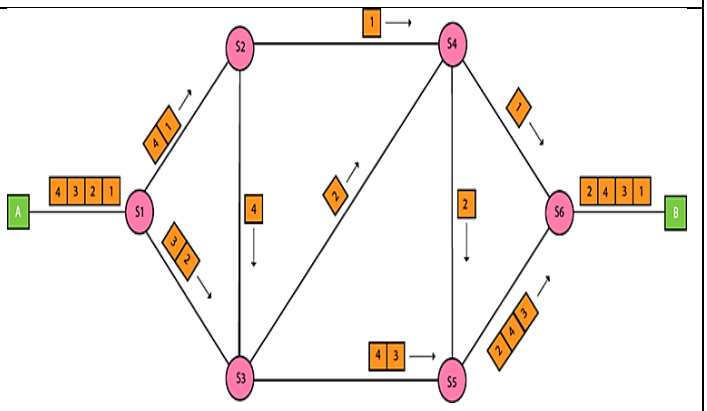
1.Radio Transmission	**2.Microwave Transmission**	**3.Infra-red Transmission**
Radio waves are the electromagnetic waves transmitted in all directions.	Microwaves are the electromagnetic waves having the frequency.	It uses infrared light to transmit signals.
These are used in long distance communication.	These are used in long distance communication.	These are used in short distance communication.
These are omni-directional in nature.	These are unidirectional in nature.	These are unidirectional in nature.
Frequency range: 3 KHz to 1GHz.	Frequency range: 1 GHz to 300 GHz.	Frequency range: 300 GHz to 400 THz.
These offers poor security.	These offers medium security.	These offers high security.
Setup and usage Cost is medium.	Setup and usage Cost is high.	Setup and usage Cost is very less.
Some frequencies in the radio-waves require government license to use these.	Some frequencies in the microwaves require government license to use these.	There is no need of government license to use these waves.

3. Define switching. Explain different types of switching techniques.
The process of moving data packets or blocks of data from one computer network to another is known as switching.

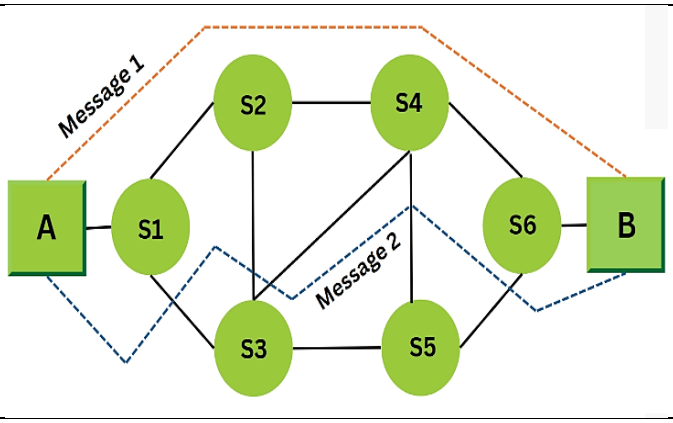
1.Circuit switching:
•Circuit switching requires a dedicated path to send data from source to destination.
•It receives the entire bandwidth in advance.
•It does not support store and forward transmission.
•Each packet follows the same route.
•Fixed data can be transferred at a time in circuit switching technology.



2. Packet switching:
• Packet switching splits a message into smaller packets that are sent individually.
• There are two methods: Datagram and Virtual Circuit.
• Each packet has a unique number.
• Packets contain information like source address, destination address, and sequence number.
• Packets travel independently, taking the shortest path available.
• At the receiving end, packets are reassembled in the correct order.
• If any packet is missing or corrupted, it is requested again.



3. Message switching:
•A complete message is passed across the network.
•In Message Switching technique, there is no dedicated path between the sender and receiver.
•Message switching treats each message as an independent entity.
•In message switching there is no limit on block size.
•Physical links are allocated dynamically.



4. Define transmission media.
Transmission media is a communication channel that carries the information from the sender to the receiver.

5. Define bandwidth.
Bandwidth measures how much data can be sent through specific connection in a given amount of time.

6. Define multiplexing and its type.
Multiplexing is a process where multiple signals are combined into one signal over a shared medium.
Types of multiplexing:
– Frequency Division Multiplexing (FDM)
– Wavelength Division Multiplexing (WDM)
– Time Division Multiplexing (TDM)
– Code Division Multiplexing (CDM)

Unit-3

1. Explain one –bit Sliding Window Protocol

•In One-bit sliding window Protocol, the Size of window is 1 (stop-and-wait protocol).
•Two-way communication: Both sender and receiver can send and receive.
•Uses 1 bit to indicate sequence numbers.
•Piggybacking Acknowledgments are included with data frames.
•Sender can send Data, Ack, and current packet sequence number.
•Both sender and receiver maintain their respective windows.

2. Explain Go Back N sliding window protocol.

•Go-Back-N Sliding window protocol using pipelining concept.
•Pipelining: Sender sends multiple frames before receiving an acknowledgment for the first one.
•The Sender can Sends multiple frames (up to N) without waiting for acknowledgment.
•The Receiver can Receives frames one by one, sends ACKs for each frame.
•Window sizes: Sender window size is N , receiver window size is 1.
•N: consider as number of frames sent before receiving acknowledgment.

3. Explain Selective repeat protocol.

• In Selective Repeat Protocol Both sender and receiver use sliding windows.
• Sender can Sends multiple frames without waiting for ACKs.
• Receiver can Receives multiple frames, buffers them, and tracks sequence numbers.
• **ACK/NACK:** Sends ACK for correctly received frames, NACK for missing/damaged frames.
• **Window sizes:** Sender window size = Receiver window size = 2^{n-1}, where **n** is the number of sequence number bits.

4. Explain Single Parity Check or Vertical Redundancy Check or One Dimension.

• Vertical Redundancy Check (VRC): Adds a parity bit to ensure even number of 1s in data.
• Even 1s: If data has even number of 1s, the parity bit is 0.
• Odd 1s: If data has odd number of 1s, the parity bit is 1.
• Receiver check: Accepts data if 1s are even, else requests retransmission.
• Error detection: Can detect single-bit errors and burst errors (if errors are odd in number).

5. Explain checksum with example. [5m/10m]

Checksum is a method used for error detection in data communication.

Sender:

- Divide data into k sections, each of n bits.
- Add all sections together.
- Complement the sum to get the checksum.
- Send the checksum with the data.

Receiver:

- Divide received data into k sections, each of n bits.
- Add all sections together.
- Complement the sum.
- If the result is zero, data is accepted.

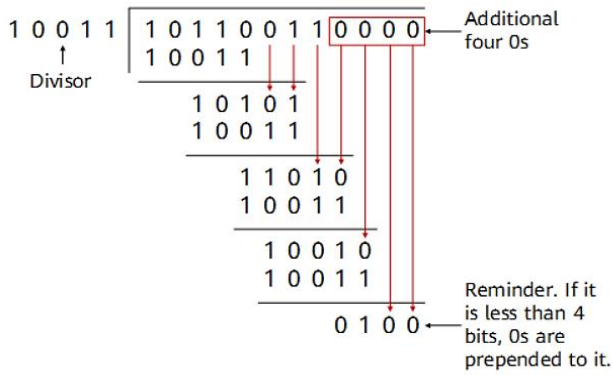
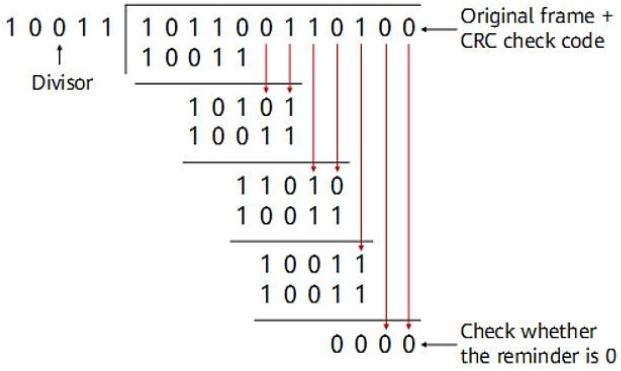
Example:

Sender Site:		**Receiver Site:**	
10101001	**subunit 1**	**10101001**	**subunit 1**
00111001	**subunit 2**	**00111001**	**subunit 2**
11100010	**sum (using 1s complement)**	**00011101**	**checksum**
00011101	**checksum (complement of sum)**	**11111111**	**sum**
		00000000	**sum's complement**
		Result is zero, it means no error.	

6. Explain CRC with example. [5m/10m]

- CRC (Cyclic Redundancy Check) is a reliable method for errors detecting.
- It uses binary division to check for errors.
- Data is divided by a preselected constant, and the remainder is the CRC value.
- The CRC remainder is appended to the data.
- The receiver divides the received data by the same constant.
- If the remainder is zero, no transmission errors occurred.

Example: Data word to be sent-10110011, key-10011

Sender side:	**Receiver side:**
	

7. Explain Hamming code correction.

- Hamming code is an error-correcting code that detects and corrects single-bit errors in digital data.
- Hamming code is an error correction system developed by R.W. Hamming.
- It can detect up to two errors and correct one single-bit error.
- The method adds redundant parity bits to the original data.
- These parity bits help detect and correct errors when the data is received.
- It is primarily designed to fix single-bit errors.

8. List the Services / functions of data link layer.

- Framing
- Error Detection
- Error Correction
- Flow control
- Physical Addressing

9.Define piggybacking.

Piggybacking is a process of attaching acknowledgment with the data packet to be sent.

10. Define error. List types of errors.

Error is a condition when the receiver's information does not match the sender's information.

Types of Error: • Single bit error • Multiple bits error • Burst error

11. Define error detection.

Error detection is the process of identifying mistakes that occur when data travels from the sender to the receiver due to noise or other issues.

12. Define error correction.

Error Correction is used to detect and correct the errors when data is transmitted from the sender to the receiver.

Unit-4

1. Explain shortest path routing algorithm with example.

Shortest Path Algorithm (Dijkstra's Algorithm):

- Used to find the shortest path between two routers in a network.
- The network is represented as a graph:
  - Nodes represent routers.
  - Edges represent communication links between routers.
- Each node is labelled with its shortest distance from the source node.
- The algorithm repeatedly updates the shortest path from the source to all other nodes.
- Example: Finding the shortest route between tolls on a road.

2. Explain Hierarchical routing.

- As networks grow, routing tables become large, consuming more memory, CPU, and bandwidth.
- Divide network into regions for efficient routing.
- Each router knows its own region.
- Router is unaware of the internal structure of other regions.
- For very large networks, more hierarchy levels may be needed (e.g., regions → clusters → zones → groups).
- Example: Hierarchical structure used in telephone networks.

3. Explain Link state routing.

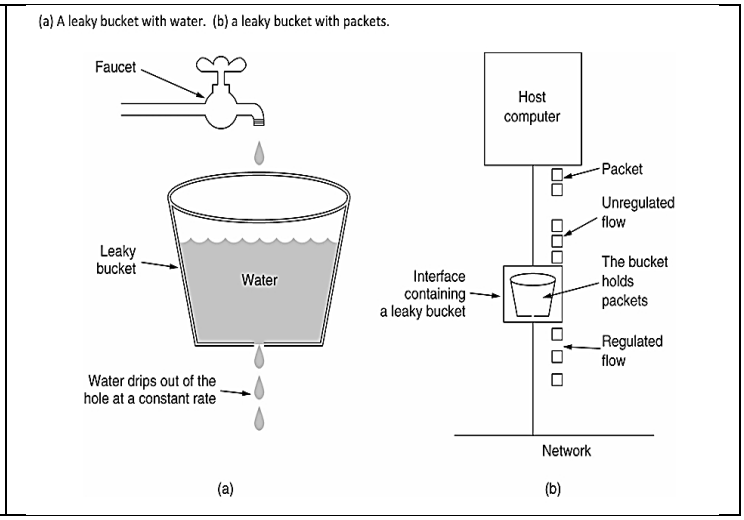
- Link-state routing allows routers to learn the entire network topology.
- Each router calculates its routing table using the shortest path algorithm.
- Key steps in link-state routing:
  1. Discover neighbouring routers and their addresses.
  2. Measure the delay or cost to each neighbour.
  3. Create a link-state packet with this information.
  4. Share the packet with all other routers.
  5. Calculate the shortest path to every other router (forming a sink tree).

4. Explain Distance vector routing.

- Distance Vector Routing is a dynamic routing algorithm.
- Based on Bellman-Ford and Ford-Fulkerson algorithms.
- Each router knows only the distance to its direct neighbours.
- Routers exchange messages with neighbours to find distances.
- Each router maintains a routing table (or vector) with:
  1. Preferred outgoing line to each destination.
  2. Estimated distance or time to each destination.
- Routers periodically update their tables (every 20 seconds).
- Distance can be measured by hops, time delay, or queue length.

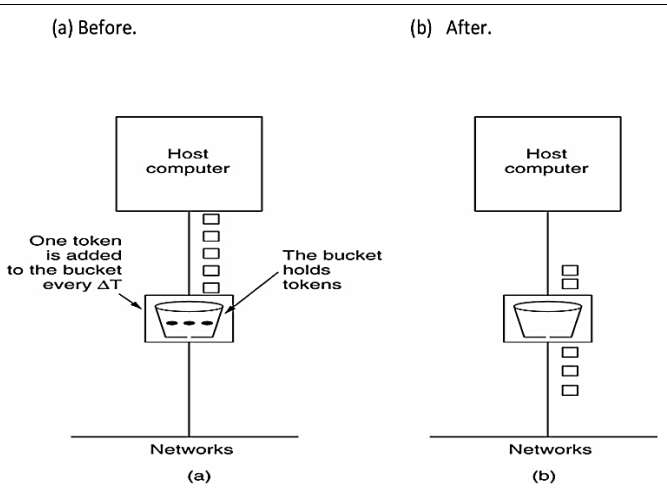
5. Explain leaky bucket traffic algorithm.

- The leaky bucket algorithm controls data flow like a bucket with a hole.
- Data is added to the bucket at a certain rate and leaks out at a fixed rate.
- If data is added too quickly, the bucket overflows and excess data is dropped.
- It limits the rate of data transmission by setting a maximum leak rate.
- Common uses:
  1. Limiting file download/ upload rates to a server.
  2. Controlling packet forwarding rates in routers.



6. Explain token bucket traffic algorithm.

• The token bucket algorithm uses tokens to control data flow.
• Tokens are added to the bucket at a specific rate.
• A sender can only transmit data if there are enough tokens available.
• If data is sent too quickly, transmission is blocked until enough tokens are available.
• Common uses:
1. Shaping traffic for real-time video streaming.
2. Managing traffic for real-time audio streaming.
3. Limiting the rate of outgoing email messages.



7. Define routing.
A Router is a process of selecting path along which the data can be transferred from source to the destination.

8. State optimality principal.

9. Define flooding.

10. Define broadcast routing.

11. Define congestion

Unit-5

1. Explain features of TCP.

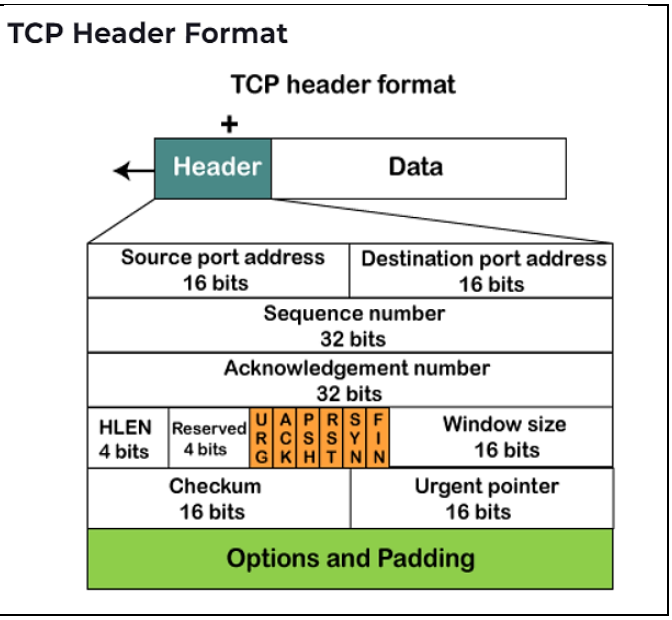
TCP is a transport-layer protocol ensuring reliable, error-free data transfer between devices.

1. Connection-Oriented: Establishes connection before data transfer.
2. Reliable Data Transfer: Ensures data delivery through acknowledgments.
3. Error Detection and Correction: Checks data integrity using checksums.
4. Sequential Data Delivery: Assembles data in original order.
5. Flow Control: Regulates data transfer rate to prevent congestion.
6. Multiplexing: Supports multiple connections over a single link.

2.Explain TCP header format.

TCP is a transport-layer protocol ensuring reliable, error-free data transfer between devices.

1.Source Port (16 bits): Port of the sender.
2.Destination Port (16 bits): Port of the receiver.
3.Sequence Number (32 bits): Keeps track of data order.
4.Acknowledgment Number (32 bits): Confirms receipt of data.
5.Data Offset (4 bits): Length of the TCP header.
6.Flags (9 bits): Controls connection (e.g., SYN, ACK, FIN).
7.Window Size (16 bits): Flow control; how much data can be received.
8. Checksum (16 bits): Error-checking for data integrity.
9. Urgent Pointer (16 bits): Marks urgent data (if URG flag is set).
10.Options: Extra options, like maximum segment size.
11.Data: The actual message or payload being sent.



3. Explain features of UDP.

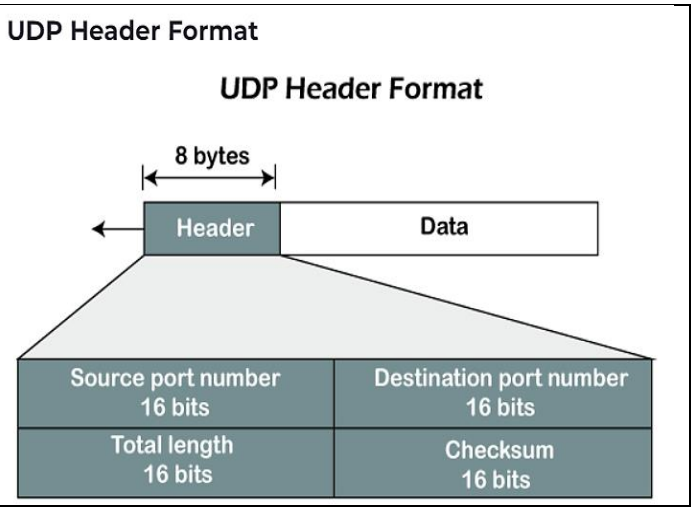
UDP (User Datagram Protocols) is internet protocol support a connectionless transport service.

1. Connectionless: No need to establish a connection before sending data.
2. Faster: No handshake or session management, so it's quicker than TCP.
3. No Retransmission: Lost packets are not resent.
4. No Error Correction: It doesn't fix errors in transmission.
5. Suitable for Real-Time: Ideal for apps like video streaming, gaming, and VoIP, where speed is more important than reliability.

4. Explain UDP frame format.

UDP (User Datagram Protocols) is internet protocol support a connectionless transport service.

1.Source Port (16 bits): Port number of the sender.
2.Destination Port (16 bits): Port number of the receiver.
3.Length (16 bits): Total length of the UDP header and data.
4.Checksum (16 bits): Used for error-checking the header and data.



5. Define Email. Explain features of email.

E-mail stands for Electronic Mail. E-mail is the electronic way of exchanging messages between the two entities.

Features of email:

1.Fast Communication: Messages are delivered almost instantly across the world.
2.Attachments: You can send files like documents, images, and videos along with the email.
3.Accessibility: Accessible from computers, smartphones, and tablets through email clients or web browsers.
4.Organized: Features like folders, labels, and search functions help organize emails.
5.Security: Supports encryption and authentication for secure communication.
6.Cost-Effective: Sending emails is typically free, requiring only internet access.

6. Explain components of email.

1.Sender: The person or entity sending the email.
2.Recipient: The person or entity receiving the email.
3.Subject: A short summary or title of the email's content.
4.Body: The main content of the email (message), which can include text, images, or links.
5.Attachments: Files like documents, images, or videos added to the email.
6.Date and Time: When the email was sent.
7.Signature: Optional text automatically added at the end
8.Email Header: Contains technical details like the sender's and recipient's email addresses, subject, date, and routing information.

7. Define WWW.

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet.

8. Define subnet.

A subnet is a smaller network within a larger network, sharing a common address space.