DATA COMMUNICATIONS AND NETWORKING

UNIT I **15 hours**

INTRODUCTION: Computer Networks-Categories of Network- Open System and OSI model- Transmission Media-Transmission mode-Interfacing-Multiplexing-Types of Errors-Error Detection- Error Correction

UNIT II **15 hours**

LAN: Types of Network and Topology-LAN Transmission Equipment- Token Bus-Token Ring-FDDI Ethernet Technologies. WAN: WAN Transmission methods- WAN carrier types- WAN Transmission Equipment-WAN Protocols

UNIT III **15 hours**

Networking and Internetworking Devices: Repeaters – Bridges – Routers – Gateways. Routing Algorithms: Distance Vector Algorithm –Link State Algorithm - Dijkstra Algorithm. TCP/IP Protocol Suite: Part-I: Network Layer-Internetwork Protocol (IP).Transport layer: UDP-TCP

UNIT IV **15 hours**

Point-to-Point Protocol PPP: Transition states – PPP Layers-Link Control Protocol LCP – Network Control Protocol - ISDN: Services - ISDN Layers- Future of ISDN

UNIT V **15 hours**

ATM: Design Goals: Packet Networks-Mixed Network packets - Cell Networks -Asynchronous TDM - ATM Architecture - ATM Layers. Network Security: Fundamental Concepts-Securing Network using Firewall

UNIT I INTRODUCTION: Computer Networks-Categories of Network- Open System and OSI model-Transmission Media-Transmission mode-Interfacing-Multiplexing-Types of Errors-Error Detection-Error Correction

INTRODUCTION

COMPUTER NETWORKS

A **computer network** is a group of computers that use a set of common communication protocols over digital interconnections for the

purpose of sharing resources located on or provided by the network nodes. The interconnections between nodes are formed from a broad spectrum of telecommunication network technologies, based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of network topologies.

The nodes of a computer network may be classified by many means as personal computers, servers, networking hardware, or general-purpose hosts. They are identified by hostnames and network addresses. Hostnames serve as memorable labels for the nodes, rarely changed after initial assignment. Network addresses serve for locating and identifying the nodes by communication protocols such as the Internet Protocol.

Computer networks may be classified by many criteria, for example, the transmission medium used to carry signals, bandwidth, communications protocols to organize network traffic, the network size, the topology, traffic control mechanism, and organizational intent.

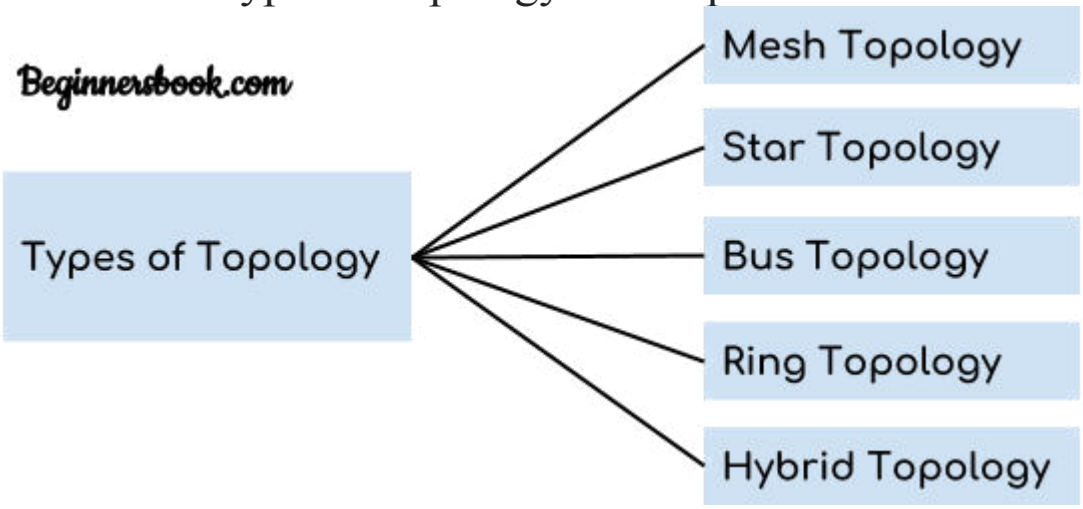
Computer networks support many applications and services, such as access to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications.

NETWORK TOPOLOGY

Geometric representation of how the computers are connected to each other is known as topology. There are five types of topology – Mesh, Star, Bus, Ring and Hybrid.

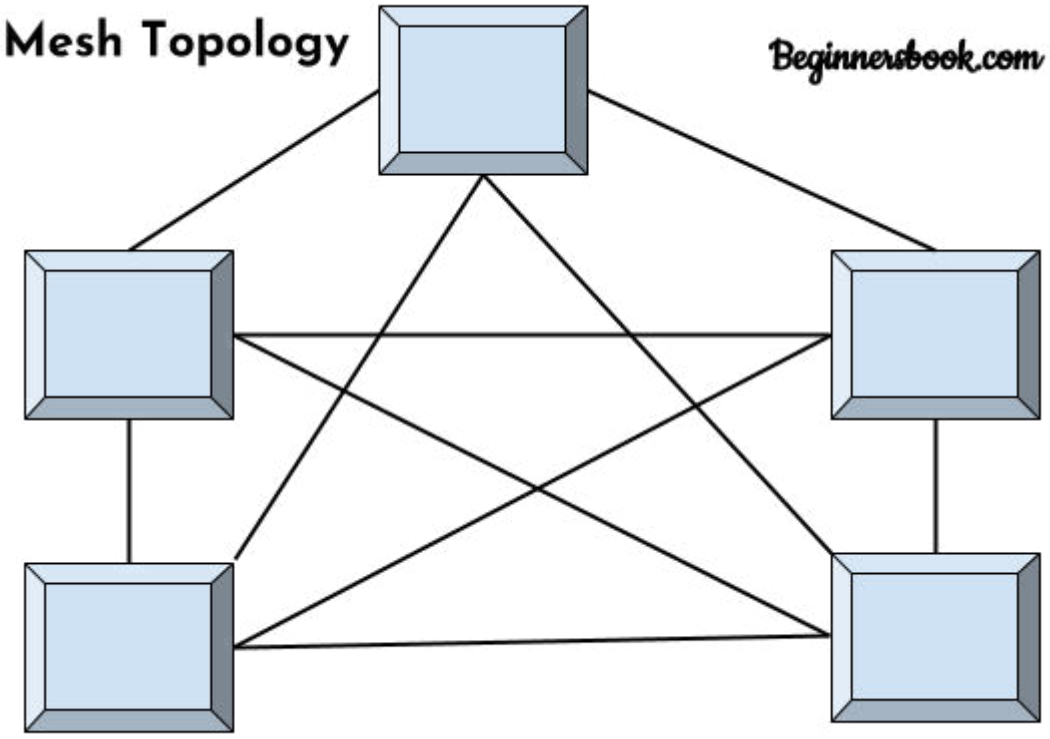
Types of Topology

There are five types of topology in computer networks:



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

Mesh Topology



In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it

means that the link only carries data for the two connected devices only. Let there be n devices in the network, then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

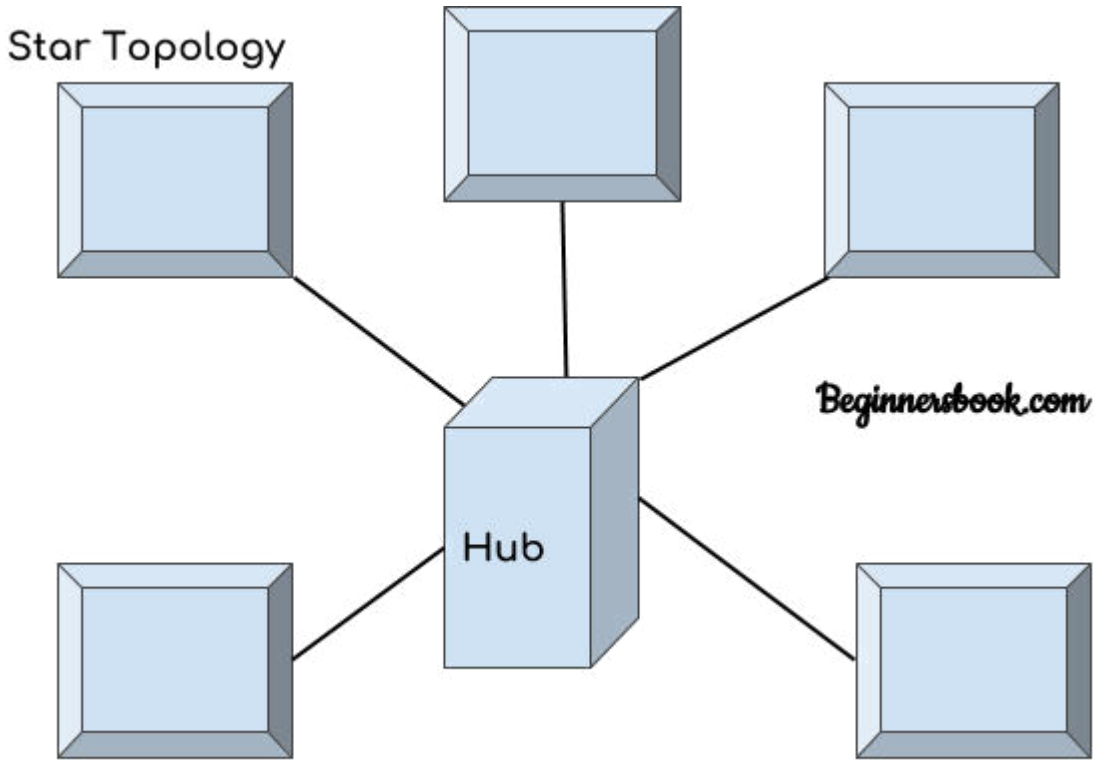
Advantages of Mesh topology

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.
3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
4. Fault detection is easy.

Disadvantages of Mesh topology

1. Amount of wires required to connected each system is tedious and headache.
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.
3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

Star Topology



In star topology each device in the network is connected to a central device called hub. Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub. If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.

Advantages of Star topology

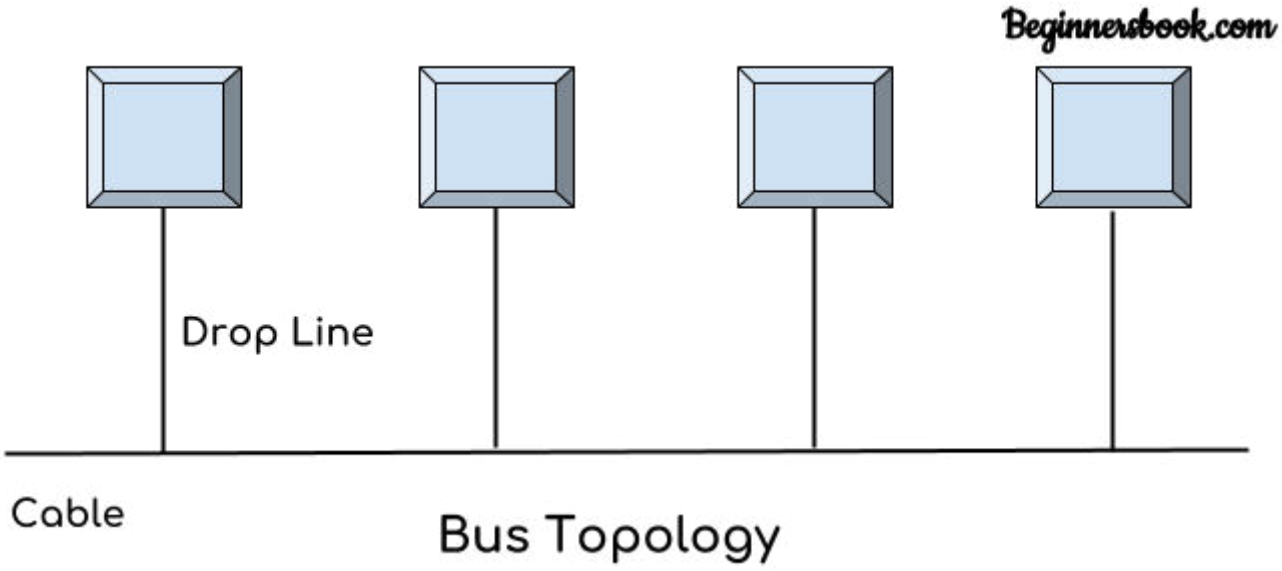
1. Less expensive because each device only need one I/O port and needs to be connected with hub with one link.
2. Easier to install
3. Less amount of cables required because each device needs to be connected with the hub only.
4. Robust, if one link fails, other links will work just fine.
5. Easy fault detection because the link can be easily identified.

Disadvantages of Star topology

1. If hub goes down everything goes down, none of the devices can work without hub.

2. Hub requires more resources and regular maintenance because it is the central system of star topology.

Bus Topology



In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

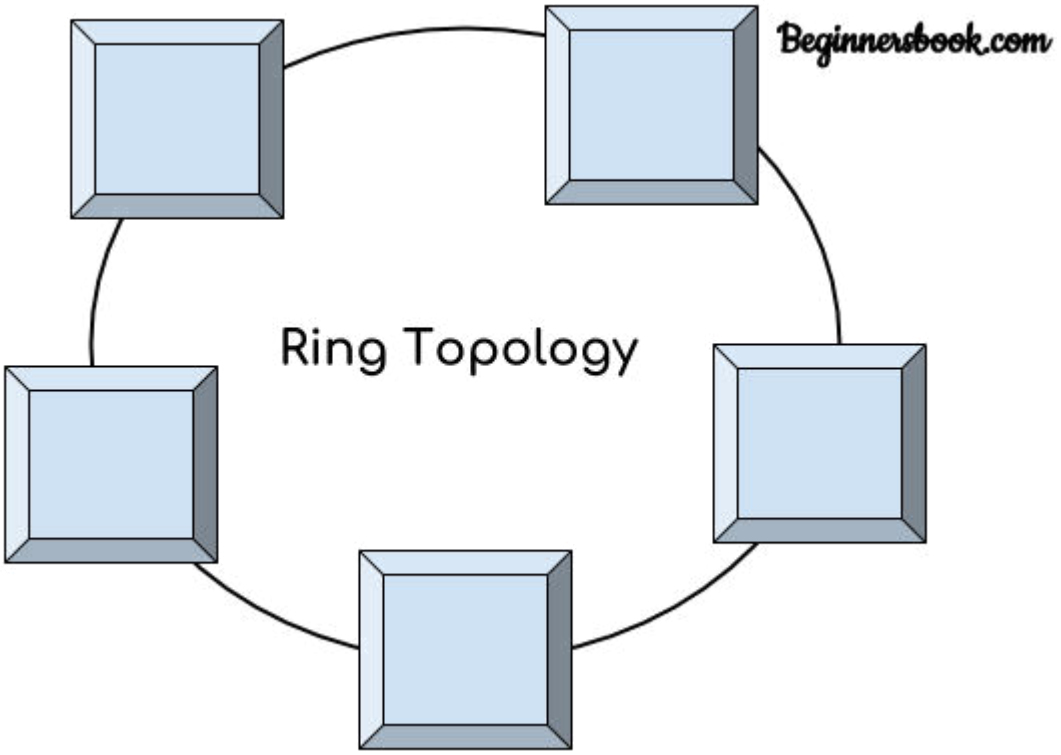
Advantages of bus topology

1. Easy installation, each cable needs to be connected with backbone cable.
2. Less cables required than Mesh and star topology

Disadvantages of bus topology

1. Difficultly in fault detection.
2. Not scalable as there is a limit of how many nodes you can connect with backbone cable.

Ring Topology



In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

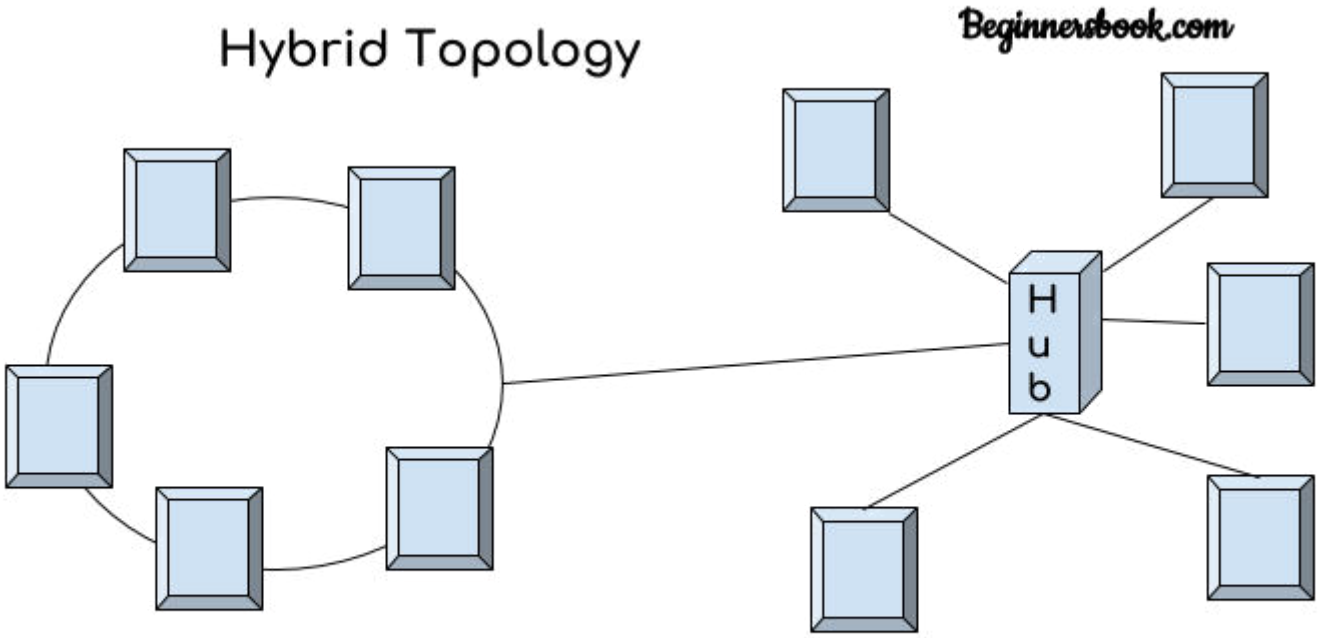
Advantages of Ring Topology

1. Easy to install.
2. Managing is easier as to add or remove a device from the topology only two links are required to be changed.

Disadvantages of Ring Topology

1. A link failure can fail the entire network as the signal will not travel forward due to failure.
2. Data traffic issues, since all the data is circulating in a ring.

Hybrid topology



A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

Advantages of Hybrid topology

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

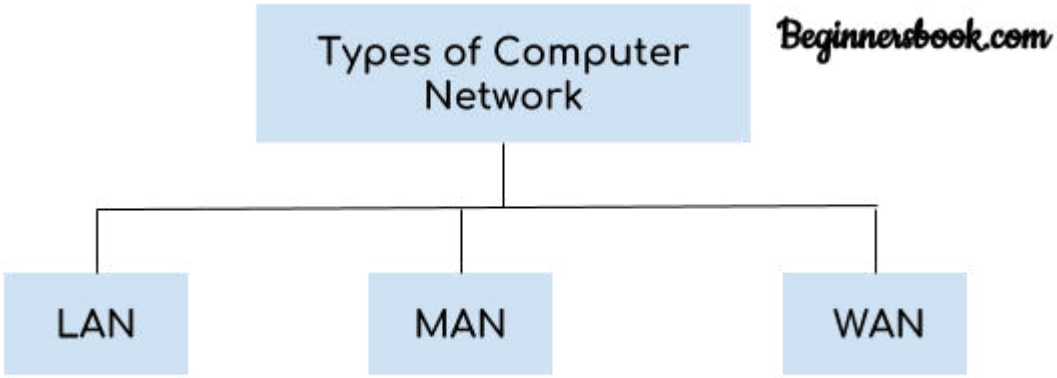
Disadvantages of Hybrid topology

1. Fault detection is difficult.
2. Installation is difficult.
3. Design is complex so maintenance is high thus expensive.

Types of Computer Network: LAN, MAN and WAN

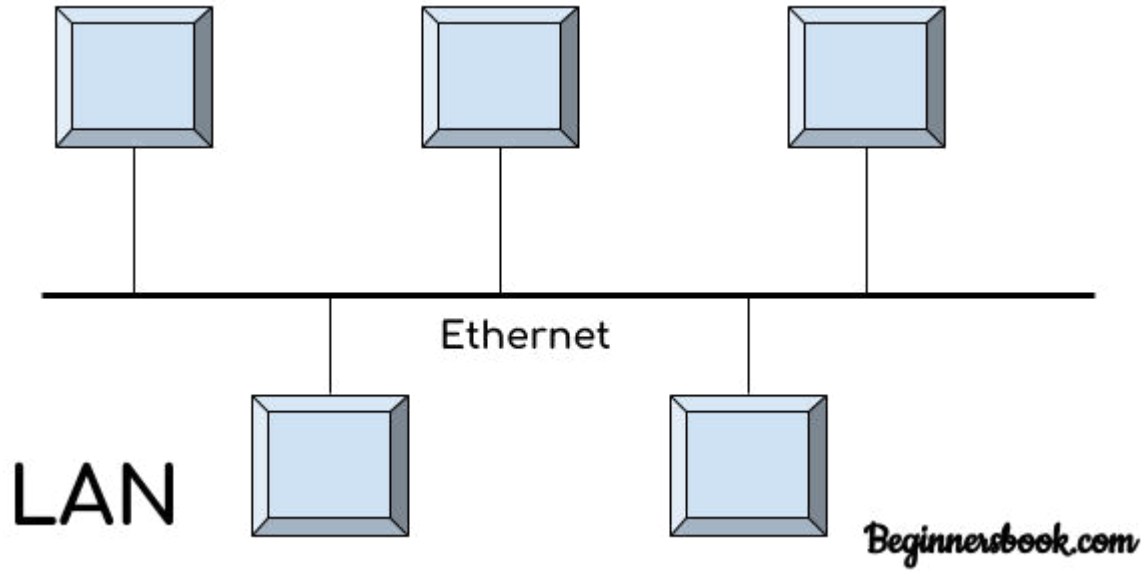
Computer network is a group of computers connected with each other through a transmission medium such as cable, wire etc. In this guide, we will discuss the types of computer networks in detail.

Types of Computer Network



There are mainly three types of computer networks based on their size:
1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

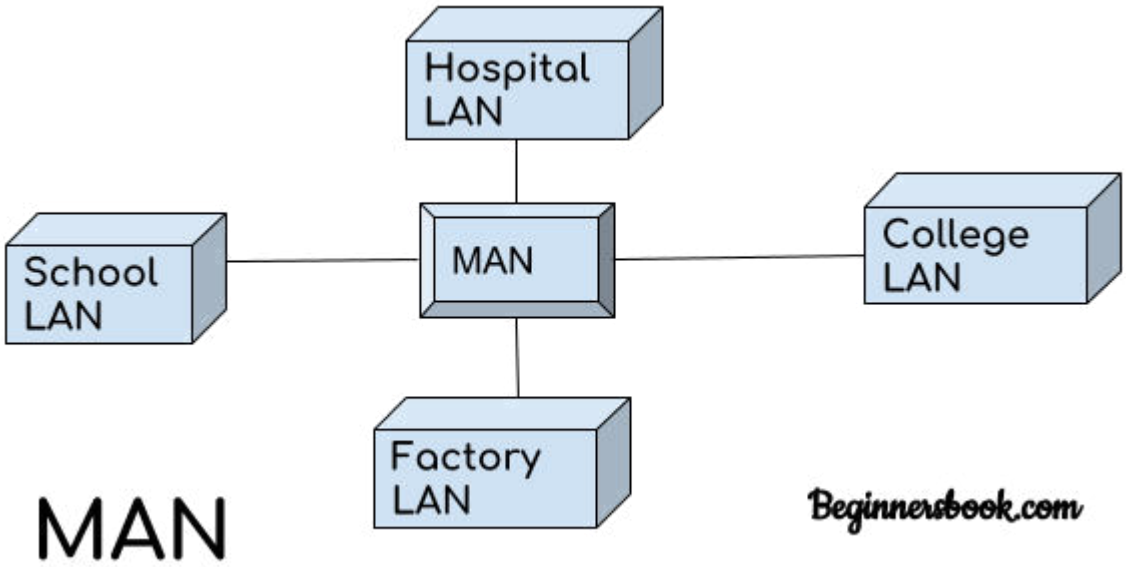
1. Local Area Network (LAN)



1. Local area network is a group of computers connected with each other

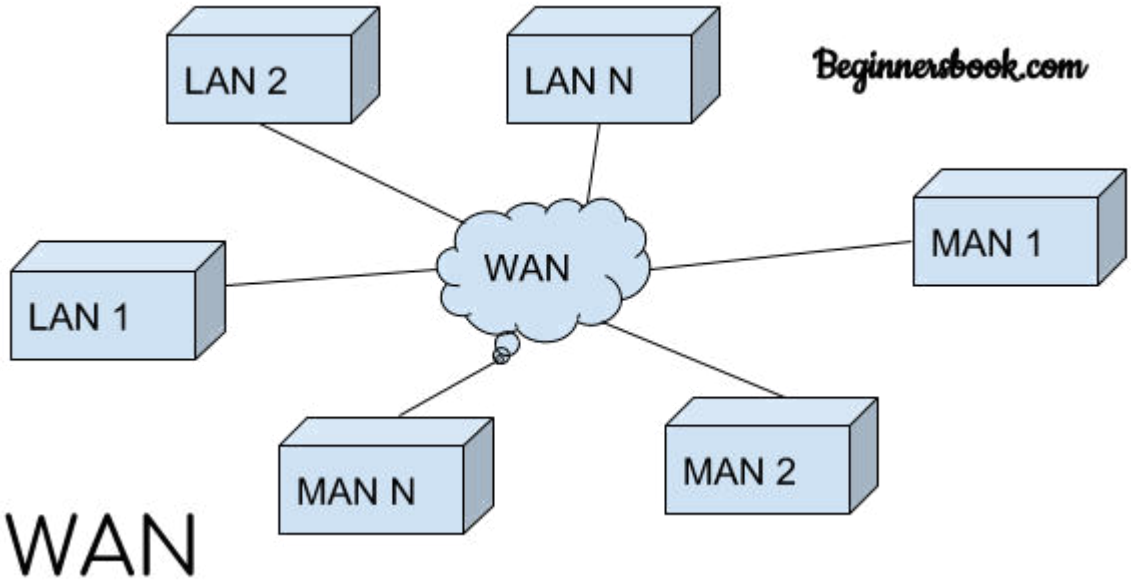
in a small places such as school, hospital, apartment etc.
2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.
3. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps.
4. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection.

2. Metropolitan Area Network (MAN)



MAN network covers larger area by connections LANs to a larger network of computers. In Metropolitan area network various Local area networks are connected with each other through telephone lines. The size of the Metropolitan area network is larger than LANs and smaller than WANs(wide area networks), a MANs covers the larger area of a city or town.

3. Wide area network (WAN)



WAN

Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

Advantages of WAN:

Centralized infrastructure: One of the main advantage of WAN is the that we do not need to maintain the backup and store data on local system as everything is stored online on a data centre, from where we can access the data through WAN.

Privacy: We can setup the WAN in such a way that it encrypts the data that we share online that way the data is secure and minimises the risk of unauthorized access.

Increased Bandwidth: With the WAN we get to choose the bandwidth based on the need, a large organization can have larger bandwidth that can carry large amount of data faster and efficiently.

Area: A WAN can cover a large area or even a whole world though internet connection thus we can connect with the person in another

country through WAN which is not possible is other type of computer networks.

Disadvantages of WAN:

Antivirus: Since our systems are connected with the large amount of systems, there is possibility that we may unknowingly download the virus that can affect our system and become threat to our privacy and may lead to data loss.
Expensive: Cost of installation is very high.
Issue resolution: Issue resolution takes time as the WAN covers large area, it is really difficult to pin point the exact location where the issues raised and causing the problem.

OSI REFERENCE MODEL

Open System Interconnection (OSI) model, an ISO standard for worldwide communication Networks that defines a networking framework for implementing protocols in seven layers. Layering the communications process means breaking down the communication process into **smaller** and **easier** to handle interdependent categories. The convention and rules used in such communications are collectively known as **layer protocol**. **Open Systems Interconnection (OSI)** model is developed by ISO (International organization for standardization) in **1984**. ISO is the organization dedicated to defining global communication and standards.

This model is called Open System Interconnection (OSI) because this model allows any two different systems to communicate regardless of their underlying architecture. Therefore OSI reference model allows open communication between different systems without requiring changes' to the logic of the underlying hardware and software.

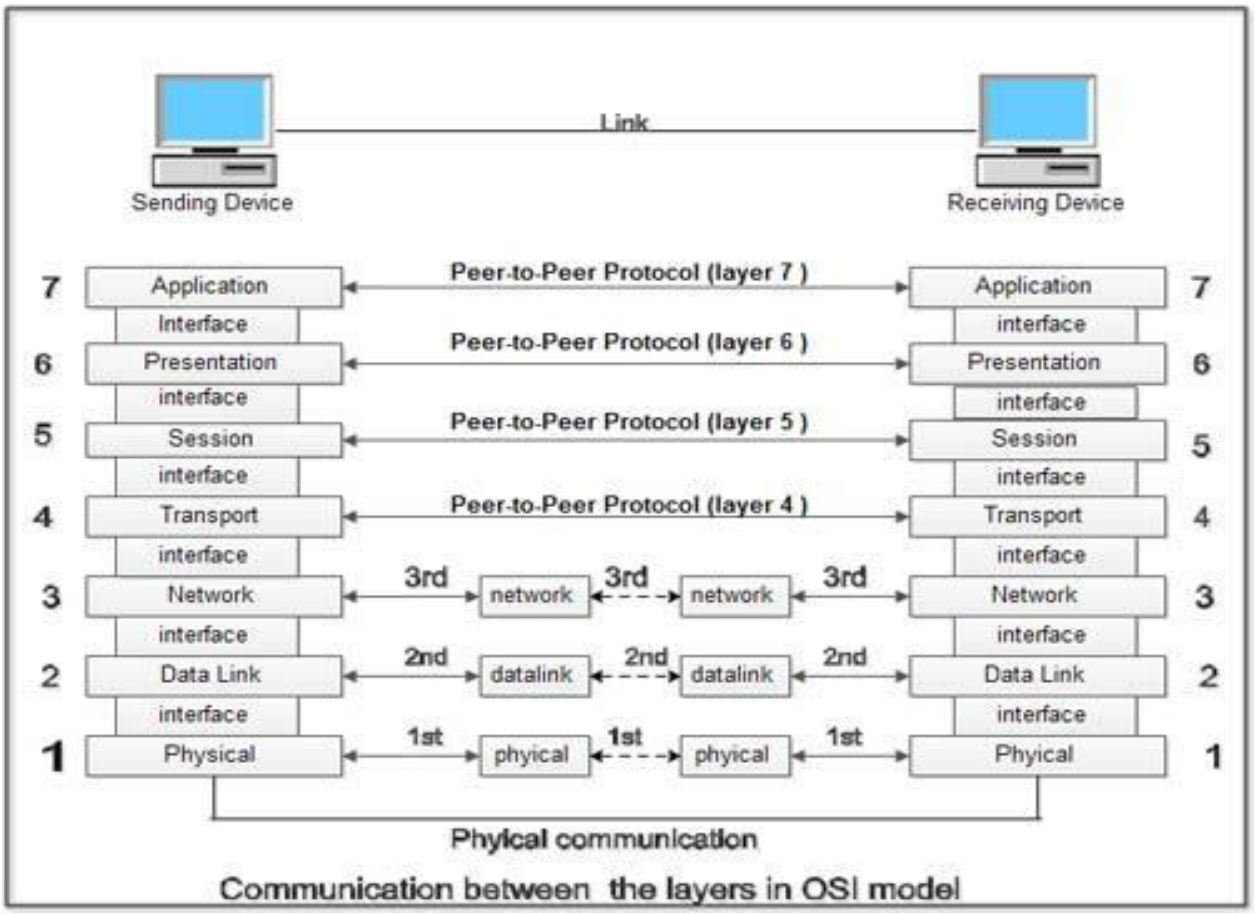
The model logically groups the functions and sets rules, called protocols, necessary to establish and conduct communication between two or more parties. The model consists of seven functions, often referred to as layers.

OSI reference model is a logical framework for standards for the network communication. OSI reference model is now considered as a primary standard for internetworking and inter computing. Today many network communication protocols are based on the standards of OSI model. In the OSI model the network/data communication is defined into seven layers. The seven layers can be grouped into three groups - Network, Transport and Application.

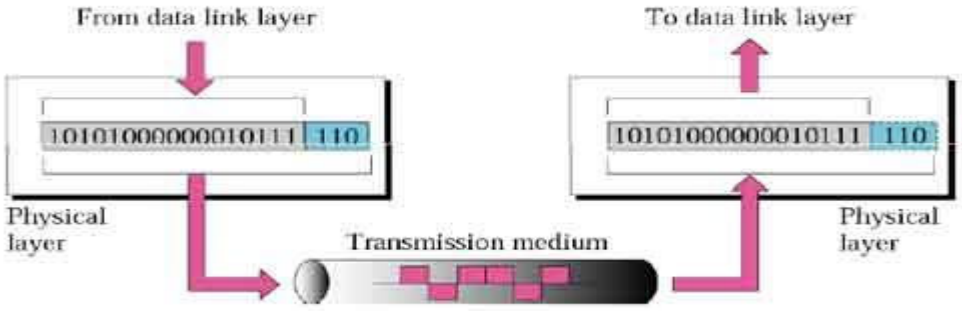
Layer 1, 2 and 3 *i.e.* physical, data link, and network are network support layers.

Layer 4, Transport layer provides end to end reliable data transmission.

Layer 5, 6 and 7 i.e. Session, Presentation, and Application layer are user support layers.



PHYSICAL LAYER

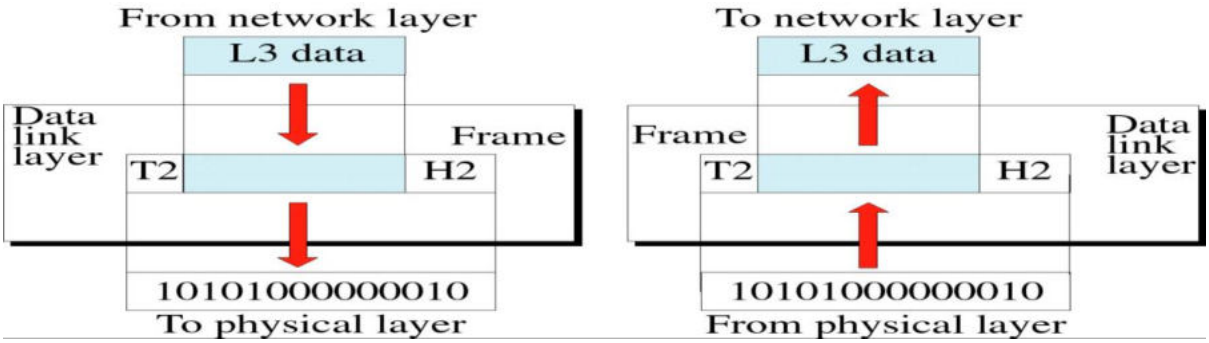


It is the bottom layer of OSI Model. It is responsible for the actual physical connection between the devices. Such physical connection may be made by using twisted pair cable. It is concerned with transmitting bits over a communication channel.

FUNCTIONS OF PHYSICAL LAYER

- Transforming bits into signals
- Provides synchronization of bits by a clock.
- Physical layer manages the way a device connects to network media.
- It defines the transmission rate.
- It defines the way in which the devices are connected to the medium.
- It provides physical topologies
- It can use different techniques of multiplexing.

DATA LINK LAYER



It is responsible for node to node delivery of data.

It receives the data from network layer and creates frames, add physical address to these

frames & pass them to physical layer.

It consists of 2 layers:

Logical Link Layer (LLC):

Defines the methods and provides addressing information for communication between network devices.

Medium Access Control (MAC):

Establishes and maintains links between communicating devices.

FUNCTIONS OF DATA LINK LAYER

- Framing:

DLL divides the bits received from N/W layer into frames. (Frame contains all the addressing information necessary to travel from S to D).

- Physical addressing:

After creating frames, DLL adds physical address of sender/receiver (MAC address) in the header of each frame.

- Flow Control:

DLL prevents the fast sender from drowning the slow receiver.

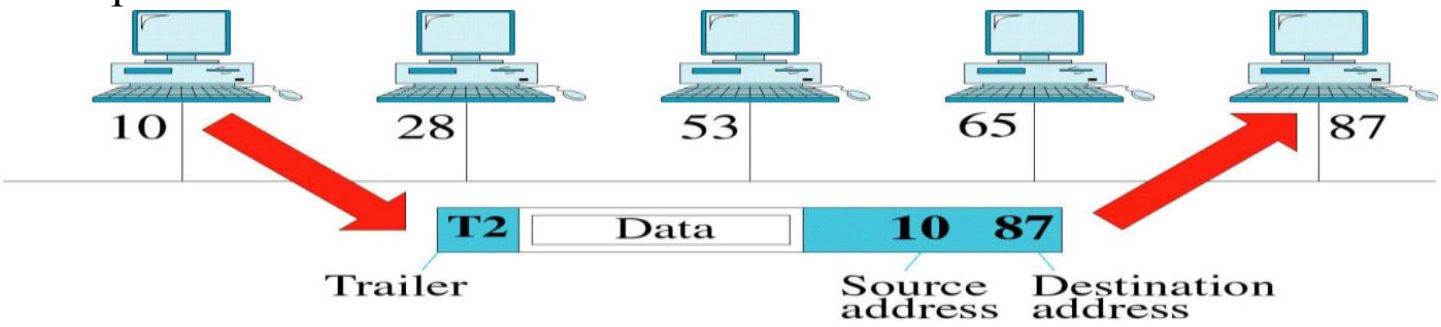
- Error Control:

It provides the mechanism of error control in which it detects & retransmits damaged or lost frames.

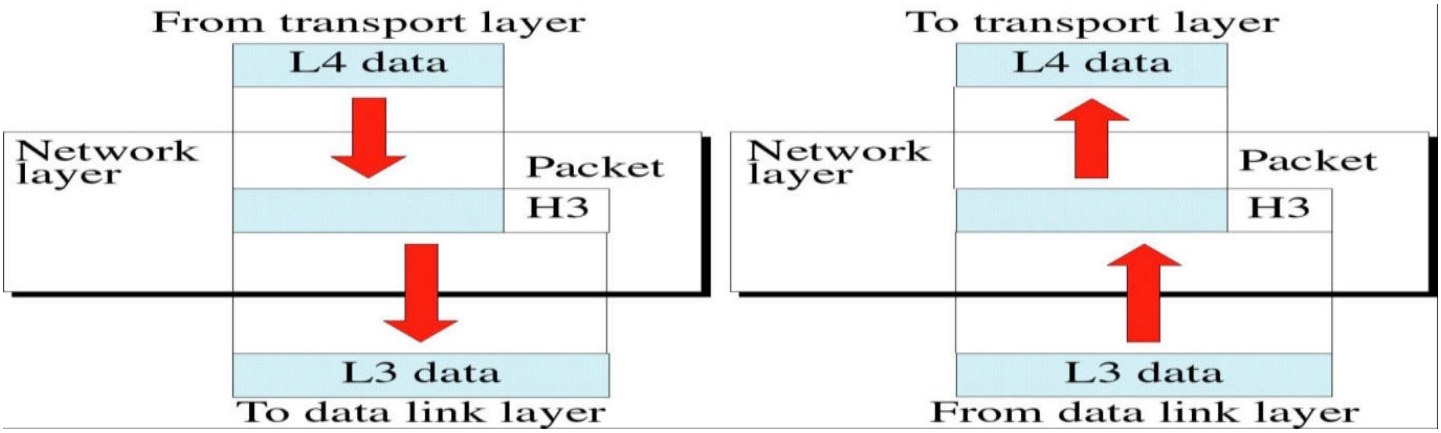
➢ Access Control:

When single comm. Channel is shared by multiple devices, MAC layer of DLL provides help to determine which device has control over the channel.

Example of DLL



NETWORK LAYER



It is responsible for the source to destination delivery of a packet across multiple networks.

If two systems are attached to different networks with devices like routers, then N/W layer is used.

Thus DLL overseas the delivery of the packet between the two systems on same network and the network layer ensures that the packet gets its point of origin to its final destination.

FUNCTIONS OF NETWORK LAYER

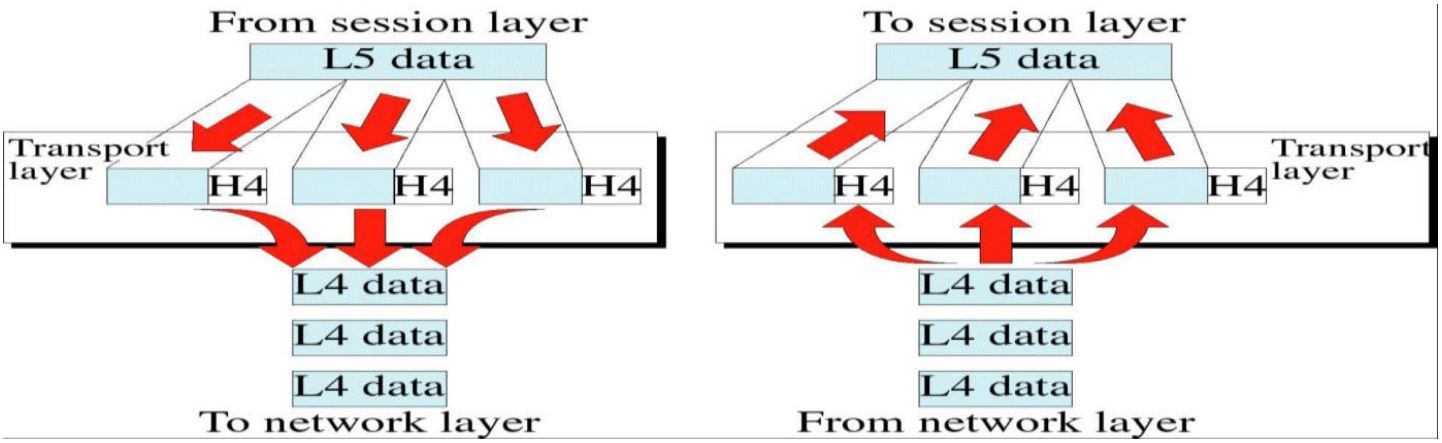
Internetworking: It provides Internetworking.

Logical Addressing: When packet is sent outside the network, N/W layer adds Logical (network) address of the sender & receiver to each packet.

Network addresses are assigned to local devices by n/w administrator and assigned dynamically by special server called DHCP (Dynamic Host Configuration Protocol)

Routing: When independent n/w are connected to create internetwork several routes are available to send the data from S to D. These n/w are interconnected by routers & gateways that route the packet to final destination.

TRANSPORT LAYER



It is responsible for process-to-process delivery of the entire message.

TL looks after the delivery of entire message considering all its packets & make sure that all packets are in order. On the other hand n/w layer treated each packet independently.

At the receiver side, TL provides services to application layer & takes services form n/w layer.

At the source side, TL receives message from upper layer into packets and reassembles these packets again into message at the destination.

TRANSPORT LAYER PROVIDES TWO TYPES OF SERVICES:

Connection Oriented Transmission: In this type of transmission the receiving devices sends an acknowledge back to the source after a packet or group of packet is received. It is slower transmission method.

Connectionless Transmission: In this type of transmission the receiving devices does not sends an acknowledge back to the source. It is faster transmission method.

Functions of Transport Layer

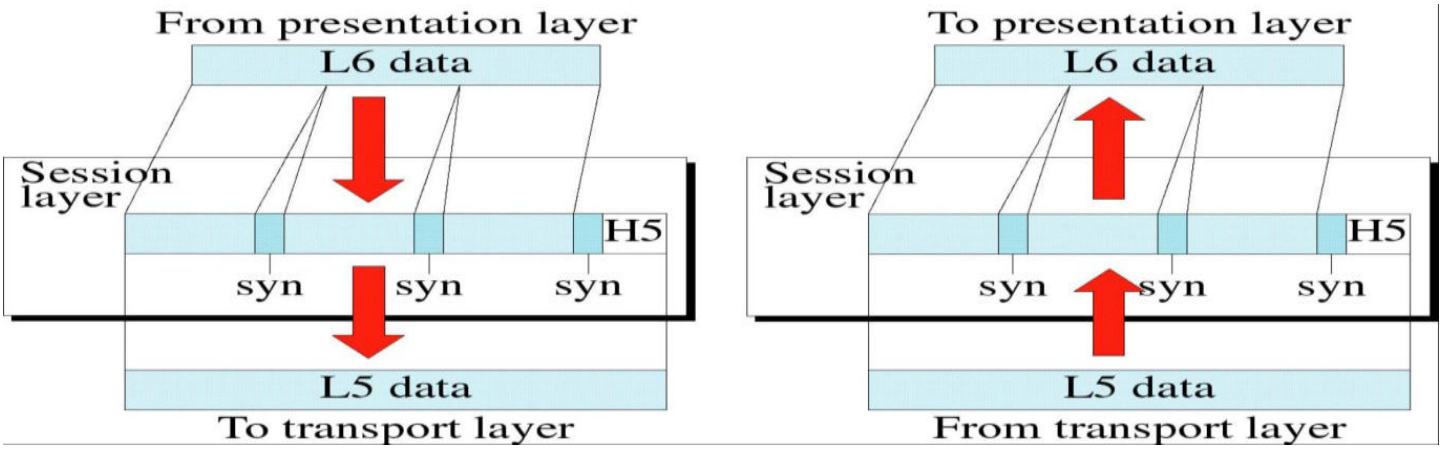
Segmentation of message into packet & reassembly of packets into message.

Port addressing: Computers run several processes. TL header include a port address with each process.

Flow Control: Flow control facility prevents the source form sending data packets faster than the destination can handle.

Error control: TL ensures that the entire message arrives at the receiving TL without error.

SESSION LAYER



Session layer is the fifth layer of OSI Model. It has the responsibility of beginning, maintaining and ending the communication between two devices, called session. It also provides for orderly communication between devices by regulating the flow of data.

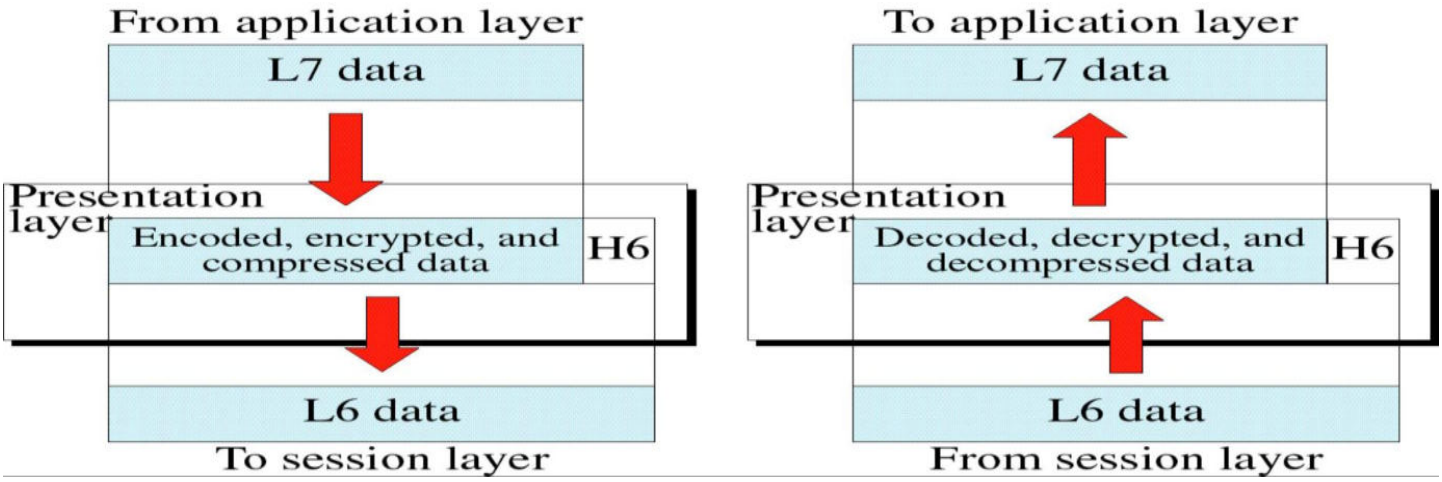
FUNCTIONS OF SESSION LAYER

Establishing, Maintaining and ending a session: When sending device first contact with receiving device, it sends ***syn***(synchronization) packet to establish a connection & determines the order in which information will be sent. Receiver sends ***ack*** (acknowledgement). So the session can be set & end.

Dialog Control: This function determines that which device will communicate first and the amount of data that will be sent.

Dialog separation: Process of adding checkpoints & markers to the stream of data is called dialog separation.

PRESENTATION LAYER



Presentation layer is the sixth layer of OSI Model. It is concerned with the syntax & semantics of the information exchanged between the two devices. It was designed for data encryption, decryption and compression.

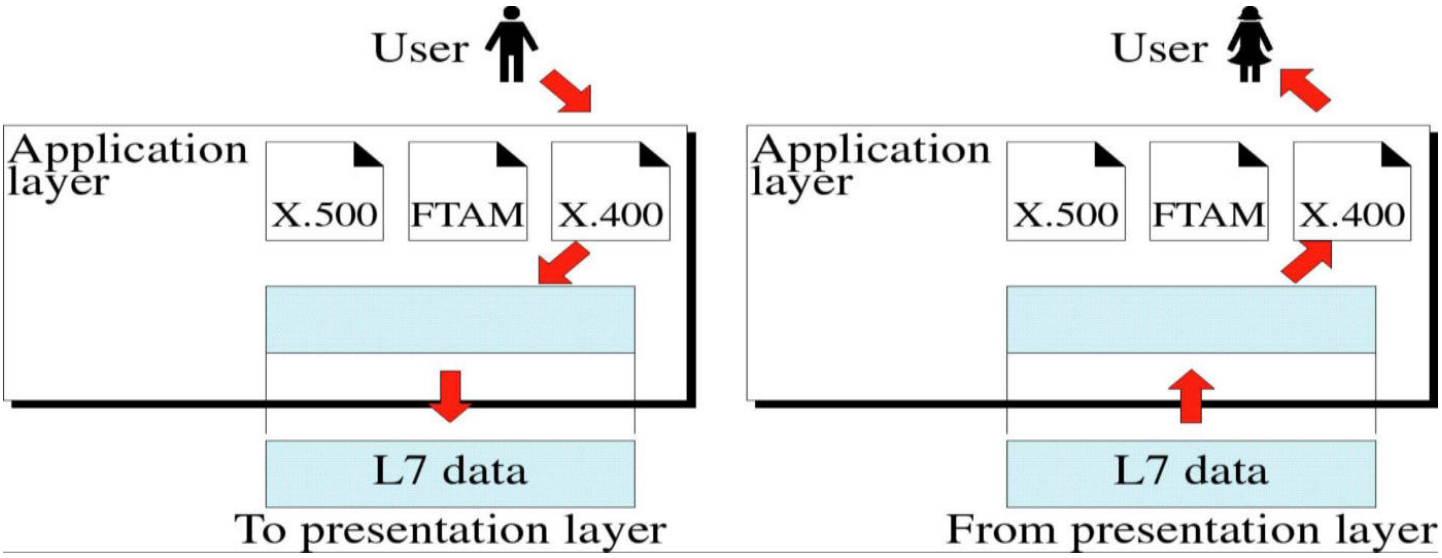
FUNCTIONS OF PRESENTATION LAYER

Data Presentation or Translation: Because different computers use different encoding systems. It ensures that the data being sent is in the format that the recipient can process.

Data Encryption: PL provides this facility by which hides the information from everyone except the person who originally sent the information & the intended recipient. When encrypted data arrives at destination, PL decrypts the message.

Data Compression: PL shrinks large amount of data into smaller pieces i.e. it reduces the size of data.

APPLICATION LAYER



It is the topmost i.e. seventh layer of OSI Model. It enables the user to access the network.

It provides user interface & supports for services such as e-mail, file transfer, access to the world wide web.

So it provides services to different user applications.

FUNCTIONS OF APPLICATION LAYER

Mail Services: This application provides various e-mail services.

File transfer & Access: It allows users to access files in a remote host, to retrieve files from remote computer for use etc.

Remote log-in: A user can log into a remote computer and access the resources of that computer.

Accessing the World Wide Web: Most common application today is the access of the World Wide Web.

TRANSMISSION MEDIA

1. The purpose of the physical layer is to transport a raw bit stream from one machine to another.

2. Media are roughly grouped into guided media, such as copper wire and fiber optics, and unguided media, such as radio and lasers through the air.

MAGNETIC MEDIA:

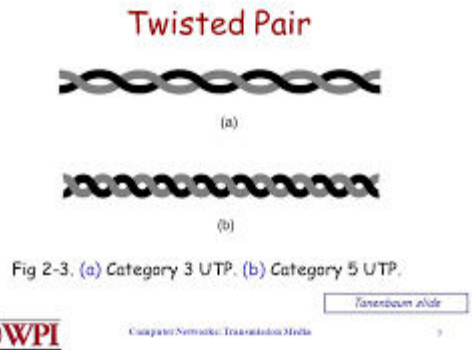
1 .One of the most common ways to transport data from one computer to another is to write them onto magnetic tape or removable media physically transport the tape or disks to the destination machine, and read them back in again.

2. Although this method is not sophisticated as using a geosynchronous communication satellite, it is often more cost effective.

TWISTED PAIR:

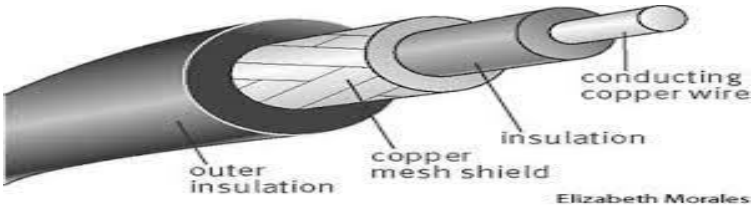
1. Most common transmission media is twisted pair.
2. A twisted pair consists of two insulated copper wires, typically about 1mm thick.
3. The wires are twisted together in a helical form, just like a DNA molecule.
4. The most common application of the **twisted pair** is the telephone system. Nearly all telephones are connected to the telephone company office by a twisted pair. Twisted pair can run several kilometers without amplification, but for longer distances, repeaters areneeded.
5. Twisted pairs can be used for transmitting either analog or digital signals.
6. **Category 3** twisted pairs consist of two insulted wires gently twisted together.
7. Around 1988, the more advanced **category 5** twisted pairs were introduced.

8. All of these writing types are often referred to as **UTP (Unshielded Twisted Pair)**



COAXIABLE CABLE:

1. Another common transmission medium is the **coaxial cable**.
2. It has better shielding than twisted pairs, so it can span longer distances at higher speeds.
3. Two kinds of coaxial cable are widely used.
4. One kind 50-ohm cable, is commonly used when it is intended for digital transmission from the start.
5. The other kind is 75-ohm cable is,commonly used for analog transmission and cable television but becoming more important with the advent of internet over cable.
6. A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulting material.
7. The insulator is encased by a cylindrical conductor,often as a closely woven braided mesh.
8. The outer conductor is covered in a protective plastic sheath.
9. Coaxial cables are used for telephone system for long distance lines

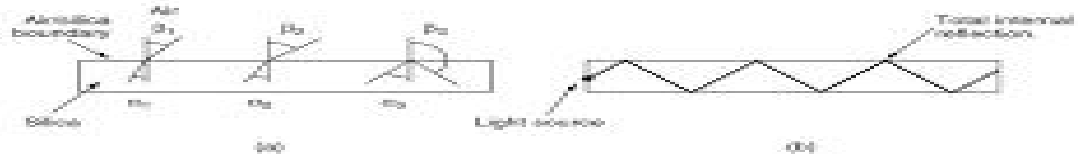


FIBER OPTICS:

1. Current fiber technology, the achievable bandwidth is certainly in excess of 50000Gbps.

2. An optical transmission system has three key components: the light source, the transmission medium, and the detector.
3. Conventionally, a pulse of light indicates a 1 bit and the absence of light indicates a 0 bit.
4. The transmission medium is an ultra-thin fiber of glass.
5. The detector generates an electrical pulse when light falls on it.
6. When a light ray passes from one medium to another, example: From fused silica to air,the ray is refracted at the silica/air boundary.
7. A light ray incident at or above the critical angle is trapped inside the fiber,and can propagate for many kilometers with virtually no loss.
8. Each ray is said to have a different **mode**, so a fiber having this property is called a **multimode fiber**.
9. The fibers diameter is reduced to a few wavelengths of light , the fiber acts like a wave guide, and the light can propagate only in a straight line, without bouncing, yielding a **single-mode fiber.**

Fiber Optics

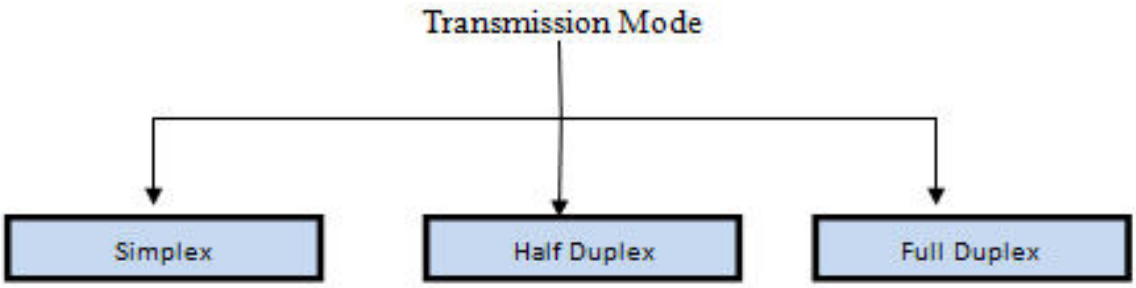


(a) Three examples of a light ray from inside a silica fiber impinging on the air/silica boundary at different angles.
(b) Light trapped by total internal reflection.

TRANSMISSION MODE

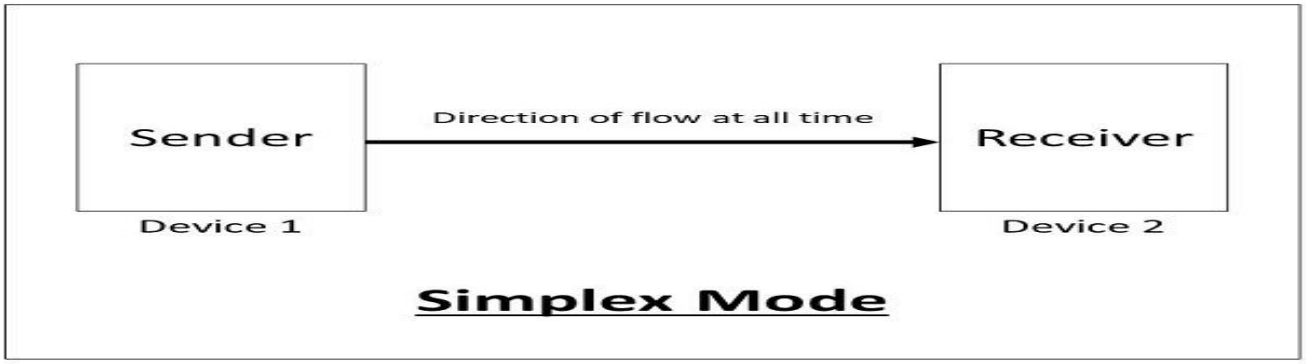
- Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called **Communication Mode**. These modes direct the direction of flow of information. There are three types of transmission modes. They are:

- Simplex Mode
- Half duplex Mode
- Full duplex Mode



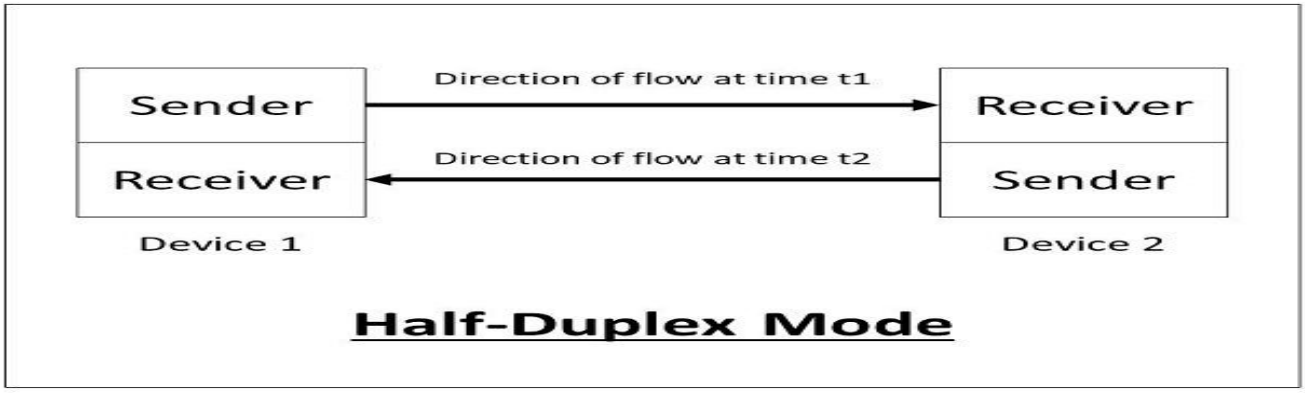
SIMPLEX MODE

- In this type of transmission mode, data can be sent only in one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems where we just need to send a command/signal, and do not expect any response back.
- Examples of simplex Mode are loudspeakers, television broadcasting, television and remote, keyboard and monitor etc.



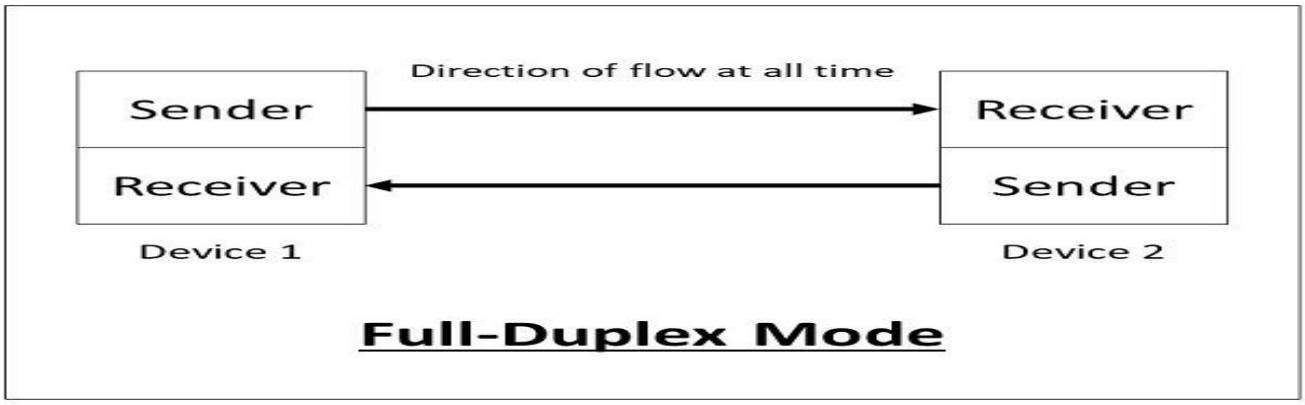
HALF DUPLEX MODE

- Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time.
- For Example, Walkie-Talkie, Internet Browsers, etc.



FULL DUPLEX MODE

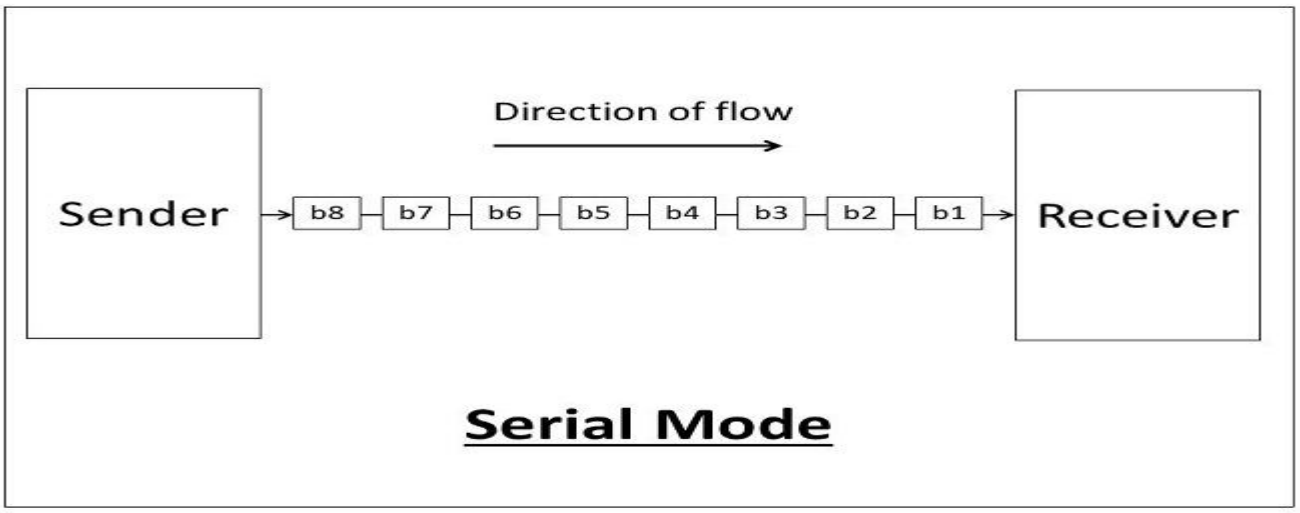
- **Full-Duplex is the data transmission mode in which the data can flow in both directions at the same time. It is bi-directional in nature.** It is two-way communication in which both the stations can transmit and receive the data simultaneously.



- ***The data transmission modes can be characterized in the following two types based on the number of bits sent simultaneously in the network:***
- Serial Transmission
- Parallel Transmission

SERIAL TRANSMISSION

- **The Serial data transmission mode is a mode in which the data bits are sent serially one after the other at a time over the transmission channel.**



- It needs a single transmission line for communication. The data bits are received in synchronization with one another. So, there is a challenge of synchronizing the transmitter and receiver.
- In serial data transmission, the system takes several clock cycles to transmit the data stream. In this mode, the data integrity is maintained, as it transmits the data bits in a specific order, one after the other.
- This type of transmission mode is best suited for long-distance data transfer, or the amount of data being sent is relatively small.

For Example, Data transmission between two computers using serial ports.

Following are the advantages of using a serial transmission mode:

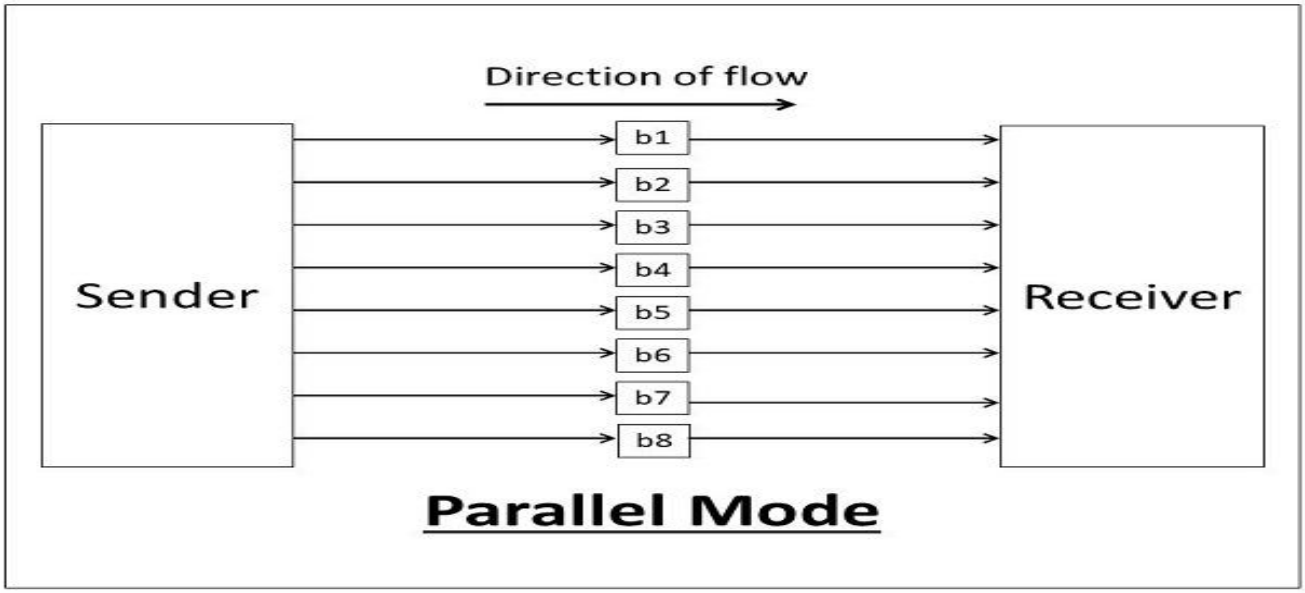
- It can be used for long-distance data transmission as it is reliable.
- The number of wires and complexity is less.
- It is cost-effective.

Following are the disadvantages of using a serial transmission mode:

- The Data transmission rate is slow due to a single transmission channel.

PARALLEL TRANSMISSION

- **The Parallel data transmission mode is a mode in which the data bits are sent parallelly at a time.** In other words, there is a transmission of n-bits at the same time simultaneously.



- Multiple transmission lines are used in such modes of transmission. So, multiple data bytes can be transmitted in a single system clock. This mode of transmission is used when a large amount of data has to be sent in a shorter duration of time. It is mostly used for short-distance communication.
- For n-bits, we need n-transmission lines. So, the complexity of the network increases but the transmission speed is high. If two or more transmission lines are too close to each other, then there may be a chance of interference in the data, degrading the signal quality.

For Example, Data transmission between computer and printer.

Following are the advantages of using a parallel transmission mode:

- It is easy to program or implement.

- Data transmission speed is high due to the n-transmission channel.

Following are the disadvantages of using a parallel transmission mode:

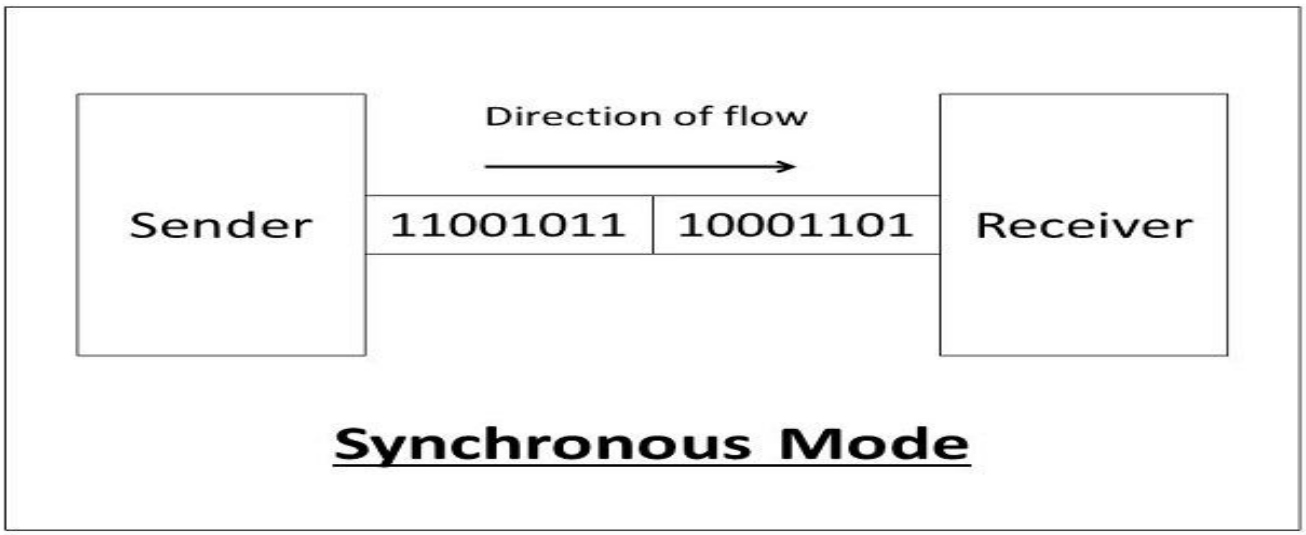
- It requires more transmission channels, and hence cost-ineffective.
- Interference in data bits, likewise in video conferencing.

The data transmission modes can be characterized in the following two types based on the synchronization between the transmitter and the receiver:

- Synchronous Transmission
- Asynchronous Transmission

THE SYNCHRONOUS TRANSMISSION

- **The Synchronous transmission mode is a mode of communication in which the bits are sent one after another without any start/stop bits or gaps between them.** Actually, both the sender and receiver are paced by the same system clock. In this way, synchronization is achieved.
- In a Synchronous mode of data transmission, bytes are transmitted as blocks in a continuous stream of bits. Since there is no start and stop bits in the message block. It is the responsibility of the receiver to group the bits correctly. The receiver counts the bits as they arrive and groups them in eight bits unit. The receiver continuously receives the information at the same rate that the transmitter has sent it. It also listens to the messages even if no bits are transmitted.
- In synchronous mode, the bits are sent successively with no separation between each character, so it becomes necessary to insert some synchronization elements with the message, this is called "**Character-Level Synchronization**".
- For Example, if there are two bytes of data, say(10001101, 11001011) then it will be transmitted in the synchronous mode as follows:



For Example, communication in CPU, RAM, etc.

Following are the advantages of using a Synchronous transmission mode:

- Transmission speed is fast as there is no gap between the data bits.

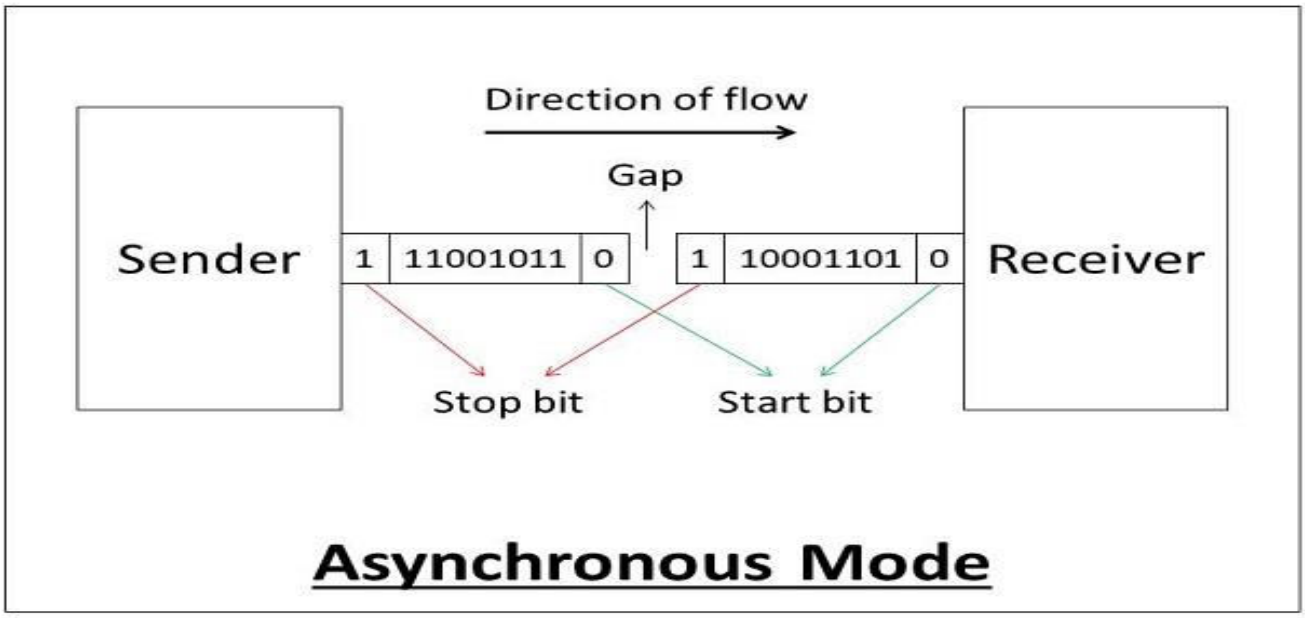
Following are the disadvantages of using a Synchronous transmission mode:

It is very expensive.

ASYNCHRONOUS TRANSMISSION

- **The Asynchronous transmission mode is a mode of communication in which a start and the stop bit is introduced in the message during transmission.** The start and stop bits ensure that the data is transmitted correctly from the sender to the receiver.
- Generally, the start bit is '0' and the end bit is '1'.Asynchronous here means 'asynchronous at the byte level', but the bits are still synchronized. The time duration between each character is the same and synchronized.

- In an asynchronous mode of communication, data bits can be sent at any point in time. The messages are sent at irregular intervals and only one data byte can be sent at a time. This type of transmission mode is best suited for short-distance data transfer.
- For Example, if there are two bytes of data, say(10001101, 11001011) then it will be transmitted in the asynchronous mode as follows:



For Example, Data input from a keyboard to the computer.

Following are the advantages of using an Asynchronous transmission mode:

- It is a cheap and effective mode of transmission.
- Data transmission accuracy is high due to the presence of start and stop bits.

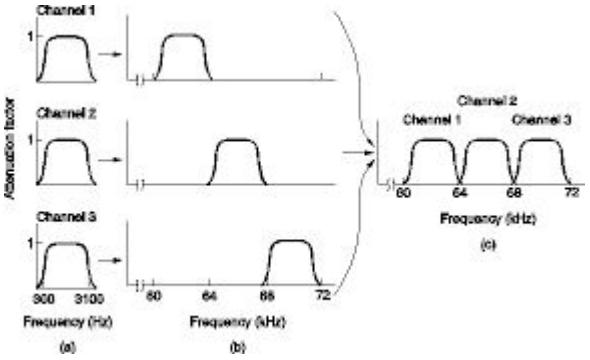
Following are the disadvantages of using an Asynchronous transmission mode:

- The data transmission can be slower due to the gaps present between different blocks of data.

- Telephone companies have developed elaborate schemes for multiplexing many conversations over a single physical trunk.
- These multiplexing schemes can be divided into two basic categories: **FDM (Frequency Division Multiplexing)** and **TDM (Time Division Multiplexing)**.
- In FDM, the frequency spectrum is divided into frequency bands, with each user having exclusive possession of some band.
- In TDM, the users take turns each one periodically getting the entire bandwidth for a little burst of time.

FREQUENCY DIVISION MULTIPLEXING:

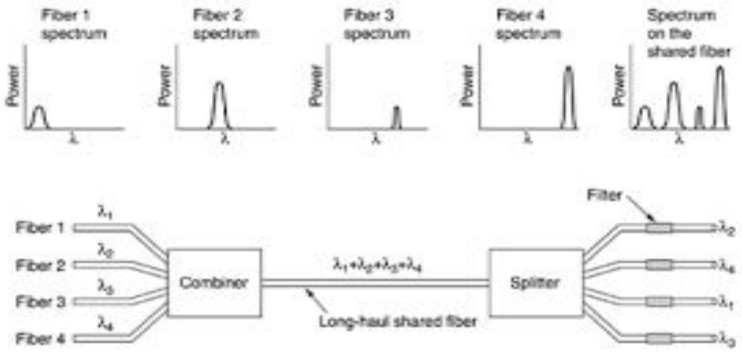
Shows how three voice-grade telephone channels are multiplexed using FDM. Filters limit the usable bandwidth to about 3100 Hz per voice-grade channel. When many channels are multiplexed together, 4000 Hz is allocated to each channel to keep them well separated.



The FDM schemes used around the world are to some degree standardized. A widespread standard is twelve 4000-Hz voice channels multiplexed into the 60-108 kHz band. This unit is called **a group**. The 12 kHz-60 kHz is sometimes used for another group. Many carries offer a 48 to 56-kbps leased line service to customers, based on the group. Five groups (60 voice channels) can be multiplexed to form a**super group**. The next unit is the master group, which are five super groups (CCITT standard) or ten super groups (Bell system). Other standards of up to 230,000 voice channels also exist.

WAVELENGTH DIVISION MULTIPLEXING:

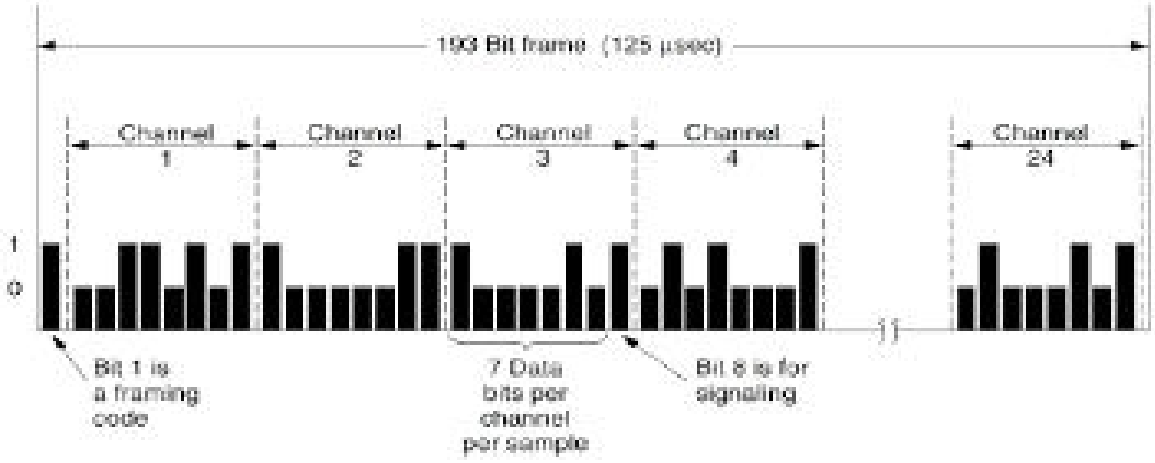
1. For fiber optic channels, a variation of frequency division multiplexing is used. It is called **WDM (Wavelength Division Multiplexing).**
2. The basic principle ofWDM on fibers is depicted. Here four fibers come together at an optical combiner, each with its energy present at a different wavelength.



3. The four beams are combined onto a single shared fiber for transmission to a distant destination.
4. WDM was invented around 1990. The first commercial systems had eight channels of 2.5 Gbps per channel.
5. By 2001, there were products with 96 channels of 10 Gbps, for a total of 960Gbps.
6. This is enough bandwidth to transmit 30 full-length movies per second (in MPEG-2).
7. When the number of channels is very large and the wavelengths are spaced closed together, for example, 0.1 nm, the system is often referred to as **DWDM (Dense WDM)**.
8. WDM is popular is that the energy on a single fiber is typically only a few gigahertz wide because it is currently impossible to convert between electrical and optical media any faster.

TIME DIVISION MULTIPLEXING:

- WDM technology is wonderful, but there is still a lot of copper wire in the telephone system, so let us turn back to it for a while.
- Although FDM is still used over copper wires or microwave channels, it requires analog circuitry and is not amenable to being done by a computer.
- In contrast, TDM can be handled entirely by digital electronics, so it has become far more widespread in recent years.
- It can only be used for digital data. Since the local loops produce analog signals, a conversion is needed from analog to digital in the end office.
- The analog signals are digitized in the end office by a device called a codec (coder-decoder), producing a series of 8-bits numbers.
- At a lower sampling rate, information would be, lost at a higher one, no extra information would be gained. This technique is called PCM (Pulse Code Modulation).
- PCM forms the heart of the modern telephone system.
- The T1 carrier consists of 24 voice channels multiplexed together.
- Each of the 24 channels, in turn, gets to insert 8 bits into the output stream. Seven bits are data and one is for control, yielding 7x8000=56000 bps of data, and 1x8000=8000 bps of signaling information per channel.



The T1 carrier (1.544 Mbps)

- A frame consists of 24x8=192 bits plus one extra bit for framing, yielding 193 bits every 125μsec. This gives a gross data rate of 1.544 Mbps. The 193rd bit is used for frame synchronization.
- When a T1 system is being used entirely for data, only 23 of the channels are used for data. The 24th one is used for a special synchronization pattern, to allow faster recovery in the event that the frame slips.
- A delta modulation is an analog to digital and digital-to-analog signal conversion technique used for transmission of voice information where quality is not of primary.

INTERFACING

1. direction of transmission

- simplex : one way (one-way street)
- half duplex : either way, but only one at a time (single line railroad)
- full duplex : both ways concurrently (two-way street)

2. synchronization

- asynchronous : data may appear at any time
- synchronous : sender and receiver work in lock-step

3. serial/parallel

- serial : one bit after the other
- parallel : multiple bits at once
- (hardware required to convert)

4. DTE / DCE

- DTE : Data Terminal Equipment (e.g. computer)
- DCE : Data Circuit-terminating Equipement (e.g. modem)
- Info originates and terminates at DTE
- DCE converts info to signals and vice versa

5. Interface

- For purposes of this chapter: Connection between DTE and DCE.

Common Physical Interface Standards

- Examples from two organizations: EIA, ITU-T
- EIA: Electronic Industries Association
- ITU-T : International Telecommunications Union - Telecom standards
- Interface standards comprise:
  - *Mechanical* : wiring and connectors
  - *Electrical* : signals
  - *Functional* : protocol for using signals

EIA-232 Standard

- aka RS-232 (Recommended Standard, from early 60s)
- *mechanical :*
  - male DB-25 connector on DTE end (cable has female)
  - female DB-25 connector on DCE end (cable has male)

    - cable length limited to 50 ft. (15 m.)
    - 20kbps limit
- *electrical:*
    - digital signal, NRZ-L (NRZ) encoding
    - 1 encoded as voltage in range -3v to -15v
    - 0 encoded as voltage in range +3v to +15v
    - (wide range allows transmission on noisy line)
- *functional:*
    - most of the 25 pins have defined functions
    - few of them are normally used, most for control
    - pin 2 for transmitted data (transmitted from DTE)
    - pin 3 for received data (transmitted from DCE)
    - can be used for half or full-duplex

Typical EIA-232 modem usage scenario (Handshakin')

Unless you have the handout (Halsall, Figure 2.32, p84), you may have difficulty following this scenario.

Connection

- calling DTE: set DTR (DTE Ready, pin 20) on
- calling DCE: set DSR (DCE Ready, pin 6) on
- calling DTE sends calling DCE the dialing command
- calling DCE dials the call
- *called DCE sets RI (ring indicator, pin 22) on (getting the ring)*

- *called DTE sets RTS (request to send, pin 4) on*
- *called DCE transmits carrier signal to calling DCE*
- *called DCE sets CTS (clear to send, pin 5) on*
- calling DCE detects carrier and sets CD (carrier detect, pin 8) on

Invitation

- *called DTE transmits "invitation to send" on TxD (Transmit data, pin 2)*
- *called DCE transmits message to calling DCE*
- calling DCE hands message DTE on RxD (Receive data, pin 3)
- *called DTE set RTS (request to send, pin 4) off*
- *called DCE stops transmitting carrier signal to calling DCE*
- *called DCE sets CTS (clear to send, pin 5) off*
- calling DCE detects carrier gone, and sets CD (carrier detect, pin 8) off

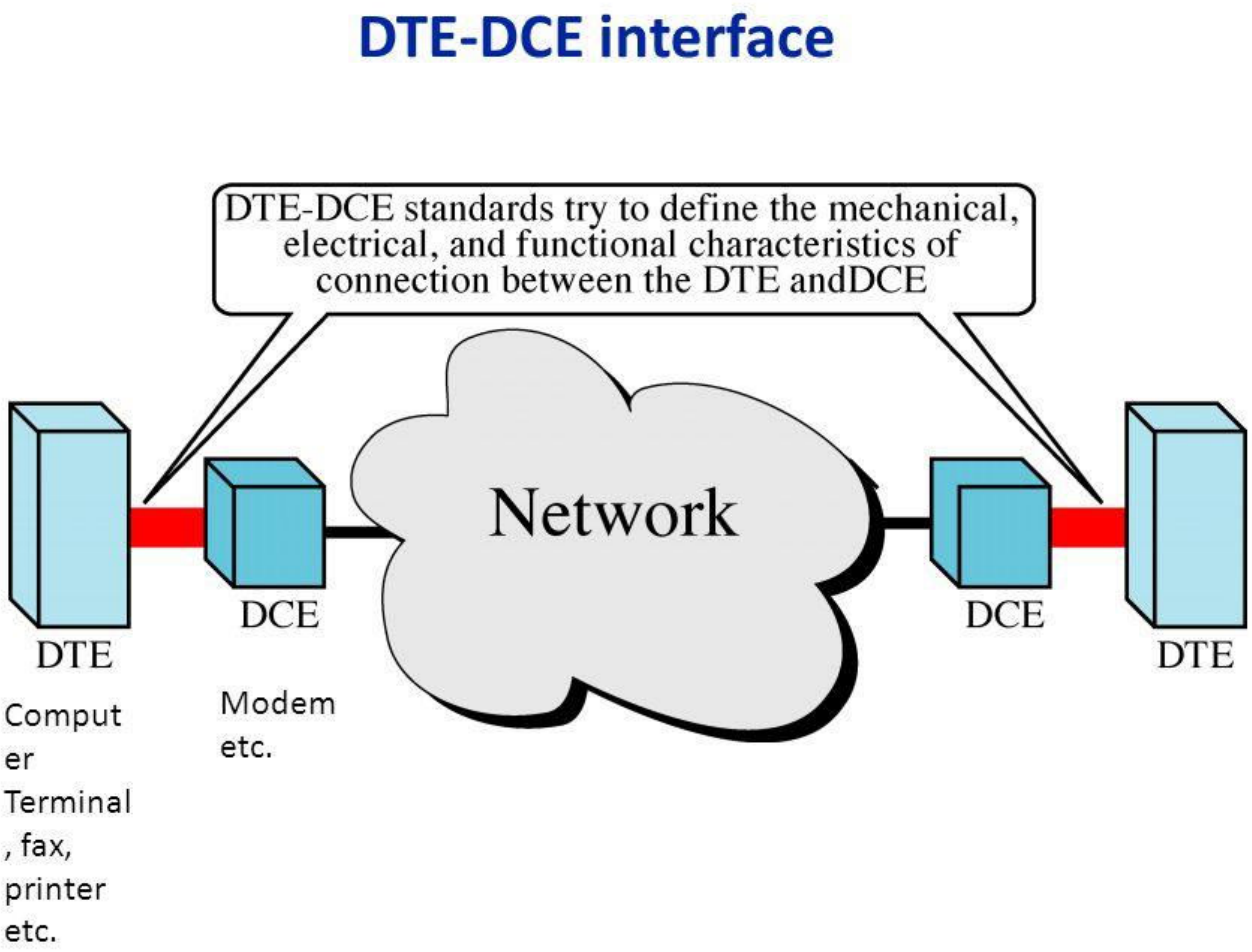
Data Transfer

- calling DTE sets RTS (request to send, pin 4) on
- calling DCE transmits carrier signal
- *called DCE sets CD (pin 8) on*
- calling DCE sets CTS (clear to send, pin 5) on
- calling DTE hands message to DCE on TxD (pin 2)
- calling DCE transmits message to called DCE
- *called DCE hands data message to DTE on RxD (pin 3)*
- **repeat in either direction until all data transfers complete**

Terminate

- both DTE set RTS (request to send, pin 4) off

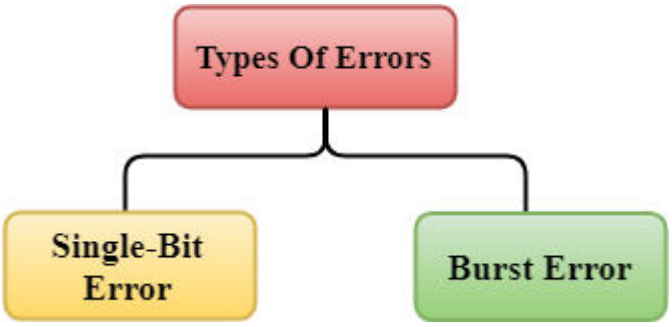
- both DCE stop transmitting carrier
- both DCE set CD (carrier detect, pin 8) off
- both DCE set CTS (clear to send, pin 5) off
- both DTE set DTR (DTE ready, pin 20) off
- both DCE set DSR (DCE ready, pin 6) off



Error Detection

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

Types Of Errors

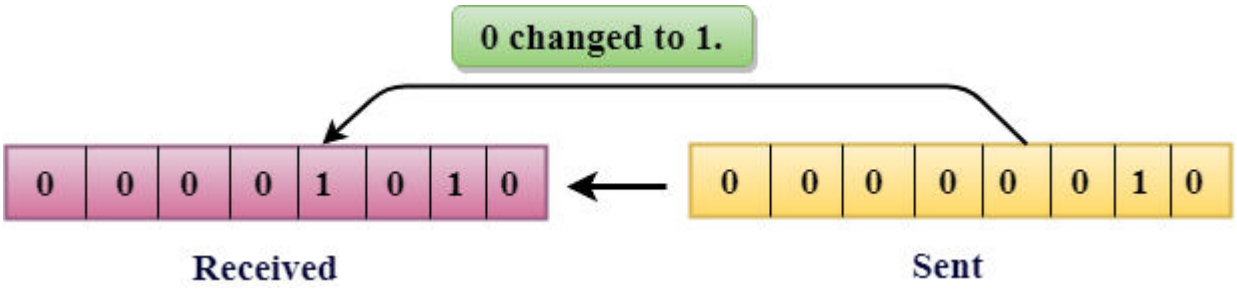


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



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

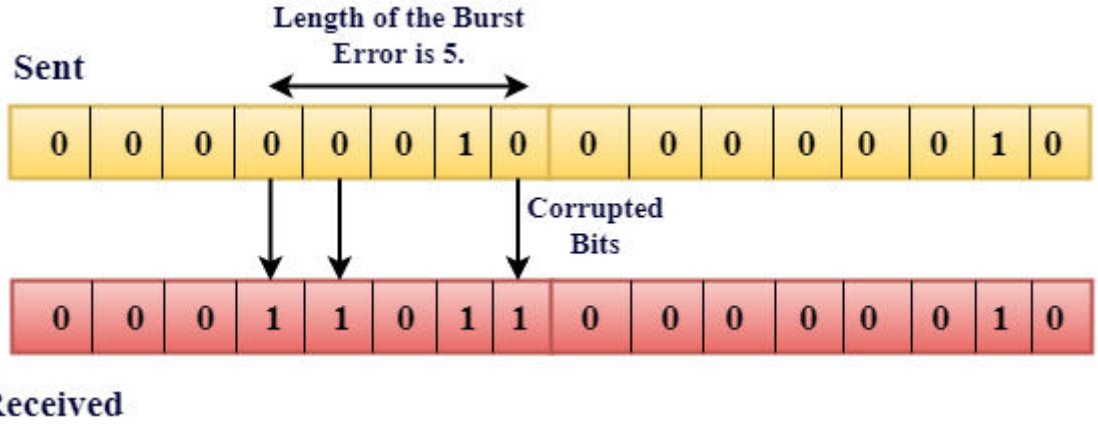
Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.



The duration of noise in Burst Error is more than the duration of noise in Single-Bit.

Burst Errors are most likely to occurr in Serial Data Transmission.

The number of affected bits depends on the duration of the noise and data rate.

Error Detecting Techniques:

The most popular Error Detecting Techniques are:

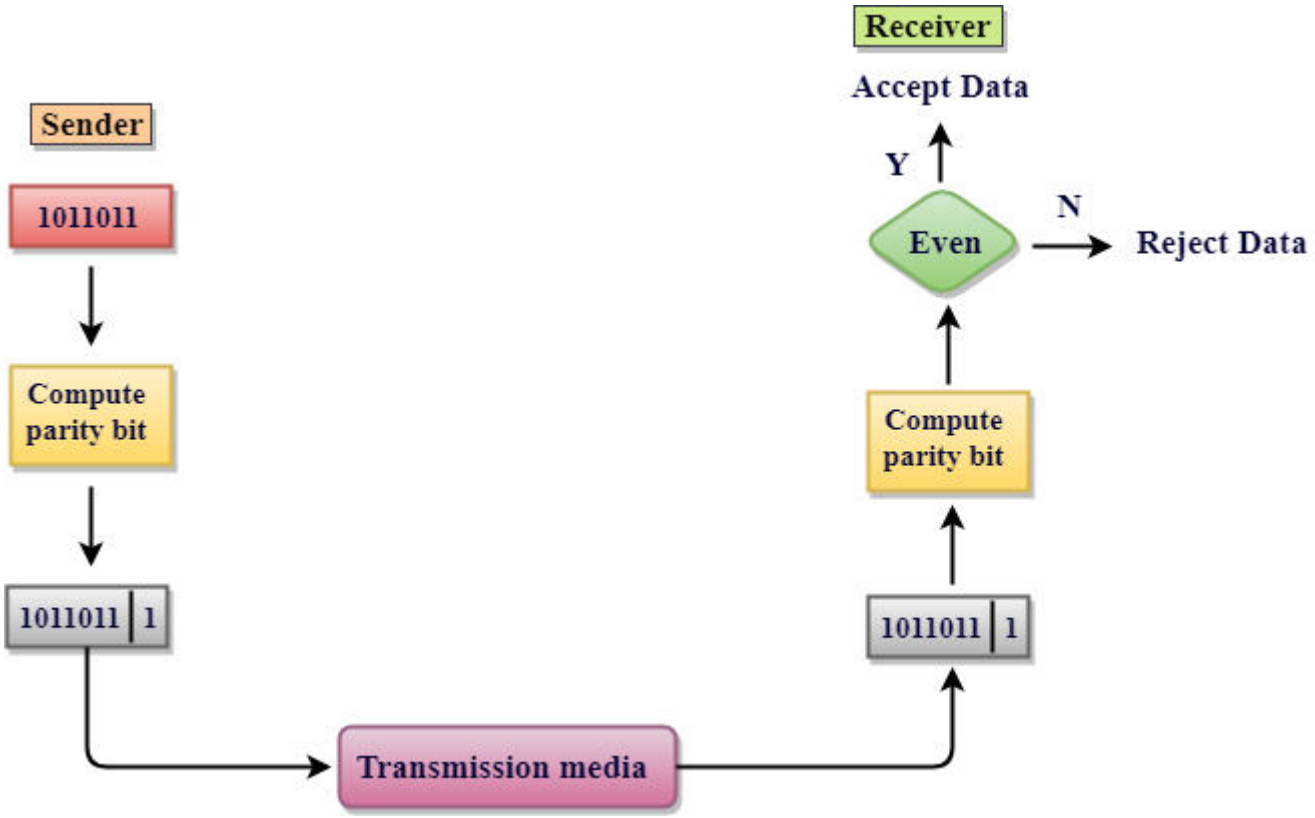
- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

Single Parity Check

- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s

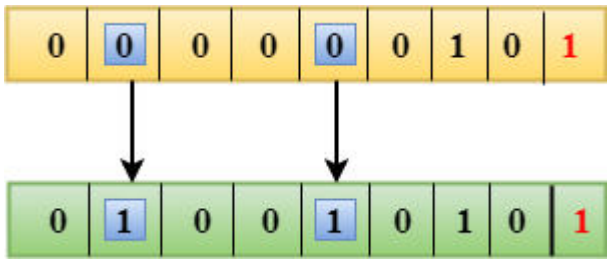
becomes even. Therefore, the total number of transmitted bits would be 9 bits.

- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.



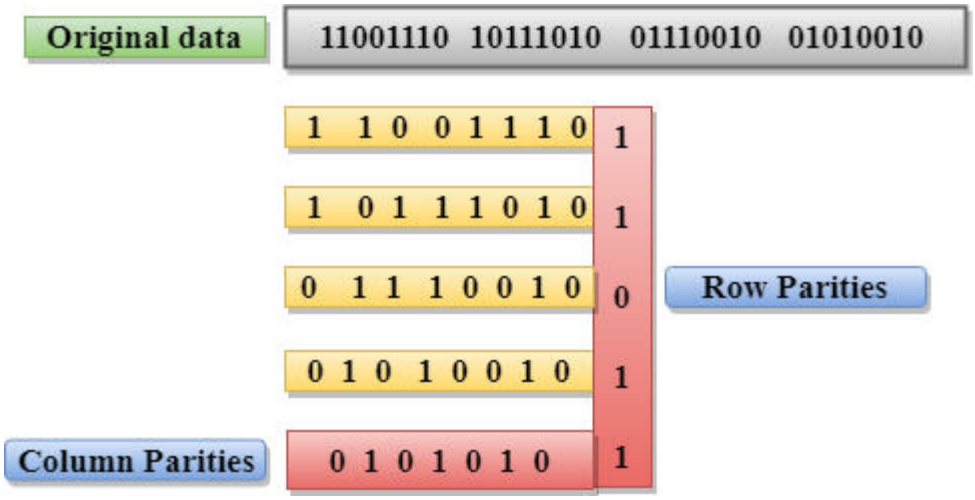
Drawbacks Of Single Parity Checking

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



Two-Dimensional Parity Check

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



Drawbacks Of 2D Parity Check

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

Checksum

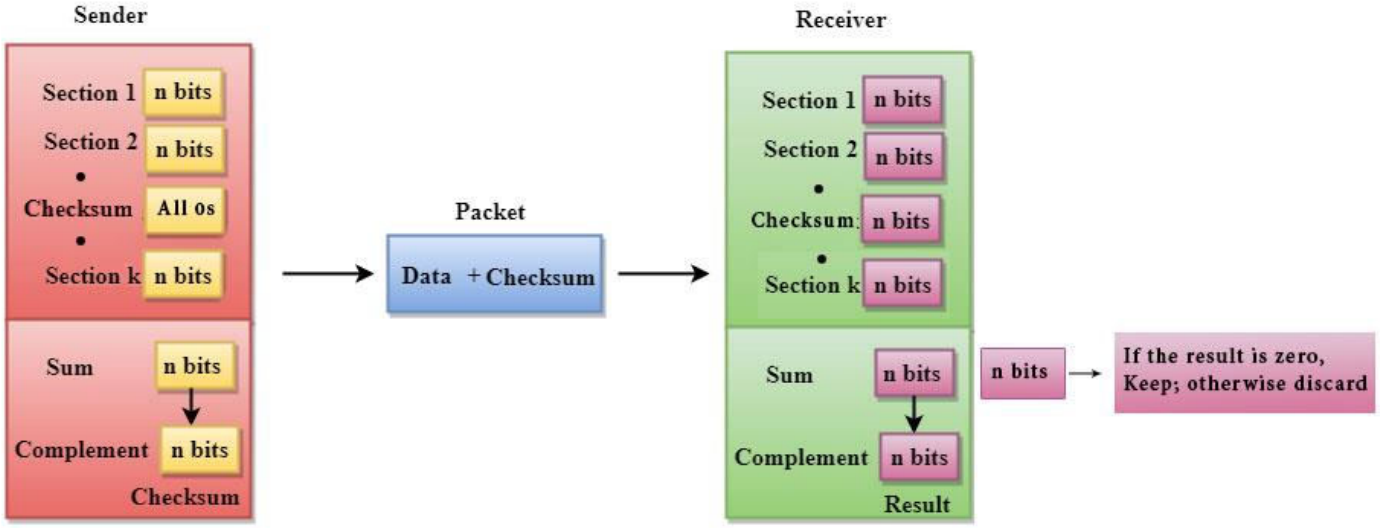
A Checksum is an error detection technique based on the concept of redundancy.

It is divided into two parts:

Checksum Generator

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

Suppose L is the total sum of the data segments, then the checksum would be ?L



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

Checksum Checker

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

1. The Receiver follows the given steps:
2. The block unit is divided into k sections and each of n bits.

3. All the k sections are added together by using one's complement alg orithm to get the sum.
4. The sum is complemented.
5. If the result of the sum is zero, then the data is accepted otherwise th e data is discarded.

Cyclic Redundancy Check (CRC)

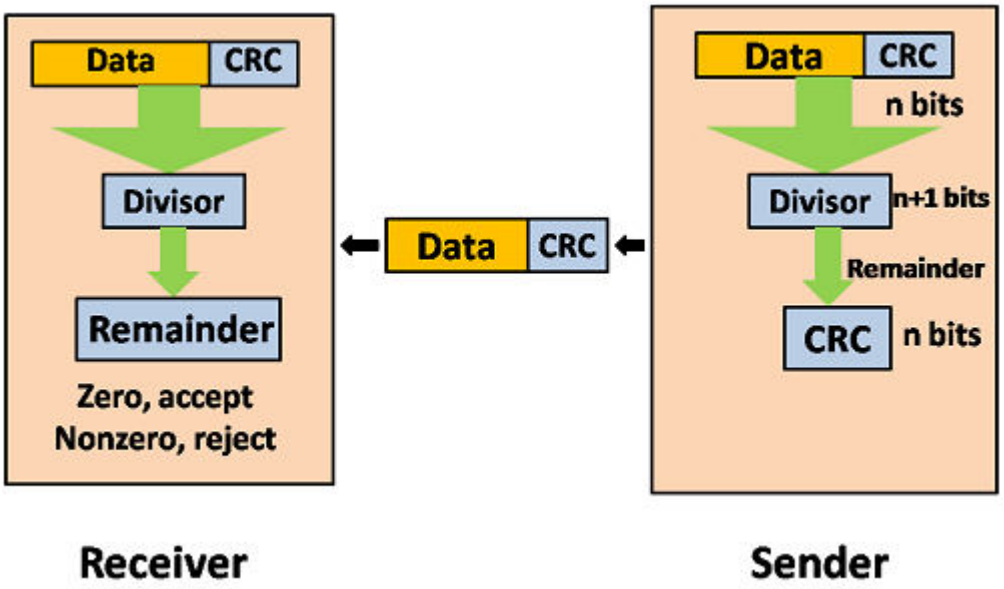
CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection:

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

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

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

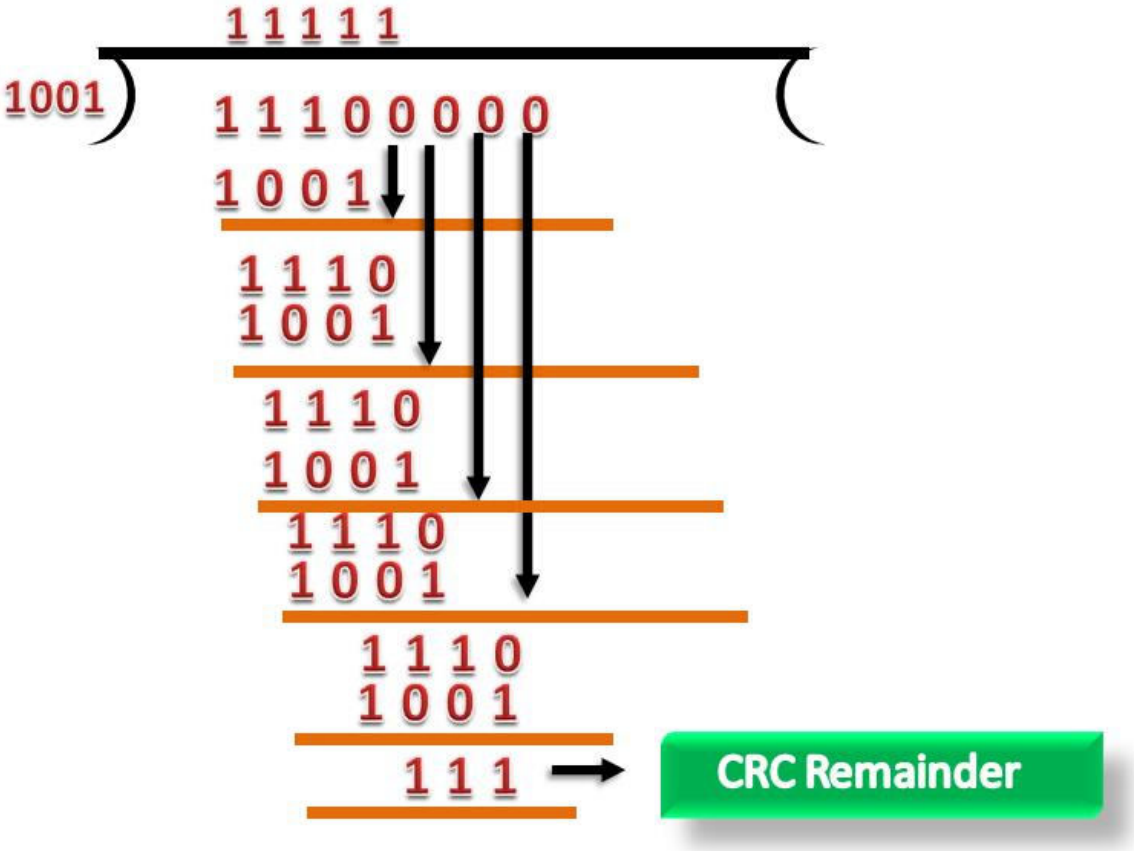


Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

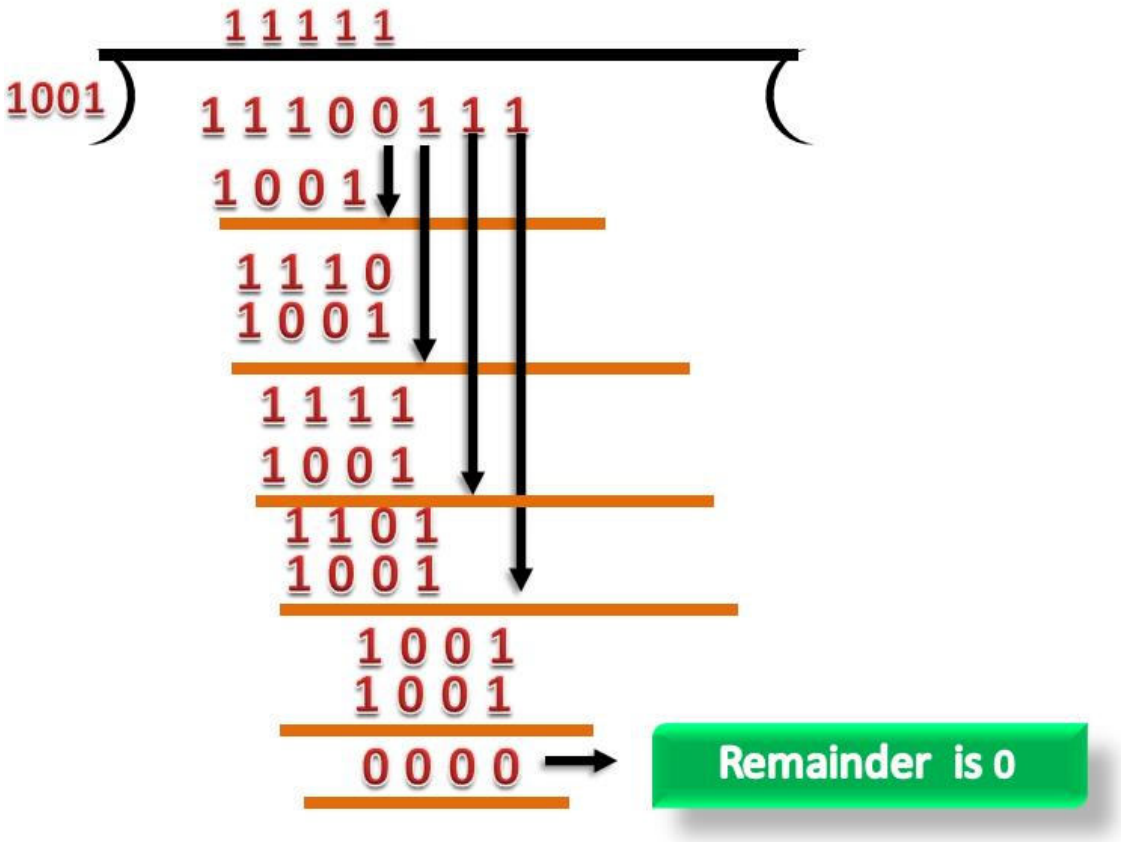
CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



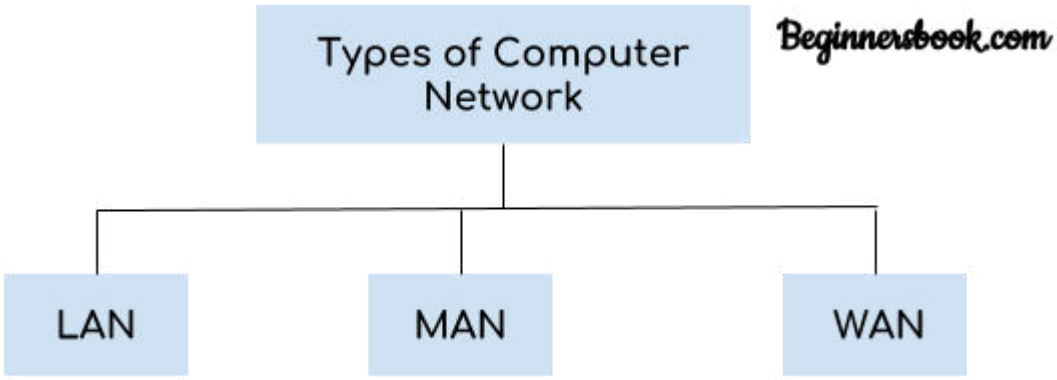
CRC Checker

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


11111
1001
11100111
1001
1110
1001
1111
1001
1101
1001
1001
1001
0000
Remainder is 0

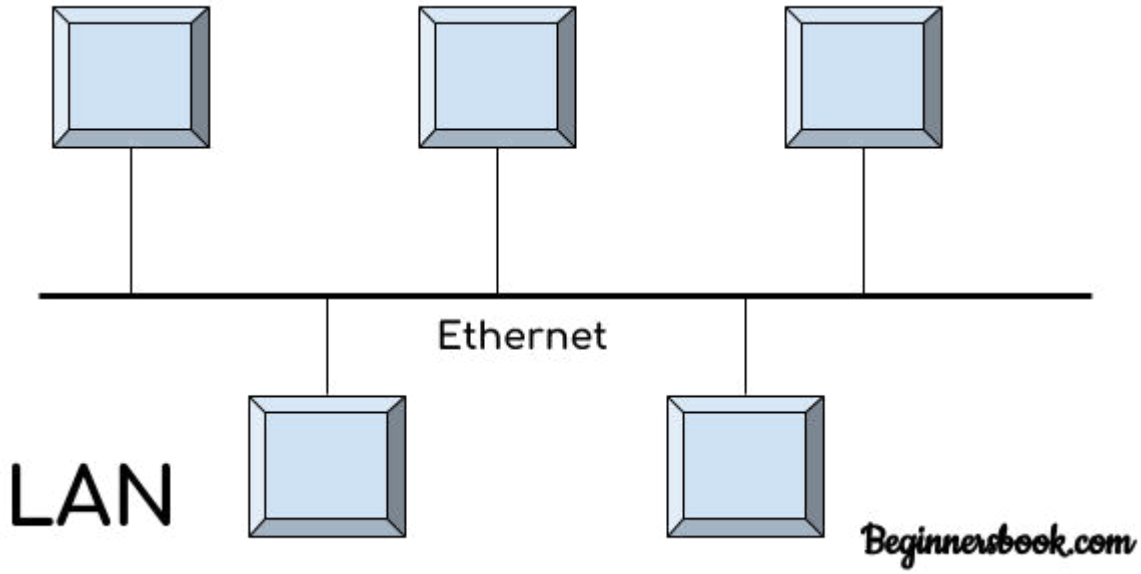
UNIT II -LAN: Types of Network and Topology-LAN Transmission Equipment- Token Bus-Token Ring-FDDI Ethernet Technologies. WAN: WAN Transmission methods- WAN carrier types- WAN Transmission Equipment-WAN Protocols

Types of Computer Network

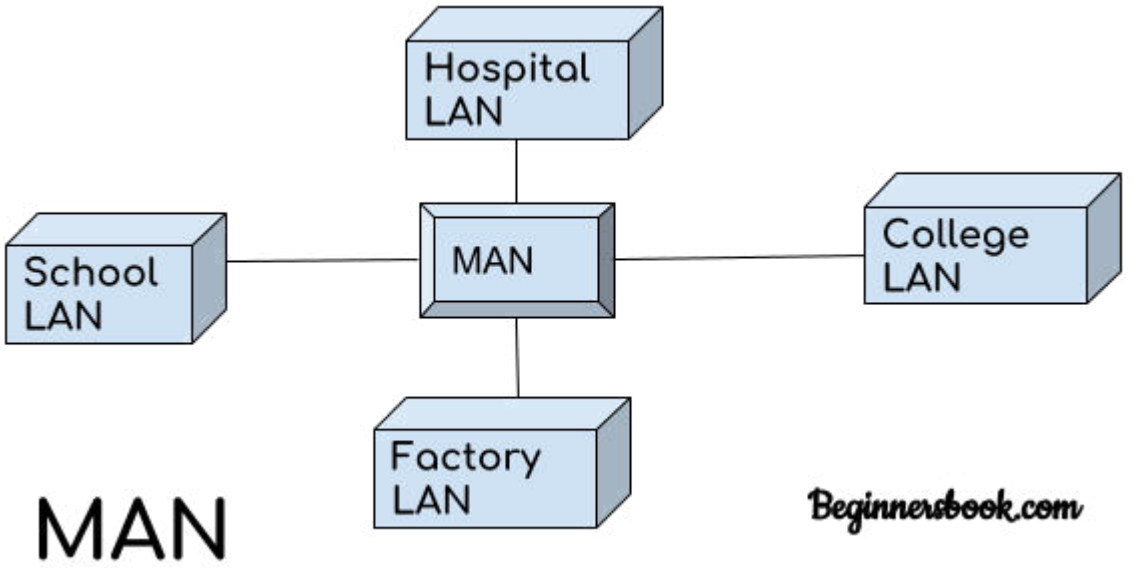


There are mainly three types of computer networks based on their size:
1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

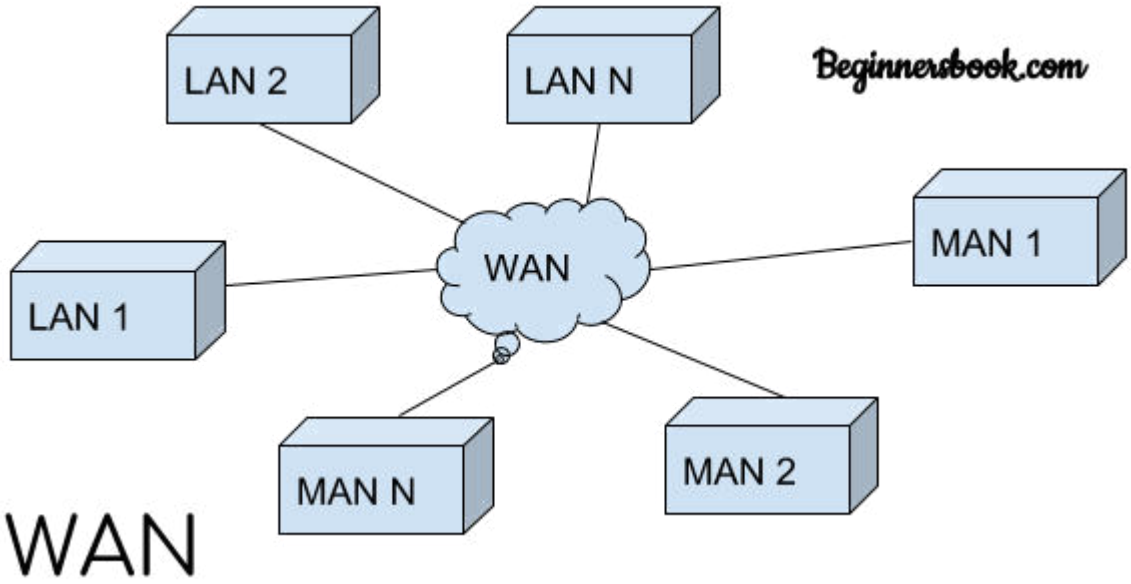
1. Local Area Network (LAN)



2. Metropolitan Area Network (MAN)



3. Wide area network (WAN)



LAN Transmission Equipment:

LAN Transmission Equipment is used to connect devise on a single network, to create and connect multiple networks or sub-networks, and to set up a campus enterprise. These are included the followings:

1. Network Interface Card
2. Repeaters
3. Hubs

4. Bridges

5. Routers

6. Brouters

7. Switches

8. Gateway

1) Network Interface Card

It is used to enable a network device, such as a computer equipment, to connect to the network. The network connection requires four components: *An appropriate connector for the network medium. *A transceiver *A controller to support the Media Access Control data link protocol *Protocol control firmware The connector and its associated circuits are designed for a specific type of medium, for example, coax, and twisted pair or optical fiber. The cable connector is attached to the transceiver, which may be external to the NIC or built into it. The MAC controller unit and the firmware work together to correctly encapsulate source and destination address, the data to be transported and the CRC information into the service data unit.

The MAC controller and firmware are customized for particular type of network transport, which can be any one of the following:

Ethernet

Fast Ethernet

Gigabit Ethernet

Token ring

Fast token ring

Fast Distributed Data Interface

Asynchronous Transfer Mode

Ethernet, Fast Ethernet, high speed communication. It is able to handle both half and full duplex transmission.

Repeaters:

It is an electronic device that operates on only the physical layer of the OSI model. It connects one or more cable segments and retransmits any incoming signal to all other segments. For example the maximum distance that a single can travel on an Ethernet cable segment is 500 meters but one repeater cans double the effective length of an Ethernet to 1,000 meters. Repeaters are not capable of connecting two dissimilar network technologies.

Hub:

It is a central network device that connects network nodes. It contains the star topology. Hub may be referred to as a connector, and is a device that can have multiple inputs and outputs, all active at one time. Provide a central unit from which to connect multiple nodes into one network. Permit large numbers of computers to be connected on single or multiple LANs. Reduce network congestion by centralizing network design. Provide multi-protocol services. Consolidate the network backbone. Enable high speed communication. Provide connections for several different media types. Enable centralizes network management. It also called multistation access unit. Operating as a central hub an MAU functions at the OSI physical and data link layers.

There are different kinds of hubs: **1. Passive hub** (acts as path way) Data to follow from one device to another. **2.Intelligent hub:** It can detect errors and provide assistance to a technician when attempting to locate a failing component. **3.Active hub:** Regenerate and process signals.

Bridge:

It is a network device that connects one LAN segment to another. It is high efficiency and security. It performs error detection, frame formatting, frame

routing. Bridges are used: Extend a LAN when the maximum connection limit such as the 30- node limit on an Ethernet segment, has been reached. Extend a LAN beyond the length limit, for example beyond 185metres with thin-net Ethernet.

Segment LANs to reduce data traffic bottlenecks.

Prevent unauthorized access to a LAN.

If the bridge knows that the destination of a frame is on the segment as the source of the frame, it drops the frame because there is no need to forward it. If the bridge does not know the destination segment, the bridge transmits the frame to all segments except the source segments, a process that is called flooding. Bridges can greatly enhance the performance of a network because they offer the ability to segment network traffic, limiting traffic to those networks where it belongs. A firewall is software or hardware that sources data from being accessed outside a network and that can also prevent data from leaving the network through an inside source.

ROUTER:

A router performs some of the same function as a bridge. Routers connect LANs at the network layer of the OSI model, which enables them to interpret more information from packet traffic than bridges can. In general, routers are used to: Efficiently direct packets from one network to another, reducing excessive traffic.

Join neighboring or distant network. Connect dissimilar networks. Prevent network bottlenecks by isolating portions of a network. Secure portions of a network from intruders. The logic that routers use to determine how to forward data is called a routing algorithm.

BROUTER: A bridge router (brouter) performs both the functions of a bridge (OSI layer 2) and a router (OSI layer 3) in a single device. A brouter is a network device that acts as a bridge in one circumstance and as a router in another. Brouters are used to:

Handle packets efficiently on a multiprotocol network that includes some protocols that can be routed and some that cannot be.

Isolate and direct network traffic to reduce congestion.

Join networks. Secure a certain portion of a network by controlling who can access it.

SWITCHES:

A switch is a device that connects two or more network segments and allows different nodes to communicate smoothly with each other as if they are the only two connecting at the time. Switches provide bridging capacity Along with the ability to increase the bandwidth on existing networks. Switches used on LANs are similar to bridges. A switch may act as a multiport bridge to connect devices or segments in a LAN. A store-and-forward switch stores the frame in the input buffer until the whole packet has arrived. A cut-through switch on the other hand. Forwards the packet to the output buffer as soon as the destination address is received.

GATEWAYS: Gateways usually operate at OSI layer 4 or higher, and basically translate the protocols to allow terminals on two dissimilar networks to communicate. Gateways can be either/or combinations of hardware and software. An internet service provider (ISP), which connects users in a home to the Internet, is a gateway. Gateways can suffer from slow performance. A dedicated computer acting as a gateway, if it is of reasonable speed, usually eliminates any performance problems. For examples, you might use a gateway to:

Convert commonly used protocols (e.g. TCP/IP) to a specialized protocol (for example, an SNA: System Network Architecture).

Convert message formats from one format to another.

Translate different addressing schemes.

Link a host computer to a LAN.

Provide terminal emulation for connections to a host computer. Direct electronic mail to the right network destination.

Connect networks with different architectures.

FIBRE DISTRIBUTED DATA INTERFACE (FDDI)

The fiber distributed data interface (FDDI) standard for a 100Mbps fiber optic LAN was developed during the mid-1980s by a subcommittee of ANSI and was completed in 1990. LANs based on the IEEE 802 standards reached capacity, optical fiber LANs based on the FDDI standard became an alternative growth path.

FDDI LANs were used to provide high-speed backbone connections between distributed LANs Two types:

Single mode fiber (SMF) and

Multimode fiber (MMF)

Single mode fiber: it can deliver connectivity over longer distances, with higher performance than MMF.

Multimode fiber is usually used to connect devices within a building or a small geographically contained area.

FDDI has implemented over twisted pair copper wire. The copper distributed data interface (CDDI) called uses only shielded twisted pair or unshielded twisted pair category 5 cabling but supports distances of 100 meters and data rates of 100 Mbps.

FDDI network contains two complete rings one that is used to send data when everything is working correctly, and another that is used only when the first ring fails.

Ethernet Technologies:

Most common Ethernet Technologies are

10 Base-2 Ethernet

Base-5 Thick Ethernet Technology

10 Base-7 and 100 Base-T

Gigabit Ethernet

WAN TRANSMISSION METHODS

WAN transmission methods use different switching techniques. Switching techniques are use to create one or more data paths called channels for transmitting data. The channels may be created using one communication cable or using several cables that offer a range of paths along which data can be transmitted. Switching can enable multiple nodes to simultaneously transmit and receive data or it can enable data to be transmitted over different routes to achieve maximum efficiency in terms of speed and cost. The following are the common switching techniques used in WANs:

Time Division Multiple Access (TDMA)

Frequency Division Multiple Access (FDMA)

Statistical Multiple Access

Circuit Switching

Message Switching

Packet Switching

Time-Division Multiple Access (TDMA)

TDMA divides the channels into distinct time slots. Each time slot is designated for a particular networks node, as if it were a dedicated line. The WAN switching deice rotates from time slot to time slot for each channel. This is similar to a 24-hour television programming, where the time has been specified for a particular program. TDMA does not guarantee the most efficient use of the network medium since transmission occurs only via one channel at a time. The timing of node transmission is also important, since a node may transmit at an interval that is out of synchronization with its time slot.

Frequency Division Multiple Access (FDMA)

FDMA divides the channels into frequencies instead of time slots. Each channel has its own broadcast frequency and bandwidth. The switching device switches from frequency to frequency as it sends data. This is similar to four listeners with headsets sharing a radio modified to have four channels. The first listener might be listening to a classical station, the send to a talk show the third to a base ball game and thr fourth to the news. Each listener is at a different frequency. The radio inputs to each channel so quickly that none can tell it is quickly switching from channel to channel as it receives the signal on each frequency.

Statistical Multiple Access (SMA)

Statistical multiple access or statistical multiplexing, is sued by many WAN technologies, such as X.25, ISDN and frame relay. This method is more efficient than TDMA and FDMA, because the physical medium bandwidth is dynamically allocated according to the application need. The switching device continuously monitors each channel to determine the communication requirements. For example, at one moment a channel may need to transmit a large graphics file, and then be quiet. Algorithms on the switch determine the bandwidth needed to transmit the file. After the file is transmitted, the switch reallocates bandwidth to another channel. This might be compared to the way in which a workstation operating system automatically decides how much memory to give to three applications running at the same time. It might give 15 KB for an active word processing file, 7 MB for an image from a scanner and 1.2MB for printing a graphic.

Circuit Switching

Circuit switching involves creating a dedicated physical circuit between the sending and receiving nodes. This acts as a straight channel on which to send data back and forth without interruption, similar to a telephone call between two parties. The transmission channel remains in the service until the two nodes disconnect. Communication via circuit switching implies that

there is a dedicated communication path between two stations. The path is a connected sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection. Communication via circuit switching involves there phases. Phase I: Circuit establishment. Before any signals can be transmitted an end-to-end (station to station) circuit must be established. For example, station A sends a request to node4, requesting a connection to Station E. Typically, the link from A to 4 is a dedicated line, so that part of the connection already exists. Node 4 must find the next leg in a route leading to node 6 based on routing information and measures of availability and perhaps cost. Node 4 selects the link to node 5, allocates a free channel (using FDM or TDM) on that link and sends a message requesting connection to E. So far, a dedicated path has been established from A through 4 to 5. Because a number of stations may attach to 4, it must be able to establish internal paths from multiple stations to multiple nodes. The remainder of the process proceeds similarly. Node 5 dedicates a channel to node 6 and internally ties that channel to the channel from node 4. Node 6 completes the connection to E. In completing the connection, a test is made to determine if E is busy or is prepared to accept the connection.

Phase II: Data Transfer. Information can now be transmitted from A through the network to E. The data may be analog or digital, depending on the nature of the network. As the carriers evolve the fully integrated digital networks, the use of digital (binary) transmission for both voice and data is becoming the dominant method. The path is: A-4 link, internal switching through4; 4-5 channel, internal switching through 5; 5-6 channel, internal switching through 6; 6-E link. Generally the connection is fully duplex.

Phase III: Circuit disconnect. After some period of data transfer, the connection is terminated, usually by the action of one of the two stations. Signals must be propagated to nodes 4,5 and 6 to deallocate the dedicated resources. Note that the connection path is established before data transmission begins. Thus, channel capacity must be reserved between each

pair of nodes in the path and each node must have available internal switching capacity to handle the request connection. The switches must have the intelligence to make these allocations and to devise a route through the network. Circuit switching can be rather inefficient. Channel capacity is dedicated for the duration of a connection, even if no data are being transferred. For a voice connection, utilization may be rather high, but it still does not approach 100 per cent. For a terminal-to-computer connection, the capacity may be ideal during most of the time of the connection. In terms of performance, there is delay prior to signal transfer for call establishment. However, once the circuit is established, the network is effectively transparent to the users. Information is transmitted at a fixed data rate with no delay other than the propagation delay through the transmission links. The delay at each node is negligible. Circuit switching was developed to handle voice traffic but is now also used for data traffic. The best known example of a circuit-switching network is the public telephone network. This is actually a collection of national networks intern-connected to form the international service. Although originally designed and implemented to service analog telephone subscribers, it handles substantial data traffic via modem and is gradually being converted to a digital network. Another well known application of circuit switching is the private branch exchange (PBX) used to interconnect telephones within a building or office 7.1.5 Message Switching Message switching uses a store-and-forward communication method to transmit data from the sending to the receiving node. The data is send from one node to another, which stores is temporarily until a route towards the data‟s final destination becomes available. Several nodes along the route store and forward the data until it reaches the destination node. Message switching is used for example, when you send an e-mail message on an enterprise network with file servers acting as “post offices”. The message goes from one post office to the next until it reaches the intended recipient.

Packet Switching Circuit switching was designed for voice communication. In a telephone conversation, for example once a circuit is established it

remains connected for the duration of the session. Circuit switching creates temporary (dialed) or permanent (leased) dedicated links that are well suited to this type of communication. A key characteristic of circuit-switching networks is that resources within the network are dedicated to a particular call. For voice connections, the resulting circuit will enjoy a high percentage of utilization because most of the time, one party or the other is talking. However, as the circuit-switching network began to be used increasingly for data connections, two shortcomings became apparent.

1) In a typical user/host data connection (for example, a personal computer user logged on to a database server) much of the time the line is idle. Thus, with data connections, a circuit-switching approach is inefficient.

2) In a circuit-switching network, the connection provides for transmission at a constant data rate. Thus, each of the two devices that are connected must transmit and receive at the same data rate as the other. This limits the utility of the network in interconnecting a variety of the host computers and workstations. To understand how packet switching addresses these problems, let us briefly summarize the packet-switching operation. Data are transmitted in short packets. A typical upper bound on packet length is 1000 octets (bytes). If the source has no longer message to send, the message is broken up into a series of packets as shown in Figure. Each packet contains a portion (or all for a short message) of the user‟s data, plus some control information that the network requires to be able to route the packet through the network and deliver it to the intended destination. At each node en route, the packet is received, stored briefly and passed on to the next node. Now assume that Figure depicts a simple packet-switching network. Consider a packet to be send from Station A to Station E. The packet includes control information that indicates that the intended destination is E. the packet is send from A to node 4 stores the packet, determines the next leg of the route (say 5) and queues the packet to to-out on that link (the 4-5 link). When the link is available, the packet is transmitted to node 5, which forwards the packet to node 6 and finally to E. This approach has a number of advantages

over circuit switching: ϖ Line efficiency is greater, because a single node-to-node link can be dynamically shared by many packets over time. The packets are queued up and transmitted as rapidly as possible over the link. By contrast, with circuit switching, time on a node-to-node link is pre-allocated using synchronous time-division multiplexing. Much of the time, such a link may be ideal because a portion of its time is dedicated to a connection that is ideal.

A packet-switching network can perform date-rate conversion. Two stations of different data rates can exchange packets because each connects to its node as its proper data rate.

When traffic becomes heavy on a circuit-switching network, some calls are blocked; that is, the network refuses to accept additional connection requests until the load on the network decreases. On a packet-switching network, packets are still accepted, but delivery delay increases.

Priorities can be used. Thus, if a node has a number of packets queued for transmission; it can transmit the higher-priority packets first. These packets will therefore experience less delay than lower-priority packets. If the station has a message to send through a packet-switching network that is of length greater than the maximum packet size, it breaks the message up into packets and sends these packets, one at a time, to the network. A question arises as to how the network will handle this stream of packets as it attempts to route them through the network and deliver them to the intended destination. There are two approaches that are used in contemporary networks: datagram and virtual circuit.

In the datagram approach to packet switching, each packet is treated independently from all others. Even when one packet represents just a piece of a multi packet transmission, the network (and network layer functions) treats it as though it existed alone. Packets in this technology are referred to as datagram‟s. Figure shows how the datagram approach can be used to deliver three packets from Station A to Station E. In this example, all the

three packets (or datagram)belong to the same message, but may go by different paths to reach their destination. This approach can cause the datagrams of transmission to arrive at their destination out of order. It is the responsibility of the transport layer in most protocols to reorder the datagrams before passing them on to the destination port. The link joining each pair of nodes can contain multiple channels. Each of these channels is capable, in turn, of carrying datagrams either from several different sources or from one source. Multiplexing can be done using TDM or FDM. In the virtual circuit approach to packet switching. The relationship between all packets belonging to a message or session is preserved. A single route is chosen between the send and receiver at the beginning of the session. When the data are sent, all packets of the transmission travel one after another along that route. The difference from the datagram approach is that, with virtual circuits, the node need not make a routing decision for each packet. It is made only once for all packets using the virtual circuit.

WAN CARRIER TYPES

There are several physical signaling or carrier methods for transporting data on WANS. Some of the most common include the following:

Point to point

T-carrier

SONET

ISDN

Wireless .

Point-to-Point

Point-to-point carrier communications through public dial-up lines and leased telephone lines represent the most basic WAN carrier communications. For example, a simple WAN is established every time you employ a modem to make a modem-to-modem connection over a dial-up line. The modem at the other end may be connected to a network or to a

computer that is a few miles away or a few thousand miles away. The physical mode of communication is an analog circuit that goes through telephone switching stations to establish a connection that lasts only as long as the communications sessions. Another form of point-point communication is a leased telephone line that is used exclusively between two points, such as between a state university and the state Government offices. It bypasses the need to dial and find a switched circuit for a connection each time a communication session is started. Leased lines sometimes come with the line conditioning to reduce noise and provide more reliable communication than dial-up lines.

T-Carrier

A T-Carrier line is a dedicated telephone line that can be used for data communications to connect two different locations for continuous point-to-point communication. For example, some universities use T-Carrier lines to connect to one another for Internet communications. Some states use T-carrier lines to connect branch offices and colleges to the government headquarters in the state capital. These lines offer dependable service over very long distances. T-carriers operate in a logical topology as the smallest T-carrier service; T-1 offers 1.544 Mbps data communication that can be switched to create multiple data channels for high speed communication, as shown in Table. T-Carrier Services and Data Rate T-Carrier Data Transmission T-1 switched channels Data Signal rate Level Functional T-1 4 Kbps T-1 Sub-Channels DS-0 T-1 1.544 Mbps 1 DS-1 T-1C 3.152 Mbps 2 DS-1C T-2 6.312 Mbps 4 DS-2 T-3 44.736 Mbps 28 DS-3 T-3C 89.471 Mbps 56 DS-3C T-4 274.176 Mbps 168 DS-4 For example, switching T-1 to the next level of service (called T-2) creates four channels T-3 has 28 channels, and T-4 has 168 channels. Because T-carrier service is expensive, telephone companies offer functional services that use a portion of the T-1 services utilizing sub-channels with 64 Kbps speeds. This is possible because each T1 service consists of 24 sub-channels, each of 64 Kbps called digital signal at level 0 (DS-0) channels. An alternative to T-carrier lines is

switched synchronous 56 Kbps communications and switched asynchronous 57.6 Kbps communications. Both provide digital communication through data compression techniques and by using circuit switching methods that combine to yield an actual throughput of up to four times the base rate. Organizations use switched 56 Kbps communications because the rates are less than for T-carrier service and for the backup line required; to be used when the main T-carrier service is down. T-carriers use one of the two types of switching techniques for transmitting information. One is time division multiple access (that is, TDMA) and the other is a combination of TDMA and statistical multiple access, which is the fast packet technology. The fast packet switching enables T-carrier service to take into account different channel access needs for handling voice, video and data.

SONET

Synchronous Optical Network (SONET) is a standard for transmitting data on optical fibers. It was originally created to allow easier connection between carriers that were using different vender‟s products for their optical networks. SONET has become the de facto standard for carrying voice and data traffic over an optical network and ANSI has written a standard for it. SONET is a high speed technology for WANs that uses single mode fiber optical cable and communications based on T-3. The base T-3 level of SONET is called Synchronous Transport Signal Level 1 (STS-1). STS-1 Can be incremented to higher levels that reflect multiples of T-3 SONET converts an electrical based STS-x signal to an optical based signal called an Optical Carrier (OC). STS-1 frames can be converted and sent at the same time in multiples, through a process that interleaves the frames with one another to achieve faster STS-x and OC-x speeds. Table 7.2 shows the STS-x to OC-x speeds that are possible with SONET Table 7.2 SONET STS-x and OC-x Transmission Rates STS Level Optical carrier Transmission rate T-3 multiple (OC) level STS-1 OC-1 51.84 Mbps 1 STS-3 OC-3 155.52 Mbps 3 STS-9 OC-9 466.56 Mbps 9 STS-12 OC-12 622.08

Mbps 12 STS-18 OC-18 933.12 Mbps 18 STS-24 OC-24 1.244 Gbps 24 STS-36 OC-36 1.866 Gbps 36 STS-48 OC-48 2.488 Gbps 48.

ISDN

The integrated Services Digital Network (ISDN) is less of a network and more of a set of standards than the name implies. The ISDN standards were developed by the ITU-T as a vision for the direction that the world‟s public telecommunications system should take. They believed that ISDN would eventually replace leased and switched circuits as we knew them. ISDN is a WAN technology for delivering voice, data, and video services over telephone lines. ISDN uses digital technology to achieve faster and more reliable communications than are possible through none ISDN POTS (Plain Old Telephone Service) lines. As ISDN line is physically a POTS or T-1 (twisted pair or fiber-optics) line; but with ISDN equipment at Telco and customer premises.

The benefits of ISDN are as follows:

It provides efficient multiplexed access to the public network.

It has the capabilities to support integrated voice and data.

It has a robust signaling channel, which is important for network management.

It provides an open system that is internationally defined.

Wireless

In wireless technologies, the carrier is a signal radiated from an antenna or dish. The amount of radiated power and the gain are governed by the communications laws and codes of individual countries. The specific frequencies authorized for wireless communications are also governed by national and international communications agreements and treaties. Wireless networking is one of the hottest topics in communications. Users want the convenience of not being tethered to a telephone jack or other communication port, especially if they are using a laptop computer.

Network managers like the flexibility that wireless technology gives them. For example, when offices are moved or rearranged, it is not necessary to rewire the office and pull new cables to the new office locations. However, security is a significant concern with wireless communication because it is accomplished using radio transmissions that are susceptible to being intercepted. However, security problems are being solved and wireless usage is growing by leaps and bounds.

WAN TRANSMISSION EQUIPMENT

- ✓ WAN transmission equipment is designed to work over POTS and leased telephone lines such as T-carrier or ISDN lines. It may have an analog component, as is true for modems, or it may be completely digital, as for ISDN communications. Most WAN transmission equipment either converts a signal for long-digital communications or creates multiple channels within a single communications medium for higher bandwidth.
- ✓ Common examples of basic WAN transmission equipment are:
- ✓ Multiplexers
- ✓ Channel banks
- ✓ PBXs, PABXs and PAXs
- ✓ Modems
- ✓ Access servers
- ✓ Routers

Multiplexers are network devices that can receive multiple inputs and transmit them to a shared network medium X.25, ISDN and frame relay use multiplexers for packet-switched communications. The multiplexer is connected to a single cable medium, which is divided into channels or virtual circuits. The multiplexers store the received packets until it can open the intended channel. The multiplexer simply switches from channel to channel. Each packet is stored until the multiplexer opens it channels for transmission. Channel banks are devices that convert multiple incoming

voice signals into a single line, and multiplexer-converted, multiple data signals into one line for transmission. The need for voice, data, and video communications has led to rapid developments in telecommunications channel banks, so that they now combine the capacity of voice communications with the functionality of a multiplexer for handling voice, data and video signals. Thus, a channel bank is a large scale multiplexer that aggregates telecommunications channels in a centralized location. Some organizations set up their own telephone service called Private Branch Exchanges (PBXs). PBXs were private, manually operated switchboards that required an operator to make connections inside the organizations. Innovations have resulted in the use of automated private telephone systems called Private Automatic Exchanges (PAXs) and Private Automatic Branch Exchanges (PABXs). PABX still includes the switchboard and manual capacity as well as automatic switching, whereas a PAX has no switchboard. The PAX or PABX may also carry voice, video, and data communications. Modems have long played a role in making WANs possible. The term modem is a shortened version of the full name, modulator/demodulator. A modem converts a computer‟s outgoing digital to an analog signal that can be transmitted over telephone line. It also converts the incoming analog signal to a digital signal that the computer can understand. An access server combines several types of WAN communications into one device. For example, one access server might combine transmission capabilities for modem, S.25,T-1, ISDN and frame relay. Some access servers are designed for small to mid-sized applications. Those servers have an Ethernet or token ring NIC to connect to the network. They also have a combination of synchronous and asynchronous communication ports for terminal modem, public telephone, and ISDN and S.25 connectivity. Smaller access servers typically have 8 or 16 asynchronous ports and one or two synchronous ports. Larger access servers are modular with slots (perhaps 10 to 20) for communication cards. Figure 7.3 illustrates access server. A remote router enables networks to be connected into WANs over long distances. Remote routers connect ATM,

ISDN, frame relay, high-speed serial, and X.25 networks. Like a local router, a remote router can support multiple protocols, enabling communication with many kinds of distant network. Also like a local router, remote routers are modular, so that different kinds of interferences can be installed in expansion slots; say, interface for ISDN and another one for frame relay.

WAN PROTOCOLS

WAN protocols have two important characteristics. One they are designed to be used on WAN media, such as fiber-optic or telephone cable. Two, they have the ability to encapsulate the commonly use LAN protocols so that the encapsulated data (payload data included) can be transported from one LAN to another over a WAN. Most WAN protocols are designed to transport at least TCP/IP. Others can host Net BEUI, IPX/SPX, and other protocols. There of the earliest WAN protocols are X.25, serial line Internet Protocol (SLIP) and Point-to-point Protocol (PPP). More recently, frame relay, ATM, SMDS and SONET have been implemented for WAN communications. **X.25**

The X.25 protocol, which is amongst the oldest WAN protocols, uses packet switching techniques, X.25 basically defines how data is sent from the data terminal equipment (DTE), such as computers to data circuit equipment (DCE), such as modem Figure 7.6 gives a conceptual overview of X.25 X.25 provides point-to-point connection-oriented communications, rather than point to multipoint connectionless communications, which are used by many other WAN protocols. Because it is connection-oriented, X.25 includes techniques to verify the continuity of the WAN connections, and to ensure that each packet reaches its intended destination. When it was introduced, the X.25 commercial carrier service was limited to a maximum transmission speed of 64 Kbps. The ITU-T updated X.25 standards in 1992 to include transmission speeds of up to 2.048 Mbps. Today, these services are more commonly used in Europe than in the United States, and some

European networks. Currently these service support speeds of up to only 9.6 Kbps X.25 is not a high-speed WAN protocol, but it does offer:

Global acceptance

Reliability

The ability to connect older LANs to WANs

The ability to connect older mainframes and minicomputers to WAN.

An X.25 network can transmit data packets using one of the three nodes: Switched Virtual Circuits (SVC), permanent Virtual Circuits (PVC) and Datagrams. A switched virtual circuit is a two-way channel established from node to node, through an x.25 switch. The circuit is a logical connection that is established only for the duration of the data transmission. Once the data transmission is completed, the channel can be made available to other nodes to other nodes. A permanent virtual circuit is a logical communications channel that remains connected at all times. The connection remains in place even when data transmission stops. Both switched and permanent virtual circuits are examples of packet switching. Datagram‟s are packaged data sent without-establishing a communications channel. They reach their destination using a form of message switching. The packets are addressed to a given destination and may arrive at different times depending on which path is selected. Datagrams are not used on international networks, but are included in the ITU-T specifications for the internet. The X.25 Internet Datagram encapsulated the IP layer within the X.25 packet, so that the X.25 device is not aware of the IP component. The IP network address is simply mapped to the X.25 destination address.

Serial Line Internet Protocol (SLIP)

Serial Line Internet Protocol was originally designed for UNIX environments for point-to-point communications between computers, servers, and hosts using TCP/IP. SLIP I used, for example, when user wants to communicate between a remote home computer and a UNIX computer

that is on a LAN at the office as shown in Figure 7.7 That user can employ a dial-up telephone line to connect the UNIX computer, and then transmit packets using TCP/IP within SLIP. SLIP merely acts as the host WAN protocol, corresponding the connection session over the telephone wire and modems. Once the protocol (with its data payload) reaches the destination, the SLIP header and trailer are removed, leaving TCP/IP. SLIP is an older remote communication protocol with more overhead than PPP. Compressed Serial Line Internet Protocol (CSLIP) is the newly developed extension of SLIP that compresses header information in each packet sent across a remote link. CSLIP reduces the overhead of a SLIP connection by decreasing the speed of communication. However, the header still must be decompressed at the receiving end. Both SLIP and CSLIP are limited in that they do not support network connection authentication. To prevent someone from intercepting a communication. They also do not support automatic setup of the network connection at multiple OSI layers at the same time for a faster connection. Another disadvantage is that SLIP and CSLIP are intended for asynchronous communications, for example a modem-to-modem connection. They do not support synchronous connections, like X.25. Many dial-up services do not support SLIP or CSLIP because these protocols do not provide authentication.

Point-to-Point Protocol (PPP)

Today, millions of Internet users need to connect their home computes to the computers of an Internet provider to access the Internet. There are also a lot of individuals who need to connect to a computer from home, but they do not want to go through the Internet. The majorities of these users have either a dialup or leased telephone line. The telephone line provides a physical link, but to control and manage the transfer of data, there is need for a point-to-point link control. Figure 7.8 shows the physical scheme for point-to-point connection. The first protocol devised for this purpose was Serial Line Internet Protocol (SLIP). However, SLIP has some deficiencies: it does not support protocols other than Internet Protocol (IP); it does not

allow the IP addresses to be assigned dynamically; and it does not support authentication of the user. The point-to-point protocol is a protocol designed to remedy these deficiencies. Table compares SLIP and PPP.

SLIP and PPP compared

Feature	SLIP	PPP
Network protocol support	TCP/IP	TCIP/IP/SPX and NETBEUI
Asynchronous communication support	Yes	Yes
Synchronous communication support	No	Yes
Simultaneous network configuration	No	Yes
Negotiation and automatic connection With multiple levels of the OSI model Between the communication nodes		
Support for connection authentication to Guard against eavesdroppers	No	Yes

Point-to-point Protocol users a stack of other protocols (Link Control Protocol, Authentication Protocols and Network Control Protocol) to establish the link, to authenticate the parties involved, and to carry the network layer data. PPP phase diagram is shown in Figure 7.9 and illustrated how home PC should to be connected to Internet Service Provider. When a PC is connecting to Internet Service Provider, the following steps are involved. Step 1: The PC calls a router via modem. Step 2: The PC and the router exchange Link Control Protocol (LCP) packets to Negotiate PPP parameters. Step 3: Check identities Step 4: Network Control Protocol (NCP) packets exchanged to configure the network layer, for example TCP/IT (requires IP address assignment) Step 5 : Data transport, for example, send/receive IP packets. Step 6: NCP used to turn down the network layer connection (free up IP address); LCP use to shut down data link connection. Step 7: Modem hands up. Link Control Protocol

(LCP) is responsible for establishing maintaining, configuring, and terminating links. It also provides negotiation mechanisms to set options between the two endpoints. Both endpoints of the link must reach an agreement about the options before the link can be established. Note that when PPP is carrying an LCP packet, it is either in the establishing state or in the terminating state. No user data is carried during these states. A particular strength of PPP is that it includes authentication protocols, which is a major issue when the computer connects to a remote network. Authentication plays a very important role in PPP because PPP is designed for use over dialup link where verification of user identity is necessary. Authentication means validating the identity of the user who needs to access a set of resources. PPP has created two protocols for authentication: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Password Authentication Protocol (PAP) is a simple authentication procedure with a two step process: ⎪ The user who wants to access a system sends authentication identification (usually the use name) and a password. ⎪ The system checks the validity of the identification and password and either accepts or denies connection. For those systems that require greater security, PAP is not enough. A third party With access to the link can easily pick up the password and access the system resources. Challenge Handshake Authentication Protocol (CHAP) is a three way handshaking authentication protocol that provides greater security than PAP. In this method the password is kept secret; it is never sent on-line.

The system sends to the user a challenge packet containing a challenge value, usually a few bytes.

The user applies a predefined function that takes the challenge value and the user‟s own password and creates a result. The user sends the result in the response packet to the system.

The system does the same. It applies the same function to the password of the user (known to the system) and the challenge value to create a result. If

the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied.

Challenge Handshake Authentication Protocol (CHAP) is more secure than Password Authentication Protocol (PAP), especially if the system continuously changes the challenge value. Even if the intruder learns the challenge value and the result, the password is still secret. PAP, which is used to verify the password entered to access a server over a WAN alone, can authenticate passwords, but it does not encrypt them. CHAP can be used in conjunction with PAP to encrypt passwords so that they will be difficult for a network intruder to intercept and decipher. After authentication has been completed, a network control protocol is use to configure each network layer protocol that is to operate over the link. PPP can subsequently transfer packets from these different network layer protocols (such as IP) over the same data link. PPP requires two parties to negotiate not only at the data link layer, but also at the network layer. Before user data can be send connection must be established at this level. The set of packets that establish and terminate a network layer connection for IP packets is called Inter network Protocol Control Protocol (IPCP). When a PC is connecting to an IP network, as in Figure 7.9, the NCP for IP negotiates a dynamically assigned IP address for the PC. In low speed lines it may also negotiate TCP and IP header compression schemes that reduce the number of bits that need to be transmitted. The PPP connection is now ready for data transfer.

Distance Vector Routing (DVR) Protocol

A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically.

Bellman Ford Basics – Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a chosen metric, are computed using information from the neighbors' distance vectors.

Information kept by DV router -

- Each router has an ID
- Associated with each link connected to a router,
- there is a link cost (static or dynamic).
- Intermediate hops

Distance Vector Table Initialization -

- Distance to itself = 0
- Distance to ALL other routers = infinity number.

Distance Vector Algorithm –

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
    - It receives a distance vector from a neighbor containing different information than before.
    - It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination

Dx(y) = Estimate of least cost from x to y

C(x,v) = Node x knows cost to each neighbor v

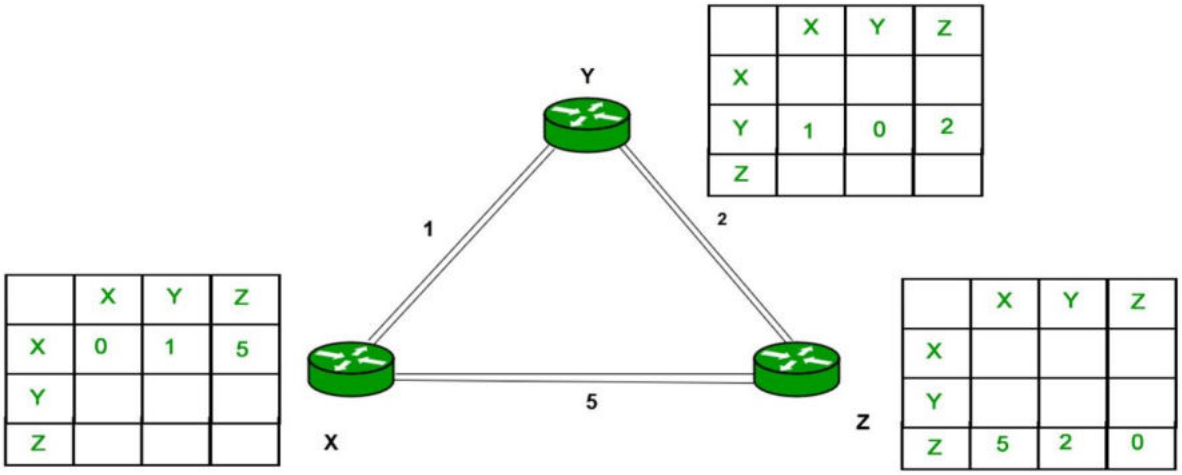
Dx = [Dx(y): y ∈ N] = Node x maintains distance vector

Node x also maintains its neighbors' distance vectors

– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N]

- Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈ N

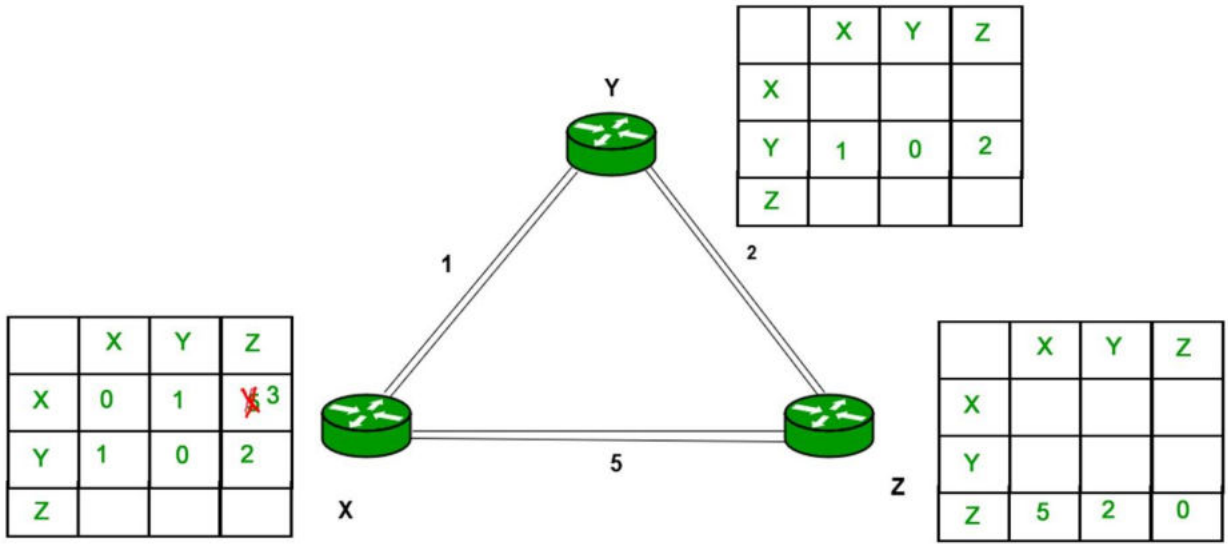
Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



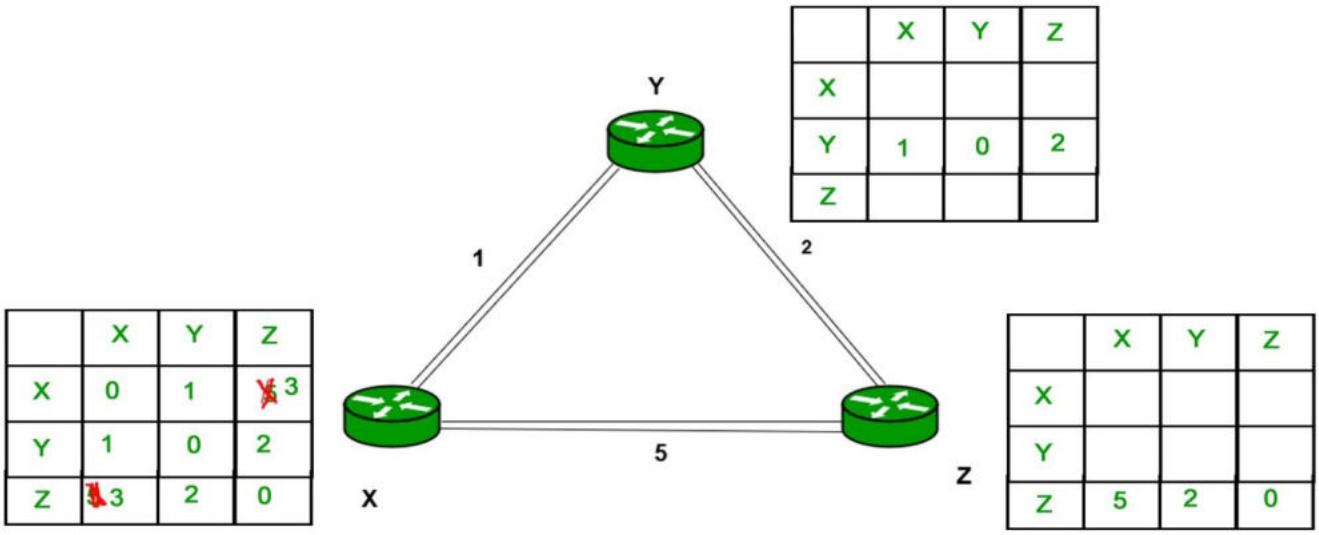
Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

$D_x(y) = \min \{ C(x,v) + D_v(y)\}$ for each node $y \in N$

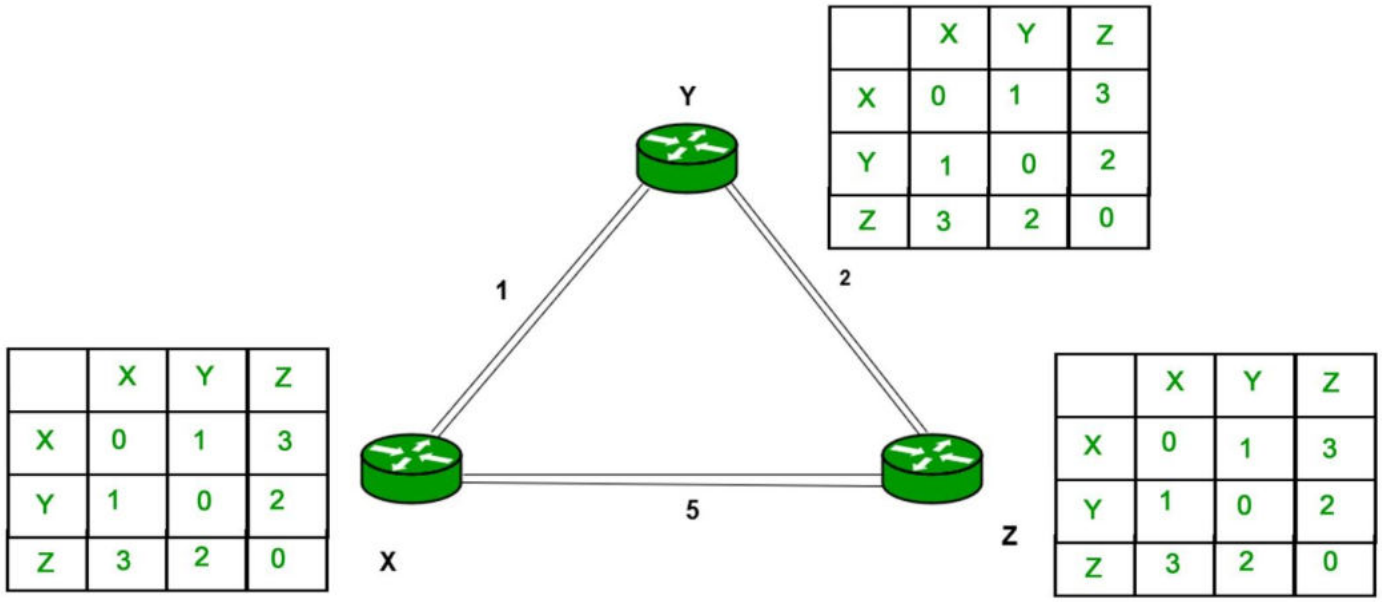
As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.



Similarly for Z also –



Finally the routing table for all –



Advantages of Distance Vector routing –

- It is simpler to configure and maintain than link state routing.

Disadvantages of Distance Vector routing –

It is slower to converge than link state.
It is at risk from the count-to-infinity problem.

It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

LINK STATE ALGORITHM

Link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.

Features of link state routing protocols –

- **Link state packet –** A small packet that contains routing information.
- **Link state database –** A collection information gathered from link state packet.
- **Shortest path first algorithm (Dijkstra algorithm) –** A calculation performed on the database results into shortest path
- **Routing table –** A list of known paths and interfaces.

Calculation of shortest path –
To find shortest path, each node need to run the famous **Dijkstra algorithm**. This famous algorithm uses the following steps:

- **Step-1:** The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database
- **Step-2:** Now the node selects one node, among all the nodes not in the tree like structure, which is nearest to the root, and adds this to the tree.The shape of the tree gets changed .
- **Step-3:** After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.
- **Step-4:** The node repeats the Step 2. and Step 3. until all the nodes are added in the tree

Link State protocols in comparison to Distance Vector protocols have:

1. It requires large amount of memory.
2. Shortest path computations require many CPU circles.
3. If network use the little bandwidth ; it quickly reacts to topology changes
4. All items in the database must be sent to neighbors to form link state packets.
5. All neighbors must be trusted in the topology.
6. Authentication mechanisms can be used to avoid undesired adjacency and problems.
7. No split horizon techniques are possible in the link state routing.

```
1  Dijkstra's Algorithm ( )
2  {
3      // Initialization
4      Tree = {root}                    // Tree is made only of the root
```

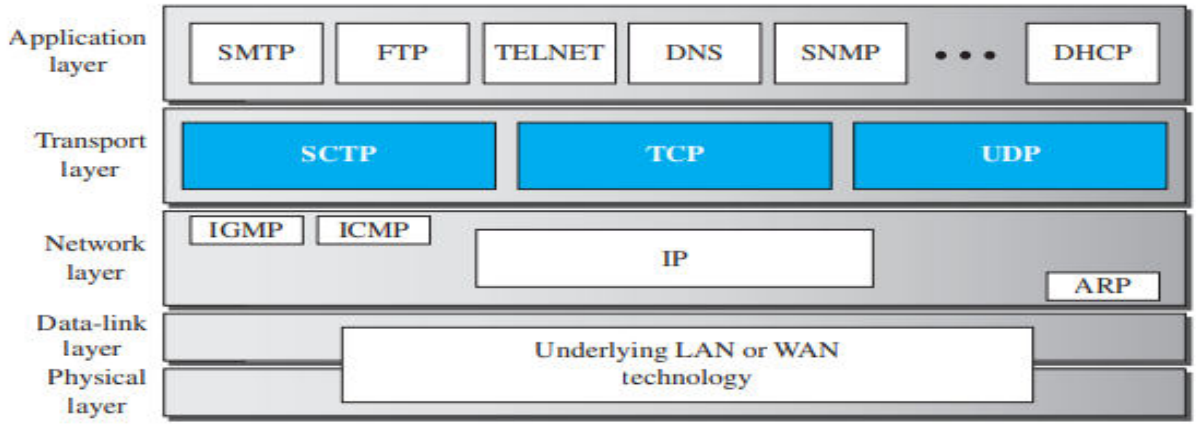

ble 20.2 *Dijkstra's Algorithm (continued)*

```
    for (y = 1 to N)                    // N is the number of nodes
    {
        if (y is the root)
            D[y] = 0                    // D[y] is shortest distance from root to node y
        else if (y is a neighbor)
            D[y] = c[root][y]           // c[x][y] is cost between nodes x and y in LSDB
        else
            D[y] = ∞
    }
    // Calculation
    repeat
    {
        find a node w, with D[w] minimum among all nodes not in the Tree
        Tree = Tree ∪ {w}               // Add w to tree
        // Update distances for all neighbors of w
        for (every node x, which is a neighbor of w and not in the Tree)
        {
            D[x] = min{D[x], (D[w] + c[w][x])}
        }
    } until (all nodes included in the Tree)
} // End of Dijkstra
```

TRANSPORT LAYER PROTOCOLS

INTRODUCTION

Figure 24.1 *Position of transport-layer protocols in the TCP/IP protocol suite*



Each protocol provides a different type of service.

UDP is an unreliable connectionless transport-layer protocol used for its simplicity and efficiency in applications where error control can be provided by the application-layer process.

TCP is a reliable connection-oriented protocol that can be used in any application where reliability is important. **SCTP** is a new transport-layer protocol that combines the features of UDP and TCP.

Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- 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.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- 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:

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

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
    - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
    - **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

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- 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.
- An ICMP protocol mainly uses two terms:

- **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
- **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.

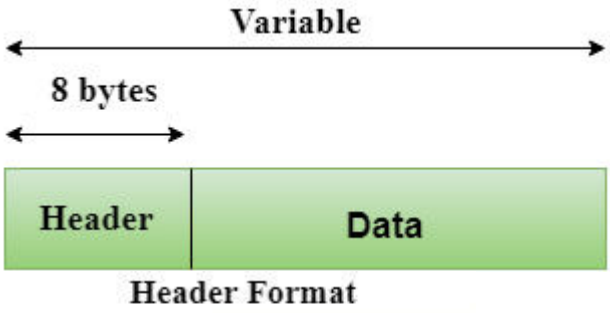
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination 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.



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.

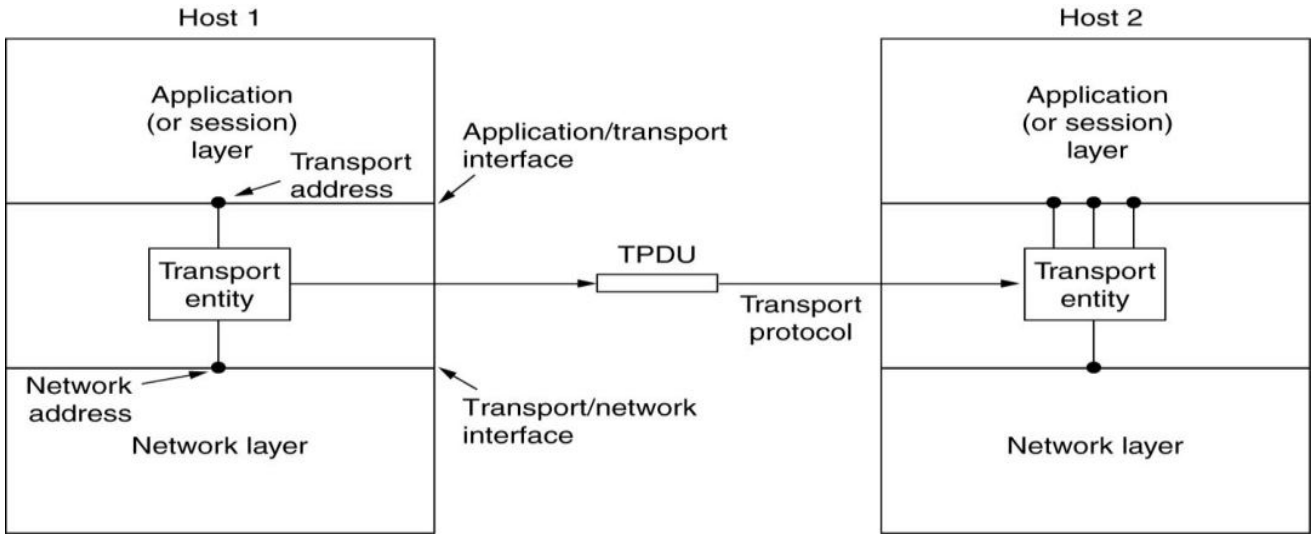
Following are the main protocols used in the application layer:

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

THE TRANSPORT SERVICE

SERVICES PROVIDED TO THE UPPER LAYER:

The goal of the transport layer is to provide efficient, reliable and cost effective service to its users. The hardware and/or software within the transport layer that does the work are called the transport entity. The transport entity can be located in the operating system. The logical relationship of the network, transport and application layers is shown in figure.



The transport layer is possible for the transport service to be more reliable than the network service. It is a key position for designing layers and the major boundary between the provider and user. The bottom four layers is known as transport service provider and upper layer as transport service user.

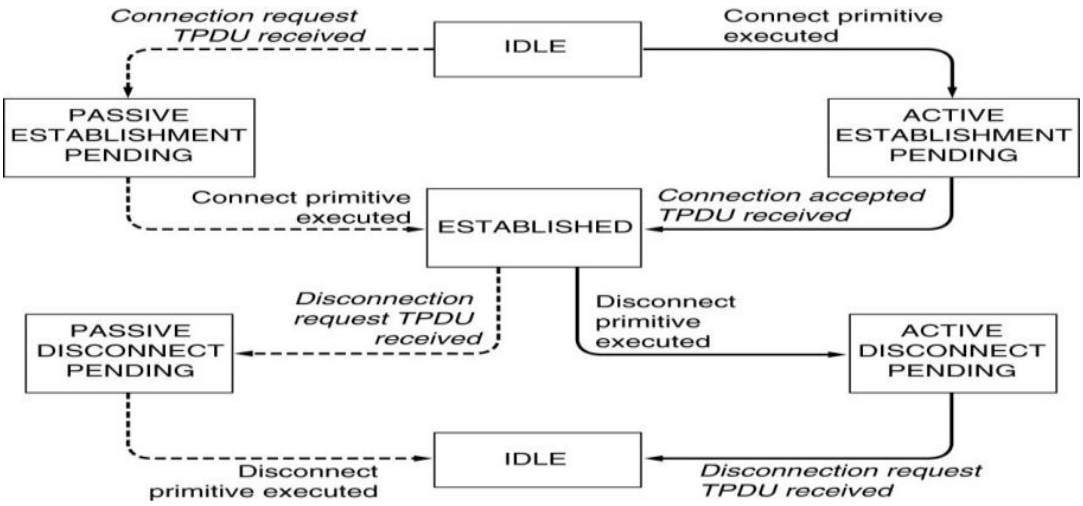
TRANSPORT SERVICE PRIMITIVES

The transport service is reliable and processes the error free bit stream in connection oriented service. In datagram service it provides unreliable service. Compare to the network service, transport service is convenient and easy to use.

PRIMITIVES ARE:

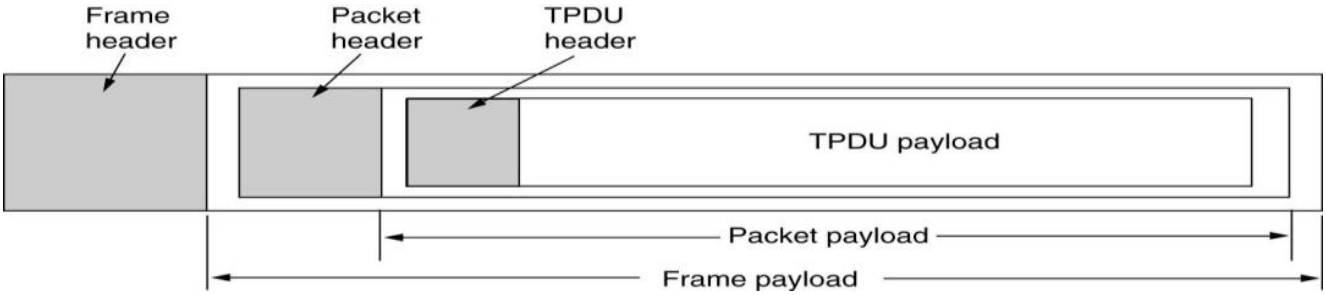
Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

A diagram for connection establishment and release for the primitives is shown below.



Transitions labeled in italics are caused by packet arrivals. The solid lines show the client's state sequence. The dashed lines show the server's state sequence.

The use of TPDU (Transport Protocol Data Unit) for messages sent from transport entity to transport entity. TPDU's are exchanged by the transport layer are contained in packets where exchanged by network layer. Packets are contained in frames exchanged by data link layer. When frame arrives the data link layer processes the frame header and passes the contents of the frame payload field up to the network entity. This entity processes the packet header and passes the contents of the payload to the transport entity. This is shown in figure.



BERKELEY SOCKETS

These primitives are widely used for internet programming. The socket primitives for TCP is shown in table.

Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

*The socket primitives create a new end point and allocate table space. The parameters specify the addressing format, types of service and the protocol.

*The bind primitive assign the network addresses.

*The listen call which allocates space to queue incoming calls from the several clients.

*The server executes the accept primitive to block waiting for an incoming connection. It returns a file descriptor for reading and writing.

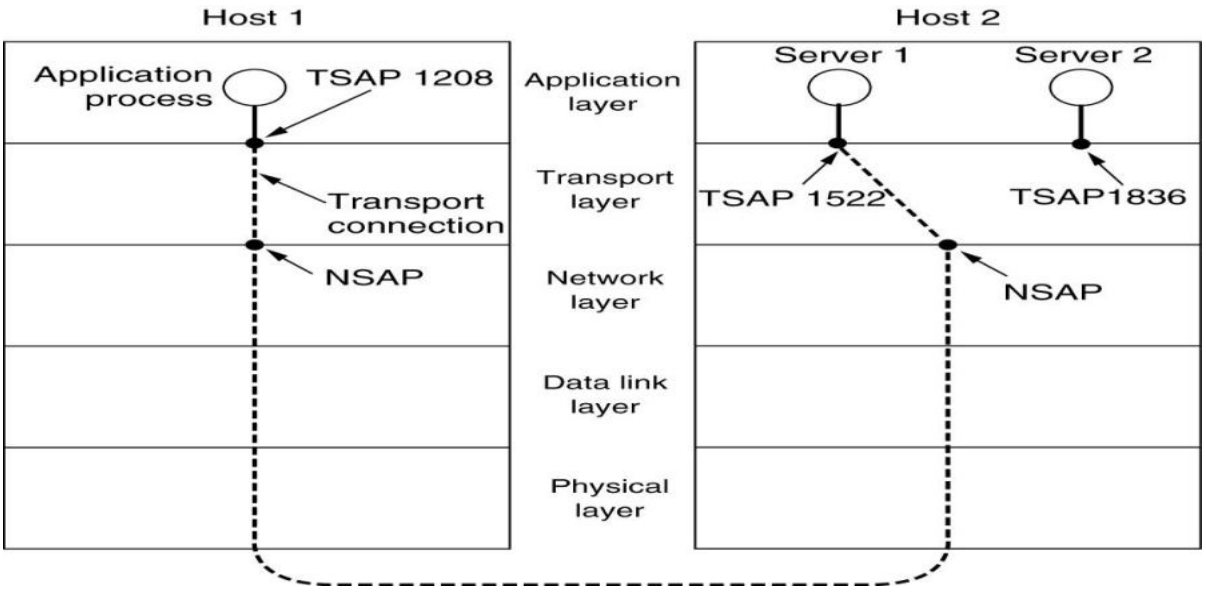
*The connect primitive blocks the caller and starts the connection.

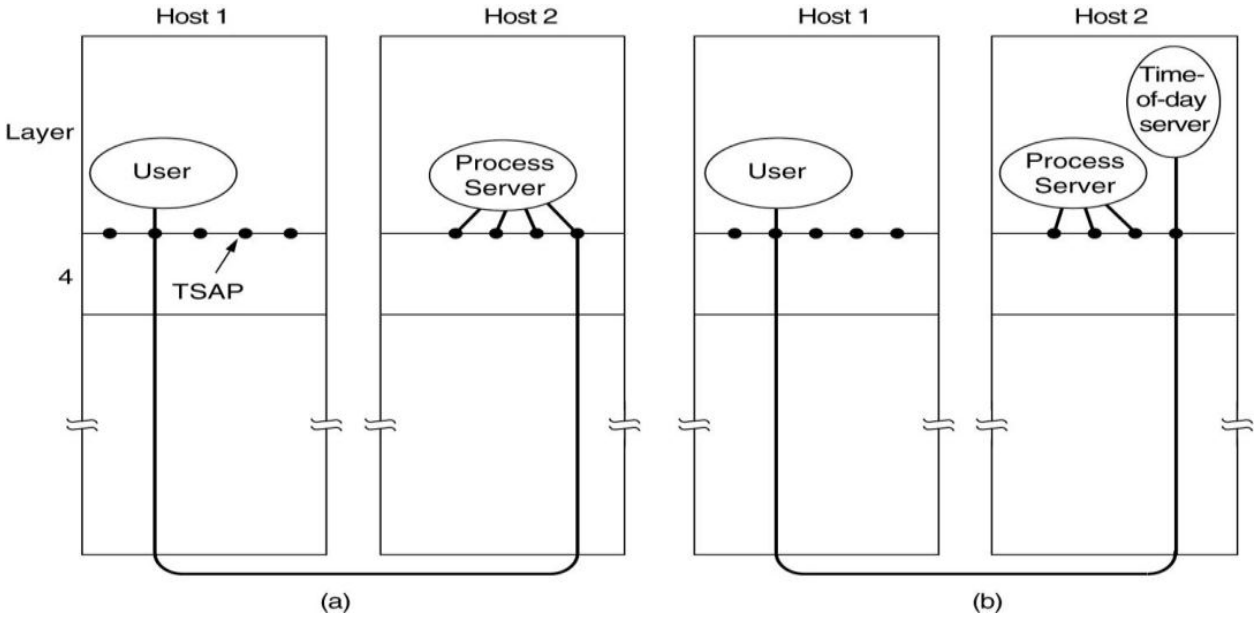
*Both sides can now use send and receive primitive to transmit and receive data over the full-duplex connection. When both sides execute the close primitive the connection is released.

ELEMENTS OF TRANSPORT PROTOCOLS

ADDRESSING

The method used to define transport addresses to which processes can establish connection is TSAP (Transport service access point). The network layer addresses are called NSAP (Network service access point). Both client and server attach TSAP to establish connection. The connections are run through NSAP's on each host. TSAP is needed to distinguish multiple transport end points that share that NSAP. The relationship between NSAP, TSAP and transport connections is shown below. The host2 attaches TSAP 1522 to wait for incoming call. On host 1 it issues the connect request specifying the TSAP 1208 as source and TSAP 1522 as destination. The transport connection being established between the application process on host1 and sever1 on host2. The application process then sends over a request for the time. The time server process responds with the current time. The transport connection is then released. To solve the problem of stable TSAP address a simplified scheme is used.

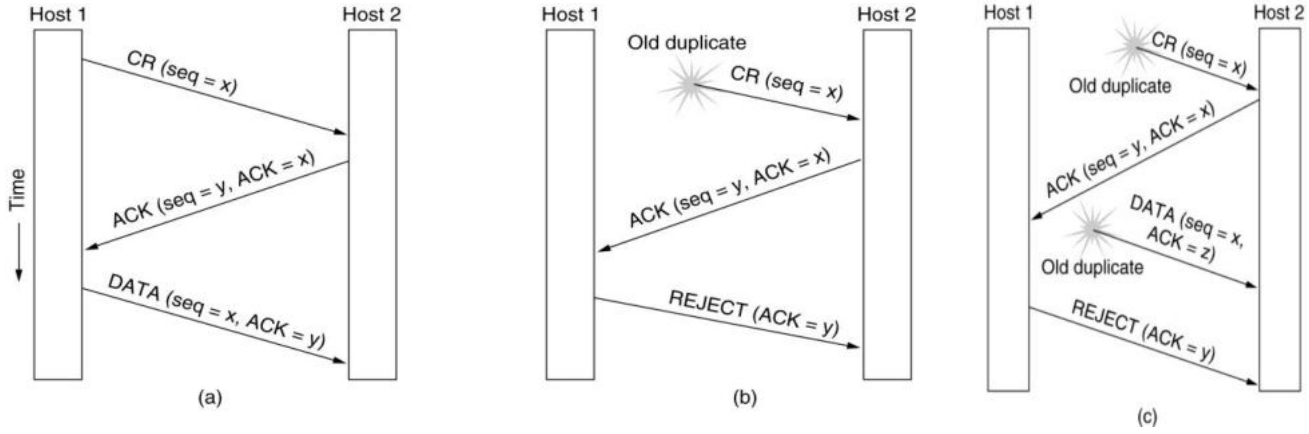




The scheme is known as initial connection protocol. The process server act as a proxy for less heavily used servers. It listens to a set of ports at the same time for a connection request. If no server is waiting for them, they get a connection to process server. The process server executes the requested server to inherit the connection with the user. The new server does the requested work; the process server goes back to listening for new requests.

CONNECTION ESTABLISHMENT

THREE WAY HANDSHAKE PROBLEM



Three protocol scenarios for establishing a connection using a three-way handshake. CR denotes CONNECTION REQUEST.
(a) Normal operation.
(b) Old CONNECTION REQUEST appearing out of nowhere.
(c) Duplicate CONNECTION REQUEST and duplicate ACK.

(a) Normal operation.

Host 1 chooses a sequence number x sends a connection request TPDU to Host 2. Host 2 replies with an ack TPDU and choose a sequence number y. Host 1 acknowledges and sends first data TPDU.

(b) Old CONNECTION REQUEST appearing out of nowhere.

The first TPDU is delayed duplicate from an old connection. This TPDU arrives at host 2 without host 1's knowledge. Host 2 send an ack TPDU asking for verification, when host 1 rejects the connection, host 2 realizes that it was tricked by delayed duplicate.

(c) Duplicate CONNECTION REQUEST and duplicate ACK.

If the connection and an ack are duplicate tells that this is an old duplicate and cause the protocol to fail which does not establish a connection.

CONNECTION RELEASE

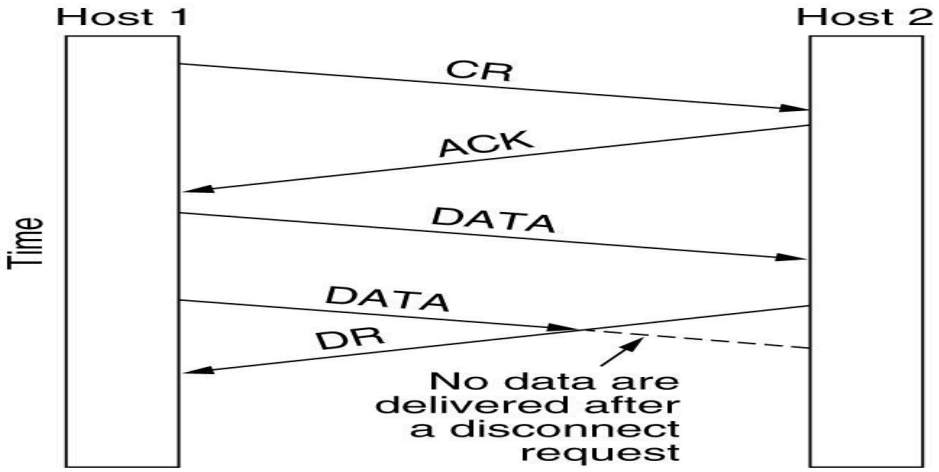
Releasing a connection is easier than establishing. Two way of terminating connection.

Asymmetric release and symmetric release.

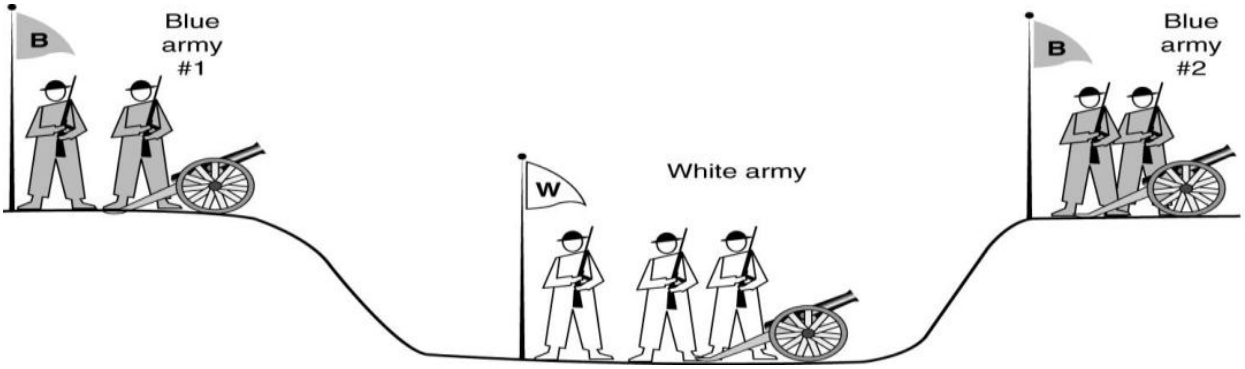
Asymmetric release means when one end is terminated the connection is broken (ex. Telephone system).

Symmetric release treats the connection as two separate unidirectional connections and requires each one to be released.

Asymmetric release causes sudden changes and may result in loss of data. For example, after the connection is established host 1 sends a TPDU that arrives properly to host 2, then host 1 sends another TPDU, unfortunately host 2 issues a DISCONNECT before the second TPDU arrives. So that the connection is released and data is lost. The below diagram shows the sudden disconnection with loss of data.

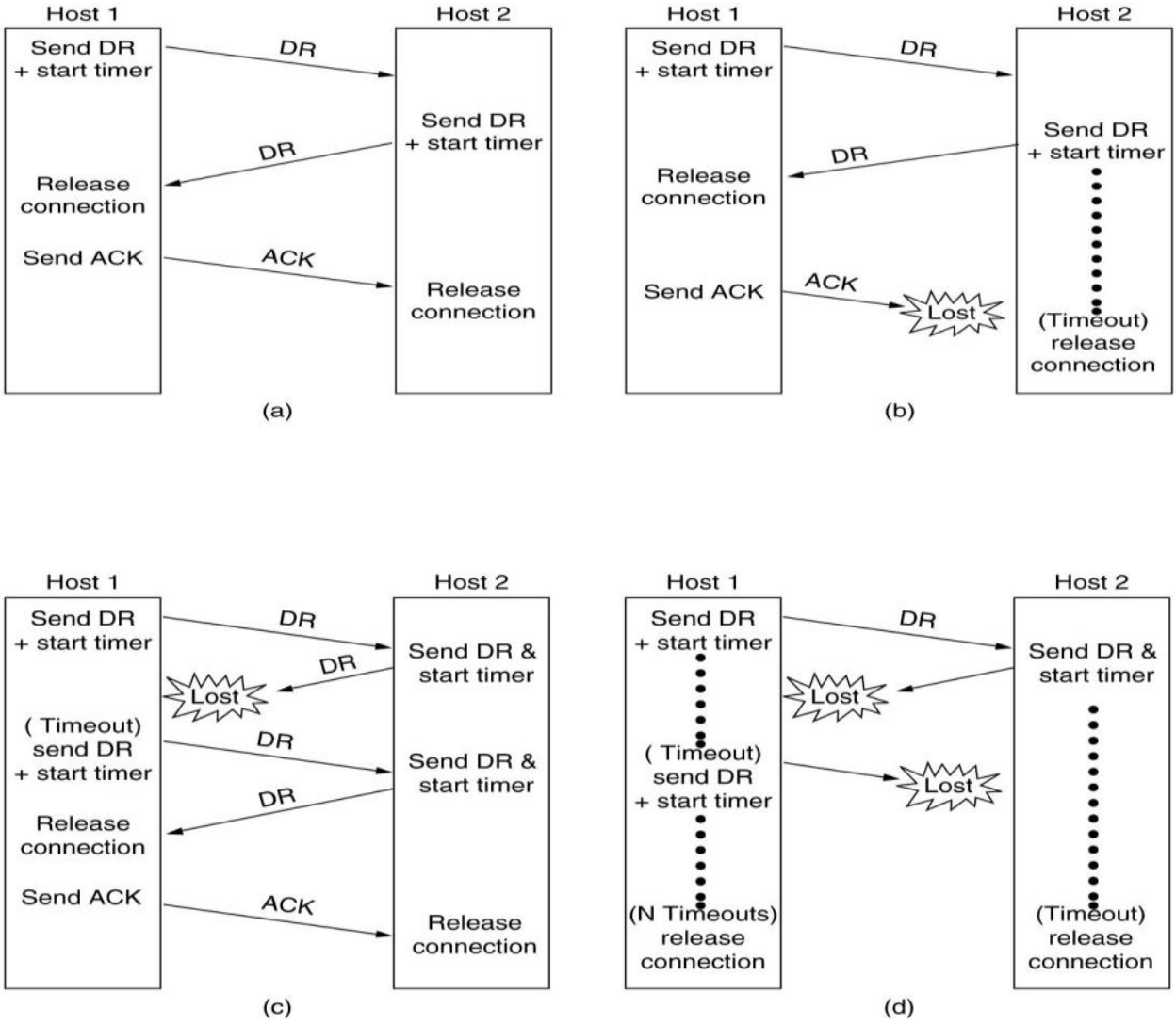


This problem can be solved by symmetric release. A host can continue to receive data even after it has sent a DISCONNECT TPDU. This problem can be solved by an issue called the two-army problem.



In this problem both of the surrounding hillsides are blue armies. The white army is larger enough than either of the blue armies alone, but together blue armies are larger than the white army. If the blue armies attack simultaneously they will be victorious.

The blue armies can send message only through the valley, but they may be captured and message will be lost. The blue army #1 send attack message to blue army #2. After receiving message the acknowledgement should send from blue army#2 and release the connection. If the connection does not take in correct time, the attack does not take place. To solve this in three way hand shake protocol four scenarios can be used.This is shown in below figure.



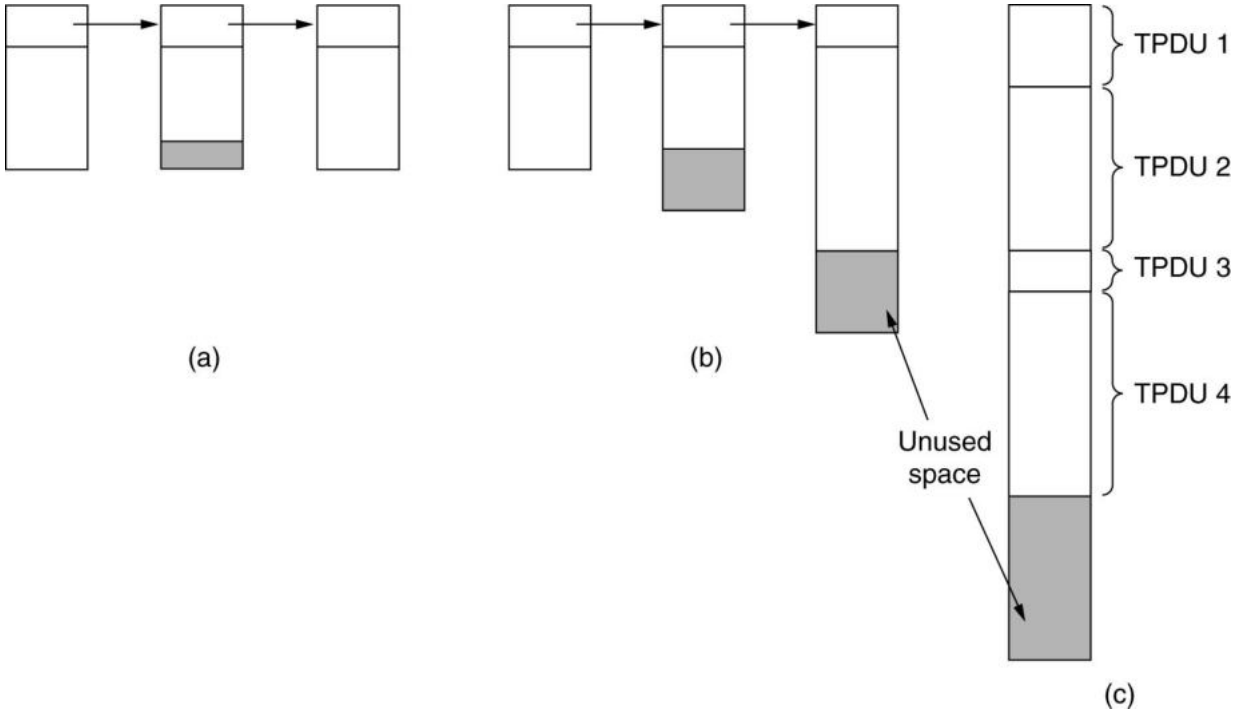
The user sends the DR (DISCONNECT REQUEST) TPDU to initiate the connection release. When it arrives the recipient send back a DR TPDU too. When this DR arrives the sender sends back an ACK TPDU and releases

the connection. If the final ACK TPDU is lost, the situation is saved by the timer. When the timer expires the connection is released anyway. If second DR being lost, the receiver will not receive the response.

Assume that the second time no TPDUs are lost and all TPDUs are delivered correctly on time. If all attempts to retransmit are failing, after N entries the sender releases the connection. Releasing the connection without data lost is not simple.

FLOW CONTROL AND BUFFERIING

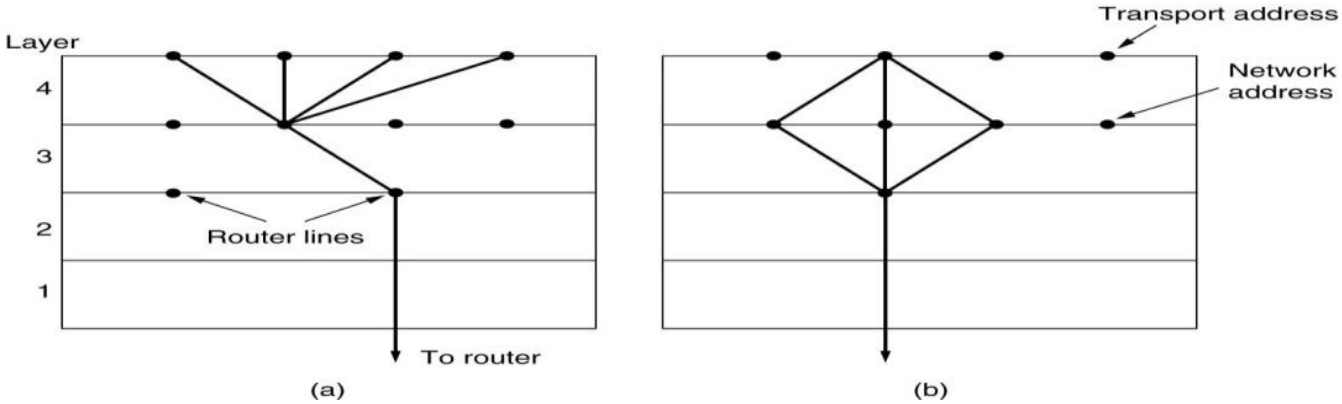
If the network service is unreliable the sender must buffer all TPDUs. The receiver also must agree to the buffering. The buffer size may be chained fixed size buffers, chained variable sized buffers and one large circular buffer per connection. The optimum trade-off between source buffering and destination buffering depends on the type of traffic carried by the connection. For low bandwidth bursty traffic the sender should buffer and for high bandwidth smooth traffic the receiver should buffer. In opened and closed connection the traffic pattern changes, the sender and receiver need to dynamically adjust buffer allocations. Dynamically management means a variable sized window. The sender requests a certain number of buffers, the receiver then grants the request.



The following shows the dynamic window management. The arrows show the direction of transmission. An ellipsis (…) indicates a lost TPDU.

	A	Message	B	Comments
1	→	< request 8 buffers>	→	A wants 8 buffers
2	←	<ack = 15, buf = 4>	←	B grants messages 0-3 only
3	→	<seq = 0, data = m0>	→	A has 3 buffers left now
4	→	<seq = 1, data = m1>	→	A has 2 buffers left now
5	→	<seq = 2, data = m2>	• • •	Message lost but A thinks it has 1 left
6	←	<ack = 1, buf = 3>	←	B acknowledges 0 and 1, permits 2-4
7	→	<seq = 3, data = m3>	→	A has 1 buffer left
8	→	<seq = 4, data = m4>	→	A has 0 buffers left, and must stop
9	→	<seq = 2, data = m2>	→	A times out and retransmits
10	←	<ack = 4, buf = 0>	←	Everything acknowledged, but A still blocked
11	←	<ack = 4, buf = 1>	←	A may now send 5
12	←	<ack = 4, buf = 2>	←	B found a new buffer somewhere
13	→	<seq = 5, data = m5>	→	A has 1 buffer left
14	→	<seq = 6, data = m6>	→	A is now blocked again
15	←	<ack = 6, buf = 0>	←	A is still blocked
16	• • •	<ack = 6, buf = 4>	←	Potential deadlock

MULTIPLEXING



(a) Upward multiplexing. (b) Downward multiplexing.Multiplexing means several conversations is made into one connections. If one network connection is available on host for all transport connections at that time if TPDU comes in it is needed to inform which process to give it. This situation is called upward multiplexing.

In figure (a) four distinct transport connections use the same network connection.

If user needs more bandwidth a virtual circuit is provided to open multiple network connections and distribute the traffic based on round robin technique. This situation is called downward multiplexing.

CRASH RECOVERY

TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet; it is bound to ACK that packet having the next sequence number expected (if it is not the last segment). When a TCP Server crashes mid-way communication and re-starts its process it sends TPDU broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards.

Each client can be in any one of state, TPDU outstanding S1 and no TPDU outstanding S0.

Three events are possible at server side, sending an acknowledgement (A), writing to the output process (W) and crashing (C). The three events can occur in six different orderings as shown below.

	Strategy used by receiving host					
	First ACK, then write			First write, then ACK		
Strategy used by sending host	AC(W)	AWC	C(AW)	C(WA)	W AC	WC(A)
Always retransmit	OK	DUP	OK	OK	DUP	DUP
Never retransmit	LOST	OK	LOST	LOST	OK	OK
Retransmit in S0	OK	DUP	LOST	LOST	DUP	OK
Retransmit in S1	LOST	OK	OK	OK	OK	DUP

OK = Protocol functions correctly
DUP = Protocol generates a duplicate message
LOST = Protocol loses a message

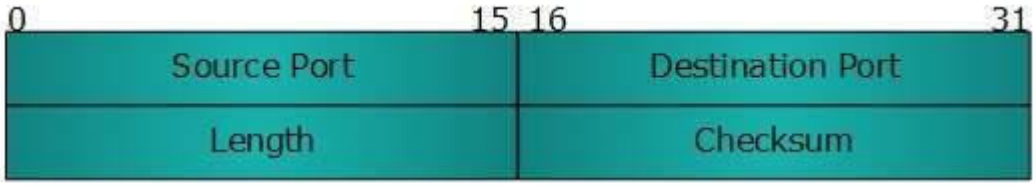
THE INTERNET TRANSPORT PROTOCOLS; UDP

INTRODUCTION TO UDP

FEATURES

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP HEADER - UDP header is as simple as its function.



UDP header contains four main parameters:

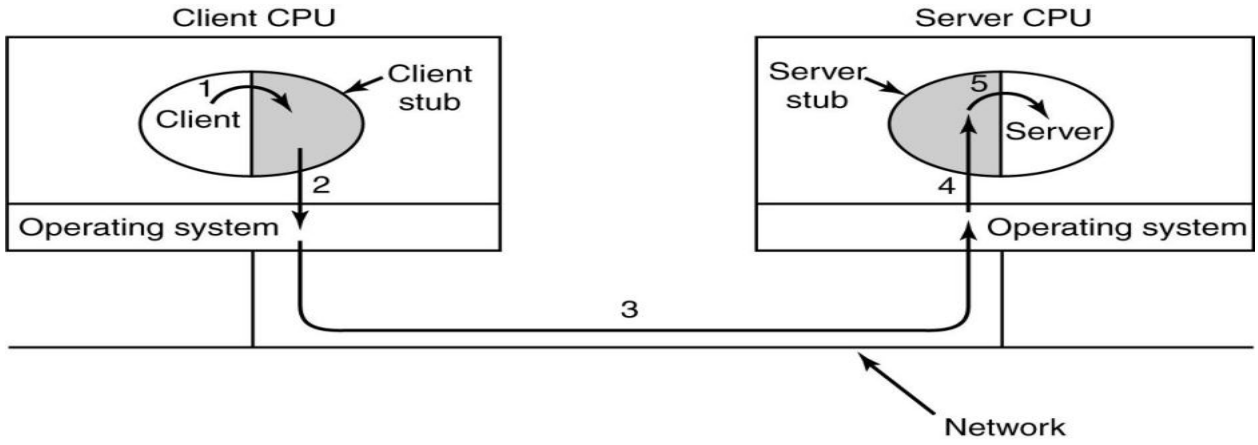
- **Source Port** - This 16 bits information is used to identify the source port of the packet.
- **Destination Port** - This 16 bits information, is used identify application level service on destination machine.
- **Length** - Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.
- **Checksum** - This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero.

UDP APPLICATION

- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

REMOTE PROCEDURE CALL

RPC comes under the Application-Oriented Design, where the client-server communication is in the form of Procedure Calls. The machine making the procedure call is known as *client* and the machine executing the called procedure as *server*. For every procedure being called there must exist a piece of code which knows which machine to contact for that procedure. Such a piece of code is called a *Stub*. On the client side, for every procedure being called we need a unique stub. However, the stub on the server side can be more general; only one stub can be used to handle more than one procedures.



The following are the steps involve in making an RPC procedure.

First the client calling the client stub is a local procedure. In second step the client stub packing the parameter into a message and making a call to send the message. Packing the parameters is called marshalling. In third step the kernel sends the message from the client machine to the server machine. Next step (4) the kernel passing the incoming packet to the server stub. Finally (5) the server stub calling the server procedure with the unmarshaled parameters. The reply traces the same path in the other direction.

THE INTERNET TRANSPORT PROTOCOLS; TCP

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

TCP PROTOCOL

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.

- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

TCP SERVICE MODEL

The TCP Service Model

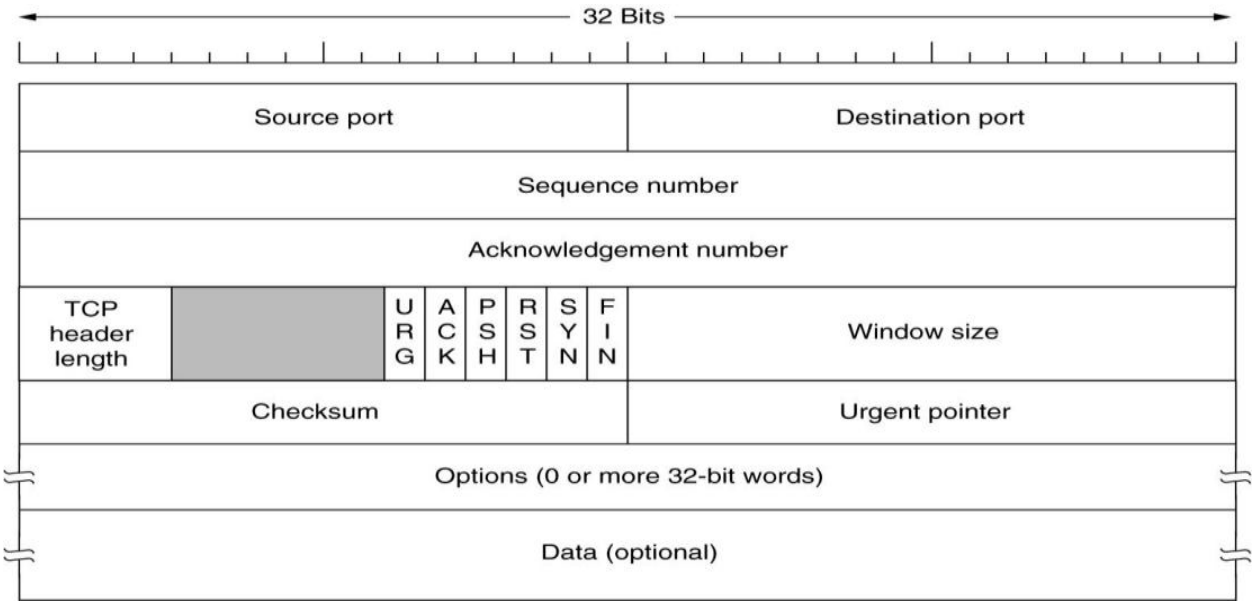
Port	Protocol	Use
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial File Transfer Protocol
79	Finger	Lookup info about a user
80	HTTP	World Wide Web
110	POP-3	Remote e-mail access
119	NNTP	USENET news

Some assigned ports.

- The service is obtained by sender and receiver creating end points called sockets. Socket as a socket number consisting of IP address of host and a 16-bit number local to that host called port. Port numbers below 1024 are called well known ports and are reserved for standard services. FTP can connect to the destination host port 21 to contact its FTP daemon; the telnet daemon is attached to port 23 at boot time and so on. Generally a single daemon called inetd (Internet daemon).

HEADER

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
    - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
    - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
    - **ECE** -It has two meanings:
        - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
        - If SYN bit is set to 1, ECE means that the device is ECT capable.
    - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
    - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
    - **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
    - **RST** - Reset flag has the following features:
        - It is used to refuse an incoming connection.
        - It is used to reject a segment.
        - It is used to restart a connection.
    - **SYN** - This flag is used to set up a connection between hosts.
    - **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.

- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

UNIT V

ATM (Asynchronous Transfer Mode)

DESIGSN GOALS

1. Use of high data rate transmission and noise degradation.

2. Mapping the packets and frames of other systems onto cells.

3. Low cost for implementation.

4. New system must be able to work with and support the existing one(local loops, local providers, long-distance carriers).

5. New system must be connection-oriented to ensure accurate and predicable delivery.

6. Move many of the software functions to hardware as possible.

PACKET NETWORKS

Different protocols use packets of varying size. As network become more complex, the information that must be carried in header becomes more expensive. To improve utilization, some protocols provide variable packet size to users.

MIXED NETWORK TRAFFIC

To get the most out of broadband technology, traffic must be time-division multiplexed onto shared paths. Imagine the results of multiplexing frames from two networks with different requirements (and frame designs) onto one link. What happens when line 1 uses large frames (usually data frames) while line 2 uses very small frames (the norm for audio and video information)

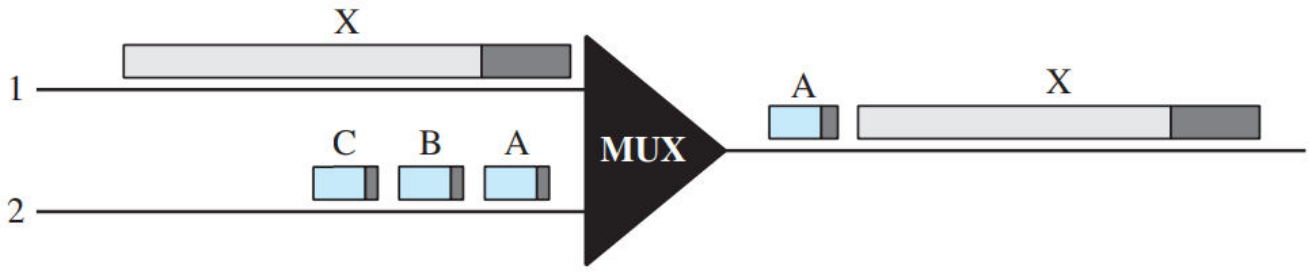


Fig: Multiplexing using different frame sizes

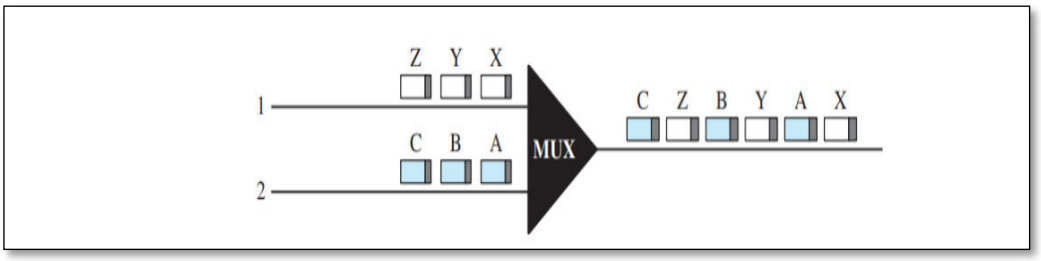
CELL NETWORKS

A cell is a small data unit of fixed size. In a cell network, which uses the cell as the basic unit of data exchange, all data are loaded into identical cells that can be transmitted with complete predictability and uniformity.

The cells are then multiplexed with other cells and routed through the cell network. Because each cell is the same size and all are small, the problems associated with multiplexing different-sized frames are avoided.

Figure shows the multiplexer with the two lines sending cells instead of frames. Frame X has been segmented into three cells: X, Y, and Z. Only the first cell from line 1 gets put on the link before the first cell from line 2. The cells from the two lines are interleaved so that none suffers a long delay.

Fig: Multiplexing using cells.

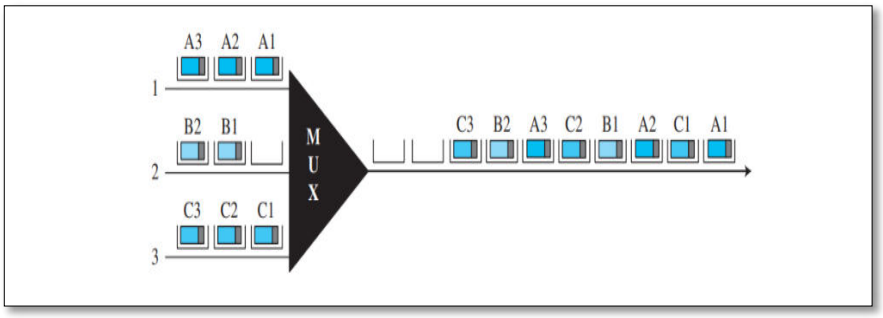


Asynchronous TDM

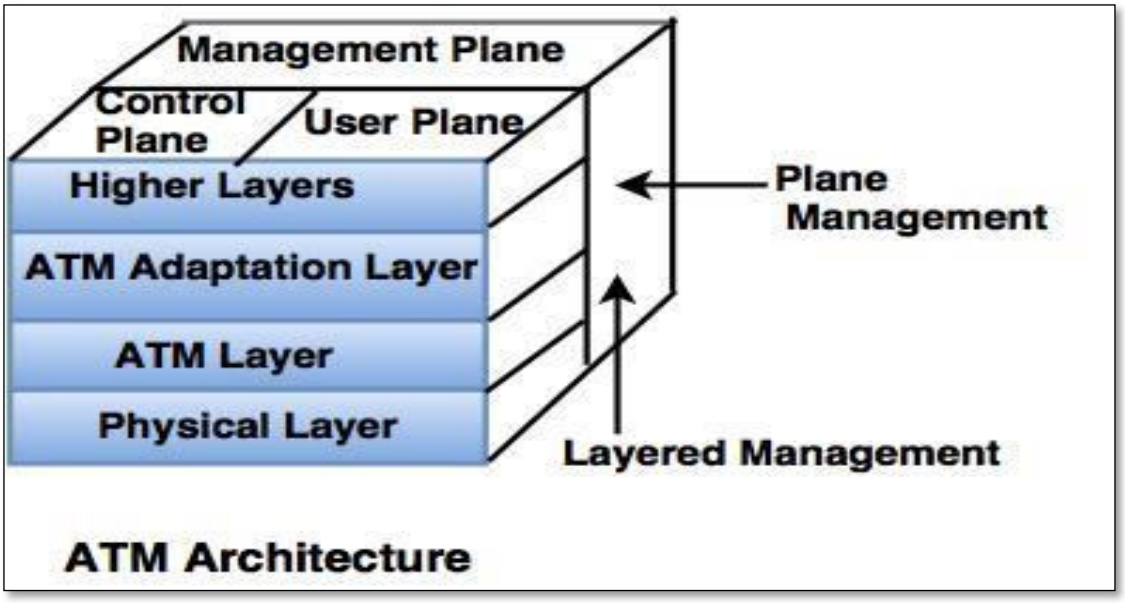
ATM uses statistical (asynchronous) time-division multiplexing—that is why it is called Asynchronous Transfer Mode—to multiplex cells coming from different channels. It uses fixed-size slots (size of a cell). ATM multiplexers fill a slot with a cell from any input channel that has a cell; the slot is empty if none of the channels has a cell to send.

Figure shows how cells from three inputs are multiplexed. At the first tick of the clock, channel 2 has no cell (empty input slot), so the multiplexer fills the slot with a cell from the third channel. When all the cells from all the channels are multiplexed, the output slots are empty.

Fig: ATM multiplexing.



ATM ARCHITECTURE-ATM LAYERS



The ATM standard defines three layers.

- the application adaptation layer
- the ATM layer
- the physical layer

1. Physical layer

- Physical layer is a point-to-point transfer mechanism at the top of hardware (it may be wire also).
- Physical layer adds its own information to each cell which is transmitted for link management.

Physical layer performs four functions:

i) Physical layer converts bits into cells.
ii) It transmits and receives the bits on physical medium.
iii) Tracks the cell boundaries.
iv) Packaging of cell into frames.

ATM layer is common to all services which can have the packet transfer capabilities.

2. ATM layer

- ATM layer provides the routing information to the data cells.
- ATM interfaces with the AAL and the Physical layer.
- Functions of ATM layer are under the network management, signaling and OAM protocol.

3. ATM Adaptation Layer

- AAL provides the flexibility of a single communication process to carry the multiple types of traffic such as data, voice, video and multimedia.
- **AAL** is divided into two major parts.
- Upper part of the AAL is called as the **convergence sublayer.** Its task is to provide the interface to the application. The lower part of the AAL is called as the **segmentation and reassembly (SAR) sublayer.** It can add headers and trailers to the data units given to it by the convergence sublayer to form cell payloads.

  ATM defines four versions of the AAL: AAL1, AAL2, AAL3/4, and AAL5.

AAL5 is used on the Internet today. For Internet applications, the AAL5 sublayer was designed. It is also called the simple and efficient adaptation layer (SEAL). AAL5 assumes that all cells belonging to a single message travel sequentially and that control functions are included in the upper layers of the sending application. Figure shows the AAL5 sublayer.

The packet at the CS uses a trailer with four fields. The UU is the user-to-user identifier. The CPI is the common part identifier. The L field defines the length of the original data. The CRC field is a two-byte error-checking field for the entire data.

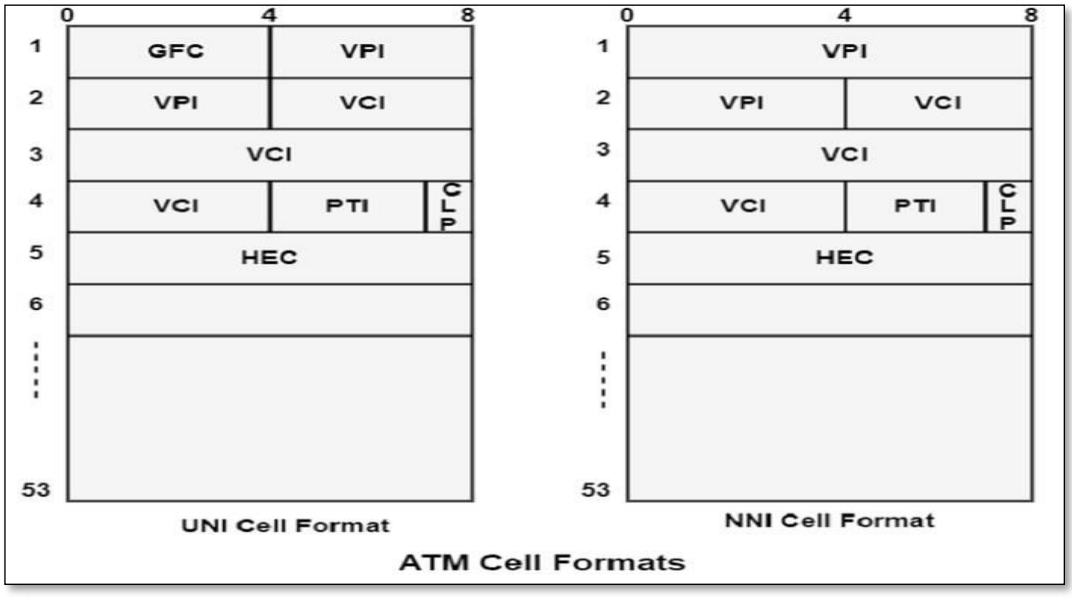
ATM services generally have four different bit rate choices:

- **Available Bit Rate:** Provides a guaranteed minimum capacity but data can be bursted to higher capacities when network traffic is minimal.
- **Constant Bit Rate:** Specifies a fixed bit rate so that data is sent in a steady stream. This is analogous to a leased line.
- **Unspecified Bit Rate:** Doesn't guarantee any throughput level and is used for applications such as file transfers that can tolerate delays.
- **Variable Bit Rate (VBR):** Provides a specified throughput, but data is not sent evenly. This makes it a popular choice for voice and videoconferencing.

ATM Cell Format

An ATM cell header can be two formats, such as User Network Interface (UNI) or Network to Network Interface (NNI). The UNI header can be used for communication between ATM endpoints and ATM switches in private ATM networks. The NNI header can be used for communication between ATM switches.

The figure shows the ATM UNI cell header format and the ATM NNI cell header format. Unlike the UNI, the NNI header does not contain the Generic Flow Control (GFC) field. The NNI header has a Virtual Path Identifier (VPI) field that appears in the first 12 bits. It is allowing for high trunks between public ATM switches.



ATM Cell Header Fields

The following definitions summarise the ATM cell header fields as shown in the figure above −

- **Generic Flow Control (GFC)** − It supports local functions, such as recognizing multiple stations that send a single ATM interface. This field is generally not used and is set to its default value of 0 (binary 0000).
- **Virtual Path Identifier (VPI)** − In conjunction with the Virtual Channel Identifier (VCI), it recognises the next destination of a cell as it transfers through a series of ATM switches on the way to its destination.
- **Virtual Channel Identifier (VCI)** − In conjunction with the VPI, it recognizes the next destination of a cell as it transfers through a series of ATM switches on the way to its destination.
- **Payload Type (PT)** − It denotes in the first bit whether the cell includes user data or control data. If the cell includes user data, the bit is set to 0. If it includes control data, it is set to 1. The second bit denotes congestion (0 = no congestion, 1 = congestion), and the third bit denotes whether the cell is the last in a sequence of cells that define a single AAL5 frame (1 = last cell for the frame).
- **Cell Loss Priority (CLP)** − It denotes whether the cell should be removed if it encounters extreme congestion as it transfers through the network. Suppose the CLP bit similar is to 1, and the cell should be discarded in preference to cells with the CLP bit equal to 0.
- **Header Error Control (HEC)** − It evaluates checksum only on the first 4 bytes of the header. It can be valid a single bit error in these bytes, thereby preserving the cell instead of discarding it.

FUNDAMENTAL CONCEPTS

Objectives, assets, threats, vulnerability, safeguards, and potential attacks on information in network environment are the fundamental concepts of network security.

OBJECTIVES

Information security has four objectives as given below:

(1) Confidentiality: Ensuring that information is not disclosed or revealed to unauthorized persons.

(2) Integrity: Preventing unauthorized creation or modification of data maintaining consistency of data.

(3) Availability. Ensuring that authorized users are not denied access to information and resources.

(4) Legitimate use: Ensuring that authorized persons do not use the information in an unauthorized way.

ASSETS

Assets are valuable resources of the organization that need to be protected. The loss of an asset means a significant loss to an organization. In some cases, a lost asset cannot be replaced, particularly in the case of goodwill, trust, or confidential research. Examples of asset categories are: users, application, services, servers, networks documentation, goodwill, reputations and manpower skills.

THREATS

A threat is an impending action by a person or event that poses some danger to an asset a loss of an asset is caused by the realization of the threat. A threat is realized via the medium of vulnerability. Threats come from organization environment and therefore cannot be totally controlled by the organization. The four major threats are as follows a threat to secrecy.

(1) Information leakage: Information is revealed to unauthorized users which is a threat to secrecy.

(2) Integrity violation: Destroying, altering or creating bogus data that results in inconsistency of data.

(3) Denial of service: Using legitimate access rights to disrupt traffic partially or completely.

(4) Illegitimate use: Exploitation of privileges by legitimate users.

The above threats can be realized in different ways us given below:

1) Authorization violation: A person authorized to use a resource uses it in an unauthorized manner.
2) By passing control: Exploiting system flaws or security weakness in order to acquire higher or unauthorized privileges.
3) Eavesdropping: Leakage of information by monitoring communication channels
4) Interception: Extracting information from radio frequency or electromagnetic equipment
5) Malicious programs: Programs that are specially written to damage other programs
6) Masquerade: A person or entity pretends to be different.
7) Traffic analysis: Leakage of information by analyzing traffic pattern.
8) Repudiation: A person participating in an exchange of information denies having participated.
9) Resource exhaustion: Using resources so as to make them unavailable for others. This results in denial of service.
10) Social engineering: Fooling a user to disclose his password. Leaning over someone's shoulder to observe the password and learning about a system by eavesdropping on conversation are also accomplished by social engineering.

VULNERABILITY

Vulnerability is weakness or absence of safeguards. Unlike threats, vulnerabilities usually exist within the organization. A possible categorization of vulnerability is security policy, procedures, administration, implementation, and apathy. Some examples of vulnerability are given in Table.

Examples of Vulnerability

Category	**Vulnerability**
1)Security policy	Granting higher rates to users than required Circumventing security procedures due to degradation in performance
2) Administration	Circumventing security procedures due to degradation in Performance.
3) Administration	Initializing insecure system.
4) Administration	Empty root/administrator passwords, particularly during installation.
5) Implementation	Failure of protection mechanism
6)Apathy	By passing or disabling security procedures for convenience.
7) Procedure	Duplication of confidential reports
8) Procedure	Unsafe handling of backups containing confidential reports.

SAFEGUARDS

Safeguards are physical controls, security policies, security mechanisms and procedures that protect assets from threats.

Physical controls

The common physical controls are.

1)Physical security

2)Personnel security

3)Administrative security

4)Emanations security

Security policy

The security policy is a set of rules established by the organization to apply to a security relevant activities. Several levels of security policies have been suggested such as management policy, operational policy and procedural policy.

Security services

The security mechanisms and procedures, which are main security safeguards, are known as security services. The security services are as follows:

- Identification and authentication service
- Access control service
- Confidentiality service
- Data integrity service non-repudiation service

ATTACK

An attack is the realization of threat. Broadly the attackers are hackers, spies, vandals and professional criminals.

Tool

The tools generally used by an attacker broadly fall into categories such as physical attack, information exchange, user commands, program and data up

Actions

Depending on the vulnerability, the attacker can perform different actions such a probe, scan, flood, bypass control spoof, steal and read/copy/modify

The Targets

The targets of attack are generally account, process, data, system components and

SECURING NETWORK USING FIREWALL

Firewalls prevent unauthorized access to networks through software or firmware. By utilizing a set of rules, the firewall examines and blocks incoming and outgoing traffic. firewalls are used to secure a computer network. Firewalls are network security systems that prevent unauthorized access to a network. It can be a hardware or software unit that filters the incoming and outgoing traffic within a private network, according to a set of rules to spot and prevent cyberattacks.

Working of Firewall

A firewall welcomes only that incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rules. These rules are based on several aspects indicated by the packet data, like their source, destination, content, and so on. They block traffic coming from suspicious sources to prevent cyberattacks.
For example, the image depicted below shows how a firewall allows good traffic to pass to the user's private network.

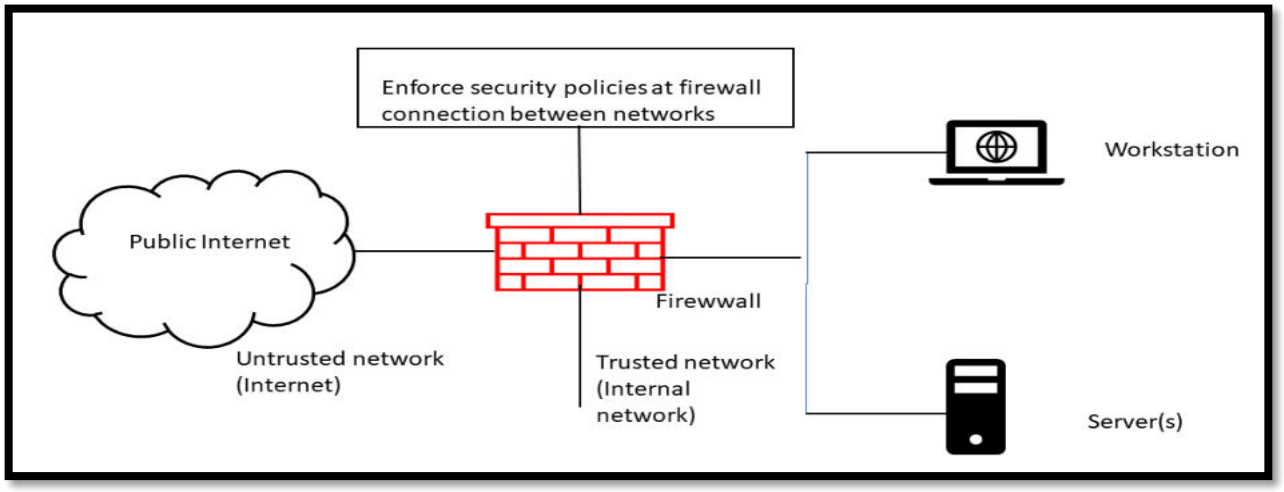


Fig: A firewall at the boundary of two networks

Advantages of Firewall:

- Firewalls play an important role in the companies for security management.
- It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.
- Firewalls provide faster response time and can handle more traffic loads.
- A firewall allows you to easily handle and update the security protocols from a single authorized device.
- It safeguards your network from phishing attacks.

Disadvantages:
Do not protect you against malicious insiders.
Do not protect you against connections that do not go through them.
Do not protect against completely new threats.
Do not protect against viruses.

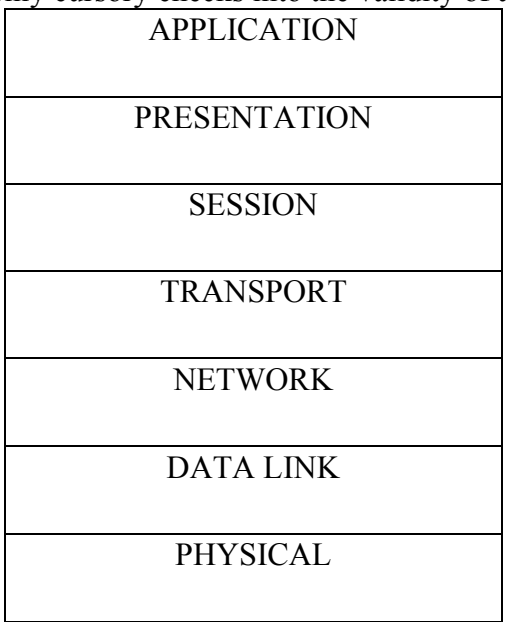
TYPES OF FIREWALLS

- Packet filtering firewall
- Application-level gateway

Packet filtering firewall

Packet filtering firewalls operate inline at junction points where devices such as routers and switches do their work. However, these firewalls don't route packets; rather they compare each packet received to a set of established criteria, such as the allowed IP addresses, packet type, port number and other aspects of the packet protocol headers. Packets that are flagged as troublesome are, generally speaking, unceremoniously dropped --

that is, they are not forwarded and, thus, cease to exist. Packet filtering firewalls are fast because they operate at the network layer and make only cursory checks into the validity of a given connection as shown in fig:



Packet filtering firewall advantages

- A single device can filter traffic for the entire network
- Extremely fast and efficient in scanning traffic
- Inexpensive
- Minimal effect on other resources, network performance and end-user experience

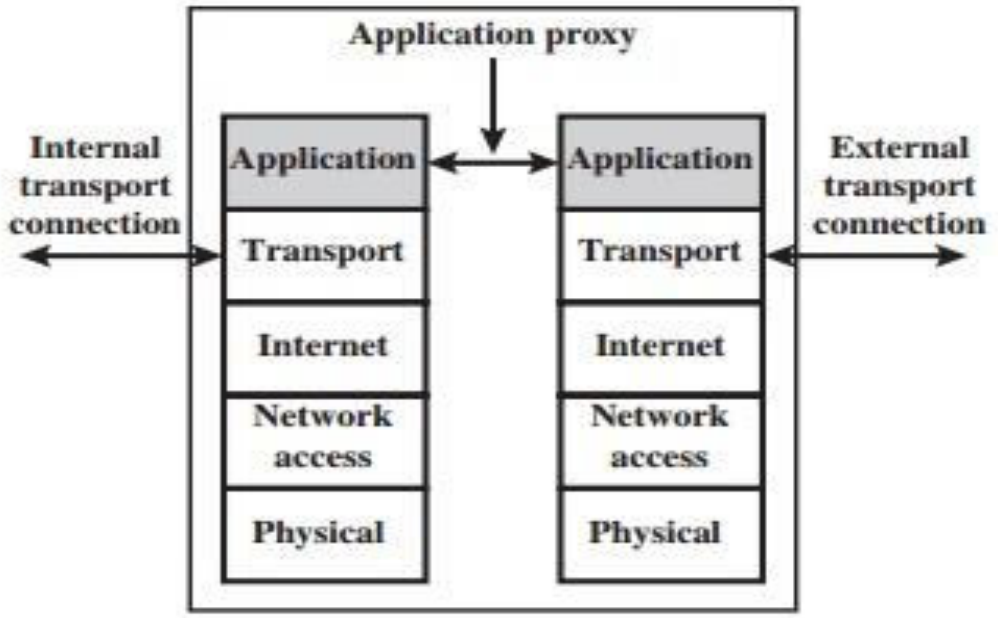
Packet filtering may not provide the level of security necessary for every use case, but there are situations in which this low-cost firewall is a solid option. For small or budget-constrained organizations, packet filtering provides a basic level of security that can provide protection against known threats. Larger enterprises can also use packet filtering as part of a layered defense to screen potentially harmful traffic between internal departments.

APPLICATION-LEVEL GATEWAY

Application-level gateways filter packets not only according to the service for which they are intended -- as specified by the destination port -- but also by other characteristics, such as the HTTP request string.

Application-level gateway advantages

- Examines all communications between outside sources and devices behind the firewall, checking not just address, port and TCP header information, but the content itself before it lets any traffic pass through the proxy.
- Provides fine-grained security controls that can, for example, allow access to a website but restrict which pages on that site the user can open.
- Protects user anonymity.



(d) Application proxy firewall

Limitations of firewalls

Firewall cannot protect against content related attacks.

It concentrates security in one spot. Thus a compromise of the firewall could be disastrous.

A firewall provides no protection within the network it is protecting.

Firewalls can be fooled by source routing or address spoofing. To combat such attacks, firewalls must be configured to support identification and authentication techniques.