Experiment 2

Name: Adwait S Purao

UID: 2021300101

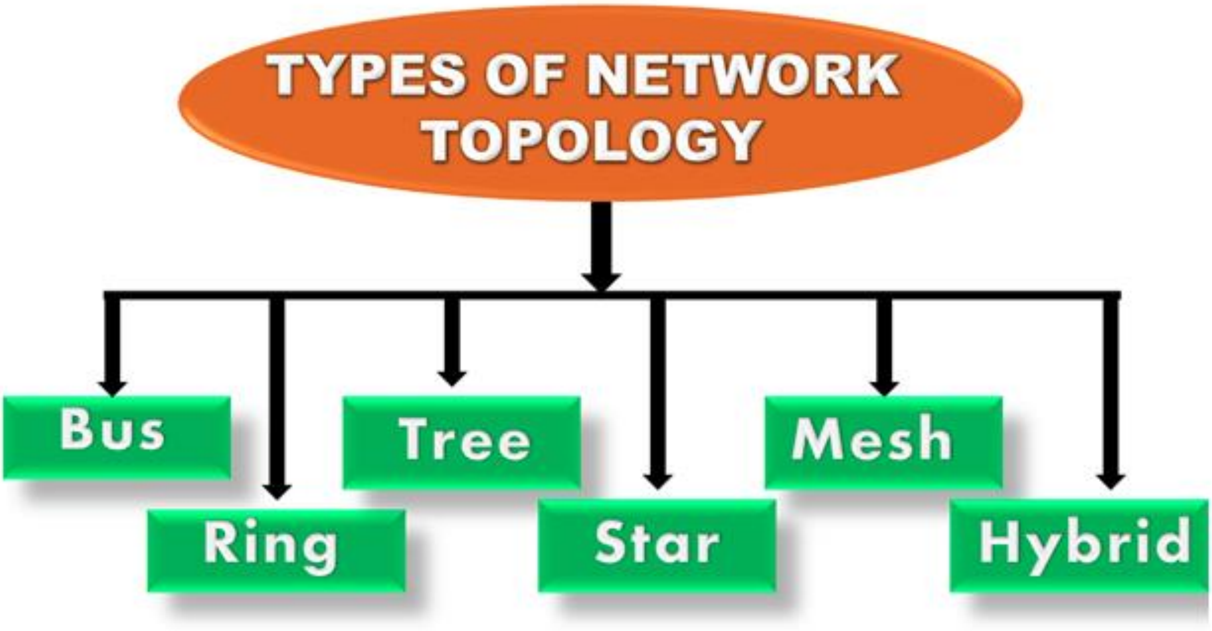
Batch: B2

What is Network Topology?

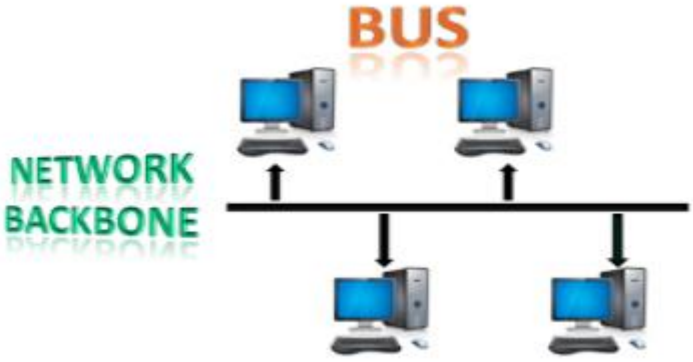
Topology defines the **structure of the network** of how all the components are interconnected to each other. There are two types of topology: **physical** and **logical** topology.

Types of Network Topology

Physical topology is the **geometric representation** of all the nodes in a network. There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.



1) Bus Topology



The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.

- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

- **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- **CSMA CA: CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

Advantages of Bus topology:

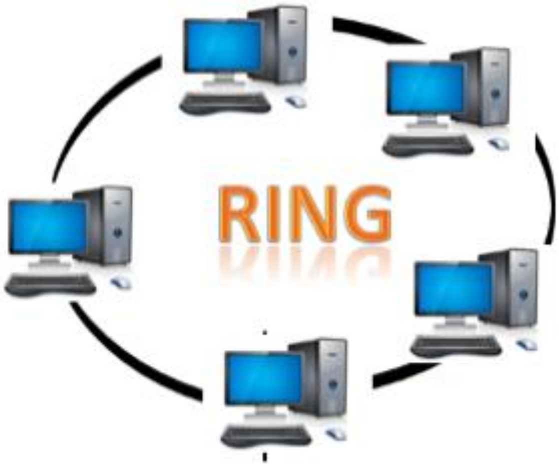
- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.

- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

2) Ring Topology



Ring topology is like a bus topology, but with connected ends.

- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
    - **Token passing:** It is a network access method in which token is passed from one node to another node.
    - **Token:** It is a frame that circulates around the network.

Working of Token passing

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

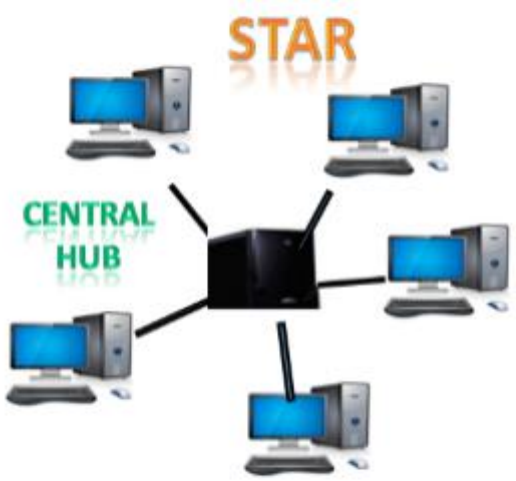
Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

3) Star Topology



Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.

- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

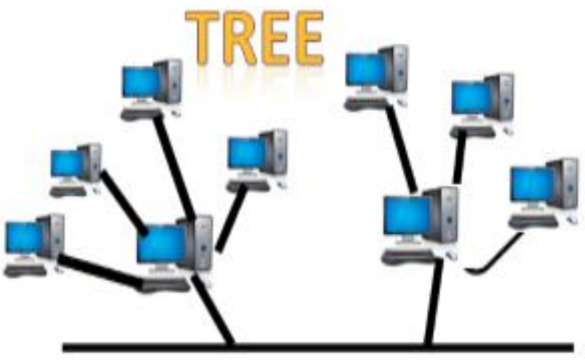
Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

4) Tree topology



Tree topology combines the characteristics of bus topology and star topology.

- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

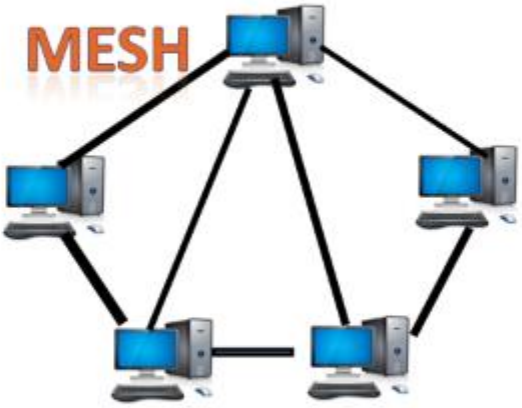
Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

5) Mesh topology



Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.

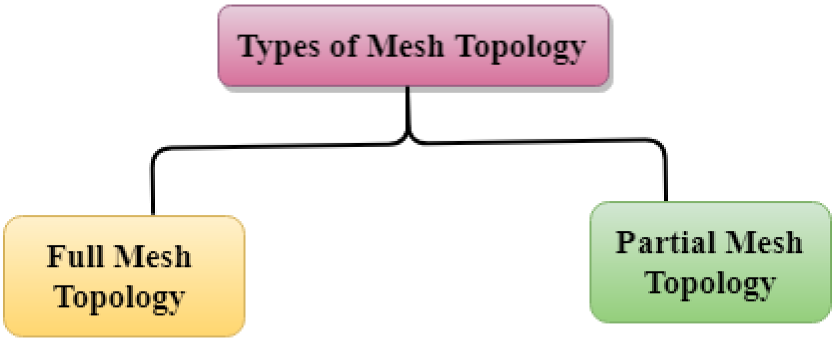
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.

- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula:
  Number of cables = (n*(n-1))/2;

- Where n is the number of nodes that represents the network.

- **Mesh topology is divided into two categories:**

- Fully connected mesh topology
- Partially connected mesh topology



Full Mesh Topology: In a full mesh topology, each computer is connected to all the computers available in the network.

- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

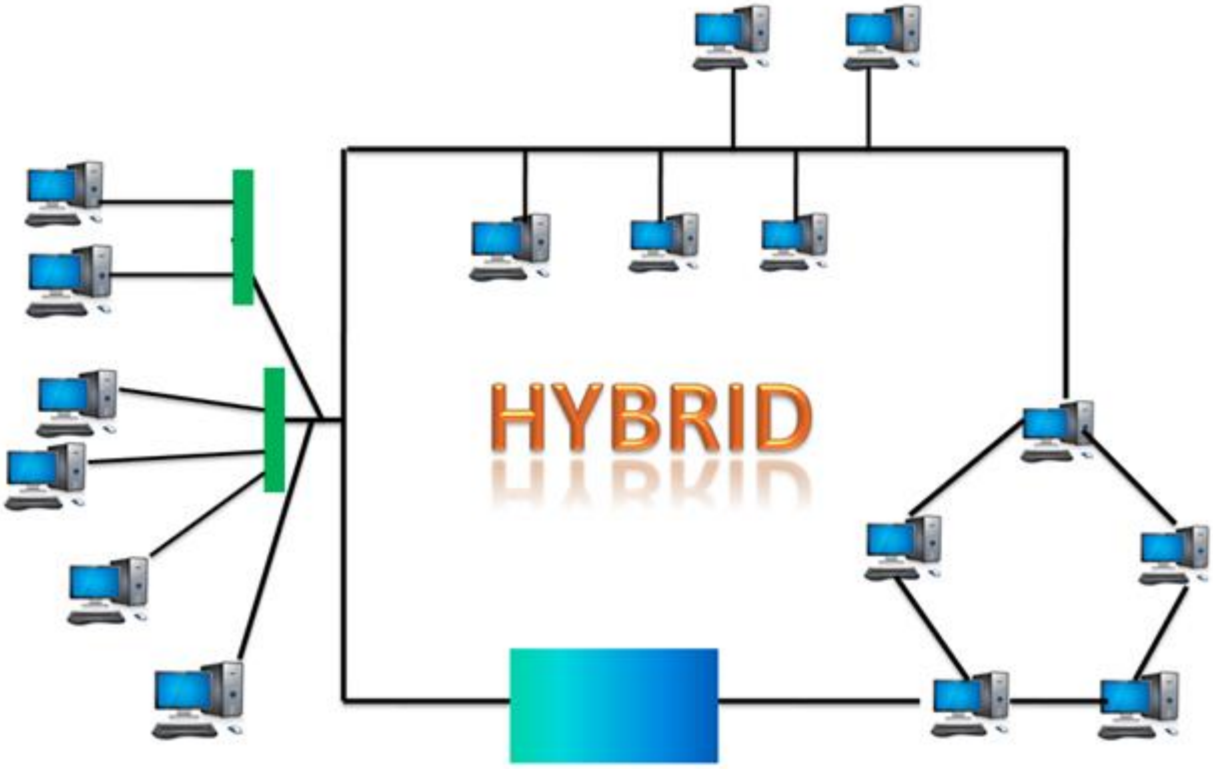
Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

6) Hybrid Topology



The combination of various different topologies is known as **Hybrid topology**.

- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.

- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc

What Is Network Hardware?

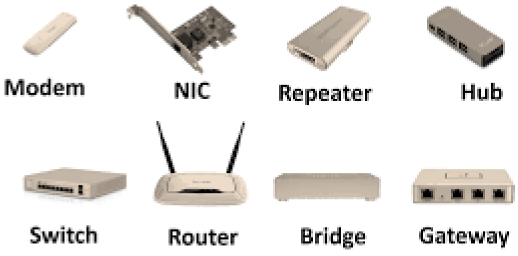
Network hardware is a set of physical or network devices that are essential for interaction and communication between hardware units operational on a computer network. These are dedicated hardware components that connect to each other and enable a network to function effectively and efficiently.

Today, technology has penetrated its tentacles into every nook and corner of our lives. It has gone from being just an industry add-on to an inevitable necessity. As tech enablement is driving the industrial transformation, it’s important for businesses to build a network that is secure, reliable and keeps the users in touch with their applications. The core of this very foundation is leveraged by the basic network hardware.

Network hardware plays a key role as industries grow as it supports scalability. It integrates any number of components depending on the enterprise’s needs. Network hardware helps establish an effective mode of communication, thereby improving the business standards. It also promotes multiprocessing and enables sharing of resources, information, and software with ease.

Network equipment is part of advancements of the Ethernet network protocol and utilizes a twisted pair or fiber cable as a connection medium. Routers, hubs, switches, and bridges are some examples of network hardware.

Let’s look at the fundamental devices of a computer network.



Types of Network Devices

- **Modems:** A modem enables a computer to connect to the internet via a telephone line. The modem at one end converts the computer’s digital signals into analog signals and sends them through a telephone line. At the other end, it converts the analog signals to digital signals that are understandable for another computer.
- **Routers:** A router connects two or more networks. One common use of the router is to connect a home or office network (LAN) to the internet (WAN). It generally has a plugged-in internet cable along with cables that connect computers on the LAN. Alternatively, a LAN connection can also be wireless (Wi-Fi-enabled), making the network device wireless. These are also referred to as wireless access points (WAPs).

- **Hubs, bridges, and switches:** Hubs, bridges, and switches are connecting units that allow multiple devices to connect to the router and enable data transfer to all devices on a network. A router is a complex device with the capabilities of hubs, bridges, and even switches.

  Hubs: A hub broadcasts data to all devices on a network. As a result, it consumes a lot of bandwidth as many computers might not need to receive the broadcasted data. The hub could be useful in linking a few gaming consoles in a local multiplayer game via a wired or wireless LAN.

  Bridges: A bridge connects two separate LAN networks. It scans for the receiving device before sending a message. This implies that it avoids unnecessary data transfers if the receiving device is not there. Moreover, it also checks to see whether the receiving device has already received the message. These practices improve the overall performance of the network.

  Switches: A switch is more powerful than a hub or a bridge but performs a similar role. It stores the MAC addresses of network devices and transfers data packets only to those devices that have requested Thus, when the demand is high, a switch becomes more efficient as it reduces the amount of latency.

- **Network interface cards**: A network interface card (NIC) is a hardware unit installed on a computer, which allows it to connect to a network. It is typically in the form of a circuit board or chip. In most modern machines, NICs are built into the motherboards, while in some computers, an extra expansion card in the form of a small circuit board is added externally.

- **Network cables**: Cables connect different devices on a network. Today, most networks have cables over a wireless connection as they are more secure, i.e., less prone to attacks, and at the same time carry larger volumes of data per second.

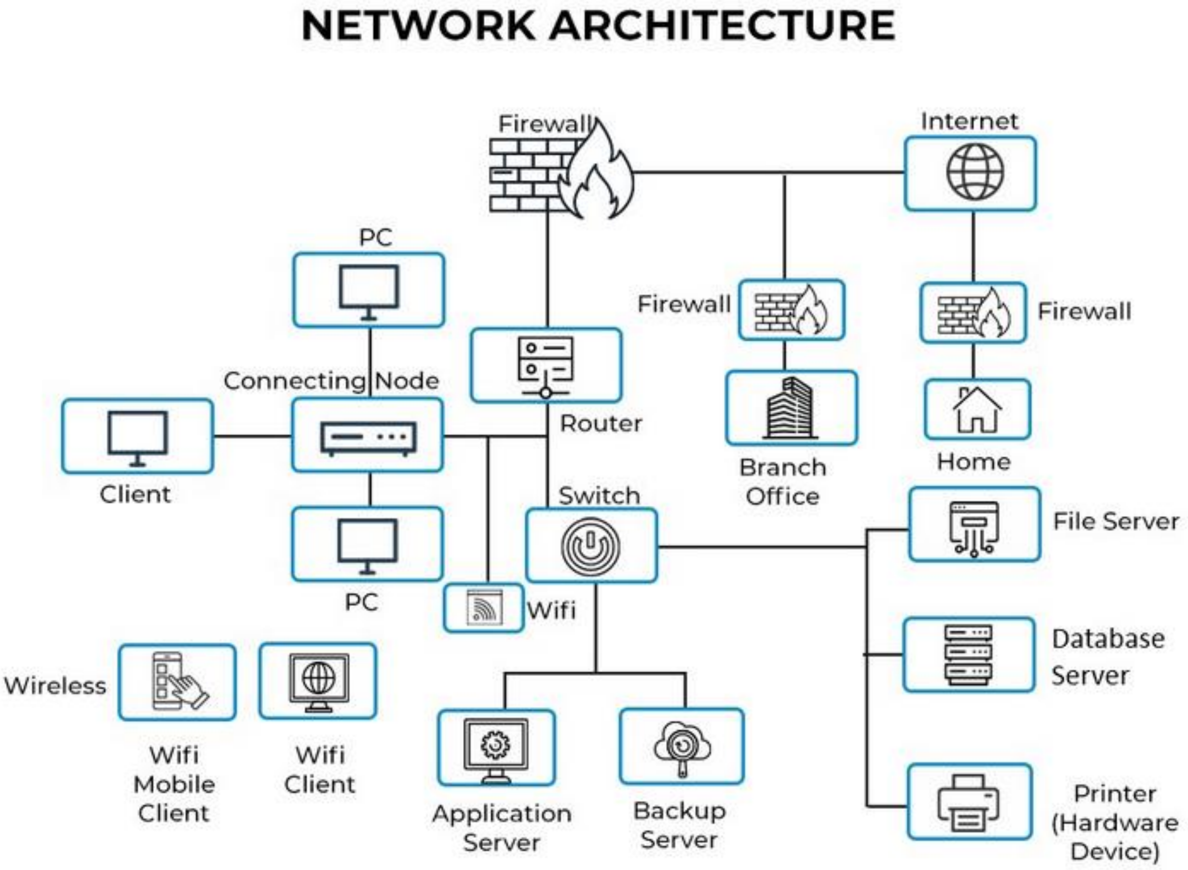
- **Firewall:** A firewall is a hardware or software device between a computer and the rest of the network open to attackers or hackers. Thus, a LAN can be protected from hackers by placing a firewall between the LAN and the internet connection. A firewall allows authorized connections and data-like emails or web pages to pass through but blocks unauthorized connections made to a computer or LAN.

  - **Gateways**

    A gateway connects entirely different networks that work upon different protocols. It is the entry and the exit point of a network and controls access to other networks.

Network Architecture: Key Components

Network architecture defines the structural and logical design of a network. It constitutes hardware devices, physical connections, software, wireless networks, protocols, and transmission media. It gives a detailed overview of the whole network, which organizations use to create LAN, WAN, and other specific communication tunnels.



Network architecture can be viewed from different vantage points depending on the size and purpose of the network. WAN refers to a group of interconnected networks distributed over large distances, while LAN refers to a computer network that interconnects computers within a limited space. Therefore, the architecture of a WAN will vary from that of a LAN in a small office.

Setting up the layout of the network architecture is critical, as it can either enhance or hamper the overall performance of the entire system. For example, selecting inappropriate transmission media or equipment for an expected server load in a network can cause slowdowns in different parts of the network.

As more user devices connect to the network, network architecture becomes even more significant by adding a security layer to protect connected devices. Additionally, modern network architectures support advanced user recognition and authorization.

Most network architectures are built on the open systems interconnection (OSI) model. Here, network tasks are segregated into seven logical layers, right from the lowest to the highest abstraction. For example, the lowest physical layer manages the wire and cable connections of the network, while the highest application layer deals with APIs that perform application-specific functions such as chat or file sharing. Overall, with the OSI model, troubleshooting the network is easier as the problems are isolated from each other at different layers.

Network architecture design is more about optimizing its fundamental building blocks. These include four key components:

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN, and WAN are the three major types of networks designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.
There are other types of Computer Networks also, like :

- PAN (Personal Area Network)
- SAN (Storage Area Network)
- EPN (Enterprise Private Network)
- VPN (Virtual Private Network)

Personal Area Network (PAN)-

PAN is a personal area network having an interconnection of personal technology devices to communicate over a short distance. It covers only less than 10 meters or 33 feet of area. PAN has fewer users as compared to other networks such as LAN, WAN, etc. PAN typically uses some form of wireless technology. PAN involves the transmission of data between information devices such as smartphones, personal computers, tablet computers, etc.

Local Area Network (LAN) –

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

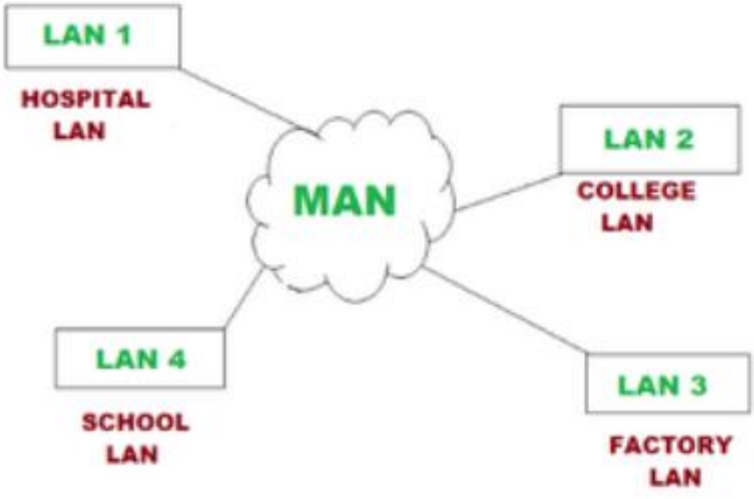
Data transmits at a very fast rate as the number of computers linked is limited. By definition, the connections must be high-speed and relatively inexpensive hardware (Such as hubs, network adapters, and Ethernet cables). LANs cover a smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, school, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example A bunch of students playing Counter-Strike in the same room (without internet).

Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service

Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It’s hard to design and maintain a Metropolitan Area Network.



The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN are moderate. Devices used for transmission of data through MAN are Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long-distance transmission, the noise and error tend to be more in WAN.

WAN’s data rate is slow about a 10th LAN’s speed since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN ranges from a few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for the transmission of data through WAN are Optic wires, Microwaves, and Satellites. An example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is a dial-up line that connects a home computer to the Internet.

Conclusion –

There are many advantages of LAN over MAN and WAN, such as LAN’s provide excellent reliability, high data transmission rate, they can easily be managed and shares peripheral devices too. Local Area Network cannot cover cities or towns and for that Metropolitan Area Network is needed, which can connect a city or a group of cities together. Further, for connecting a Country or a group of Countries one requires a Wide Area Network.

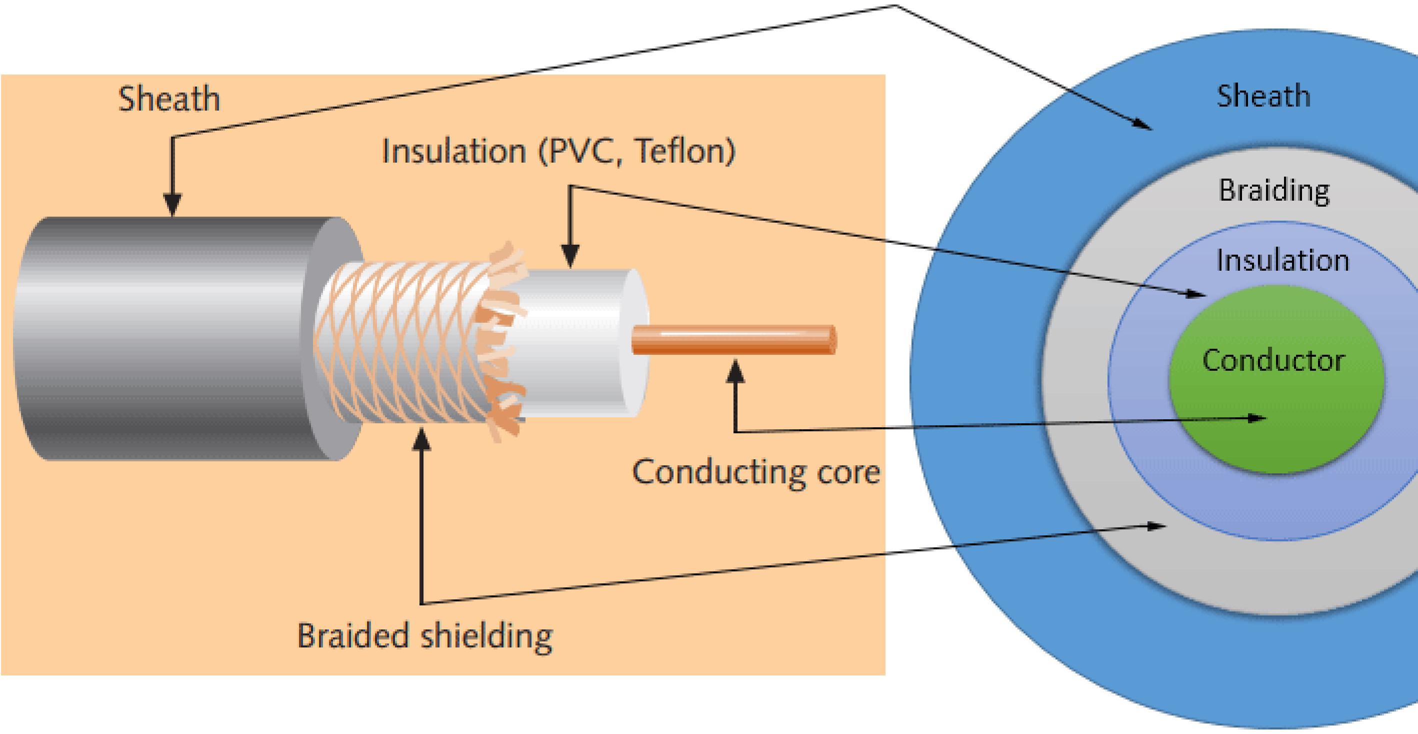
Network Cable Types and Specifications

To connect two or more computers or networking devices in a network, network cables are used. There are three types of network cables; coaxial, twisted-pair, and fiber-optic.

Coaxial cable

This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, the braiding covers the insulation, and the insulation covers the conductor.

The following image shows these components.



Sheath

This is the outer layer of the coaxial cable. It protects the cable from physical damage.

Braided shield

This shield protects signals from external interference and noise. This shield is built from the same metal that is used to build the core.

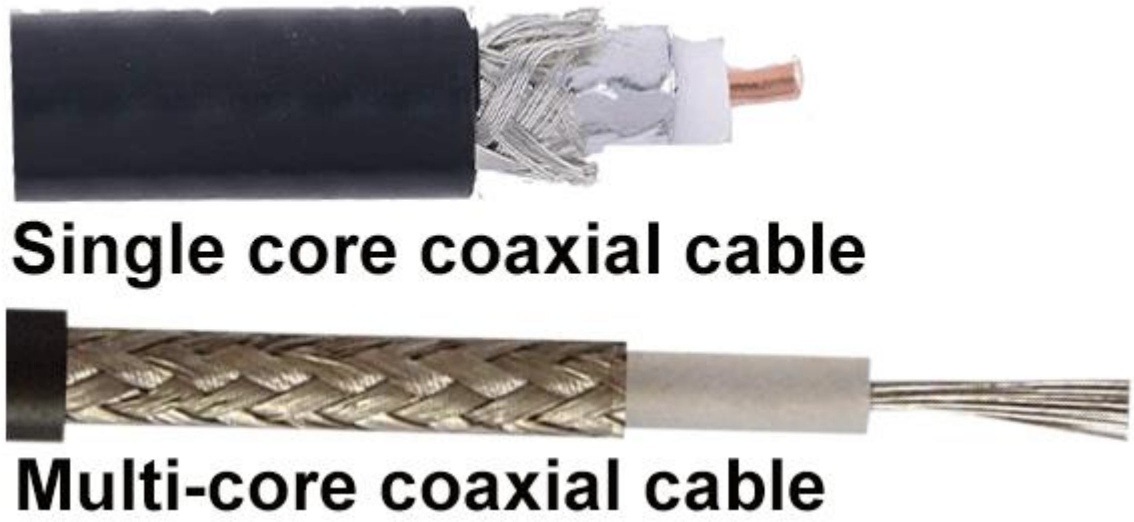
Insulation

Insulation protects the core. It also keeps the core separate from the braided shield. Since both the core and the braided shield use the same metal, without this layer, they will touch each other and create a short-circuit in the wire.

Conductor

The conductor carries electromagnetic signals. Based on conductor a coaxial cable can be categorized into two types; single-core coaxial cable and multi-core coaxial cable.

A **single-core** coaxial cable uses a single central metal (usually copper) conductor, while a **multi-core** coaxial cable uses multiple thin strands of metal wires. The following image shows both types of cable.



Coaxial cables in computer networks

The coaxial cables were not primarily developed for the computer network. These cables were developed for general purposes. They were in use even before computer networks came into existence. They are still used even their use in computer networks has been completely discontinued.

At the beginning of computer networking, when there were no dedicated media cables available for computer networks, network administrators began using coaxial cables to build computer networks.

Because of its low cost and long durability, coaxial cables were used in computer networking for nearly two decades (the 80s and 90s). Coaxial cables are no longer used to build any type of computer network.

Specifications of coaxial cables

Coaxial cables have been in use for the last four decades. During these years, based on several factors such as the thickness of the sheath, the metal of the conductor, and the material used in insulation, hundreds of specifications have been created to specify the characteristics of coaxial cables.

From these specifications, only a few were used in computer networks. The following table lists them.

Type	Ohms	AWG	Conductor	Description
RG-6	75	18	Solid copper	Used in cable network to provide cable Internet service and

				cable TV over long distances.
RG-8	50	10	Solid copper	Used in the earliest computer networks. This cable was used as the backbone cable in the bus topology. In Ethernet standards, this cable is documented as the 10base5 Thicknet cable.
RG-58	50	24	Several thin strands of copper	This cable is thinner, easier to handle and install than the RG-8 cable. This cable was used to connect a system with the backbone cable. In Ethernet standards, this cable is documented as the 10base2 Thinnet cable.
RG-59	75	20 - 22	Solid copper	Used in cable networks to provide short-distance service.

- Coaxial cable uses RG rating to measure the materials used in shielding and conducting cores.
- RG stands for the Radio Guide. Coaxial cable mainly uses radio frequencies in transmission.
- Impedance is the resistance that controls the signals. It is expressed in the ohms.
- AWG stands for American Wire Gauge. It is used to measure the size of the core. The larger the AWG size, the smaller the diameter of the core wire.

Twisted-pair cables

The twisted-pair cable was primarily developed for computer networks. This cable is also known as **Ethernet cable**. Almost all modern LAN computer networks use this cable.

This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green, and orange. In stripped color, the solid color is mixed with the white color.

Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable; UTP and STP.

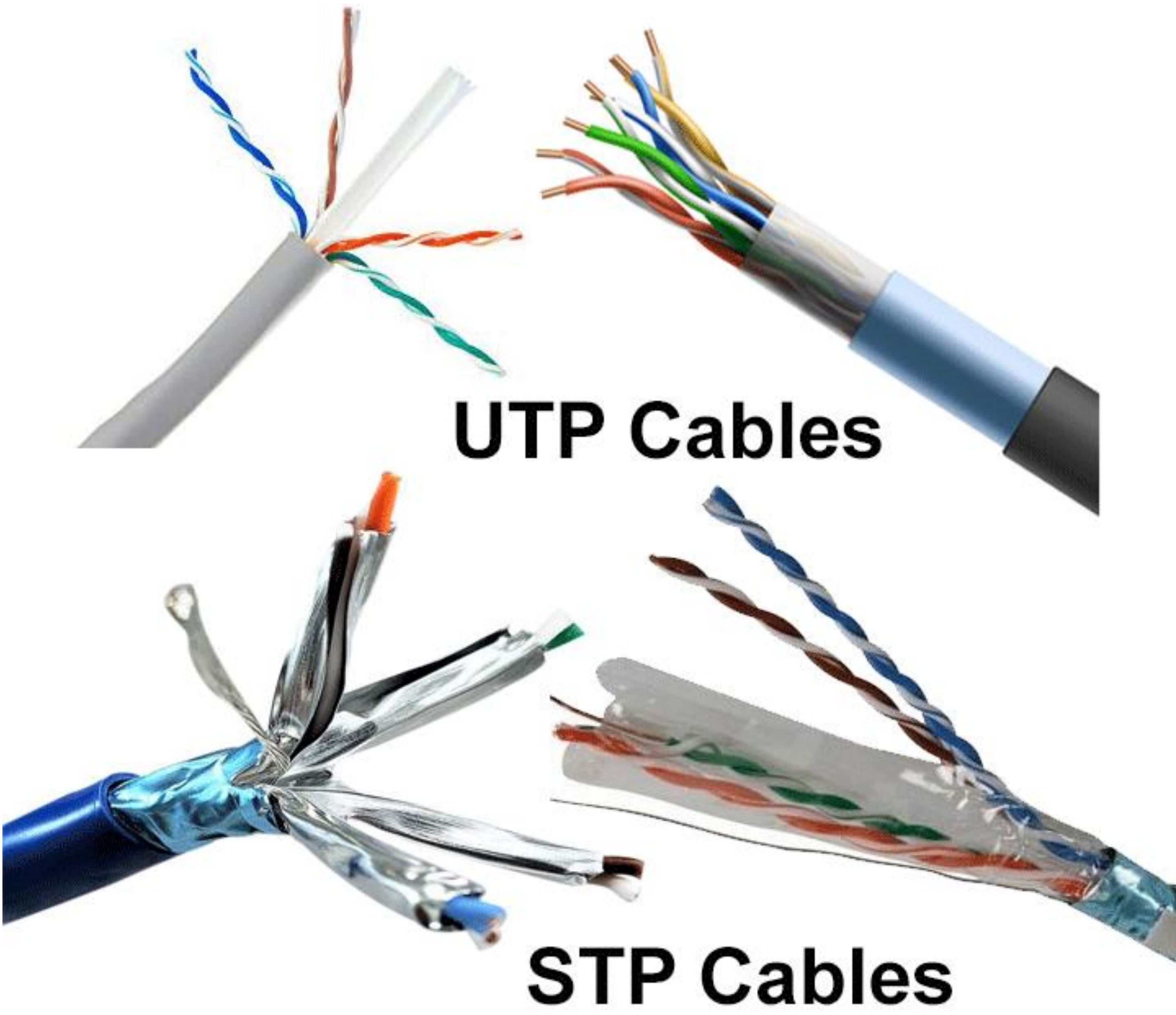
In the **UTP (*Unshielded twisted-pair*) cable**, all pairs are wrapped in a single plastic sheath.

In the **STP (*Shielded twisted-pair*) cable**, each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.

Similarities and differences between STP and UTP cables

- Both STP and UTP can transmit data at 10Mbps, 100Mbps, 1Gbps, and 10Gbps.
- Since the STP cable contains more materials, it is more expensive than the UTP cable.
- Both cables use the same RJ-45 (registered jack) modular connectors.
- Both cables can accommodate a maximum of 1024 nodes in each segment.
- The STP provides more noise and EMI resistance than the UTP cable.
- The maximum segment length for both cables is 100 meters or 328 feet.

The following image shows both types of twisted-pair cables.



The TIA/EIA specifies standards for the twisted-pair cable. The first standards were released in 1991, known as **TIA/EIA 568**. Since then, these standards have been continually revised to cover the latest technologies and developments of the transmission media.

The TIA/EIA 568 divides the twisted-pair cable into several categories. The following table lists the most common and popular categories of twisted-pair cable.

Category/name of the cable	**Maximum supported speed**	**Bandwidth/support signals rate**	**Ethernet standard**	**Description**
Cat 1	1Mbps	1MHz	Not used for data	This cable contains only two pairs (4 wires). This cable was used in the telephone network for voice transmission.
Cat 2	4Mbps	10MHz	Token Ring	This cable and all further cables have a minimum of 8 wires (4

				pairs). This cable was used in the token-ring network.
Cat 3	10Mbps	16MHz	10BASE-T Ethernet	This is the first Ethernet cable that was used in LAN networks.
Cat 4	20Mbps	20MHz	Token Ring	This cable was used in advanced Token-ring networks.
Cat 5	100Mbps	100MHz	100BASE-T Ethernet	This cable was used in advanced (fast) LAN networks.
Cat 5e	1000Mbps	100MHz	1000BASE-T Ethernet	This cable/category is the minimum requirement for all modern LAN networks.
Cat 6	10Gbps	250MHz	10GBASE-T Ethernet	This cable uses a plastic core to prevent cross-talk between twisted-pair. It also uses a fire-resistant plastic sheath.
Cat 6a	10Gbps	500MHz	10GBASE-T Ethernet	This cable reduces attenuation and cross-talk. This cable also potentially removes the length limit. This is the recommended cable for all modern Ethernet LAN networks.
Cat 7	10Gbps	600MHz	Not drafted yet	This cable sets a base for further development. This cable uses multiple twisted-pair and shields each pair by its plastic sheath.

- Cat 1, 2, 3, 4, 5 are outdated and not used in any modern LAN network.
- Cat 7 is still a new technology and not commonly used.
- Cat 5e, 6, 6a are the commonly used twisted-pair cables.

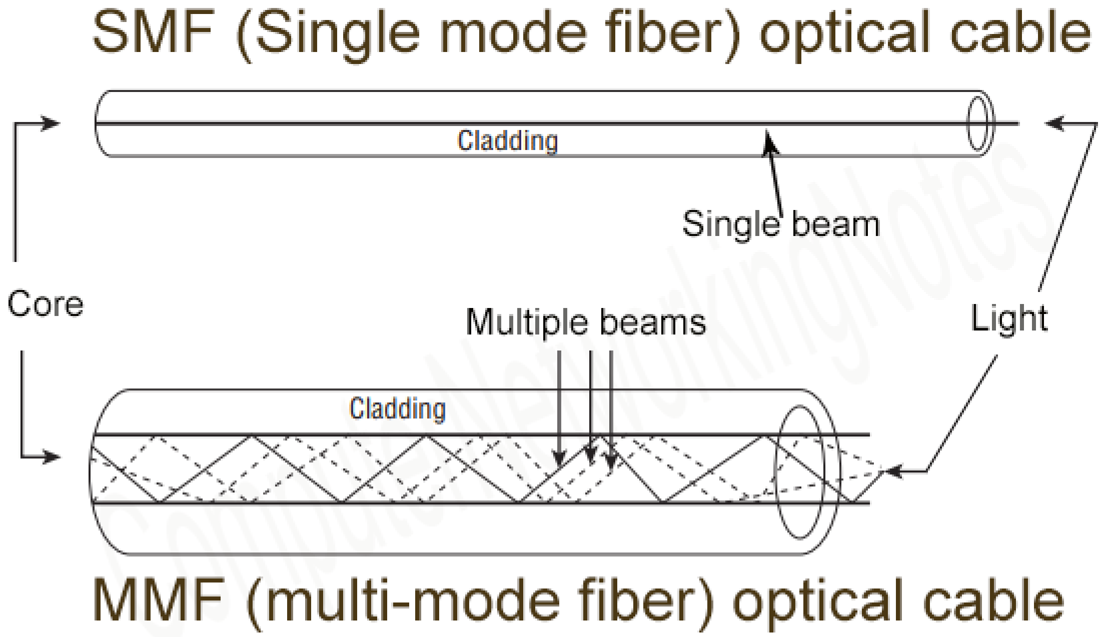
Fiber optic cable

This cable consists of a core, cladding, buffer, and jacket. The core is made from thin strands of glass or plastic that can carry data over a long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket.

- Core carries the data signals in the form of light.
- Cladding reflects light back to the core.
- Buffer protects the light from leaking.
- The jacket protects the cable from physical damage.

Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps.

Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.


SMF (Single mode fiber) optical cable
Cladding
Single beam
Core
Multiple beams
Light
Cladding
MMF (multi-mode fiber) optical cable

SMF (Single-mode fiber) optical cable

This cable carries only a single beam of light. This is more reliable and supports much higher bandwidth and longer distances than the MMF cable. This cable uses a laser as the light source and transmits 1300 or 1550 nano-meter wavelengths of light.

MMF (multi-mode fiber) optical cable

This cable carries multiple beams of light. Because of multiple beams, this cable carries much more data than the SMF cable. This cable is used for shorter distances. This cable uses an LED as the light source and transmits 850 or 1300 nano-meter wavelengths of light.

D-Link Switches

D-Link Fully Managed Switches can be deployed as core, distribution, or access switches, featuring high port densities, stacking, and versatile management. They support a complex suite of Layer 2, Layer 2+ and Layer 3 switching functions.
Choose a D-Link Fully Managed Switch when network performance and security are critical, and compromise is not an option.

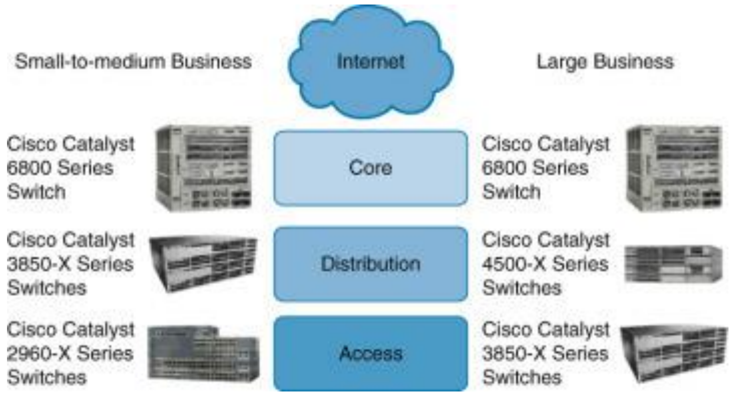
High Speed and Bandwidth
D-Link managed switches offer high bandwidth and are available in a wide range of port configurations including 1G, 10G, 25G, 40G, and 100G. These fully-featured L3 switches are suitable for a variety of enterprise, campus, and telco applications.

High Availability
All D-Link fully managed switches support redundant power supplies (RPS) to provide backup power in the event of a power outage, surge damage, or primary power supply failure. This high-redundancy design minimizes network downtime and lowers maintenance costs.

Flexible Upgrades
D-Link's range of fully managed switches supports upgradable software images. With the D-Link License Management System (DLMS), the switch software image can be easily upgraded on a need-only basis to unlock additional advanced features such as VLAN and L3 routing protocols to facilitate more demanding applications.

Stacking
Several D-Link fully managed switches can be combined in a physical or virtual stack to increase port count and bandwidth, which allows them to be managed using a single IP address through SSH, Telnet, the GUI interface, or SNMP. You can also manage them through a single out-of-band port.

Cisco Switches


Small-to-medium Business
Internet
Large Business
Cisco Catalyst 6800 Series Switch
Core
Cisco Catalyst 6800 Series Switch
Cisco Catalyst 3850-X Series Switches
Distribution
Cisco Catalyst 4500-X Series Switches
Cisco Catalyst 2960-X Series Switches
Access
Cisco Catalyst 3850-X Series Switches

Interesting enough, the Catalyst 6500 was not detailed in Figure 2-12. Despite its extremely long life cycle, Cisco marketing has finally shifted focus to the Catalyst 6800. For a large number of you reading this book, you have likely come across the Catalyst 6500 at some point in your career.

Cisco offers two types of network switches: fixed configuration and modular switches. With fixed configuration switches, you cannot swap or add another module, like you can with a modular switch. In enterprise access layers, you will find fixed configuration switches, like the Cisco Catalyst, 2960-X series. It offers a wide range of deployments.

In the enterprise distribution layer, you will find either fixed or modular switches depending on campus network requirements. An example of a modular switch that can be found in the distribution layer is the Cisco Catalyst 3850-X series. This series of switches allows you to select different network modules (Ethernet or fiber optic) and redundant power supply modules. In small businesses without a distribution layer, the 3850-X can be found in the core layer. In large enterprise networks, you might find 3850-X in the access layer in cases where high redundancy and full Layer 3 functionality at the access layer are requirements.

In the enterprise core layer, you will often find modular switches such as the Cisco Catalyst 6500 or the Catalyst 6800 series. With the 6800 switch, nearly every component, including the route processing/supervisor module and Ethernet models to power supplies) is individually installed in a chassis. This individualization allows for customization and high-availability options when necessary.

If you have a network where there is a lot of traffic, you have the option to leverage the Cisco Catalyst 4500-X series switches into the distribution layer. The Catalyst 4500-X supports supervisor/route process redundancy and supports 10 Gigabit Ethernet.

All switches within the 2960-X, 3850-X, 4500-X, and 6800-X series are managed. This means that you can configure an IP address on the device. By having a management IP address, you can connect to the device using Secure Shell (SSH) or Telnet and change device settings. An unmanaged switch is only appropriate for a home or very small business environment. It is highly recommended not to use an unmanaged switch in any campus network.

Conclusion :

In the above experiment we learnt about various types of network Hardware . Further we studied the various types of toplogies in computer networks along with their advantages and disadvantages.

We learnt about the architecture of networks . We learnt about the various types of cables . We learnt about man , wan , wlan and pan . At the end we studied about cisco and d-link switches.