502: NETWORK TECHNOLOGY

[As Per VNSGU Syllabus]

Year: 2025-26

UNIT:2
Internet & Intranet

Index

***

2.1 Concepts of Internet and Intranet:

- **What is the Internet?**

The Internet is a **worldwide network** that connects millions of computers and devices. It is often called the "**network of networks**" because it links different networks together.

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.** It allows users to:

- Communicate across the globe
- Share data and information
- Access websites, services, and online platforms

- **Main Uses of the Internet:**
  - Web browsing (Google, Wikipedia, etc.)
  - Email communication (Gmail, Outlook)
  - Social networking (Facebook, Instagram)
  - Video streaming (YouTube, Netflix)
  - Online shopping (Amazon, Flipkart)
  - E-learning and online courses
  - Online banking and transactions
- **Advantages of the Internet:**
  - Global connectivity
  - Quick access to vast information
  - Instant communication (emails, chat, video calls)
  - Supports online education and remote work
  - E-commerce and digital payments
- **Disadvantages of the Internet:**
  - Cybersecurity threats (viruses, hacking)
  - Privacy issues
  - Can lead to time wastage or addiction
  - Misinformation or fake news

- **What is an Intranet?**

The Intranet is a **private network** used only within an organization, like a company, school, or government office. It works similarly to the Internet but is accessible only to authorized users.

It is used for internal communication, sharing documents, managing tasks, and storing employee-related information.

- **Main Uses of the Intranet:**
  - Internal communication among employees
  - Sharing documents and files
  - HR services (leave forms, salary slips)
  - Employee announcements
  - Training materials and internal tools

- **Advantages of the Intranet:**
  - Improves communication inside the organization
  - Secured and controlled access
  - Increases productivity by centralizing information
  - Reduces paper usage
  - Easy sharing of company updates
- **Disadvantages of the Intranet:**
  - Limited to internal use only
  - Can be expensive to set up and maintain
  - Needs regular updates and monitoring
  - Access is restricted to organization members only

2.1.1 Working of Internet and its architecture:

The working of the Internet is based on **data communication, networking protocols, and layered architecture.** Internet 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.

- **How the Internet Works?**
  - **User Sends a Request**

    When you open a browser and type a website address (like www.google.com), your device sends a **request** to access that website.

  - **DNS Converts Website Name to IP Address**

    Computers don't understand names — they use numbers called **IP addresses**. A system called **DNS (Domain Name System)** converts the website name to its corresponding IP address (e.g., 142.250.196.78 for google.com).

  - **Request Travels Through Your ISP**

    The request goes from your device to your **router**, then to your **Internet Service Provider (ISP)**, and then across the network to the destination server.

  - **Data Travels Through Routers**

    The data travels in small units called **packets**. These packets pass through many **routers**, which guide them toward the correct server.

  - **Server Receives the Request**

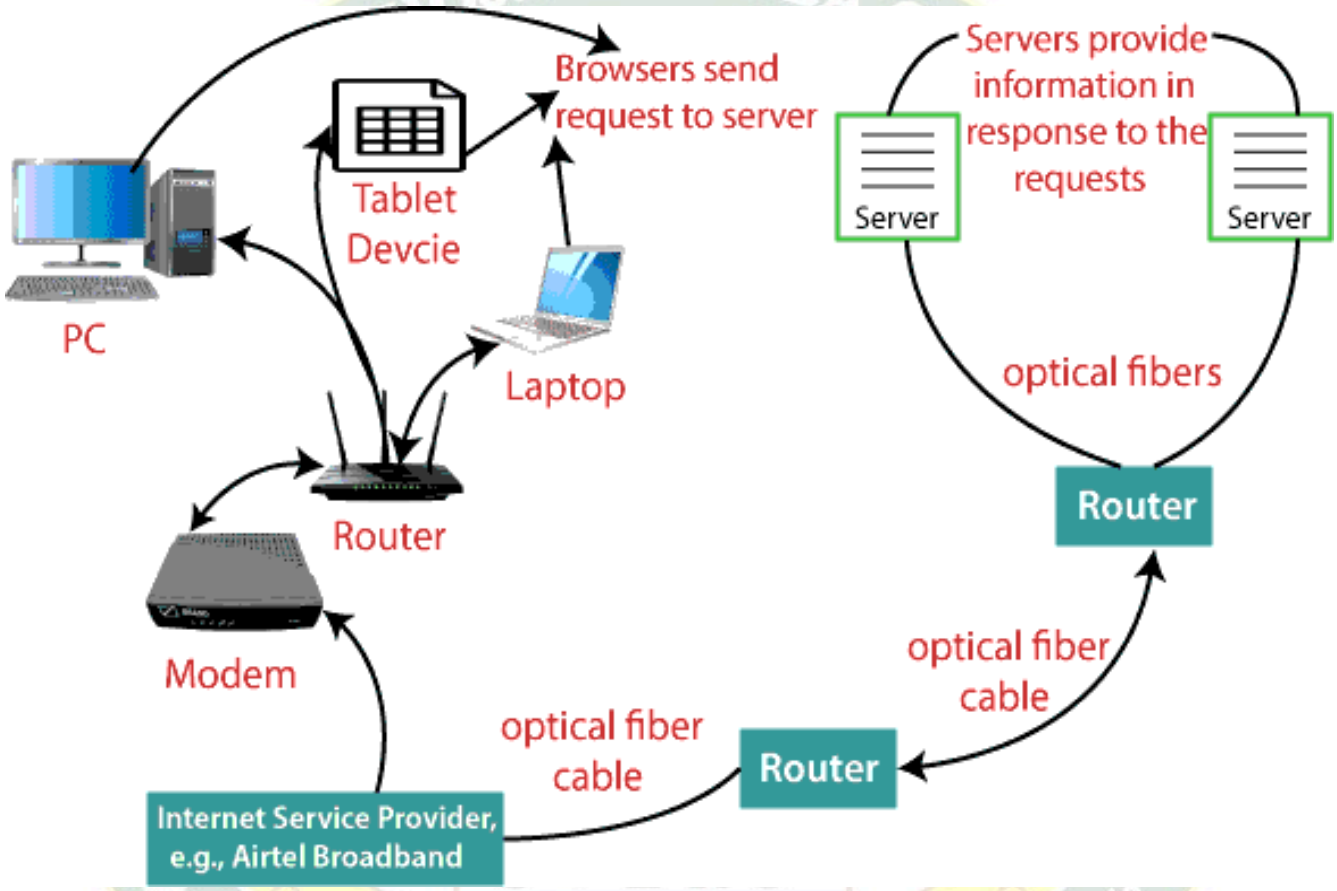
    The destination **web server** receives your request, finds the requested data (like a web page), and sends it back.

- **Packets Return to You**

  The server breaks the data into packets and sends them back through the Internet, again passing through routers and networks.

- **Your Device Reassembles the Packets**

  Your device collects and reassembles all packets into a complete web page or file, which you see on your screen.



- **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:

I. 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.**

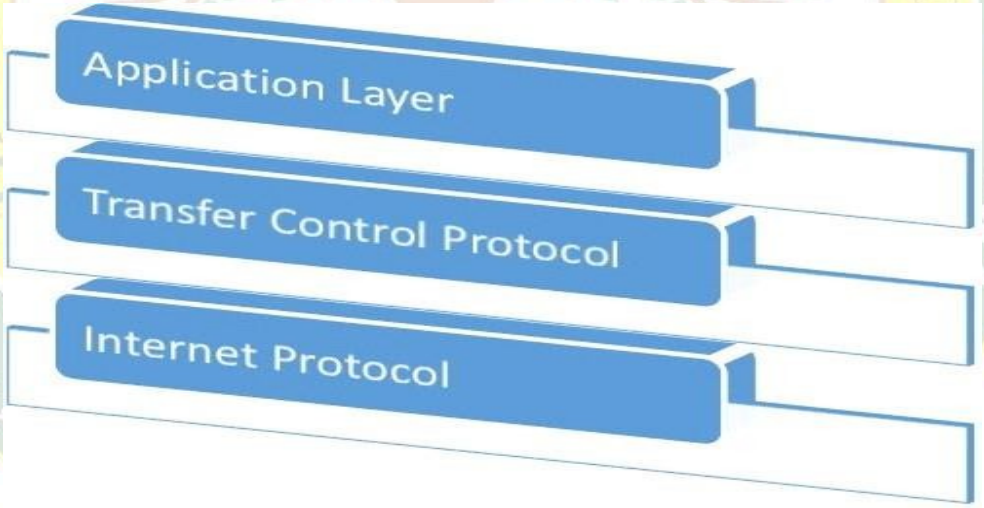
II. TCP

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.**

III. 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.

SMTP: Simple Mail Transfer Protocol
FTP: File Transfer Protocol



The three layers of internet

- **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:*

- **Private Network Setup:**

  The organization sets up a local network using servers, routers, and computers. This network is not connected to the public internet, or it's protected by firewalls to prevent outside access.

- **Central Server:**

  All intranet content (like files, web pages, apps, announcements) is stored on a central server. Employees access this server using their web browser, similar to how we open websites on the internet.

- **Login & Authentication:**

  Users need a username and password to access the intranet. Only authorized users (staff or members) can log in.

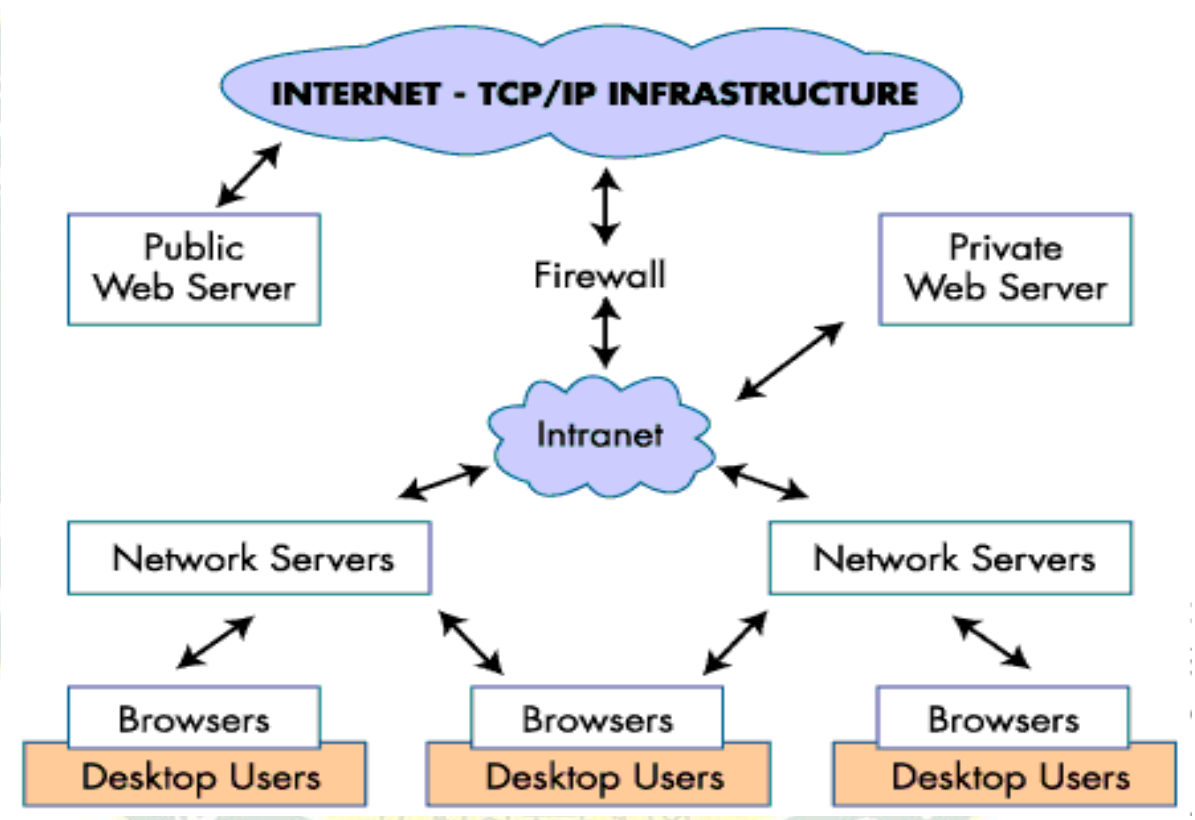
- **Content Access:**

  Users can:

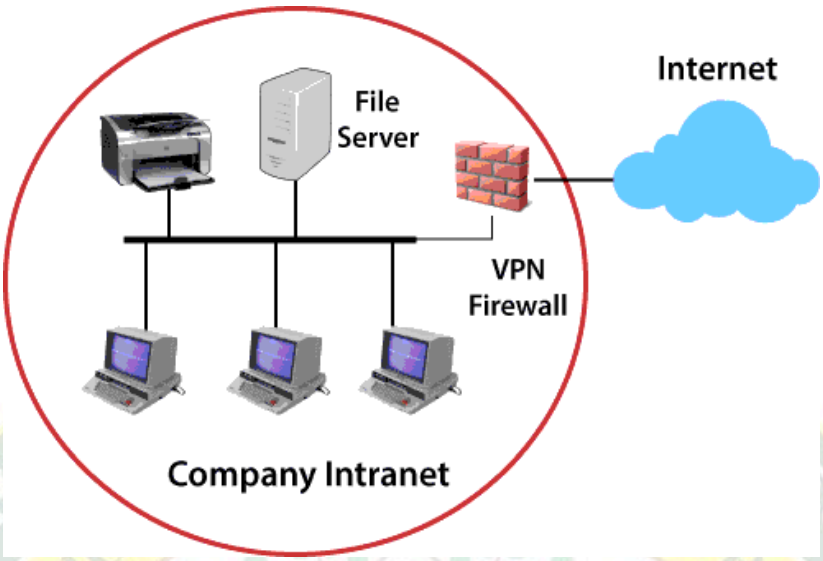
  - Share documents
  - Read company news
  - Fill forms (like leave applications)
  - Use internal apps (HR, Payroll, Inventory, etc.)

- **Communication Tools:**
  Intranet may include tools like:
  - Internal messaging/chat
  - Video calls
  - Email systems

- **Firewall & Security:**
  A firewall blocks unauthorized external access. Antivirus and encryption keep data safe.



- **Basics of Intranet Architecture:**



Intranet basically comprises three components:

- a web server,
- an intranet platform,
- applications.

➢ **Web Server (Hardware Component):**

- The **web server** is a physical machine (hardware) that hosts all intranet-related data and software.
- It handles **all user requests** for files, applications, or services hosted on the intranet.
- When a user requests a file or a page, the web server:
  - **Finds the file**
  - **Retrieves it**
  - **Sends it** back to the user's device via the network.
- It ensures smooth **data delivery** within the internal network.

➢ **Intranet Platform (Software Component)**

- The intranet platform is the main software framework running on the server.
- It enables integration and coordination of:
  - Communication tools (like chat or email)
  - Collaboration applications (like file sharing, project tracking)
  - Databases (like employee directories or document repositories)
- It provides a user-friendly interface for employees to access resources.
- Supports navigation, search, access control, and content management.

➢ **Applications**

- Applications are the software tools that help users perform their day-to-day tasks.
- These include:
  - Document editors
  - Email and messaging tools
  - Scheduling and calendar apps
  - HR and payroll systems
- Applications:
  - Allow users to **create, edit, and manage content**
  - Facilitate **communication and collaboration**
  - Help in **data retrieval, storage, and processing**
- To access the intranet, a user must be connected to the organization's **Local Area Network (LAN)** and possess a valid network password. Remote users can securely access the intranet by connecting through a **Virtual Private Network (VPN),** which enables them to sign in and retrieve the necessary information from outside the office.

- **Some of the benefits of the intranet are:**
  - The intranet is **cost-effective** and easy to set up and maintain. It also offers better **security** compared to the internet and extranet.
  - It helps improve **communication within the company** by allowing **fast and easy sharing** of data, information, and resources among employees.
  - It provides a secure environment to store and develop applications that support the company's daily operations.
  - By speeding up workflows and reducing errors, the intranet **boosts the company's efficiency,** helping teams complete tasks on time and meet their goals.
  - It can be used as a testing platform for new ideas before making them public on the company's official website. This helps in protecting the company's credibility and image.
  - Information is **updated instantly** and is **immediately visible** to all authorized users in real-time.

- **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 assessed or used by anyone using an internet-enable devices, 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.

- **What Is Extranet?**

An Extranet is a controlled private network that uses internet technologies to securely share part of a business's internal information or operations with people **outside the organization**, such as:

  - Customers
  - Suppliers
  - Vendors
  - Business partners
  - Stakeholders

It extends the functionalities of an **intranet** to trusted third parties **outside the company**, allowing collaboration and information sharing **without giving full access to the internal network.**

- **Main Components of an Extranet:**

1. **User Authentication System**
   - Ensures only approved users can access the network using usernames and passwords.
2. **Firewalls and Security Tools**
   - Protects sensitive internal data from unauthorized access.

3. **Web-based Interface**
   - Allows access through a web browser, making it easy to use from anywhere.
4. **Document Management and Sharing Tools**
   - Used for sharing files, reports, forms, and other information.
5. **Communication Tools**
   - Chat, video conferencing, emails, and forums to connect with external users.

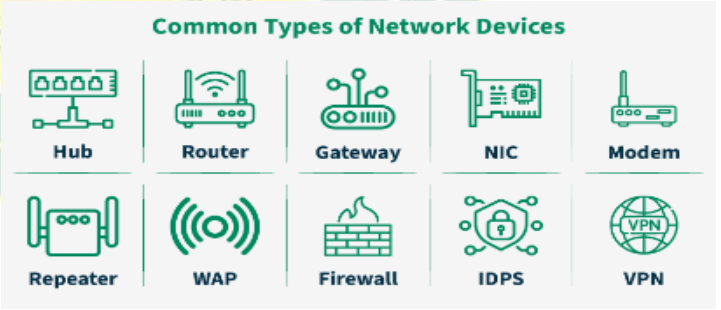
- **How It's Used in Business:**
  - A retail company can allow suppliers to check inventory levels and place restocking orders.
  - A construction firm can let contractors and engineers upload reports or access blueprints.
  - A university can give online learning partners access to student progress and materials.

- **Benefits of Extranet:**
  - Enhances **collaboration between the business and its partners.**
  - Reduces **communication delays** by offering real-time updates.
  - Improves **efficiency in supply chains and project management.**
  - Offers a **secure** and **organized** way to share confidential documents.

2.1.3 Network Devices:

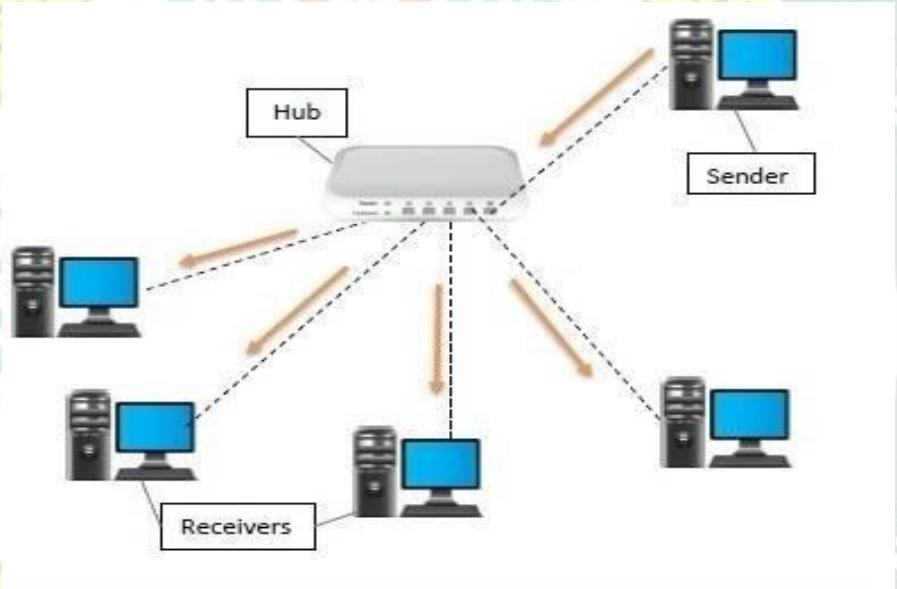
Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.

- **Types of network devices:**
  - Hub
  - Modem
  - Switch
  - Router
  - Gateway
  - Access Point



- **HUB:**
  - A hub is a device used to connect many computers in a network (like at home or in a small office).
  - It works at the physical layer (Layer 1) of the OSI model.

- When one computer sends data to the hub, the hub sends (broadcasts) that data to all the other computers.
- Each computer checks if the data is meant for it:
  - If yes, it accepts the data.
  - If not, it ignores the data.
- A hub has many ports (like plug points), where each computer is connected.
- When data comes to one port, the hub sends it to all other ports, even if only one computer needs it.
- This creates extra traffic in the network, because all devices receive all the data.
- A hub does not check where the data should go—it just passes it to everyone.



- **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:**
  - Has its own power supply.
  - Can boost (amplify) the signal before sending it to other devices.
  - Works like a repeater to extend the distance of the network.
  - Used in larger networks where signal strength needs to be maintained.
- **Passive Hub:**
  - Does not have its own power supply.
  - Just passes the data from one device to others without boosting the signal.
  - Used in small networks where boosting is not required.
- **Intelligent Hub (Smart Hub):**
  - Has monitoring and management features.
  - Can check network traffic, errors, and sometimes filter data.
  - More expensive than active and passive hubs.
  - Used in larger or managed networks where control is important.

- **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.**

- **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.

- **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.

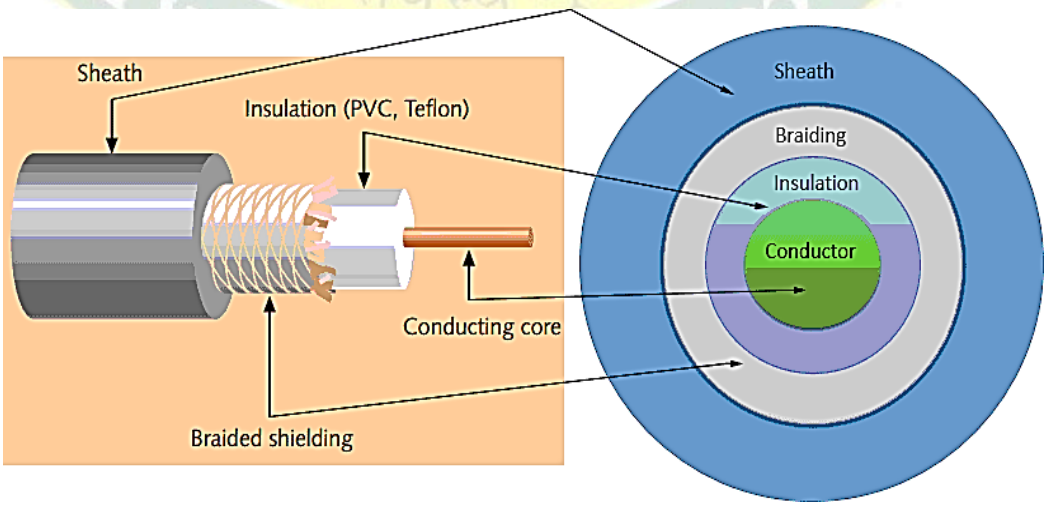
- **Gateway:**
  - **Gateway** is a network device used to connect two or more dissimilar networks.
  - In networking phraseology, networks that use different protocols are **dissimilar networks**.
  - A gateway usually is a computer with multiple **NICs** connected to different networks.
  - A gateway 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.

- **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 Application 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.

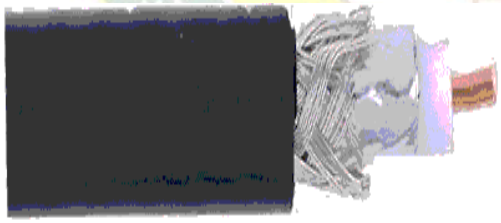
2.2 Types of Cables:

- 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:**
  - A **coaxial cable** (also called **coax cable**) is a type of electrical cable used to transmit high-frequency signals.
  - It is widely used in television systems, internet connections, and other communication applications.
  - 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 layer is made of **metal** (usually the same as the core) and helps block external interference and electrical noise, ensuring a cleaner signal.
  - 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.



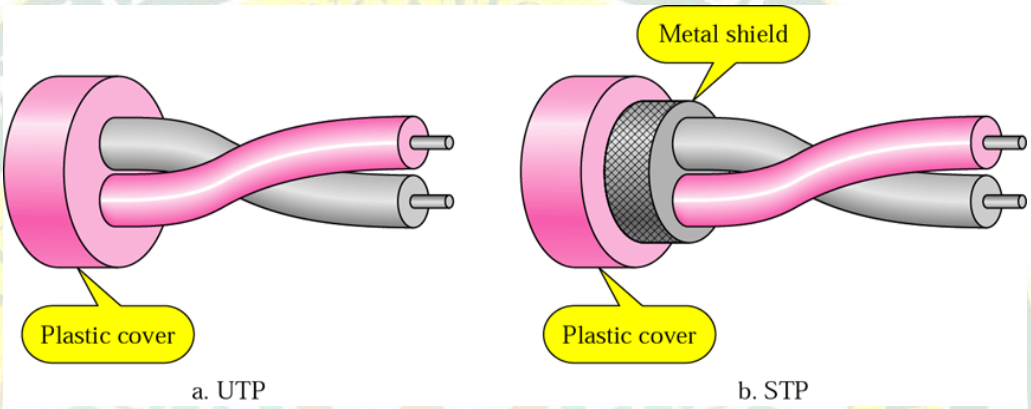
Single core coaxial cable

Multi-core coaxial cable

- Coaxial cables were originally developed for general-purpose use, not specifically for computer networks.
- They were in use even before the concept of computer networking existed.
- In the early days of computer networking, there were no dedicated media cables available.
- As a solution, network administrators began using coaxial cables to build computer networks.
- Coaxial cables became popular due to their low cost and long durability.
- They were widely used in computer networking during the 1980s and 1990s.
- Today, coaxial cables are no longer used to build any type of computer network.

- **Twisted Pair:**
  - Twisted-pair cable was primarily developed for computer networks.
  - It is commonly known as an **Ethernet cable.**
  - Almost all modern **LAN (Local Area Network)** computer networks **use twisted-pair cables.**
  - The cable consists of **color-coded pairs of insulated copper wires**.
  - Each pair is formed by **twisting two wires around each other** to reduce interference.
  - Typically, there are **four pairs** of wires in one cable.
  - Each pair includes one solid color wire and one striped wire (with white mixed with a solid color).
  - The solid colors used are blue, brown, green, and orange.
  - Based on shielding, twisted-pair cables are **classified into two types**:
    - **UTP (Unshielded Twisted-Pair):** All pairs are wrapped together in a **single plastic sheath** without any additional shielding.
    - **STP (Shielded Twisted-Pair):** Each pair is individually wrapped in a metal shield before being enclosed in an outer plastic sheath.

- **Similarities and Differences between STP and UTP cables:**
  - Both STP and UTP cables support data transmission speeds of 10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps.
  - STP cables are more expensive than UTP cables due to additional shielding material.
  - Both types use the **RJ-45 (Registered Jack)** modular connectors.
  - Each cable type can support up to **1024 nodes per segment.**
  - The maximum cable length for both is 100 meters (328 feet).
  - The following image shows **both types** of twisted-pair cables.

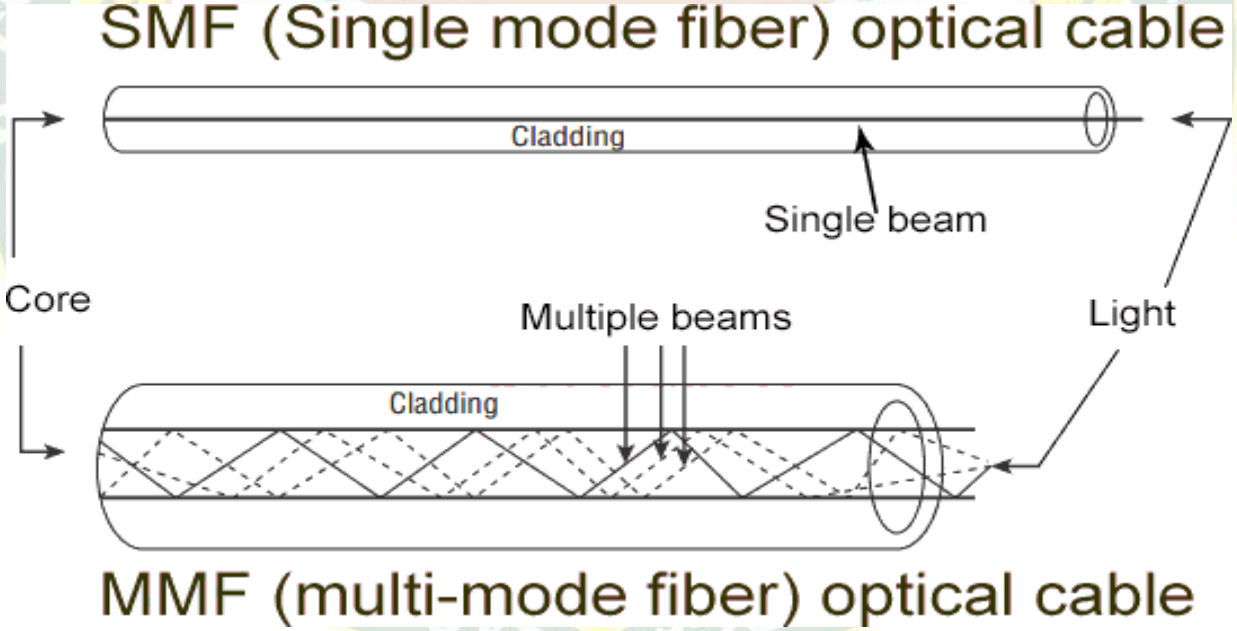


- **Fiber Optic Cable:**
  - A **Fiber Optic Cable** is a type of network cable that uses **light** to send data.
  - It is used for **very fast and long-distance** data communication.
  - It is much **faster and more reliable** than old copper cables.
  - A fiber optic cable has **four** main parts:
    - **Core** – A very thin glass or plastic thread where data travels as light.
    - **Cladding** – A layer around the core that keeps the light inside the core.
    - **Buffer** – Protects the core and cladding from damage or light loss.
    - **Jacket** – The outer cover that protects the cable from physical damage.
  - It is not affected by electrical signals or radio signals (no interference).
  - It can send data up to 40 kilometers at speeds up to 100 Gbps.
  - Based on **how many beams of light** are transmitted at a given time, there are **two** types of fiber optical cable-

- **Single-Mode Fiber (SMF)**
- **Multi-Mode Fiber (MMF):**

- **Single-Mode Fiber (SMF):**
  - Sends **only one light beam at a time.**
  - Best for **long-distance and high-speed data**.
  - Uses a **laser** to send light.
  - Works with **1300 or 1550 nanometer** wavelength light.
  - More **reliable** than multi-mode.

- **Multi-Mode Fiber (MMF):**
  - Sends **many light beams at the same time**.
  - Can carry **more data**, but only for **shorter distances**.
  - Uses an **LED light source**.
  - Works with **850 or 1300 nanometer** wavelength light.
  - Used in buildings or **smaller network setups**.



***

Short Questions

1. Which of the following protocol is considered as unreliable and connection less protocol? **[March 25]**
   (a) UDP (b) TCP (c) IP (d) None of these

2. What is Internet? **[March 25]**
   (a) Combination of LANs (b) Group of unrelated computers
   (c) Group of WANs (d) An Internal Network

3. Which of the protocol is used for Electronic Mail? **[March 25]**
   (a) SMTP (b) HTTP (c) FTP (d) SIP

4. With respect to physical media, STP cables stands for_____ **[Nov 24]**
   (a) Shielded Twisted Pair Cable (b) Spanning Tree Protocol Cable
   (c) Static Transport Protocol Cable (d) Shielded Two Power Cable

5. The slowest transmission speeds are those of **[Nov 24]**
   (a) Coaxial cable (b) Fiber Optic cable
   (c) Twisted Pair wire (d) Microwaves

Long Questions

1. Write a note on architecture of internet. **[March 25]**
2. Explain twisted pair and co-axial cable in detail. **[Nov 24]**
3. Explain HUB and Switch. **[Nov 24]**

***