Unit-2

INTERNET AND INTRANET

Intranet and its Architecture

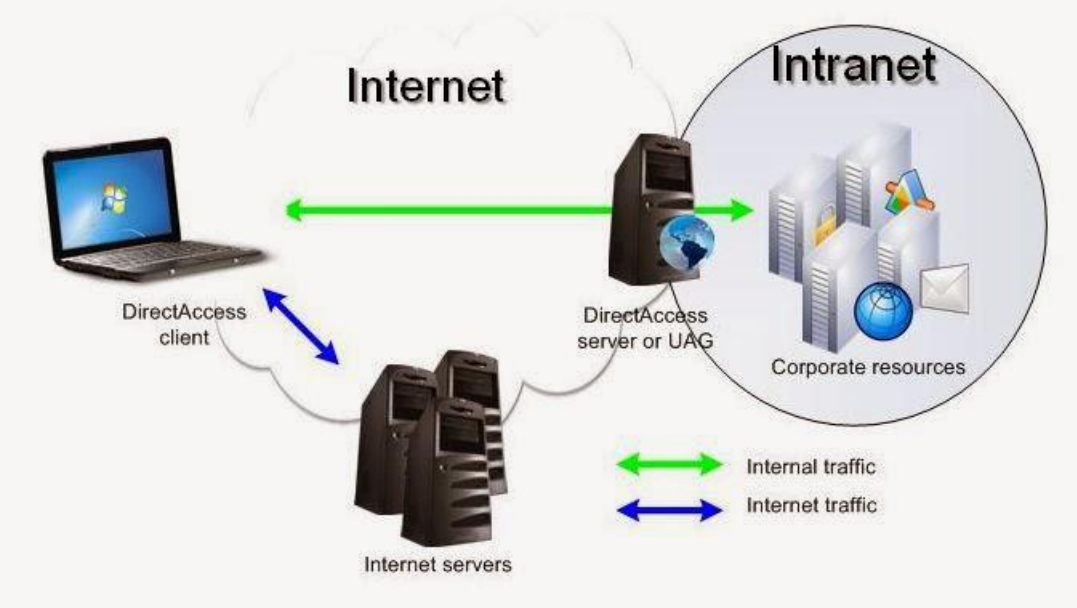
An intranet is a private computer network that is used within an organization to facilitate internal communication, collaboration, and information sharing. It is designed to be accessible only to authorized users within the organization and is not accessible to the public or the internet at large.

Intranets serve as a centralized platform that provides employees or members of an organization with access to various resources and tools. Here are some key features and benefits of intranets:

1. **Communication and Collaboration:** Intranets offer a range of communication tools, such as email, instant messaging, discussion forums, and team collaboration spaces. They enable employees to exchange messages, share ideas, collaborate on projects, and work together regardless of their physical location.
2. **Document and Content Management:** Intranets provide a centralized repository for documents, files, and other types of content. Employees can upload, organize, and share files, making it easier to collaborate on documents and ensure everyone has access to the most up-to-date information.
3. **Company News and Information:** Intranets often feature news sections or portals where organizations can share updates, announcements, and important information with their employees. This helps keep everyone informed about company news, events, policies, and procedures.
4. **Employee Directories and Profiles:** Intranets often include directories or employee profiles that provide information about individuals within the organization. This makes it easier for employees to find and connect with colleagues, fostering collaboration and networking within the organization.
5. **Resource Sharing:** Intranets can provide access to shared resources, such as company-wide calendars, project management tools, HR portals, training materials, and internal databases. This streamlines access to important resources and ensures consistency in processes and workflows.
6. **Enhanced Productivity and Efficiency:** By providing a centralized platform for communication, collaboration, and access to resources, intranets help improve productivity and efficiency within an organization. Employees can find information quickly, communicate seamlessly, and collaborate effectively, leading to streamlined workflows and better outcomes.

7. **Security and Access Control:** Intranets are designed to be secure environments, with restricted access only to authorized users. This ensures that sensitive company information and data remain protected from external threats.

   Intranets can be customized and tailored to meet the specific needs of an organization, including its structure, departments, and workflows. They are widely used in businesses, educational institutions, government agencies, and nonprofit organizations to facilitate internal communication, knowledge sharing, and collaboration among employees or members.

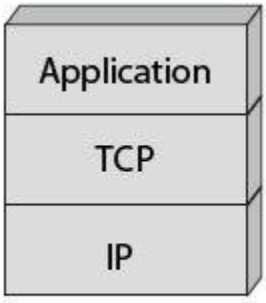


Internet

The internet, short for **"interconnected network,"** is a global network of computers and other devices that are interconnected and communicate with each other using standardized protocols. It is a vast network infrastructure that **connects millions of devices worldwide**, allowing them to **exchange data, information, and services.**

The Internet model completed with a third layer called the application level, which includes different protocols for building Internet services. Email **(SMTP)**, file transfer **(FTP)**, the transfer of hypermedia pages, transfer of distributed databases

(World Wide Web), etc., are some of these services. The figure shows the three layers of Internet architecture.



The Three Layers of the Internet

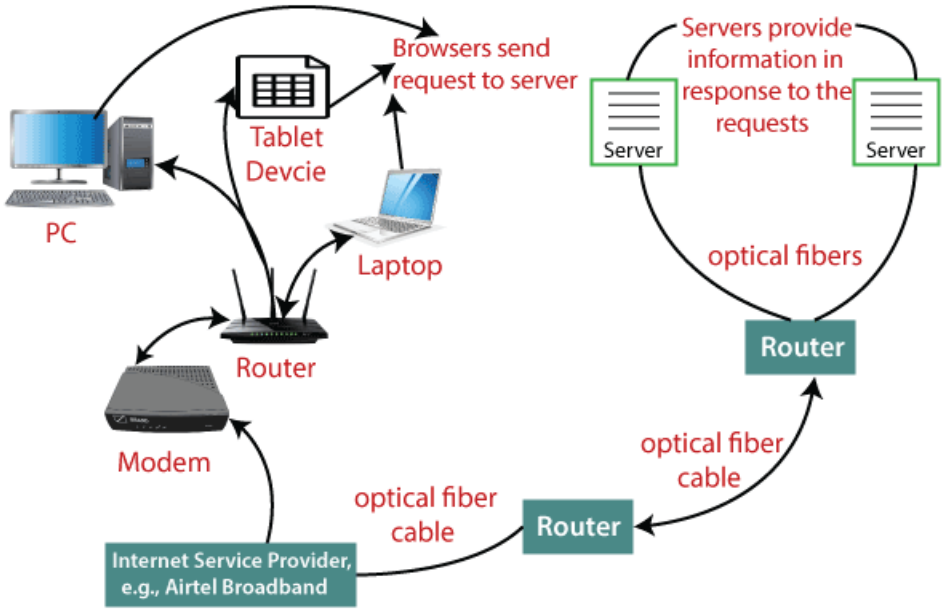
How Internet Works?

The internet works with the help of clients and servers. A device such as a laptop, which is connected to the internet is called a client, not a server as it is not directly connected to the internet. However, it is indirectly connected to the internet through an Internet Service Provider (ISP) and is identified by an IP address, which is a string of numbers. Just like you have an address for your home that uniquely identifies your home, an IP address acts as the shipping address of your device. The IP address is provided by your ISP, and you can see what IP address your ISP has given to your system.

A server is a large computer that stores websites. It also has an IP address. A place where a large number of servers are stored is called a **data center**. The server accepts requests send by the client through a browser over a network (internet) and responds accordingly.

To access the internet we need a domain name, which represents an IP address number, i.e., each IP address has been assigned a domain name. For example, youtube.com, facebook.com, paypal.com are used to represent the IP addresses. Domain names are created as it is difficult for a person to remember a long string of numbers. However, internet does not understand the domain name, it understands the IP address, so when you enter the domain name in the browser search bar, the internet has to get the IP addresses of this domain name from a huge phone book, which is known as DNS (Domain Name Server).

For example, if you have a person's name, you can find his phone number in a phone book by searching his name. The internet uses the DNS server in the same way to find the IP address of the domain name. DNS servers are managed by ISPs or similar organizations.



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. As the servers are placed at distant places, the data may have to travel thousands of miles through optical fiber cable to reach your computer.

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.

The internet is managed by ICANN (Internet Corporation for Assigned Names and Numbers) located in the USA. It manages IP addresses assignment, domain name registration, etc.

Three main categories of **Internet Connection Protocols** are discussed below:

- **TCP/IP Network Model:** The most popular protocols for linking networks are Transmission Control Protocol (TCP) and Internet Protocol (IP). Any communication is split up into a number of packets that are sent from source to destination.
- **File Transfer Protocol:** With the help of FTP (File Transfer Protocol), a user can transfer documents, text files, multimedia files, program files, etc., from one device to another.
- **Hypertext Transfer Protocol:** It is used to move a hypertext between two or more computers or other devices. Links can be made using HTML tags and can take the form of text or graphics.

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 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.

Disadvantages of the Internet

- **Time wastage:** Although, Internet has a lot of advantages, it also contains some limitations. Time wasting is one of among them. It can decrease your productivity if you are spending too much time on the Internet using social media apps while doing nothing. Rather than squandering time, one should use that time to do something useful and even more productive.
- **Bad impacts on health:** You can get health related issues if you spend too much time online; your body needs outside activities, exercise, and many other things. If you look at the screen for a long time, it causes negative effects on the eyes.
- **Cyber Crimes:** These days, crimes including cyber bullying, spam, viruses, hacking, and data theft are increasing day by day. Cybercriminals can quickly break into your system, which store all of your private information.
- **Effects on children:** The constant watching of videos and playing games on the Internet by young children is bad for their social and overall personality development.
- **Bullying and spreading negativity:** Social media applications have provided a free tool to all those people who regularly attempt to spread negativity with really repulsive and humiliating comments and try to bully each other, which is wrong and does bad impact on society.

Network Devices Terminologies

HUB

A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

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.

Types of Hub

- **Active Hub:-** These are the hubs that have their **power supply** and can clean, **boost**, and relay the signal along with the network. It serves both as a **repeater** as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub:-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without

cleaning and boosting them and **can't be used to extend the distance** between nodes.

Features of Hub

- It acts with shared bandwidth and broadcasting.
- It includes only one **collision domain and broadcast domain**.
- It works at the **physical layer of the OSI model** and also offers support for **half-duplex transmission mode**.
- It cannot create a virtual LAN and does not support spanning tree protocol.
- Furthermore, mainly packet collisions occur inside the hub.
- It also has a feature of flexibility, which means it includes a high transmission rate to different devices.

Applications of Hub

The important applications of a hub are given below:

- Hub is used to create small home networks.
- It is used for network monitoring.
- They are also used in organizations to provide connectivity.
- It can be used to create a device that is available through out of the network.

What hubs do?

Hubs work as a central connection between all network equipment and handle a data type, which is called frames. If a frame is received, it is transmitted to the port of the destination computer after amplifying it. A frame is passed to each of its ports in the hub, whether it is destined only for one port. It does not include the way of deciding a frame to which port it should be sent. Therefore, a frame has to transmit to every port, which ensures that it will reach its intended destination that generates a lot of traffic on the network and can be caused to damage the network. The hub is slower as compared to standard switch as it is not able to send or receive information at the same time.

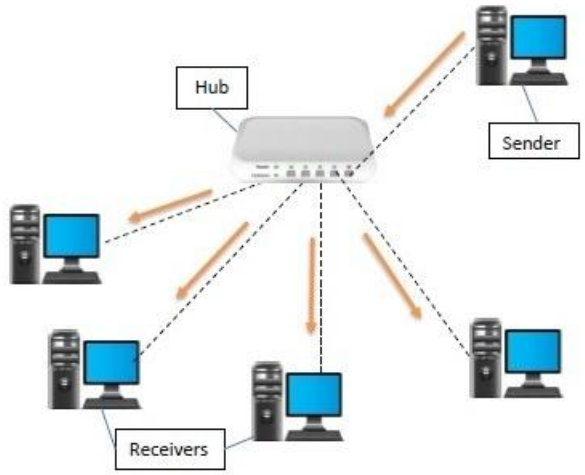
Advantages of Hub

- It provides support for different types of Network Media.
- It can be used by anyone as it is very cheap.

- It can easily connect many different media types.
- The use of a hub does not impact on the network performance.
- Additionally, it can expand the total distance of the network.

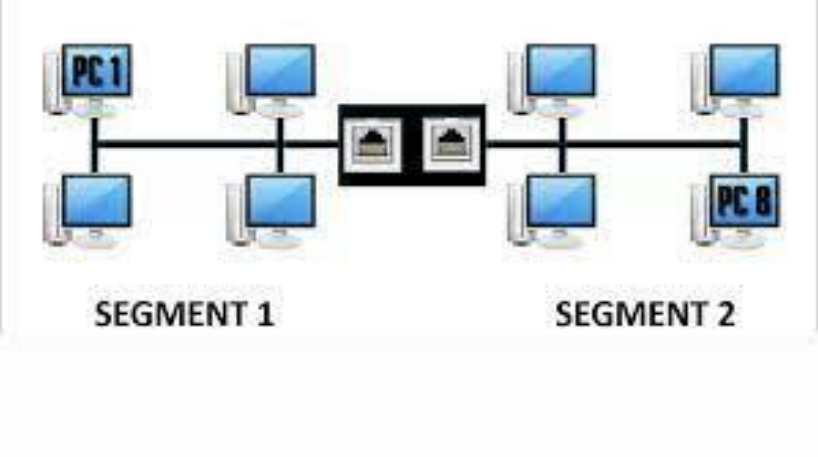
Disadvantages of Hub

- It has no ability to choose the best path of the network.
- It does not include mechanisms such as collision detection.
- It does not operate in full-duplex mode and cannot be divided into the Segment.
- It cannot reduce the network traffic as it has no mechanism.
- It is not able to filter the information as it transmits packets to all the connected segments.
- Furthermore, it is not capable of connecting various network architectures like a ring, token, and Ethernet, and more.



BRIDGE

A bridge operates at the **data link layer**. A bridge is a repeater; with add on the functionality of filtering content by reading the **MAC addresses** of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.



Types of Bridges

- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

Uses of Bridge in Computer Network:

- Bridges are used to increase the network capacity as they can integrate multiple LANs together.
- On receiving a data frame, databases use the bridge to decide whether to accept or reject the data.
- In the OSI model, it can be used to transmit the data to multiple nodes of the network.
- Used to broadcast the data if the MAC address or destination address is unavailable.
- It forwards data packets despite faulty nodes.
- The data packet can be forwarded or discarded by the bridge when the MAC address is available.

Advantages:

- Bridges can be used as a network extension like they can connect two network topologies together.
- It has a separate collision domain, which results in increased bandwidth.
- It can create a buffer when different MAC protocols are there for different segments.
- Highly reliable and maintainable. The network can be divided into multiple LAN segments.
- Simple installation, no requirement of any extra hardware or software except the bridge itself.
- Protocol transparency is higher as compared to other protocols.

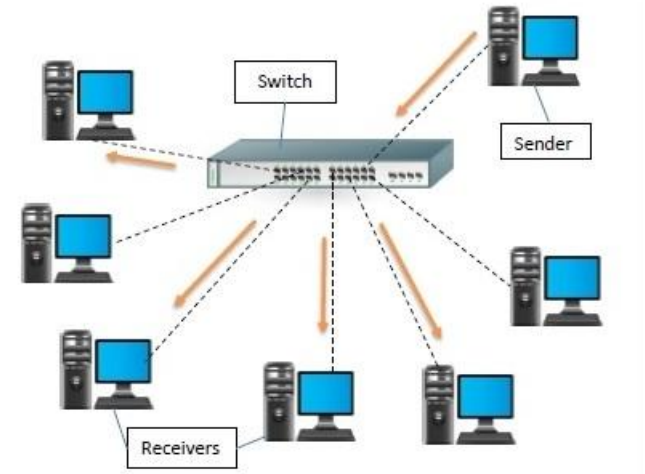
Disadvantages:

- Expensive as compared to hubs and repeaters.
- Slow in speed.
- Poor performance as additional processing is required to view the MAC address of the device on the network.
- As the traffic received is in bulk or is broadcasted traffic, individual filtering of data is not possible.
- During the broadcasting of data, the network has high broadcast traffic and broadcast storms can be formed.

SWITCH

A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.

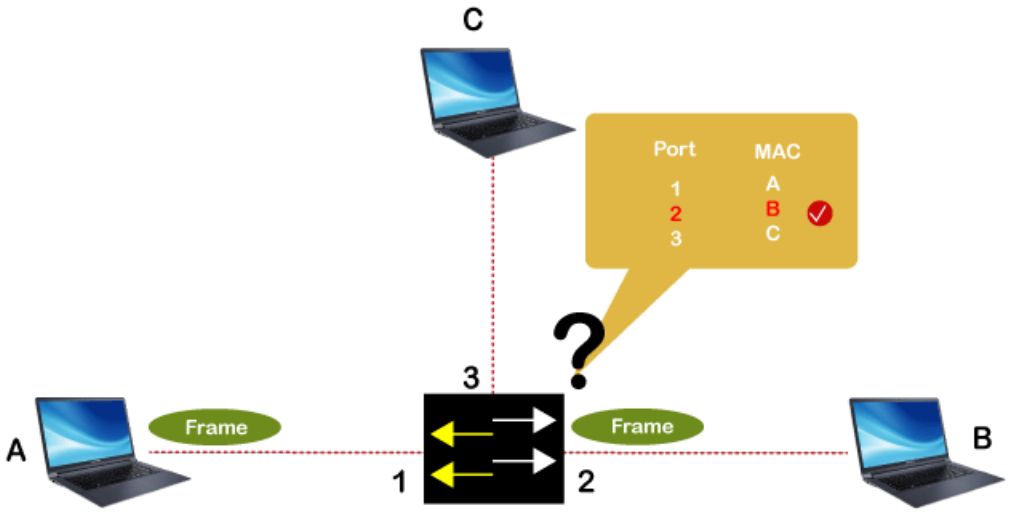
Like a hub, a switch also has many ports, to which computers are plugged in. However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s). Thus, it supports both unicast and multicast communications.



How does a switch work?

As we know, each networking device contains a **unique MAC (Media Access Control) address**. When a device or computer sends an IP packet to another device, then switch put the IP packet with source MAC address and destination MAC address, and encapsulate it with a Frame, and then send it to another device.

When Frame reaches the destination device, it is stripped, and the device gets the IP packets and reaches only that device, which matches the entered destination MAC address.



Types of Switch

There are mainly two types of switches in the network, which are given below:

- **Store and Forward Switch:** The switch buffers and verifies (checks for error) each frame before forwarding it. It's slow but very reliable.
- **Cut Through Switch:** The switch reads only up to the frame Hardware address before starting to forward it, it doesn't do Error Checking.
- **Unmanaged Switches:** The unmanaged switches are mainly used for basic connectivity. These are mostly used in small networks or wherever only few more ports are required, such as at home, in a lab, or in a conference room. In unmanaged switches, there is no requirement for any configuration, which means by just plugging in, they will work.
- **Managed Switches:** Managed switches are more secure than unmanaged switch, and provide other features and flexibility because we can easily configure them to custom-fit our network. Hence, we can have the greater control, and can also better protect our network and improve service quality for those who access the network.
- **Smart Switches**: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
- **Layer 2 Switches:** These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
- **Layer 3 Switches:** These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
- **PoE Switches:** These switches have Power over Ethernet capabilities, which allow them to supply power to network devices over the same cable that carries data.
- **Gigabit Switches:** These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
- **Rack-mounted Switches:** These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
- **Desktop Switches:** These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.

- **Modular Switches:** These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

Advantages of Switch

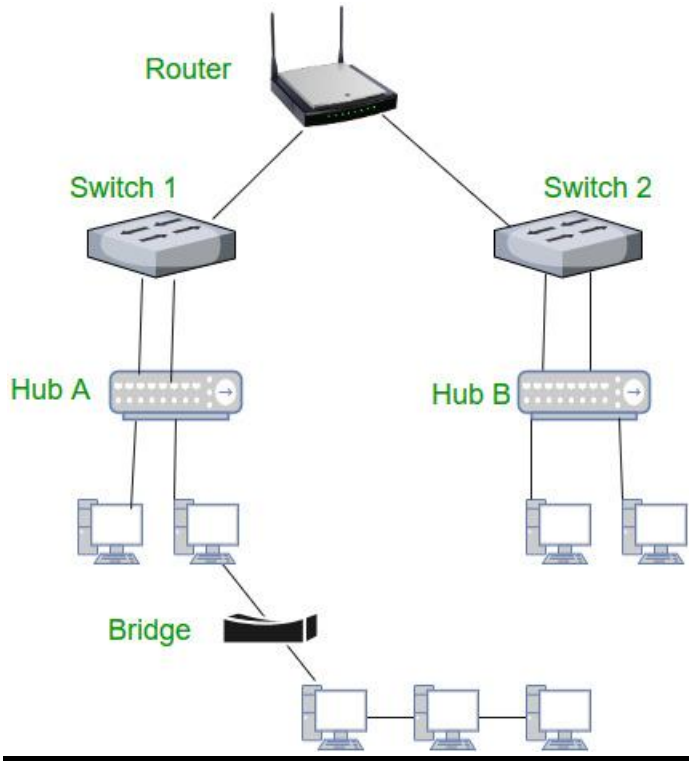
- It enhances the available bandwidth of the network.
- It can be directly connected to the workstations or devices.
- Enhances the performance of the network.
- Networks with switches have less frame collision, and it is because switches develop the collision domain for each network.
- It helps in reducing the workload on the individual host such as PCs.

Disadvantages of Switch

- It cannot stop traffic destined for a different LAN segment from traveling to all other LAN segments.
- Switches are more expensive.

ROUTER

A router is a device like a switch that routes data packets based on their **IP addresses**. The router is mainly **a Network Layer device**. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.



Functions of a Router

The router performs major functions as:

1. **Forwarding:** The router receives the packets from its input ports, checks its header, performs some basic functions like checking checksum, and then looks up to the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.
2. **Routing:** Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table that is made using different algorithms by the router only.
3. **Network Address Translation (NAT):** Routers use NAT to translate between different IP address ranges. This allows devices on a private network to access the internet using a single public IP address.
4. **Security:** Routers can be configured with firewalls and other security features to protect the network from unauthorized access, malware, and other threats.
5. **Quality of Service (QoS):** Routers can prioritize network traffic based on the type of data being transmitted. This ensures that critical applications and services receive adequate bandwidth and are not affected by lower-priority traffic.

6. **Virtual Private Network (VPN) connectivity:** Routers can be configured to allow remote users to connect securely to the network using a VPN.
7. **Bandwidth management:** Routers can be used to manage network bandwidth by controlling the amount of data that is allowed to flow through the network. This can prevent network congestion and ensure that critical applications and services receive adequate bandwidth.
8. **Monitoring and diagnostics**: Routers can be configured to monitor network traffic and provide diagnostics information in the event of network failures or other issues. This allows network administrators to quickly identify and resolve problems.

Advantages of Router

1. **Easier Connection:** Sharing a single network connection among numerous machines is the router's main job. This enables numerous people to connect to the internet, boosting total productivity. In addition, routers have connections between various media and network designs.
2. **Security:** Undoubtedly, installing a router is the first step in securing a network connection. Because using a modem to connect directly to the internet exposes your PC to several security risks. So that the environment is somewhat secure, routers can be utilized as an intermediary between two networks. While not a firewall or antivirus replacement.
3. **NAT Usage:** Routers use Network Address Translation (NAT) to map multiple private IP addresses into one public IP address. This allows for a better Internet connection and information flow between all devices connected to the network.
4. **Supports Dynamic Routing:** The router employs dynamic routing strategies to aid in network communication. The internet work's optimum path is chosen through dynamic routing. Additionally, it creates collision and broadcast domains. Overall, this can lessen network traffic.
5. **Filtering of Packets:** Switching between packets and filtering packets are two more router services. A collection of filtering rules is used by routers to filter the network. The packets are either allowed or passed through.

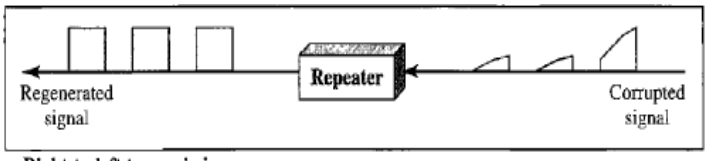
Disadvantages of Router

1. **Slower:** Routers analyze multiple layers of information, from the physical layer to the network layer, which slows down connections. The same issue can also be encountered when multiple devices are connected to these network devices, causing "connection waiting".

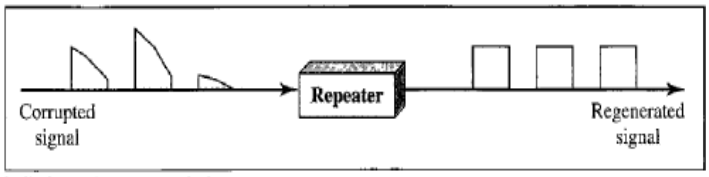
2. **High Cost:** They are more expensive than some other tools for systems administration. This includes security, extension, and the focal point. As a result, routers are typically not the greatest option for issues.
3. **Need for configuration:** The router must be properly configured to work properly. In general, the more complex the intended use, the more configurations is required. This requires professional installation, which can add to the cost of buying a router.
4. **Quality Issues:** The time transitions are not always accurate. Even yet, some modern devices use the 2.4GHz band, which is frequently deactivated. These kinds of separations are frequently possible for those who live in apartments and condominiums.
5. **Bandwidth shortages:** Dynamic routing techniques used by routers to support connections tend to cause network overhead, consuming a lot of bandwidth. This leads to a bandwidth shortage that significantly slows down the internet connection between connected devices.

REPEATER

- Repeater operates on physical layer.
- It receives the signal before it becomes corrupted and regenerates & amplifies the original bit pattern.
- It allows extending the physical length of the network.
- It doesn't change the functionality of network.



a. Right-to-left transmission.



b. Left-to-right transmission.

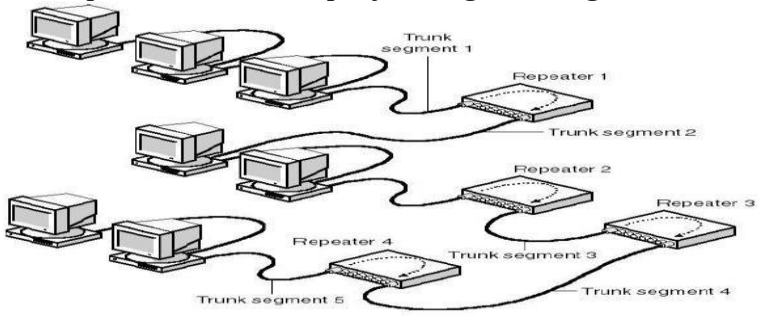
How it works:

•Forward bits from one network to another using two networks logically like one network.

•Don't alter the content of the packet moving across the wire. I.e. it simply copy bits without understandingwhat they are doing.

•An amplifier can't discriminate between the intended signaland noise; it amplifies equally everything fed in to it.

•A repeater does not amplify the signal, it regenerates it.



Advantages

•Can connect different types of media

•Can extend the network in terms of distance

•Cost effective

Disadvantages

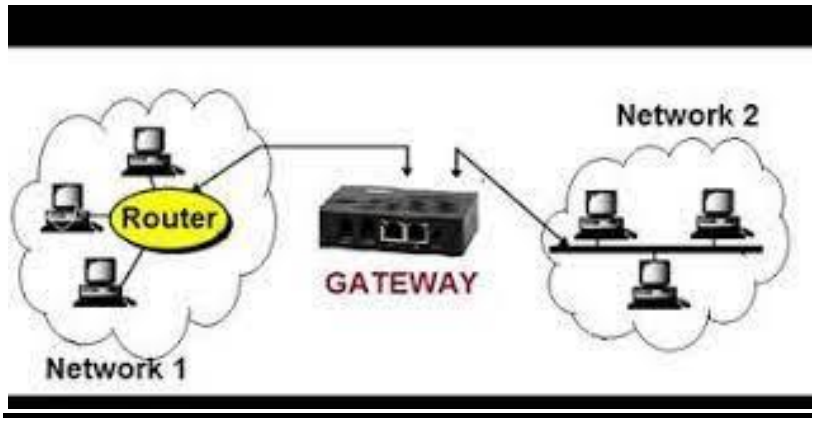
•Cannot filter the data

•Cannot connect different network architectures

GATEWAY

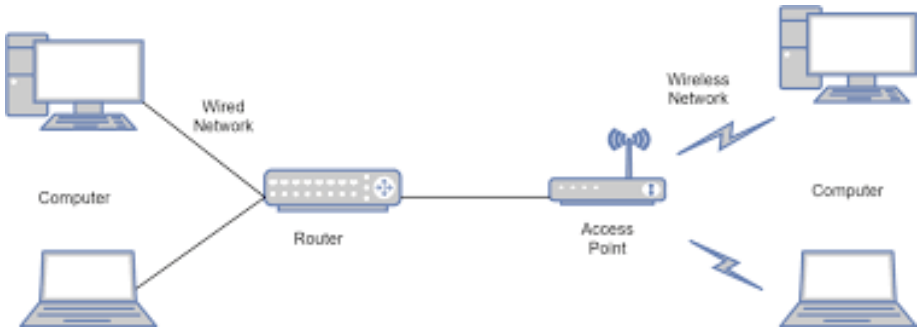
A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways

are generally more complex than switches or routers.



ACCESS POINT

- An access point (AP) is a wireless network device that acts as a portal for devices to connect to a local area network.
- Access points can extend an existing network's wireless coverage and increase the number of users who can connect.
- Wireless access points (WAPs) are devices that combine a transmitter and receiver (transceiver) to form a wireless LAN (WLAN).
- The access point operates at the OSI model's Data Link layer (Layer 2).



Advantages of the **Access Point** network device are: -

- Installing is easier and faster.
- Allows data transmission even when the user is moving.
- It is simple to extend to places where wires and cables are inaccessible.

Disadvantages of the **Access Point** network device are: -

- The range of network devices is limited, which causes issues for many users.

● Installing this network device is difficult and time-consuming.
● Because these network devices are susceptible to interference, fog and radiation can cause them to malfunction.

MODEM

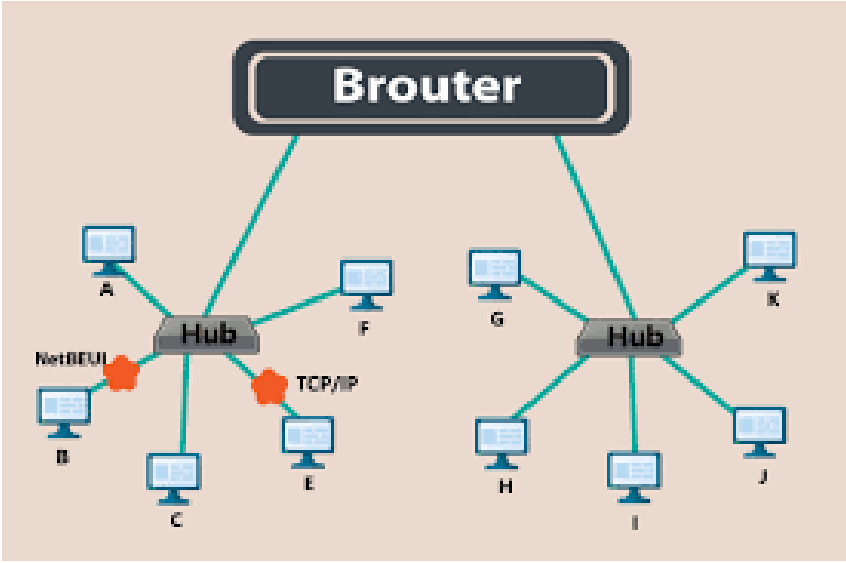
- A modem is a piece of hardware that enables a computer to transmit and receive data over telephone lines that connects a computer or router to a broadband network.
- When a signal is sent, the device converts digital data to an analog audio signal and sends it over a phone line. Similarly, when an analog signal is received, it is converted back to a digital signal by the modem.
- Onboard modems, internal modems, external modems, and removable modems are all examples of modems. A modem operates at the OSI model's physical layer (Layer 1) or Data link layer (Layer 2), depending on the type.

NIC

NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

BROUTER

It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as the bridge, it is capable of filtering local area network traffic.



Transmission Media

- **What is Cable?**

  - Cable is the **medium through which information normally moves** from one device toanother.
  - There are several types of cable which are commonly used with LAN. The **type of cable chosen for a network is related to the network topology, protocol and size.**
  - Transmission media can be divided into two categories one is guided and second is unguided.

- **Guided Media**
  - Guided media are those that provide a tube protecting electric wiring from one device to another.
  - Guided media are divided in three categories that is.
    - Twisted Pair cable
    - Co-axial cable
    - Fiber optic cable
  - Twisted pair and co-axial cable use copper that accept and transport single in the form of electric current.
  - Fiber Optic is a glass or plastic cables that and transport single in the form of **light.**
  - **Twisted Pair Cable**

    Twisted Pair come in two forms.

    a. Unshielded Twisted Pair cable

    b. Shielded Twisted pair cable

a. Unshielded Twisted Pair Cable

- Unshielded Twisted pair cable is a **most common** type of telecommunication medium.
- It is **used in the telephone system**.
- The cable **has four pair of wires inside the jacket.**
- **White / orange, orange / white, white / green , green / white, white / blue, blue /white, white / brown, brown / white**
- Each pair is twisted with different number of twist per inch to **help**

to eliminateinterface from adjacent pair.

- The electronic industry association(EIA)/Telecommunication Industry Association (TIA) has establish standard of UTP and rated five category of wires:

Type	Use
Category 1	Voice Only(Telephone Wire)
Category 2	Data Transmission of up to 4 MBPS(Local talk)
Category 3	Data Transmission of up to 10 MBPS(Ethernet)
Category 4	Data transmission of up to 20mbps(16 mbps token)
Category 5	Data transmission of up to 100mbps(Fast Ethernet)

- Unshielded twisted pair is also popular for token ring network, which were traditionally wired with shielded twisted pair.
- A disadvantage of unshielded twisted pair is that it may be harm to radio and electrical frequency interface.
- Each wire in a cable is attached to one pin in the connector.
- The most frequency use of this plug is RJ45 connector with 8 pin.
- One for each wire of four twisted pair.

Advantages

- UTP system is **color coded cabling**.
- UTP is **less expensive** then co-axial and fibber.
- UTP is a very **easy media to install and reconfigure**.

b. Shielded twisted pair

- STP cable has a metal foil covering each pair of conductor.
- It can eliminate cross talk, which is the undesired effect of one circuit on another line.
- It occurs when line pick up some of the signals travelling down another signal or another line.
- Shielded twisted pair's shielded increase its immunity to electromagnetic interface which allows it to transmit data over

longer distance then UTP.

- Shielded twisted pair (STP) has the same quality consideration and uses the same connector as UTP.
- Materials and manufacturing requirement make STP more expensive then UTP.

- **CO-axial cable**

  - Co-axial is the oldest network cable. It is easy to use. It has a larger bandwidth and can support transmission over long distance.
  - The metal shield help to block any outside interface from florescent light, motors and other computers.
  - Although Co-axial cable is difficult to install. It is highly resistance to signal interface.
  - It can support greater cable length then twisted pair cable.
  - There are **two types** of co-axial cable.

    a. Thick co-axial cable
    b. Thin co-axial cable

a. Thin co-axial cable

- Thin co-axial cable is **also referred to as a thin net**.
- 10base2 refers to the specification for thin co-axial cable carrying Ethernet signals. The 2 refers to approximate maximum segment length being 200 meters.
- Thin co-axial cable is **popular in school network**.

b. Thick Co-axial Cable

- Thick co-axial cable is also **referred to as a thick net**.
- 10base5 refers to the specification for thick co-axial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters.
- Thick co-axial cable **has extracted protective plastic cover**.
- One disadvantage of thick co-axial cable is that it **does not band easily and is difficult toinstall**.

- The advantage of thick co-axial cable is that it is **most robust, harder to change and transmitdata over a longer distance.**

Advantages of Co-axial cable

- Co-axial has a sufficient frequency range to support multiple channels, which allows for much greater throughput. Because it has a greater bandwidth per channel, it supports a mix range of services. For ex, voice, data and video.
- Because the inner conductor is in a shield, it has lower error rate.
- It reduces the noise and cross talk.

Disadvantages of Co-axial cable

- Co-axial cable may be damage by lighting sock.
- Installation cost in the local environment is high.
- It is not supported for some network standard.

➢ **Co-axial cable connecter**
- The most common type of connecter used with co-axial cable is the BNC connector.
- Different types of adapter are available for BNC connector.

- **Fiber Optics Cable**
  - Fiber Optics is long, thin of very pure glass about the diameter of human hair.
  - They are arranged in bundles called optical and used to transmit light signals over long distance.
  - It has a following parts:
    - **Core:**
      - Thin glass centre of the fiber where the light travels.
    - **Cladding:**
      - Outer optical material surrounding the core that reflects light back into the core.
    - **Buffer coating:**

- Plastic coating that protect the fiber from damage.
- Hundreds or thousands of this optical fiber are arranged in bundles in optical cables. The bundles are protected by the cables outer covering called a jacket.
- In a fiber cable the electrical signals are converted into appropriate light signals and converted into appropriated light signals and transmitted through it.
- An emitter sends the signals from one end of the cable and a light sensor senses this signals and then convert into its digital equivalence.
- There are transited which located at both end of cable, where the signals are converted from electrical to light signal and vice-versa.
- Fiber optic cables are available in different size with different size with different core and cladding diameters.
- The most commonly used fiber optic cable is the 62.5/125 micrometer. Core-62.5 and cladding 125.
- There are two source of light:
- Laser
- LED [Light Emitting Diode]
- Fiber optic cables use the principle of total reflection to transmit light signals.
- Speed of a light defers depending on the medium.

➢ **Use and Need of the fiber optics**

- Fiber optic cables are mainly used in environment that is highly susceptible to noise otherinterface.
- These cables are **highly secure** as they do not emit any external signals.
- It is use due to the following characteristics:

  - **Bandwidth:**
    - Carries huge amount of data ranging from 100 mbps to 1gbps.
  - **Segment length:**
    - Transmit readable data signals in a range of 2km to100km. This allows theuser to transmit data over a long distance.
  - **Interface:**
    - Secured data from being securely read as no electrical

signal pass through this type of cable. It is used in TV towers, radio station and electric transformer.

- **Propagation**

  - Fiber optic cables can support two modes for propagation light.
    a. Single Mode
    b. Multi Mode

a. Single Mode:

- In this type cable the **light travels straight down the fiber**, which means data can **travelgreater distance.**
- Single mode cable has a larger diameter then multi mode cable. It is header to manufacture.

  - Disadvantage of single mode

  - **Only one signal can be transmitted** through it.
  - To transmit two signals you need two strands of fiber optic cables.

b. Multi Mode:

- In multimode cable the **light bounce off the cables** was as it travels down, which causesthe **signal to be slower** and therefore data cannot **travel great distance**.
- Multi mode code is often used in LAN, since Data is not required to travel across thecountry.
- **Two or more signal can be transmitted** through it.

- **Advantages of Fiber Optics**

  - **Expensive:**
    - Several miles of optic cable can be made chipper then equivalent length of copperwire.

  - **Thinner:**

- Optical fiber can be drawn to smaller diameter then copper wire.

- **Higher carrying capacity:**
  - Because optical fiber are thinner then copper wire, more fiber can be bundled in to agiven diameter cable then copper wire.

- **Less Signal Degradation:**
  - The loss of signal in optic fiber is less then copper wire.

- **Light signal:**
  - Unlike electrical in copper wire, light signal from one fiber do not interfere with otherfiber in the same cable.

- **Digital signal**
  - Optical fibers are ideally suited for carrying digital information which is useful incomputer network.

- **Light weight**
  - This cable weight is less then as compare to copper wire.

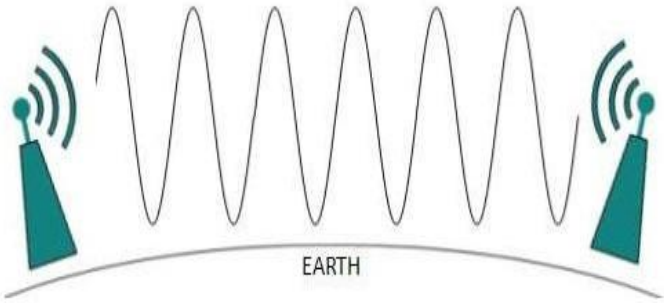
➢ **Disadvantage Of optical fiber**
- Fiber optic cable is **expansive**.
- **Glass fiber is more easily broken then wire**. It **is less useful for applications wherehardware portability is required.**

➢ **Fiber Optic Connector :**
- The most common connecter used with fiber optic cable is an **ST connecter**. It is similar toBNC connector.

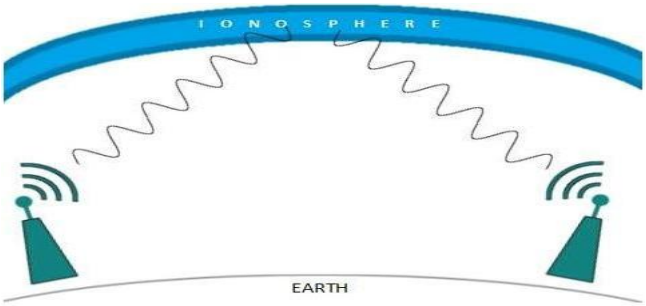
❖ **Wireless transmission – Radio waves, Microwaves, Infrared waves, <u>Satellite communication</u>**

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the airand are received and interpreted by appropriate antennas.

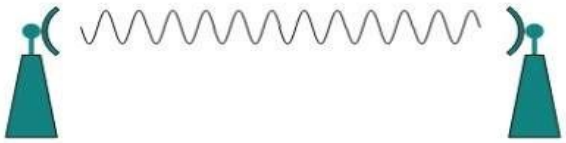
Radio Waves



Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike. It's frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). The power of low frequency waves decreases sharply as they cover long distance. High frequency radio waves have more power. Lower frequencies such as VLF, LF, MF bands can travel on the ground up to 1000 kilometers, over the earth's surface.



High frequency radio waves such as HF and VHF bands are spread upwards.



Microwaves

Microwaves are the form of electromagnetic transmission used in wireless communication systems. Electromagnetic waves above 100 MHz tend to travel in a straight line. Microwave transmission depends highly upon the weather conditions and the frequency it is using. The frequency varies from 300MHz to 300GHz. These are widely used for long distance communications and are relatively less expensive. The microwave does not pass through buildings.

Infrared Waves

Infrared radiations are electromagnetic radiations with longer wavelengths than visible light. Its frequency ranges from 300-GHz to 430-THz. Infrared wave is used for very short range communication purposes such astelevision and it's remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles. Examples like Television remote control, mobile data sharing.

Satellite Communication

Satellite communication is a wireless technology having significant importance across the globe. This allows users to stay connected virtually from anywhere on the earth.