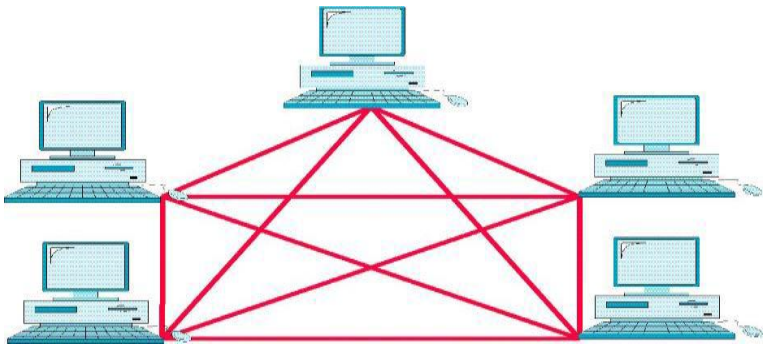
Computer Networks (UNIT - 1)

Topology: Network topologies refer to the diagrammatic representation of the arrangement of network devices and computers. Such representation illustrates the actual organization of the devices:-

Following are the main types of network topologies used in LAN:-

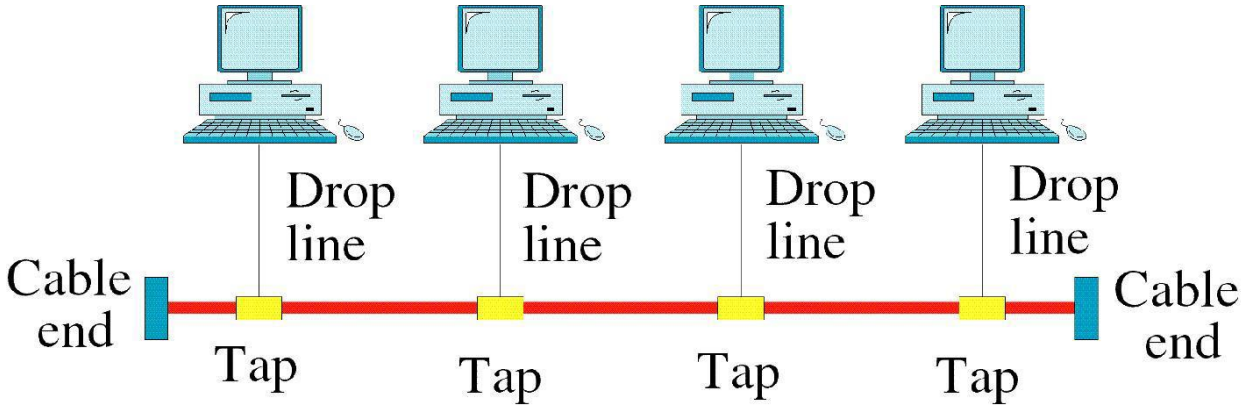
- • Star Topology
- • Bus Topology
- • Ring Topology
- • Mesh Topology
- • Tree Topology
-

• a) **Mesh Topology:** The advantages of a mesh topology are that the two nodes are using the entire capacity of the link exclusively. In terms of robustness, a mesh topology network can withstand the destruction of anyone of its components without incapacitating the entire network. Due to its nature, the mesh network physically prevents any intrusion on the information sent. Total number links required:- n(n-1)/2



To connect all its nodes together, a mesh topology would require n(n-1)/2 wires, or channels. This number increases exponentially when new nodes are added to the network. Each node itself would, then, be equipped with n-1 I/O ports to connect itself to the network. The disadvantage of the mesh topology is, simply, the amount of cabling itself.

(b) Bus Topology: The alternative to the simple network topology is by using a shared media. On such topology is the bus topology which makes use of a common shared media. In this case, a linear bus network would dramatically reduce the amount of wiring needed.

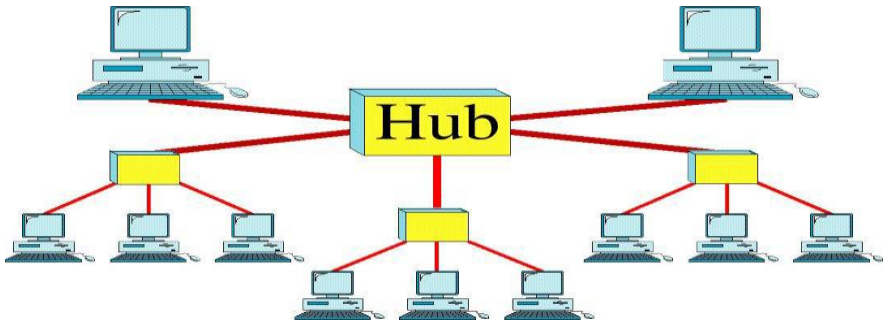


Each node is connected to the backbone via a combination of a drop line and a tap. This configuration reduces the amount of wires when compared to the mesh topology. The backbone itself can be stretched to be physically closer to the individual nodes themselves, thus reducing the length of the drop line.

The bus topology fails in terms of fault detection and isolation. Should there be a break in the backbone; a network administrator would have to test the link physically to find the problem. Secondly, since a tap must physically be connected to the backbone, it would have to undergo constant change in order to incorporate new nodes.

(c) Tree Topology:

Addition of new networks to a bus topology would be hard. A tree topology, however, is an extension of the bus. In a tree, the trunk is usually a high capacity device or connection which facilitates data transmission amongst the branches.

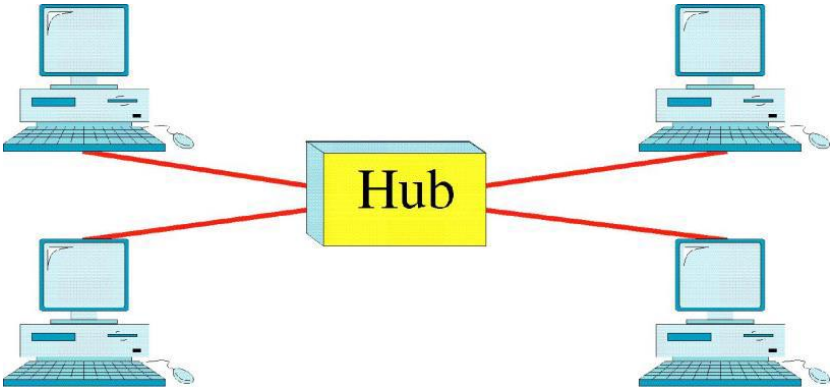


The advantage of a tree topology is usually that the privacy of transmissions is isolated in a particular branch.

Also, if a particular branch is incapacitated, the trunk and the other branches may still function.

The disadvantage is naturally the fault isolation. Should a transmission fails to be sent, a fault detection exercise may have to cover the entire distance of the cabling. The trunk of the tree must also be properly configured to be robust.

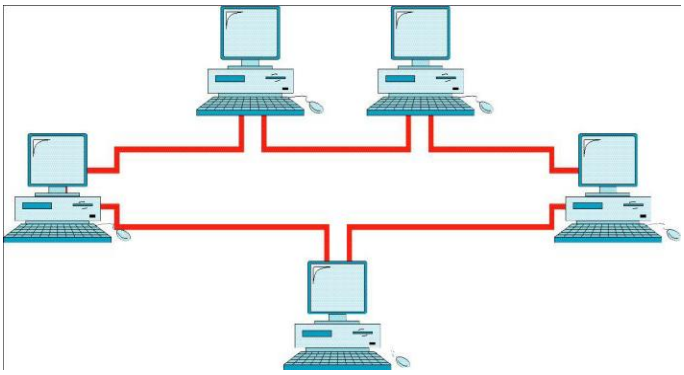
(d) Star Topology: The star topology is logically similar to a bus topology, though physically different. In a star topology, every node is connected to a hub, which acts as a central facilitator of transmissions. Each node has a dedicated link to the hub.



The advantage of the star topology is that fault isolation and detection can be done centrally. The hub can act as a monitor to network conditions. In some more intelligent hubs, multiple transmission channels can be directly be re-routed to the destination, simultaneously

While the hub is the star topology's chief advantage, it is also the main disadvantage of the topology. The network is fully dependent on the hub for it to work. Cabling sometimes poses a problem to the star topology too, as each node must have a dedicated link to the hub making for a potentially messy infrastructure.

(e) Ring Topology: The final structure to link a network is the ring topology. In the ring topology, a node has direct connections only to the two nodes on either sides. This "chain" would then provide a unidirectional transmission channel for all the nodes connected to it



The ring topology provides a relatively easy way installing and reconfiguring a network. The process of adding and removing a node would have to only consider the two nodes beside it. Fault isolation can be easily done when a station has not received any signals for a time. It would then issue an alarm to the administrator. The disadvantage of a ring topology is often the unidirectional traffic it can handle. If a node is down, signals can no longer circulate amongst the network, thus preventing the network from operating further.

Switching:

Switching refers to the concept of establishing path from source to destination to transfer data between these two.

Switching is of three types
(1) Circuit Switching.
(2) Packet Switching.
(3) Message Switching.

Circuit Switching

In circuit switching first of all optimized path is established, complete data is transferred then through that path. Main advantage of this kind of switching is reliability; time-consumption in path establishment at beginning is the main disadvantage of circuit-switching.

In Circuit switching a dedicated path establishes between two communicating nodes before actual data transfer begins. The path means that connected sequence of physical links in which logical channel is dedicated to the connection

Example: Telephonic Communication.

Phase of Circuit Switching:

There are three phases of circuit switching.
1. Circuit Establishment
2. Data Transfer
3. Circuit Disconnect

Circuit Establishment:

In **circuit switching**, data transfer can't start automatically, before data transfer, a dedicated link is to established end-to-end. At first, the sender sends a request for connection to its attached switch. The switch depending on the destination address and the condition of traffic routes the connection request to the next switch.

The second switch also does the same work. This process goes on until a switch is reached with which the destination node is connected directly. The last switch sends the connection request then it sends an acknowledgement signal to the sender. The time required for circuit establishment is 2-10 seconds depending on the network and distance between the endpoints.

Data Transfer:

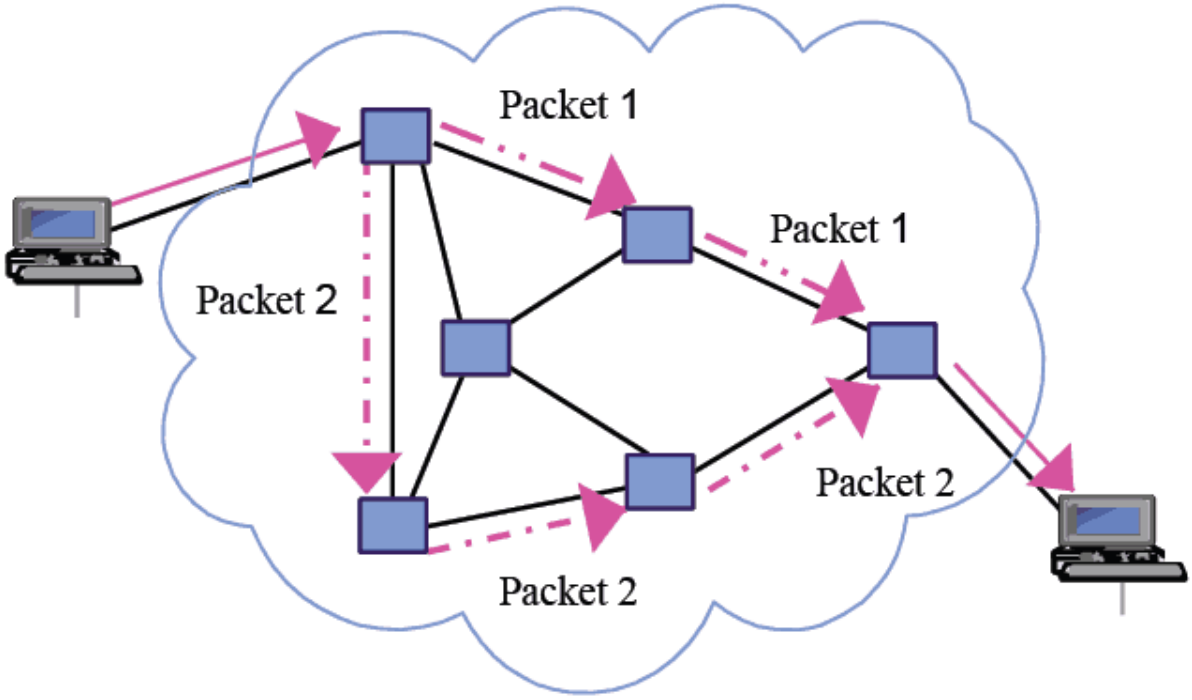
Once the connection establish, the data can transfer from one sender to receiver. Generally, the connection is full-duplex. In that case, the data can be exchanged both ways simultaneously. Data may be digital or analogue depending on the network architecture. The Data exchange is in a block and sent continuously. No routing or other controlling mechanisms require during data transfer.

Tear Down:

The circuit may disconnect by either end and the disconnection information transfers from one end to another following the dedicated path. The intermediate switches after passing the disconnection information release the path. In this way, the dedicated path becomes free and can be used for a new connection.

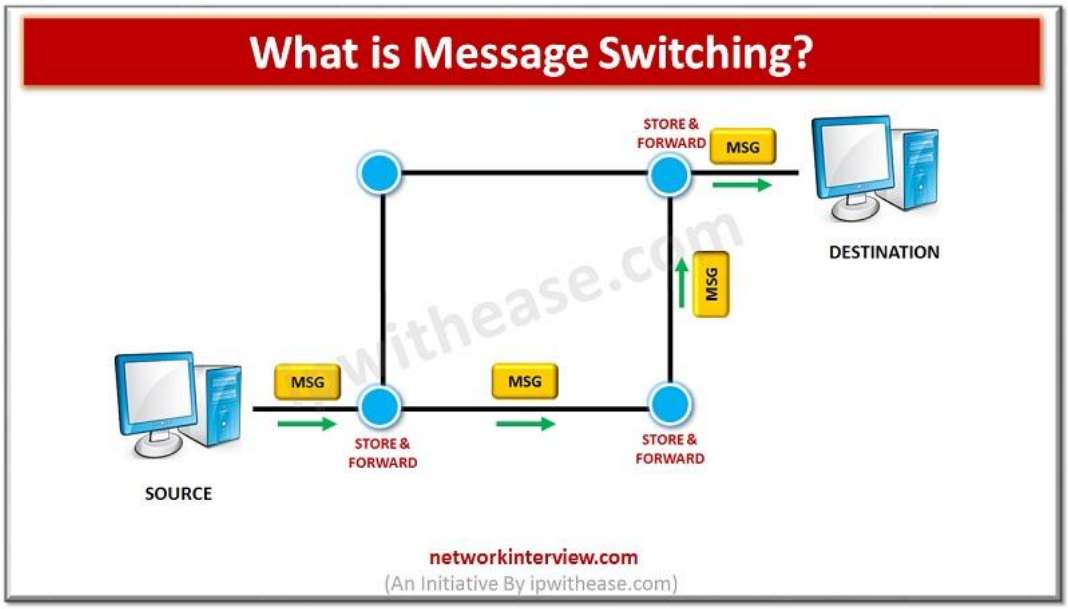
Packet Switching:

In **Packet Switching**, the sender breaks the whole message into several packets of suitable length and consisting of sequential packet numbers. No dedicated path establishes between the two end parties before data communication. The sender sends packets to the next node sequentially. Each node after receiving a packet decides the next route for the packet, the routing decision is done by a node in the path before sending every packet.



Message Switching:

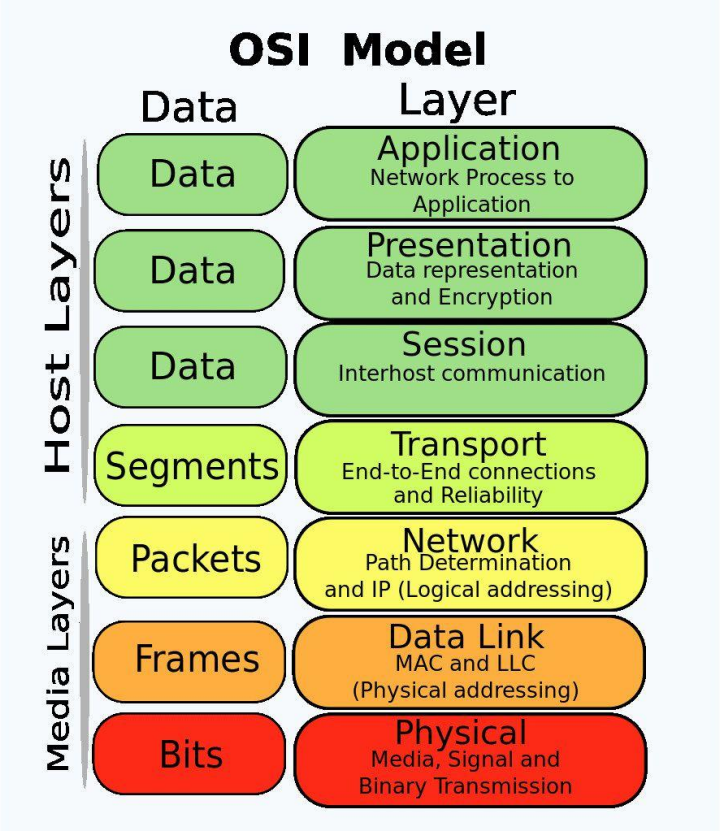
It is a combination of circuit switching and packet switching. Like circuit switching, the message is not broken into packets rather it is sent to the next node as a whole. Like packet switching, no dedicated path establishes between the two end parties before data communication. The routing decision is done at each node for the whole message.



OSI Model

Developed in 1984, the **Open Systems Interconnection** or **OSI model** is a seven-layer model used to describe networking connections. It was initially developed by ISO, the International Organization for Standardization in 1984 and is now common practice for learning networking concepts.

The OSI models specifies **how information is transmitted** from a network device like a router to its destination through a physical medium and how it interacts with the application. In other words, it provides a standard for different systems to communicate with each other.



7 Layers of the OSI Model

We will go through the different layers in detail below, but keep in mind that the upper layers (first 4) are about **transport issues** like the physical characteristics of the network and data transmission.

The lower layers (last 3) are about **application issues** like data formatting and user interfacing.

Some people argue that the OSI model is obsolete because it is less important than the four layers of the TCP/IP model, but this is not true. The OSI model is essential theory for understanding modern computer network technology in a connection-oriented way.

Most discussions on network communication include references to the OSI model and its conceptual framework.

The purpose of this model is to enhance interoperability and functionality between different vendors and connectors. It describes the functions of a networking system. From a design point of view, it divides larger tasks into smaller, more manageable ones.

The OSI model allows network administrators to focus on the design of particular layers. It is also useful when troubleshooting network problems by breaking them down and isolating the source.

Layer 1: Physical Layer

At the lowest layer of the OSI reference model, the physical layer is responsible for **transmitting unstructured data bits** across the network between the physical layers of the sending and receiving devices. In other words, it takes care of the transmission of raw bit streams.

The physical layer may include physical resources like cables, modems, network adapters, and hubs, etc.

Layer 2: Data Link Layer

The data link layer **corrects any errors** that may have occurred at the physical layer. It ensures that any data transfer is error-free between nodes over the physical layer. It is responsible for reliable transmission of data frames between connected nodes.

The data is packaged into frames here and transferred node-to-node. The data layer has the following sub-layers

- **Media Access Control (MAC):** The MAC address layer is responsible for flow control and multiplexing devices transmissions over the network.
- **Logical link control (LLC):** The LLC layer provides error control and flow control over the physical medium and identifies line protocols.

Layer 3: Network Layer

The network layer **receives frames from the data link layer** and **delivers them** to the intended destination based on the addresses inside the frame. It also handles packet routing. The network layer locates destinations using logical addresses like the IP. Routers are a crucial component at this layer as they route information to where it needs to go between different networks.

The main functions of the Network layer are:

- **Routing:** The network layer protocols determine which routes from source to destination.
- **Logical Addressing:** The network layer defines an addressing scheme to uniquely identify devices. The network layer places the IP addresses from the sender and receiver in the header.

Layer 4: Transport Layer

The transport layer is responsible for **delivering, error checking, flow control**, and **sequencing data packets**. It regulates the sequencing, size, and transfer of data between systems and hosts. It gets the data from the session layer and breaks it into transportable segments.

Two examples of the Transport Layer are the *UDP (User Datagram Protocol)* and *TCP (Transmission Control Protocol)* that is build on top of the Internet Protocol (IP model), which work at layer 3.

Layer 5: Session Layer

The session layer will create communication channels, called **sessions**, between different devices. This layer is responsible for opening those sessions and ensuring that they're functional during data transfer.

In other words, the session layer is responsible for establishing, managing, and terminating communication sessions with the lower layers with the presentation and application layer. It is also responsible for authentication and reconnections, and it can set checkpoints during a data transfer—if.

Layer 6: Presentation Layer

The presentation layer is responsible for ensuring that the data is **understandable for the end system** or useful for later stages. It translates or formats data based on the application's syntax or semantics. It also manages any encryption or decryption required by the application layer. It is also called the *syntax layer*.

Layer 7: Application Layer

The application layer is where the user directly interacts with a software application, so it is **closest to the end user**. When the user wants to transmit files or pictures, this layer interacts with the application communicating with the network. The application layer identifies resources, communication partners, and synchronizes communication.

Other functions of the application layer are the Network Virtual Terminal and FTAM-File transfer access, and mail/directory services. The protocol used depends on the information the user wants to send. Some common protocols include:

- POP3 or SMTP for emails
- FTP for emails
- Telnet for controlling remote devices

Examples of communications that use Layer 7 are web browsers (Chrome, Firefox, Safari).

Data flow example

Here is how data flows through the OSI model. Let's say you send an email to a friend. Your email passes through the **application layer** to the **presentation layer**. This layer will compress your data.

Next, the **session layer** initializes communication. It will then be segmented in the transportation layer, broken up into packets in the network layer, and then into frames at the data link layer. It will then be sent to the **physical layer** where it is converted to 0s and 1s and sent through a physical medium like cables.

When your friend gets the email through the physical medium, the data flows through the **same layers but in the opposite order**. The physical layer will convert the 0s and 1s to frames that will be passed to the data link layer. This will reassemble the frames into packets for the next layer.

The **network layer** will assemble the segments into data. The data is then passed on to the presentation layer that ends the communication session. The **presentation layer** will then pass the data to the application layer. The **application layer** feeds the human-readable data to the email software that will allow your friend to read your email.

Backbone Design

Distributed backbone

A distributed backbone is a backbone network that consists of a number of connectivity devices connected to a series of central connectivity devices, such as hubs, switches, or routers, in a hierarchy. This kind of topology allows for simple expansion and limited capital outlay for growth, because more layers of devices can be added to existing layers. In a distributed backbone network, all of the devices that access the backbone share the transmission media, as every device connected to this network is sent all transmissions placed on that network.

Distributed backbones, in all practicality, are in use by all large-scale networks. Applications in enterprise-wide scenarios confined to a single building are also practical, as certain connectivity devices can be assigned to certain floors or departments. Each floor or department possesses a LAN and a wiring closet with that workgroup's main hub or router connected to a bus-style network using backbone cabling. Another advantage of using a distributed backbone is the ability for network administrator to segregate workgroups for ease of management.

There is the possibility of single points of failure, referring to connectivity devices high in the series hierarchy. The distributed backbone must be designed to separate network traffic circulating on each individual LAN from the backbone network traffic by using access devices such as routers and bridges.

Collapsed backbone

A conventional backbone network spans distance to provide interconnectivity across multiple locations. In most cases, the backbones are the links while the switching or routing functions are done by the equipment at each location. It is a distributed architecture.

A collapsed backbone (also known as inverted backbone or backbone-in-a-box) is a type of backbone network architecture. In the case of a collapsed backbone, each location features a link back to a central location to be connected to the collapsed

backbone. The collapsed backbone can be a cluster or a single switch or router. The topology and architecture of a collapsed backbone is a star or a rooted tree.

The main advantages of the collapsed backbone approach are

1. ease of management since the backbone is in a single location and in a single box, and
2. since the backbone is essentially the back plane or internal switching matrix of the box, proprietary, high performance technology can be used.

However, the drawback of the collapsed backbone is that if the box housing the backbone is down or there are reachability problem to the central location, the entire network will crash. These problems can be minimized by having redundant backbone boxes as well as having secondary/backup backbone locations.

Parallel backbone

There are a few different types of backbones that are used for an enterprise-wide network. When organizations are looking for a very strong and trustworthy backbone they should choose a parallel backbone. This backbone is a variation of a collapsed backbone in that it uses a central node (connection point). Although, with a parallel backbone, it allows for duplicate connections when there is more than one router or switch. Each switch and router are connected by two cables. By having more than one cable connecting each device, it ensures network connectivity to any area of the enterprise-wide network.

Parallel backbones are more expensive than other backbone networks because they require more cabling than the other network topologies. Although this can be a major factor when deciding which enterprise-wide topology to use, the expense of it makes up for the efficiency it creates by adding increased performance and fault tolerance. Most organizations use parallel backbones when there are critical devices on the network. For example, if there is important data, such as payroll, that should be accessed at all times by multiple departments, then your organization should choose to implement a Parallel Backbone to make sure that the connectivity is never lost.

Serial backbone

A serial backbone is the simplest kind of backbone network. Serial backbones consist of two or more internet working devices connected to each other by a single cable in a daisy-chain fashion. A daisy chain is a group of connectivity devices linked together in a serial fashion. Hubs are often connected in this way to extend a network. However, hubs are not the only device that can be connected in a serial backbone. Gateways, routers, switches and bridges more commonly form part

of the backbone. The serial backbone topology could be used for enterprise-wide networks, though it is rarely implemented for that purpose.

Local Access Network Design :

The first step in Local Area Network design is determining network needs. Before building a Local Area Network, identify the number of devices, which determines the number of ports required. A switch can extend the number of ports as the number of devices increases.

In order to connect devices wirelessly, a router is required to broadcast a wireless LAN. A router is also required to establish an internet connection for devices on the network. The distance between hardware devices should be measured in order to determine the length of cables required. Switches can connect cables for very long distances.

The setup simply requires connecting the router to a power source, connecting the modem to the router, connecting the switch to the router (if using), and connecting the devices to the open LAN ports on the router via Ethernet. Next, set up one computer as a Dynamic Host Configuration Protocol server by installing a third-party utility. This will enable all of the connected computers to easily obtain IP addresses. Turn on “Network Discovery” and “File and Printer Sharing” capabilities.

For wireless Local Area Network Installation, start by connecting the computer into one of the router's LAN ports via Ethernet. Enter the router's IP address into any Web Browser and log in with the network administrator account when prompted for a username and password. Open the “Wireless” section in the router settings and change the name of the network in the “SSID” field.

Enable “WPA-2 Personal” as the security or authentication option. Create a password under “"Pre-Shared Key," ensure that the wireless network is “enabled,” save changes, restart the router, and connect wireless devices to the wireless network, which should appear on the available network list of devices within range.

Characteristics of wireless Local Area Network include: high capacity load balancing, scalability, network management system, role-based access control, indoor and outdoor coverage options, performance measuring abilities, mobile device management, web content and application filtering, roaming, redundancy, wireless Local Area Network Application prioritization, network switching, and network firewalls.

A common Local Area Network issue is a disabled Local Area Network adapter or adapter error, which can be caused by faulty network adapter settings or by VPN software. Typical solutions include: updating the network adapter driver, resetting the network connection, and checking WLAN AutoConfig dependency services.

Transmission media

Transmission media can be classified into two categories:-

(a) Guided Media–(i.e. Wired media) **(b)** Un-Guided Media–(i.e. Wireless media)

(a) Guided Media:- Guided Media covered following three kind of media:-

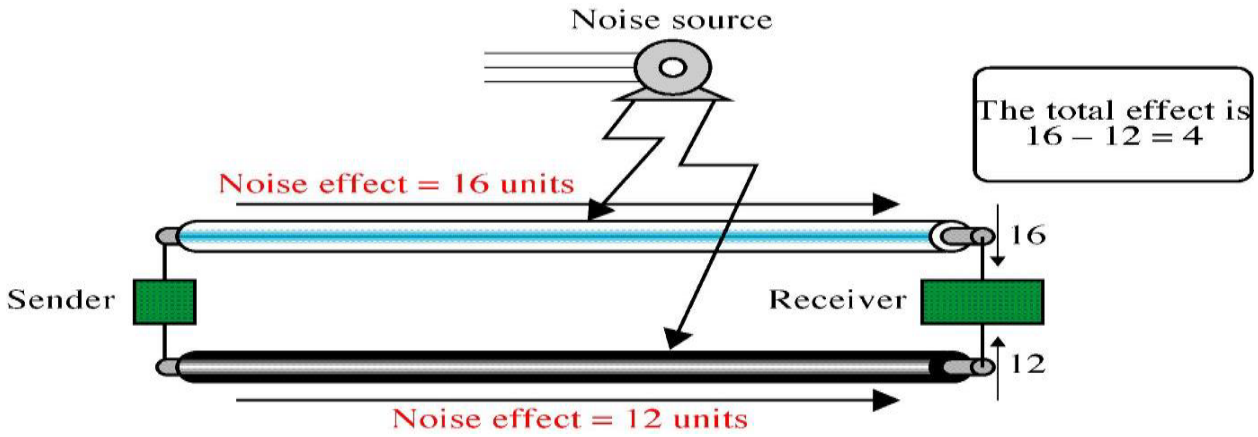
- - Twisted Pair Cables (Unshielded, Shielded)
- - Coaxial Cables
- - Optical Fiber Cables

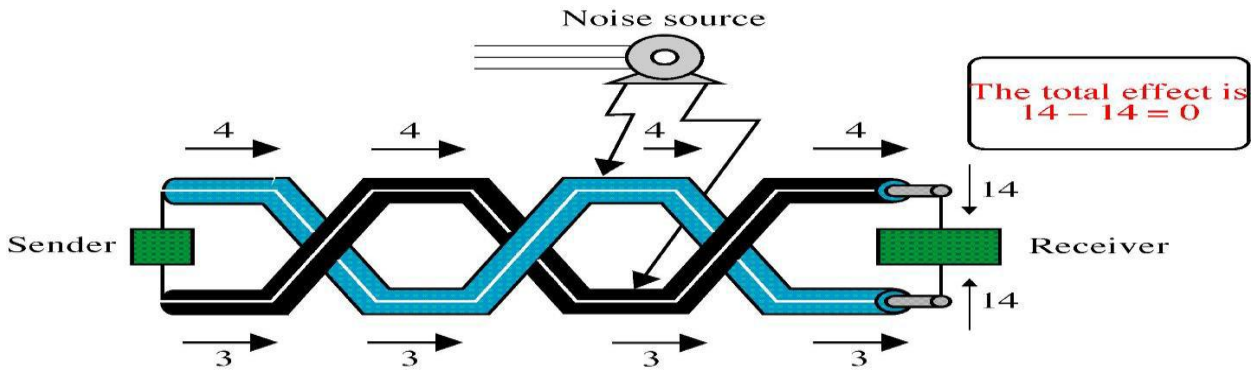
Twisted Pair:- Twisted pair refers to the collection of two insolated wires that are twisted with one another.

Twisted pair can be of two types:-

UTP (Unshielded Twisted Pair) :

- UTP cables are the most common telecommunications medium.
- The frequency range of the twisted pair cables enable both voice and data transmission.
- Usually consists of two copper wires wrapped in individual plastic insulation.
- Previously, two flat wires were used for communications but interference caused extremely high levels of damaged signals.
-





– Cost

– Ease of Use

– Flexibility

- Ease of Installation

Advantages of UTP cables:

The Electronic Industries Association (EIA) has developed standards to gauge the quality of cables.

• Category 1 – basic twisted pair cabling used in telecommunications system

• Category 2 – transmission up to 4Mbps

• Category 3 – transmission up to 10Mbps

• Category 4 – transmission up to 16Mbps

• Category 5 – transmission up to 100Mbps

• UTP cables come with connectors which is similar to that of telephone jacks. Male connectors snap into female connectors with a lock to hold them in place.

STP (Shielded Twisted Pair):-

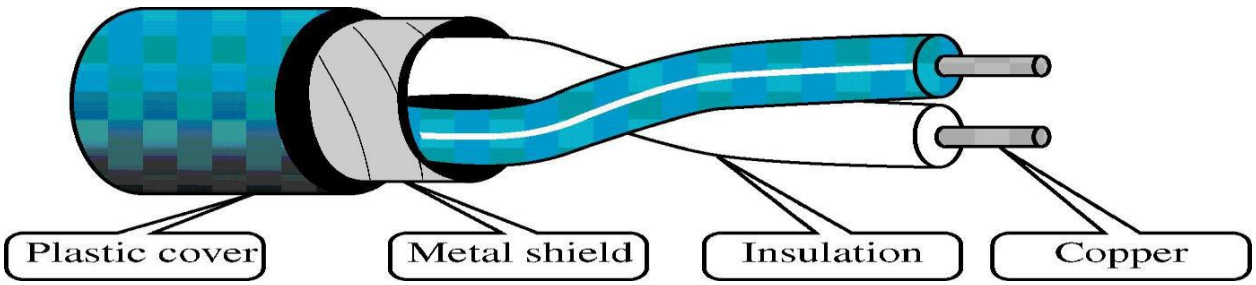
• An alternative to UTP

• The metal mesh around the insulated wires eliminates a phenomenon called crosstalk.

• Crosstalk occurs when one line picks up some of the other signals traveling down another line.

• Shielding each pair individually can eliminate most crosstalk.

• STP shares the same standards and considerations as UTP except that its more expensive.



Coaxial Cable

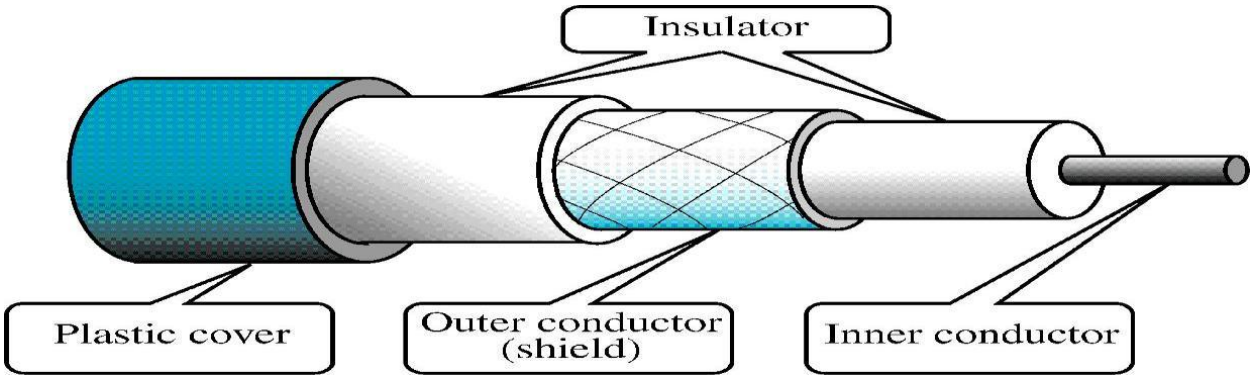
• Coax cables operate at a higher frequency range.

• Due to the construction which is more noise resistant and is very durable

• Due to their ability to transfer more information than standard telephone cables.

• Was primarily used to connect cable television. Now, coaxial cables are used as backbones of bus topologies.

• Connectors for coax cables are T-connectors and terminators.



Optical Fiber Cable

• Optical fiber technology differs from the previous conductive cables in that it uses light instead of currents.

• Before discussing about optical fiber, we need to explore the rationale behind its technology, which is light

Nature of Light

• The main criteria of light which matters toward the context of optical fiber technology are as follows: - Refraction • Angle of incidence

• Angle of refraction

- Critical Angle
- Reflection

Refraction

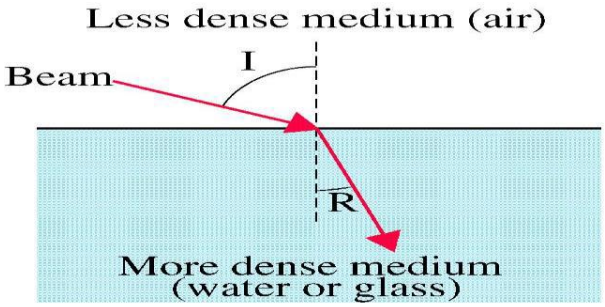
• Describes how light changes direction when it enters a different medium, due to its sudden change in speed.

• The angle of incidence describes the degree of deviation from the vertical axis before the source enters the new medium

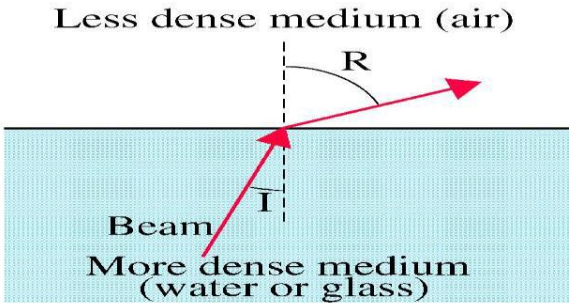
• The angle of refraction refers to the deviation degree from the vertical axis after the change of medium

• The angle of incidence will always be larger than the angle of refraction when light is traveling into a medium which is more dense.

• And the angle of refraction will be larger when light travels into a medium less dense.



a. From less dense to more dense medium



b. From more dense to less dense medium

Critical Angle

• If we increase the angle of incidence when light is traveling to a less dense medium, we know that the refracted angle will stray towards the horizontal

• At some point in the process, the refracted angle will be traveling along the horizontal.

• The angle of incidence will then be known as the critical angle.

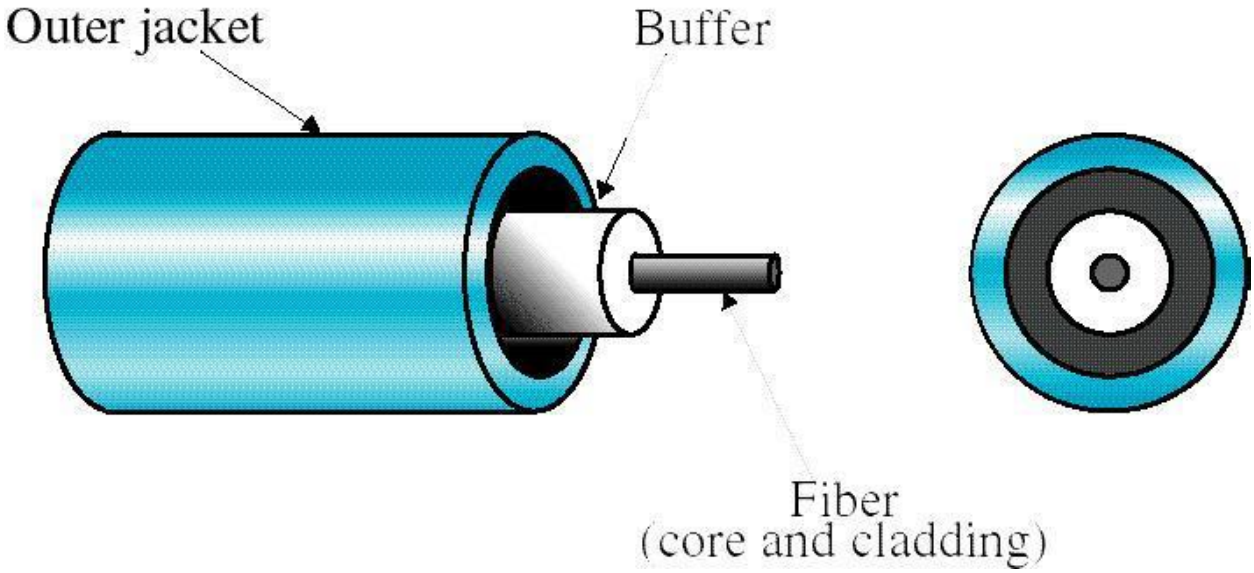
Optical Fiber

• Optical fiber utilizes reflection to guide light along.

• Optical fiber cables consists of a core surrounded by a less dense cladding.

• Both core and cladding can be made out of glass or plastic

• The difference of density is calculated to a point that light is reflected along the wire instead of refracted into it.



Advantage of Fiber Optic

• Noise resistance – Because optical fiber uses light, it is completely immune to the effects of noise

• Less signal attenuation – Transmissions can travel large distances before requiring regeneration

• Higher bandwidth – Fiber cables can transport much higher data rates than twisted pair or coax cables. Currently, data rates are limited by transmission and reception technology, not the medium.

Disadvantage of Fiber Optic

• Cost – Due to their need for perfection in the cable's core, manufacturers have to undergo very precise procedures.

– Also, a laser transmitter costs significantly more than electrical generators

• Installation – The entire length of the fiber cable must be crack-free and all splices must be perfectly fused. Also, the entire network must be light-proof.

• Fragility – Because of its nature, fiber cables are not very portable as shocks could crack the fiber and render it useless.

Delay Analysis

In Network Terminology, Delay refers to total Time Consumed during Message Transferring from sender to receiver.
There are three types of Delay.

1) **Propagation-Delay**:->>Due to distance
Tp=d/V, where d=Distance V=velocity.

2) **Transmission-Delay**:->>Time taken by Frame to come out fro Transmitter.
Tt=L/U where L=Frame-size U=Data-rate.

3) **Node-Delay or Processing-Delay** :->> Time taken at each node.
Tn=Time consumed at each node for Processing etc.

Delay-Consideration in Topological Design.
*Propagation Delay can not be reduced, as it depends upon distance between transmitter-receiver & velocity of Signal.
*Transmission Delay can be reduced, by increasing the data-rate of the line. It can also be reduced by limiting the size of frame.
*Node delay can be reduced, by more dedicated paths. i.e. in Circuit-Switching, However Call-Set-up time increased here.

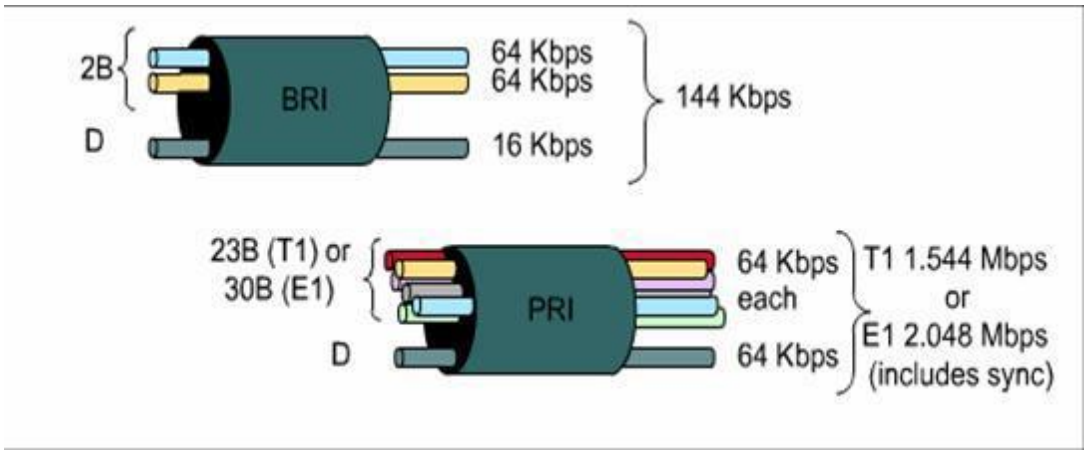
Characteristics of ISDN

ISDN (Integrated Service Digital): ISDN is a WAN technology based on digital communication, media is usually optical fiber. ISDN connections can support multiple services such as voice, internet and video conferencing services through same telephone line.

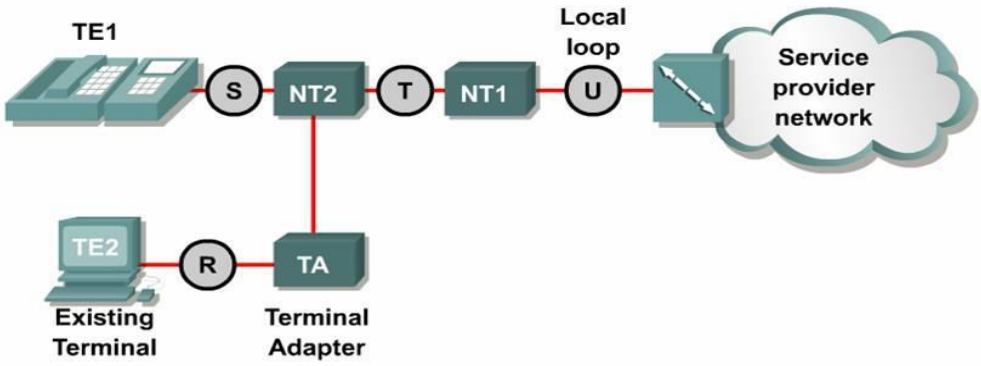
ISDN Connections can be of two types:-

(a) BRI (Basic Rate ISDN):- In BRI two B channels are used to carry data and one D channel is used to carry control information. Every B channel is of 64 Kbps and one D channel is of 16 Kbps.

(b) PRI (Primary Rate ISDN):- In PRI 23(T1) or 30(E1) B channels are used to carry data and one D channel is used to carry control information. Every B channel is of 64 Kbps and one D channel is of 64 Kbps.



ISDN-Network Structure:- A typical scenario for ISDN-Network may be as follows:-
The Meaning of various ISDN reference points and special devices are mentioned below:-



- Functional groups are devices or hardware
- Reference points are demarcations or interfaces

ISDN-Reference Point:-

R: The connection between a non-ISDN Terminal Equipment (TE2) and a Terminal Adapter (TA), e.g. an RS-232 serial interface.

S: References the points that connect into the customer switching device Network Termination type 2 (NT2) and enables calls between the various types of customer premises equipment.

T: Electrically identical to the S interface, it references the outbound connection from the NT2 to the ISDN network or Network Termination type 1 (NT1).

U: The connection between the NT1 and the ISDN network owned by the telephone company.

Device	Device Type	Device Function
TE1	Terminal Equipment 1	Designates a device with a native ISDN interface, such as an ISDN router or ISDN telephone.
TE2	Terminal Equipment 2	Designates a non-ISDN device, such as a workstation or router, that requires a TA to connect to an ISDN service provider.
TA	Terminal Adapter	Converts EIA/TIA 232, V.35, and other signals into BRI signals.
NT2	Network Termination 2	The point at which all ISDN lines at a customer site are aggregated and switched using a customer switching device.
NT1	Network Termination 1	Controls the physical and electrical termination of the ISDN at the customer's premises. Converts the four-wire BRI signals into two-wire signals used by the ISDN digital line.