UNIT I

Introduction to Computer Networks: Introduction, Network Hardware, Network Software, Reference Models, Data Communication Services & Network Examples, Internet Based Applications.
Data Communications: Transmission Media, Wireless Transmission, Multiplexing, Switching, Transmission in ISDN, Broad Band ISDN, ATM Networks

UNIT II
Data Link Control, Error Detection & Correction, Sliding Window Protocols, LANs & MANs: IEEE Standards for LANs & MANs-IEEE Standards 802.2, 802.3, 802.4, 802.5, 802.6, High Speed LANs.
Design Issues in Networks: Routing Algorithms, Congestion Control Algorithms, Network Layer in the Internet, IP Protocol, IP Address, Subnets, and Internetworking.

UNIT III
Internet Transport Protocols: Transport Service, Elements of Transport Protocols, TCP and UDP Protocols, Quality of Service Model, Best Effort Model, Network Performance Issues.
Over View of DNS, SNMP, Electronic Mail, FTP, TFTP, BOOTP, HTTP Protocols, World Wide Web, Firewalls.

UNIT IV
Network Devices: Over View of Repeaters, Bridges, Routers, Gateways, Multiprotocol Routers, Brouters, Hubs, Switches, Modems, Channel Service Unit CSU, Data Service Units DSU, NIC, Wireless Access Points, Transceivers, Firewalls, Proxies.
Overview of Cellular Networks, Ad-hoc Networks, Mobile Ad-hoc Networks, Sensor Networks
ADDITIONAL INPUT:

An Introduction to Electronic Commerce: Aspects of Electronic Commerce, Types of E Commerce, Approaches for Developing E Commerce Solutions, Electronic Procurement, Phases in a Procurement

Process, E-Procurement Models, E-Procurement Solutions, Trading Models, Buyer Side Purchasing, Supply Chain Management (SCM) and Customer Relationship Management (CRM).

Text Books:
1. Computer Networks, Andrews S Tanenbaum, Edition 5, PHI, ISBN: -81-203-1165-5
2. Data Communications and Networking, Behrouz A Forouzan, Tata McGraw-Hill Co Ltd, Second Edition

Reference Books:
1. Computer networks, Mayank Dave, Cengage.
2. Computer Networks, A System Approach, 5th ed, Larry L Peterson and Bruce S Davie, Elsevier.
3. An Engineering Approach to Computer Networks-S.Keshav, 2nd Edition,Pearson Education.
4. Understanding Communications and Networks, 3rd Edition, W.A. Shay.

Introduction to computer networks

- o **Computer Network** is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.

- o The aim of the computer network is the sharing of resources among various devices.

- o In the case of computer network technology, there are several types of networks that vary from simple to complex level.

Components Of Computer Network:
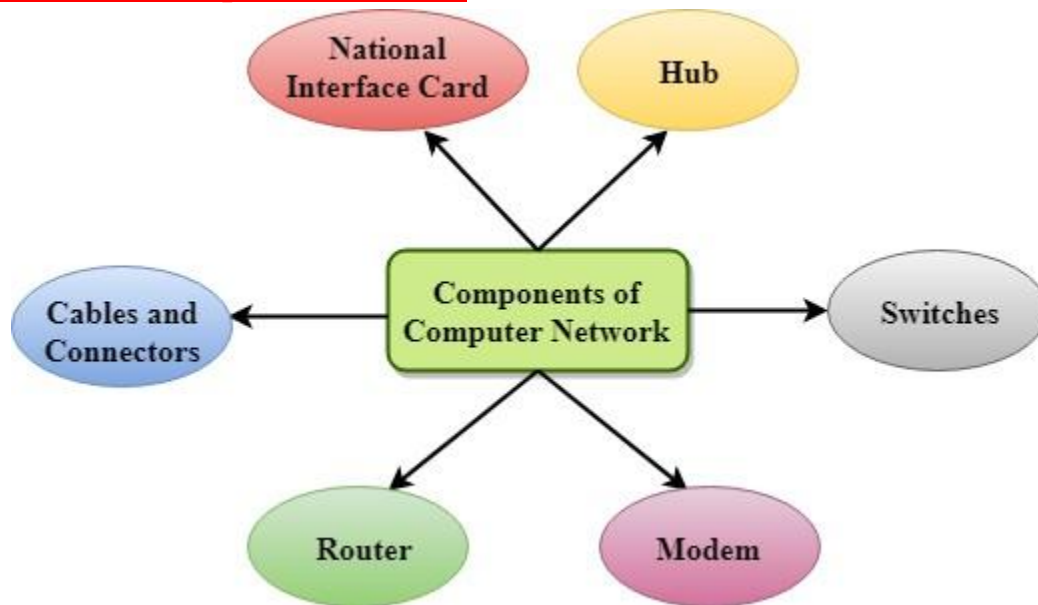
NIC(National interface card)

NIC is a device that helps the computer to communicate with another device. The network interface card contains the hardware addresses, the data-link layer protocol use this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC: wireless NIC and wired NIC.

- o **Wireless NIC:** All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the **radio wave technology**.

- o **Wired NIC:** Cables use the **wired NIC** to transfer the data over the medium.

Hub

Hub is a central device that splits the network connection into multiple devices. When computer requests for information from a computer, it sends the request to the Hub. Hub distributes this request to all the interconnected computers.

Switches

Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network, i.e., it sends the message to the device for which it belongs to. Therefore, we can say that switch sends the message directly from source to the destination.

Cables and connectors

Cable is a transmission media that transmits the communication signals. **There are three types of cables:**

- o **Twisted pair cable:** It is a high-speed cable that transmits the data over **1Gbps** or more.
- o **Coaxial cable:** Coaxial cable resembles like a TV installation cable. Coaxial cable is more expensive than twisted pair cable, but it provides the high data transmission speed.
- o **Fibre optic cable:** Fibre optic cable is a high-speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables. It is more expensive as compared to other cables, so it is installed at the government level.

Router

Router is a device that connects the LAN to the internet. The router is mainly used to connect the distinct networks or connect the internet to multiple computers.

Modem

Modem connects the computer to the internet over the existing telephone line. A modem is not integrated with the computer motherboard. A modem is a separate part on the PC slot found on the motherboard.

Uses Of Computer Network

- o **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- o **Server-Client model:** Computer networking is used in the **server-client model**. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
- o **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.

- o **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

Network Hardware:

Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:
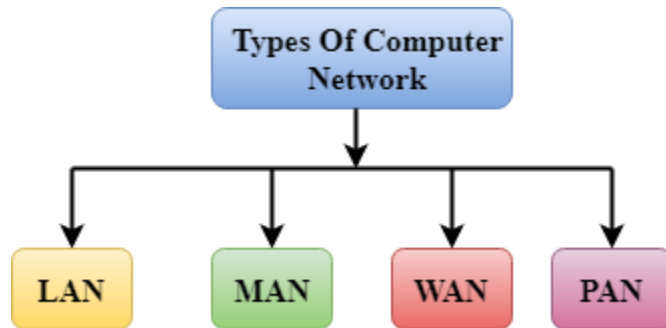
- o LAN(Local Area Network)
- o PAN(Personal Area Network)
- o MAN(Metropolitan Area Network)
- o WAN(Wide Area Network)

LAN(Local Area Network)

- o Local Area Network is a group of computers connected to each other in a small area such as building, office.
- o LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- o It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- o The data is transferred at an extremely faster rate in Local Area Network.
- o Local Area Network provides higher security.

PAN(Personal Area Network)

- o Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.

- o Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.

- o **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.

- o Personal Area Network covers an area of **30 feet**.

- o Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of Personal Area Network:
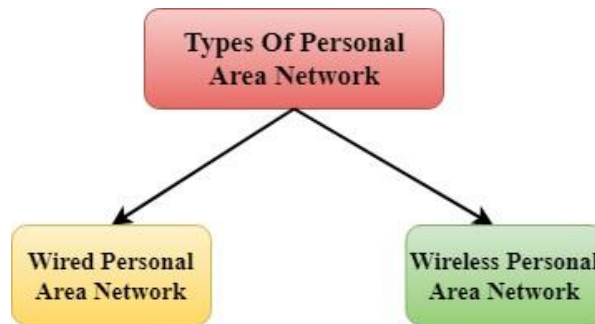
- o   Wired Personal Area Network
- o   Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

- o   **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.

- o   **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.

- o   **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN(Metropolitan Area Network)

- o   A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.

- o   Government agencies use MAN to connect to the citizens and private industries.

- o   In MAN, various LANs are connected to each other through a telephone exchange line.

- o   The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.

- o   It has a higher range than Local Area Network(LAN).
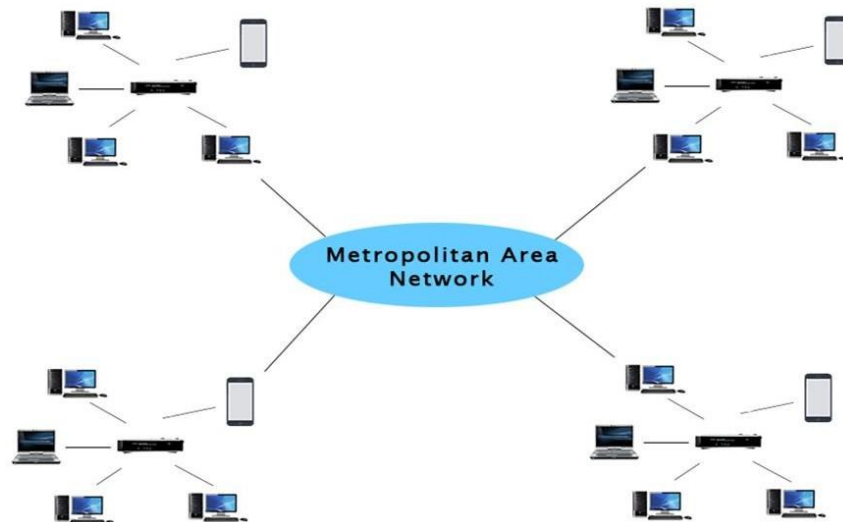
Uses Of Metropolitan Area Network:

- o MAN is used in communication between the banks in a city.

- o It can be used in an Airline Reservation.

- o It can be used in a college within a city.

- o It can also be used for communication in the military.

WAN(Wide Area Network)

- o A Wide Area Network is a network that extends over a large geographical area such as states or countries.

- o A Wide Area Network is quite bigger network than the LAN.

- o A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.

- o The internet is one of the biggest WAN in the world.

- o A Wide Area Network is widely used in the field of Business, government, and education.
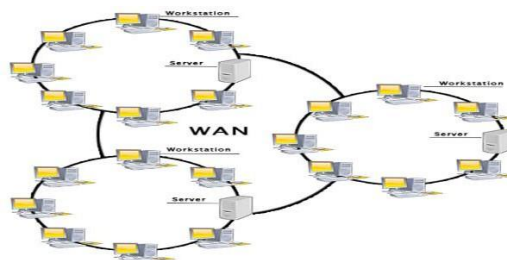
Examples Of Wide Area Network:

- o **Mobile Broadband:** A 4G network is widely used across a region or country.

- o **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.

- o **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- o **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.

- o **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.

- o **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.

- o **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.

- o **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.

- o **Global business:** We can do the business over the internet globally.

- o **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- o **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.

- o **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.

- o **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.

- o **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internetwork

- o An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.

- o An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.

- o An internetworking uses the **internet protocol**.

- o The reference model used for internetworking is **Open System Interconnection(OSI)**.

Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

- o **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.

- o **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.

o **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.

o **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.

o **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

Network software

The first computer designed with the hardware as the major concern and the software as an afterthought. This no longer works. Network software is now highly structured.

- Protocol Hierarchies
- Design Issues for the Layers
- Connection-Oriented and Connectionless Services
- Service Primitives
- The Relationship of Services to Protocol

Protocol Hierarchies

- To reduce the design complexity, most networks are organized as a series of layers or levels. Each one built upon the one below it.
- The number of layers, name of each layer, contents of each layer and the function of each layer differ from network to network
- Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the layer n protocol
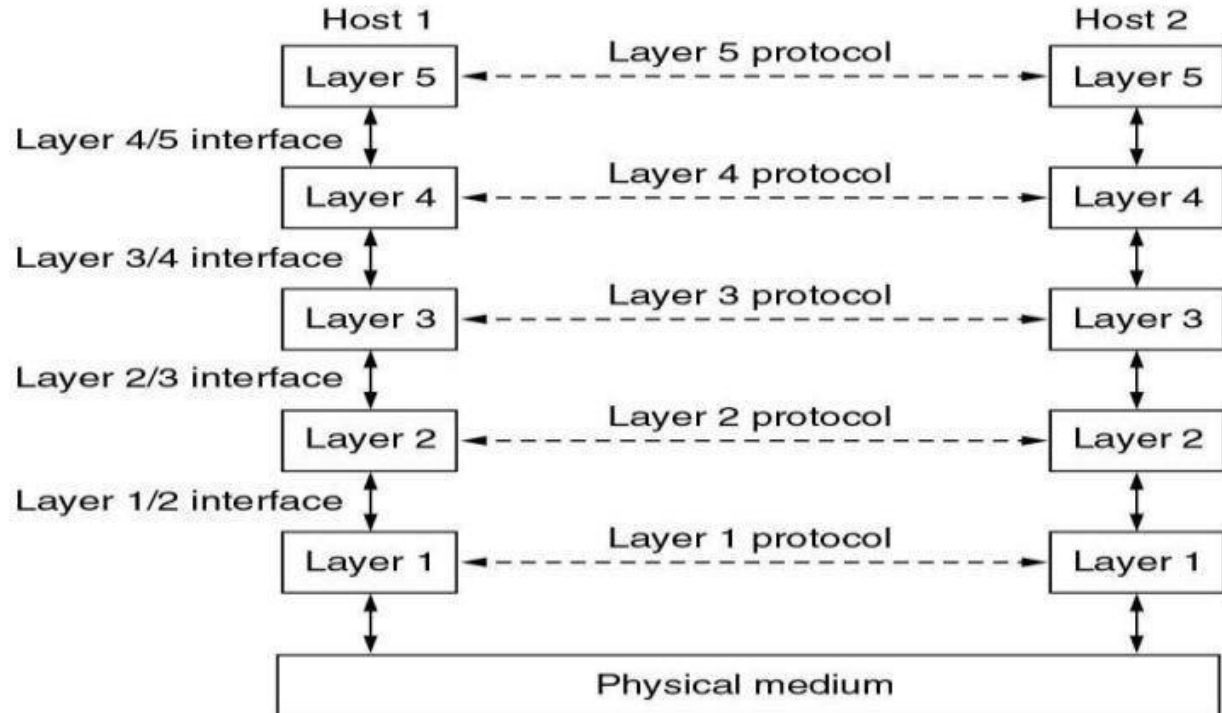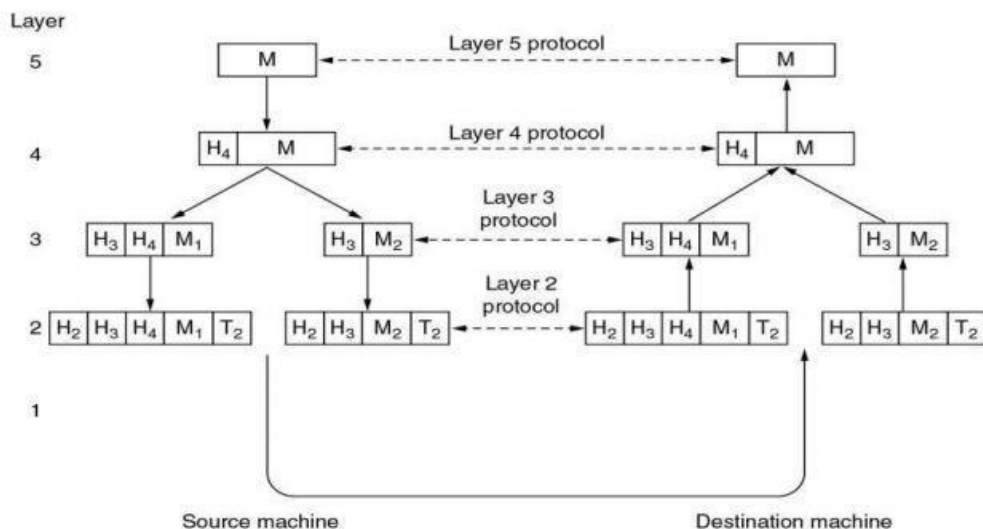
Protocol Hierarchies

- Between each pair of adjacent layers there is an interface
- A set of layers and protocols is called a network architecture.
- A list of protocols used by a certain system , one protocol per layer, is called a protocol stack

Protocol Hierarchies (2)
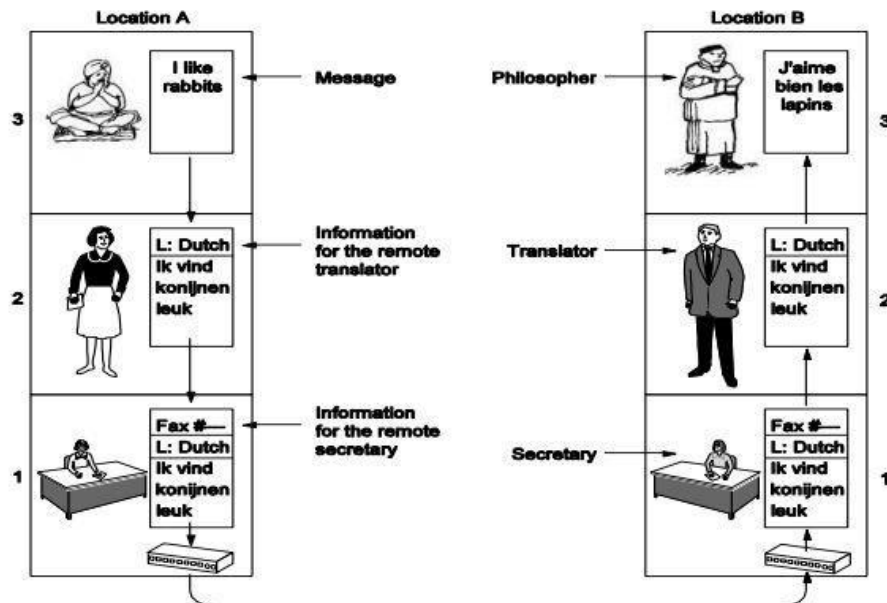
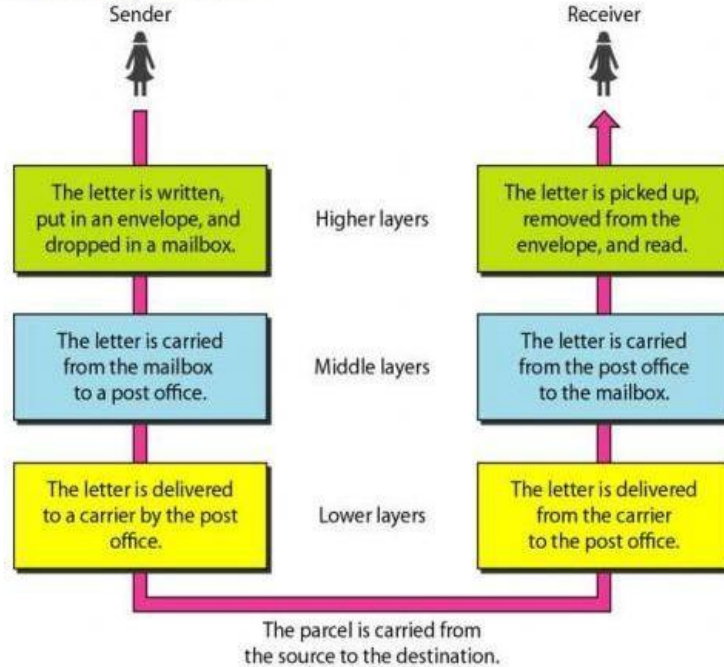

- The philosopher-translator-secretary architecture.

Protocol Hierarchies (3)

- Example information flow supporting virtual communication in layer 5.

Tasks involved in sending a letter

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail.

Sender

The letter is written, put in an envelope, and dropped in a mailbox.	Higher layers
The letter is carried from the mailbox to a post office.	Middle layers
The letter is delivered to a carrier by the post office.	Lower layers

Receiver

The letter is picked up, removed from the envelope, and read.	
The letter is carried from the post office to the mailbox.	
The letter is delivered from the carrier to the post office.	

The parcel is carried from the source to the destination.

Design Issues for the Layers

• Addressing – each layer needs a mechanism for identifying senders and receivers.

• The rules of data transfer – simplex, half-duplex, fullduplex

 • Error Control – error-correction and error-detection

• Flow Control - The communication channels must preserve the order of messages sent on them – disassembling, transmitting, and then reassembling

. • Multiplexing – inconvenient or expensive to set up a connection for each pair of communication process.

 • Routing – multiple paths between source and destination , a route must be chosen

Connection-Oriented and Connectionless Services

 • Connection-oriented is modeled after the telephone system.

 • To talk to someone, you pick up the phone, dial the number, talk, and then hang up

 . • To use a connection-oriented network service, the service user first establish a connection, uses the connection, and then releases the connection

. • Connectionless service is modeled after postal system.

 • Each message carries the full destination address, and each one routed through the system independent of all the routers.

• When two messages sent to the same destination, the first one sent will be first one to arrive. If first one is delayed the second one arrives first. • With connection-oriented service this is not possible.

Service Primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

• Five service primitives for implementing a simple connection-oriented service

Services to Protocols Relationship

• The relationship between a service and a protocol.

 • A service is a set of primitives(operations)that a layer provides to the layer above it

 • A protocol is a set of rules governing the format and meaning of the frames, packets, or messages that are exchanged by the peer entities within the layer
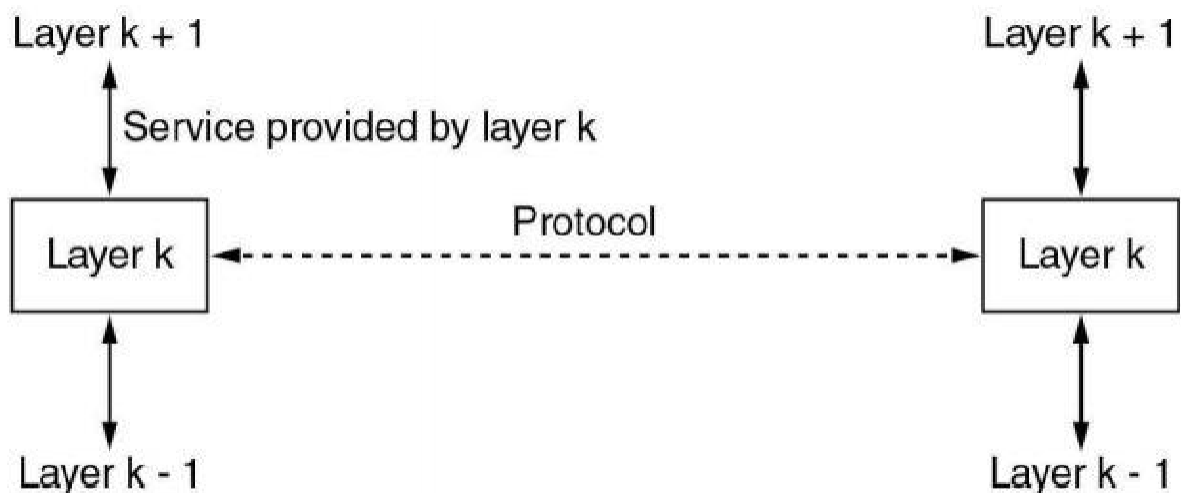
Reference Models

OSI Model

1. OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

2. OSI consists of seven layers, and each layer performs a particular network function.

3. OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.

4. OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

5. Each layer is self-contained, so that task assigned to each layer can be performed independently.
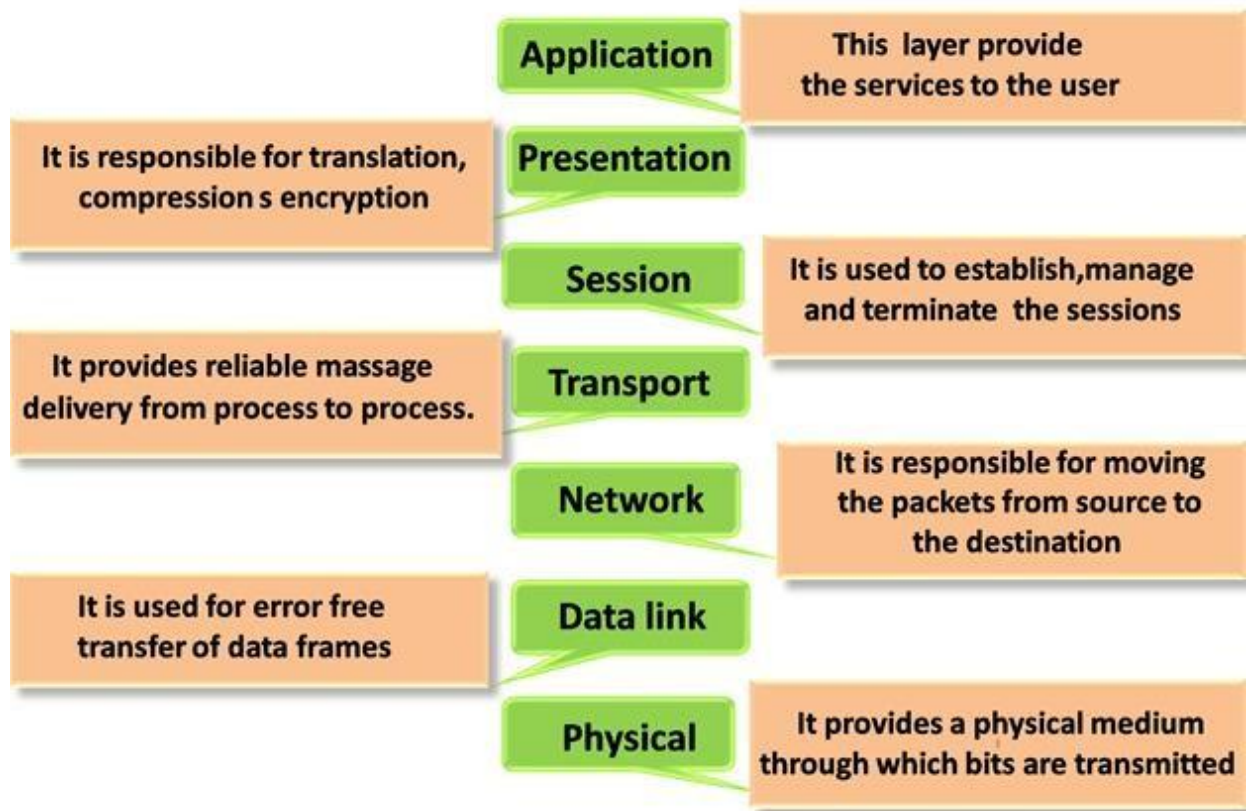
Characteristics of OSI Model:
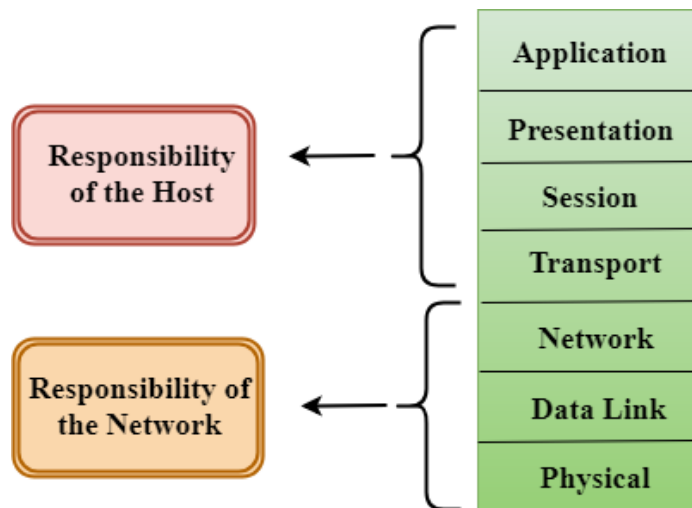
o The OSI model is divided into two layers: upper layers and lower layers.

o The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

o The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is

the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.
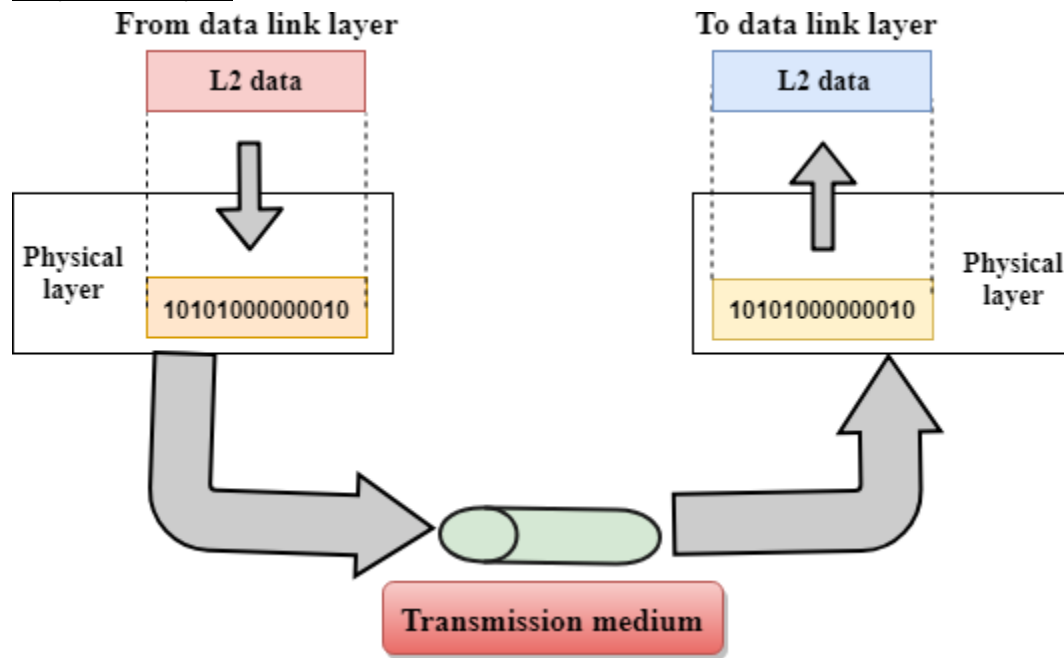
Functions of the OSI Layers

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer

2. Data-Link Layer

3. Network Layer

4. Transport Layer

5. Session Layer

6. Presentation Layer

7. Application Layer

Application — This layer provide the services to the user

It is responsible for translation, compression s encryption — **Presentation**

Session — It is used to establish, manage and terminate the sessions

It provides reliable massage delivery from process to process. — **Transport**

Network — It is responsible for moving the packets from source to the destination

It is used for error free transfer of data frames — **Data link**

Physical — It provides a physical medium through which bits are transmitted

Physical layer

- ○ The main functionality of the physical layer is to transmit the individual bits from one node to another node.

- ○ It is the lowest layer of the OSI model.

- ○ It establishes, maintains and deactivates the physical connection.

- ○ It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- ○ **Line Configuration:** It defines the way how two or more devices can be connected physically.

- ○ **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.

- ○ **Topology:** It defines the way how network devices are arranged.

- ○ **Signals:** It determines the type of the signal used for transmitting the information.
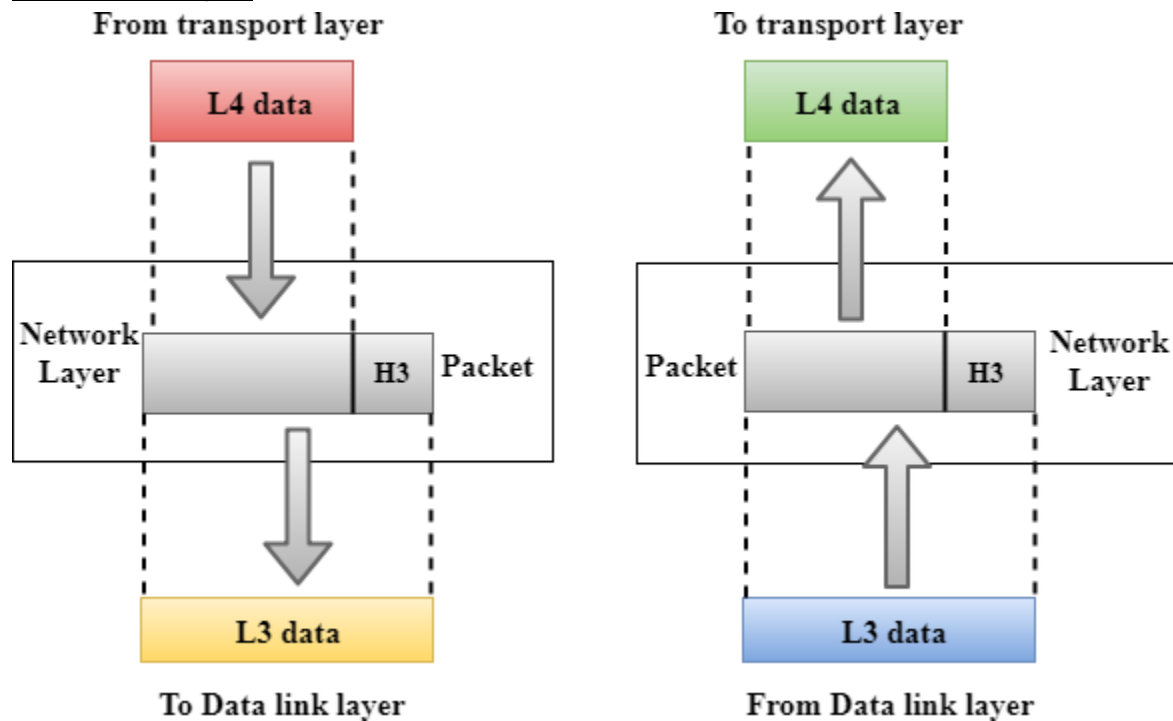
Data-Link Layer
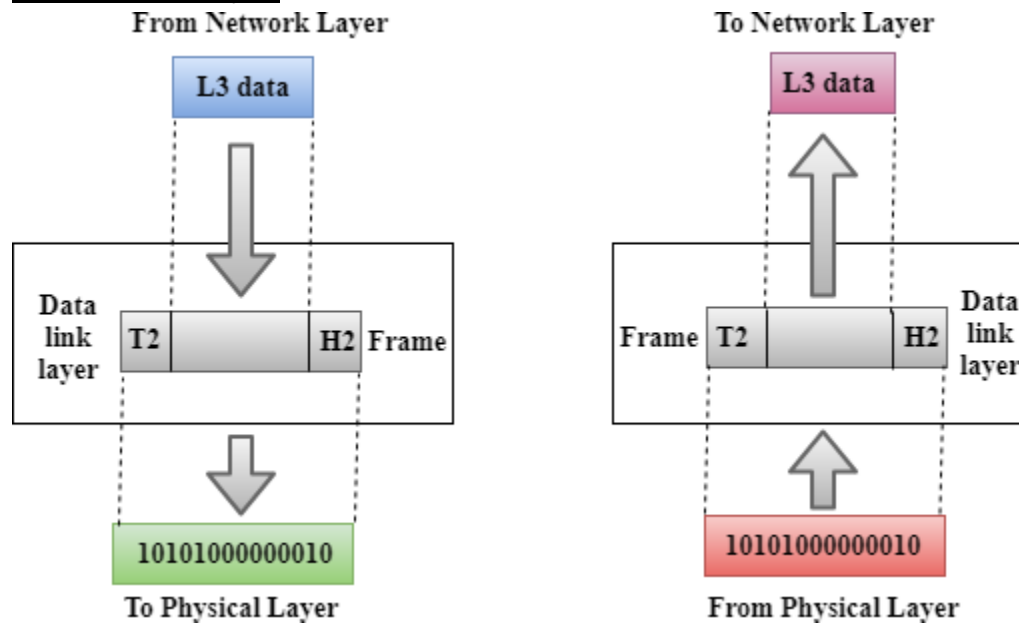
- o This layer is responsible for the error-free transfer of data frames.
- o It defines the format of the data on the network.
- o It provides a reliable and efficient communication between two or more devices.
- o It is mainly responsible for the unique identification of each device that resides on a local network.
- o It contains two sub-layers:
    - o **Logical Link Control Layer**
        - o It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - o It identifies the address of the network layer protocol from the header.
        - o It also provides flow control.
    - o **Media Access Control Layer**
        - o A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
        - o It is used for transferring the packets over the network.

Functions of the Data-link layer

- o **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

Header	Packet	Trailer

- o **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.

- o **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.

- o **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.

- o **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer

From transport layer

| L4 data |

Network Layer

| | H3 | Packet |

To Data link layer

| L3 data |

To transport layer

| L4 data |

| Packet | | H3 |

Network Layer

From Data link layer

| L3 data |

- o It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- o It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- o The Data link layer is responsible for routing and forwarding the packets.
- o Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- o The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- o **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- o **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- o **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

- o **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer
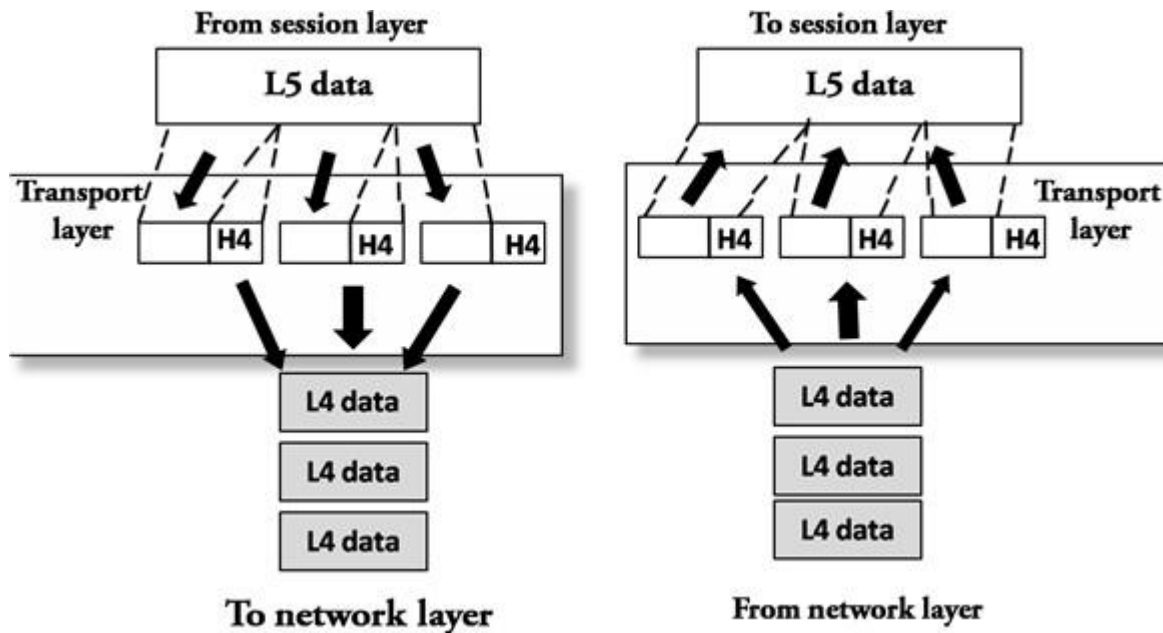
- o The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- o The main responsibility of the transport layer is to transfer the data completely.
- o It receives the data from the upper layer and converts them into smaller units known as segments.
- o This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- o **Transmission Control Protocol**
    - o It is a standard protocol that allows the systems to communicate over the internet.
    - o It establishes and maintains a connection between hosts.
    - o When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet

using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

- **User Datagram Protocol**
    - User Datagram Protocol is a transport layer protocol.
    - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer
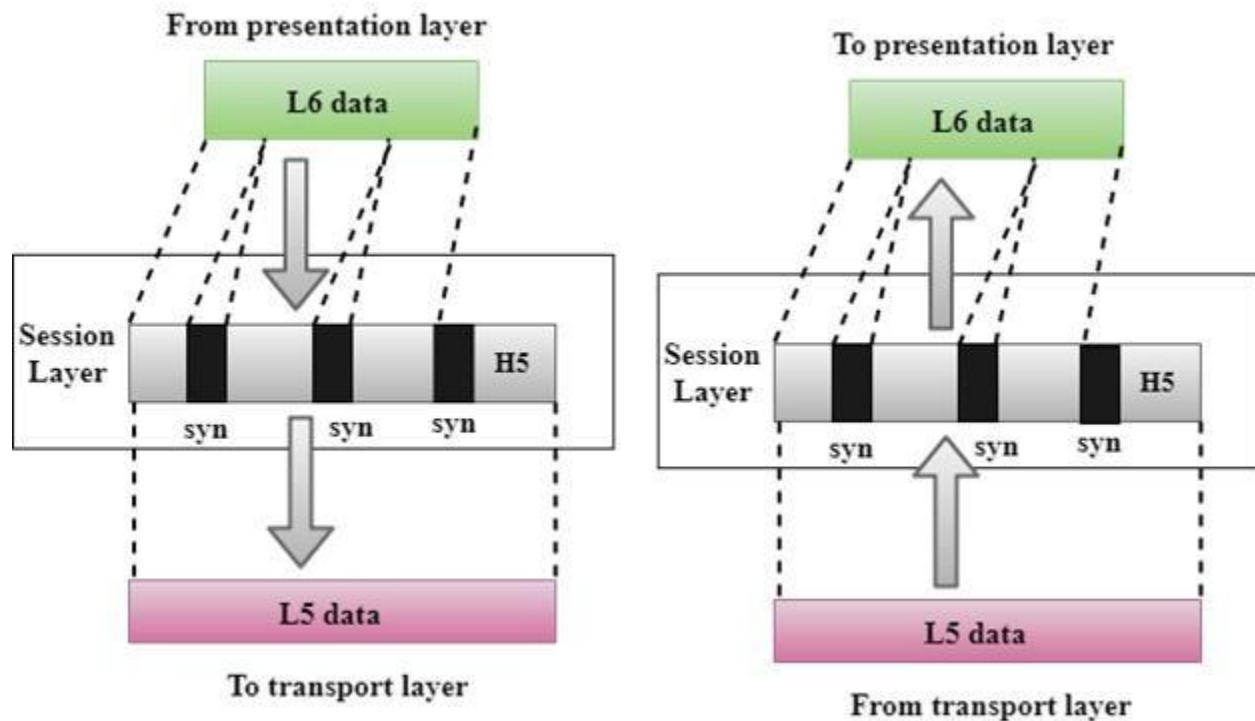
o It is a layer 3 in the OSI model.

o The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

o **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

o **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer
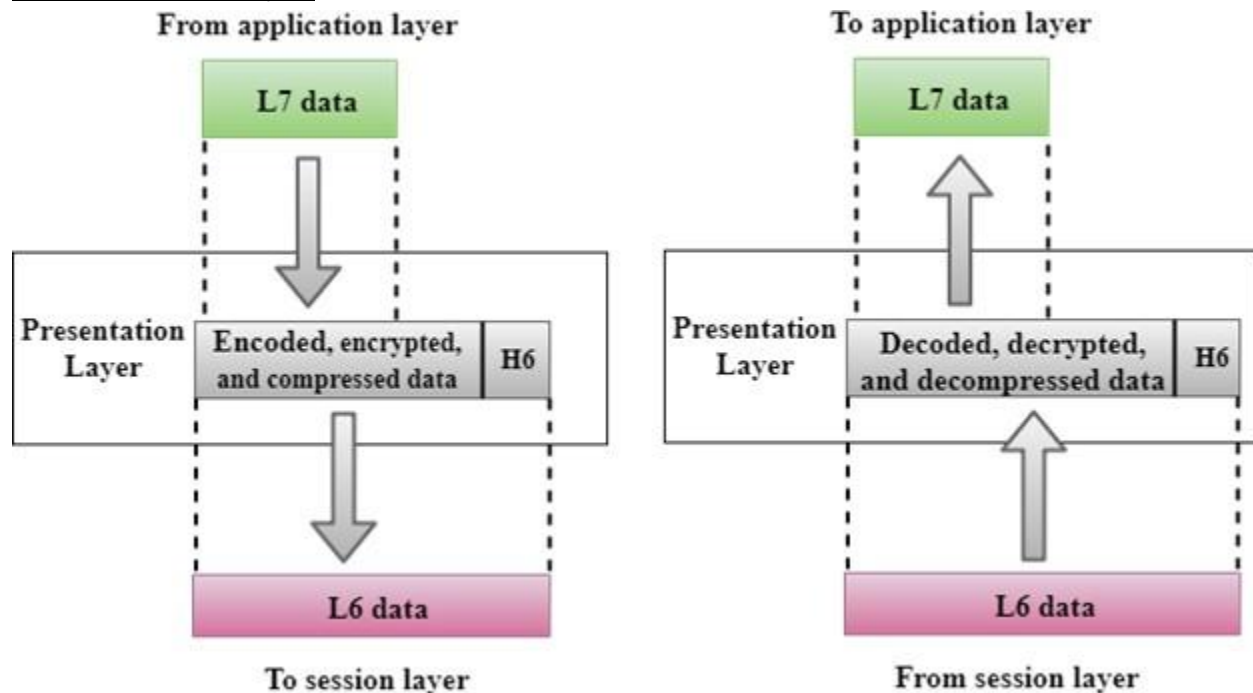
- o A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- o It acts as a data translator for a network.
- o This layer is a part of the operating system that converts the data from one presentation format to another format.
- o The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- o **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

- o **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

- o **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer
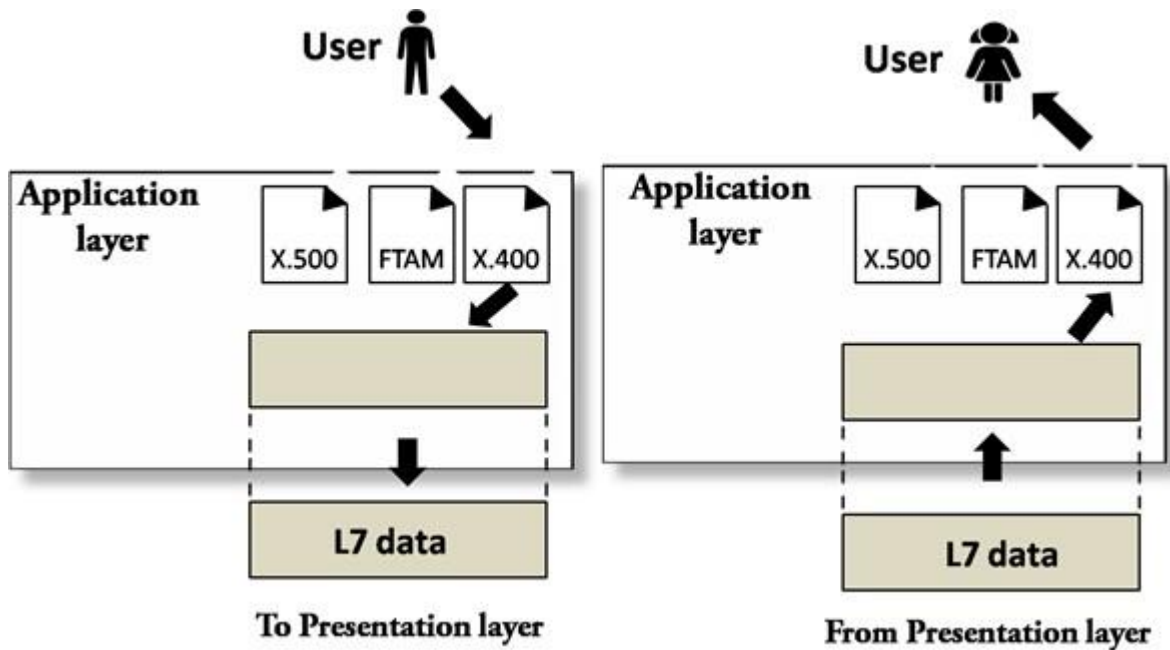
- o An application layer serves as a window for users and application processes to access network service.
- o It handles issues such as network transparency, resource allocation, etc.
- o An application layer is not an application, but it performs the application layer functions.
- o This layer provides the network services to the end-users.

Functions of Application layer:

- o **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.

- o **Mail services:** An application layer provides the facility for email forwarding and storage.

o Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

TCP/IP model

o The TCP/IP model was developed prior to the OSI model.

o The TCP/IP model is not exactly similar to the OSI model.

o The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.

o The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

o TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:
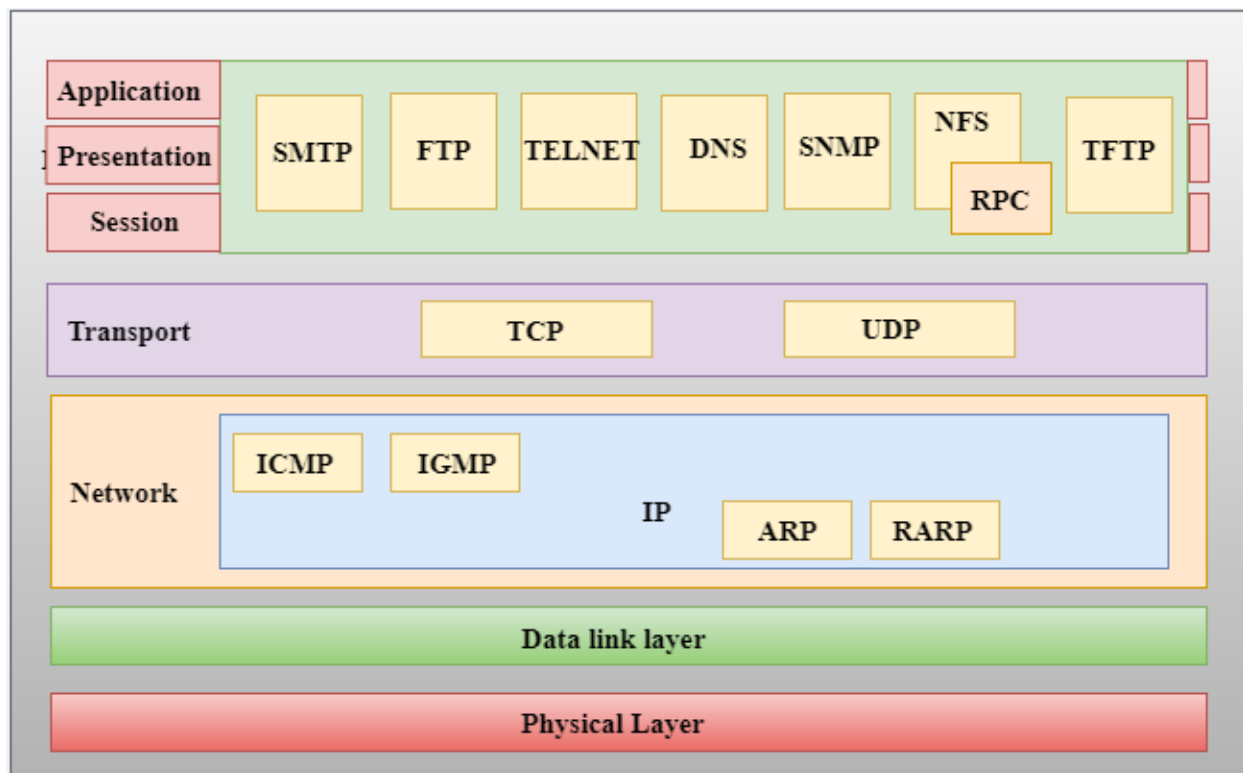
Network Access Layer

- o A network layer is the lowest layer of the TCP/IP model.

- o A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.

- o It defines how the data should be sent physically through the network.

- o This layer is mainly responsible for the transmission of the data between two devices on the same network.

- o The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

- o The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

nternet Layer

- o An internet layer is the second layer of the TCP/IP model.

- o An internet layer is also known as the network layer.

- o The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- o **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.

- o **Host-to-host communication:** It determines the path through which the data is to be transmitted.

- o **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

- o **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into

smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.

o **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

o ARP stands for **Address Resolution Protocol**.

o ARP is a network layer protocol which is used to find the physical address from the IP address.

o **The two terms are mainly associated with the ARP Protocol:**

    o **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

    o **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

o **ICMP** stands for Internet Control Message Protocol.

o It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.

o A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

o An ICMP protocol mainly uses two terms:

    o **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.

    o **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.

- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.

- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

- **User Datagram Protocol (UDP)**

    - It provides connectionless service and end-to-end delivery of transmission.

    - It is an unreliable protocol as it discovers the errors but not specify the error.

    - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

    - **UDP consists of the following fields:**
      Source port address: The source port address is the address of the application program that has created the message.
      Destination port address: The destination port address is the address of the application program that receives the message.
      Total length: It defines the total number of bytes of the user datagram in bytes.
      Checksum: The checksum is a 16-bit field used in error detection.

    - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

Variable

8 bytes

Header	Data
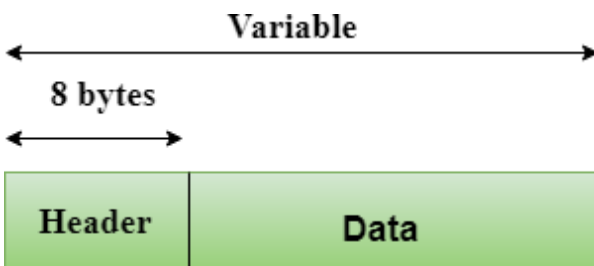
Header Format

Source port address 16 bits	Destination port address 16 bits
Total length 16 bits	Checksum 16 bits

- **Transmission Control Protocol (TCP)**
  - It provides a full transport layer services to applications.
  - It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  - TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- o **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

- o **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

- o **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

- o **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

- o **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

- o **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

DATA COMMUNICATION SERVICES

The following are some of the data communication services SMDS, X.25, frame relay, and broadband ISDN.

A switched multimegabit data service (SMDS) is a connectionless telecommunications service allowing organizations to exchange large amounts of data over a wide area network (WAN) on a non-constant or burst basis.

SMDS is usually provided by telephone companies as a value-added service. SMDS extends the abilities of an organization's local area network (LAN) over a wide area on an as-needed basis.

If a regional office of a commercial bank only needs to send data once a day to the central headquarters, there is no need to have a dedicated wide area network (WAN) connection, which will be idle most of the day.

SMDS offers a solution through use of public telecommunications facilities to periodically send a burst of data, but only when and as needed.

To see a situation in which SMDS would be useful, consider a company with four offices in four different cities, each with its own LAN. The company would like to connect all the LANs, so that packets can go from one LAN to another. One solution would be to lease six high-speed lines and fully connect the LANs as shown in Fig. l-27(a). Such a solution is certainly possible, but expensive.
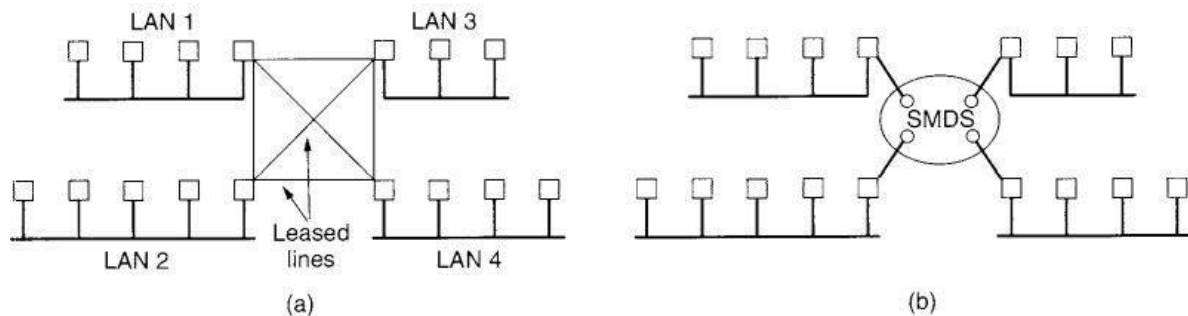
Fig. 1-27. (a) Four LANs interconnected with leased lines. (b) Interconnection using SMDS.

An alternative solution is to use SMDS, as shown in Fig. l-27(b). The SMDS network acts like a high-speed LAN backbone, allowing packets from any LAN to follow to any other LAN. Between the LANs, in the customer's offices, and the SMDS network, in the telephone company's offices, is a (short) access line leased from the telephone company. Usually, this line is a MAN and uses DQDB, but other options may also be available.

The basic SMDS service is a simple connectionless packet delivery service. The packet format is shown in Fig. 1-28. It has three fields: the destination (where the packet is to go to), the source (who sent it), and a variable length payload field for up to 9188 bytes of user data. The machine on the sending LAN that is connected to the access line puts the packet on the access line, and SMDS makes a best effort attempt to deliver it to the correct destination. No guarantee is given.

Fig. 1-28. The SMDS packet format.

X.25 Network:-

X.25 is the name given to a suite of protocols used for packet-switched wide area network communication. Defined by the International Telegraph and Telephone Consultative Committee in 1976, X.25 had the original purpose of carrying voice signals over analog telephone lines.

X.25 is the oldest packet-switching technique available and was commonly used before the Open System Interconnection (OSI) reference model became standard. Originally developed for use in the 1970s and used widely in the 1980s, X.25 has since fallen out of favor, having been replaced by less complex protocols such as Internet Protocol. Today, it is mostly relegated to ATMs and credit card verification networks. X.25 protocols work at the physical, data link and network layers of the network. Each X.25 packet contains 128 bytes of data. The protocols themselves cover such tasks as packet assembly at the source, delivery, disassembly at destination, error-checking and retransmission in case of errors.

X.25 has Three Protocol Layers:-

1. Physical Layer: It lays out the physical, electrical and functional characteristics that interface between the computer terminal and the link to the packet switched node. X.21 physical implementer is commonly used for the linking.

2. Data Link Layer: It comprises the link access procedures for exchanging data over the link. Here, control information for transmission over the link is attached to the packets from the packet layer to form the LAPB frame (Link Access Procedure Balanced). This service ensures a bit-oriented, error-free, and ordered delivery of frames.

3. Packet Layer: This layer defines the format of data packets and the procedures for control and transmission of the data packets. It provides external virtual circuit service. Virtual circuits may be of two types: virtual call and permanent virtual circuit. The virtual call is established dynamically when needed through call set up procedure, and the circuit is relinquished through call clearing procedure. Permanent virtual circuit, on the other hand, is fixed and network assigned.

Frame Relay:-

Frame Relay is a virtual-circuit wide-area network that was designed in response to demands for a new type of WAN in the late 1980s and early 1990s. ϖ Prior to Frame Relay, some organizations were using a virtual-circuit switching network called X.25 that performed switching at the network layer. For example, the Internet, which needs wide-area networks to carry its packets from one place to another, used X.25. And X.25 is still being used by the Internet, but it is being replaced by other WANs. However, X.25 has several drawbacks:

X.25 has a low 64-kbps data rate. By the 1990s, there was a need for higher data- rate WANs.

• X.25 has extensive flow and error control at both the data link layer and the network layer. This was so because X.25 was designed in the 1970s, when the available transmission media were more prone to errors. Flow and error control at both layers create a large overhead and slow down transmissions. X.25 requires acknowledgments for both data link layer frames and network layer packets that are sent between nodes and between source and destination.

• Originally X.25 was designed for private lise, not for the Internet. X.25 has its own network layer. This means that the user's data are encapsulated in the network layer packets of X.25. The Internet, however, has its own network layer, which means if the Internet wants to use X.25, the Internet must deliver its network layer packet, called a datagram, to X.25 for encapsulation in the X.25 packet. This doubles the overhead

Disappointed with X.25, some organizations started their own private WAN by leasing T-l or T-3 lines from public service providers. This approach also has some drawbacks.

• If an organization has n branches spread over an area, it needs n(n - 1)/2 T-I or T-3 lines. The organization pays for all these lines although it may use the lines only 10 percent of the time. This can be very costly.

• The services provided by T-I and T-3 lines assume that the user has fixedrate data all the time. For example, a T-l line is designed for a user who wants to use the line at a consistent 1.544 Mbps. This type of service is not suitable for the many users today that need to send bursty data.

In response to the above drawbacks, Frame Relay was designed. Frame Relay is a wide area network with the following features:

• Frame Relay operates at a higher speed (1.544 Mbps and recently 44.376 Mbps). This means that it can easily be used instead of a mesh of T-I or T-3 lines.

• Frame Relay operates in just the physical and data link layers. This means it can easily be used as a backbone network to provide services to protocols that already have a network layer protocol, such as the Internet.

Frame Relay allows bursty data.

• Frame Relay allows a frame size of 9000 bytes, which can accommodate all local area network frame sizes.

• Frame Relay is less expensive than other traditional WANs.

• Frame Relay has error detection at the data link layer only. There is no flow control or error control. There is not even a retransmission policy if a frame is damaged; it is silently dropped. Frame Relay was designed in this way to provide fast transmission capability for more reliable media and for those protocols that have flow and error control at the higher layers

Architecture:-

Frame Relay provides permanent virtual circuits and switched virtual circuits. Figure shows an example of a Frame Relay network connected to the Internet. The routers are used, as we will see, to connect LANs and WANs in the Internet. In the figure, the Frame Relay WAN is used as one link in the global Internet.
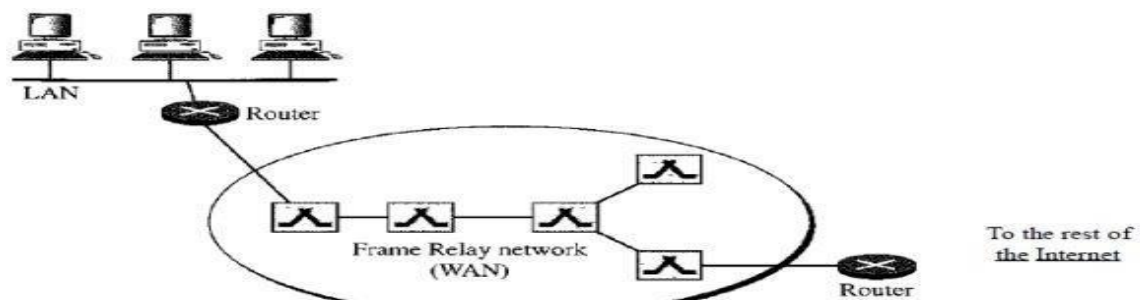

Fig: Frame Relay Network

NETWORK EXAMPLES

Numerous networks are currently operating around the world. Some of these arc public networks run by common carriers or PTTs. others are research networks, yet others arc cooperative networks run by their users, and still others are commercial or corporate networks.

These are the popular commercial LAN networking package, Novell NetWare®, the worldwide Internet (including its predecessors, the ARPANET and NSFNET), and the first gigabit networks.

ARPANET stands for **Advanced Research Projects Agency NET**. ARPANET was first network which consisted of distributed control. It was first to implement TCP/IP protocols. It was basically beginning of Internet with use of these technologies. It was designed with a basic idea in mind that was to communicate with scientific users among an institute or university.

History of ARPANET :
ARPANET was introduced in the year 1969 by Advanced Research Projects Agency (ARPA) of US Department of Defense. It was established using a bunch of PCs at various colleges and sharing of information and messages was done. It was for playing as long separation diversions and individuals were asked to share their perspectives. In the year 1980, ARPANET was handed over to different military network, Defense Data Network.

Characteristics of ARPANET :
1. It is basically a type of WAN.
2. It used concept of Packet Switching Network.
3. It used Interface Message Processors(IMPs) for sub-netting.
4. ARPANETs software was split into two parts- a host and a subnet.

Advantages of ARPANET :
- ARPANET was designed to service even in a Nuclear Attack.
- It was used for collaborations through E-mails.
- It created an advancement in transfer of important files and data of defense.

Limitations of ARPANET :
- Increased number of LAN connections resulted in difficulty handling.
- It was unable to cope-up with advancement in technology.

The internet
The number of networks, machines, and users connected to the ARPANET grew rapidly after TCPIIP became the only official protocol on Jan. I, 1983. When NSFNET and the ARPANET were interconnected, the growth became exponential. Many regional networks joined up, and connections were made to networks in Canada, Europe, and the Pacific.

What does it actually mean to be on the Internet? Our definition is that a machine is on the Internet if it runs the TCP/IP protocol stack, has an IP address, and has the ability to send IP packets to all the other machines on the Internet. The mere ability to send and receive electronic

mail is not enough, since email is gatewayed to many networks outside the Internet. However, the issue is clouded somewhat by the fact that many personal computers have the ability to call up an Internet service provider using a modem, be assigned a temporary IP address, and send IP packets to other Internet hosts. It make sense to regard such machines as being on the Internet for as long as they are connected to the service provider's router.

Internet

Internet is defined as an Information super Highway, to access information over the web. However, It can be defined in many ways as follows:

- Internet is a world-wide global system of interconnected computer networks.

- Internet uses the standard Internet Protocol (TCP/IP).

- Every computer in internet is identified by a unique IP address.

- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.

- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.

- For example, a DNS server will resolve a name **http://www.DNRCOLLEGE.com** to a particular IP address to uniquely identify the computer on which this website is hosted.

- Internet is accessible to every user all over the world.

Advantages

Internet covers almost every aspect of life, one can think of. Here, we will discuss some of the advantages of Internet:

- Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the wed that uses Internet as a medium for communication. One can find various social networking sites such as:

  - Facebook
  - Twitter
  - Yahoo
  - Google+
  - Flickr
  - Orkut

- One can surf for any kind of information over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a search engine.

- Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.

- o Online Television
- o Online Games
- o Songs
- o Videos
- o Social Networking Apps
- Internet allows us to use many services like:
  - o Internet Banking
  - o Matrimonial Services
  - o Online Shopping
  - o Online Ticket Booking
  - o Online Bill Payment
  - o Data Sharing
  - o E-mail
- Internet provides concept of **electronic commerce**, that allows the business deals to be conducted on electronic systems

Disadvantages

However, Internet has prooved to be a powerful source of information in almost every field, yet there exists many disadvanatges discussed below:

- There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while sharing such information. One should use credit cards only through authenticated sites.
- Another disadvantage is the **Spamming**.Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of entire system.
- **Virus** can easily be spread to the computers connected to internet. Such virus attacks may cause your system to crash or your important data may get deleted.
- Also a biggest threat on internet is pornography. There are many pornographic sites that can be found, letting your children to use internet which indirectly affects the children healthy mental life.
- There are various websites that do not provide the authenticated information. This leads to misconception among many people.

Internet based applications:

An **Internet application** does something for end users. It is generally not concerned with how data is actually transmitted between the hosts. Here are some distributed applications that require well-defined application level protocols:

- Sending and receiving email
- Searching and browsing information archives
- Copying files between computers
- Conducting financial transactions
- Navigating (in your car, smart scooter, smart bike, or other)
- Playing interactive games
- Video and music streaming
- Chat or voice communication (direct messaging, video conferencing)

In addition, there are a number of **network services** such as:

- Name servers
- Configuration servers
- Mail gateways, transfer agents, relays
- File and print servers

Data Communications

Transmission media

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.

- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).

- It is a physical path between transmitter and receiver in data communication.

- In a copper-based network, the bits in the form of electrical signals.

- In a fibre based network, the bits in the form of light pulses.

- In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.

- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.

- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.

- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.

- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.

- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Some factors need to be considered for designing the transmission media:

- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.

- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.

o   **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment:
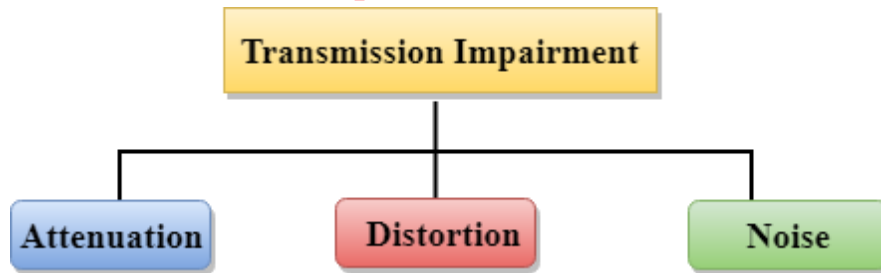
o   **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.

o   **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.

o   **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Classification Of Transmission Media:
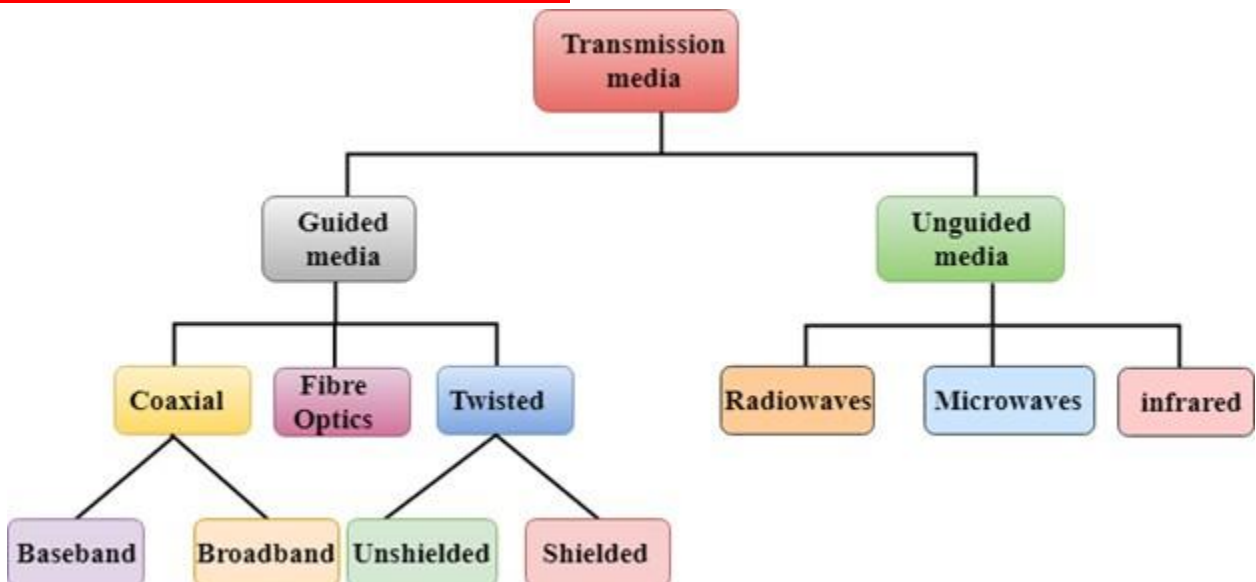
Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types Of Guided media:

Twisted pair:

Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.
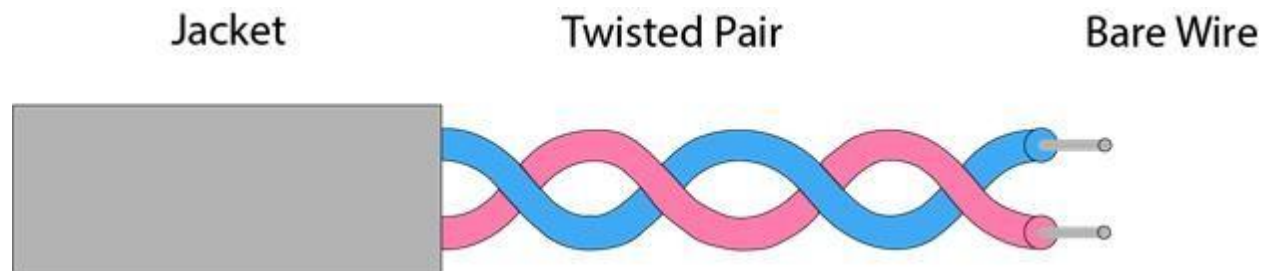
Types of Twisted pair:
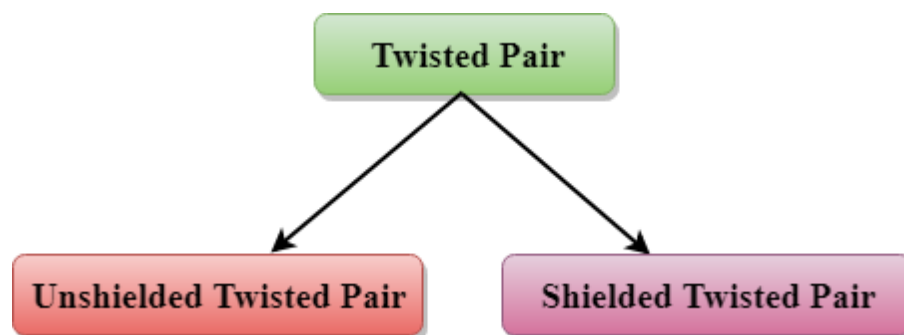
Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.

- **Category 2:** It can support upto 4Mbps.

- **Category 3:** It can support upto 16Mbps.

- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.

- **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.

- Installation of the unshielded twisted pair is easy.

- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

# Characteristics Of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.

- An installation of STP is easy.

- It has higher capacity as compared to unshielded twisted pair cable.

- It has a higher attenuation.

- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.

- It has a higher attenuation rate.

Coaxial Cable

- o Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- o The name of the cable is coaxial as it contains two conductors parallel to each other.
- o It has a higher frequency as compared to Twisted pair cable.
- o The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- o The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).

| Jacket | Shield | Insulator | Centre Conductor |
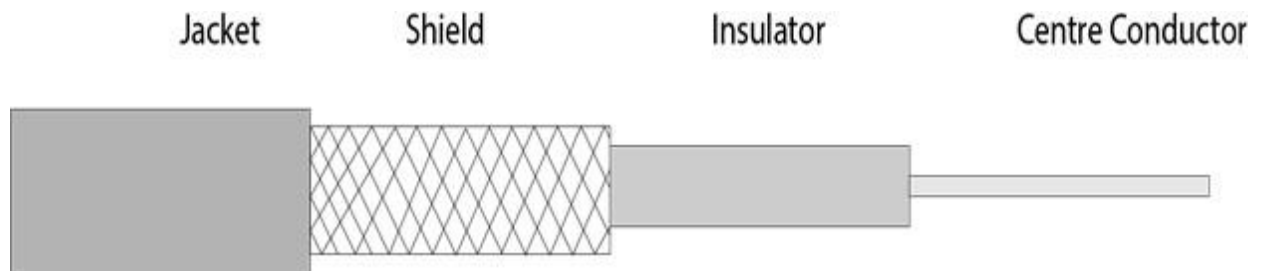
Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- o The data can be transmitted at high speed.
- o It has better shielding as compared to twisted pair cable.
- o It provides higher bandwidth.

Disadvantages Of Coaxial cable:

- o It is more expensive as compared to twisted pair cable.
- o If any fault occurs in the cable causes the failure in the entire network.

Fibre Optic

- o Fibre optic cable is a cable that uses electrical signals for communication.
- o Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- o The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- o Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:
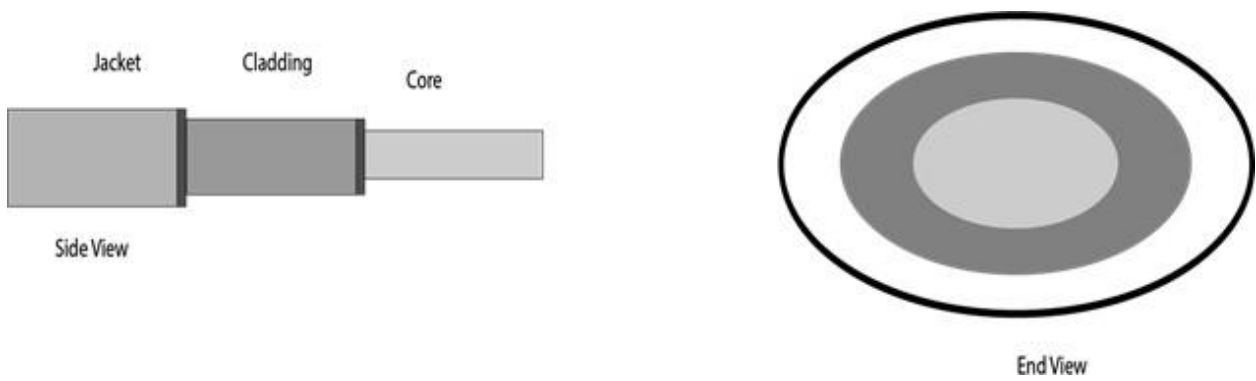
Basic elements of Fibre optic cable:

- o **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- o **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- o **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

- o **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.

- o **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.

- o **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.

- o **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.

- o **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

UnGuided Transmission

- o An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.

- o In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

Radio waves

- o Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.

- o Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.

- o The range in frequencies of radio waves is from 3Khz to 1 khz.

- o In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.

- o An example of the radio wave is **FM radio**.
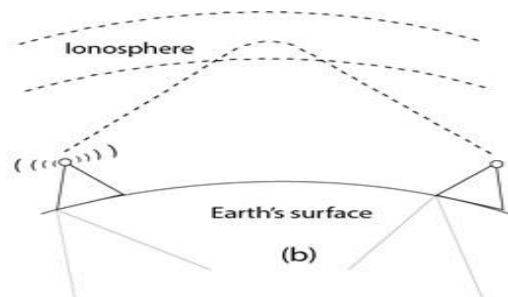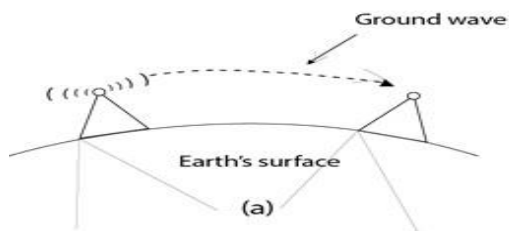
Applications Of Radio waves:

- o A Radio wave is useful for multicasting when there is one sender and many receivers.
- o An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- o Radio transmission is mainly used for wide area networks and mobile cellular phones.
- o Radio waves cover a large area, and they can penetrate the walls.
- o Radio transmission provides a higher transmission rate.

Microwaves
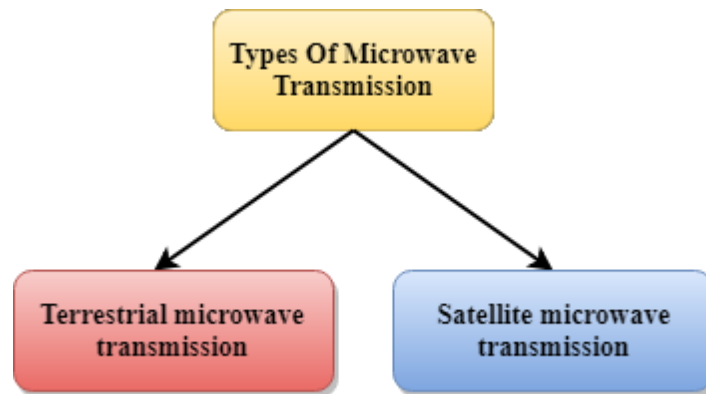
Microwaves are of two types:

- o Terrestrial microwave
- o Satellite microwave communication

Terrestrial Microwave Transmission

- o Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- o Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- o Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- o In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.

o It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

o **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.

o **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.

o **Short distance:** It is inexpensive for short distance.

o **Long distance:** It is expensive as it requires a higher tower for a longer distance.

o **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

o Microwave transmission is cheaper than using cables.

o It is free from land acquisition as it does not require any land for the installation of cables.

o Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.

o Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

o **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.

o **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.

o **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.

o **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- o A satellite is a physical object that revolves around the earth at a known height.
- o Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- o We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

- o The coverage area of a satellite microwave is more than the terrestrial microwave.
- o The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- o Satellite communication is used in mobile and wireless communication applications.
- o It is easy to install.
- o It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- o Satellite designing and development requires more time and higher cost.
- o The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- o The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

- o An infrared transmission is a wireless technology used for communication over short ranges.
- o The frequency of the infrared in the range from 300 GHz to 400 THz.

- o It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- o It supports high bandwidth, and hence the data rate will be very high.
- o Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- o An infrared communication provides better security with minimum interference.
- o Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

What is Multiplexing?

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

Why Multiplexing?

- o The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.

- o If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.

- o When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.

- o Transmission services are very expensive.

History of Multiplexing

- o Multiplexing technique is widely used in telecommunications in which several telephone calls are carried through a single wire.

- o Multiplexing originated in telegraphy in the early 1870s and is now widely used in communication.

- o George Owen Squier developed the **telephone carrier multiplexing** in 1910.

Concept of Multiplexing
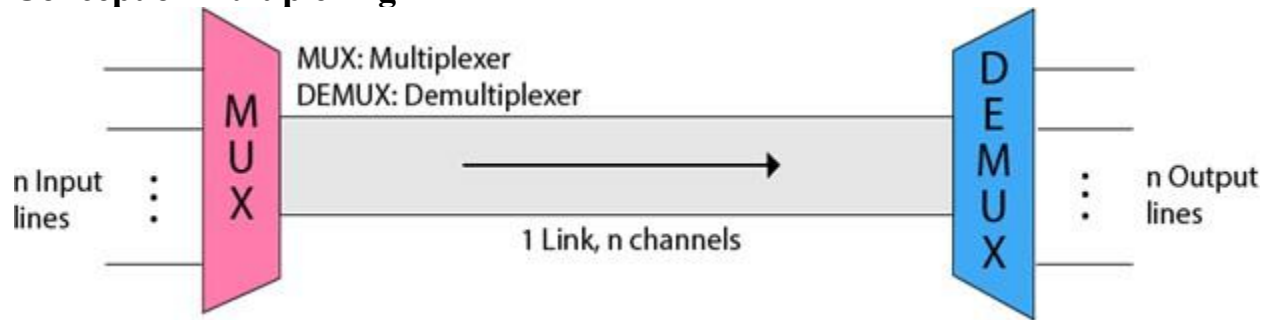
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.

- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

- More than one signal can be sent over a single medium.
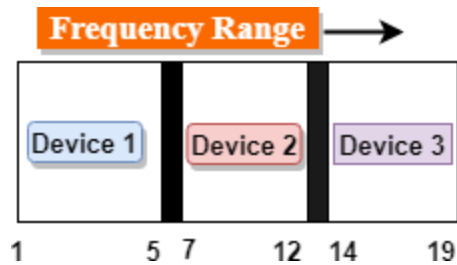- The bandwidth of a medium can be utilized effectively.

Multiplexing Techniques

Multiplexing techniques can be classified as:
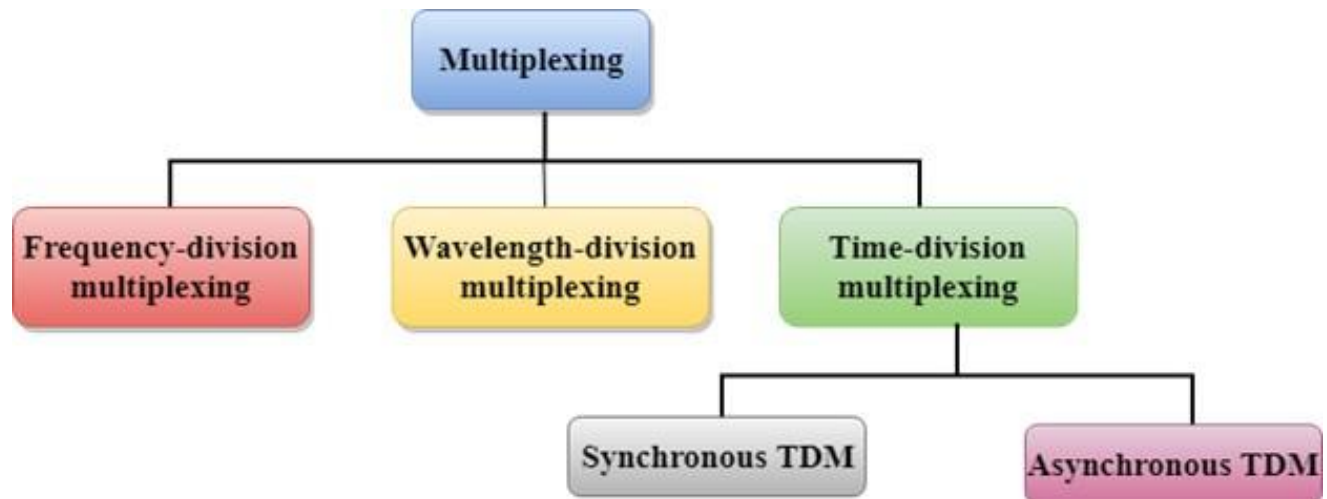
<u>Frequency-division Multiplexing (FDM)</u>

- It is an analog technique.
- **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.

o In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.

o The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.

o The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.

o Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.

o The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.

o **FDM** is mainly used in radio broadcasts and TV networks.
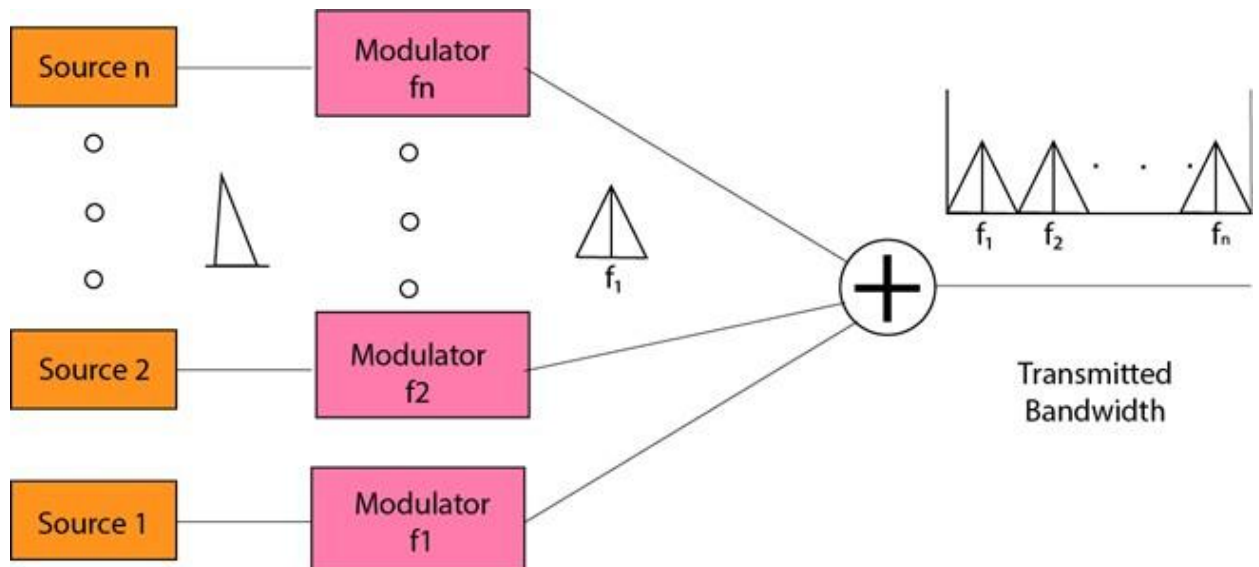
Advantages Of FDM:

FDM is used for analog signals.

- o FDM process is very simple and easy modulation.
- o A Large number of signals can be sent through an FDM simultaneously.
- o It does not require any synchronization between sender and receiver.

Disadvantages Of FDM:

- o FDM technique is used only when low-speed channels are required.
- o It suffers the problem of crosstalk.
- o A Large number of modulators are required.
- o It requires a high bandwidth channel.

Applications Of FDM:

- o FDM is commonly used in TV networks.
- o It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)
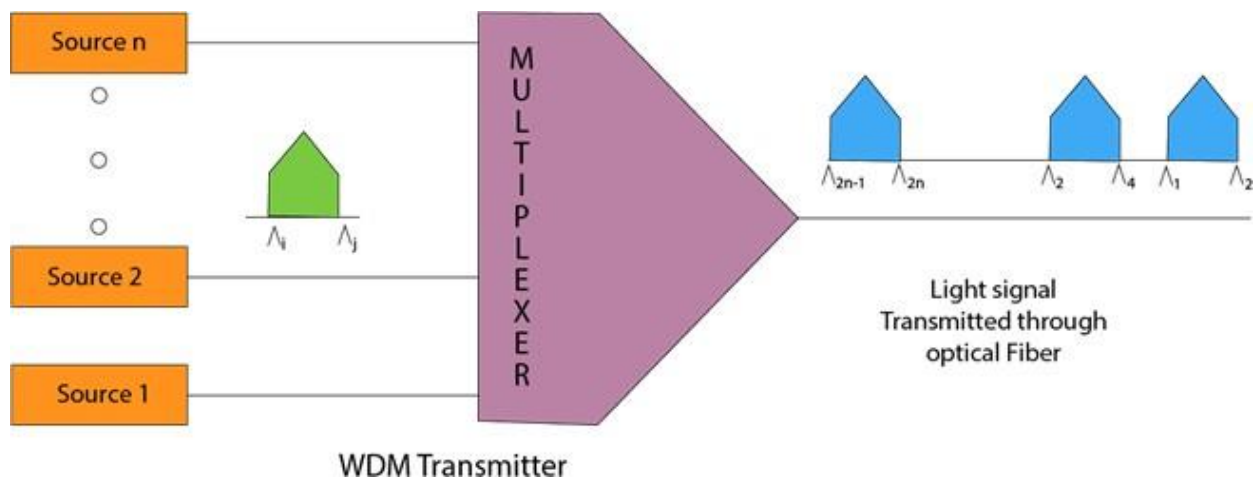
WDM Transmitter

o Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.

o WDM is used on fibre optics to increase the capacity of a single fibre.

o It is used to utilize the high data rate capability of fibre optic cable.

o It is an analog multiplexing technique.

o Optical signals from different source are combined to form a wider band of light with the help of multiplexer.

o At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.

o Multiplexing and Demultiplexing can be achieved by using a prism.

o Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.

o Prism also performs a reverse operation, i.e., demultiplexing the signal.

Fiber optic cable

Multiplexer   Demultiplexer
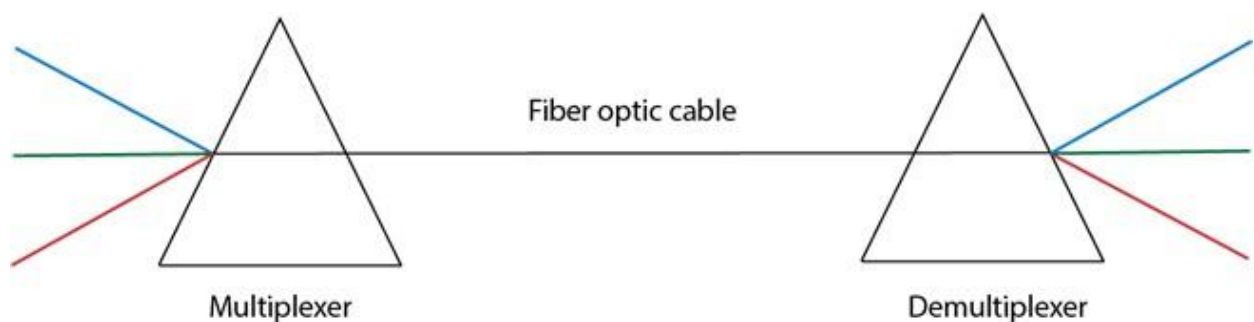
Time Division Multiplexing

o It is a digital technique.

o In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.

o In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.

o A user takes control of the channel for a fixed amount of time.

o In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.

o   In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.

o   It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

There are two types of TDM:

o   Synchronous TDM

o   Asynchronous TDM

Synchronous TDM

o   A Synchronous TDM is a technique in which time slot is preassigned to every device.

o   In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.

o   If the device does not have any data\, then the slot will remain empty.

o   In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.

o   The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.

o   If there are n devices, then there are n slots.
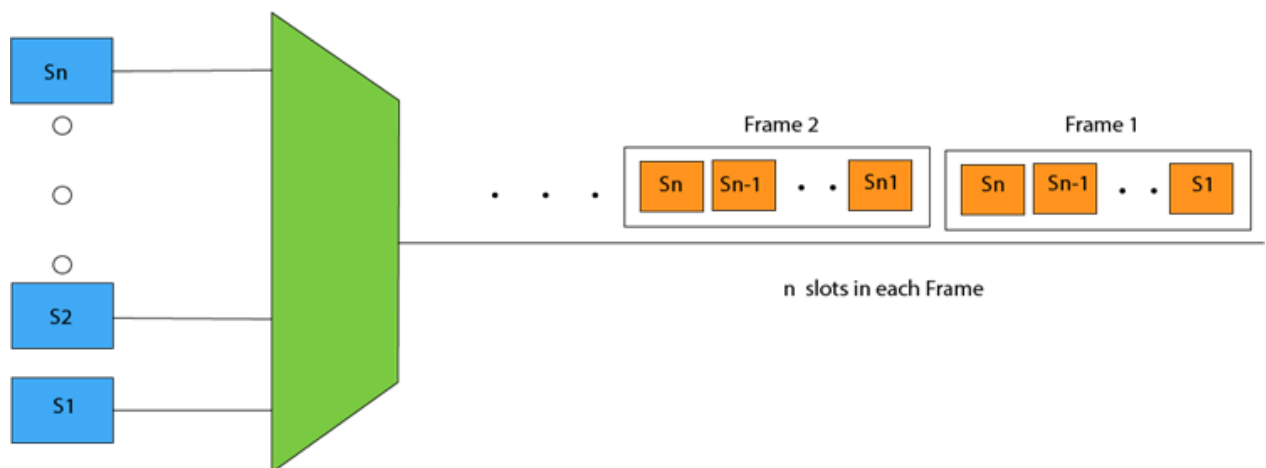
Concept Of Synchronous TDM
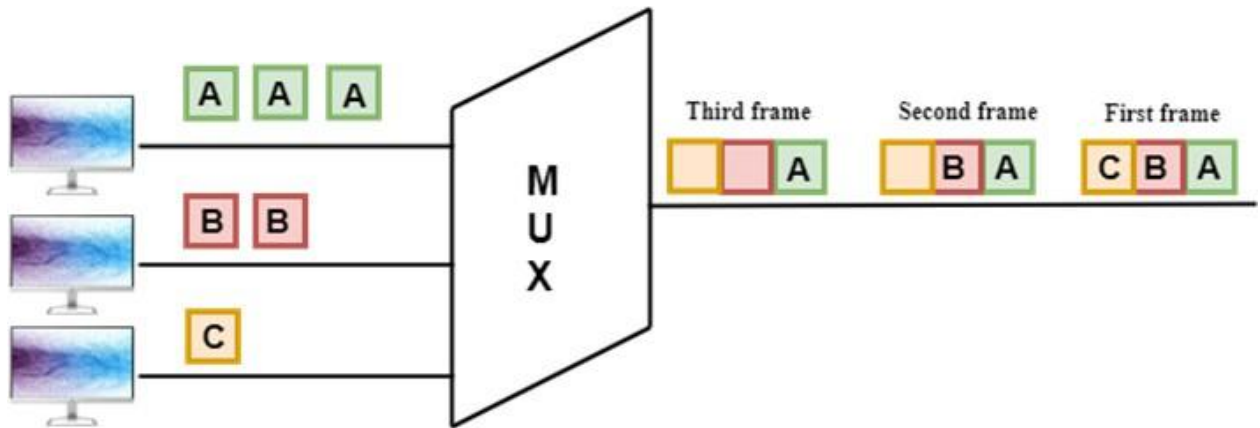
In the above figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

Disadvantages Of Synchronous TDM:

○ The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.

○ The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

Asynchronous TDM

○ An asynchronous TDM is also known as **Statistical TDM**.

○ An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.

○ An asynchronous TDM technique dynamically allocates the time slots to the devices.

○ In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
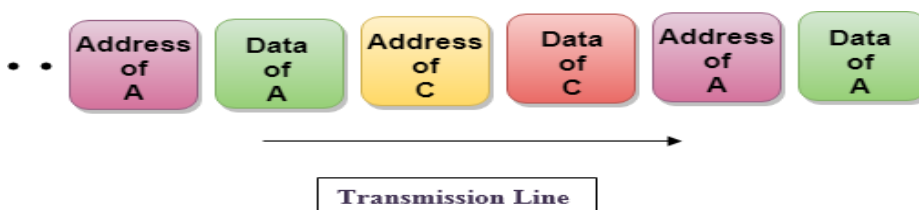
ADDRESS	DATA

o The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.

o In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (**m<n**).

o The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept Of Asynchronous TDM
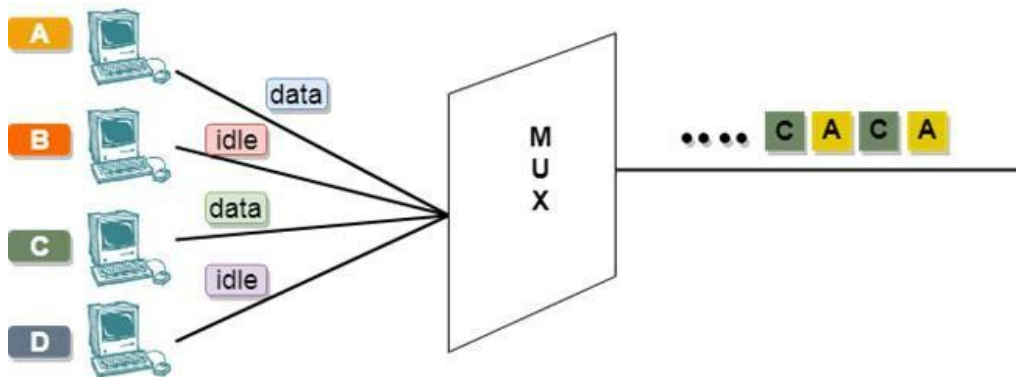
In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

## Frame of above diagram can be represented as:

The above figure shows that the data part contains the address to determine the source of the data.

Switching:

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques
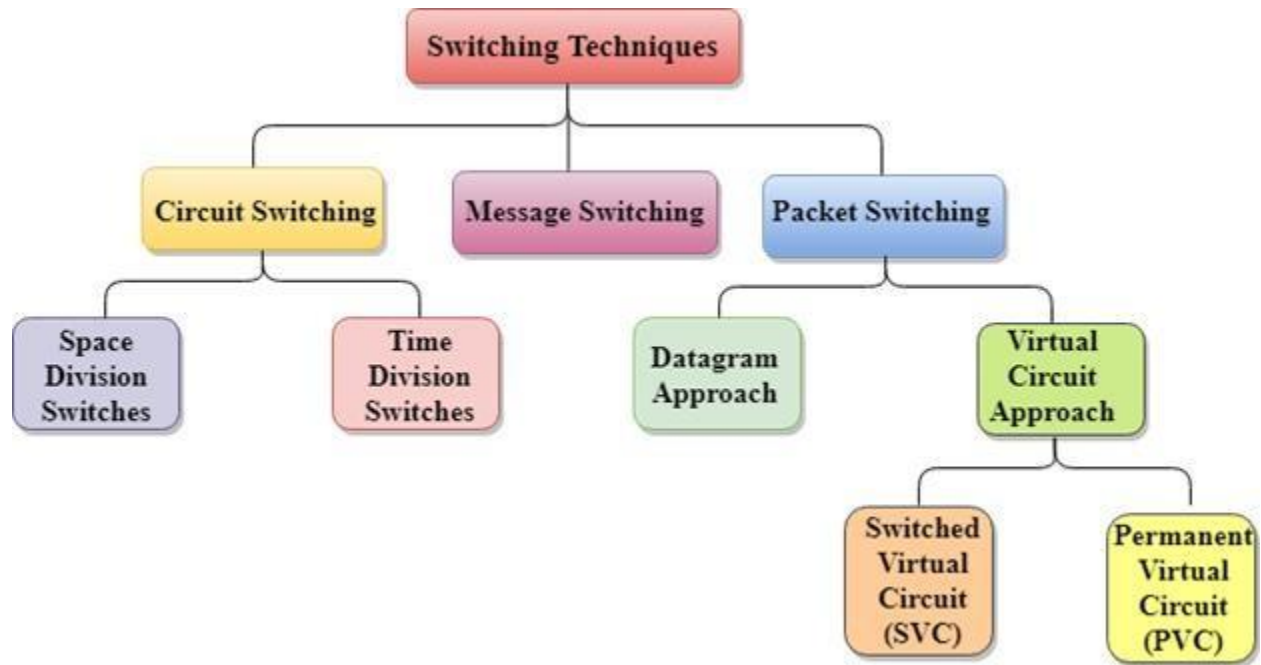
Circuit Switching

- o Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- o In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- o Circuit switching in a network operates in a similar way as the telephone works.
- o A complete end-to-end path must exist before the communication takes place.
- o In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- o Circuit switching is used in public telephone network. It is used for voice transmission.
- o Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

o   Circuit establishment

o   Data transfer

o   Circuit Disconnect
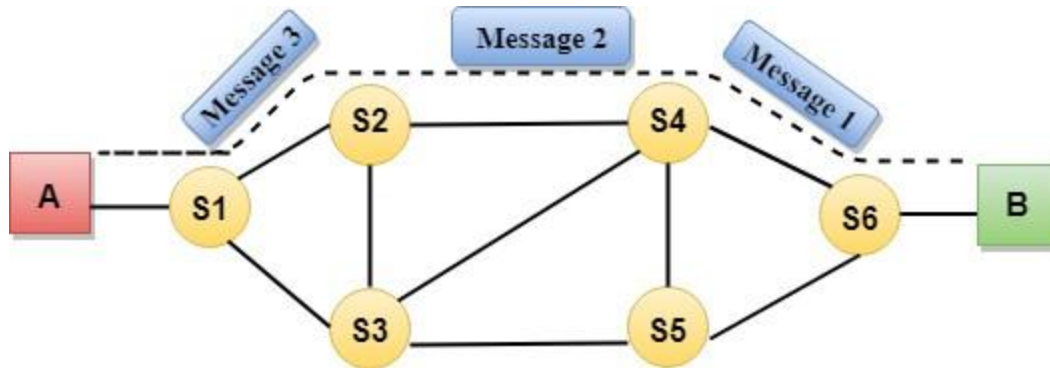
Circuit Switching can use either of the two technologies:

Space Division Switches:

o   Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of cross points.

o   Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic cross point or semiconductor gate that can be enabled or disabled by a control unit.

o   The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switch using FPGAs.

o   Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

o   **Crossbar Switch**

o   **Multistage Switch**

Crossbar Switch

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- o Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- o It reduces the number of crosspoints.
- o If one path fails, then there will be an availability of another path.

Advantages Of Circuit Switching:

- o In the case of Circuit Switching technique, the communication channel is dedicated.
- o It has fixed bandwidth.

Disadvantages Of Circuit Switching:

- o Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- o It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- o It is more expensive than other switching techniques as a dedicated path is required for each connection.
- o It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- o In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- o Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- o In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- o The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.

- o Message switches are programmed in such a way so that they can provide the most efficient routes.

- o Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**

- o Message switching treats each message as an independent entity
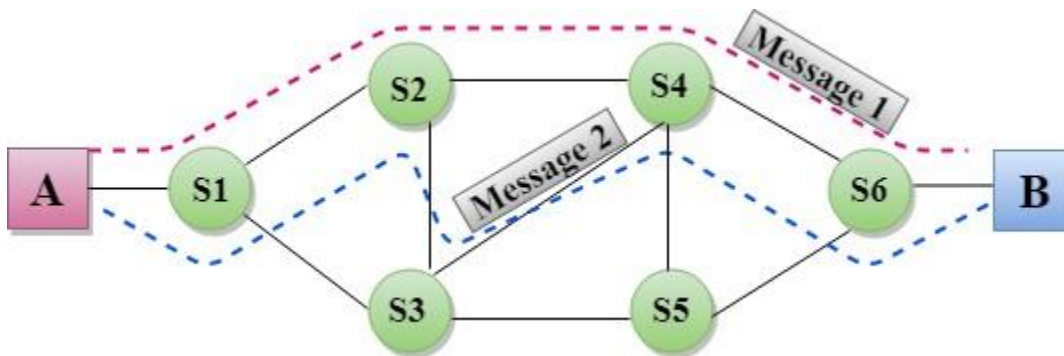
Advantages Of Message Switching

- o Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.

- o Traffic congestion can be reduced because the message is temporarily stored in the nodes.

- o Message priority can be used to manage the network.

- o The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

- o The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.

- o The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- o The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.

- o The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.

- o Every packet contains some information in its headers such as source address, destination address and sequence number.

- o Packets will travel across the network, taking the shortest path as possible.

- o All the packets are reassembled at the receiving end in correct order.

- o If any packet is missing or corrupted, then the message will be sent to resend the message.

- o If the correct order of the packets is reached, then the acknowledgment message will be sent.
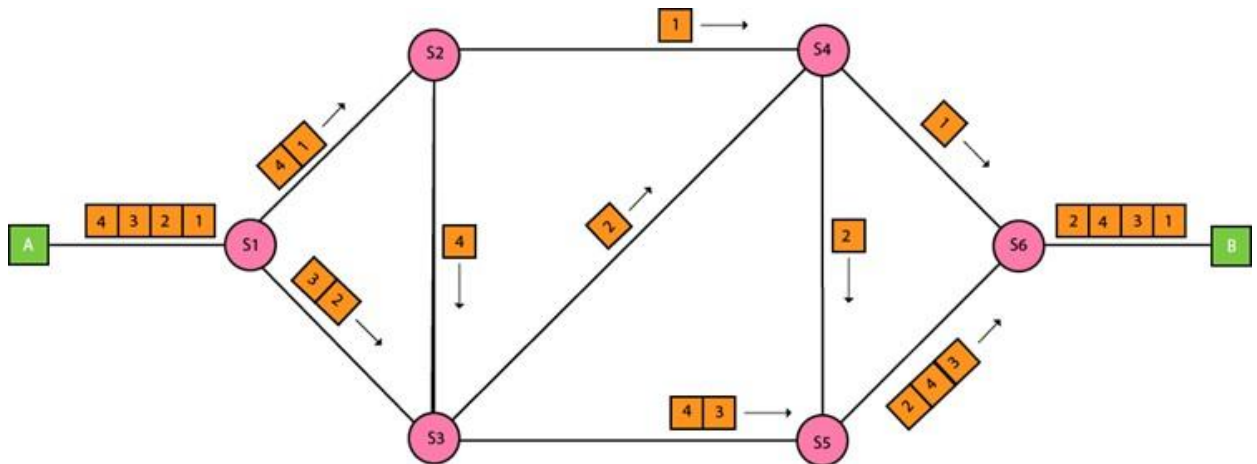
Approaches Of Packet Switching:

There are two approaches to Packet Switching:

Datagram Packet switching:

- o It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.

- o The packets are reassembled at the receiving end in correct order.

- o In Datagram Packet Switching technique, the path is not fixed.

- o Intermediate nodes take the routing decisions to forward the packets.

- o Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- o Virtual Circuit Switching is also known as connection-oriented switching.

- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.

- Call request and call accept packets are used to establish the connection between sender and receiver.

- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:
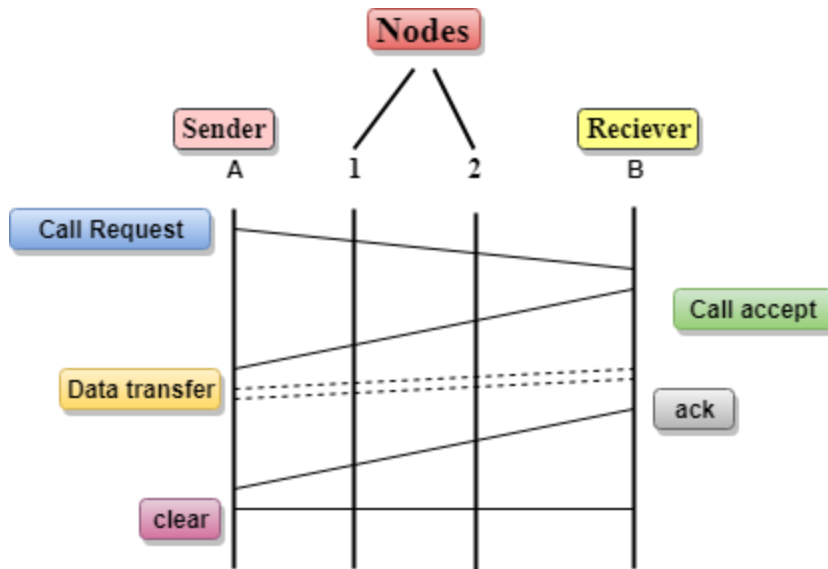
- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.

- Call request and call accept packets are used to establish a connection between the sender and receiver.

- When a route is established, data will be transferred.

- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.

- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

| Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

- o **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- o **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- o **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- o Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- o The protocols used in a packet switching technique are very complex and requires high implementation cost.
- o If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are not recovered.

Transmission in ISDN

o Earlier, the transmission of data and voice both were possible through normal POTS, Plain Old Telephone Systems. With the introduction of Internet came the advancement in telecommunication too. Yet, the sending and receiving of data along with voice was not an easy task. One could use either the Internet or the Telephone. The invention of ISDN helped mitigate this problem.

o The process of connecting a home computer to the Internet Service Provider used to take a lot of effort. The usage of the modulator-demodulator unit, simply called the MODEM was the essential thing to establish a connection. The following figure shows how the model worked in the past.
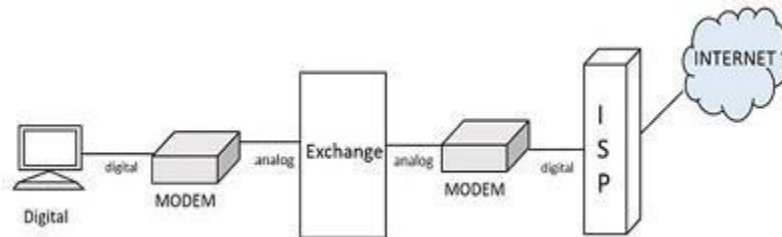

The above figure shows that the digital signals have to be converted into analog and analog signals to digital using modem during the whole path. What if the digital information at one end reaches to the other end in the same mode, without all these connections? It is this basic idea that lead to the development of **ISDN.**

As the system has to use the telephone cable through the telephone exchange for using the Internet, the usage of telephone for voice calls was not permitted. The introduction of ISDN has resolved this problem allowing the transmission of both voice and data simultaneously. This has many advanced features over the traditional PSTN, Public Switched Telephone Network.

ISDN is a telephone network based infrastructure that allows the transmission of voice and data simultaneously at a high speed with greater efficiency. This is a circuit switched telephone network system, which also provides access to Packet switched networks.

The model of a practical ISDN is as shown below.
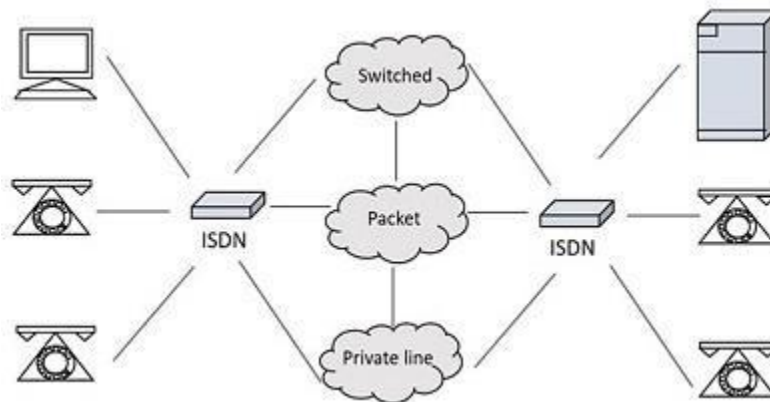
ISDN supports a variety of services. A few of them are listed below −

- Voice calls
- Facsimile
- Videotext
- Teletext
- Electronic Mail
- Database access
- Data transmission and voice
- Connection to internet
- Electronic Fund transfer
- Image and graphics exchange
- Document storage and transfer
- Audio and Video Conferencing
- Automatic alarm services to fire stations, police, medical etc.

Types of ISDN

Among the types of several interfaces present, some of them contains channels such as the **B-Channels** or Bearer Channels that are used to transmit voice and data simultaneously; the **D-Channels** or Delta Channels that are used for signaling purpose to set up communication.

The ISDN has several kinds of access interfaces such as −

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)
- Narrowband ISDN
- Broadband ISDN

Basic Rate Interface (BRI)

The Basic Rate Interface or Basic Rate Access, simply called the **ISDN BRI Connection** uses the existing telephone infrastructure. The BRI configuration provides **two data** or bearer channels at **64 Kbits/sec** speed and one control or delta channel at **16 Kbits/sec**. This is a standard rate.

The ISDN BRI interface is commonly used by smaller organizations or home users or within a local group, limiting a smaller area.

Primary Rate Interface (PRI)

The Primary Rate Interface or Primary Rate Access, simply called the ISDN PRI connection is used by enterprises and offices. The PRI configuration is based on T-carrier or T1 in the US, Canada and Japan countries consisting of **23 data** or bearer channels and one control or delta channel, with 64kbps speed for a bandwidth of 1.544 M bits/sec. The PRI configuration is based on E-carrier or E1 in Europe, Australia and few Asian countries consisting of **30 data** or bearer channels and **two-control** or delta channel with 64kbps speed for a bandwidth of 2.048 M bits/sec.

The ISDN BRI interface is used by larger organizations or enterprises and for Internet Service Providers.

Narrowband ISDN

The Narrowband Integrated Services Digital Network is called the **N-ISDN**. This can be understood as a telecommunication that carries voice information in a narrow band of frequencies. This is actually an attempt to digitize the analog voice information. This uses 64kbps circuit switching.

The narrowband ISDN is implemented to carry voice data, which uses lesser bandwidth, on a limited number of frequencies.

Broadband ISDN

The Broadband Integrated Services Digital Network is called the **B-ISDN**. This integrates the digital networking services and provides digital transmission over ordinary telephone wires, as well as over other media. The CCITT defined it as, "Qualifying a service or system requiring transmission channels capable of supporting rates greater than primary rates."

The broadband ISDN speed is around 2 MBPS to 1 GBPS and the transmission is related to ATM, i.e., Asynchronous Transfer Mode. The broadband ISDN communication is usually made using the fiber optic cables.

As the speed is greater than 1.544 Mbps, the communications based on this are called **Broadband Communications**. The broadband services provide a continuous flow of information, which is distributed from a central source to an unlimited number of authorized receivers connected to the network. Though a user can access this flow of information, he cannot control it.

Advantages of ISDN

ISDN is a telephone network based infrastructure, which enables the transmission of both voice and data simultaneously. There are many advantages of ISDN such as −

- As the services are digital, there is less chance for errors.
- The connection is faster.
- The bandwidth is higher.
- Voice, data and video − all of these can be sent over a single ISDN line.

Disadvantages of ISDN

The disadvantage of ISDN is that it requires specialized digital services and is costlier.

However, the advent of ISDN has brought great advancement in communications. Multiple transmissions with greater speed are being achieved with higher levels of accuracy.

ATM Networks

ATM stands for Asynchronous Transfer Mode. It is a switching technique that uses time division multiplexing (TDM) for data communications.

ATM networks are connection oriented networks for cell relay that supports voice, video and data communications. It encodes data into small fixed - size cells so that they are suitable for TDM and transmits them over a physical medium.

The size of an ATM cell is 53 bytes: 5 byte header and 48 byte payload(actual data). There are two different cell formats - user-network interface (UNI) and network-network interface (NNI). The below image represents the Functional Reference Model of the Asynchronous Transfer Mode.
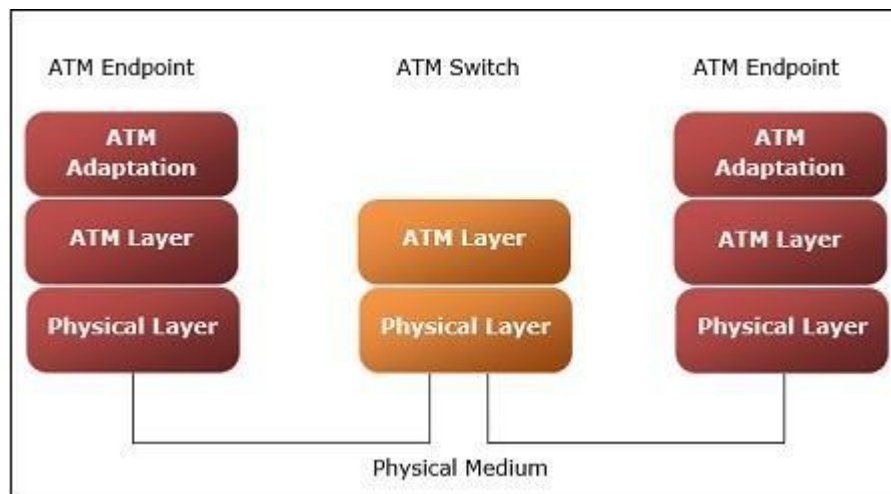
Benefits of ATM Networks are

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.
- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

ATM reference model comprises of three layers

- **Physical Layer** − This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.

- **ATM Layer** −This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.

- **ATM Adaptation Layer (AAL)** −This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate. This layer has two sub layers − Convergence sub layer and Segmentation and Reassembly sub layer.

- **ATM endpoints** − It contains ATM network interface adaptor. Examples of endpoints are workstations, routers, CODECs, LAN switches, etc.

- **ATM switch** −It transmits cells through the ATM networks. It accepts the incoming cells from ATM endpoints (UNI) or another switch (NNI), updates cell header and retransmits cell towards destination.

UNIT-2

Data Link Controls

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

- o Line discipline
- o Flow Control
- o Error Control
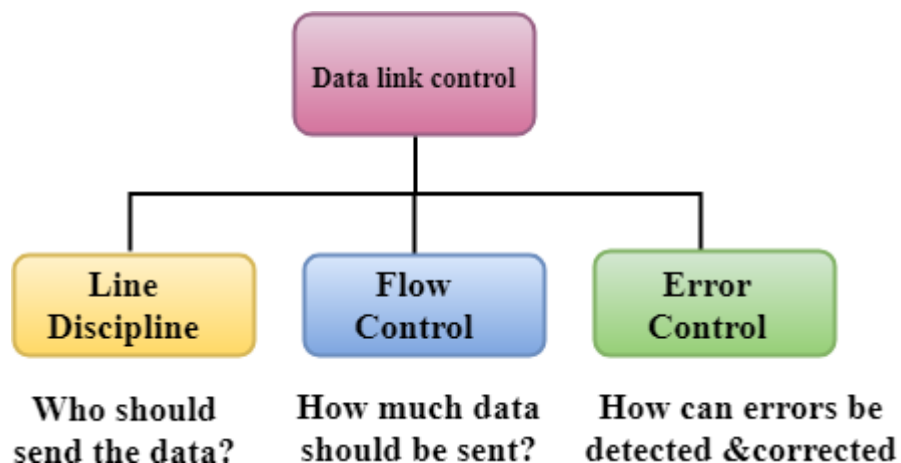
Line Discipline

- o Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways:

- o ENQ/ACK
- o Poll/select

ENQ/ACK

ENQ/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.

ENQ/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

Working of ENQ/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

- o If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.

- o If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.

- o If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.
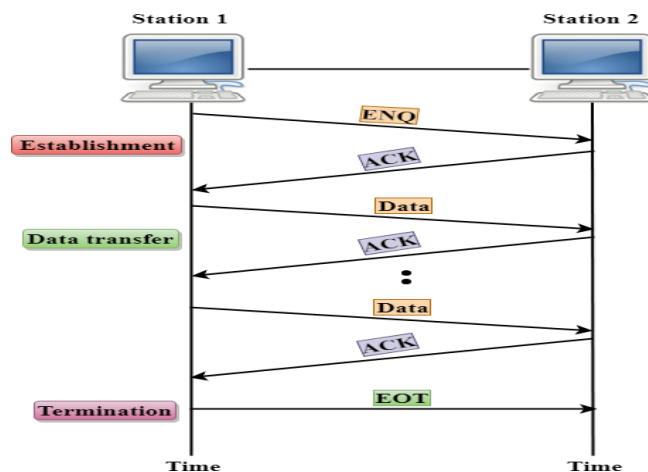
Poll/Select

The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.
- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.
- The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.
- If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as **polling**.
- If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as **selecting**.

Select

- The select mode is used when the primary device has something to send.
- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.
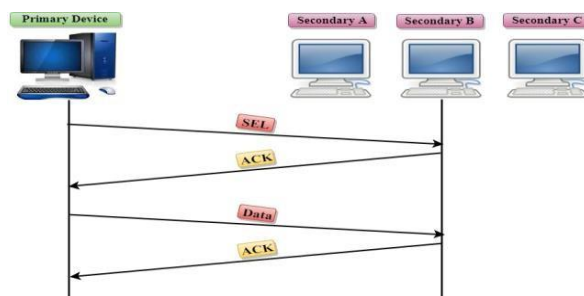
Poll

- o The Poll mode is used when the primary device wants to receive some data from the secondary device.
- o When a primary device wants to receive the data, then it asks each device whether it has anything to send.
- o Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.
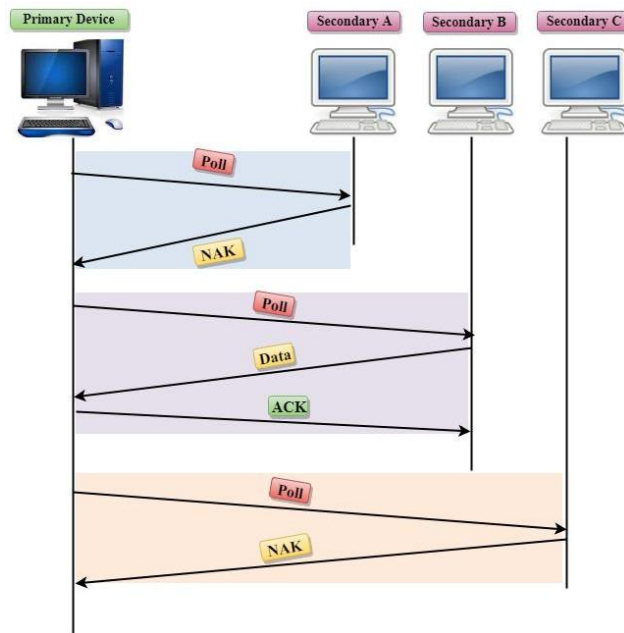
Flow Control

- o It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
- o The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- o It requires a buffer, a block of memory for storing the information until they are processed.

COMPUTER NETWORKS

Two methods have been developed to control the flow of data:

- o Stop-and-wait
- o Sliding window

Stop-and-wait

- o In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- o When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

Sliding Window

- o The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- o In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- o A single ACK acknowledge multiple frames.
- o Sliding Window refers to imaginary boxes at both the sender and receiver end.
- o The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- o Frames can be acknowledged even when the window is not completely filled.
- o The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1........
- o The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.

o When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

Sender Window

o At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.

o Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.

o For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).
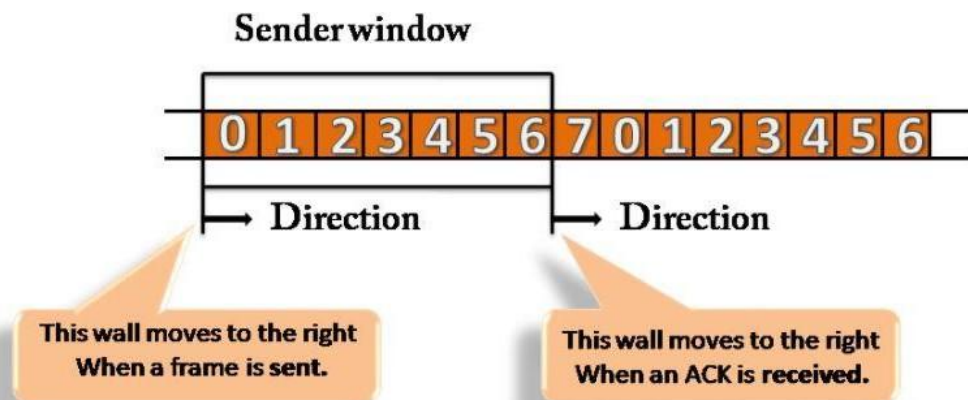
Receiver Window

o At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.

o When the new frame arrives, the size of the window shrinks.

o The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For

example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).

o   Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.

o   Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.
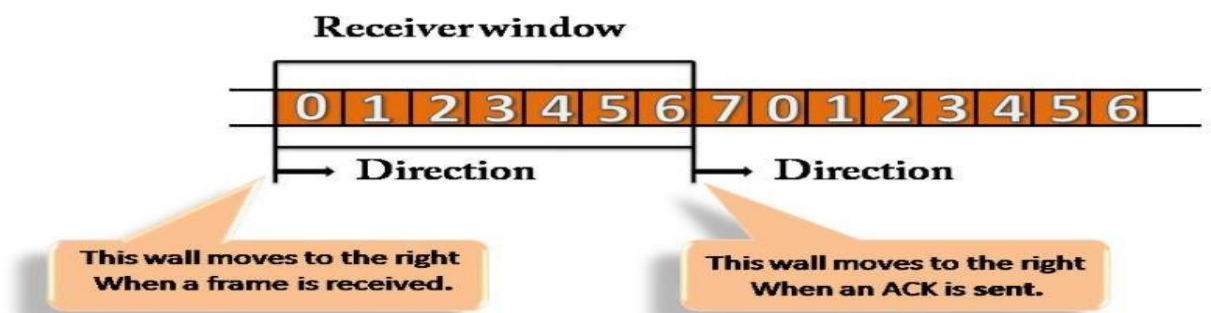
Error Control

Error Control is a technique of error detection and retransmission.

Categories of Error Control:
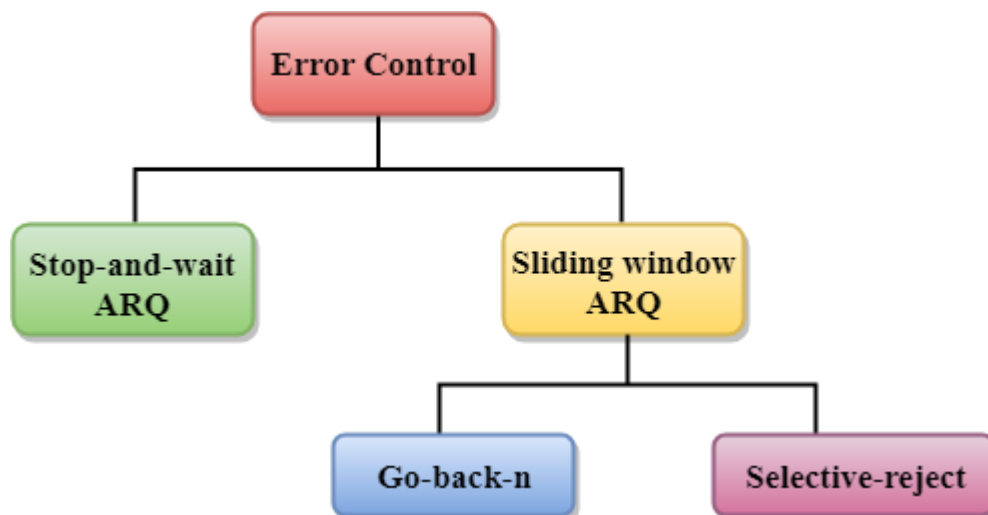
Stop-and-wait ARQ

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

COMPUTER NETWORKS

This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

- o The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.

- o Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.

- o If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.

- o It works with the timer. If the acknowledgement is not received within the alltotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

- o **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.

- o **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

SlidingWindow ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

- o In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.

- o The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.

- o The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ:

- o **Go-Back-n ARQ:** In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.
- o Three possibilities can occur for retransmission:
- o **Damaged Frame:** When the frame is damaged, then the receiver sends a NAK frame.
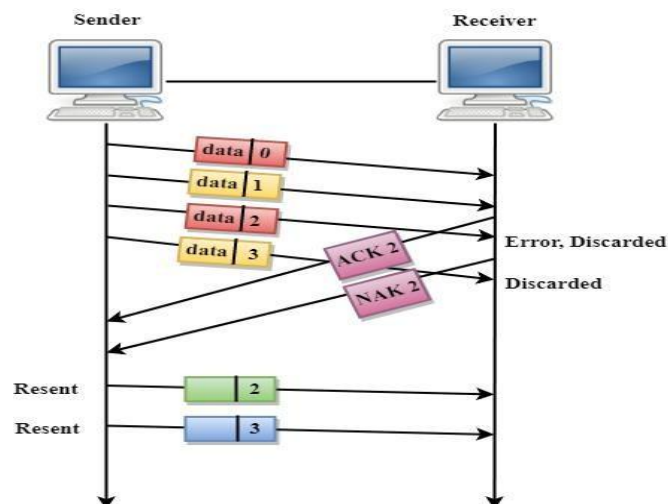
In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.

- o **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.

- o **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective-Reject ARQ

- o Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.
- o In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- o The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- o The receiver must have an appropriate logic for reinserting the frames in a correct order.
- o The sender must consist of a searching mechanism that selects only the requested frame for retransmission.
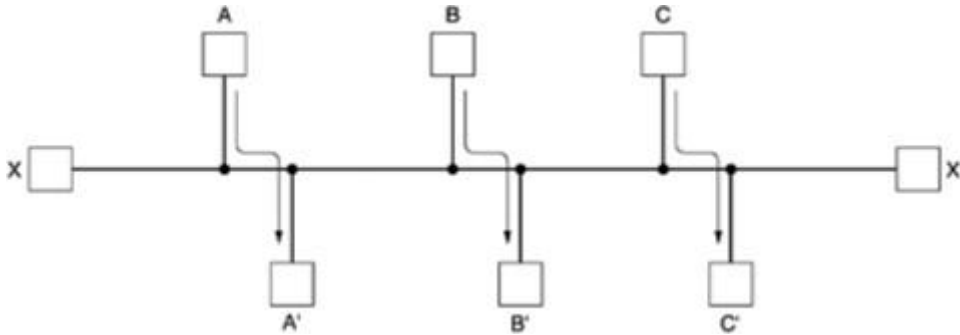
ROUTING ALGORITHMS

The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.

PROPERTIES OF ROUTING ALGORITHM:

Correctness, simplicity, robustness, stability, fairness, and optimality

FAIRNESS AND OPTIMALITY.

Fairness and optimality may sound obvious, but as it turns out, they are often contradictory goals. There is enough traffic between A and A', between B and B', and between C and C' to saturate the horizontal links. To maximize the total flow, the X to X' traffic should be shut off altogether. Unfortunately, X and X' may not see it that way.

Evidently, some compromise between global efficiency and fairness to individual connections is needed.

CATEGORY OF ALGORITHM

Routing algorithms can be grouped into two major classes:

Nonadaptive and adaptive.

Nonadaptive algorithms do not base their routing decisions on measurements or estimates of the current traffic and topology.

Instead, the choice of the route to use to get from I to J is computed in and downloaded to the routers when the network is booted. in advance, off-line,
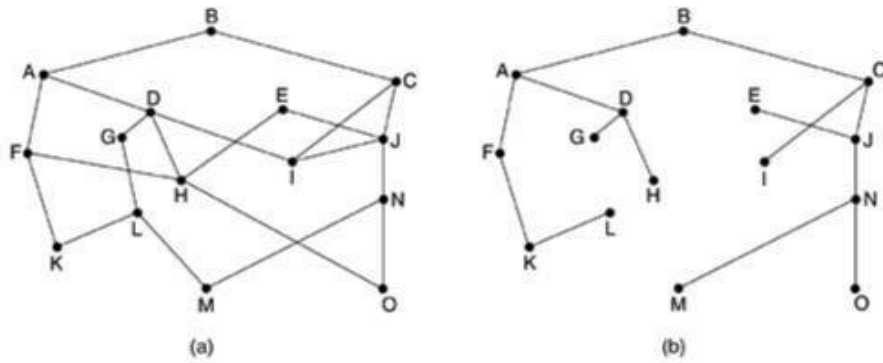
This procedure is sometimes called Static routing.

THE OPTIMALITY PRINCIPLE

If router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.

The set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a sink tree

(a) A subnet. (b) A sink tree for router B.

o As a direct consequence of the optimality principle, we can see that the set of optimal routes from all sources to a given destination form a tree rooted at the destination.

o Such a tree is called a sink tree where the distance metric is the number of hops.

o Note that a sink tree is not necessarily unique; other trees with the same path lengths may exist. The goal of all routing algorithms is to discover and use the sink trees for all routers

SHORTEST PATH ROUTING

 • A technique to study routing algorithms: The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line (often called a link)

 • To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.

 • One way of measuring path length is the number of hops. Another metric is the geographic distance in kilometers. Many other metrics are also possible. For example, each arc could be labeled with the mean queuing and transmission delay for some standard test packet as determined by hourly test runs.

 • In the general case, the labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured

delay, and other factors. By changing the weighting function, the algorithm would then compute the "shortest" path measured according to any one of a number of criteria or to a combination of criteria.
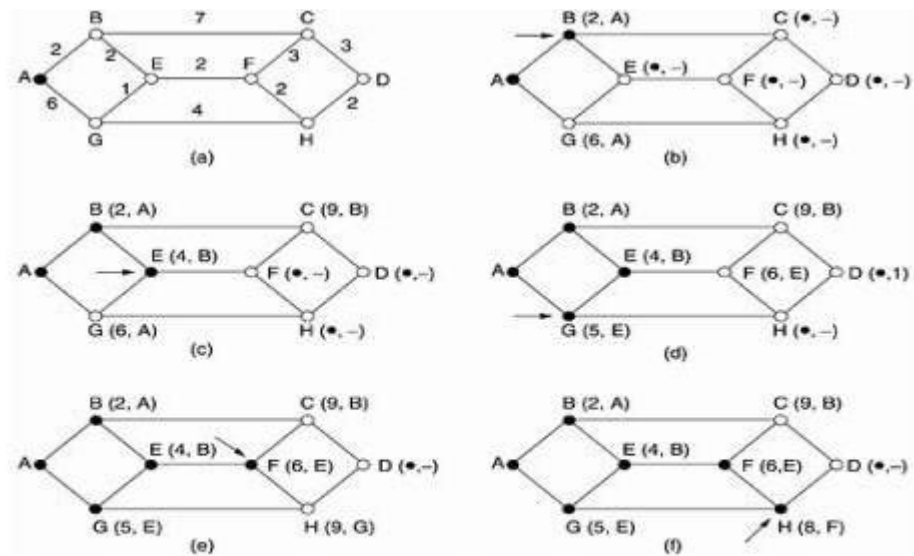
The first five steps used in computing the shortest path from A to D. The arrows indicate the working node.

o   To illustrate how the labelling algorithm works, look at the weighted, undirected graph of Fig. 5-7(a), where the weights represent, for example, distance.

o   We want to find the shortest path from A to D. We start out by marking node A as permanent, indicated by a filled-in circle.

o   Then we examine, in turn, each of the nodes adjacent to A (the working node), relabeling each one with the distance to A.

o   Whenever a node is relabelled, we also label it with the node from which the probe was made so that we can reconstruct the final path later.

o   Having examined each of the nodes adjacent to A, we examine all the tentatively labelled nodes in the whole graph and make the one with the smallest label permanent, as shown in Fig. 5-7(b).

o   This one becomes the new working node. We now start at B and examine all nodes adjacent to it. If the sum of the label on B and the distance from B to the node being considered is less than the label on that node, we have a shorter path, so the node is relabelled.

o   After all the nodes adjacent to the working node have been inspected and the tentative labels changed if possible, the entire graph is searched for the tentatively-labelled node with the smallest value.

o   This node is made permanent and becomes the working node for the next round. Figure 5-7 shows the first five steps of the algorithm.

o   To see why the algorithm works, look at Fig. 5-7(c). At that point we have just made E permanent. Suppose that there were a shorter path than ABE, say AXYZE. There are two possibilities: either node Z has already been made permanent, or it has not been. If it has, then E has already been probed (on the round following the one when Z was made permanent), so the AXYZE path has not escaped our attention and thus cannot be a shorter path. Now consider the case where Z is still tentatively labelled. Either the label at Z is greater than or equal to that at E, in which case AXYZE cannot

- be a shorter path than ABE, or it is less than that of E, in which case Z and not E will become permanent first, allowing E to be probed from Z.
- o This algorithm is given in Fig. 5-8. The global variables n and dist describe the graph and are initialized before shortest path is called. The only difference between the program and the algorithm described above is that in Fig. 5-8, we compute the shortest path starting at the terminal node, t, rather than at the source node, s. Since the shortest path from t to s in an undirected graph is the same as the shortest path from s to t, it does not matter at which end we begin (unless there are several shortest paths, in which case reversing the search might discover a different one). The reason for searching backward is that each node is labelled with its predecessor rather than its successor.
- o When the final path is copied into the output variable, path, the path is thus reversed. By reversing the search, the two effects cancel, and the answer is produced in the correct order.

FLOODING

- o Another static algorithm is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on.
- o Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite number unless some measures are taken to damp the process.
- o One such measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero. Ideally, the hop counter should be initialized to the length of the path from source to destination.
- o If the sender does not know how long the path is, it can initialize the counter to the worst case, namely, the full diameter of the subnet.

DISTANCE VECTOR ROUTING

- o Distance vector routing algorithms operate by having each router maintain a table (i.e, a vector) giving the best known distance to each destination and which line to use to get there.
- o These tables are updated by exchanging information with the neighbors.
- o The distance vector routing algorithm is sometimes called by other names, most commonly the distributed Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm, after the researchers who developed it (Bellman, 1957; and Ford and Fulkerson, 1962).
- o It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP.

New estimated delay from J

To	A	I	H	K		Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	—
K	24	22	22	0	6	K
L	29	33	9	9	15	K

JA delay is 8   JI delay is 10   JH delay is 12   JK delay is 6   New routing table for J

Vectors received from J's four neighbors

(a)   (b)
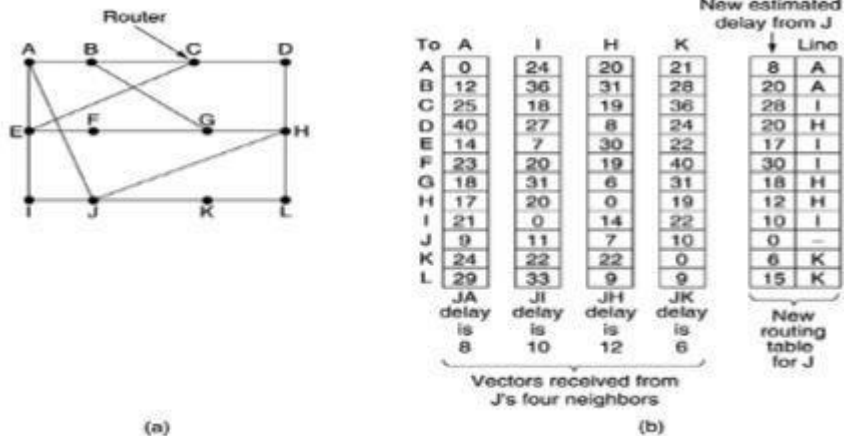
(a) A subnet. (b) Input from A, I, H, K, and the new routing table for J.

- o   Part (a) shows a subnet. The first four columns of part (b) show the delay vectors received from the neighbours of router J.
- o   A claims to have a 12-msec delay to B, a 25-msec delay to C, a 40-msec delay to D, etc. Suppose that J has measured or estimated its delay to its neighbours, A, I, H, and K as 8, 10, 12, and 6 msec, respectively.
- o   Each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.
  1. The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.
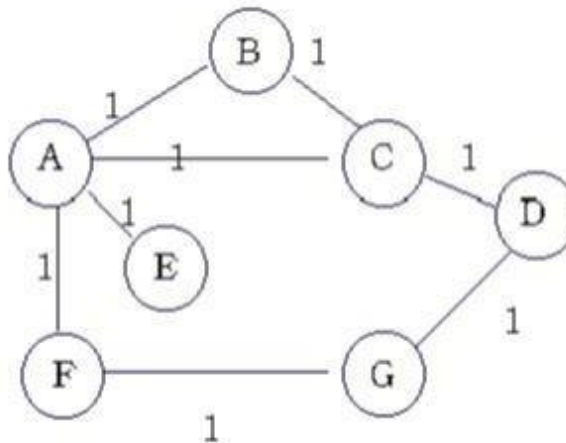 2. A link that is down is assigned an infinite cost

Example.

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

COMPUTER NETWORKS

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

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

Note that each node only knows the information in one row of the table.

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

2. If any of the recipients of the information from A find that A is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through A. (node B learns from A that node E can be reached at a cost of 1; B also knows it can reach A at a cost of 1, so it adds these to get the cost of reaching E by means of A. B records that it can reach E at a cost of 2 by going through A.)

3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.

4. In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table. (for example, B knows that it was A who said " I can reach E in one hop" and so B puts an entry in its table that says " To reach E, use the link to A.)

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

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

In practice, each node's forwarding table consists of a set of triples of the form: (Destination, Cost, NextHop).
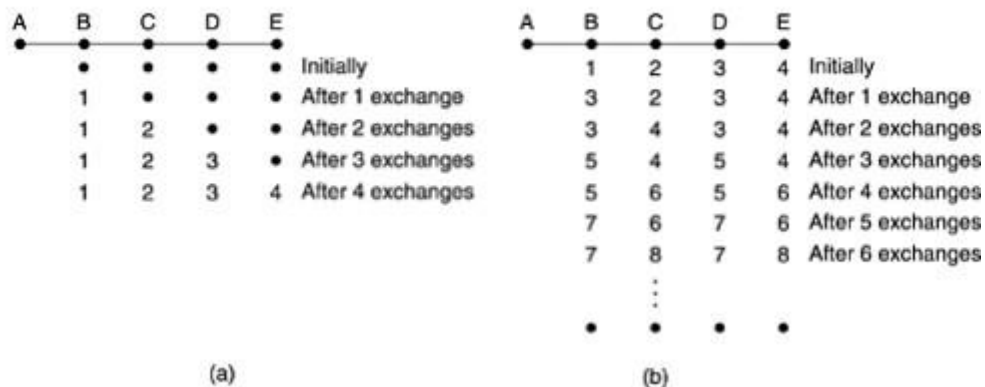For example, Table 3 shows the complete routing table maintained at node B for the network in figure1.

Table 3. Routing table maintained at node B.

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

THE COUNT-TO-INFINITY PROBLEM

The count-to-infinity problem.

(a)

| | | | | | |

(b)

A   B   C   D   E   A   B   C   D   E

B	C	D	E		B	C	D	E	
•	•	•	•	Initially	1	2	3	4	Initially
1	•	•	•	After 1 exchange	3	2	3	4	After 1 exchange
1	2	•	•	After 2 exchanges	3	4	3	4	After 2 exchanges
1	2	3	•	After 3 exchanges	5	4	5	4	After 3 exchanges
1	2	3	4	After 4 exchanges	5	6	5	6	After 4 exchanges
					7	6	7	6	After 5 exchanges
					7	8	7	8	After 6 exchanges

Consider the five-node (linear) subnet of Fig. 5-10, where the delay metric is the number of hops. Suppose A is down initially and all the other routers know this. In other words, they have all recorded the delay to A as infinity.
Now let us consider the situation of Fig. 5-10(b), in which all the lines and routers are initially up. Routers B, C, D, and E have distances to A of 1, 2, 3, and 4, respectively. Suddenly A goes down, or alternatively, the line between A and B is cut, which is effectively the same thing from B's point of view.
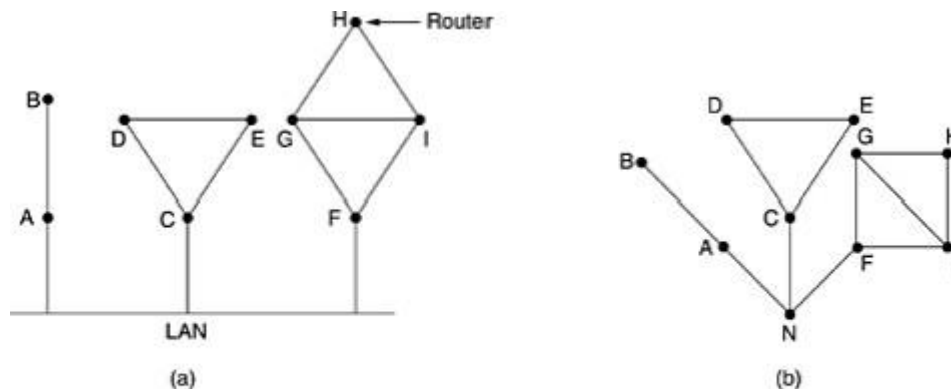
LINK STATE ROUTING

 The idea behind link state routing is simple and can be stated as five parts.
Each router must do the following:
1. Discover its neighbors and learn their network addresses.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router Learning about the Neighbours
When a router is booted, its first task is to learn who its neighbours are. It accomplishes
this goal by sending a special HELLO packet on each point-to-point line. The router on
the other end is expected to send back a reply telling who it is

(a) Nine routers and a LAN. (b) A graph model of (a).
(b)

- Measuring Line Cost The link state routing algorithm requires each router to know, or at least have a reasonable estimate of, the delay to each of its neighbors.
- The most direct way to determine this delay is to send over the line a special ECHO packet that the other side is required to send back immediately.
- By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay.
- For even better results, the test can be conducted several times, and the average used. Of course, this method implicitly assumes the delays are symmetric, which may not always be the case
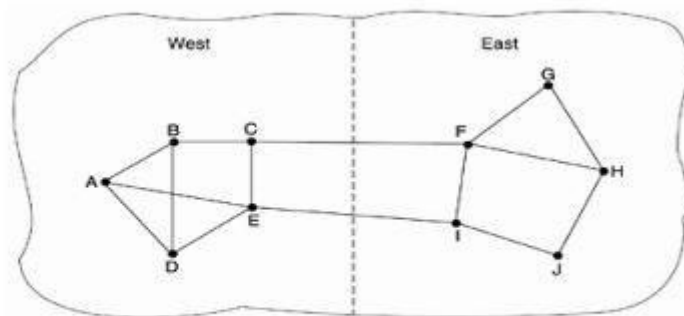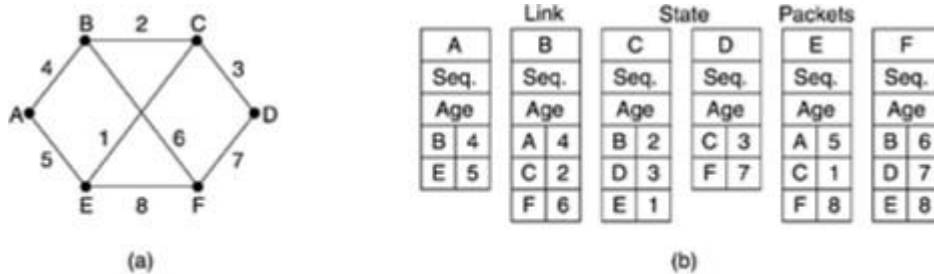

Figure: A subnet in which the East and West parts are connected by two lines.

Unfortunately, there is also an argument against including the load in the delay calculation. Consider the subnet of Fig. 5-12, which is divided into two parts, East and West, connected by two lines, CF and EI.

Building Link State Packets

(a) A subnet. (b) The link state packets for this subnet.

- Once the information needed for the exchange has been collected, the next step is for each router to build a packet containing all the data.
- The packet starts with the identity of the sender, followed by a sequence number and age (to be described later), and a list of neighbours.
- For each neighbour, the delay to that neighbour is given.
- An example subnet is given in Fig. 5-13(a) with delays shown as labels on the lines. The corresponding link state packets for all six routers are shown in Fig. 5-13(b).

Distributing the Link State Packets

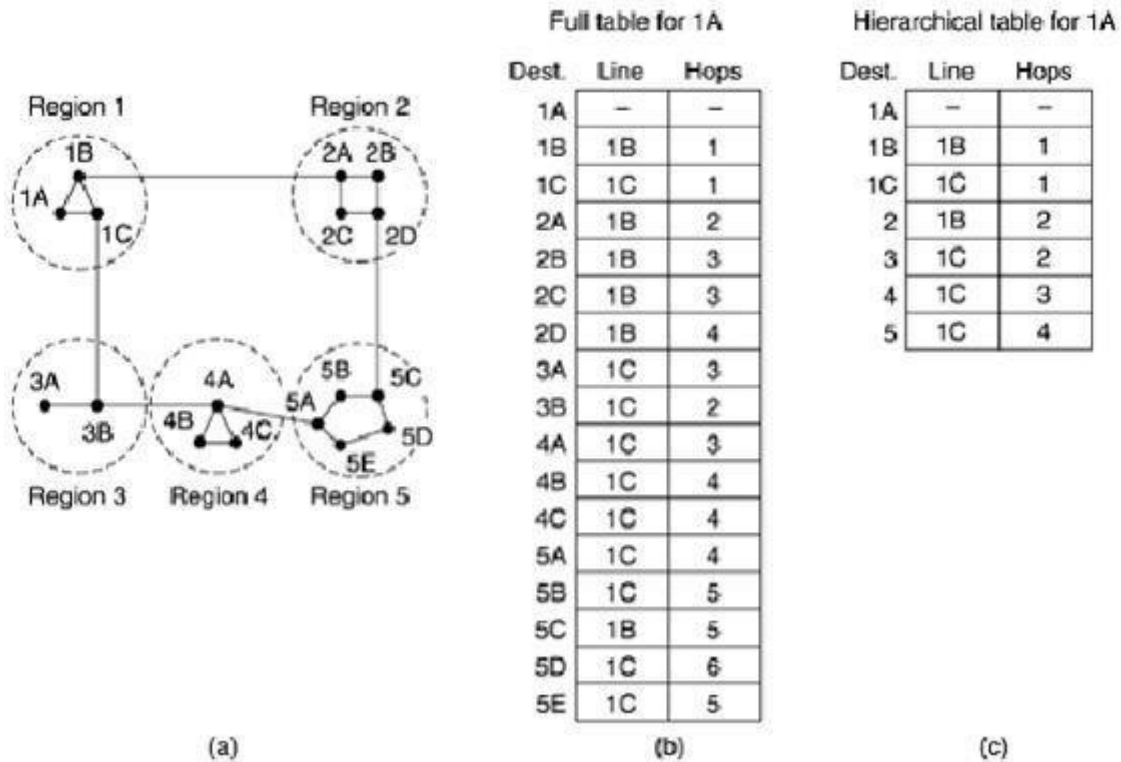| Source	Seq.	Age	Send flags A	C	F	ACK flags A	C	F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

The packet buffer for router B in Fig. 5-13.

In Fig. 5-14, the link state packet from A arrives directly, so it must be sent to C and F and acknowledged to A, as indicated by the flag bits. Similarly, the packet from F has to be forwarded to A and C and acknowledged to F.

HIERARCHICAL ROUTING

- The routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.

  For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations.

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(a)   (b)   (c)

- Figure 5-15 gives a quantitative example of routing in a two-level hierarchy with five regions. The full routing table for router 1A has 17 entries, as shown in Fig. 5-15(b).
- When routing is done hierarchically, as in Fig. 5-15(c), there are entries for all the local routers as before, but all other regions have been condensed into a single router, so all traffic for region 2 goes via the 1B -2A line, but the rest of the remote traffic goes via the 1C -3B line.
- Hierarchical routing has reduced the table from 17 to 7 entries. As the ratio of the number of regions to the number of routers per region grows, the savings in table space increase.

BROADCAST ROUTING

Sending a packet to all destinations simultaneously is called broadcasting.

1) The source simply sends a distinct packet to each destination. Not only is the method wasteful of bandwidth, but it also requires the source to have a complete list of all destinations.

2) Flooding. The problem with flooding as a broadcast technique is that it generates too many packets and consumes too much bandwidth.
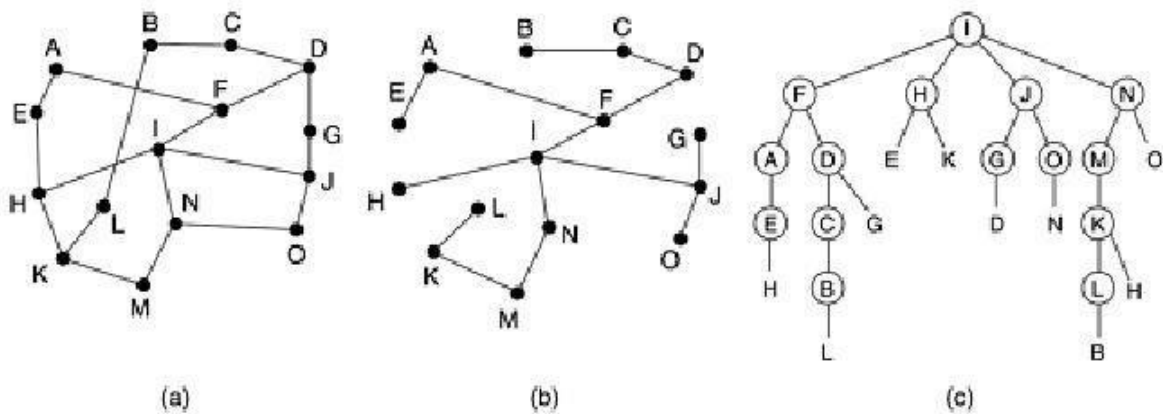
Reverse path forwarding. (a) A subnet. (b) A sink tree. (c) The tree built by reverse path forwarding.

Part (a) shows a subnet, part (b) shows a sink tree for router I of that subnet, and part (c) shows how the reverse path algorithm works.

- When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of the broadcast. If so, there is an excellent chance that the broadcast packet itself followed the best route from the router and is therefore the first copy to arrive at the router.
- This being the case, the router forwards copies of it onto all lines except the one it arrived on. If, however, the broadcast packet arrived on a line other than the preferred one for reaching the source, the packet is discarded as a likely duplicate.

MULTICAST ROUTING
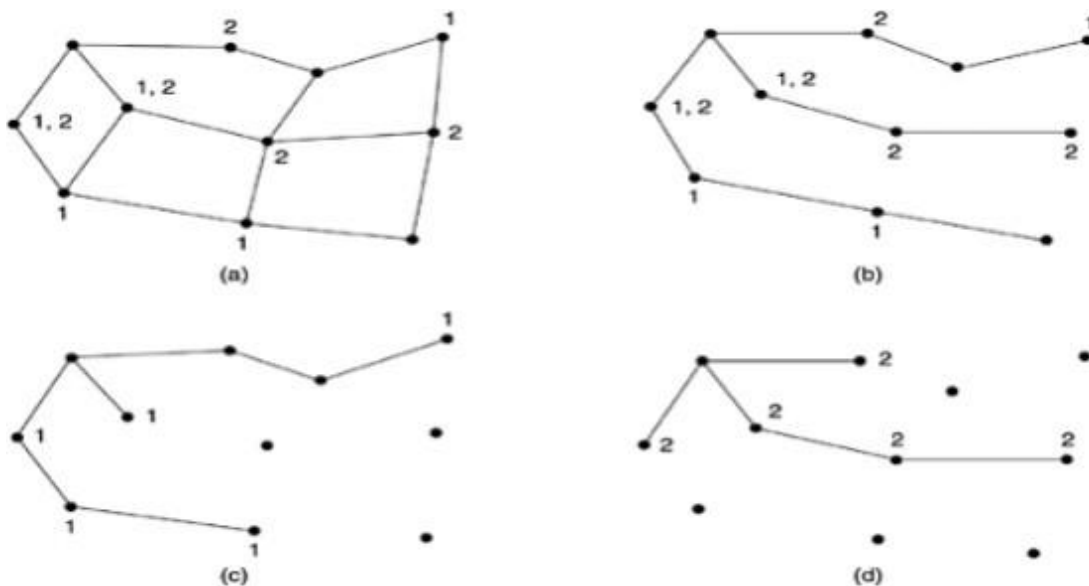
- To do multicast routing, each router computes a spanning tree covering all other routers. For example, in Fig. 5-17(a) we have two groups, 1 and 2.
- Some routers are attached to hosts that belong to one or both of these groups, as indicated in the figure. A spanning tree for the leftmost router is shown in Fig. 5-17(b). When a process sends a multicast packet to a group, the first router examines its spanning tree and prunes it, removing all lines that do not lead to hosts that are members of the group.

  In our example, Fig. 5-17(c) shows the pruned spanning tree for group 1. Similarly, Fig. 5-17(d) shows the pruned spanning tree for group 2. Multicast packets are forwarded only along the appropriate spanning tree.

ROUTING FOR MOBILE HOSTS
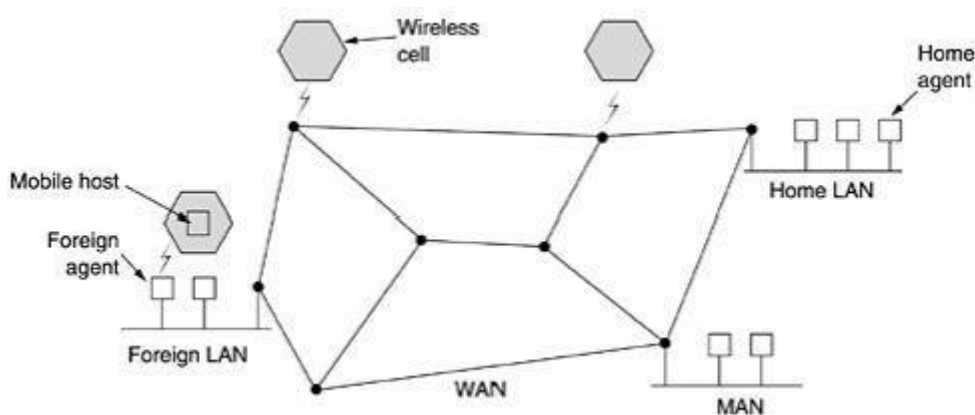
Hosts that never move are said to be stationary.

They are connected to the network by copper wires or fiber optics. In contrast, we can distinguish two other kinds of hosts.

Migratory hosts are basically stationary hosts who move from one fixed site to another from time to time but use the network only when they are physically connected to it. Roaming hosts actually compute on the run and want to maintain their connections as they move around. We will use the term mobile hosts to mean either of the latter two categories, that is, all hosts that are away from home and still want to be connected

The registration procedure typically works like this:

 1. Periodically, each foreign agent broadcasts a packet announcing its existence and address. A newly-arrived mobile host may wait for one of these messages, but if none arrives quickly enough, the mobile host can broadcast a packet saying: Are there any foreign agents around?

 2. The mobile host registers with the foreign agent, giving its home address, current data link layer address, and some security information.

3. The foreign agent contacts the mobile host's home agent and says: One of your hosts is over here. The message from the foreign agent to the home agent contains the foreign agent's network address. It also includes the security information to convince the home agent that the mobile host is really there.

4. The home agent examines the security information, which contains a timestamp, to prove that it was generated within the past few seconds. If it is happy, it tells the foreign agent to proceed.

5. When the foreign agent gets the acknowledgement from the home agent, it makes an entry in its tables and informs the mobile host that it is now registered.

ROUTING IN AD HOC NETWORKS

We have now seen how to do routing when the hosts are mobile but the routers are fixed. An even more extreme case is one in which the routers themselves are mobile.

 Among the possibilities are:

1. Military vehicles on a battlefield with no existing infrastructure.

 2. A fleet of ships at sea.

3. Emergency workers at an earthquake that destroyed the infrastructure.

4. A gathering of people with notebook computers in an area lacking 802.11.

In all these cases, and others, each node consists of a router and a host, usually on the same computer. Networks of nodes that just happen to be near each other are called ad hoc networks or MANETs (Mobile Ad hoc NETworks).

What makes ad hoc networks different from wired networks is that all the usual rules about fixed topologies, fixed and known neighbours, fixed relationship between IP address and location, and more are suddenly tossed out the window.

Routers can come and go or appear in new places at the drop of a bit. With a wired network, if a router has a valid path to some destination, that path continues to be valid indefinitely (barring a failure somewhere in the system).

With an ad hoc network, the topology may be changing all the time.

 A variety of routing algorithms for ad hoc networks have been proposed. One of the more interesting ones is the AODV (Ad hoc On-demand Distance Vector) routing algorithm (Perkins and Royer, 1999).

It takes into account the limited bandwidth and low battery life found in environment. Another unusual characteristic is that it is an on-demand algorithm, that is, it determines a route to some destination only when somebody wants to send a packet to that destination. Let us now see what that means

Route Discovery
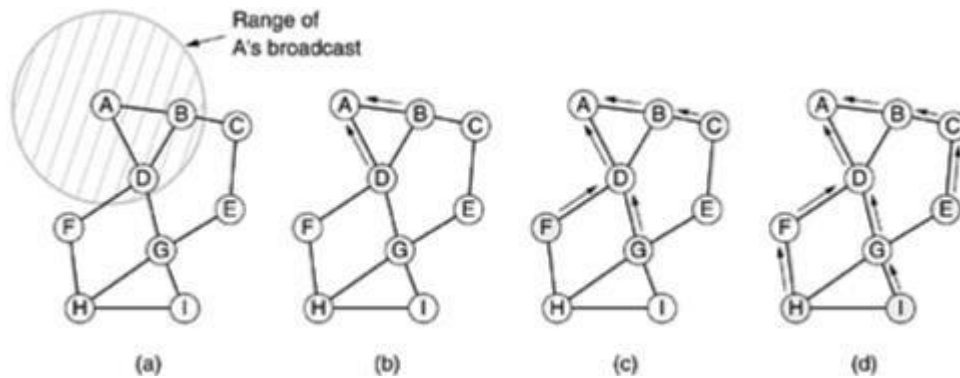
(a) Range of A's broadcast. (b) After B and D have received A's broadcast. (c) After C, F, and G have received A's broadcast. (d) After E, H, and I have received A's broadcast. The shaded nodes are new recipients. The arrows show the possible reverse routes.

To locate I, A constructs a special ROUTE REQUEST packet and broadcasts it. The packet reaches B and D, as illustrated in Fig. 5-20(a). The format of the ROUTE REQUEST packet is shown in Fig. 5-21

Format of a ROUTE REQUEST packet.

Source address	Request ID	Destination address	Source sequence #	Dest. sequence #	Hop count

The format of the ROUTE REQUEST packet is shown in Fig. 5-21. It contains the source and destination addresses, typically their IP addresses, which identify who is looking for whom. It also contains a Request ID, which is a local counter maintained separately by each node and incremented each time a ROUTE REQUEST is broadcast. Together, the Source address and Request ID fields uniquely identify the ROUTE REQUEST packet to allow nodes to discard any duplicates they may receive.

Format of a ROUTE REPLY packet

Source address	Destination address	Destination sequence #	Hop count	Lifetime

In addition to the Request ID counter, each node also maintains a second sequence counter incremented whenever a ROUTE REQUEST is sent (or a reply to someone else's ROUTE REQUEST). It functions a little bit like a clock and is used to tell new routes from old routes. The fourth field of Fig. 5-21 is A's sequence counter; the fifth field is the most recent value of I's sequence number that A has seen (0 if it has never seen it).

The use of these fields will become clear shortly. The final field, Hop count, will keep track of how many hops the packet has made. It is initialized to 0.

1. No route to I is known.
2. The sequence number for I in the ROUTE REPLY packet is greater than the value in the routing table.
3. The sequence numbers are equal but the new route is shorter

CONGESTION CONTROL ALGORITHMS

Introduction

As Internet can be considered as a Queue of packets, where transmitting nodes are constantly adding packets and some of them (receiving nodes) are removing packets from the queue. So, consider a situation where too many packets are present in this queue (or internet or a part of internet), such that constantly transmitting nodes are pouring packets at a higher rate than receiving nodes are removing them. This degrades the performance, and such a situation is termed as Congestion. Main reason of congestion is more number of packets into the network than it can handle. So, the objective of congestion control can be summarized as to maintain the number of packets in the network below the level at which performance falls off dramatically. The nature of a Packet switching network can be summarized in following points: • A network of queues • At each node, there is a queue of packets for each outgoing channel • If packet arrival rate exceeds the packet transmission rate, the queue size grows without bound • When the line for which packets are queuing becomes more than 80% utilized, the queue length grows alarmingly When the number of packets dumped into the network is within the carrying capacity, they all are delivered, expect a few that have too be rejected due to transmission errors). And then the number delivered is proportional to the number of packets sent. However, as traffic increases too far, the routers are no longer able to cope, and they begin to lose packets. This tends to make matter worse. At very high traffic, performance collapse completely, and almost no packet is delivered. In the following sections, the causes of congestion, the effects of congestion and various congestion control techniques are discussed in detail.

Causes Of Congestion

Congestion can occur due to several reasons. For example, if all of a sudden a stream of packets arrive on several input lines and need to be out on the same output line, then a long queue will be build up for that output. If there is insufficient memory to hold these packets, then packets will be lost (dropped). Adding more memory also may not help in certain situations. If router have an infinite amount of memory even then instead of congestion being reduced, it gets worse; because by the time packets gets at the head of the queue, to be dispatched out to the output line, they have already timed-out (repeatedly), and duplicates may also be present. All the packets will be forwarded to next router up to the destination, all the way only increasing the load to the network more and more. Finally when it arrives at the destination, the packet will be discarded, due to time out, so instead of been dropped at any

intermediate router (in case memory is restricted) such a packet goes all the way up to the destination, increasing the network load throughout and then finally gets dropped there.

Slow processors also cause Congestion. If the router CPU is slow at performing the task required for them (Queuing buffers, updating tables, reporting any exceptions etc.), queue can build up even if there is excess of line capacity. Similarly, LowBandwidth lines can also cause congestion. Upgrading lines but not changing slow processors, or vice-versa, often helps a little; these can just shift the bottleneck to some other point. The real problem is the mismatch between different parts of the system.

Congestion tends to feed upon itself to get even worse. Routers respond to overloading by dropping packets. When these packets contain TCP segments, the segments don't reach their destination, and they are therefore left unacknowledged, which eventually leads to timeout and retransmission.

So, the major cause of congestion is often the bursty nature of traffic. If the hosts could be made to transmit at a uniform rate, then congestion problem will be less common and all other causes will not even led to congestion because other causes just act as an enzyme which boosts up the congestion when the traffic is bursty (i.e., other causes just add on to make the problem more serious, main cause is the bursty traffic).

This means that when a device sends a packet and does not receive an acknowledgment from the receiver, in most the cases it can be assumed that the packets have been dropped by intermediate devices due to congestion. By detecting the rate at which segments are sent and not acknowledged, the source or an intermediate router can infer the level of congestion on the network. In the following section we shall discuss the ill effects of congestion.

Effects of Congestion

Congestion affects two vital parameters of the network performance, namely throughput and delay. In simple terms, the throughput can be defined as the percentage utilization of the network capacity. Figure 7.5.1(a) shows how throughput is affected as offered load increases. Initially throughput increases linearly with offered load, because utilization of the network increases. However, as the offered load increases beyond certain limit, say 60% of the capacity of the network, the throughput drops. If the offered load increases further, a point is reached when not a single packet is delivered to any destination, which is commonly known as deadlock situation. There are three curves in Fig. 7.5.1(a), the ideal one corresponds to the situation when all the packets introduced are delivered to their destination up to the maximum capacity of the network. The second one corresponds to the situation when there is no congestion control. The third one is the case when some congestion control technique is used. This prevents the throughput collapse, but provides lesser throughput than the ideal condition due to overhead of the congestion control technique.

The delay also increases with offered load, as shown in Fig. 7.5.1(b). And no matter what technique is used for congestion control, the delay grows without bound as the load approaches the capacity of the system. It may be noted that initially there is longer delay when congestion control policy is applied. However, the network without any congestion control will saturate at a lower offered load.
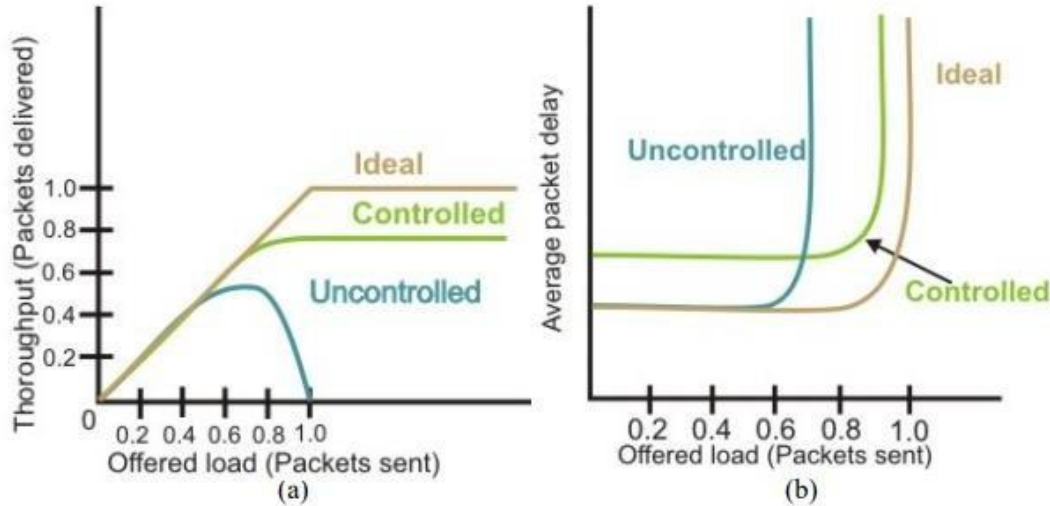
Figure 7.5.1 (a) Effect of congestion on throughput (b) Effect of congestion on delay

Congestion Control Techniques

Congestion control refers to the mechanisms and techniques used to control congestion and keep the traffic below the capacity of the network. As shown in Fig. 7.5.2, the congestion control techniques can be broadly classified two broad categories:

• Open loop: Protocols to prevent or avoid congestion, ensuring that the system (or network under consideration) never enters a Congested State.

• Close loop: Protocols that allow system to enter congested state, detect it, and remove it.
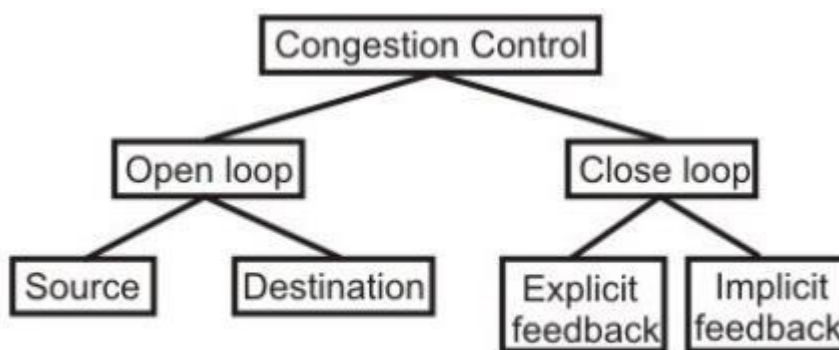
Figure 7.5.2 Congestion control categories

The first category of solutions or protocols attempt to solve the problem by a good design, at first, to make sure that it doesn't occur at all. Once system is up and running midcourse corrections are not made. These solutions are somewhat static in nature, as the policies to control congestion don't change much according to the current state of the system. Such Protocols are also known as Open Loop solutions. These rules or policies include

deciding upon when to accept traffic, when to discard it, making scheduling decisions and so on. Main point here is that they make decision without taking into consideration the current state of the network. The open loop algorithms are further divided on the basis of whether these acts on source versus that act upon destination.

The second category is based on the concept of feedback. During operation, some system parameters are measured and feed back to portions of the subnet that can take action to reduce the congestion. This approach can be divided into 3 steps:
 • Monitor the system (network) to detect whether the network is congested or not and what's the actual location and devices involved.
• To pass this information to the places where actions can be taken
 • Adjust the system operation to correct the problem.

These solutions are known as Closed Loop solutions. Various Metrics can be used to monitor the network for congestion. Some of them are: the average queue length, number of packets that are timed-out, average packet delay, number of packets discarded due to lack of buffer space, etc. A general feedback step would be, say a router, which detects the congestion send special packets to the source (responsible for the congestion) announcing the problem. These extra packets increase the load at that moment of time, but are necessary to bring down the congestion at a later time. Other approaches are also used at times to curtail down the congestion. For example, hosts or routers send out probe packets at regular intervals to explicitly ask about the congestion and source itself regulate its transmission rate, if congestion is detected in the network. This kind of approach is a pro-active one, as source tries to get knowledge about congestion in the network and act accordingly.

Yet another approach may be where instead of sending information back to the source an intermediate router which detects the congestion send the information about the congestion to rest of the network, piggy backed to the outgoing packets. This approach will in no way put an extra load on the network (by not sending any kind of special packet for feedback). Once the congestion has been detected and this information has been passed to a place where the action needed to be done, then there are two basic approaches that can overcome the problem. These are: either to increase the resources or to decrease the load. For example, separate dial-up lines or alternate links can be used to increase the bandwidth between two points, where congestion occurs. Another example could be to decrease the rate at which a particular sender in transmitting packets out into the network.

The closed loop algorithms can also be divided into two categories, namely explicit feedback and implicit feedback algorithms. In the explicit approach, special packets are sent back to the sources to curtail down the congestion. While in implicit approach, the source itself acts pro-actively and tries to deduce the existence of congestion by making local observations. In the following sections we shall discuss about some of the popular algorithms from the above categories

In the following sections we shall discuss about some of the popular algorithms from the above categories.

Leaky Bucket Algorithm

Consider a Bucket with a small hole at the bottom, whatever may be the rate of water pouring into the bucket, the rate at which water comes out from that small hole is constant. This scenario is depicted in figure 7.5.3(a). Once the bucket is full, any additional water entering it spills over the sides and is lost (i.e. it doesn't appear in the output stream through the hole underneath). The same idea of leaky bucket can be applied to packets, as shown in Fig. 7.5.3(b). Conceptually each network interface contains a leaky bucket. And the following steps are performed:

 • When the host has to send a packet, the packet is thrown into the bucket.
• The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
 • Bursty traffic is converted to a uniform traffic by the leaky bucket.
 • In practice the bucket is a finite queue that outputs at a finite rate.

This arrangement can be simulated in the operating system or can be built into the hardware. Implementation of this algorithm is easy and consists of a finite queue. Whenever a packet arrives, if there is room in the queue it is queued up and if there is no room then the packet is discarded.
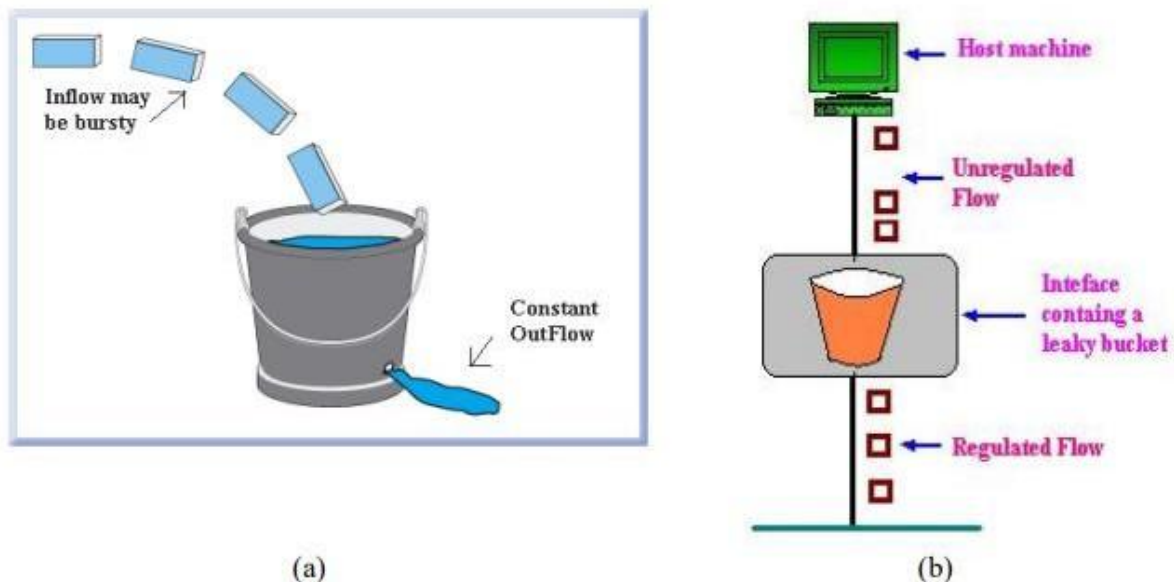
Figure 7.5.3(a) Leaky bucket (b) Leaky bucket implementation

Token Bucket Algorithm

The leaky bucket algorithm described above, enforces a rigid pattern at the output stream, irrespective of the pattern of the input. For many applications it is better to allow the output to speed up somewhat when a larger burst arrives than to loose the data. Token Bucket algorithm provides such a solution. In this algorithm leaky bucket holds token, generated at regular intervals. Main steps of this algorithm can be described as follows:

ƒ In regular intervals tokens are thrown into the bucket.

ƒ The bucket has a maximum capacity.

ƒ If there is a ready packet, a token is removed from the bucket, and the packet is send.

ƒ If there is no token in the bucket, the packet cannot be send.

Figure 7.5.4 shows the two scenarios before and after the tokens present in the bucket have been consumed. In Fig. 7.5.4(a) the bucket holds two tokens, and three packets are waiting to be sent out of the interface, in Fig. 7.5.4(b) two packets have been sent out by consuming two tokens, and 1 packet is still left.

The token bucket algorithm is less restrictive than the leaky bucket algorithm, in a sense that it allows bursty traffic. However, the limit of burst is restricted by the number of tokens available in the bucket at a particular instant of time.

The implementation of basic token bucket algorithm is simple; a variable is used just to count the tokens. This counter is incremented every t seconds and is decremented whenever a packet is sent. Whenever this counter reaches zero, no further packet is sent out as shown in Fig. 7.5.5.
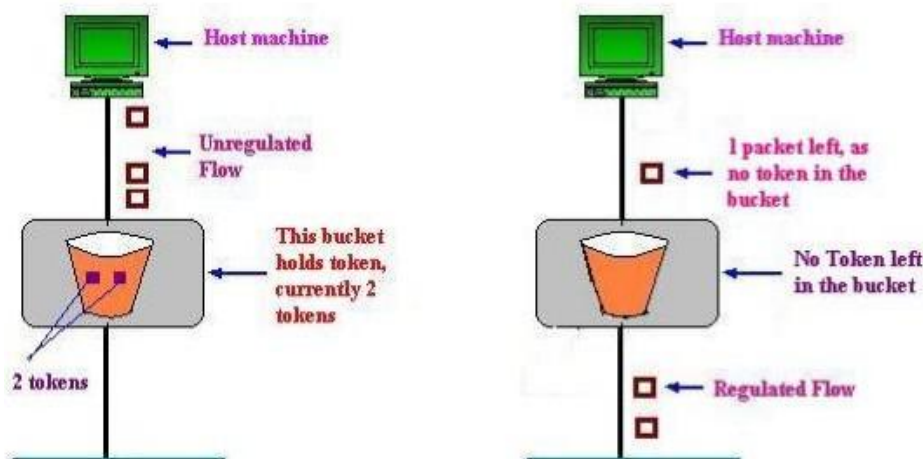

Figure 7.5.4(a) Token bucket holding two tokens, before packets are send out, (b) Token bucket after two packets are send, one packet still remains as no token is left
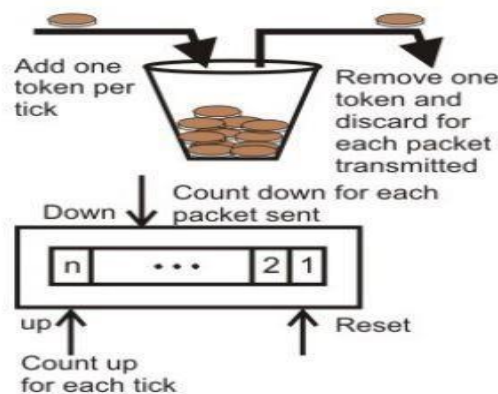

Figure 7.5.5 Implementation of the Token bucket algorithm

COMPUTER NETWORKS

What is IP?

Here, IP stands for **internet protocol**. It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.

An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP and UDP/IP, so internet protocol is also known as TCP/IP or UDP/IP.

The first version of IP (Internet Protocol) was IPv4. After IPv4, IPv6 came into the market, which has been increasingly used on the public internet since 2006.

History of Internet Protocol

The development of the protocol gets started in 1974 by **Bob Kahn and Vint Cerf**. It is used in conjunction with the Transmission Control Protocol (TCP), so they together named the TCP/IP.

The first major version of the internet protocol was IPv4, which was version 4. This protocol was officially declared in RFC 791 by the Internet Engineering Task Force (IETF) in 1981.

After IPv4, the second major version of the internet protocol was IPv6, which was version 6. It was officially declared by the IETF in 1998. The main reason behind the development of IPv6 was to replace IPv4. There is a big difference between IPv4 and IPv6 is that IPv4 uses 32 bits for addressing, while IPv6 uses 128 bits for addressing.

Function

The main function of the internet protocol is to provide addressing to the hosts, encapsulating the data into a packet structure, and routing the data from source to the destination across one or more IP networks. In order to achieve these functionalities, internet protocol provides two major things which are given below.

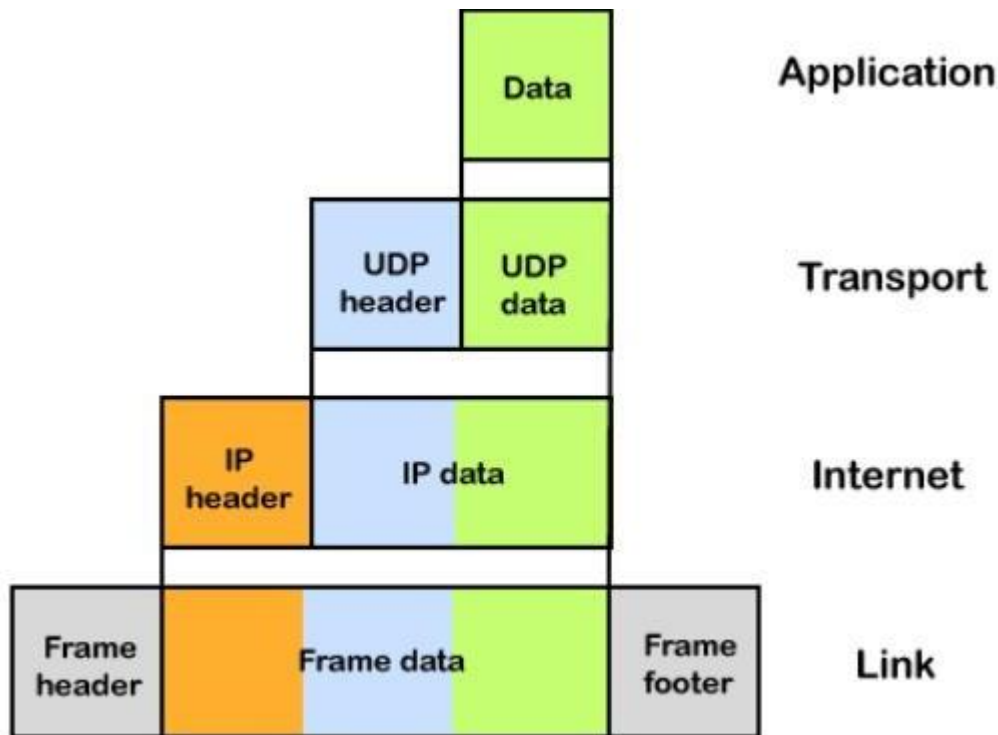### An internet protocol defines two things:

- o   Format of IP packet
- o   IP Addressing system

What is an IP packet?

Before an IP packet is sent over the network, two major components are added in an IP packet, i.e., **header** and a **payload**.

An IP header contains lots of information about the IP packet which includes:

- Source IP address: The source is the one who is sending the data.

- Destination IP address: The destination is a host that receives the data from the sender.

- Header length

- Packet length

- TTL (Time to Live): The number of hops occurs before the packet gets discarded.

- Transport protocol: The transport protocol used by the internet protocol, either it can be TCP or UDP.

There is a total of 14 fields exist in the IP header, and one of them is optional.

Payload: Payload is the data that is to be transported.

How does the IP routing perform?

IP routing is a process of determining the path for data so that it can travel from the source to the destination. As we know that the data is divided into multiple packets, and each packet will pass through a web of the router until it reaches the final destination. The path that the data packet follows is determined by the routing algorithm. The routing algorithm considers various factors like the size of the packet and its header to determine the efficient route for the data from the source to the destination. When the data packet reaches some router, then the source address and destination address are used with a routing table to determine the next hop's address. This process goes on until it reaches the destination. The data is divided into multiple packets so all the packets will travel individually to reach the destination.

For example, when an email is sent from the email server, then the TCP layer in this email server divides the data into multiple packets, provides numbering to these packets and transmits them to the IP layer. This IP layer further transmits the packet to the destination email server. On the side of the destination server, the IP layer transmits these data packets to the TCP layer, and the TCP layer recombines these data packets into the message. The message is sent to the email application.

What is IP Addressing?

An IP address is a unique identifier assigned to the computer which is connected to the internet. Each IP address consists of a series of characters like 192.168.1.2. Users cannot access the domain name of each website with the help of these characters, so DNS resolvers are used that convert the human-readable domain names into a series of characters. Each IP packet contains two addresses, i.e., the IP address of the device, which is sending the packet, and the IP address of the device which is receiving the packet.

Types of IP addresses

IPv4 addresses are divided into two categories:

- **Public address**
- **Private address**

Public address

The public address is also known as an external address as they are grouped under the WAN addresses. We can also define the public address as a way to communicate outside the network. This address is used to access the internet. The public address available on our computer provides the remote access to our computer. With the help of a public address, we can set up the home server to access the internet. This address is generally assigned by the ISP (Internet Service Provider).

Key points related to public address are:

- The scope of the public address is global, which means that we can communicate outside the network.

- This address is assigned by the ISP (Internet Service Provider).

- It is not available at free of cost.

- We can get the Public IP by typing on Google "What is my IP".

Private address

A private address is also known as an internal address, as it is grouped under the LAN addresses. It is used to communicate within the network. These addresses are not routed on the internet so that no traffic can come from the internet to this private address. The address space for the private address is allocated using **InterNIC** to create our own network. The private addresses are assigned to mainly those computers, printers, smartphones, which are kept inside the home or the computers that are kept within the organization. For example, a private address is assigned to the printer, which is kept inside our home, so that our family member can take out the print from the printer.

If the computer is assigned with a private address, then the devices available within the local network can view the computer through the private ip address. However, the devices available outside the local network

cannot view the computer through the private IP address, but they can access the computer if they know the router's public address. To access the computer directly, NAT (Network Address Translator) is to be used.

Key points related to private address are:

- o   Its scope is local, as we can communicate within the network only.

- o   It is generally used for creating a local area network.

- o   It is available at free of cost.

- o   We can get to know the private IP address by simply typing the "ipconfig" on the command prompt.

Subnetting in Networking-

Subnetting is the practice of dividing a network into two or smaller networks. It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.

IP Subnetting designates high-order bits from the host as part of the network prefix. This method divides a network into smaller subnets.

It also helps you to reduce the size of the routing tables, which is stored in routers. This method also helps you to extend the existing IP address base & restructures the IP address.

Why Use Subnetting?

Here are important reasons for using Subnetting:

- It helps you to maximise IP addressing efficiency.
- Extend the life of IPV4.
- Public IPV4 Addresses are scarce.
- IPV4 Subnetting reduces network traffic by eliminating collision and broadcast traffic and thus improves overall performance.
- This method allows you to apply network security policies at the interconnection between subnets.
- Optimized IP network performance.
- Facilitates spanning of large geographical distances.
- Subnetting process helps to allocate IP addresses that prevent large numbers of IP network addresses from remaining unused.
- Subnets are usually set up geographically for specific offices or particular teams within a business that allows their network traffic to stay within the location.

What is Subnet Mask?

A subnet mask is a 32 bits address used to distinguish between a network address and a host address in IP address. A subnet mask identifies which part of an IP address is the network address and the host address. They are not shown inside the data packets traversing the Internet. They carry the destination IP address, which a router will match with a subnet.

Valid Subnet Masks

| Subnet Value	Bit Value							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Two types of subnet masks are:

- The default Subnet Mask is the number of bits which is reserved by the address class. Using this default mask will accommodate a single network subnet in the relative class.
- A Custom Subnet Mask can be defined by an administrator to accommodate many Network

How to Use a Subnet Mask?

The subnet mask is used by the router to cover up the network address. It shows which bits are used to identify the subnet.

Every network has its own unique address, Like here, class B network has network address 172.20.0.0, which has all zeroes in the host portion of the address.

Example IP address: 11000001. Here 1st and 2nd bits are 1, and the 3rd bit is 0; hence, it is class C.
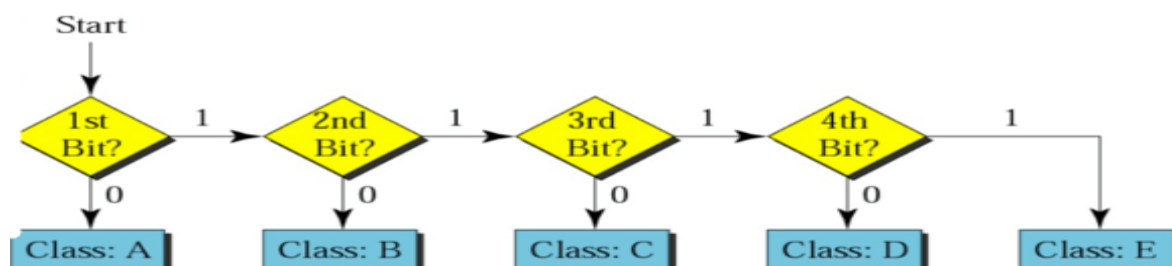
Above example shows how IP addresses should be deconstructed, which makes it simple for Internet routers to find the right Network to route data into. However, in a Class A network there could be millions of connected devices, and it could take some time for the router to find the right device.

Methods of Subnet Masking

We can subnet the masking process in two ways: Straight or Short-cut.

1) Straight

You should use the binary notation method for both the address and the mask and then apply the AND operation to get the block address.

2) Short-Cut Method

- In case the byte in the mask is 255, you need to copy the byte in the destination address.
- When the byte in the mask is 0, then you need to replace the byte in the address with 0.
- When the byte in the mask is neither 255 nor 0, then you should write the mask and the address in binary and use the AND operation.
- In case if the extracted network address matches the local network ID, and the destination is located on the local Network. However, if they do not match, the message must be routed outside the local Network.

Class	Default subnet mask	No. of networks	No. of host per network
A	255.0.0.0	256	16,777,214
B	255.255.0.0	65,536	65,534
C	255.255.255.0	16,77,216	126

UNIT III

Transport Layer

- The transport layer is a 4th layer from the top.

- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.

- The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.

- The transport layer protocols are implemented in the end systems but not in the network routers.

- A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.

- All transport layer protocols provide multiplexing/demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.

- Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols. Both TCP and UDP will then communicate with the internet protocol in the internet layer. The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.
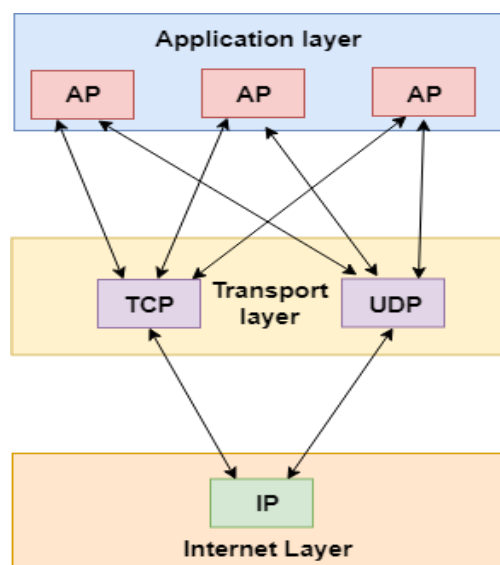
Services provided by the Transport Layer

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

- o End-to-end delivery
- o Addressing
- o Reliable delivery
- o Flow control
- o Multiplexing
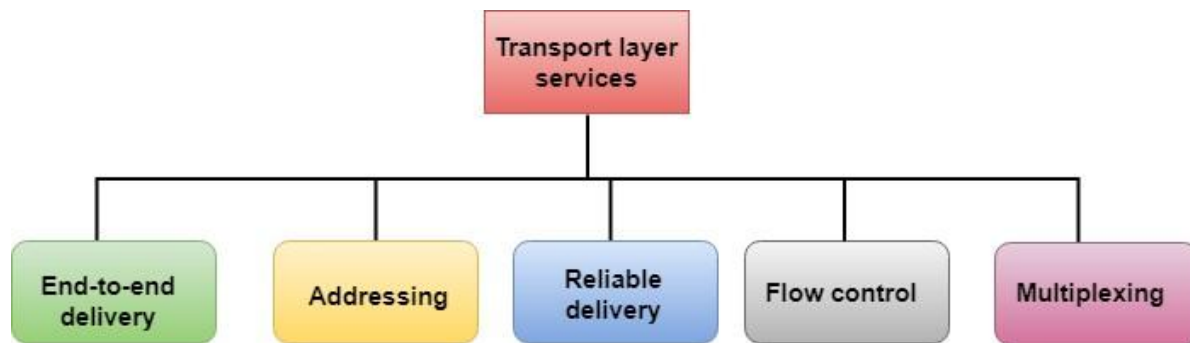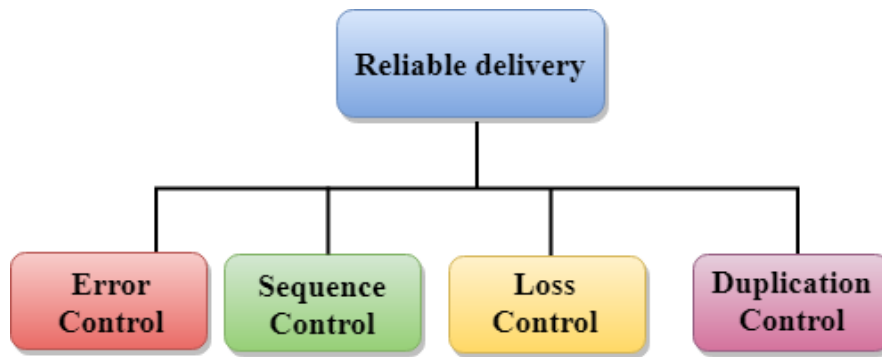

End-to-end delivery:

The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

Reliable delivery:

The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects:

- o Error control
- o Sequence control
- o Loss control
- o Duplication control

Error Control

- o The primary role of reliability is **Error Control**. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.

- o The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.

- o The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.
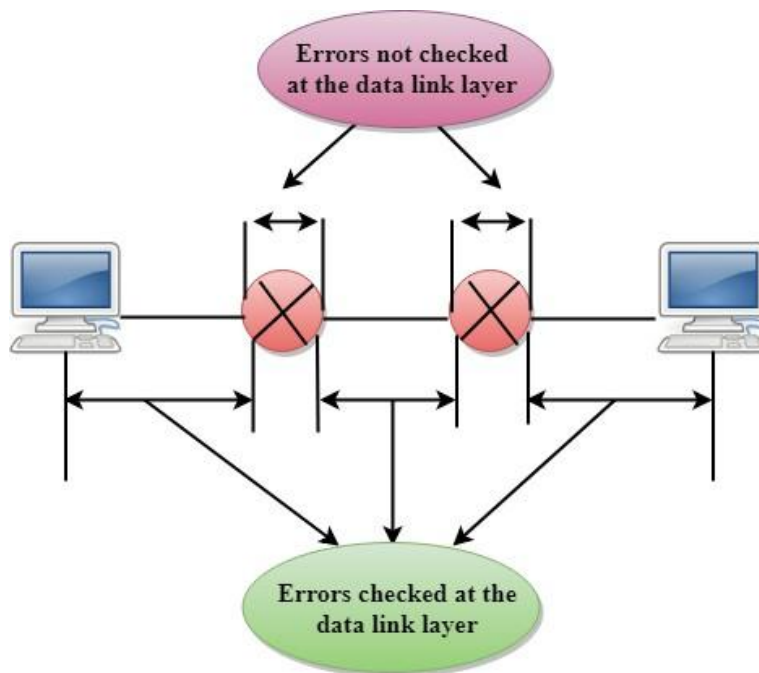
Sequence Control

- The second aspect of the reliability is sequence control which is implemented at the transport layer.

- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

Loss Control

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.

Duplication Control

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Flow Control

Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Multiplexing

The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.

Upward
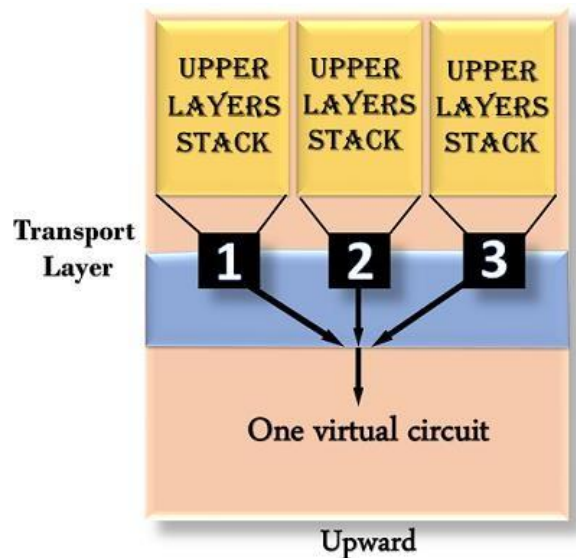
- o **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

Downward
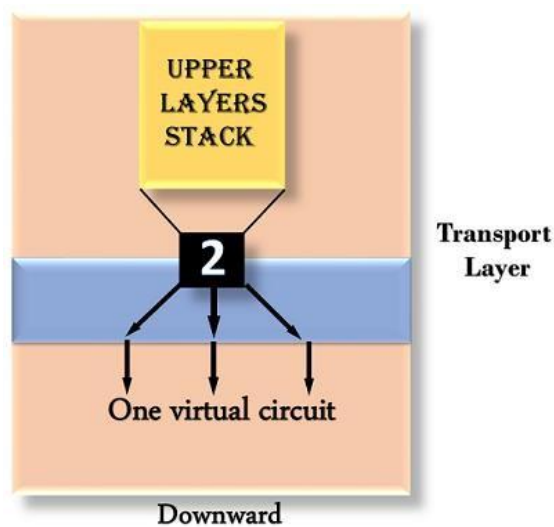
Addressing

- o According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.

o   The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.

o   The transport layer protocols need to know which upper-layer protocols are communicating.
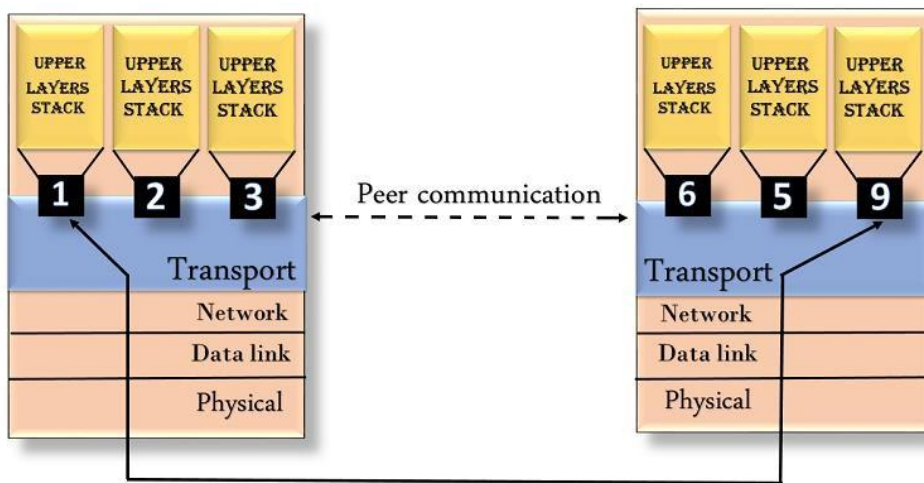
Transport Layer protocols

o   The transport layer is represented by two protocols: TCP and UDP.

o   The IP protocol in the network layer delivers a datagram from a source host to the destination host.

o   Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.

o   An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.

o   Each port is defined by a positive integer address, and it is of 16 bits.

UDP
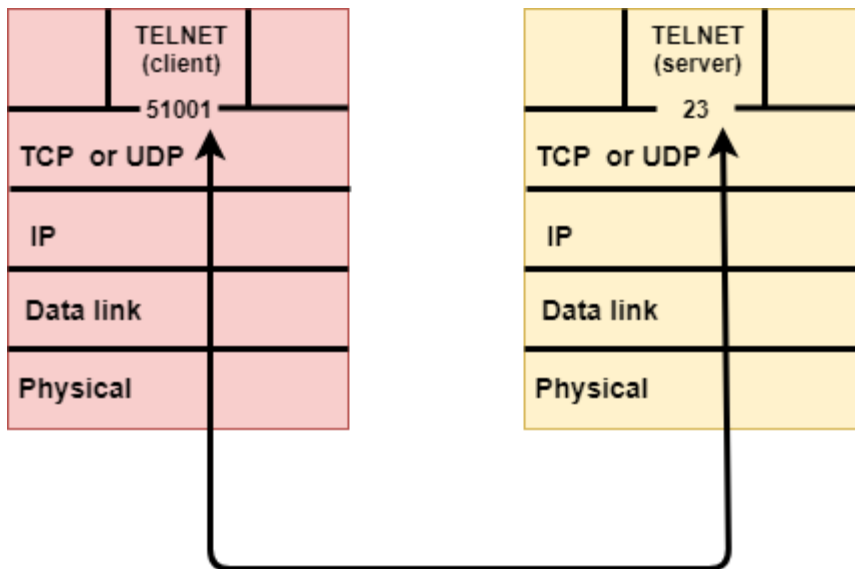
- o   UDP stands for **User Datagram Protocol**.
- o   UDP is a simple protocol and it provides nonsequenced transport functionality.
- o   UDP is a connectionless protocol.
- o   This type of protocol is used when reliability and security are less important than speed and size.
- o   UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- o   The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:

Where,

- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.

- **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.

- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.

- **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.

- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.

- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

TCP

- TCP stands for Transmission Control Protocol.

- It provides full transport layer services to applications.

- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.

- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination. The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.

- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.

- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.

- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.

- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:

  - Establish a connection between two TCPs.

  - Data is exchanged in both the directions.

  - The Connection is terminated.

Source port address 16 bits								Destination port address 16 bits
Sequence number 32 bits								
Acknowledgement number 32 bits								
HLEN 4 bits	Reserved 6 bits	URG	ACK	PSH	RST	SYN	FIN	Window size 16 bits
Checksum 16 bits								Urgent pointer 16 bits
Options & padding								

Where,

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.

- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.

- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.

- o **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.

- o **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.

- o **Reserved:** It is a six-bit field which is reserved for future use.

- o **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

here are total six types of flags in control field:

- o **URG:** The URG field indicates that the data in a segment is urgent.

- o **ACK:** When ACK field is set, then it validates the acknowledgement number.

- o **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.

- o **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.

- o **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement.

- o **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.

    - o **Window Size:** The window is a 16-bit field that defines the size of the window.

    - o **Checksum:** The checksum is a 16-bit field used in error detection.

    - o **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.

    - o **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

Differences b/w TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

<u>Quality of Service</u> (QoS)

In one word, **Quality of Service** (QoS) can be referred as **efficiency**. We define Quality of Service as "**How well or efficiently data transmissions are taking place**".

So the question arises "How can we improve our network's efficiency?" or "How can we improve our Quality of Service?". It can be achieved by **managing data traffic** which results in **reduced packet loss**, **latency**, and jitter on the respective network. This is all done by setting up priorities for specific types of data that traverse through the network.

The enterprise networks or commercial networks (*networks which connects all the users and the system connected through a local area network, to the applications in the data center*) they provide services in the form of applications, for example, WhatsApp, from which we can send and receive various kinds of data, like audio, video, text, etc. Organizations like this use Quality of Service to **meet the traffic requirements** which results in the prevention of the degradation of the quality, which can be caused by packet loss, delay, and jitter.

How to achieve Quality of Service?

Let's get into some details and say, your organization wants to achieve Quality of Service, which can be done by using some tools and techniques, like **jitter buffer** and **traffic shaping**.

Jitter buffer

This is a **temporary storage buffer** which is used to store the incoming data packets, it is used in **packet-based networks** to ensure that the **continuity of the data streams** doesn't get disturbed, it does that by **smoothing out the packet arrival** times during periods of network congestion.

Traffic shaping

This technique which is also known as **packet shaping**, is a **congestion control or management technique** that helps to regulate network data transfer by delaying the flow of least important or least necessary data packets.

QoS is included in the service-level agreement when an organization signs it with its network service provider which guarantees the selected performance level.

There are 2 types of Quality of Service Solutions:

1. **Stateless solution:** Here, the server is not required to keep or store the server information or session details to itself. The **routers** maintain no fine-grained state about traffic, one positive factor of this is, that it's **scalable and robust**. But also, it has weak services as there is **no guarantee about the kind of performance delay** in a particular application which we encounter. In the stateless solution, the server and client are **loosely coupled** and can act.
2. **Stateful solution:** Here, the server is required to maintain the **current state and session information**, the **routers maintain per-flow state** as the flow is very important in providing the Quality-of-Service which is providing powerful services such as guaranteed services and high resource utilization, provides protection, and is much **less scalable and robust**. Here, the server and client are **tightly bounded**.

Quality of Service Parameters:

QoS can be measured quantitatively by using several parameters

- **Packet loss:** it happens when the network links become congested and the routers and switches start dropping the packets. When these packets are dropped during real-time communication, such as audio or video, these sessions can experience jitter and gaps in speech.
- **Jitter:** occurs as the result of network congestion, timing drift, and route changes. And also, too much jitter can degrade the quality of audio communication.
- **Latency:** is the time delay, which is taken by a packet to travel from its source to its destination. For a great system, latency should be as low as possible, ideally, it should be close to zero.
- **Bandwidth:** is the capacity of a network channel to transmit maximum possible data through the channel in a certain amount of time. QoS optimizes a network by managing its bandwidth and setting the priorities for those applications which require more resources as compared to other applications.
- **Mean opinion score:** it is a metric for rating the audio quality which uses a five-point scale, with a five indicating the highest or best quality.

Implementing Quality of Service:

We can implement Quality of service through three of the following existing models:

1. **Best Effort**: if we are applying this model then, it means that we are prioritizing all the data packets equally. But since we all setting the priority order like this, then there is no guarantee that all the data packets will be delivered, but it will put up the best effort to deliver all of them. Point to remember is, that the best-effort model is applied when networks haven't configured with the QoS policies or incase their network infrastructure does not support QoS.
2. **Integrated Services**: or IntServ, this QoS model reserves the bandwidth along a specific path on the network. The applications ask the network's resource reservation for themselves and parallelly the network devices monitor the flow of packets to make sure network resources can accept packets. Point to remember: while implementing Integrated Services Model, the IntServ-capable routers and resource reservation protocol is necessary. This model has limited scalability and high consumption of the network resources.
3. **Differentiated Services**: in this QoS model, the network elements such as routers and switches are configured to serve multiple categories of traffic with different priority orders. A company can categorize the network traffic based on its requirements. Eg. Assigning higher priority to audio traffic etc.

Common Network Performance Problems

1. High CPU Usage

The CPU or Central Processing Unit is the key component of the computer that is responsible for receiving and processing instructions for systems and applications. High CPU usage on a network is a warning bell for slow network performance. The most common cause of high CPU usage is the network is being bogged down by enormous amounts of traffic. CPU usage spikes when processes require longer to execute or when many network packets are exchanges throughout the network. When the CPU is overused, latency, jitter and packet loss may increase which will result in the entire IT infrastructure to deteriorate. The Fix There are devices such as switches that have hardware components (ASICs and NPUs) that can take some of the responsibilities off the CPU. They can take charge and process packets quickly.

2. High bandwidth Usage

Bandwidth is the network's capacity to exchange data between devices within a given period. Higher bandwidth enables faster data exchange and allows more devices to be connected at once. When someone, or something, is monopolizing the bandwidth by downloading gigabytes worth of data, it creates a congestion. When there is congestion, there isn't enough bandwidth left for other parts or users, which then leads to problems like slow speeds. The Fix Instead of increasing the bandwidth, it is best to first see what is eating away at it in the first place. If there is a faulty system which is eroding the bandwidth and you go ahead and increase it, it will continue to eat away leaving you with the same cyclical problem. Therefore, Monitoring the network to get to the root of the problem is always a good start.

3. Poor Physical Connectivity

It is basic, but the last thing you will check – the cables. Testing all your cables one by one to look for damages can be a nightmare. Nevertheless, when a cable or connector is defective, the interface of the network equipment to which it is connected will show errors. The Fix A simple way to monitor

cables on a defective connector is to have a network monitoring solution that will measure errors on all network interfaces and send warning signals in case of potential problems.

4. **Malfunctioning**

Devices Another common network problem is when devices or hardware equipment is not functioning properly, perhaps due to misconfiguration or redundancy. It is important to consistently check switches and devices on your network to ensure they are working optimally, so you can react quickly when they are not. The Fix Make sure all your devices are up to date. Replace old devices and hardware equipment on time. When you install new devices to the network, test it and make sure it is configured properly. Many performance issues are caused by misconfigurations that can turn into major problems down the line.

5. **DNS Problems**

DNS, Domain Name System, is essentially a directory that matches domain names to IP addresses. Every website has its own IP address on the web, and computers can connect to other computers via the internet and look up websites using their IP addresses. DNS errors occur when you cannot connect to an IP address, signaling you may have lost your internet access or network. For instance, your site may appear online to you, but offline to your visitors. The inability to access the internet or sites can have a significant impact on your business. It is thus very importance to find and fix problems as soon as possible. The Fix Network monitoring solutions proactively monitor all devices, equipment, system and applications of a network. A complete network overview will allow easy spotting and fixing of DNS and other network problems.

DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- o DNS stands for Domain Name System.
- o DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- o DNS is required for the functioning of the internet.
- o Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- o DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- o For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.
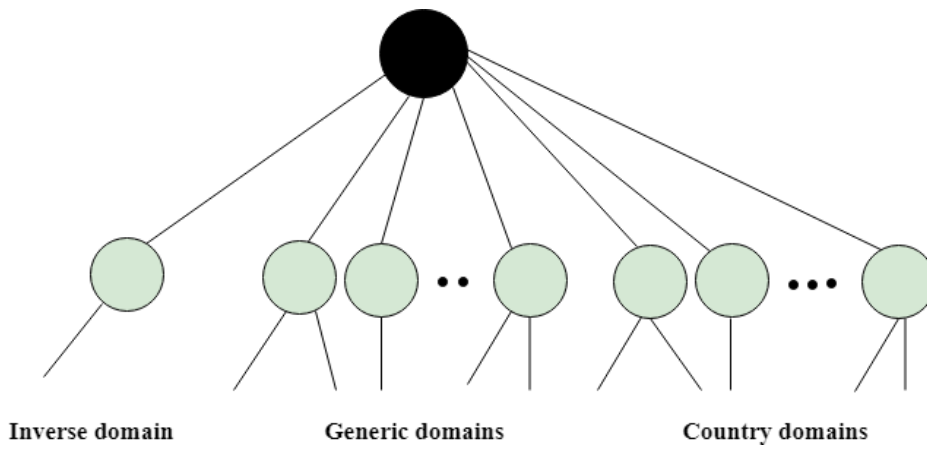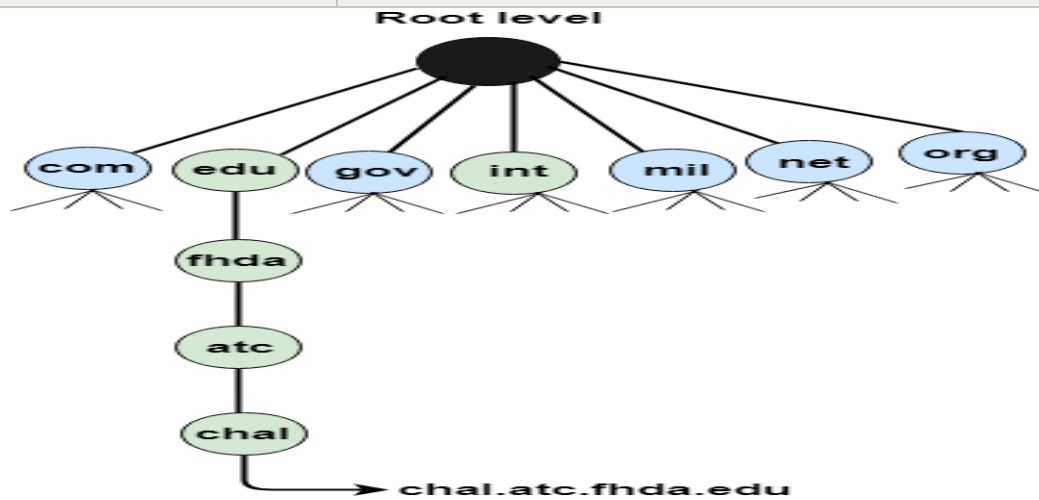
Generic Domains

- o It defines the registered hosts according to their generic behavior.

- o Each node in a tree defines the domain name, which is an index to the DNS database.

- o It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups

museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations

chal.atc.fhda.edu

Country Domain
The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain
The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- o DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.

- o Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.

- o DNS implements a distributed database to store the name of all the hosts available on the internet.

- o If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

SNMP

- o SNMP stands for **Simple Network Management Protocol**.
- o SNMP is a framework used for managing devices on the internet.
- o It provides a set of operations for monitoring and managing the internet.

SNMP Concept
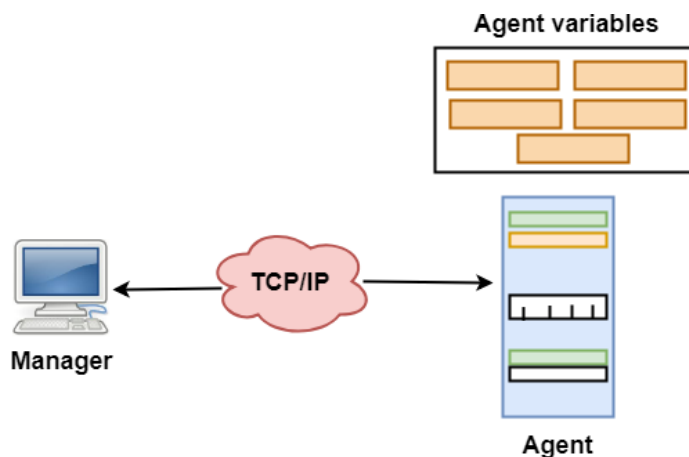
- o SNMP has two components Manager and agent.
- o The manager is a host that controls and monitors a set of agents such as routers.

- It is an application layer protocol in which a few manager stations can handle a set of agents.
- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

Managers & Agents

- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

Management with SNMP has three basic ideas:

- A manager checks the agent by requesting the information that reflects the behavior of the agent.
- A manager also forces the agent to perform a certain function by resetting values in the agent database.
- An agent also contributes to the management process by warning the manager regarding an unusual condition.

Management Components

- Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base).
- Management is a combination of SMI, MIB, and SNMP. All these three protocols such as abstract syntax notation 1 (ASN.1) and basic encoding rules (BER).
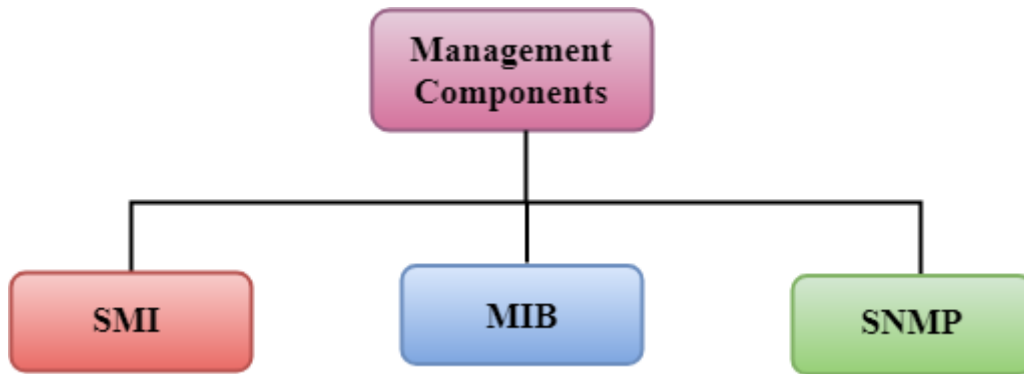
SMI

The SMI (Structure of management information) is a component used in network management. Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.

MIB

- The MIB (Management information base) is a second component for the network management.

- Each agent has its own MIB, which is a collection of all the objects that the manager can manage. MIB is categorized into eight groups: system, interface, address translation, ip, icmp, tcp, udp, and egp. These groups are under the mib object.
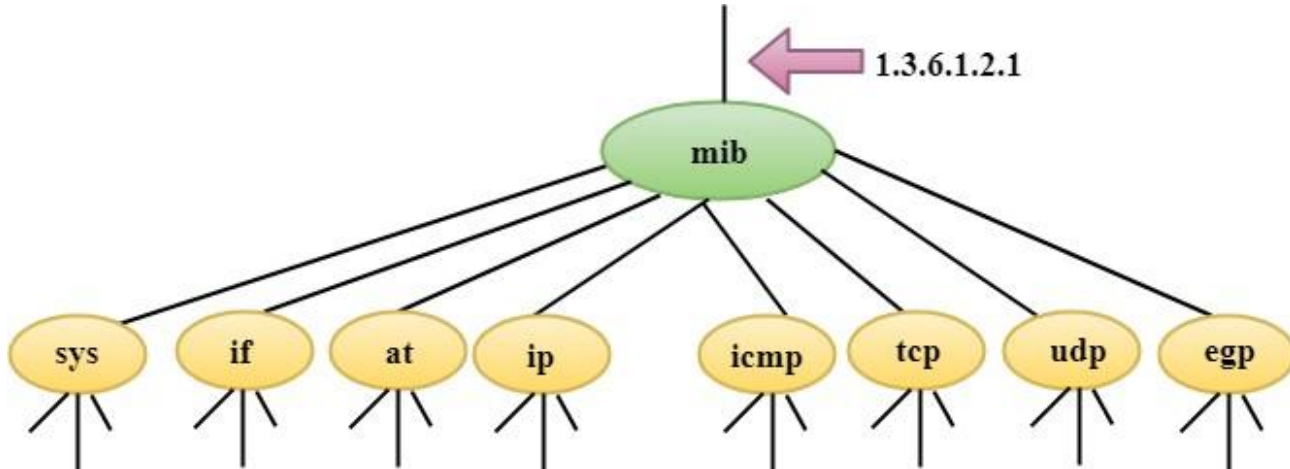
SNMP

SNMP defines five types of messages: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.
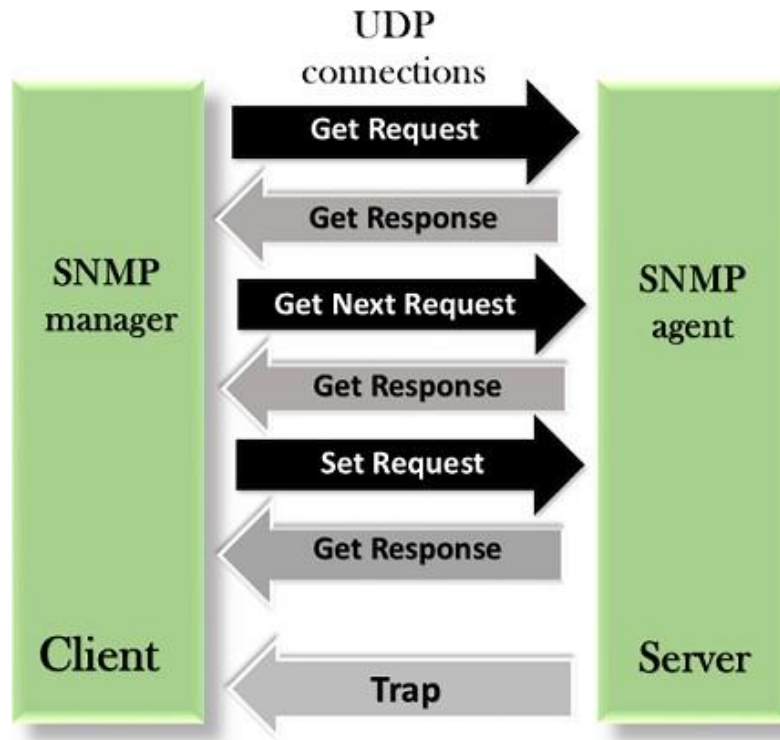
GetRequest: The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.

GetNextRequest: The GetNextRequest message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table. If the manager does not know the indexes of the entries, then it will not be able to retrieve the values. In such situations, GetNextRequest message is used to define an object.

GetResponse: The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This message contains the value of a variable requested by the manager.

SetRequest: The SetRequest message is sent from a manager to the agent to set a value in a variable.

Trap: The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.

Electronic Mail

What is E-mail?

E-mail is defined as the transmission of messages on the Internet. It is one of the most commonly used features over communications networks that may contain text, files, images, or other attachments. Generally, it is information that is stored on a computer sent through a network to a specified individual or group of individuals.

Email messages are conveyed through email servers; it uses multiple protocols within the TCP/IP suite. For example, SMTP is a protocol, stands for simple mail transfer protocol and used to send messages whereas other protocols IMAP or POP are used to retrieve messages from a mail server. If you want to login to your mail account, you just need to enter a valid email address, password, and the mail servers used to send and receive messages.

Although most of the webmail servers automatically configure your mail account, therefore, you only required to enter your email address and password. However, you may need to manually configure each account if you use an email client like Microsoft Outlook or Apple Mail. In addition, to enter the email address and password, you may also need to enter incoming and outgoing mail servers and the correct port numbers for each one.

- o **Message envelope:** It depicts the email's electronic format.
- o **Message header:** It contains email subject line and sender/recipient information.
- o **Message body:** It comprises images, text, and other file attachments.

The email was developed to support rich text with custom formatting, and the original email standard is only capable of supporting plain text messages. In modern times, email supports HTML (Hypertext markup language), which makes it capable of emails to support the same formatting as websites. The email that supports HTML can contain links, images, CSS layouts, and also can send files or "email attachments" along with messages. Most of the mail servers enable users to send several attachments with each message. The attachments were typically limited to one megabyte in the early days of email. Still, nowadays, many mail servers are able to support email attachments of 20 megabytes or more in size.

FTP

- o FTP stands for File transfer protocol.
- o FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- o It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- o It is also used for downloading the files to computer from other servers.

Objectives of FTP

- o It provides the sharing of files.
- o It is used to encourage the use of remote computers.
- o It transfers the data more reliably and efficiently.

Why FTP?

Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP
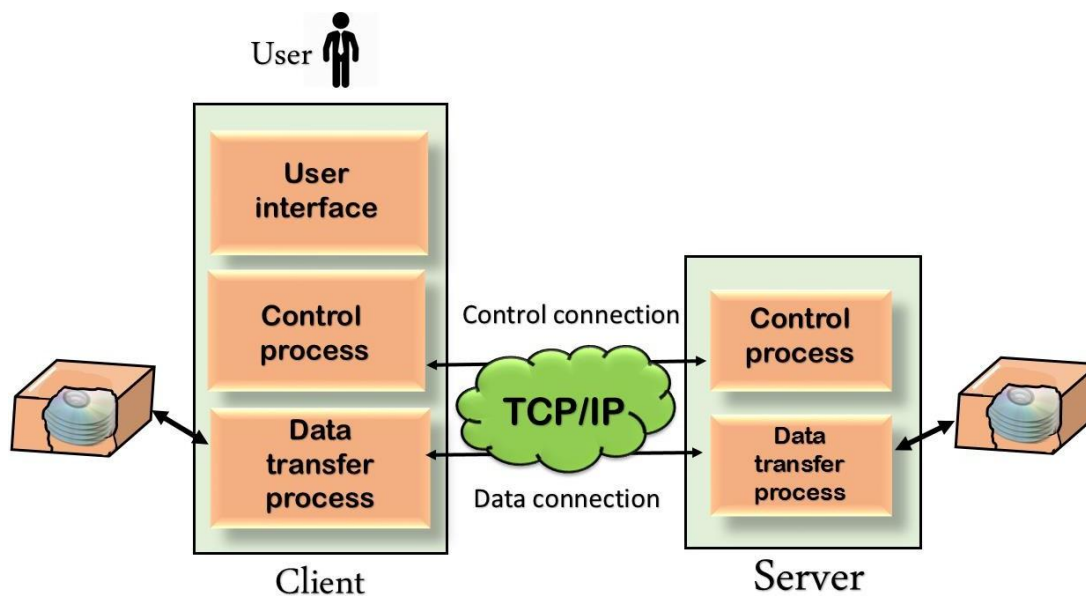
The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:
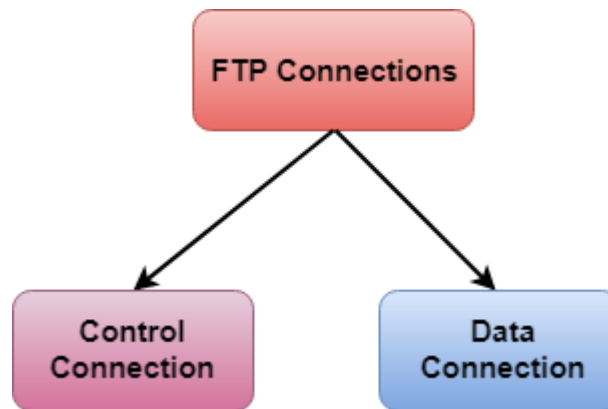
- o **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

- o **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

- o FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.

- o It allows a user to connect to a remote host and upload or download the files.

- o It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.

- o The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- o **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.

- o **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.

- o **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.

- o **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- o The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.

- o FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.

- o Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.

- o It is not compatible with every system.

Trivial File Transfer Protocol (TFTP) is a simple protocol used for transferring files. TFTP uses the User Datagram Protocol (UDP) to transport data from one end to another. TFTP is mostly used to read and write files/mail to or from a remote server.

File transfer is one of the most essential technologies for client/server and computer network infrastructures.

Trivial File Transfer Protocol is very simple in design and has limited features as compared to File Transfer Protocol (FTP). TFTP provides no authentication and security while transferring files. As a result, it is usually used for transferring boot files or configuration files between

machines in a local setup. Because of its simple design, it is rarely used interactively by users in a computer network. Its lack of security also makes it dangerous for use over the Internet.

TFTP is very useful for boot computers and devices that do not have hard disk drives or storage devices because it can easily be implemented using a small amount of memory. This characteristic of TFTP makes it one of the core elements of network boot protocol, or preboot execution environment (PXE).

Data transfer through TFTP is usually initiated through port 69. However, the data transfer ports are selected by the sender and receiver when the connection is initialized.

BOOTP

BOOTP stands for **Bootstrap Protocol.** and **DHCP** stands for <u>Dynamic host configuration protocol</u>. These protocols square measure used for getting the information science address of the host along side the bootstrap info. The operating of each protocols is totally different in some manner.Dynamic host configuration protocol is also the extended version of the Bootstrap Protocol.
BOOTP stands for **Bootstrap Protocol.** and **DHCP** stands for <u>Dynamic host configuration protocol</u>. These protocols square measure used for getting the information science address of the host along side the bootstrap info. The operating of each protocols is totally different in some manner.Dynamic host configuration protocol is also the extended version of the Bootstrap Protocol.
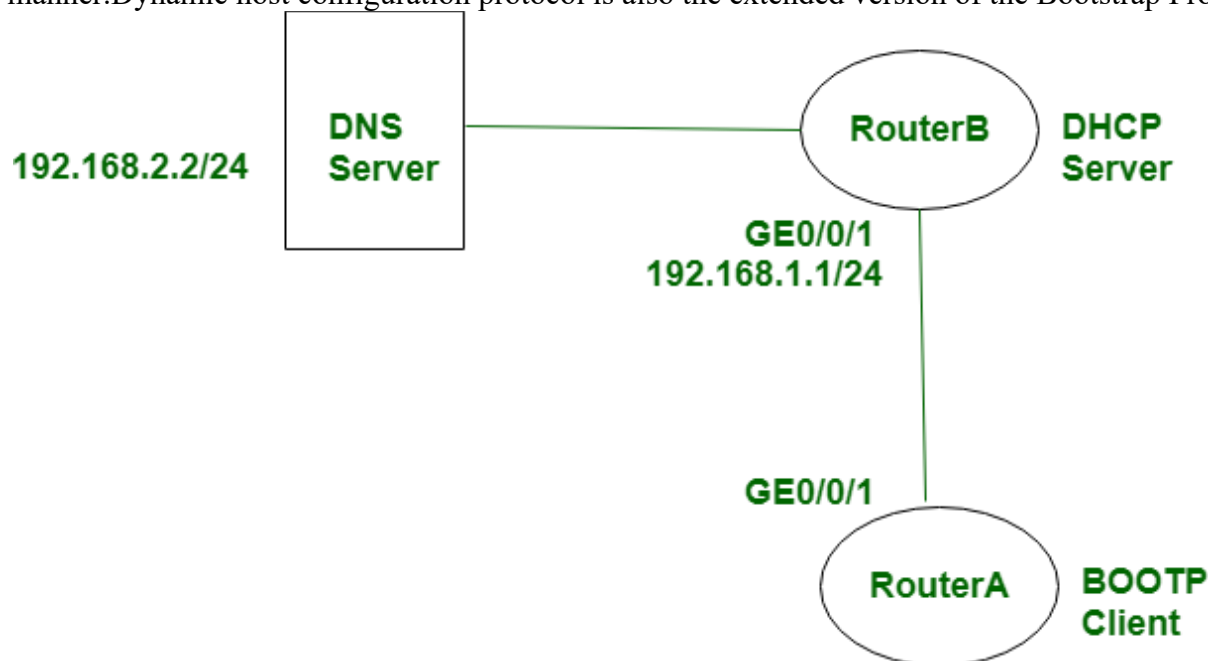
Difference between that BOOTP and DHCP:

S.NO	BOOTP	DHCP
1.	BOOTP stands for Bootstrap Protocol.	While DHCP stands for Dynamic host configuration protocol.
2.	BOOTP does not provide temporary IP addressing.	While DHCP provides temporary IP addressing for only limited amount of time.
3.	BOOTP does not support DHCP clients.	While it support BOOTP clients.
4.	In BOOTP, manual-configuration takes place.	While in DHCP, auto-configuration takes place.
5.	BOOTP does not support mobile machines.	Whereas DHCP supports mobile machines.
6.	BOOTP can have errors due to manual-configuration.	Whereas in DHCP errors do not occure mostly due to auto-configuration.

Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.

Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

Basic Features

There are three basic features that make HTTP a simple but powerful protocol:

- **HTTP is connectionless:** The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client waits for the response. The server processes the request and sends a response back after which client disconnect the connection. So client and server knows about each other during current request and response only. Further requests are made on new connection like client and server are new to each other.

- **HTTP is media independent:** It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type.

- **HTTP is stateless:** As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.

HTTP/1.0 uses a new connection for each request/response exchange, where as HTTP/1.1 connection may be used for one or more request/response exchanges.

Basic Architecture

The following diagram shows a very basic architecture of a web application and depicts where HTTP sits:
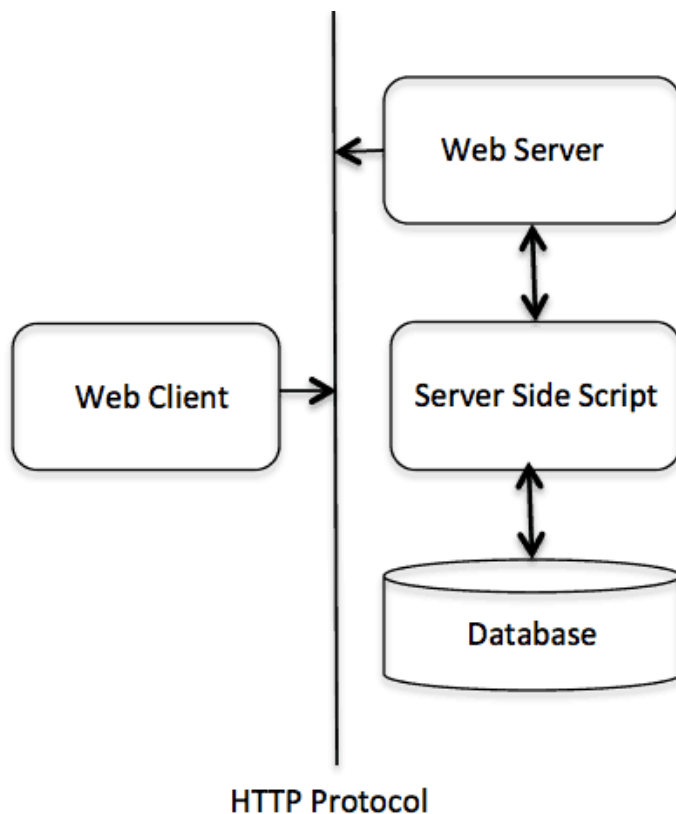
HTTP Protocol

The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients, and the Web server acts as a server.

Client

The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.

Server

 The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

World Wide Web?

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. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.

The building blocks of the Web are web pages which are formatted in HTML and connected by links called "hypertext" or hyperlinks and accessed by HTTP. These links are electronic connections that link related pieces of information so that users can access the desired information quickly. Hypertext offers the advantage to select a word or phrase from text and thus to access other pages that provide additional information related to that word or phrase.

A web page is given an online address called a Uniform Resource Locator (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., *www.facebook.com*, *www.google.com*, etc. So, the World Wide Web is like a huge electronic book whose pages are stored on multiple servers across the world.

Small websites store all of their WebPages on a single server, but big websites or organizations place their WebPages on different servers in different countries so that when users of a country search their site they could get the information quickly from the nearest server.

So, the web provides a communication platform for users to retrieve and exchange information over the internet. Unlike a book, where we move from one page to another in a sequence, on World Wide Web we follow a web of hypertext links to visit a web page and from that web page to move to other web pages. You need a browser, which is installed on your computer, to access the Web.

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply
A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.
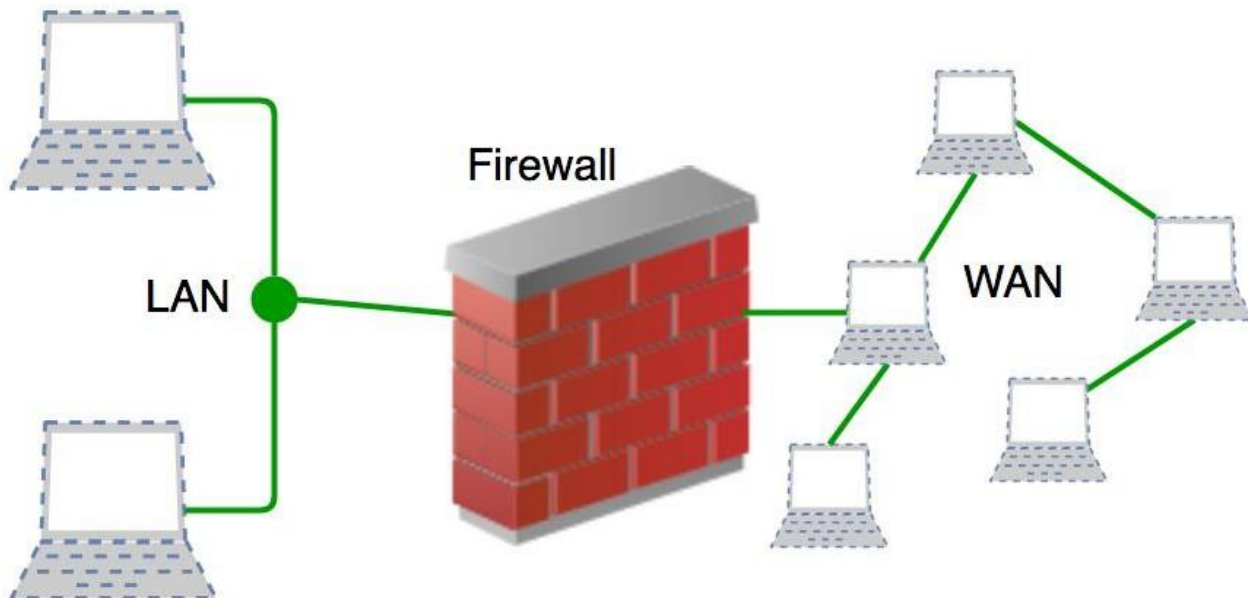
Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.
But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How Firewall Works
Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.
From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.
Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these

three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).

Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

Generation of Firewall

Firewalls can be categorized based on its generation.

1. **First Generation- Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).
   Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

   Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

   1. Incoming packets from network 192.168.21.0 are blocked.
   2. Incoming packets destined for internal TELNET server (port 23) are blocked.
   3. Incoming packets destined for host 192.168.21.3 are blocked.
   4. All well-known services to the network 192.168.21.0 are allowed.
2. **Second Generation- Stateful Inspection Firewall :** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection

travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

3. **Third Generation- Application Layer Firewall :** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.
   In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.
   Note: Application layer firewalls can also be used as Network Address Translator(NAT).

4. **Next Generation Firewalls (NGFW) :** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

UNIT IV (CN)

Over View of Repeaters

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.
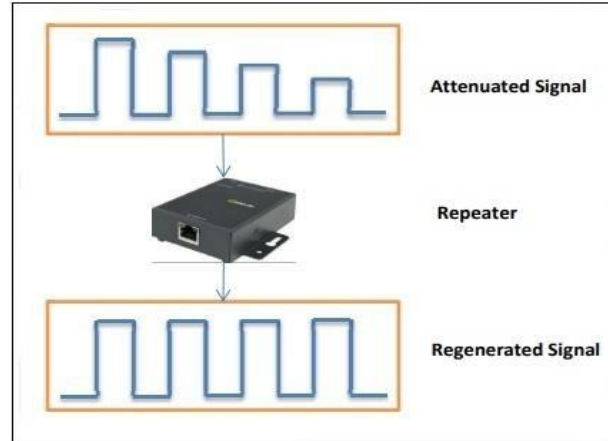
Why are Repeaters needed?

When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.

Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss.So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN. This is shown in the following diagram −
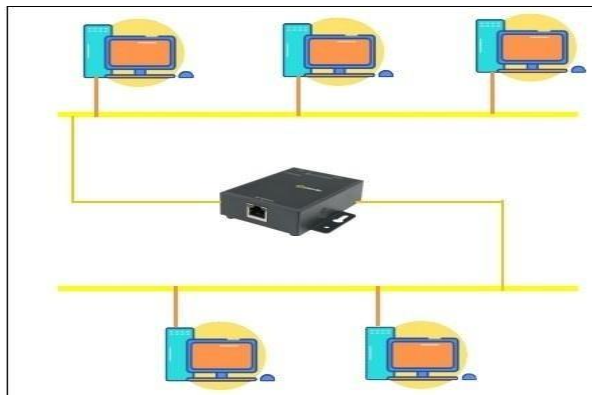
Types of Repeaters

According to the types of signals that they regenerate, repeaters can be classified into two categories

- **Analog Repeaters** − They can only amplify the analog signal.
- **Digital Repeaters** − They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types −

- **Wired Repeaters** − They are used in wired LANs.
- **Wireless Repeaters** − They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

- **Local Repeaters** − They connect LAN segments separated by small distance.
- **Remote Repeaters** − They connect LANs that are far from each other.

Advantages of Repeaters

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don't require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

Disadvantages of Repeaters

- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

Bridges

A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.

The following diagram shows a bridges connecting two LANs −
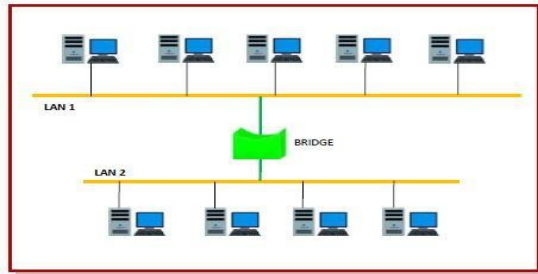

Uses of Bridge

- Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.
- By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
- Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
  - If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.
  - If the frame has a destination MAC address in a connected network, it will forward the frame toward it.
- By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
- In cases where the destination MAC address is not available, bridges can broadcast data frames to each node. To discover new segments, they maintain the MAC address table.
- In order to provide full functional support, bridges ideally need to be transparent. No major hardware, software or architectural changes should be required for their installation.
- Bridges can switch any kind of packets, be it IP packets or AppleTalk packets, from the network layer above. This is because bridges do not examine the payload field of the data frame that arrives, but simply looks at the MAC address for switching.
- Bridges also connect virtual LANs (VLANs) to make a larger VLAN.
- A wireless bridge is used to connect wireless networks or networks having a wireless segment.

Routers

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

Router Connecting Two Networks
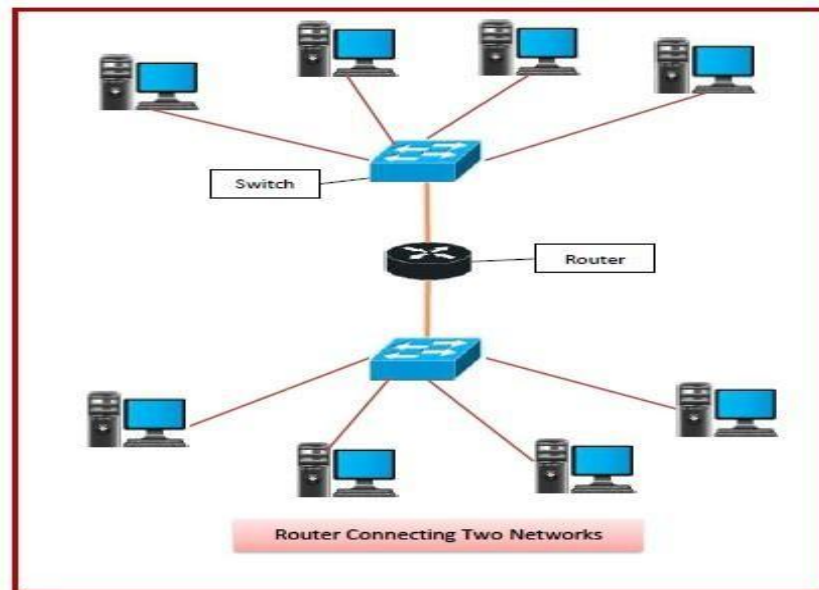
Features of Routers

- A router is a layer 3 or network layer device.

- It connects different networks together and sends data packets from one network to another.

- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).

- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.

- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.

- In order to prepare or refresh the routing table, routers share information among each other.

- Routers provide protection against broadcast storms.

- Routers are more expensive than other networking devices like hubs,bridges and switches.

- Routers are manufactured by some popular companies like –

- Cisco
- D-Link
- HP
- 3Com
- Juniper
- Nortel

Routing Table

The functioning of a router depends largely upon the routing table stored in it. The routing table stores the available routes for all destinations. The router consults the routing table to determine the optimal route through which the data packets can be sent.

A routing table typically contains the following entities –

- IP addresses and subnet mask of the nodes in the network

- IP addresses of the routers in the network

- Interface information among the network devices and channels

Routing tables are of two types –

- **Static Routing Table** – Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.

- **Dynamic Routing Table** – Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large number of routers.

Types of Routers

A variety of routers are available depending upon their usages. The main types of routers are –

- **Wireless Router** – They provide WiFi connection WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.

- **Broadband Routers** – They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).

- **Core Routers** – They can route data packets within a given network, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.

- **Edge Routers** – They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.

- **Brouters** − Brouters are specialised routers that can provide the functionalities of bridges as well. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

Gateway

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

Gateway between a LAN and Internet
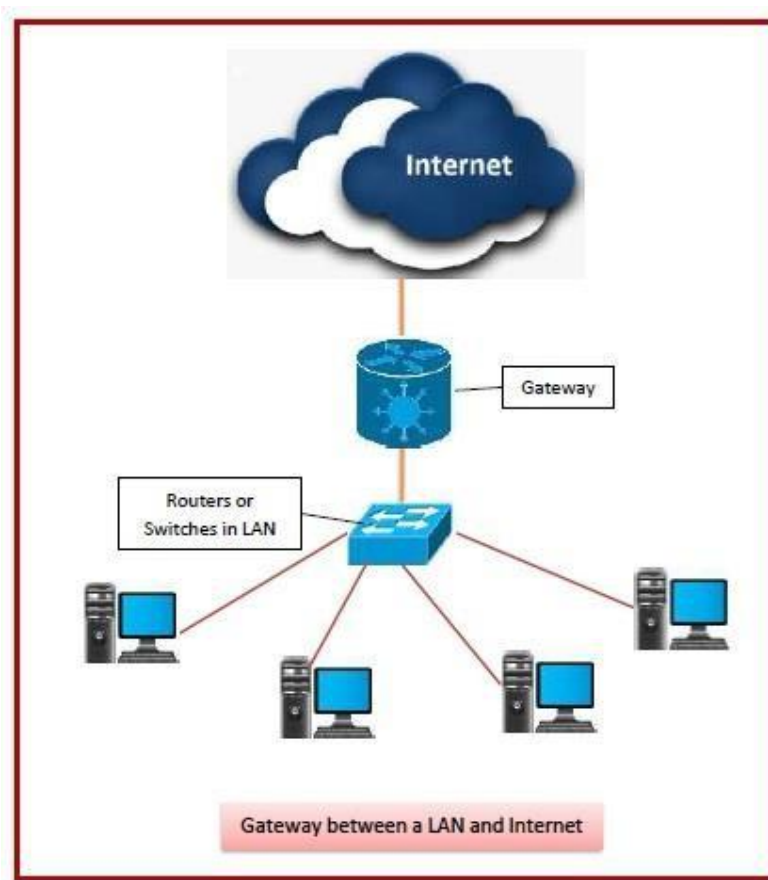
Features of Gateways

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.

- It forms a passage between two different networks operating with different transmission protocols.

- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.

- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.

- It also stores information about the routing paths of the communicating networks.

- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.

- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.

- It uses packet switching technique to transmit data across the networks.

Types of Gateways

On basis of direction of data flow, gateways are broadly divided into two categories −

- **Unidirectional Gateways** − They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.

- **Bidirectional Gateways** − They allow data to flow in both directions. They can be used as synchronization tools.

On basis of functionalities, there can be a variety of gateways, the prominent among them are as follows −

- **Network Gateway** − This is the most common type of gateway that provides as interface between two dissimilar networks operating with different protocols. Whenever the term gateway is mentioned without specifying the type, it indicates a network gateway.

- **Cloud Storage Gateway** − It is a network node or server that translates storage requests with different cloud storage service API calls, such as SOAP (Simple Object Access Protocol) or REST (REpresentational State Transfer).It facilitates integration of private cloud storage into applications without necessitating transfer of the applications into any public cloud, thus simplifying data communication.

- **Internet-To-Orbit Gateway (I2O)** − It connects devices on the Internet to satellites and spacecraft orbiting the earth. Two prominent I2O gateways are Project HERMES and Global Educational Network for Satellite Operations (GENSO).

- **IoT Gateway** − IoT gateways assimilates sensor data from IoT (Internet of Things) devices in the field and translates between sensor protocols before sending it to the cloud network. They connect IoT devices, cloud network and user applications.

- **VoiP Trunk Gateway** − It facilitates data transmission between plain old telephone service (POTS) devices like landline phones and fax machines, with VoIP (voice over Internet Protocol) network.

Both **router** and **brouter** are connecting devices in networking.

1. <u>Router</u> :
A router is a networking device that is designed to receive, analyze, and forward data packets between computer networks. A router is used to connect <u>LAN (Local Area Network)</u> and <u>WAN (Wide Area Network)</u>.

2. Brouter :
A brouter is a networking device that functions both as a bridge and a router. It can forward data between networks (serving as a bridge), but can also route data to individual systems within a network (serving as a router).

Difference between Router and Brouter

S.No	Router	Brouter
1	A router is a networking device that forwards data packets between computer network.	Brouter is a networking device which is used both as a bridge and as a router,It is combination of network bridge and a router.
2	It operates at Network layer.	It operates either at Data link layer or a Network layer.
3	Router stores routing table.	Brouter stores routing table when it is configured as a router and stores MAC address when configured as a bridge.
4	It takes forwarding decisions based on IP address.	Forwarding decision are taken based on IP address when it is configured as a router, or It takes forwarding decisions based on MAC address when configured as a bridge.
5	Router transmits data in the form of packets.	Brouter transmits data in the form of packets when it is configured as a router and It transmits data in the form of frames when configured as a bridge.
6	Router works on more than one broadcast domain.	Brouter works on more than one broadcast domain when it is configured as a router and It works on single broadcast domain when configured as a bridge.

Hubs

Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.

Broadcasting by a Hub
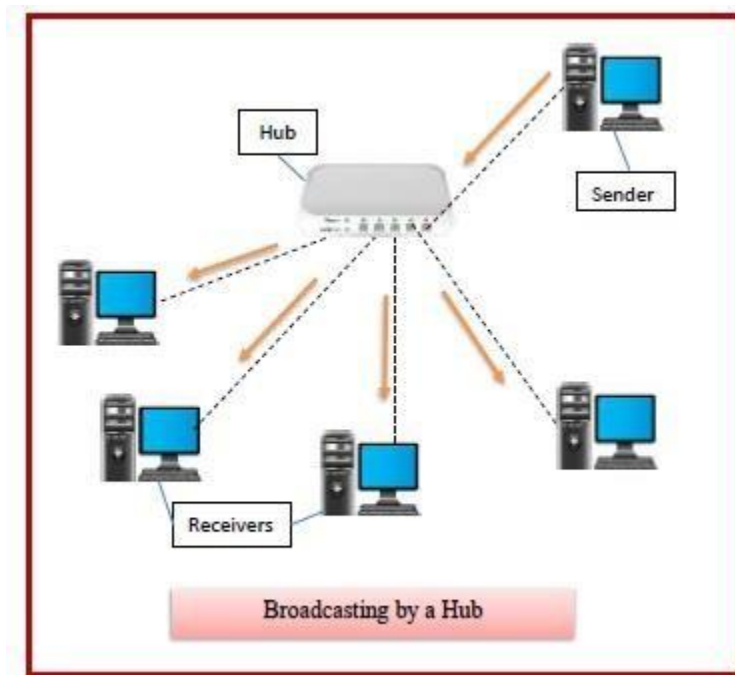
Features of Hubs

- A hub operates in the physical layer of the OSI model.

- A hub cannot filter data. It is a non-intelligent network device that sends message to all ports.

- It primarily broadcasts messages. So, the collision domain of all nodes connected through the hub stays one.

- Transmission mode is half duplex.

- Collisions may occurs during setup of transmission when more than one computers place data simultaneously in the corresponding ports.

- Since they lack intelligence to compute best path for transmission of data packets, inefficiencies and wastage occur.

- They are passive devices, they don't have any software associated with it.

- They generally have fewer ports of 4/12.

Types of Hubs

Initially, hubs were passive devices. However, with development of advanced technology, active hubs and intelligent hubs came into use.


- **Passive Hubs** − Passive hubs connects nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the LAN.

- **Active Hubs** − Active hubs amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serves both as a repeater as well as connecting centre. Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN.

- **Intelligent Hubs** − Intelligent hubs are active hubs that provide additional network management facilities. They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc.

Switches

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.

Multicasting by a Switch
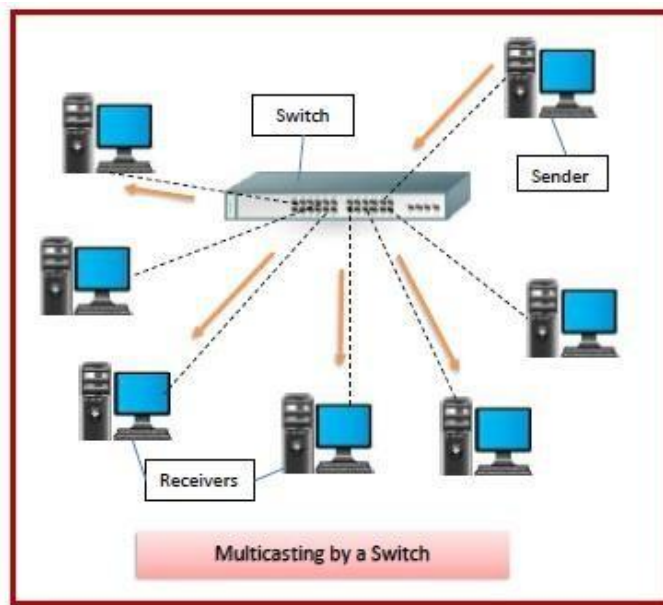
Features of Switches

- A switch operates in the layer 2, i.e. data link layer of the OSI model.

- It is an intelligent network device that can be conceived as a multiport network bridge.

- It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.

- It uses packet switching technique to receive and forward data packets from the source to the destination device.

- It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.

- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.

- Switches are active devices, equipped with network software and network management capabilities.

- Switches can perform some error checking before forwarding data to the destined port.

- The number of ports is higher – 24/48.

Types of Switches

There are variety of switches that can be broadly categorised into 4 types −
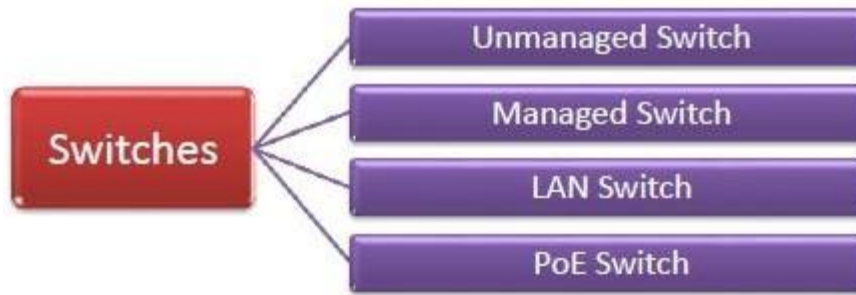
- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.

- **Managed Switch** − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.

- **LAN Switch** − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.

- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gogabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections
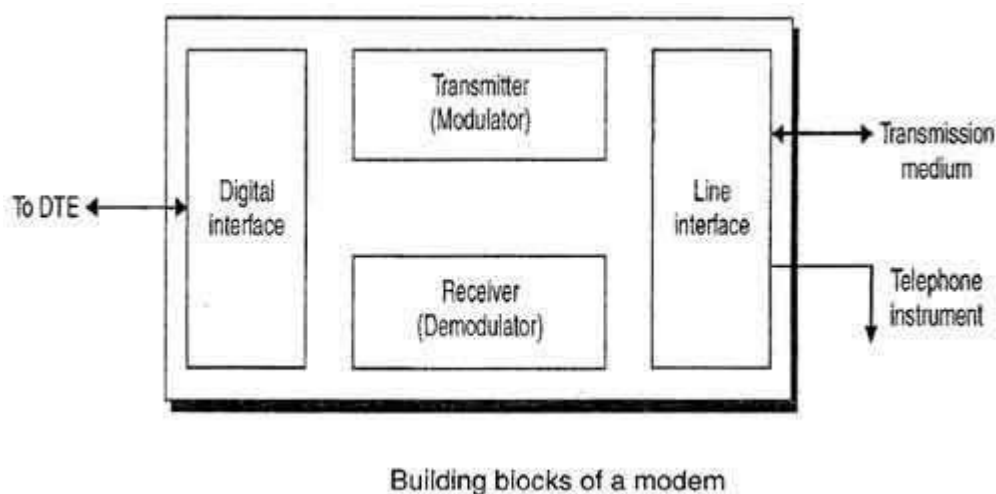
Modems

Modem is abbreviation for Modulator – De-modulator. Modems are used for data transfer from one computer network to another computer network through telephone lines. The computer network works in digital mode, while analog technology is used for carrying massages across phone lines.

Modulator converts information from **digital mode to analog mode** at the transmitting end and de-modulator converts the same from **analog to digital at receiving end**. The process of converting analog signals of one computer network into digital signals of another computer network so they can be processed by a receiving computer is **referred to as digitizing.**

When an analog facility is used for data communication between two digital devices called Data Terminal Equipment (DTE), modems are used at each end. DTE can be a terminal or a computer.

Modulation/DeModulation
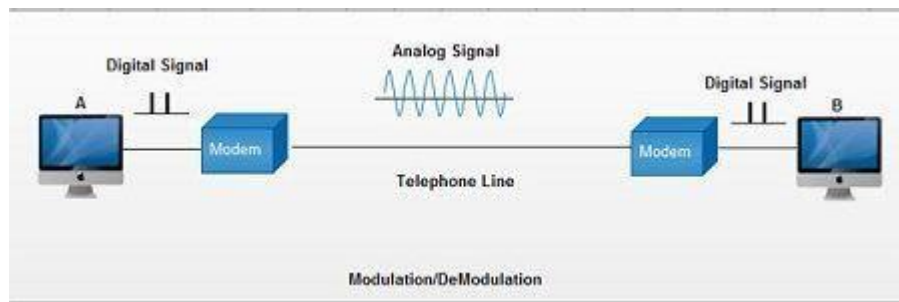
he modem at the transmitting end converts the digital signal generated by DTE into an analog signal by modulating a carrier. This modem at the receiving end demodulates the carrier and hand over the demodulated digital signal to the DTE.

Building blocks of a modem

The transmission medium between the two modems can be dedicated circuit or a switched telephone circuit. If a switched telephone circuit is used, then the modems are connected to the local telephone exchanges. Whenever data transmission is required connection between the modems is established through telephone exchanges.

Channel Service Unit/ Data Service Unit

A CSU/DSU (Channel Service Unit/Data Service Unit) is a hardware device that converts a digital data frame from the communications technology used on a local area network (LAN) into a frame appropriate to a wide-area network (WAN) and vice versa. Think of it as a high end modem which is used to connect a data terminal equipment (DTE), such as a router, to a digital circuit, such as a Digital Signal 1 (T1) line.

For example, if you have a Web business from your own home and have leased a digital line (perhaps a T-1 or fractional T-1 line) to a phone company or a gateway at an Internet service provider, you have a CSU/DSU at your end, and the phone company or gateway host has a CSU/DSU at its end, and the units at both ends must be set to the same communications standard.

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.

- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).

- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NIC Cards

NIC cards are of two types −
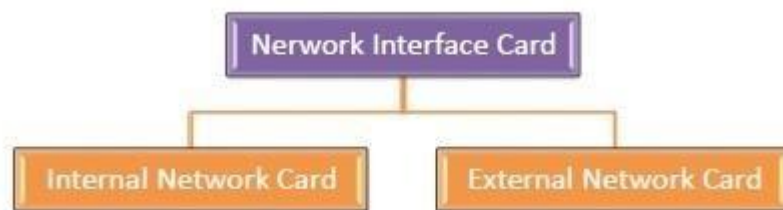
Internal Network Cards

In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).

External Network Cards

In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

What is a wireless access point?

A wireless access point (WAP) is a networking device that allows wireless-capable devices to connect to a wired network. It is simpler and easier to install WAPs to connect all the computers or devices in your network than to use wires and cables.
Why use a WAP to set up a wireless network?

Using a WAP lets you create a wireless network within your existing wired network, so you can accommodate wireless devices.
You can also use a WAP or mesh extenders to extend the signal range and strength of your wireless network to provide complete wireless coverage and get rid of "dead spots," especially in larger office spaces or buildings. Additionally, you can configure the settings of your WAPs using a single device.

Transceiver

It is a combination of transmitter (Tx)/receiver (Rx) in an only package. This device is used in wireless communications devices like cordless telephone sets, cellular telephones, radios, etc.. Irregularly the transceiver name is used as a reference to Tx or Rx devices within cable otherwise optical fiber systems. The **transceiver diagram** is shown below.

The main function of this device is to transmit as well as receive different signals. This is most commonly used to illustrate the component in LAN to apply signals over the network wire & detect signals flowing through the wire. For several LANs, it is embedded in the NIC (network interface card). Some kinds of networks require an exterior transceiver.

Working

In a radio transceiver, as the transmitter transmits the signals, the receiver will be silenced. An electronic switch lets the transmitter & receiver to be allied to the similar antenna, so that transmitter o/p can be protected from the damage of the receiver.

In a transceiver type, it is not possible to get signals while transmitting, which is known as half-duplex. Some of the transceivers are mainly designed for permitting reception of signals throughout transmission stages which are known as full-duplex. The transmitter & receiver operate on different frequencies so that the transmitter signal does not interfere with the receiver. This kind of operation is used in cordless & cellular phones.

Satellite communication networks frequently use full-duplex transceivers on the subscriber points based on the surface. The transceiver to satellite or transmitted signal is known as the uplink, whereas the satellite to the transceiver or received signal is known as the downlink.

Types of Transceivers

Transceivers are classified into different types which include the following.

- RF Transceivers
- Fiber-optic Transceivers
- Ethernet Transceivers
- Wireless Transceivers

In the above-mentioned types are different but the working remains the same. Each type has its own characteristics like the no. of ports accessible for connecting the network and supports full-duplex communication.

1). RF Transceivers

RF transceiver is one type of module that includes both a Tx as well as Rx. Generally, this can be used in any wireless communication system by arranging in between baseband modem as well as PA/LNA. Here PA is a power amplifier whereas LNA is a low noise amplifier. Baseband Modem includes chipsets of numerous analog or digital modulation methods & ADC/DAC chips. RF Transceivers are used to transmit the data in the form of voice or video over the wireless medium. RF Transceiver is used to convert intermediate frequency (IF) to radiofrequency (RF). These are used in satellite communication for transmission & reception of TV signal, radio transmission & reception, and ITE networks/Zigbee/ WiMax/WLAN.

rf-transceivers

2). Fiber-optic Transceivers

This is also called as fiber optical transceiver, optics module, optical module, etc. This device employs fiber optic technology for data transmission. This is an essential component in the optical network devices that include <u>electronic components</u> to encode or decode the information into light signals. After that, these signals can be transmitted as electrical signals through another end. Here the data can be transmitted in the form of light which uses a light source like VSCEL, DFB laser, and FP.

fiber-optic-transducers

3). Ethernet Transceivers

An Ethernet transceiver is used to connect electronic devices or computers in a network to transmit & receive messages. An alternate name of an Ethernet transceiver is MAU (media access unit). This is used in the specifications of IEEE 802.3 & Ethernet. In the ISO network model, Ethernet is the physical layer component and the main **functions of transceivers** are for detecting a collision, conversion of digital data, Ethernet interface processing, and provides access for the network.

ethernet-transceivers

4). Wireless Transceivers

A wireless transceiver is an essential component in the wireless communication system and the quality of this can be determined by the efficiency as well as data delivery within the wireless system. This includes two functional layers like a physical layer & a media access control layer. The physical layer includes an RF front end as well as a baseband processor, this processor changes a bitstream to a collection symbol flow for data transmission. The MAC layer gives link traffic control used for the transmitter to contact the wireless links, evade collisions & enhance data throughput.

wireless-transceivers

Applications of Transceiver

The transceiver applications are

- This module is applicable in wireless communication
- The main function of this is to transmit the data in the form of voice or data or video over the wireless medium.
- This modem is used to change the frequency from IF to RF
- RF transceiver module is used in satellite communication, radio transmission for TV signal transmission.

Cellular Network

Cellular Network is formed of some cells, **cell** covers a geographical region, has a base station analogous to 802.11 AP which helps mobile users attach to network and there is an air-interface of physical and link layer protocol between mobile and base station. All these base stations are connected to *Mobile Switching Center* which connects cells to wide area net, manages call setup and handles mobility.

There is certain radio spectrum that is allocated to base station and to a particular region and that now needs to be shared. There are 2 techniques for sharing mobile-to-base station radio spectrum are:

1. **Combined FDMA/TDMA:**
   It divide spectrum in frequency channel and divide each channel into time slots.
2. **Code Division Multiple Access (CDMA):**
   It allows reuse of same spectrum over all cells. Net capacity improvement. Two frequency bands are used one of which is for forward channel (cell-site to subscriber) and one for reverse channel (sub to cell-site).

Cell Fundamentals –

In practice cells are of arbitrary shape(close to a circle) because it has the same power on all sides and has same sensitivity on all sides, but putting up two three circles together may result in interleaving gaps or may intersect each other so in order to solve this problem we can use equilateral triangle, square or a regular hexagon in which hexagonal cell is close to a circle used for a system design.

Co-channel reuse ratio is given by:

DL/RL = Square root of (3N)

Where,

DL = Distance between co-channel cells

RL = Cell Radius

N = Cluster Size

The number of cells in a cluster N determines the amount of co-channel interference and also the number of frequency channels available per cell.

Cell Splitting –

When number of subscribers in a given area increases allocation of more channels covered by that channel is necessary, which is done by cell splitting. A single small cell midway between two co-channel cells is introduced.

Need for Cellular Hierarchy –

Extending the coverage to the areas that are difficult to cover by a large cell. Increasing the capacity of the network for those areas that have a higher density of users. Increasing number of wireless devices and the communication between them.

Cellular Hierarchy –

1. **Femtocells:**
   Smallest unit of the hierarchy, these cells need to cover only a few meters where all devices are in the physical range of the uses.

2. **Picocells:**
   Size of these networks is in the range of few tens of meters, e.g., WLANs.
3. **Microcells:**
   Cover a range of hundreds of meters e.g. in urban areas to support PCS which is another kind of mobile technology.
4. **Macro cells:**
   Cover areas in the order of several kilometers, e.g., cover metropolitan areas.
5. **Mega cells:**
   Cover nationwide areas with ranges of hundreds of kilometers, e.g., used with satellites.

Fixed Channel Allocation –
For a particular channel the frequency band which is associated is fixed.
Total number of channels is given by
$Nc = W/B$

Where,

W = Bandwidth of the available spectrum,

B = Bandwidth needed by each channels per cell,

$Cc = Nc/N$ where N is the cluster size

Adjacent radio frequency bands are assigned to different cells. In analog each channel corresponds to one user while in digital each RF channel carries several time slots or codes (TDMA/CDMA). Simple to implement as traffic is uniform.

Global System for Mobile (GSM) Communications –
GSM uses 124 frequency channels, each of which uses an 8-slot Time Division Multiplexing (TDM) system. There is a frequency band which is also fixed. Transmitting and receiving does not happen in the same time slot because the GSM radios cannot transmit and receive at the same time and it takes time to switch from one to the other. A data frame is transmitted in 547 micro seconds, but a transmitter is only allowed to send one data frame every 4.615 micro seconds, since it is sharing the channel with seven other stations. The gross rate of each channel is 270, 833 bps divided among eight users, which gives 33.854 kbps gross.

Control Channel (CC) –
Apart from user channels there are some control channels which is used to manage the system.
1. **The broadcast control channel (BCC):**
   It is a continuous stream of output from the base station's identity and the channel status. All mobile stations monitor their signal strength to see when they moved into a new cell.
2. **The dedicated control channel (DCC):**
   It is used for location updating, registration, and call setup. In particular, each base station maintains a database of mobile stations. Information needed to maintain this database and is sent on the dedicated control channel.

Common Control Channel –
Three logical sub-channels:
1. Is the paging channel, which the base station uses to announce incoming calls. Each mobile station monitors it continuously to watch for call it should answer.

2. Is the random access channel that allows the users to request a slot on the dedicated control channel. If two requests collide, they are garbled and have to be retried later.
3. Is the access grant channel which is the announced assigned slot.

Mobile Ad hoc Network (MANET)

MANET stands for Mobile adhoc Network also called a wireless adhoc network or adhoc wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network.. They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently. Each node behaves as a router as they forward traffic to other specified nodes in the network.
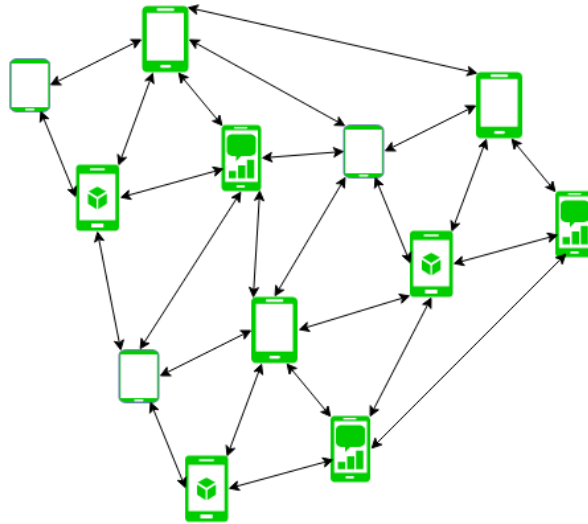

Figure - Mobile Ad Hoc Network

MANET may operate a standalone fashion or they can be part of larger internet. They form a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes. The main challenge for the MANET is to equip each device to continuously maintain the information required to properly route traffic. MANETs consist of a peer-to-peer, self-forming, self-healing network MANET's circa 2000-2015 typically communicate at radio frequencies (30MHz-5GHz). This can be used in road safety, ranging from sensors for the environment, home, health, disaster rescue operations, air/land/navy defense, weapons, robots, etc.

Characteristics of MANET –

- **Dynamic Topologies:**
  Network topology which is typically multihop, may change randomly and rapidly with time, it can form unidirectional or bi-directional links.

- **Bandwidth constrained, variable capacity links:**
  Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to a wired network

- **Autonomous Behavior:**
  Each node can act as a host and router, which shows its autonomous behavior.

- **Energy Constrained Operation:**
  As some or all the nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized by less memory, power, and lightweight features.

- **Limited Security:**
  Wireless networks are more prone to security threats. A centralized firewall is absent due to its distributed nature of the operation for security, routing, and host configuration.

Pros and Cons of MANET –
Pros:
1. Separation from central network administration.
2. Each node can play both the roles ie. of router and host showing autonomous nature.
3. Self-configuring and self-healing nodes do not require human intervention.

Cons:
1. Resources are limited due to various constraints like noise, interference conditions, etc.
2. Lack of authorization facilities.
3. More prone to attacks due to limited physical security.