

Unit: 2 Internet & Intranet

2.1 Concept of Internet and Intranet

2.1.1 Working of Internet & its Architecture

2.1.2 Working of Intranet and its architecture

2.1.3 Network Devices terminologies:

2.2 Types of Cables: co-axial, UTP, Fiber Optic

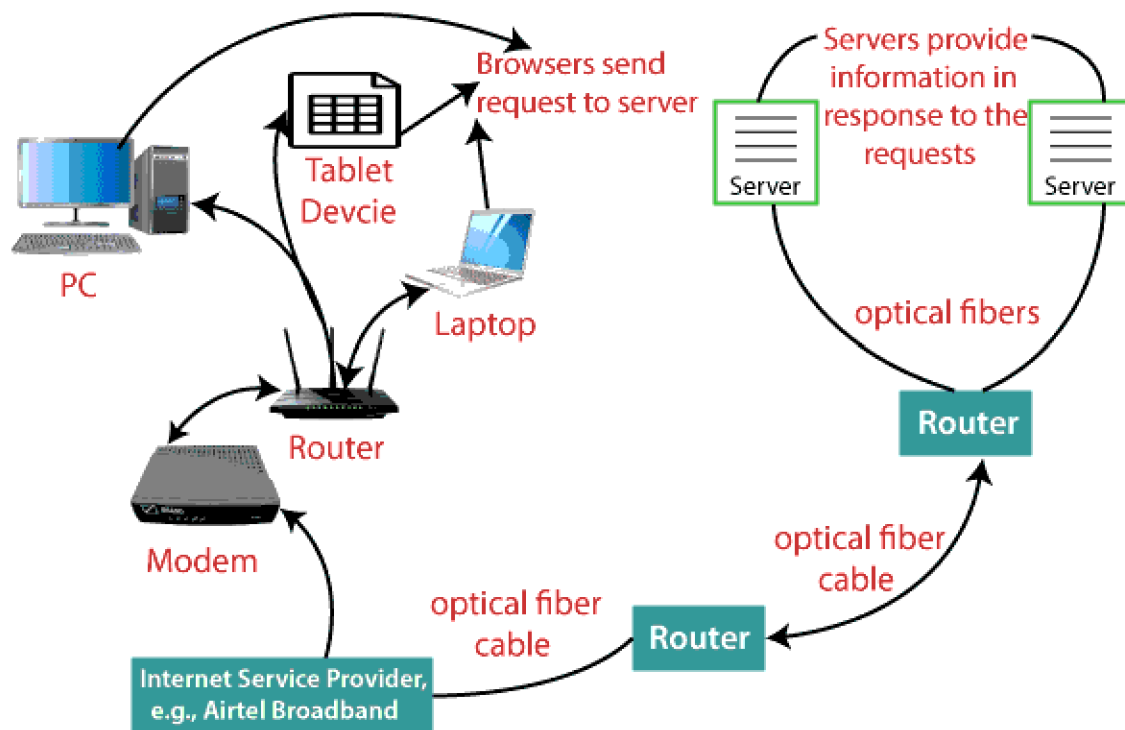
2.1 Concept of Internet and Intranet

2.1.1 Working of Internet & its Architecture

Internet is a global network that connects billions of computers across the world with each other and to the World Wide Web. It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies.

It is believed that the internet was developed by "Defense Advanced Research Projects Agency" (DARPA) department of the United States. And, it was first connected in 1969.

How does internet work?



When you turn on your computer and type a domain name in the browser search bar, your browser sends a request to the DNS server to get the corresponding IP address. After getting the IP address, the browser forwards the request to the respective server.

Once the server gets the request to provide information about a particular website, the data starts flowing. The data is transferred through the optical fiber cables in digital format or in the form of light pulses

The optical fiber is connected to a router, which converts the light signals into electrical signals. These electrical signals are transmitted to your laptop using an Ethernet cable. Thus, you receive the desired information through the internet, which is actually a cable that connects you with the server.

Furthermore, if you are using wireless internet using wifi or mobile data, the signals from the optical cable are first sent to a cell tower and from where it reaches to your cell phone in the form of electromagnetic waves.

Basics of Internet Architecture

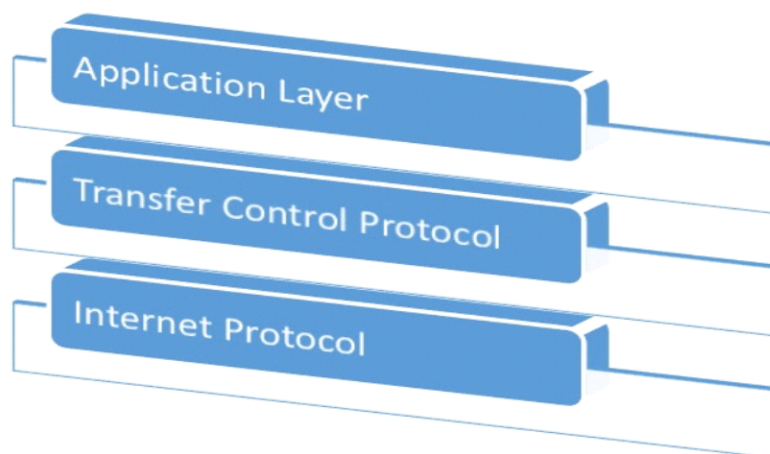
Internet architecture is referred as an internet work that is connected using protocols. Protocol used is TCP/IP. This protocol connects any two networks that differ in hardware, software and design.

Process

TCP/IP provides end to end transmission, i.e., each and every node on one network has the ability to communicate with any other node on the network.

Layers of Internet Architecture

Internet architecture consists of three layers –



The three layers of internet

IP

In order to communicate, we need our data to be encapsulated as Internet Protocol (IP) packets. These IP packets travel across number of hosts in a network through routing to reach the destination. However IP does not support error detection and error recovery, and is incapable of detecting loss of packets.

TCP

TCP stands for "Transmission Control Protocol". It provides end to end transmission of data, i.e., from source to destination. It is a very complex protocol as it supports recovery of lost packets.

Application Protocol

Third layer in internet architecture is the application layer which has different protocols on which the internet services are built. Some of the examples of internet services include email (SMTP facilitates email feature), file transfer (FTP facilitates file transfer feature), etc.

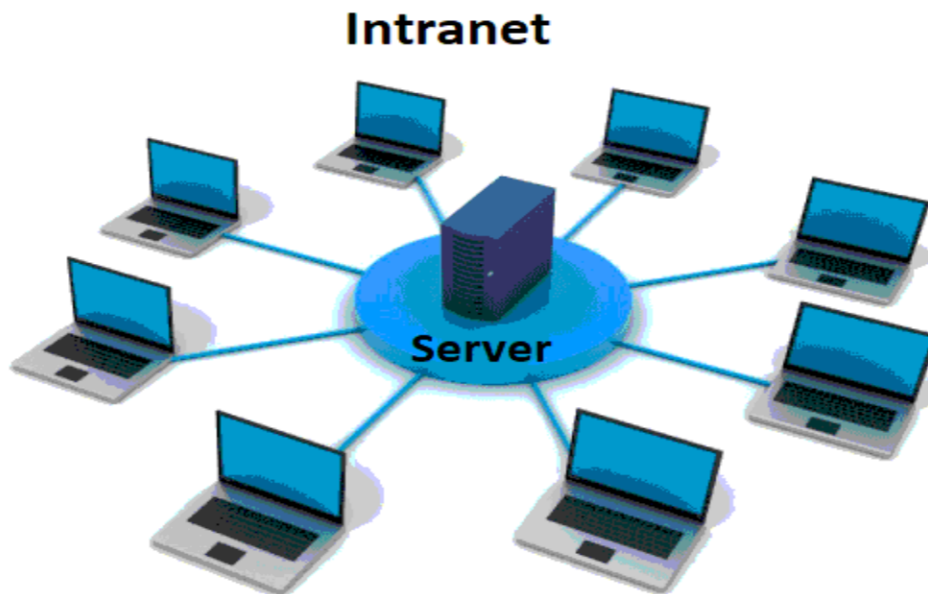
Advantages of the Internet:

- **Instant Messaging:** You can send messages or communicate to anyone using internet, such as email, voice chat, video conferencing, etc.
- **Get directions:** Using GPS technology, you can get directions to almost every place in a city, country, etc. You can find restaurants, malls, or any other service near your location.
- **Online Shopping:** It allows you to shop online such as you can be clothes, shoes, book movie tickets, railway tickets, flight tickets, and more.
- **Pay Bills:** You can pay your bills online, such as electricity bills, gas bills, college fees, etc.
- **Online Banking:** It allows you to use internet banking in which you can check your balance, receive or transfer money, get a statement, request cheque - book, etc.
- **Online Selling:** You can sell your products or services online. It helps you reach more customers and thus increases your sales and profit.
- **Work from Home:** In case you need to work from home, you can do it using a system with internet access. Today, many companies allow their employees to work from home.
- **Entertainment:** You can listen to online music, watch videos or movies, play online games.

- **Cloud computing:** It enables you to connect your computers and internet-enabled devices to cloud services such as cloud storage, cloud computing, etc.
- **Career building:** You can search for jobs online on different job portals and send you CV through email if required.

2.1.2 Working of Intranet & its Architecture

How the Intranet Works:

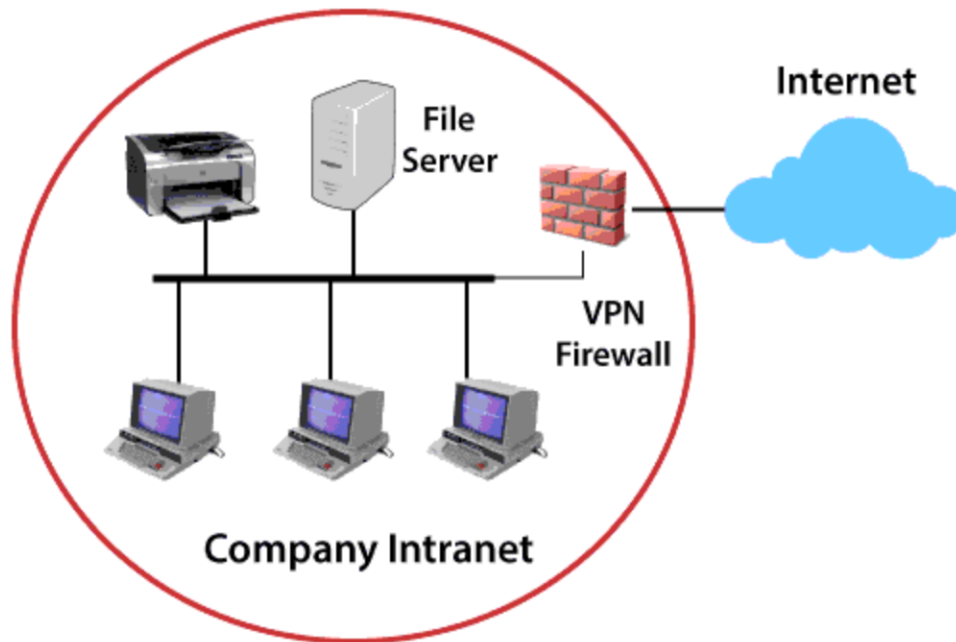


The intranet is a private network that belongs to a particular organization. It is designed for the exclusive use of an organization and its associates, such as employees, customers, and other authorized people. It offers a secure platform to convey information and share data with authorized users. Confidential information, database, links, forms, and applications can be made available to the staff through the intranet.

It is based on internet protocols (TCP/IP) and is protected from unauthorized access with firewalls and other security systems. The firewall monitors the incoming and outgoing data packets to ensure they don't contain unauthorized requests. So, users on the intranet can access the internet, but the internet users can't access the intranet if they are not authorized for it. Furthermore, to access the intranet, the authorized user is required to be connected to its LAN (Local Area Network).

Architecture of Intranet

Intranet basically comprises three components: a web server, an intranet platform, and applications. The web server is hardware that contains all the intranet software and data. It manages all requests for files hosted over the server and finds the requested files and then delivers it to the user's computer.



The intranet platform, which is software, allows communication tools, collaboration apps, and databases to work with each other.

The applications are required to enable users to work smoothly. They are the computing tools that allow users to do their work, communicate, and coordinate with each other and retrieve and store information.

Furthermore, the user who wants to access the intranet is required to have a special network password and should be connected to the LAN. A user who is working remotely can gain access to the intranet through a virtual private network (VPN) that allows them to sign in to the intranet to access the information.

Some of the benefits of the intranet are:

- It is cheap and easy to implement and run, and is more safe than the internet and extranet.
- It streamlines communication that enables the company to share its data, information, and other resources among employees without any delay.
- It provides a secure space to store and develop applications to support business operations.

- It improves the efficiency of the company by speeding up workflow and reducing errors. Thus, it helps achieve targets by completing the tasks on time.
- It offers a testing platform for new ideas before they are uploaded on the company's internet webpage. Thus, it helps maintain the credibility of the company.
- Information is shared in real-time, or updates are reflected immediately to all the authorized users.

Difference between Intranet and Internet:

Internet	Intranet
It is a medium such as optical fiber cable that connects billions of computers with each other to establish a worldwide network.	It is a small, private network as it belongs to a specific organization.
It has billions of users as it is a public network with a worldwide presence.	It has limited users.
It is not as safe as an intranet.	It is a safer network than the internet.
It can be accessed or used by anyone using an internet-enabled device, such as laptop, mobile phone, etc.	Only authorized persons can use this network.
It offers a wide range of information, such as news, blogs, websites, etc.	It offers limited information related to its organization's work, policies, updates, etc.
It is not owned by a single person or an organization.	It can be owned by a person or an organization.

2.1.3 Network Devices:

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.

Types of network devices:

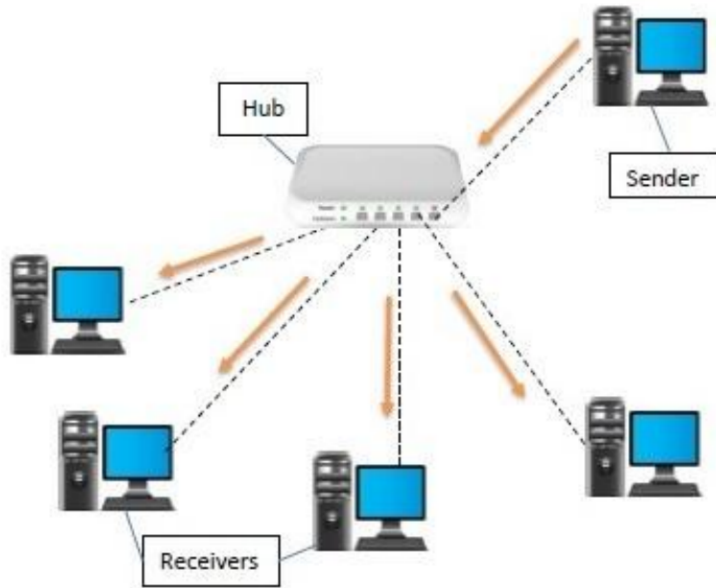
- Hub
- Modem
- Switch
- Router
- Gateway
- Access Point

1. Hub:

A network hub is a central connection point for multiple devices in a LAN. It operates at the physical layer of the OSI model, which is responsible for transmitting data across a network.

A network hub works by receiving data packets from one device and transmitting them to all the other devices connected to the hub. This is known as broadcasting. When a device on the network wants to communicate with another device, it sends a data packet to the network hub. The hub then sends this packet to all the other devices connected to the network. This is called broadcasting. Each device checks the packet to see if it is meant for them. If it is not, they ignore it, and if it is, they accept and process the data.

A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.



Features of Hubs

- A hub operates in the physical layer of the OSI model.
- A hub cannot filter data.
- It primarily broadcasts messages.
- Transmission mode is half duplex.
- They are passive devices; they don't have any software associated with it.

Types of Hubs

There are three types of Hubs:

- Active Hub
- Passive Hub
- Intelligent Hub

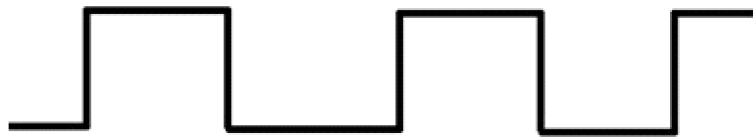
Active Hub: An active hub amplifies and regenerates the signals that pass through it, allowing signals to be transmitted over greater distances. Active hubs are typically used in larger networks with more devices and longer cable runs.

Passive Hub: A passive hub simply extends the network by connecting multiple devices together. It does not amplify or regenerate the signals that pass through it. Passive hubs are typically used in small networks with few devices.

Intelligent Hub: Intelligent hubs are active hubs that provide additional network management facilities.

2. Modem:

Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.



Digital Data Waveform



Analog Data Waveform

The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices – **modulator** and **demodulator**. The **modulator** converts digital data into analog data when the data is being sent by the computer. The **demodulator** converts analog data signals into digital data when it is being received by the computer.

Types of Modem

Modem can be categorized in several ways like direction in which it can transmit data, type of connection to the transmission line, transmission mode, etc.

Depending on direction of data transmission, modem can be of these types –

- **Simplex** – A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digital device (demodulator).
- **Half duplex** – A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.
- **Full duplex** – A full duplex modem can transmit data in both the directions simultaneously.

3. Switch:

Switch is a network device that connects other devices to Ethernet networks through twisted pair cables. It uses packet switching technique to receive, store and forward data packets on the network. The switch maintains a list of network addresses of all the devices connected to it.

On receiving a packet, it checks the destination address and transmits the packet to the correct port. Before forwarding, the packets are checked for collision and other network errors. The data is transmitted in full duplex mode.

Data transmission speed in switches can be double that of other network devices like hubs used for networking. This is because switch shares its maximum speed with all the devices connected to it. This helps in maintaining network speed even during high traffic. In fact, higher data speeds are achieved on networks through use of multiple switches.



4. Router:

A **router** is a **network layer** hardware device that transmits data from one LAN to another if both networks support the same set of protocols. So a **router** is typically connected to at least two LANs and the **internet service provider** (ISP). It receives its data in the form of **packets**, which are **data frames** with their **destination address** added. Router also strengthens the signals before transmitting them. That is why it is also called **repeater**.

Routing Table

A router reads its routing table to decide the best available route the packet can take to reach its destination quickly and accurately. The routing table may be of these two types –

- **Static** – In a static routing table the routes are fed manually. So it is suitable only for very small networks that have maximum two to three routers.
- **Dynamic** – In a dynamic routing table, the router communicates with other routers through protocols to determine which routes are free. This is suited for larger networks where manual feeding may not be feasible due to large number of routers.

5. Gateway:

Gateway is a network device used to connect two or more dissimilar networks. In networking parlance, networks that use different protocols are **dissimilar networks**. A gateway usually is a computer with multiple **NICs** connected to different networks. A gateway can also be configured completely using software. As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network.

Gateway uses **packet switching** technique to transmit data from one network to another. In this way it is similar to a **router**, the only difference being router can transmit data only over networks that use same protocols.

6. Access Point:

An AP operates on the second OSI layer, the data link layer, and can either act as a bridge that connects a standard wireless network to wireless devices or as a router that transmits data to another access point. Wireless connectivity points (WAPs) are a device that is used to generate a wireless LAN (WLAN) transmitter and receiver. Access points are usually networked separate machines with an integrated antenna, transmitter, and adapter.

In order to provide a link between WLAN and wired Ethernet LAN, APs are using wireless infrastructure network mode. They have several ports, which allow you to extend the network to support other customers. One or more APs may need to have full coverage, depending on the size of the network.

2.2 Types of Cables

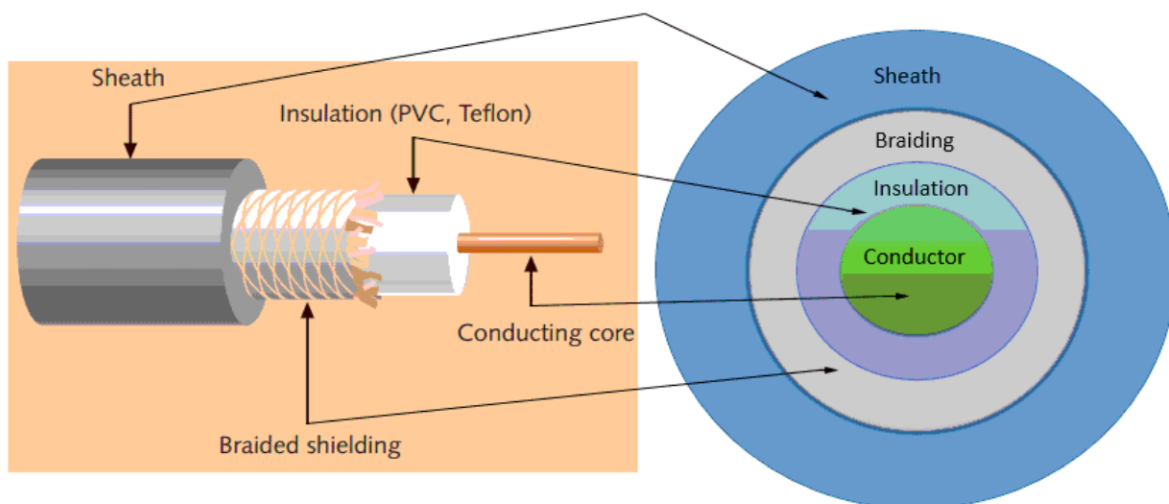
To connect two or more computers or networking devices in a network, network cables are used. There are three types of network cables:

- Coaxial
- Twisted-pair
- 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.

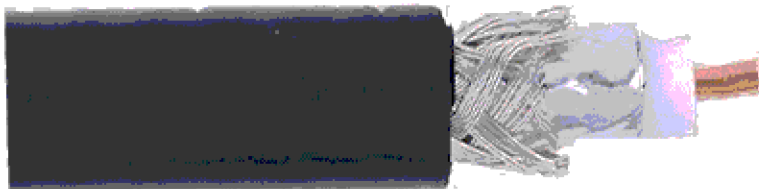
Insulation

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.



Single core coaxial cable



Multi-core coaxial cable

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.

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.

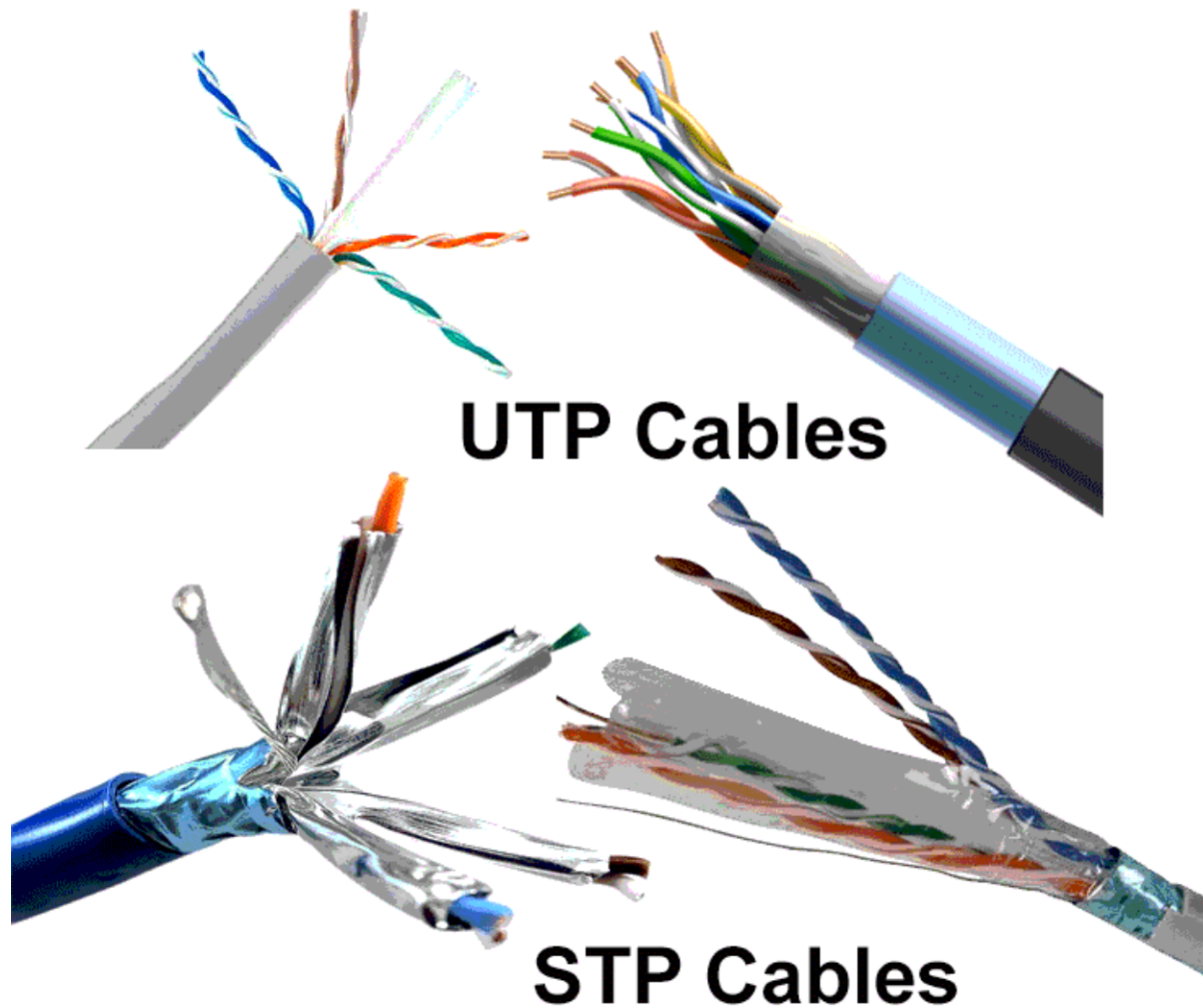
In the **UTP (*Unshielded twisted-pair*) cable**, all pairs are wrapped in a single plastic sheath.

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 maximum segment length for both cables is 100 meters or 328 feet.

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

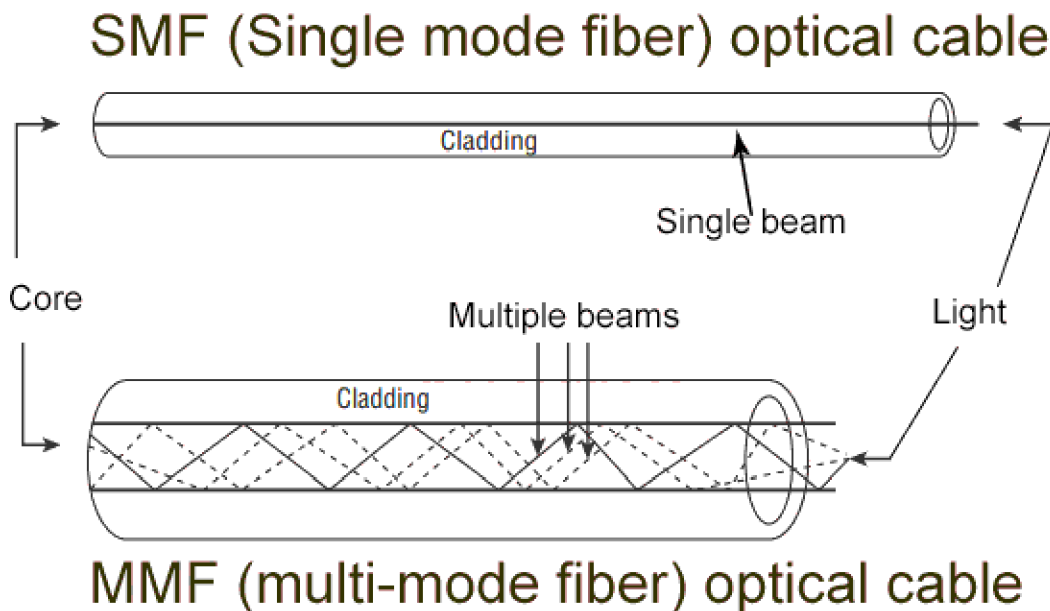
**Fiber optic cable:**

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 Electromagnetic Interference (EMI) and Radio Frequency Interference (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 (**Single-mode fiber**) and MMF (**multi-mode fiber**).



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.