Transmission Media
&
Network Devices

UNIT-3

Course Outcome:

Select proper transmission media and devices based on network requirements

What is Transmission & Transmission Media?

❑Transmission

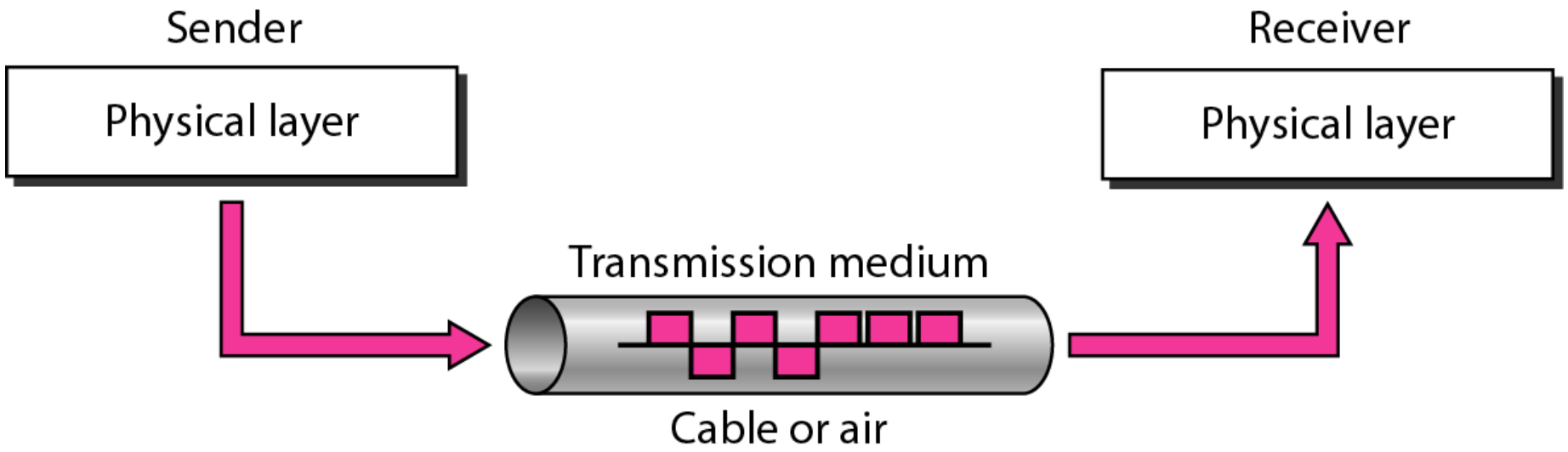
- Transmission is the **process of sending data from one device to another** device.

❑Transmission Media

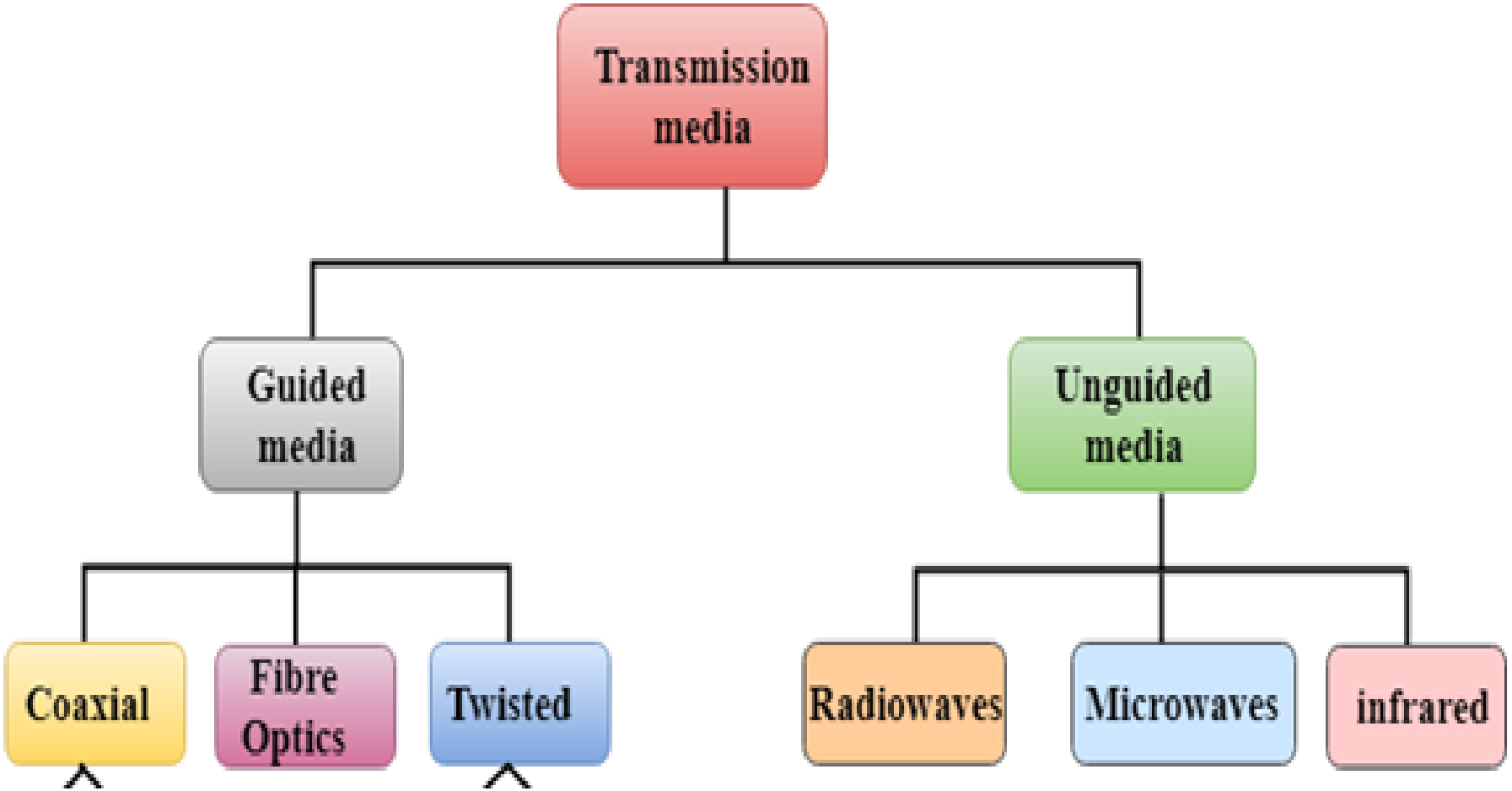
- Transmission media is the **physical path on which data travels between devices in a network**. It can be **wired**, like **cables**, or **wireless**, like **signals** through the air.

Figure 3.1 *Transmission medium and physical layer*

For any networking to be effective, raw stream of data is to be transported from one device to other over some medium.



TYPES OF TRANSMISSION MEDIA



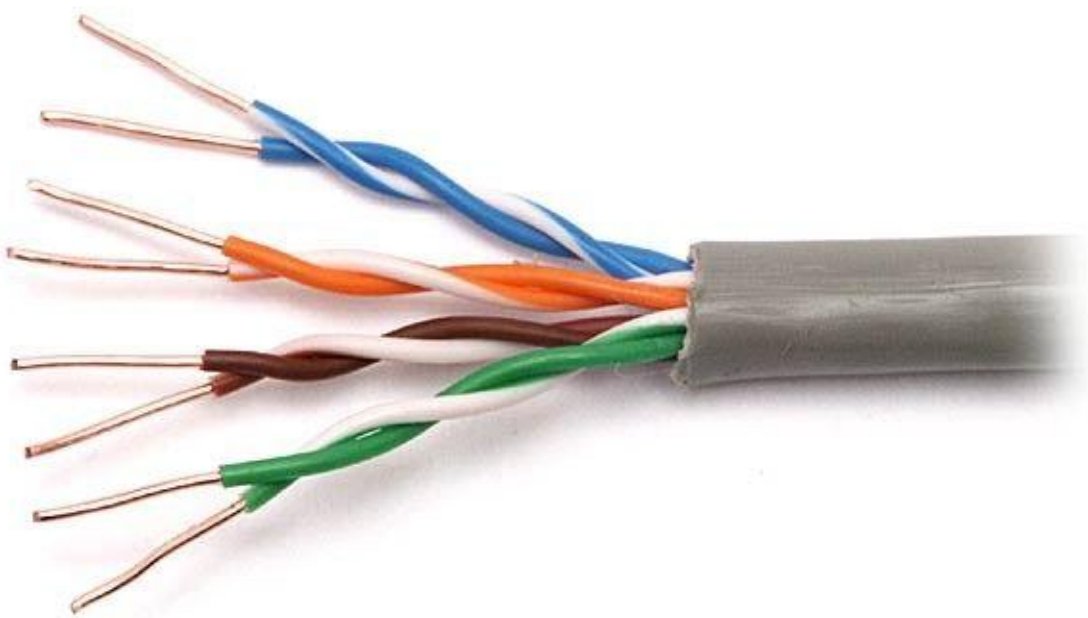
GUIDED MEDIA

- *Guided transmission media uses a "cabling" system that guides the data signals along a specific path.*
- *Guided media is also known as "Bound Media".*
- *Guided media which are those that provide medium from one device to another.*

❑ *Guided Transmission media includes*

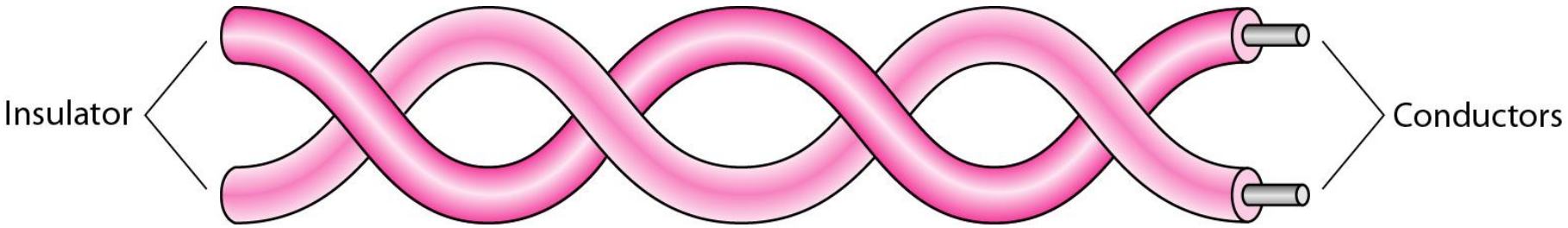
- Twisted-Pair Cable
- Coaxial Cable
- Fiber-Optic Cable

Twisted-pair cable



Twisted-pair cable

- Twisted pair is a physical media made up of a pair of cables twisted with each other.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

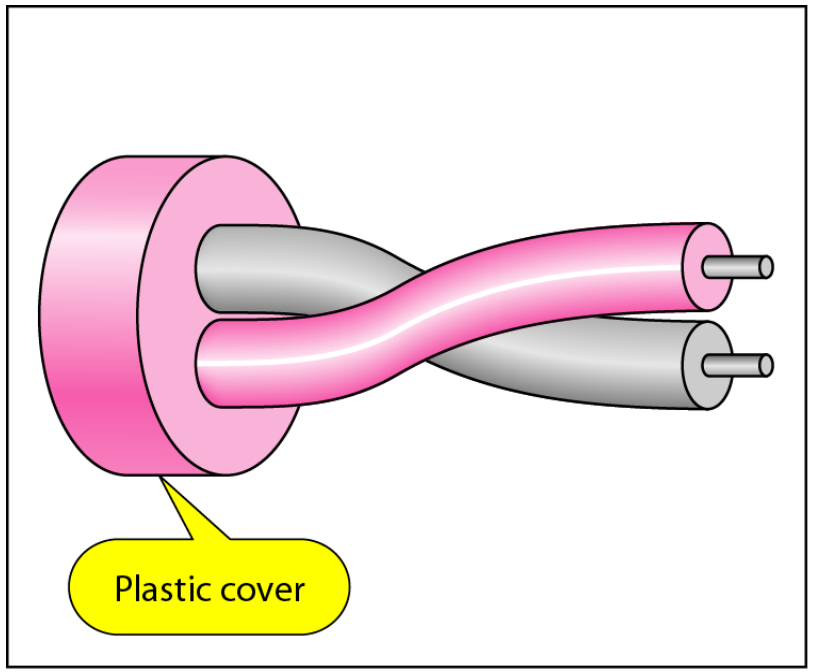


Twisted-pair cable

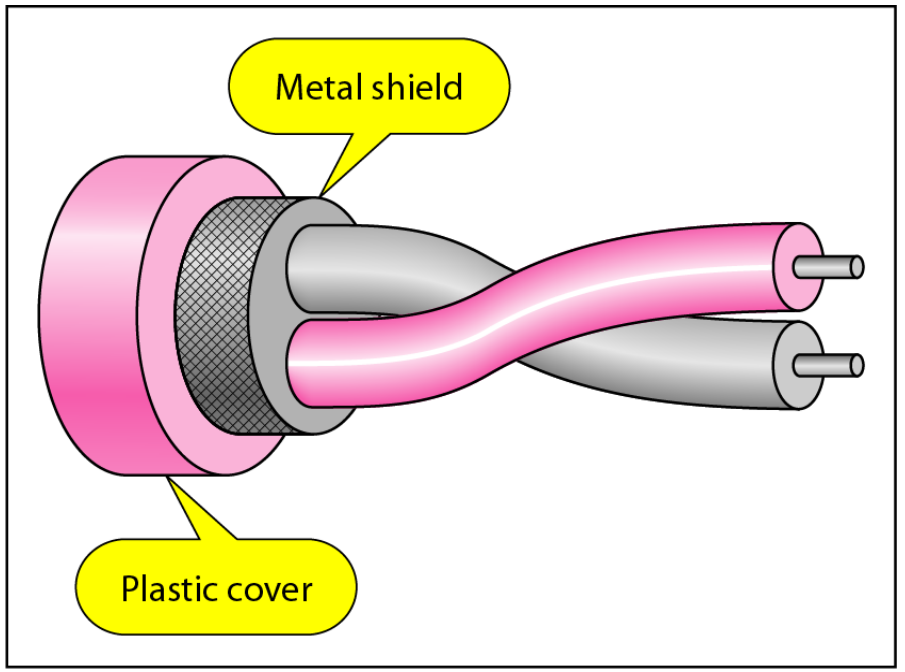
- The pair of wires are twisted together to decrease interference by adjacent wires.
- All electricity creates magnetism; taking two wires that send electricity in opposite direction (such as sending and receiving) and twisting them together reduces the magnetism.
- This makes Twisted Pair cabling less susceptible to Elector Magnetic Interference.

Twisted pair cable comes in two forms:

- 1)Unshielded twisted pair cable(UTP) and
- 2)Shielded twisted pair cable(STP).



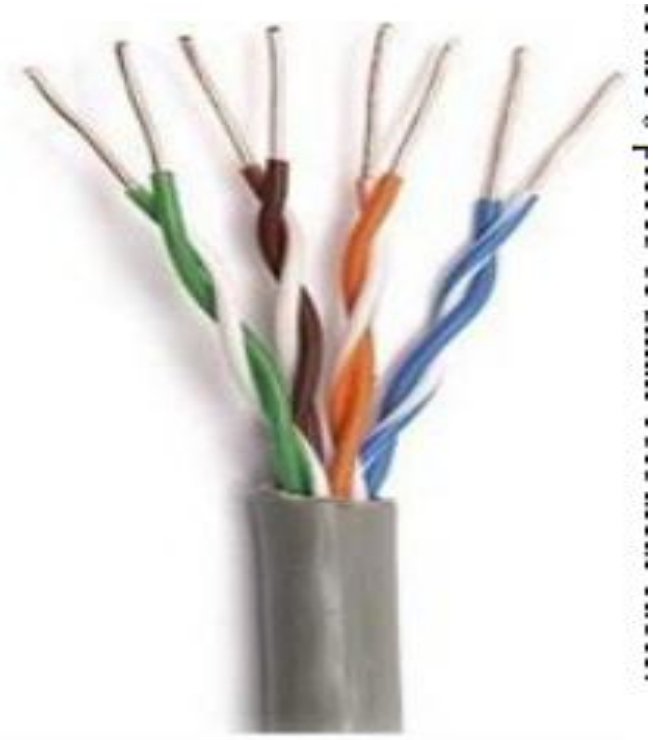
a. UTP



b. STP

Unshielded Twisted Pair Cable(UTP):-

- These are a pair of two insulated copper wires twisted together without any other insulation or shielding and hence are called unshielded twisted pair cables.
- They reduce the external interference due to the presence of insulation.
- It is used mostly in telephone system; its frequency range is suitable for transmitting both data and voice.
- Frequency range suitable for UTP is 100Hz to 5MHz.



Just for info

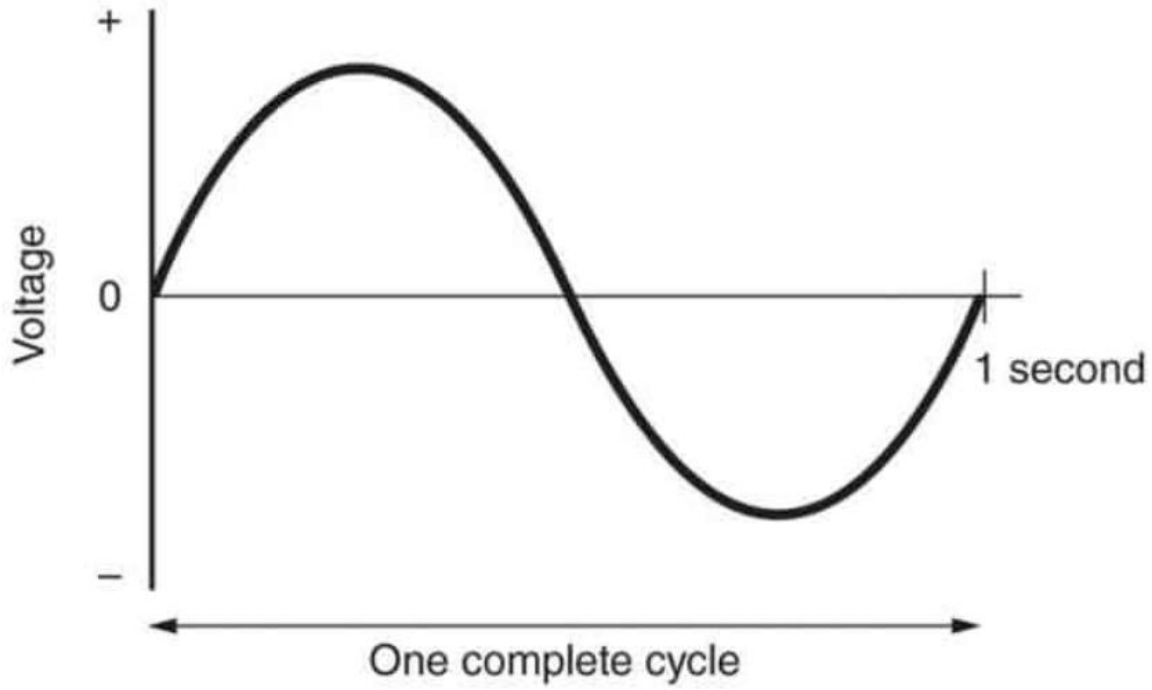


Figure 1: 1 cycle completed = 1 hertz.

Characteristics of UTP

✓ Low cost

✓ Easy to use

✓ Flexible

✓ Easy to install

✓Light weight

Disadvantages of UTP

- One potential problem of UTP is that its wire can be affected by EMI (Electromagnetic interference) from devices.
- This can create a noise over wires, which can damage the signal.
- This cable can only be used for shorter distances because of attenuation.

Application of UTP

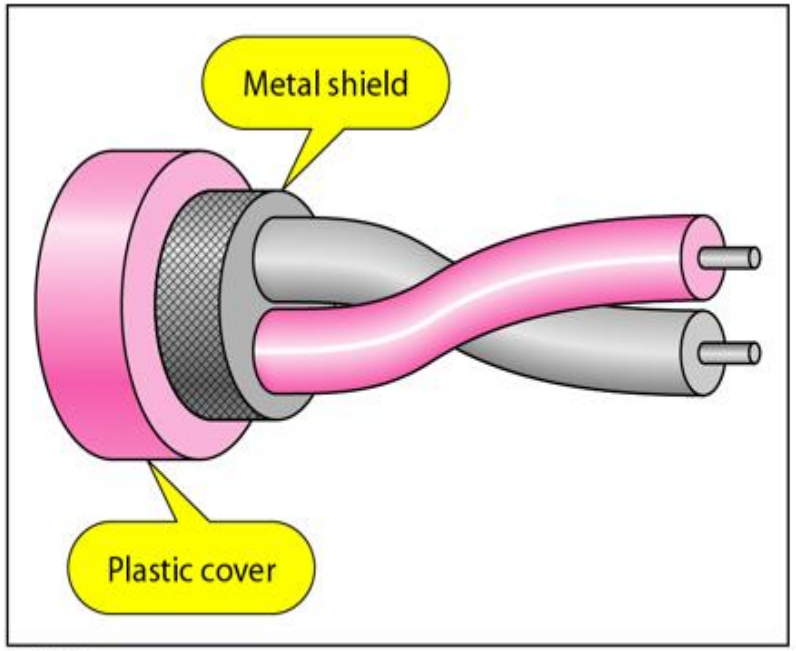
- UTP are used in many LAN technologies, including Ethernet & token ring.
- They can be used for voice,high-speed data, audio, transmission.
- Telephone lines.

Category of UTP

- Category 1:- The basic twisted pair cabling used in telephone system. This level of quality is fine for all. But low speed data **communication**.
- Category 2:- It is suitable for voice and for data transmission of up to 4Mbps.
- Category 3:- It can be used for data transmission up to 10Mbps. It is now standard cable for most telephone system.
- Category 4:-It can be used for data transmission up to 16Mbps.
- Category 5:- It can be used for data transmission up to 100Mbps.

Shielded Twisted Pair Cable(STP):-

- STP cable **contains an extra wrapping foil or copper braid jacket to protect the cable from defects** like **cuts**, **losing bandwidth, noise, and signal to the interference.**
- It supports the **higher data transmission rates across** the **long distance**.



b. STP

Shielded Twisted Pair Cable(STP):-

- This gives STP excellent insulation to protect the transmitted data from outside interference.
- STP is less susceptible to electrical interference and supports higher transmission rates over longer distance than UTP.
- Materials and Manufacturing requirements make STP more expensive then UTP, but supports higherband width over longer distance than UTP.

Advantages of twisted pair cable

- Simple and easy to setup
- It can carry both analog and digital data
- Easy to install, maintain, and terminate.
- Less expensive than co-axial and fiber optic cable
- Provide better performance.

Dis-advantage of Twisted pair cable

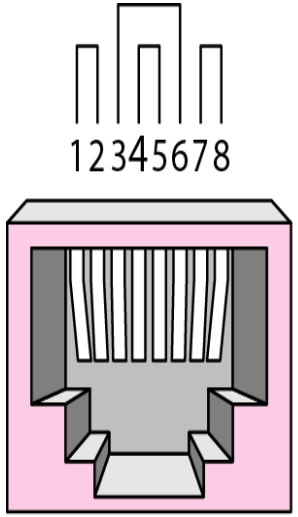
- Susceptible to electromagnetic interference(EMI)
- It has wors noise immunity
- Got break easy as thin in size
- It has higher attenuation.

UTP	STP
It is an unshielded twisted pair.	It is a shielded twisted pair.
UTP cable is a twisted pair cable with wires that are twisted together.	It is enclosed within a foil or mesh shield.
The price of UTP is lower as compared to the STP.	The price of STP is much costlier than UTP.
It does not require a grounding cable.	It requires a grounding cable.
In UTP, the electromagnetic interference is more than the STP while transferring the signal to the transmission media.	It reduces electromagnetic interference while transferring the signal to the transmission media.
UTP has high crosstalk.	STP has low crosstalk.
Transferring speed of the data signal is slow as compared to the STP.	Transferring speed of the data signal is high as compared to the UTP.
Installation of UTP cables is easy as they are lighter, small in size, and flexible.	Installation of STP cable is quite difficult as compared to the UTP. Its size is heavy, bigger, and stiffer.
It does not require much maintenance.	It requires more maintenance.
UTP cables are noisier.	STP cables are less noisy.
However, the UTP cable is used to establish the connection within a short distance, like a home or small industry.	Generally, it is used to establish the connection for enterprises over a long distance.

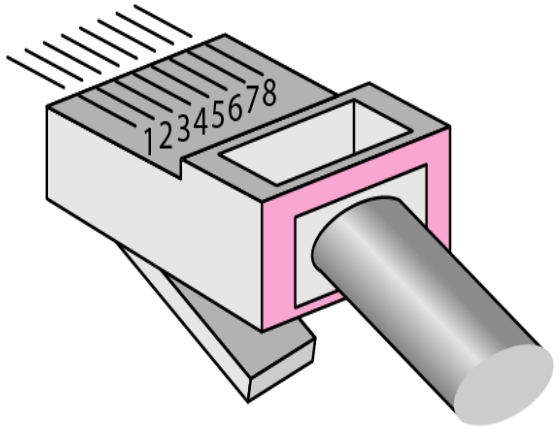
UTP/STP CONNECTORE :(RJ-45)

- RJ45 stands for Registered Jack 45 and is the most commonly used connector in wired networks.
- The jacks are mainly used to connect to the Local Area Network (LAN).
- RJ-45 Connector is a tool that we put on the end of the UTP cable to plug the cable in the LAN port.
- It was earlier devised for telephones(RJ-11) but is now widely used in Ethernet Networking.
- The 45 in RJ45 basically stands for the listing number.
- The width of RJ45 is usually greater than that of the telephone cables or other Registered Jacks.

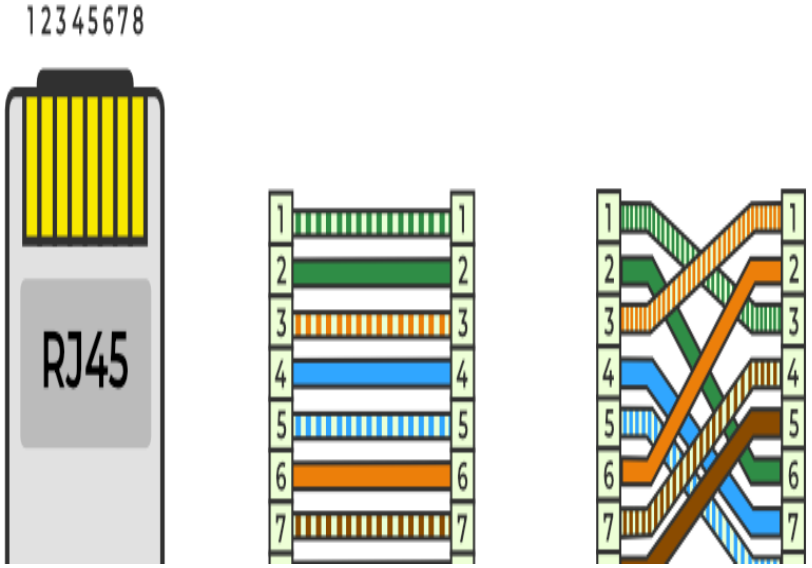
Rj-45 connector



RJ-45 Female

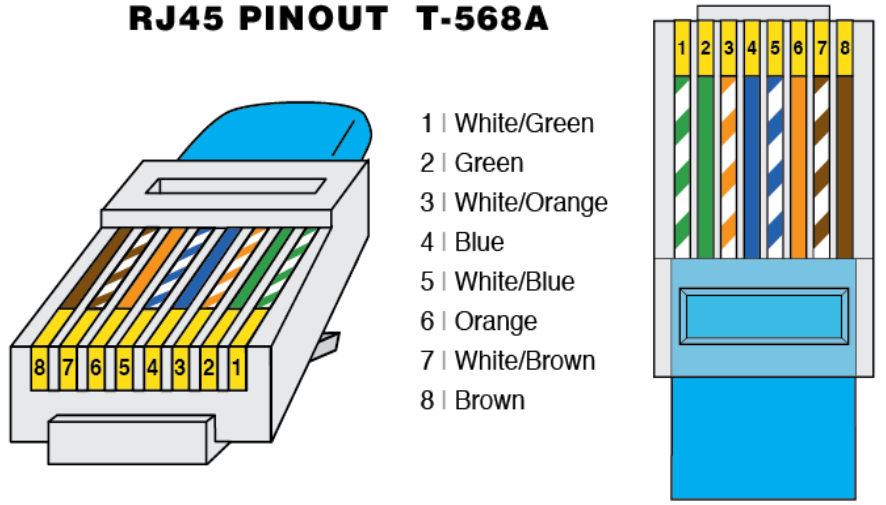


RJ-45 Male



Structure of RJ45

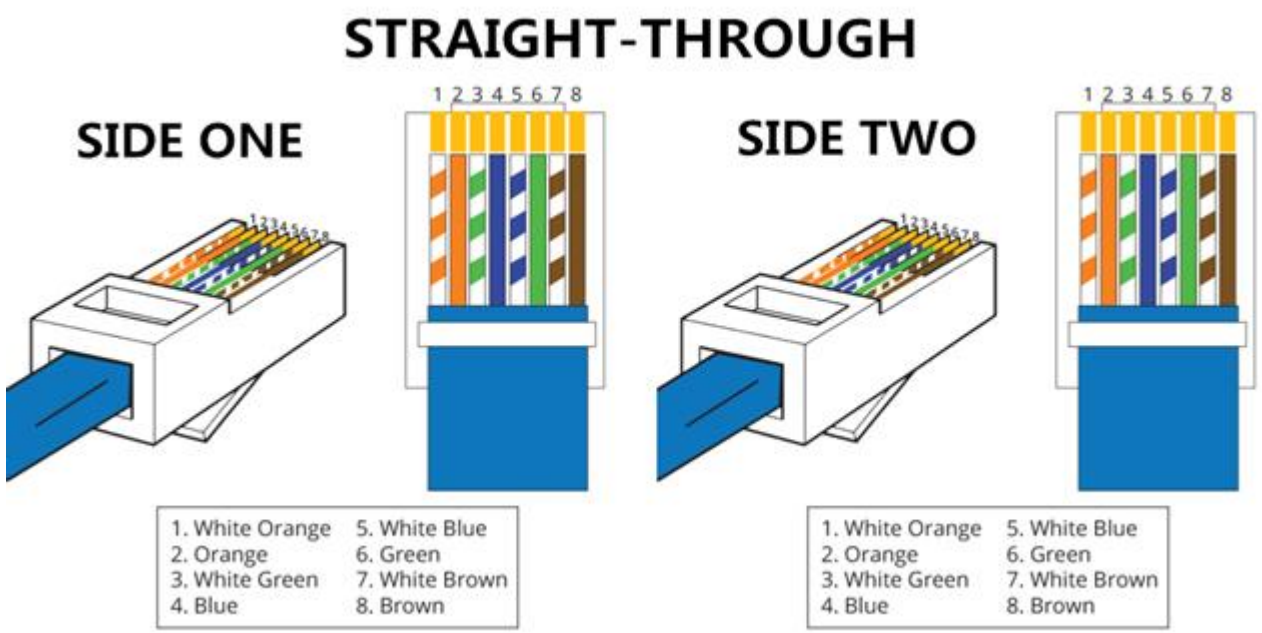
- RJ45 has a transparent plastic structure and is an 8-pin connector. It is an 8P8C connector and the number of wires that can be connected is 8.
- The jacks are mostly used with Shielded Twisted Pair (**STP**) cables or Unshielded Twisted Pair (**UTP**) cables.
- In RJ45 we can see the 8 wires out of which 4 wires are solid colored and 4 are strip colored.
- The classification of RJ45 is done based on the wiring.

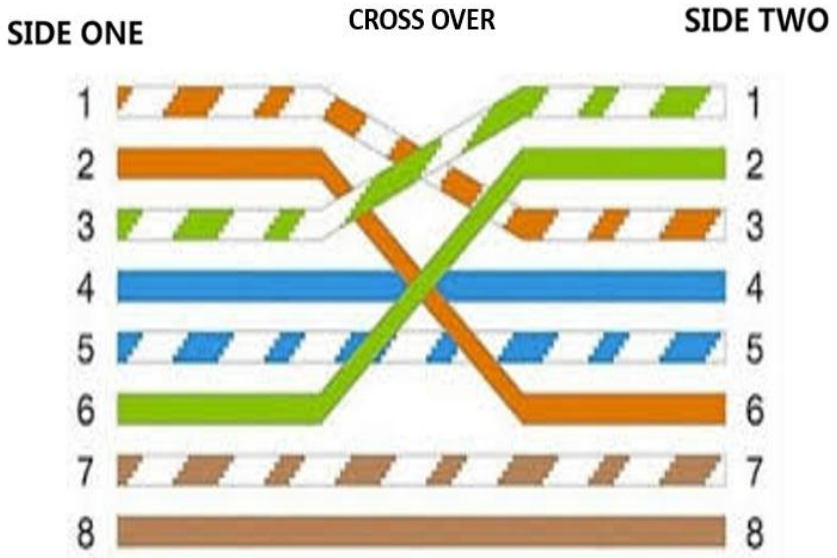


Structure of RJ45

- **THERE ARE TWO TYPES**

1. **STAIGHT THOUGH CABLE**
2. **CROSS OVER CABEL**

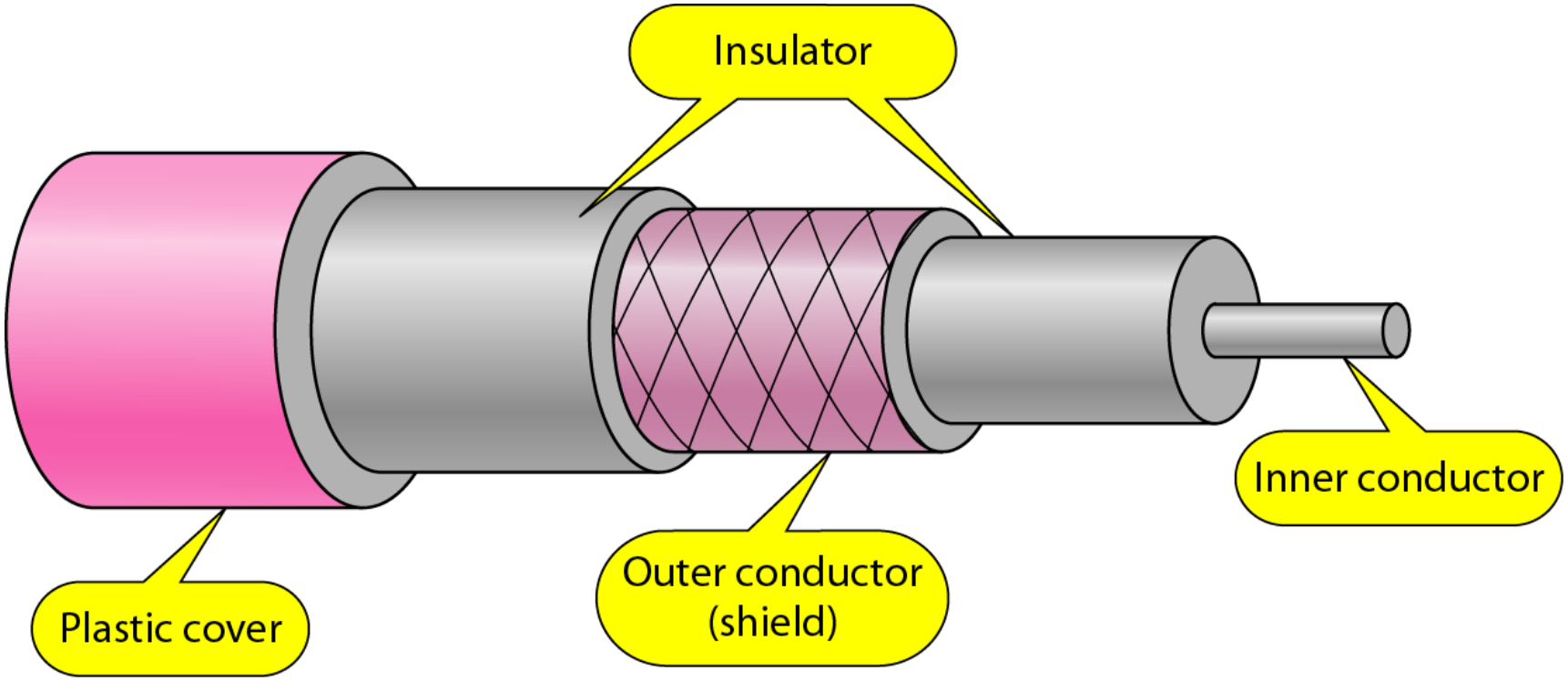




Coaxial Cable:-

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- It contains two conductors parallel to each other.
- Co-axial cable has better shielding than twisted pairs, so it can span longer distances at higher speed.
- It has a higher frequency as compared to Twisted pair cable. i.e. 100KHz to 500MHz.

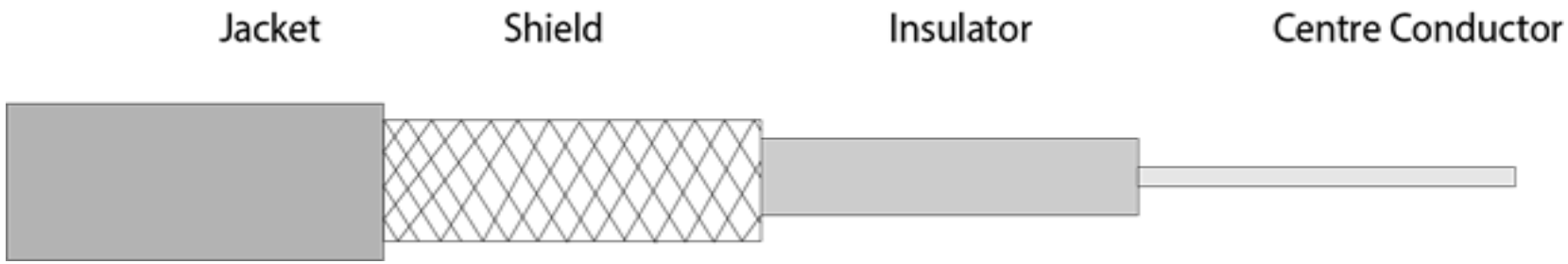
Coaxial Cable:-



- It has 2 conductor run parallel to each other or on same axis hence name is “coaxial” cable

Coaxial Cable:-

- The Coaxial cable has central core conductor of solid or standard wire (usually copper) enclosed in an insulating shield, which is in turn encased in an outer conductor of metal foil, braid-mesh or combination of two.
- It has 2 conductor run parallel to each other or on same axis hence name is “coaxial” cable



Coaxial Cable:-

- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. And protects from interference.
- This outer conductor is also enclosed in an insulating sheath and whole cable is protected by plastic cover(cladding).

There are two types of coaxial cable

- 1. Thin coaxial cable(Thin net)
- 2. Thick (Thick net)

1. Thin coaxial cable(Thinnet)

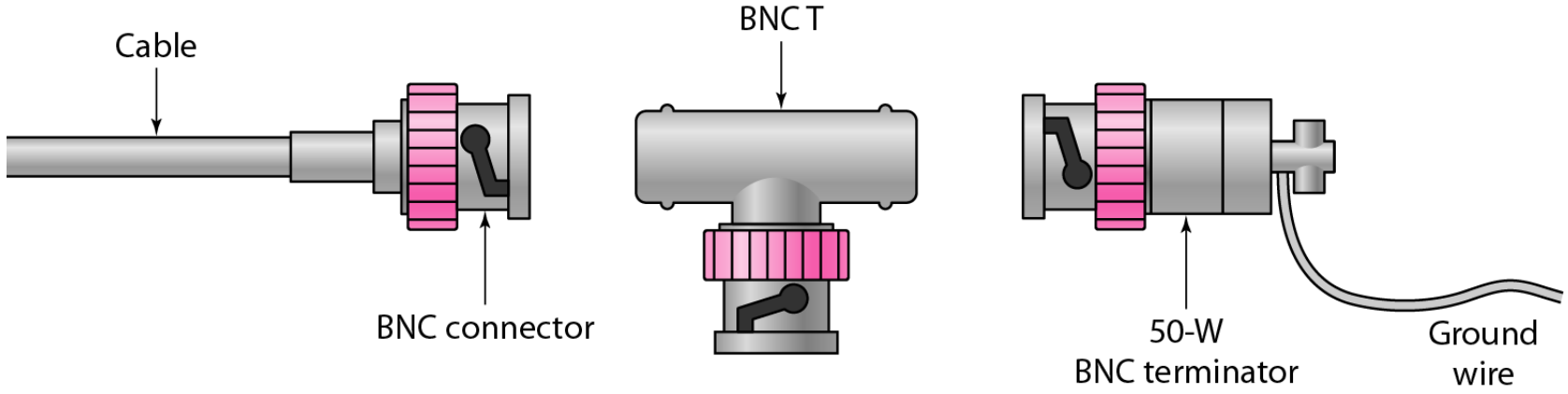
- It is a flexible coaxial cable about 0.25 inches(thin).
- It is 10Base2 (10Mbsp over 200m)
- i.e medium and operates at a speed of 10 Mbps to carry out baseband transmission.
- And 2 refers to approximate maximum segment length being 200meters.(actual-185m)
- Thinnet is included in a group that referred to as the RG-58 (radio grade) family and has 50-ohm impedance.
- Commonly used for digital transmission.

(2) Thick-net Coaxial Cable:

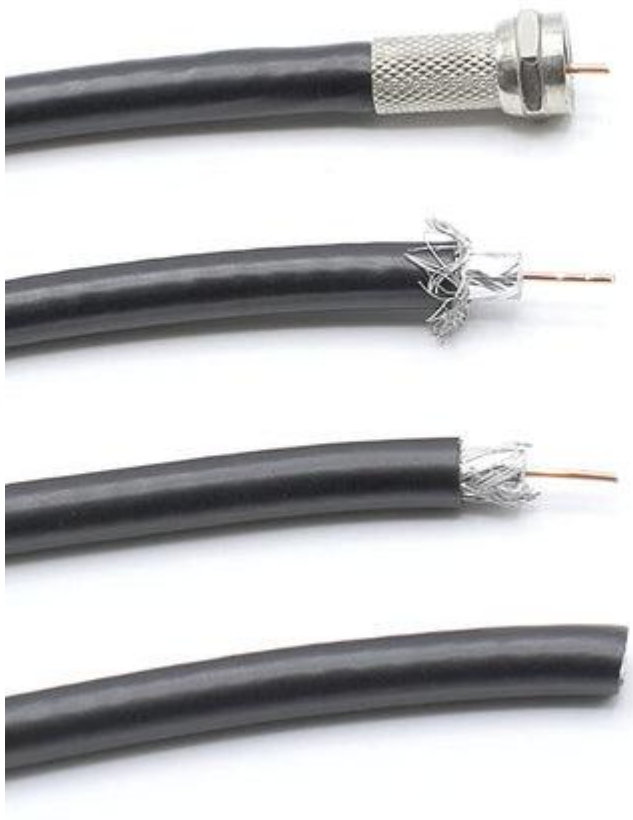
- Thicknet is relatively rigid coaxial cable about 0.5 inches in diameter.
- It is 10Base5. (10Mbsp over 500m)
- Thick net can carry signal for 500 meters [about 1640 ft] .
- Thicknet's ability to support data transfer over longer distance it is sometimes used as backbone to connect several smaller thinnet based networks
- A device called a transceiver connects the thinnet coaxial to the larger thicknet coaxial cable.

Coaxial Cable Connector

- To connect coaxial cable to devices, we need coaxial connectors.
- The most common type of connector used today is the Bayonne-Neill-Concelman (BNC), connector.
- Figure shows three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator



Coaxial Cable Connector



Step 4: Screw on Connector

(Connector must be flush with inside of dielectric material)

Step 3: Peal Back Braid

Step 2: Prepare Coax at 1/4" Braid & 1/4" Stinger

Step 1: Cut Coax


S-2 COMPLIANT
18 AWG
CATV OR CL2

BNC

- **Applications:** BNC connectors are commonly used in applications such as RF test equipment, CCTV cameras, oscilloscopes, and many other video and RF devices. They are popular in applications where frequent connections and disconnections are required.
- **Cable Types:** BNC connectors can be attached to various types of coaxial cables, including RG-58 50Ω(ethernet) or RG-62 75 Ω cable.(CCTV).

Threaded Neill–Concelman (TNC) CONNECTOR

- A TNC connector is a type of coaxial connector used in RF (Radio Frequency) and microwave applications.
- It is **similar** in design **to the more common BNC** connector **but has a threaded coupling** mechanism that **provides** a more **secure connection**.
- **Threaded Coupling:** TNC connectors use a threaded coupling mechanism. To connect two TNC connectors, you twist them together until they lock into place.
- This design provides a more secure connection compared to connectors like BNC, which use a bayonet coupling.

TNC

- **Outer Shell:** The outer shell of a TNC connector is typically made of metal, such as stainless steel or brass.
- It has a threaded design, which allows for a secure and stable connection when mated with a compatible TNC connector.
- **Center Pin:** The center pin is the inner conductor of the TNC connector. It extends from the center of the connector and is responsible for carrying the signal. It is also typically made of metal.
- **Dielectric:** Surrounding the center pin is a dielectric material, which provides insulation between the center pin and the outer shell of the connector. This prevents electrical contact between the inner and outer conductors.
- **Applications:** TNC connectors are commonly used in applications such as Wi-Fi antennas, RF test equipment, telecommunications equipment, and other RF and microwave devices.

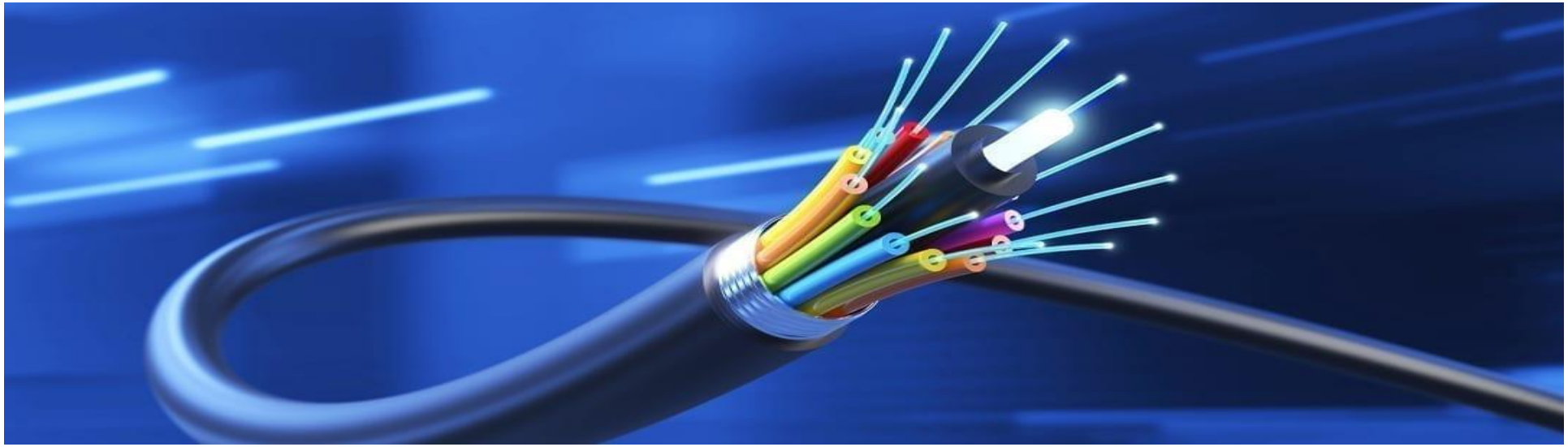
Coaxial Cable Advantages

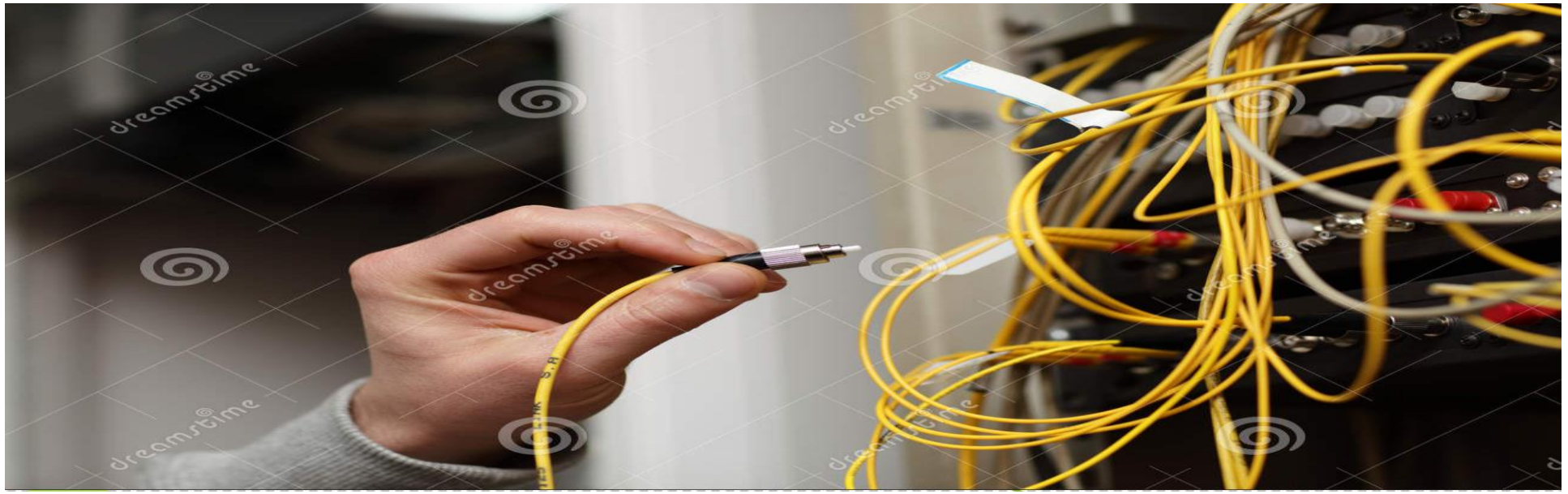
- Coaxial cable is the most widely used in n/w cable.
- Can go longer distance and has better protection from EMI than twisted pair.
- It can be easily installed.
- Better data transmission rate than twisted pair.
- Used for broadband transmission.

Coaxial Cable Disadvantages

- single cable failure can break down an entire n/w.(because generally used as backbone for smaller networks)
- it is expensive to install compare to twisted pair cable.
- High maintenance cost

Fiber Optics cable



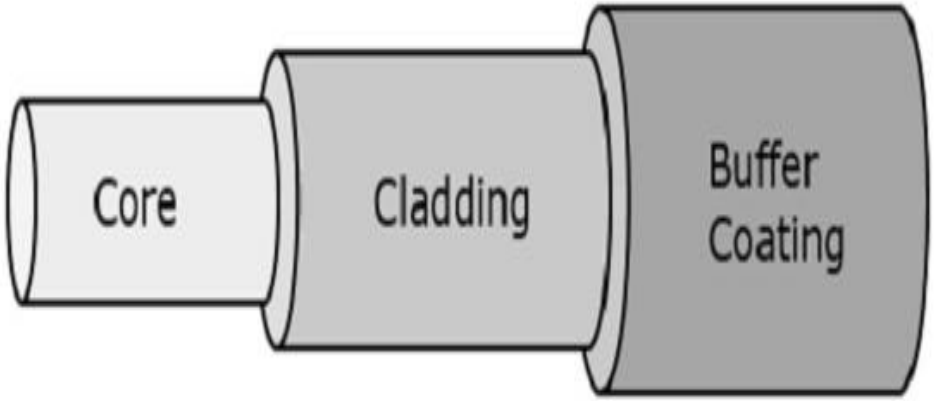


Fiber Optics cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- A cable may contain a single fiber, but often fibers are bundled together in the centre of cable.
- Optical fiber are smaller and lighter than copper wire.
- One optical fiber is approximate the same diameter as a human hair. It is greatly more efficient than the other network transmission media.

Fiber Optics cable

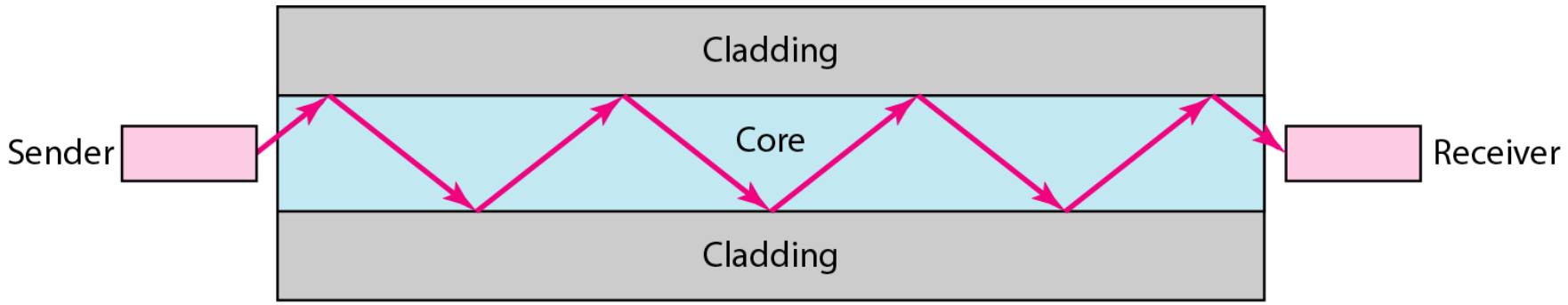
- Fiber optic cabling consists of a centre glass core surrounded by several layers of protective materials.
- It has inner core of glass that conducts light.
- This inner core is surrounded by glass cladding.
- This glass cladding reflects light back into the core.
- Outer side thin plastic jacket protect the cladding.



Parts of an Optical fiber

Fiber Optics cable

- It **transmits light rather than electronic signals** eliminating the problem of electrical Interference.
- This makes it ideal for certain environments that contain a large amount of electrical interference.



Fiber Optics cable

- An optical transmission system has three components:
- The **transmission medium, the light source and the detector.**
- The transmission medium is an ultra-thin fiber of glass or fused silica.
- The light source is either a LED (Light Emit Diode) or a laser diode, both of which emits light pulses when electrical current is applied.
- The detector is a photo diode, which generates an electrical pulse when light falls on it.

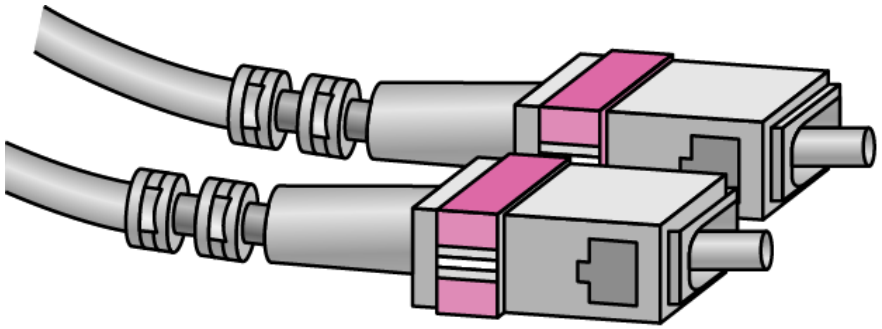
advantages of fiber optic cable over copper:

- Fiber cable are lighter and thinner, so they use less area as compared to copper wires.
- Data transfer rate is very high.
- Signal carrying capacity is very large.
- The fiber optic cable carries the data at a longer distance as compared to copper cable.
- Not affected by ELECTOMAGNETIC INTERFERENCE(EMI).

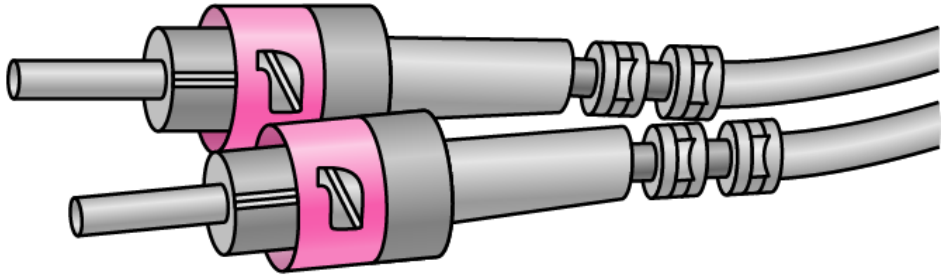
Disadvantages

- It is more expensive than twisted pair and co-axial cable.
- Its installation is very difficult.
- it needs costly splicing machines and trained specialists to place in fiber optic cables.

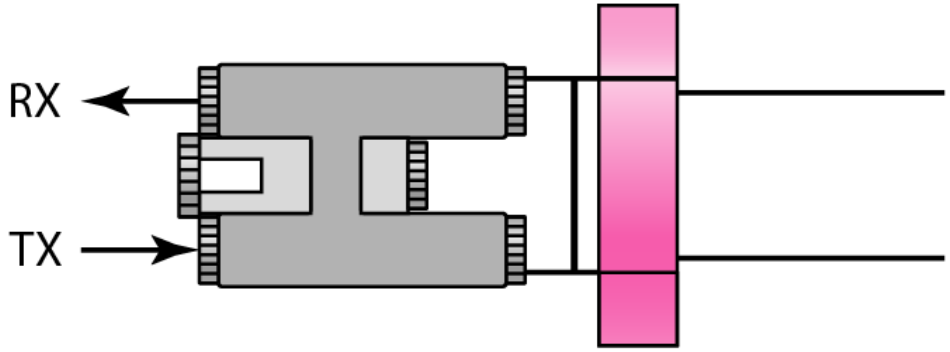
Fiber-optic cable connectors



SC connector



ST connector

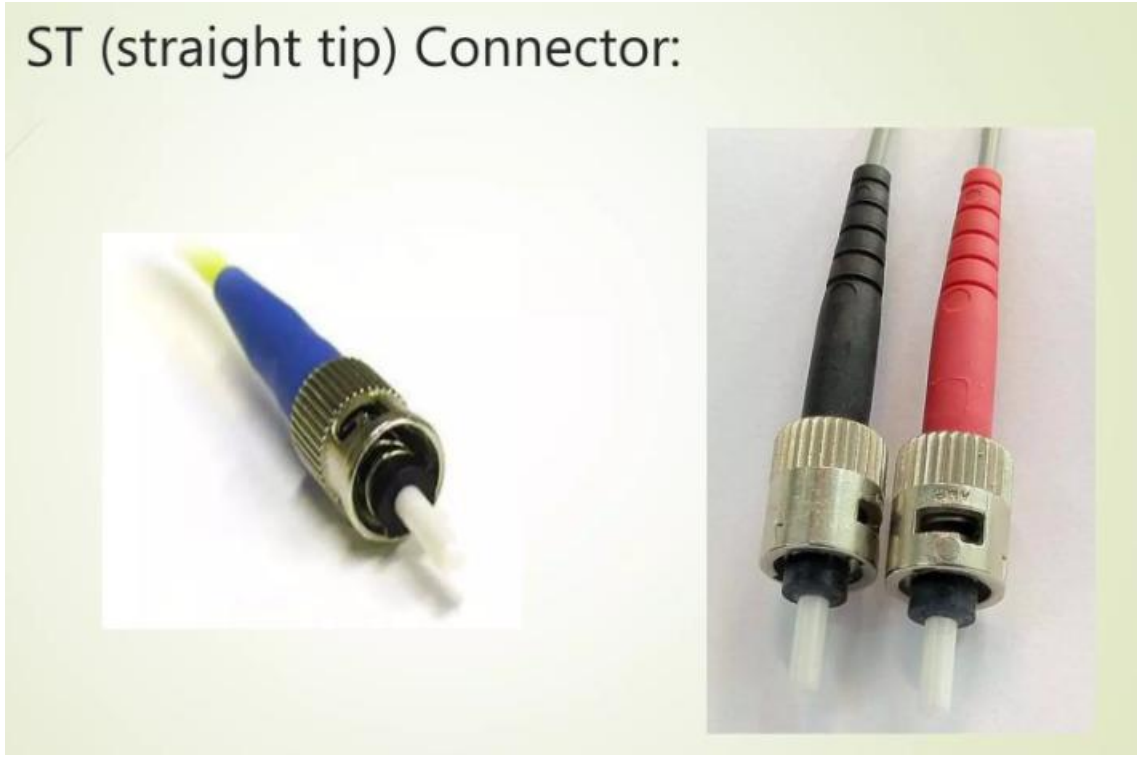


MT-RJ connector

SQUARE OR STANDARD CONNECTOR

SC
(Subscriber *or* Square or Standard connector)

STRAIT TIP CONNECTOR



UNGUIDED MEDIA: WIRELESS

- Unguided media transport electromagnetic waves without using a physical conductor. Or physical link between sender and receiver.

- This type of communication is often referred to as wireless communication.
- Signal are normally broadcast through the air and thus available to any one who has a device capable of receiving them.

UNGUIDED MEDIA: WIRELESS

- *Topics discussed in this section:*

  Radio Waves

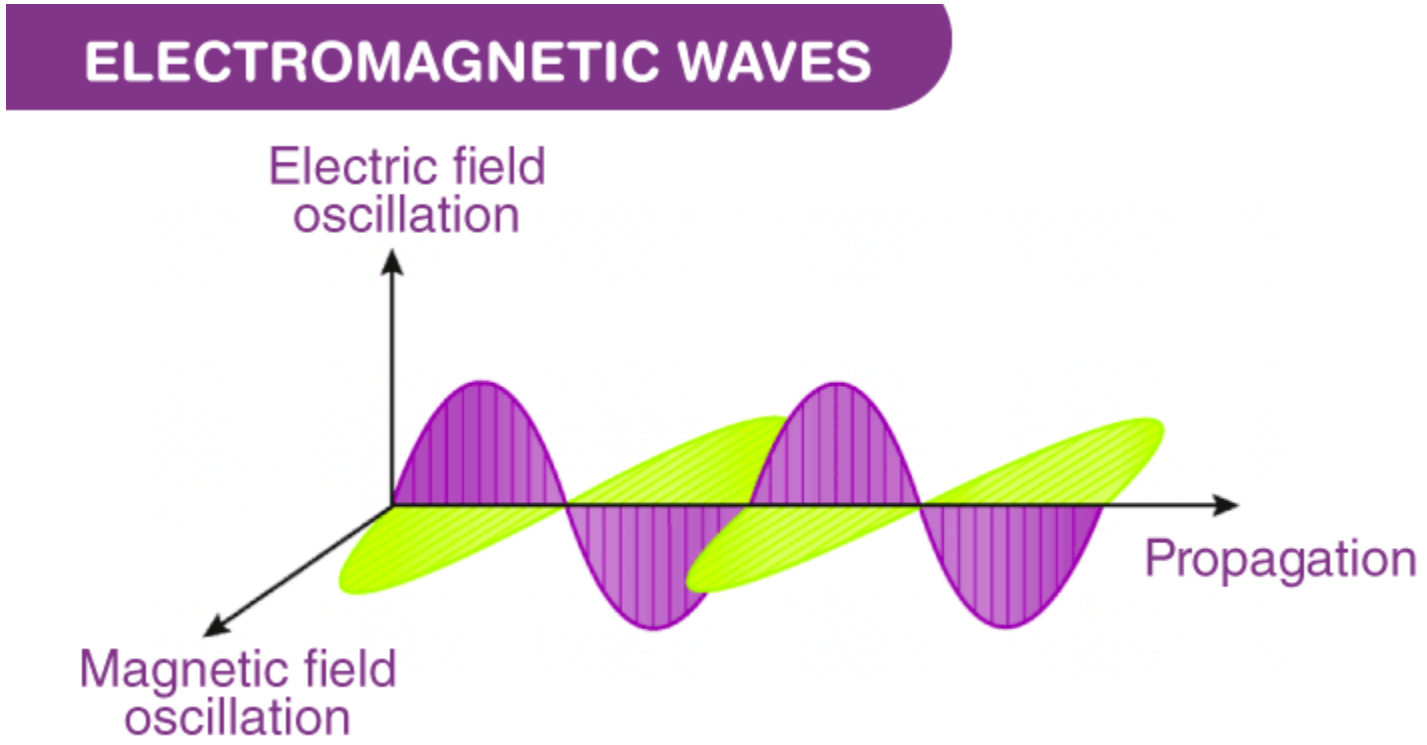
  Microwaves

  Infrared

  Satellite communication

- *Before that let's see what we need to transmit this electromagnetic signals?*

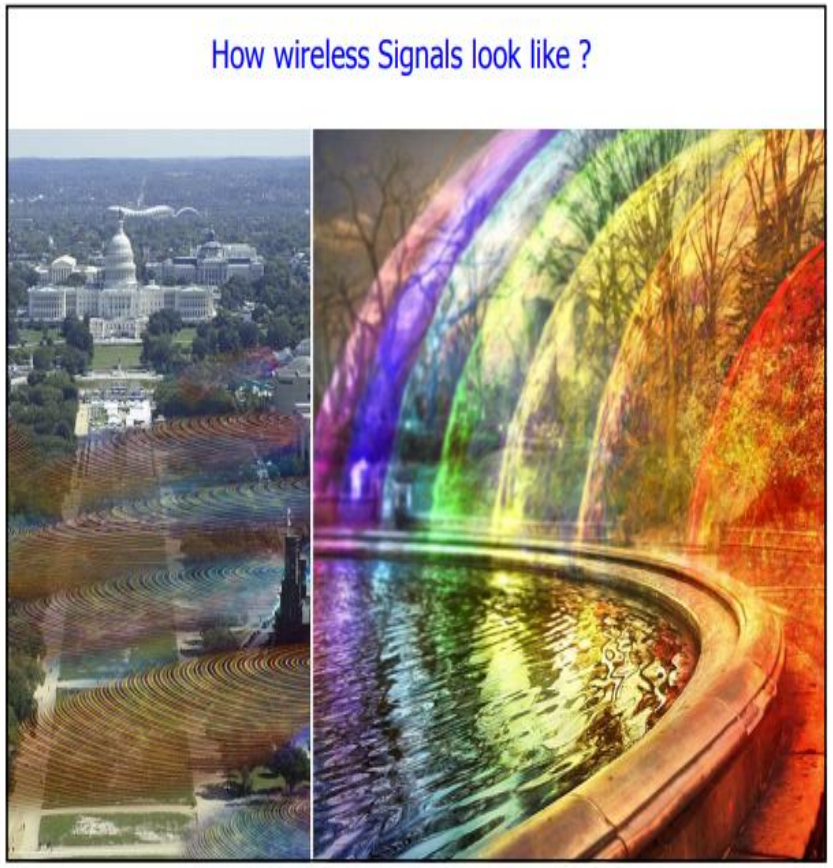
Electromagnetic Waves



How electromagnetic waves are formed?

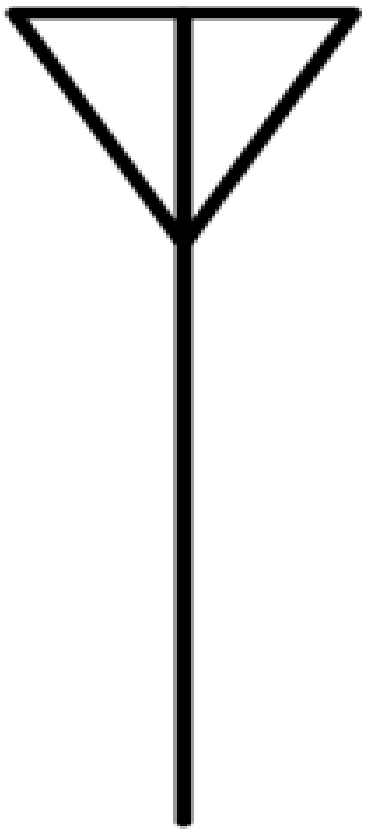
- an electric field is produced by a charged particle. A force is exerted by this electric field on other charged particles.
- The Magnetic field is produced by a moving charged particle
- So, the electromagnetic field is produced by an accelerating charged particle. Electromagnetic waves are nothing but electric and magnetic fields travelling through free space with the speed of light c

How wireless signals look like?



Antennas

electrical conductor used to radiate or collect electromagnetic energy



1)transmission antenna
2)reception antenna

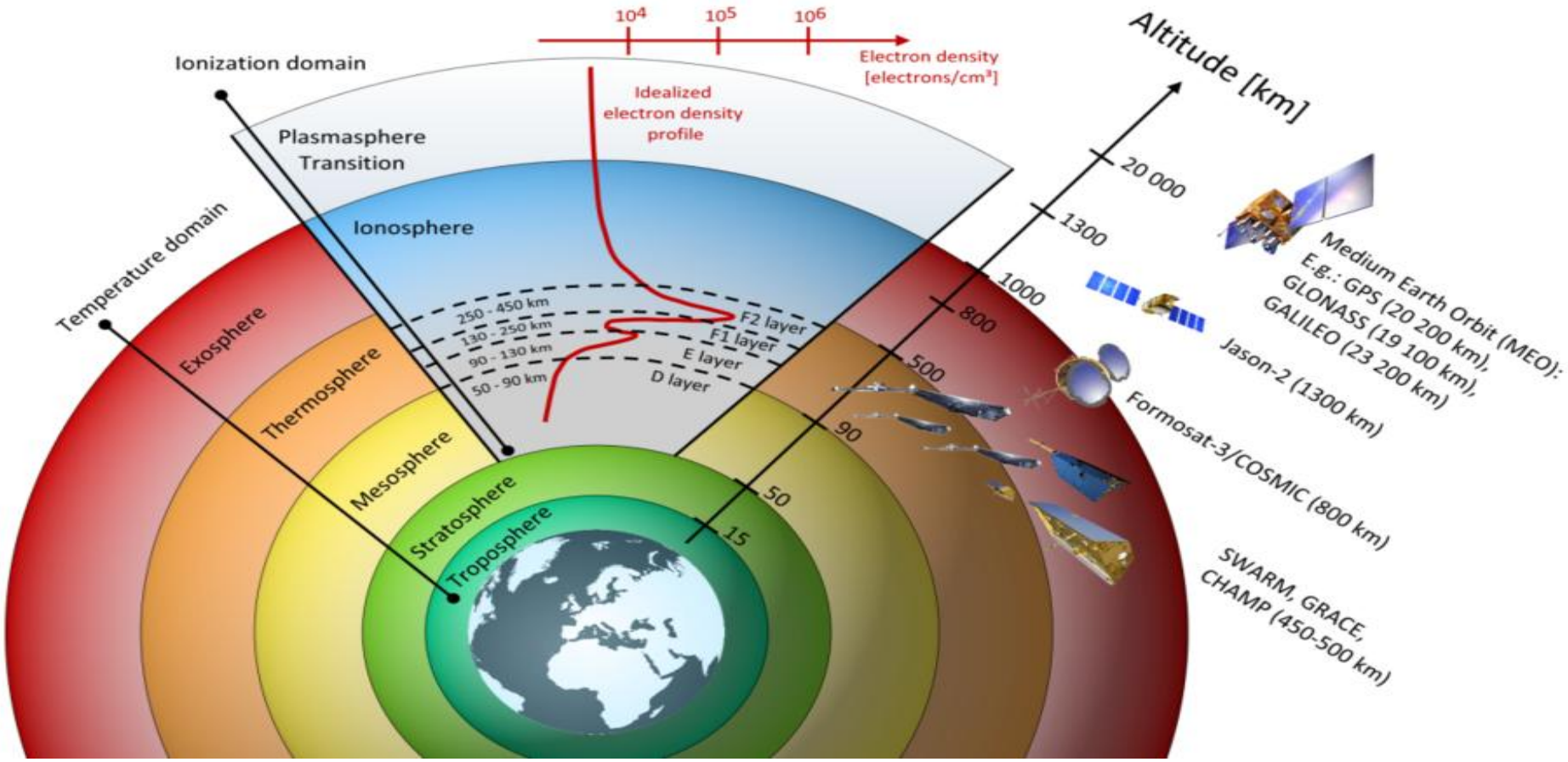
NOTE: in two way communication same antenna is often used for both purposes

Propagation Modes:

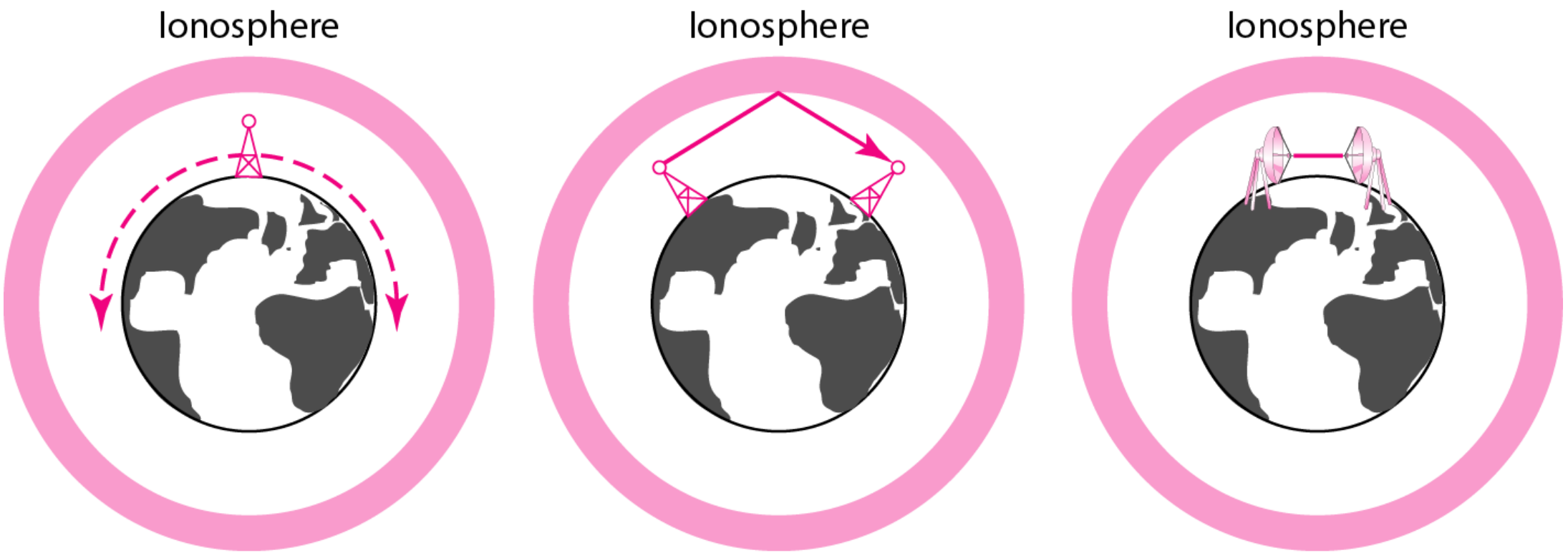
- There are three ways unguided signals can be travel from source to destination.
- These waves propagation can be classified depending upon the frequencies as

  - Ground waves propagation
  - Skywave propagation
  - Line-of-sight propagation

Layers of Earths Atmosphere



Propagation methods



Ground propagation
(below 2 MHz)

Sky propagation
(2–30 MHz)

Line-of-sight propagation
(above 30 MHz)

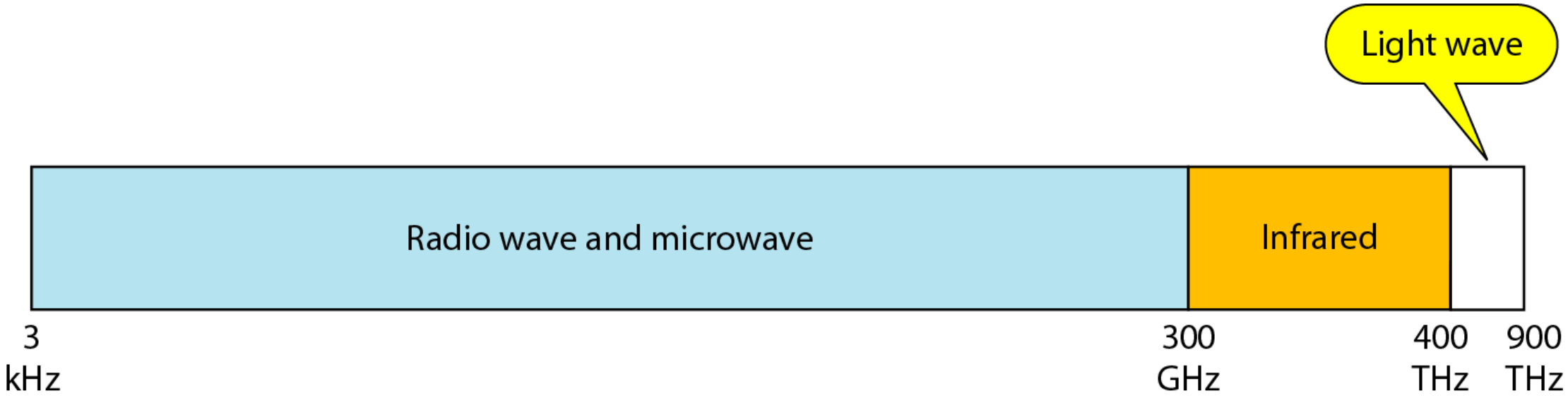
Propagation methods

- In **ground propagation**, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance.

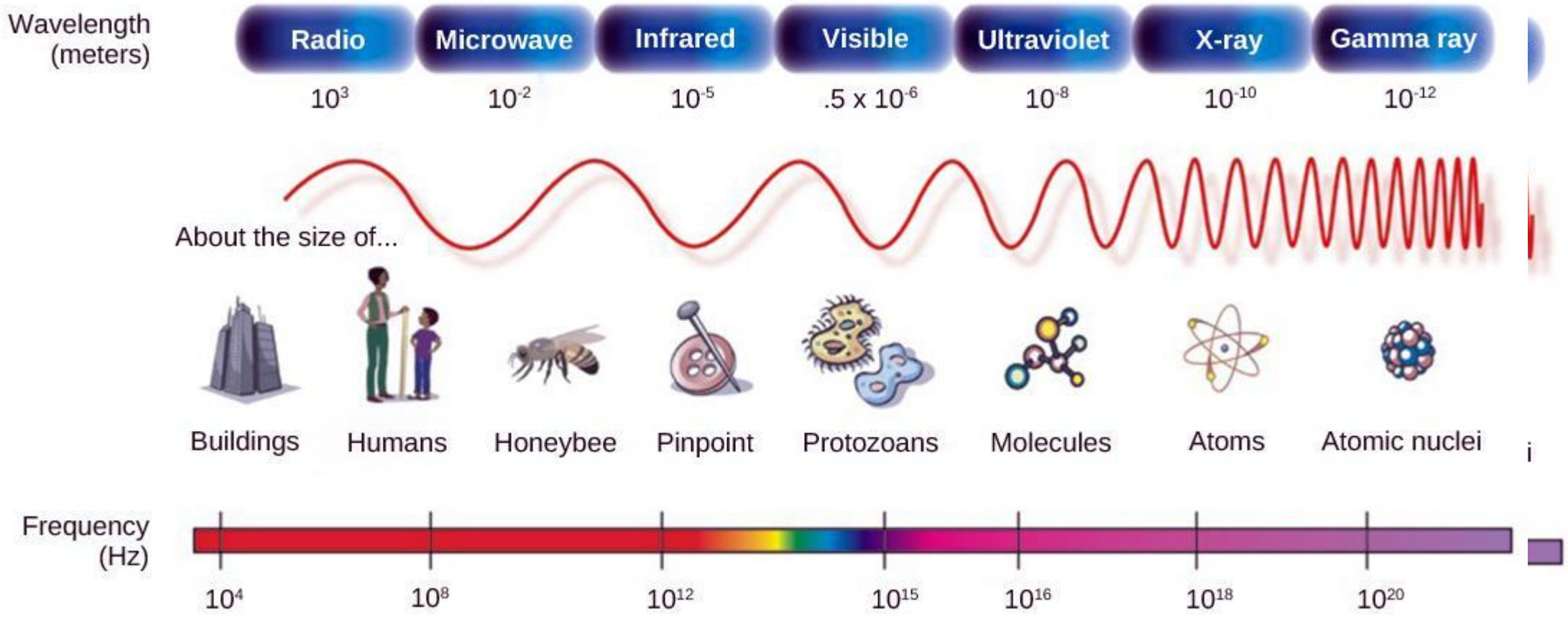
- In **sky propagation**, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower output power.

- In **line-of-sight propagation**, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of sight propagation is tricky because radio transmissions cannot be completely focused.

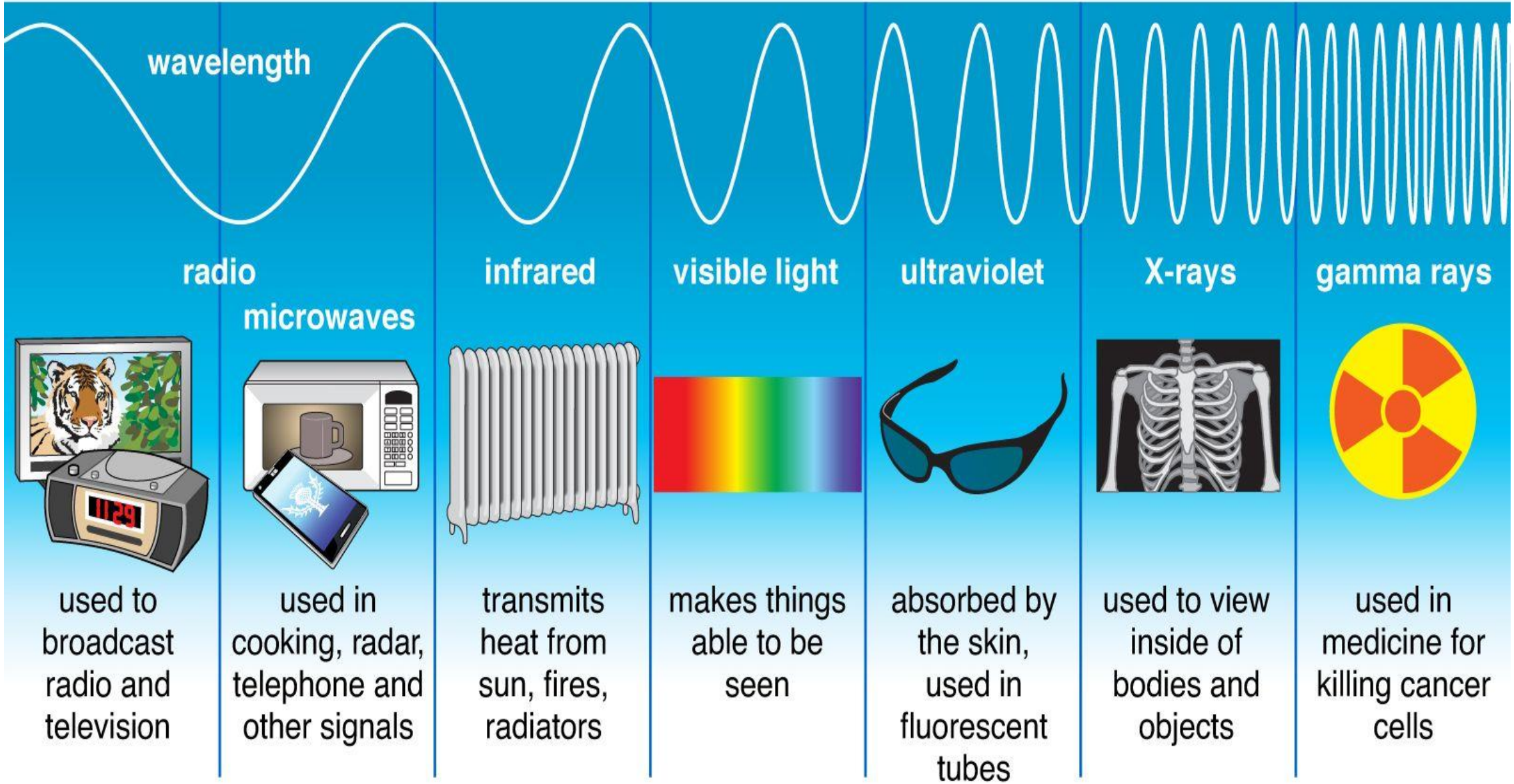
Electromagnetic spectrum for wireless communication



Electromagnetic spectrum for wireless communication



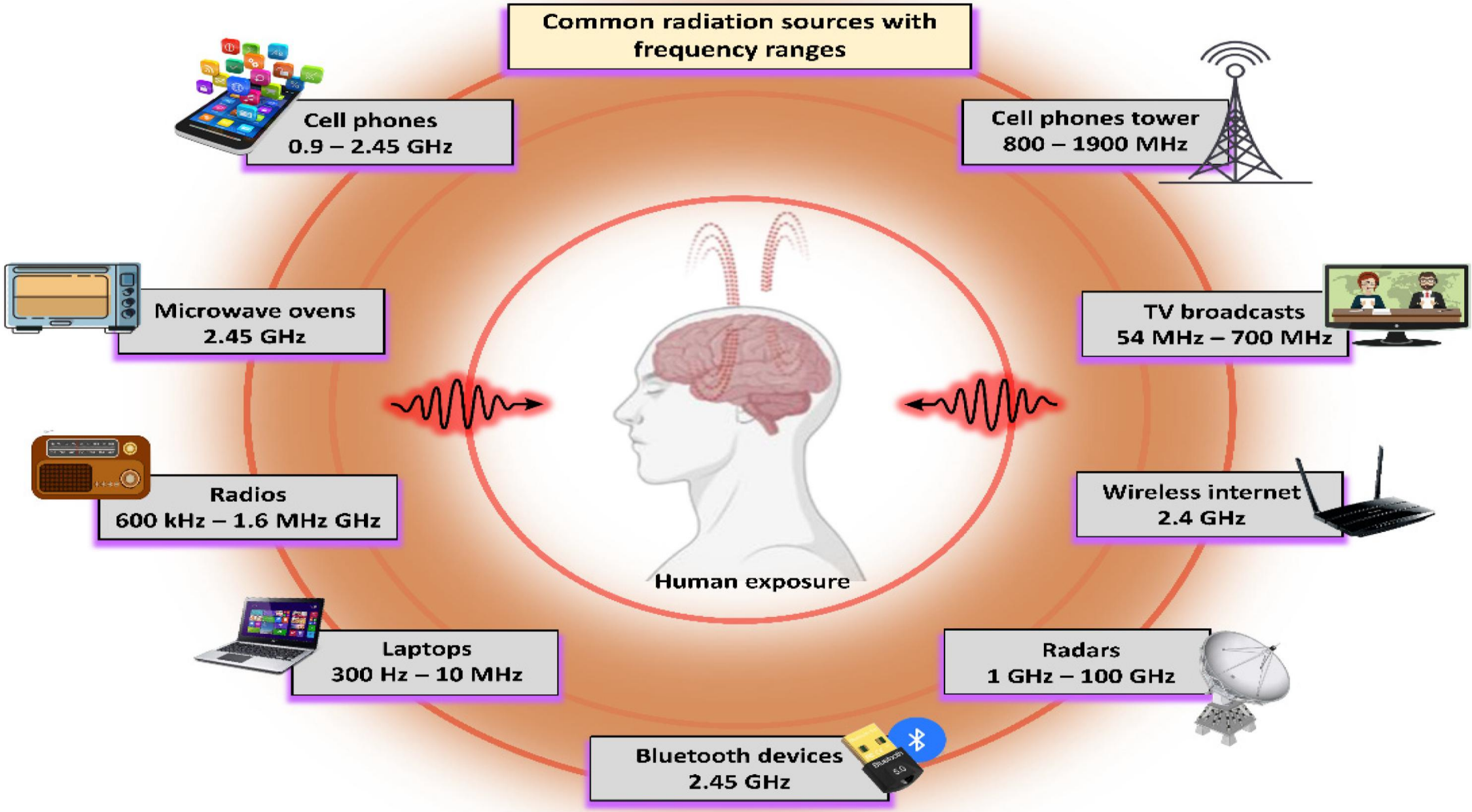
Types of Electromagnetic Radiation



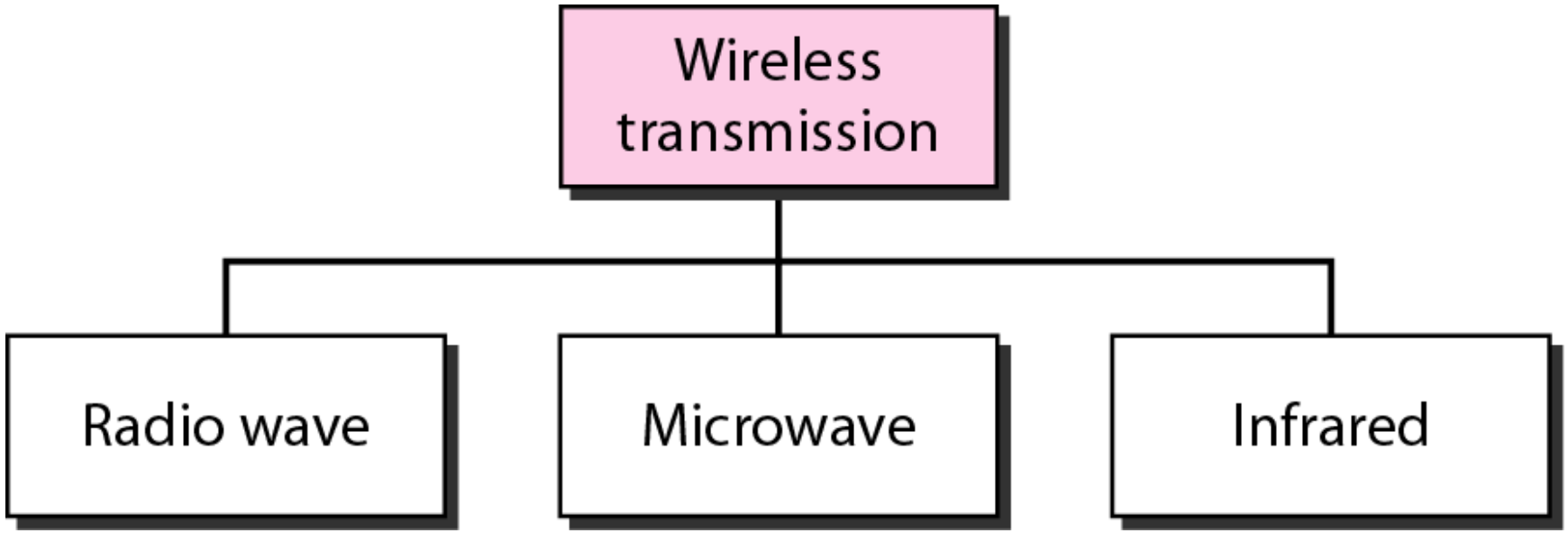
Frequency and signal travel relation.

- **Lower frequency** EM waves (longer wavelength) **travel farther** because they experience **less attenuation (signal loss) and can penetrate** obstacles better.
- **Higher frequency** EM waves (shorter wavelength) **travel shorter** distances because they **suffer higher attenuation, absorption, and scattering.**

Frequency Range	Example	Propagation Characteristics
Low Frequency (LF) - Below 300 kHz	AM Radio, Submarine Communication	Long-range, penetrates water and buildings
Medium Frequency (MF) - 300 kHz to 3 MHz	AM Radio	Moderate range, reflects off the ionosphere
High Frequency (HF) - 3 MHz to 30 MHz	Shortwave Radio	Long-distance via ionospheric reflection
Very High Frequency (VHF) - 30 MHz to 300 MHz	FM Radio, TV Broadcast	Line-of-sight, limited by Earth's curvature
Ultra High Frequency (UHF) - 300 MHz to 3 GHz	Mobile Phones, Wi-Fi	Shorter range, obstructed by buildings
Microwave & Millimeter Waves (3 GHz to 300 GHz)	Satellite, 5G, Radar	Short range, high data capacity, absorbed by atmosphere


Common radiation sources with frequency ranges
Cell phones
0.9 – 2.45 GHz
Cell phones tower
800 – 1900 MHz
Microwave ovens
2.45 GHz
TV broadcasts
54 MHz – 700 MHz
Radios
600 kHz – 1.6 MHz GHz
Wireless internet
2.4 GHz
Human exposure
Laptops
300 Hz – 10 MHz
Radars
1 GHz – 100 GHz
Bluetooth devices
2.45 GHz

Wireless transmission waves



Radio waves (3KHz to 1GHz)

- The type of electromagnetic waves which are transmitted in every direction of free space.
- The sending and receiving antenna are not aligned.
- It is used in Wide Area Network or Larger geographical areas.
- This wave has a 3 KHz to 1 GHz frequency range.
- It provides a higher data transmission rate.
- It is useful for multicasting when there is one sender and many receivers.

Omnidirectional Antenna

Omnidirectional Antennas Radiate Signals in all directions.

Omnidirectional antennas are widely used for **radio broadcasting antennas**, and in mobile devices that use **radio** such as **cell phones, FM radios, walkie-talkies, wireless computer networks, cordless phones, GPS**

Radio waves

- The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- Radio waves, particularly those waves that propagate in the sky mode, can travel long distances.
- This makes radio waves a good candidate for long-distance broadcasting such as AM radio

Advantages of Radio Waves :

- Free from land acquisition rights.
- Provides easy communication over difficult area.
- It can travel longer distance.
- Radio wave can penetrate walls, so they are widely used for both indoors and outdoors.
- Radio waves are Omni directional. It can propagate in all directional. (no need to aligned antenas)

Disadvantages of Radio Waves :

- Insecure communication.
- Easily influenced to weather effects.
- Radio wave can penetrate walls, so we cannot isolate a communication to just inside and outside a building.

Application of Radio Waves :

- The omni directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers.
  - 1. Am and FM radio
  - 2. GPS receivers
  - 3. Television broadcasts
  - 4. Cordless phones
  - 5. Police radio

Note

Radio waves are used for multicast communications, such as radio and television, and paging systems. They can penetrate through walls. Highly regulated. Use omni directional antennas

Microwaves (1GHz and 300 GHz)

- Electromagnetic waves having frequencies between 1GHz and 300 GHz are called micro waves.
- Microwaves are unidirectional.
- When an antenna transmits microwaves, they can be narrowly focused.
- sending and receiving antennas need to be aligned.
- A pair of antennas can be aligned without interfering with another pair of aligned antennas.

UniDirectional Antenna

Uninidirectional Antennas or Directional antennas Or Parabolic Antennas Radiate Signals in a particular direction.

in applications such as microwave relay links that carry telephone and television signals between nearby cities, wireless WAN/LAN links for data communications, satellite communications and spacecraft communication antennas. The other large use of parabolic antennas is for radar antennas,

Microwaves

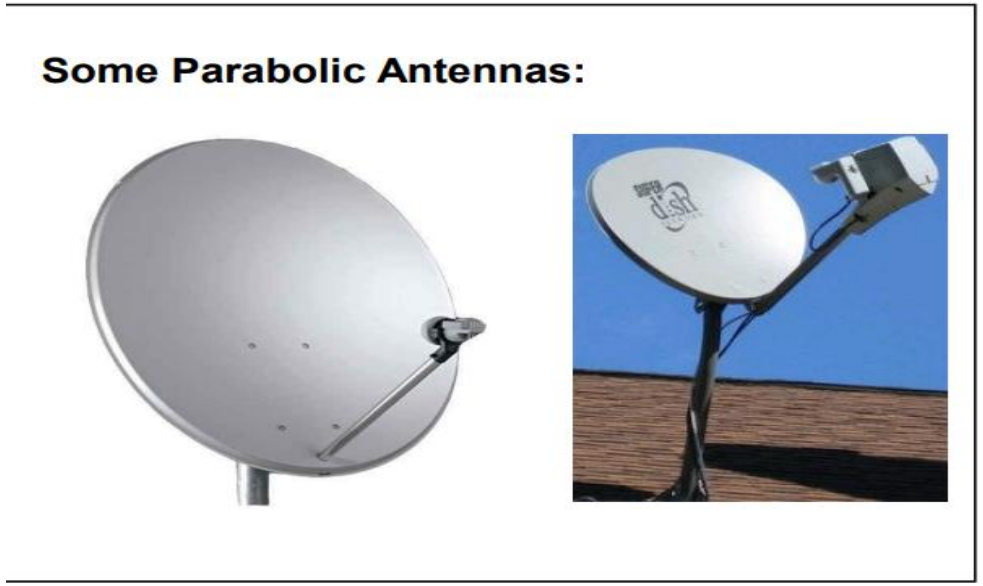
- Microwave uses line-of-sight propagation.
- Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall.
- The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves.
- Repeaters are often needed for long distance communication.

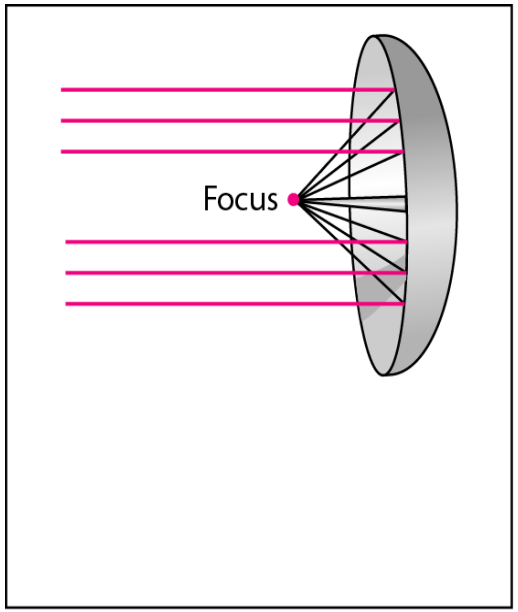
Microwaves

- Very high-frequency microwaves cannot penetrate walls.
- The microwave band is relatively wide, almost 299 GHz. Therefore wider sub-bands can be assigned, and a high data rate is possible.
- Use of certain portions of the band requires permission from authorities.

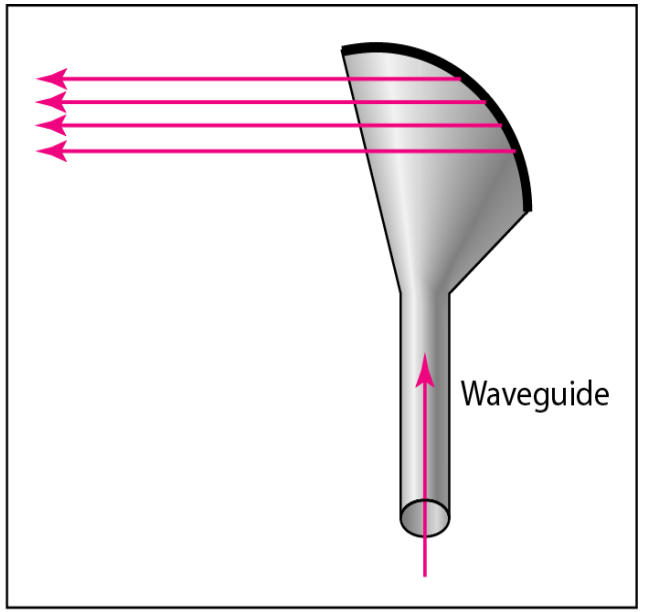
Microwaves

- Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn .





a. Dish antenna



b. Horn antenna

Advantages of Micro Waves:

- 1. Micro waves are **unidirectional,** and sending and receiving antenna need to be aligned, so they are not interfering with another pair of aligned antenna.
- 2. The micro wave's band is relatively wider, compared to the radio wave band. When this band is divided into sub bands, the sidebands are also wider, leading to a higher data rate for digital communications.
- 3. Micro waves are relatively inexpensive and simple to install.

Disadvantages of Micro Waves :

- . The micro waves travel in a straight line, if the towers are too far apart, the earth will get in the way.
- Consequently, repeaters are often needed for long distance communication periodically.
- 2. Very high frequency micro waves can not able to penetrated walls. Its disadvantage if receivers are inside the buildings.

Application of Micro Waves :

- 1. Cellular Phones
- 2. Satellite Networks
- 3. Wireless LANS

Note

Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

Higher frequency ranges cannot penetrate walls.

Use directional antennas - point to point line of sight communications.

Infrared signals(300 GHz to 400 THz)

- Electromagnetic waves having frequencies from 300 GHz to 400 THz are called Infrared waves.
- Infrared waves are widely used for short-range communication.
- The remote controls used on televisions, VCRS, and stereos all use infrared communication.
- Infrared waves use line-of-sight propagation.

Advantages of Infrared Waves :

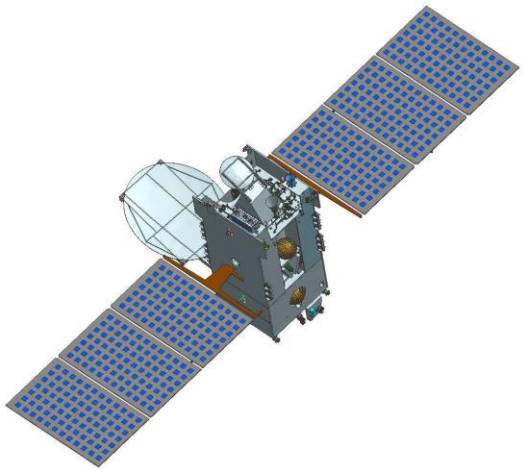
- . Infrared waves are relatively directional, cheap, and easy to build.
- 2. Infrared waves having a high frequency, so they are not able to penetrate the walls.
    - So, Infrared system in one room will not interfere with a similar system in adjacent room.
- 3. Infrared waves are useful for short range communication.
- 4. It is more secure against taping.
- 5. It is useful to communicate wireless keyboard and mouse with the PC by using Infrared port.

Disadvantages of Infrared Waves :

- Infrared waves are useless for long range communication.
- They do not pass through solid objects.
- We cannot use infrared waves outside buildings because the sun's ray contains infrared that can interfere with the communication

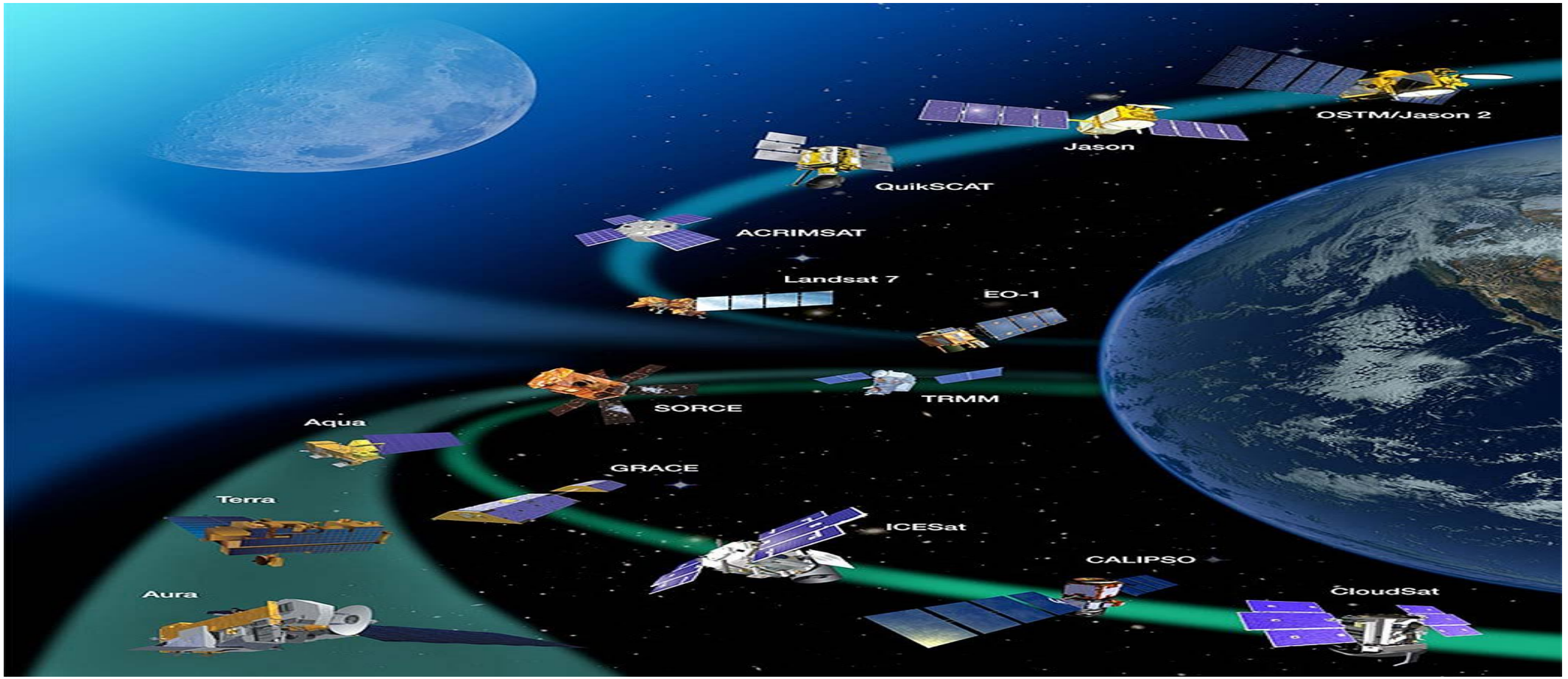
Satellite Communication

- **Satellite**
- The satellite is man-made equipment that is placed in orbit around the earth.
- It is the wireless receiver /transmitter that is launched by rocket and placed in orbit.



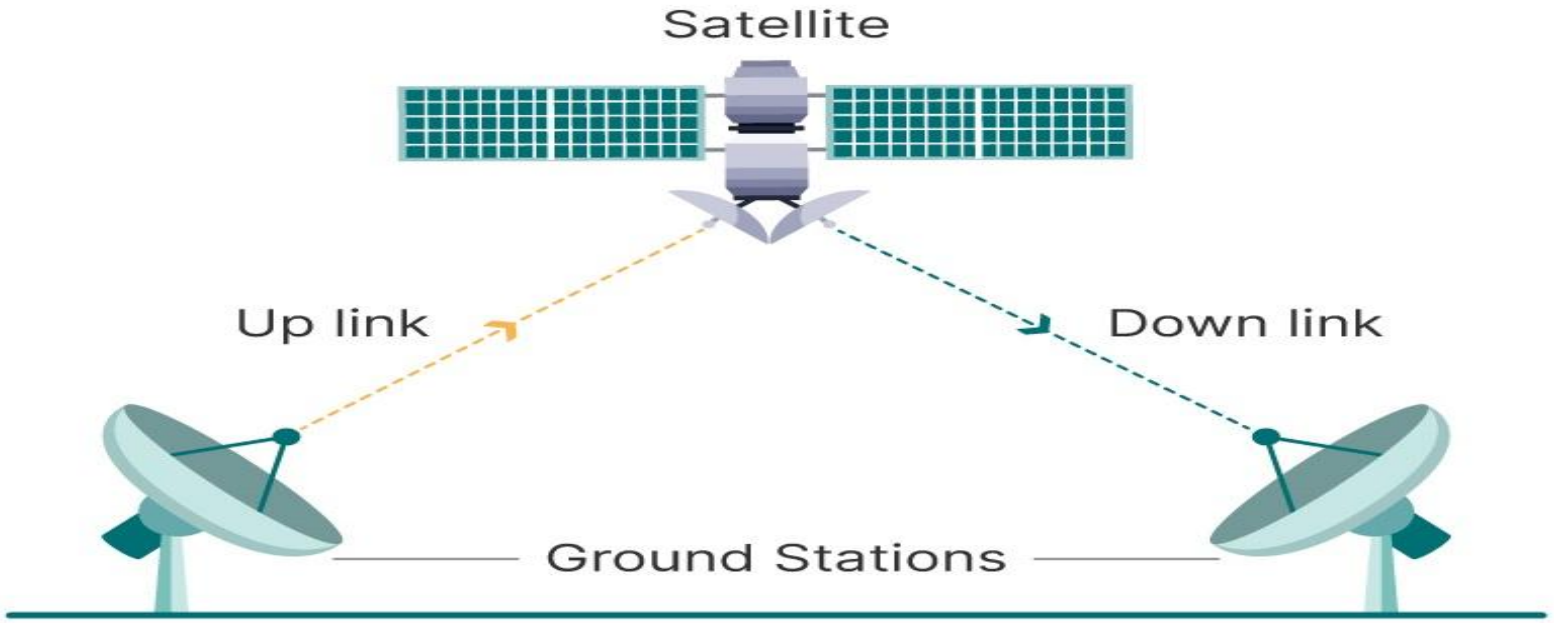
India's first communication satellite was Ariane Passenger Payload Experiment (APPLE), which was launched on June 19, 1981. It was an experimental satellite designed and built by ISRO.

Satellite


OSTM/Jason 2
Jason
QuikSCAT
ACRIMSAT
Landsat 7
EO-1
TRMM
SORCE
Aqua
GRACE
Terra
ICESat
CALIPSO
CloudSat
Aura

Satellite Communication

- Satellite communication involves transmitting signals between Earth-based stations via satellites in orbit.
- Used for TV broadcasting, GPS, internet services, weather forecasting, military applications, etc.



How it works

- Ground stations send radio signals called "uplinks" to the satellite.
- The satellite receives the signals, strengthens them, and then re-transmits them back to Earth.
- These signals back to Earth are called "downlinks".
- The satellite enables communications to be established over large distances - well beyond the line of sight.

How it works

- Satellite transmission is similar to line-of-sight microwave transmission, where signals travel in straight lines.
- A satellite acts as both an antenna (for receiving signals) and a repeater (for amplifying and retransmitting signals).
- On Earth, terrestrial microwave communication is limited by the curvature of the Earth, restricting direct communication to a few hundred kilometers.
- A satellite placed in orbit overcomes this limitation by relaying signals over much longer distances, enabling global communication.

Advantages of Satellite Communication

- Global coverage, no geographical barriers. i.e covers large area of earth.
- In expensive compared to the cable transmission.
- Reliable and secure communication.
- Ideal for remote and rural areas.
- High bandwidth and efficient data transmission

Disadvantages of Satellite Communication

- High initial cost for satellite deployment.
- Signal latency, especially in GEO satellites.
- Prone to space weather effects (solar storms, space debris).
- Limited lifespan (typically 10-15 years).

Applications of Satellite Communication

- Telecommunication: Mobile and broadband internet services.
- Broadcasting: DTH TV, radio, satellite news gathering.
- Navigation: GPS, GLONASS, Galileo, IRNSS.
- Remote Sensing: Weather forecasting, disaster management, environmental monitoring.
- Military & Defence: Surveillance, secure communication, missile guidance.

Frequency Bands

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3–30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30–300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz–3 MHz	Sky	AM radio
HF (high frequency)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3–30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30–300 GHz	Line-of-sight	Radar, satellite

Network Devices

- *A hardware devices used to connect computers, printers, fax machines and other electronic devices to a network is called network devices.*
  - They allow us to connect large number of nodes to be connected to the network.
  - They extend the distance over which a network can extend.
  - They localize traffic on the network.
  - They isolate network problems so that they can be diagnosed more easily.

Network Devices

- **1.Intranetwork devices(LAN)**
  - **Repeater**
  - **Hub**
  - **Bridge**
- 2. ***Internetworking Device(WAN)***
  - ***Switch***
  - ***Router***
  - ***Gateway***
  - ***Modem***
  - ***Access point***

How the data Travels?

1. The data is broken down into packets by the network interface card (NIC) on your PC.
2. The packets are then sent to the switch that connects your PC to the network.
3. The switch examines the destination address in each packet and forwards it to the appropriate port to reach the destination device.

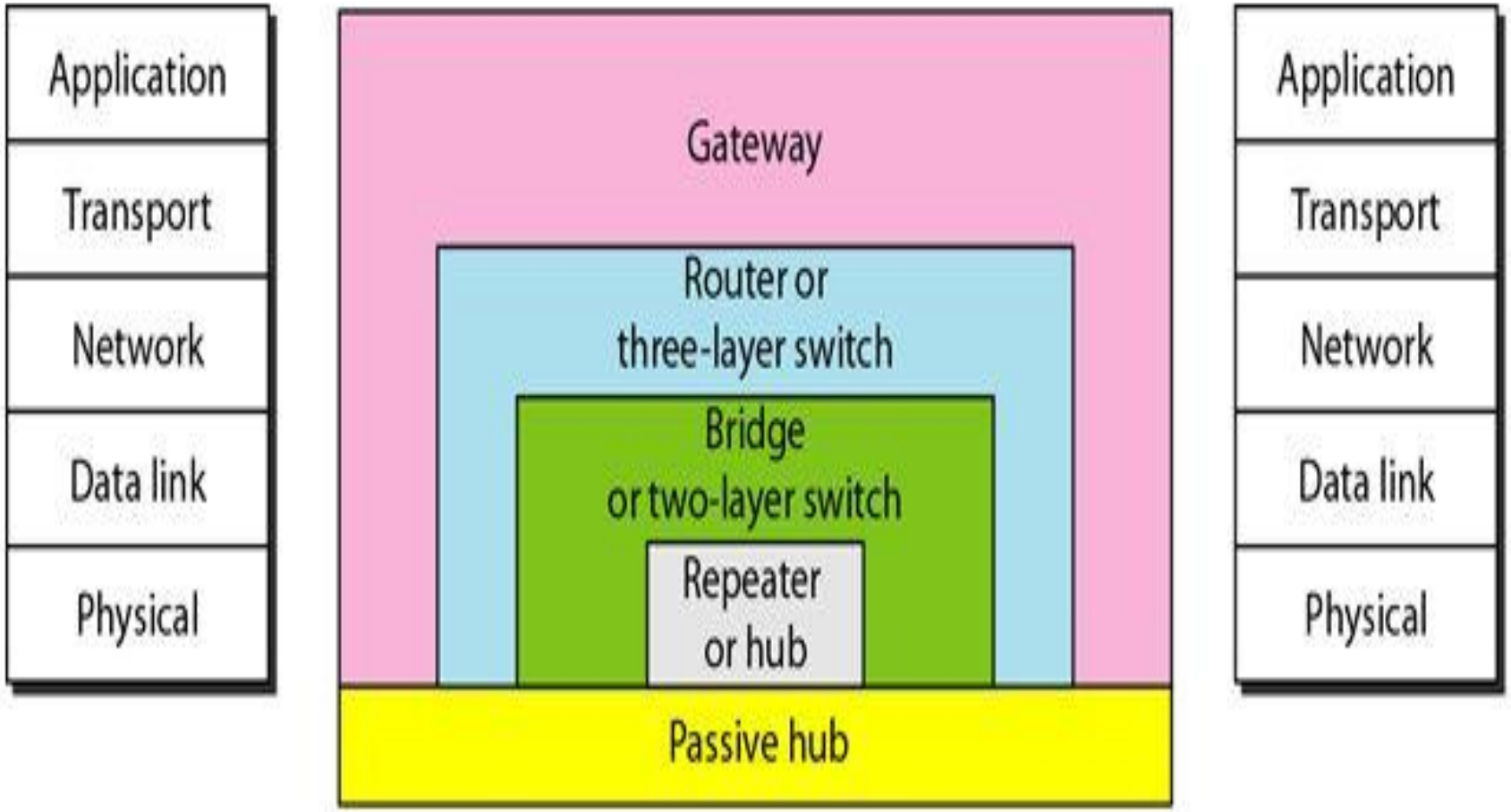
How the data Travels?

- 4.If the destination device is not on the same network as your PC, the packet will be sent to a router.
- 5.The router examines the destination IP address and determines the best path to send the packet to reach the server.
- 6. packet is then sent through various switches and routers on the way to the server, with each device examining the destination address and forwarding the packet to the next device on the path.

How the data Travels?

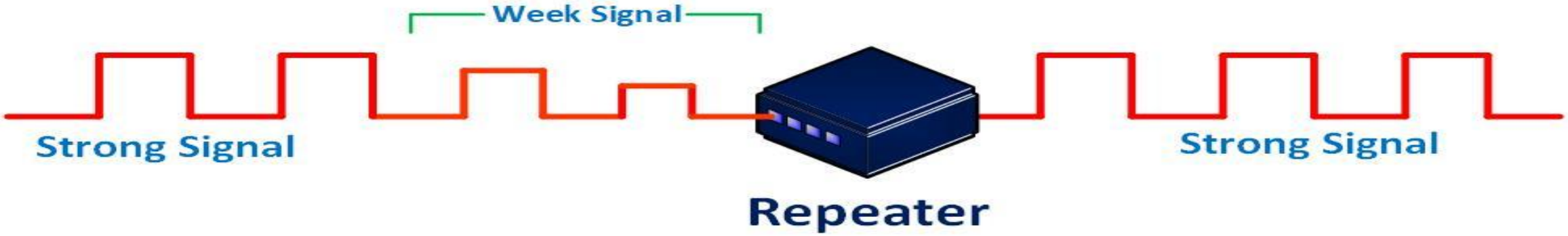
1. Once the packet reaches the server, it is reassembled by the server's NIC and the data is extracted from the packet.
2. The server then sends a response back to your PC in the same way, with the data broken down into packets and sent through the network devices back to your PC.

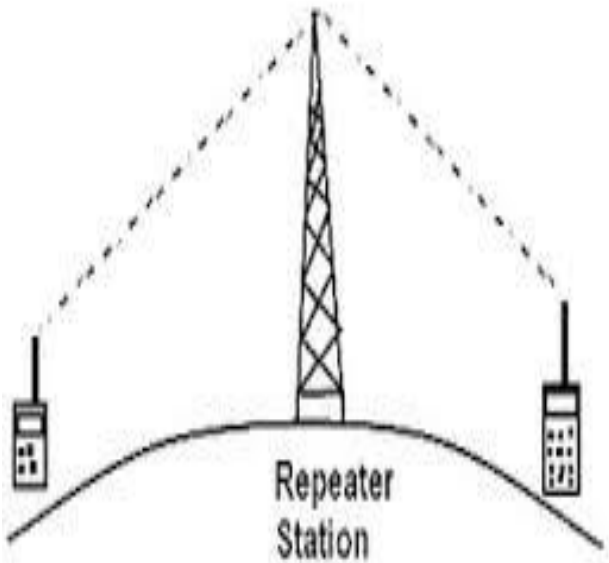
Network Devices at different layers in TCP IP MODEL



Repeaters

- The transmission distance of network media, such as copper or fiber optic cable, is limited by factors such as signal attenuation, noise, and interference.
- When a signal is transmitted over a network medium, it gradually loses strength as it travels further away from the source.
- resulting in data loss and network performance issues.





VHF UHF Repeater

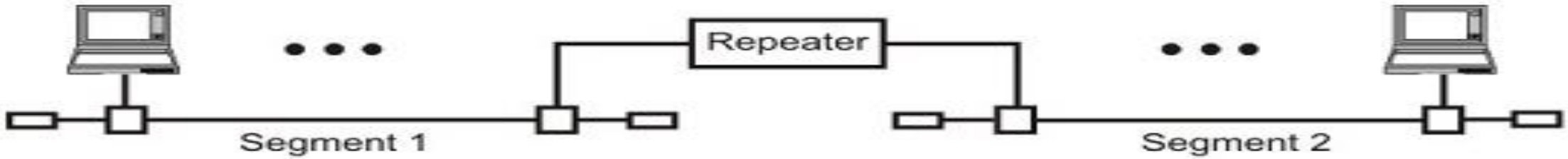


Figure 6.1.1 Repeater connecting two LAN segments

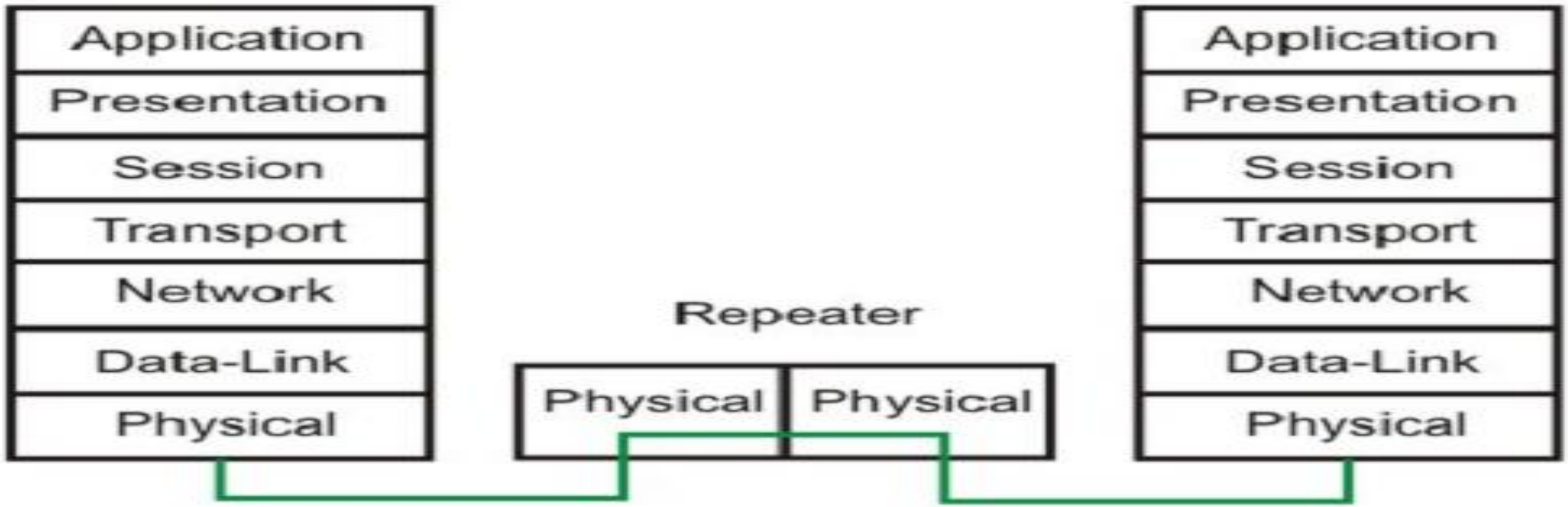


Figure 6.1.2 Operation of a repeater as a level-1 relay

Repeaters

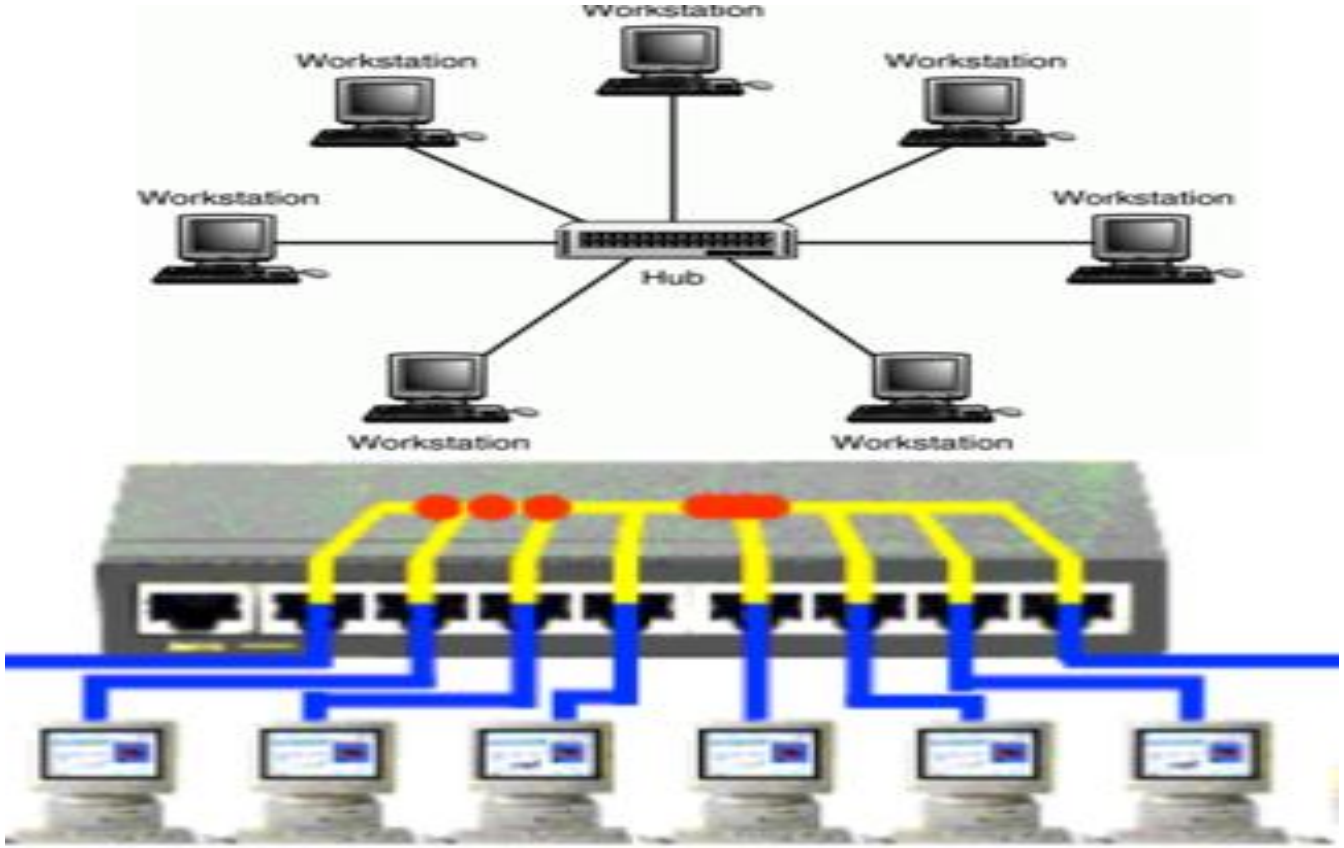
- Repeaters operate at the physical layer of the network and are used to extend the range of network signals without affecting their quality.
- Repeaters receive the incoming signal, regenerate it, and retransmit it on the next segment of the network, allowing the signal to reach devices that are farther away.
- Repeaters are commonly used in wired networks such as Ethernet and fiber optic networks, as well as wireless networks such as Wi-Fi and cellular networks.

Give the reason: Repeater are not Amplifiers.

Note: Repeater and Amplifier have absolutely different functionalities.

- Repeater regenerates the deteriorated signal, whereas
- amplifier enhances the amplitude of the input signal.

HUB


Workstation
Workstation
Workstation
Workstation
Workstation
Hub
Workstation
Workstation

Hub

- a hub is a device that connects multiple devices together to form a network.
- Hubs operate at the physical layer of the network.
- A hub receives data from one device and broadcasts it to all other devices that are connected to it.
- This means that all devices on the network receive all data transmissions, even if the data is intended for only one device.

Hub

- As a result, the network can become congested, leading to slower network performance and increased data collisions.
- Hubs can be used in both wired and wireless networks.
- In a wired network, a hub is typically used to connect multiple devices to a single Ethernet network segment
- There are main 3 types of hubs:
  - Passive Hub
  - Active Hub
  - Intelligent Hub

PASSIVE HUB

- A passive hub is just like a connector.
- It connects wire coming from different segments or simply combines the signals of network segments.
- There is no signal processing or regeneration.
- For example, if a segment normally allows a reliable transmission distance of 200 meters, the distance between a passive hub and a device can be only 100 meters.
- Passive hub merely acts as a connection point and does not amplify or regenerate the signal.
- Passive hubs do not require electrical power to run.

Active Hub

- Active hubs have electronic components that regenerate or amplify signals (depending of type of hub).
- Because of this, the distance between devices can be increased.
- The hub that regenerates the electrical signal and sends it to all the computers connected to it.
- It is often called a multiport repeater.
- Active hub requires electrical power to run.

Intelligent Hub

- In addition to signal regeneration, intelligent hubs perform some network management and intelligent path selection.
- A switching hub chooses only the port of the device where the signal needs to go, rather than sending the signal along all paths.

Advantages of Hub

- Active hub regenerates signals, it increases the distance that can be covered by LAN.
- Hubs can also be connected locally to a maximum of two other hubs, thereby increasing the number of devices that can be attached to the LAN.
- Active hubs are usually used against attenuation, which is a decrease in the strength of the signal over distance.

Disadvantages of Hub

- It can't filter information.
- It does not have a mechanism to reduce the network traffic
- It runs half-duplex mode
- It can't connect different type of network architecture such as a token ring and Ethernet
- Most Hubs are unable to utilise Virtual LANS.

HUB summary slide

- Physical layer device
- multi port repeater
- Simple receive and Forward
- No filter (broadcast)
- Collision high

Switch

- It works on Datalink layer of OSI model(Packets=frames, MAC address).
- It provides bridging with greater efficiency.
- They have buffer for each link to which it is connected.

Switch

Switch

- Switches connect devices on a local area network (LAN).
- Such devices are attached to the switch by cables that plug into a port on the switch.
- When a device sends data through the network, the switch receives the data packet and examines the packet's destination Media Access Control (MAC) address.
- the MAC address is a unique label for each device on the network.

Working of Switch

- The switch then determines which port the destination device is connected to and forwards the packet to that port.
- If the destination device is not on the same LAN, the switch forwards the packet to the appropriate router to send it to the intended destination.
- The switch normally has a buffer for each link to which it is connected.
- When it receives packets, it store the packets in buffer of the receiving link and check address to find the out going link.
- If outgoing link free then switch sends the frames(datalink layer) to that particular link.

Working of Switch

- If the destination device is on the same network as the sender, the switch forwards the packet directly to that device.
- If the destination device is on a different network, the switch forwards the packet to the router that connects the two networks.
- The switch keeps track of the MAC addresses of devices connected to each port and updates its forwarding table accordingly.

Types of Switch

- Store-and-forward Switches
- Cut-through Switches:
- Back Pressure Switches:
- Unmanaged switches:
- Workgroup Switch:

1. Store-and-forward Switches :

- This switch stores the entire data packet in its buffer before forwarding it to the destination device.
- If the packet is corrupted or contains errors, the switch discards the packet.
- Good packets are forwarded to the correct segment
- Detect more errors than the cut-through variety
- Impose a small delay in packet throughput

2. Cut-through Switches:

- This switch forwards data packets as soon as the destination address is received, without waiting for the entire packet to be received.
- Examine only the first few bytes of the packet to obtain the source and destination addresses
- The packets are then passed through to the destination segment without checking the rest of the packet for errors
- Invalid(corrupted) packets can still be passed onto other segments
- There is little delay involved in packet throughput

3. Back Pressure Switches:

- Switches often have buffering of packets.
- This is done so when a packet arrive for a busy port, the packet is temporarily stored till the port becomes free.
- When the buffer becomes full, packets become lost.
- Back pressure switches overcome this problem by sending the overflow packets back to the workstation.
- This effectively slows the workstation transmission rate, and hence slows the arrival of new packets at the port

4. Unmanaged switches:

- This is a basic switch that requires no configuration and is plug-and-play.
- This switches are inexpensive.
- It's ideal for small networks with a limited number of devices.
- Lacks feature of management
- used in home networks or wherever a few more ports are needed, such as at your desk, in a lab, or in a conference room.`

5. Workgroup Switch:

- Similar to unmanages except it provides management of unit.
- It gives greater security and more features and flexibility because you can configure them to custom-fit your network.
- With this greater control, you can better protect your network and improve the quality of service for those who access the network.

Advantages

❑**Increased speed:**

➢Switches provide higher data transfer rates than hubs because they offer dedicated bandwidth for each device.

➢This means that each device can communicate with the network at the full speed of its network interface, without being slowed down by other devices on the network.

❑**Improved security:**

➢Switches help to improve network security by preventing packets from being sent to unintended devices.

➢This is achieved through MAC address filtering and VLAN segmentation, which restrict access to the network and separate devices into logical groups.

Advantages

- **Reduced network congestion:** Switches can help to reduce network congestion by directing data packets only to the intended destination, rather than broadcasting them to all devices on the network, as is the case with hubs.
- **Efficient use of network resources:** Switches use a store-and-forward or cut-through approach to forwarding data packets, which helps to reduce network latency and improve network performance.

Dis-advantages

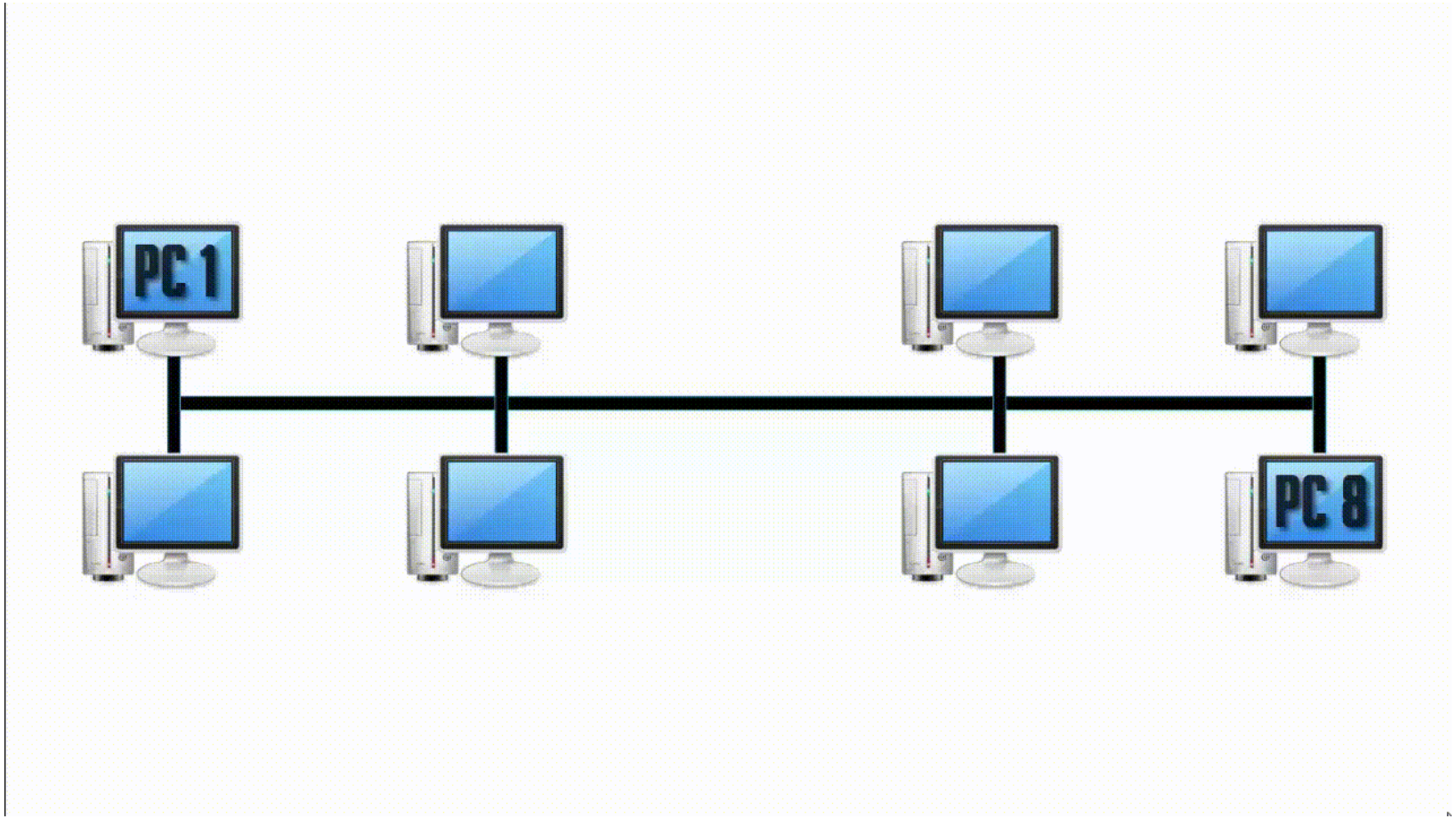
- **Cost**: Network switches can be more expensive than other networking devices, such as hubs or routers.
- **Complexity:** Advanced network switches can be complex to configure and manage, requiring specialized knowledge and expertise.
- **Single point of failure:** If a network switch fails, it can affect all devices connected to it, potentially causing network downtime or data loss.

Bridge

- Bridges operate in both the physical and data link layer of OSI model.
- Bridge basically works in a bus topology.
- Bridge in networking divides a LAN into multiple segments.
- It is used to connect two or more LANs.
- It has a single input and single output port so; it is 2 port devices.
- Bridge operates at the data link layer, so it accesses the physical addresses of all devices connected to it.

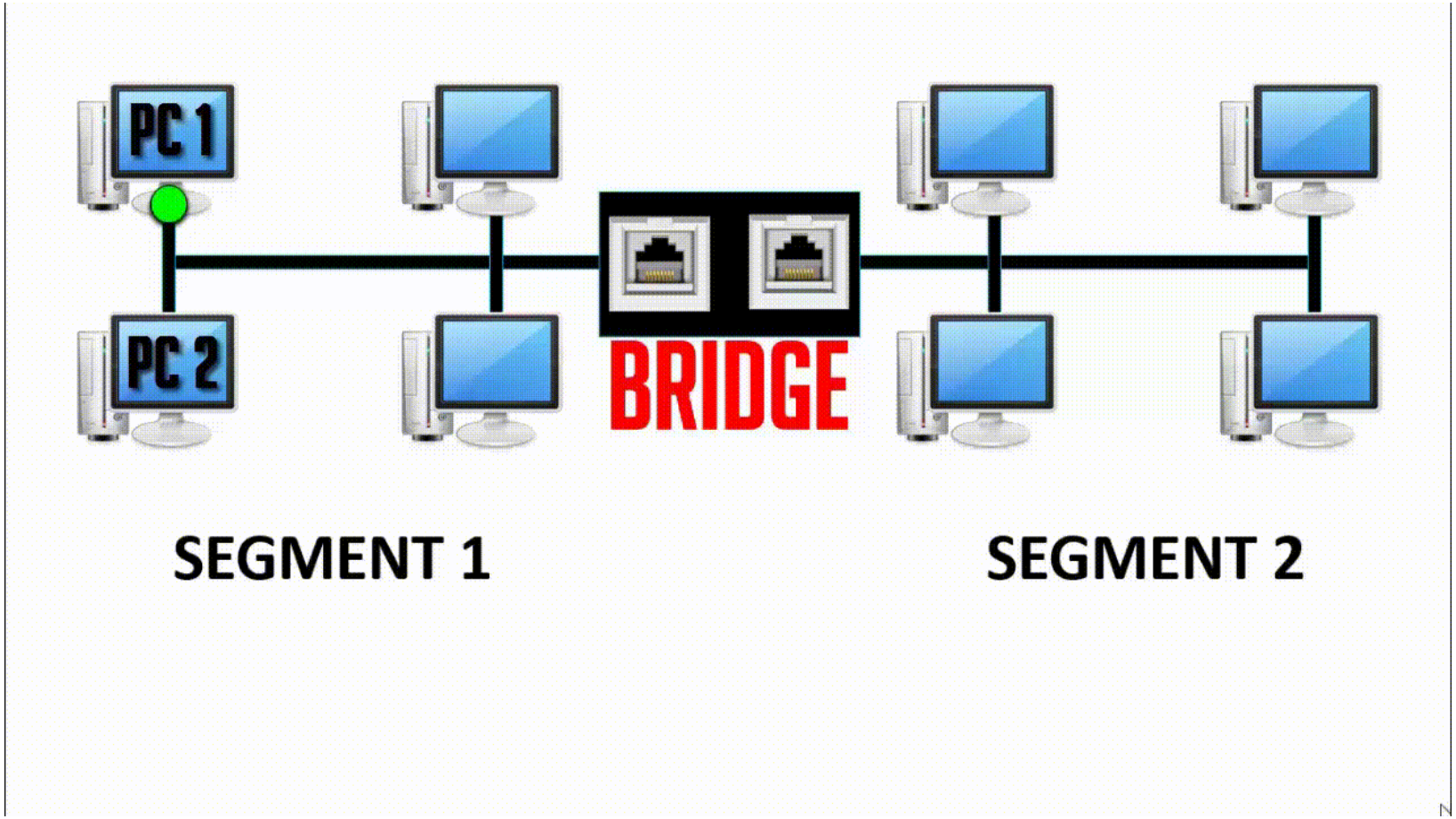
LAN WITHOUT BRIDGE

- PC-1 wants to send data to PC-8



LAN WITH BRIDGE

Case-1: PC-1 wants to send data to PC-2



LAN WITH BRIDGE

Case-2: PC-1 wants to send data to PC-8

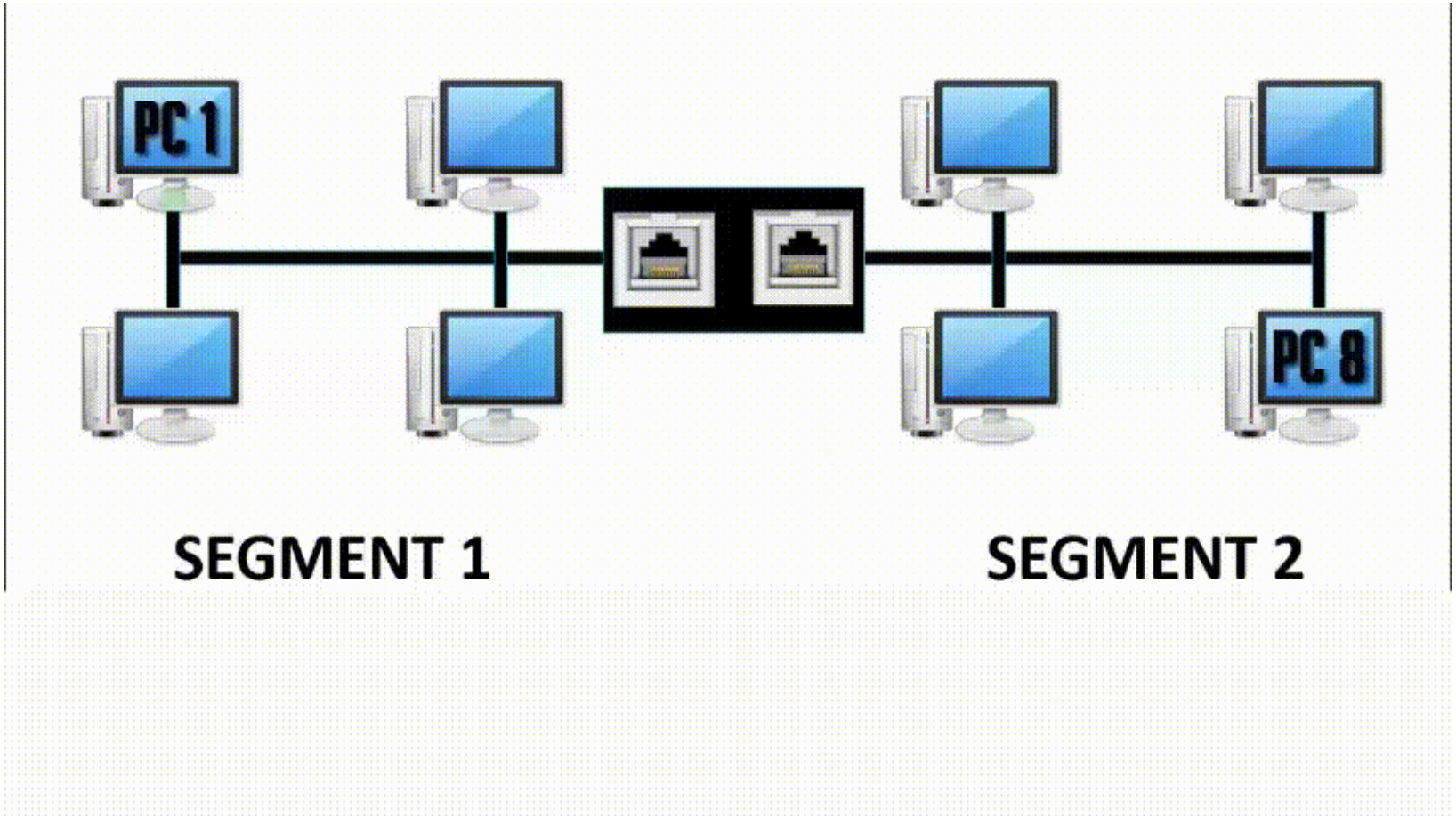
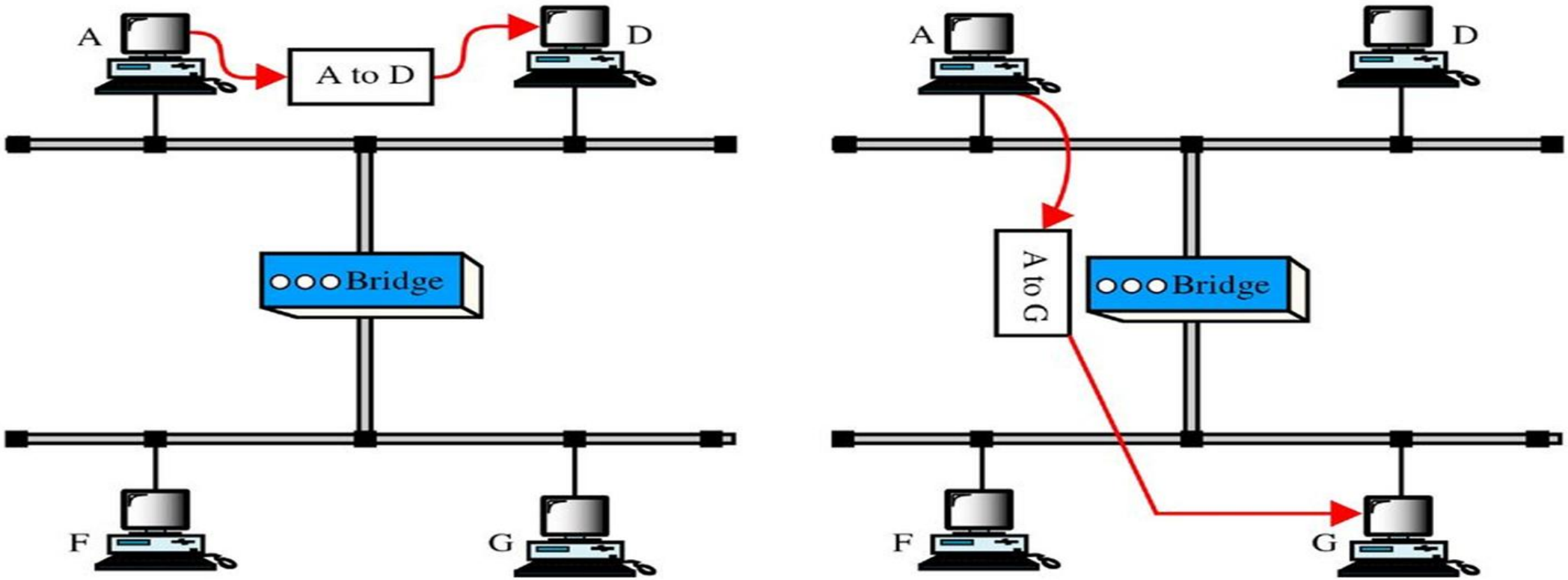


Figure 17-8

Function of a Bridge



a. A packet from A to D

b. A packet from A to G

Bridge

- A bridge's primary function is to filter traffic between network segments.
- When a frame enters into bridge, bridge regenerates the signal and it checks the destination address and forwards signal to the destination segment.
- As a bridge receive frame, it reads the address in the frame and compare that address with all address available in table.

Working of Bridge

- When the bridge finds correct match, it find to segment the station belongs and send the frame only to that segments.
- Bridge must have a look up table, which contains the physical addresses of every station connected to it.
- The table also indicate device or station belongs to which segment.
- There are three types of bridges: simple, learning/ transparent, and multiport.

Simple Bridge

- Simple bridges are the least expensive types of bridge.
- A simple bridge links two segments and contains a table that lists the address of all the stations included in each segment.
- Before a simple bridge can be used, operator must program the addresses of every station manually.
- Whenever a new station is added or removed, the table must be updated.
- Installation and maintenance of simple bridges are time consuming

Learning/Transparent Bridge

- A bridge builds its table of station addresses on its own, as it performs its bridging function.
- When the learning bridge is first installed, its table is empty.
- As it encounters each packet, looks at both, the destination and the source addresses.
- It checks the destination to decide where to send the packet.

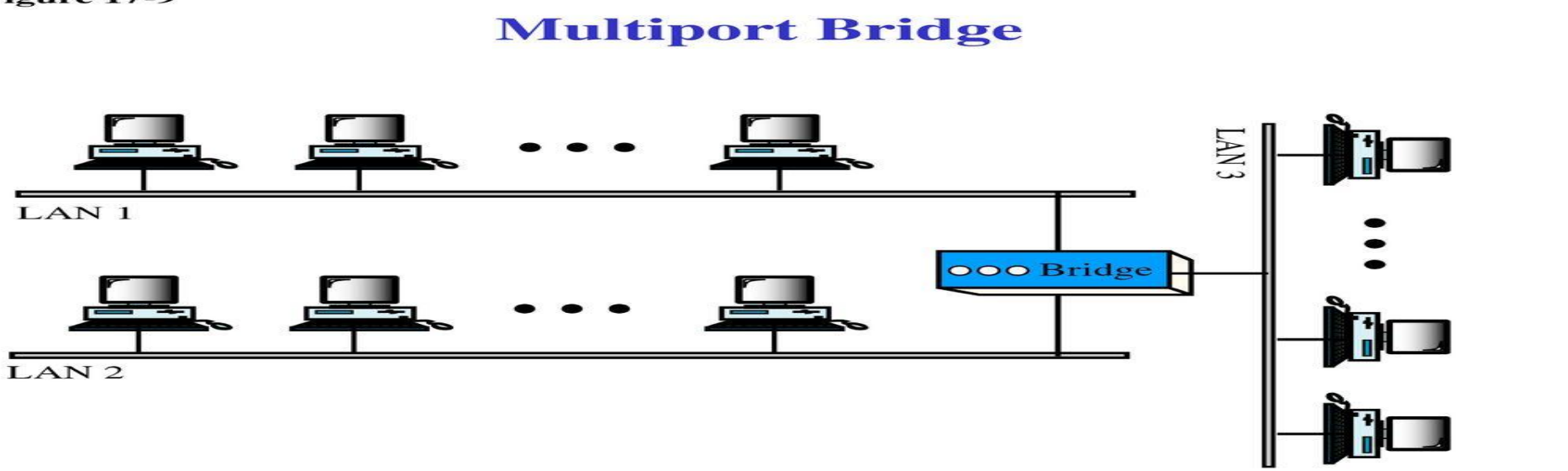
Learning/Transparent Bridge

- if it does not yet recognize the destination address, it relays packet to all of the station on both segments.
- It uses the source address to build its table.
- As it reads the source address, it notes which side the packet came from and associates that address with the segment to which it belongs.
- Using the same algorithm, the learning bridge is also self-updating

Multiport Bridge

- A multiport bridge can be either simple or learning, and is used to interconnect more than two same type segments.
- Generally a multiport bridge can be used to connect more than two LAN

Figure 17-9



Advantages

- It reduces network traffic with minor segmentation
- It reduces collisions
- It extends the physical network
- Bridges also can reduce network traffic on a segment by subdividing network communications
- Some bridges connect network having different architectures and media types(ring and ethernet topology)

Dis-advantages

- It is slower compare to repeaters due to the filtering process
- A bridge is more expensive than repeaters or hubs'
- Complex network topology, it can pose a problem for transparent bridge
- Does not scale to extremely large network
- Buffering and processing introduces delays

Bridge summary slide

- Bridges works at physical layer and data link layers
- So it works with MAC address
- Used to connect two different LAN(e.g. Ethernet LAN and token ring LAN)
- Forward packets to destination segment
- Filtering- using mac address it filter packets to send to which segment
- Collision domain (less)

Routers

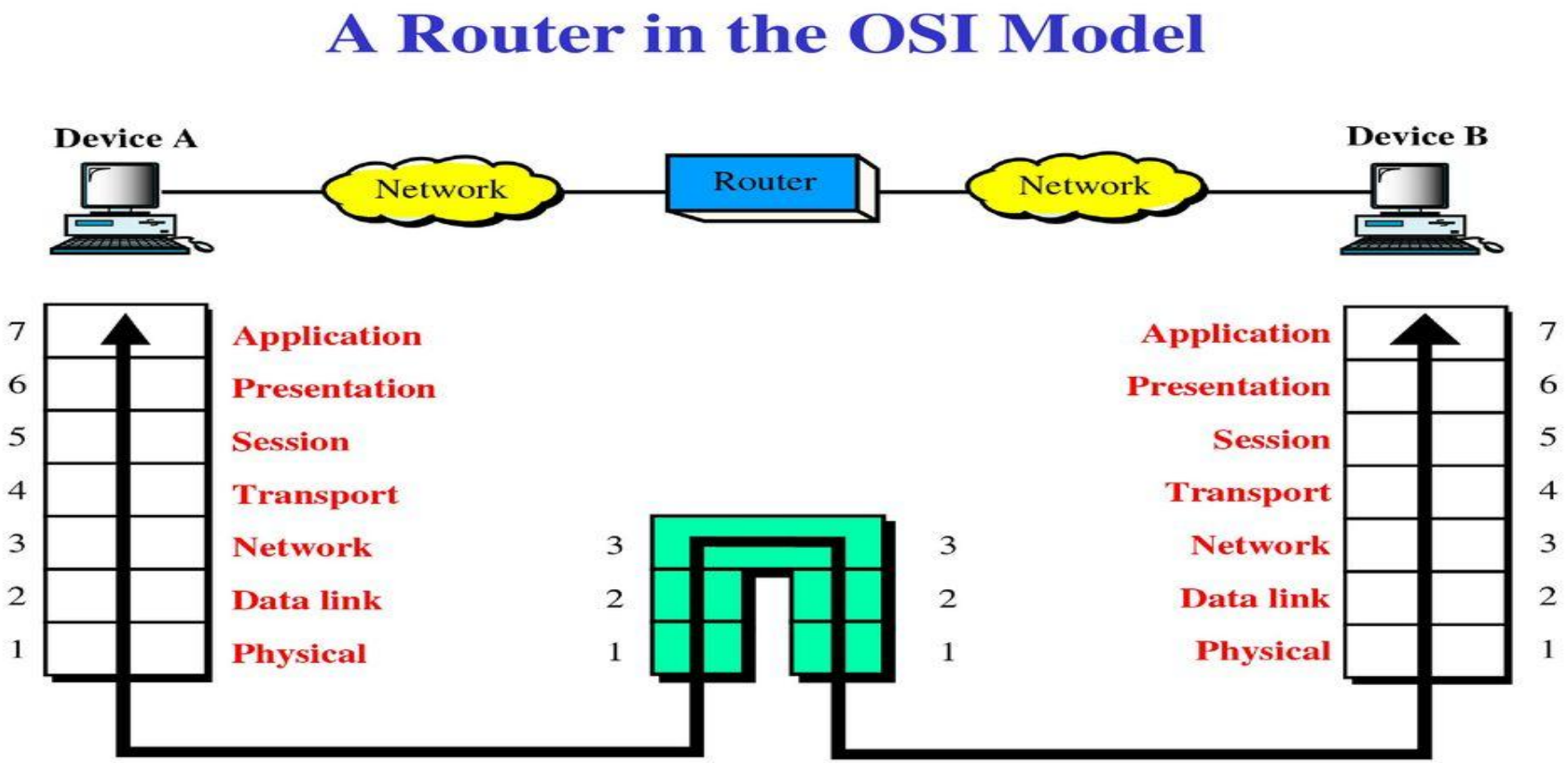
- 

Routers

- A router is a networking device that connects multiple networks together and directs traffic between them.
- It is an internetworking device, that receives IP packets from one computer network and forwards it to another computer network
- Routers are used to connect LANs and WANs.
- It operates at layer 3 of OSI reference model.
- It is network layer device.

Routers

Figure 17-10

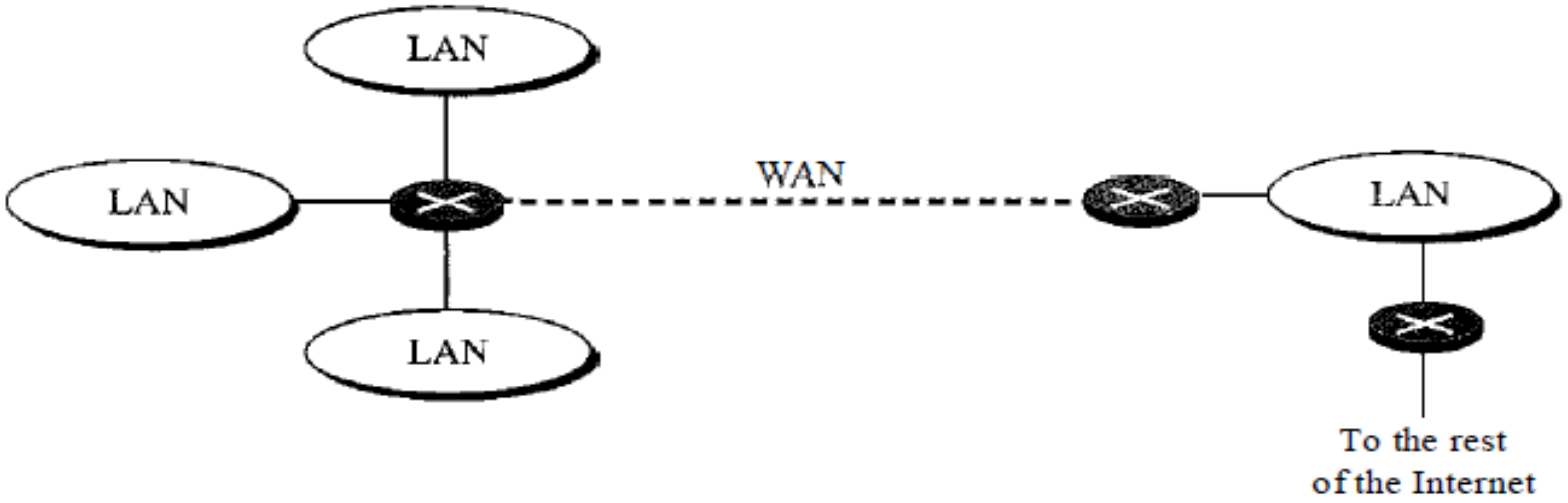


Routers

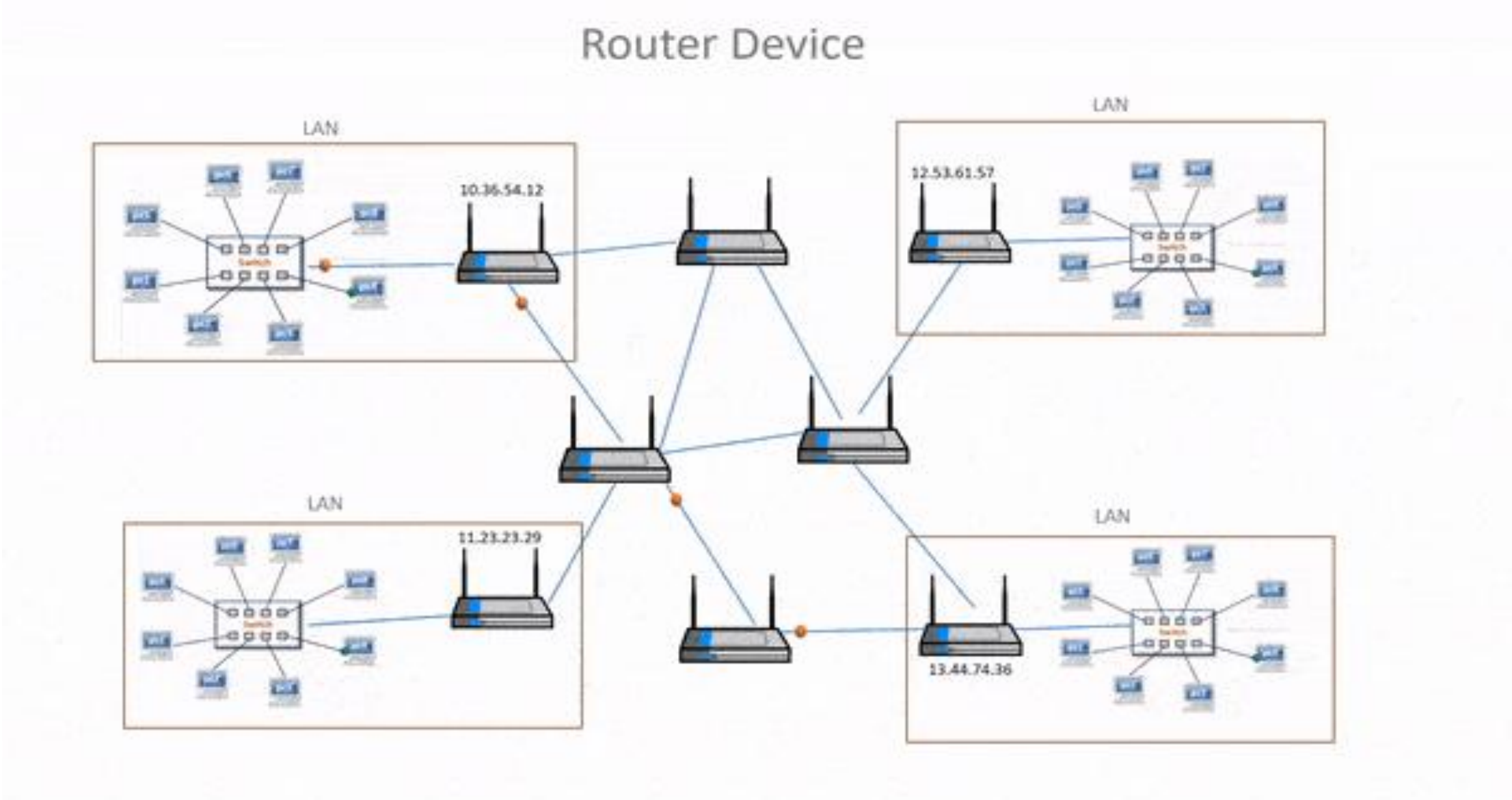
- Router used to connect two or more independent network such as FDDI (Fiber Distributed Data Interface) network and Ethernet network.
- This kind of translation reduces network speed.
- Unlike bridges routers have ability to select best path that is faster and efficient to route packet destination.

Routers

- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route.



ROUTER’S in Internet



What is a routing table?

- Routing table is an electronic document that stores network information in his table.
- The routing table is stored in the router device.
- Router uses this table and determines the path on the network. When a packet comes to a router, it checks its routing table, which helps to find the other network's router using the IP address and forward it to the other network routing device, and so on.

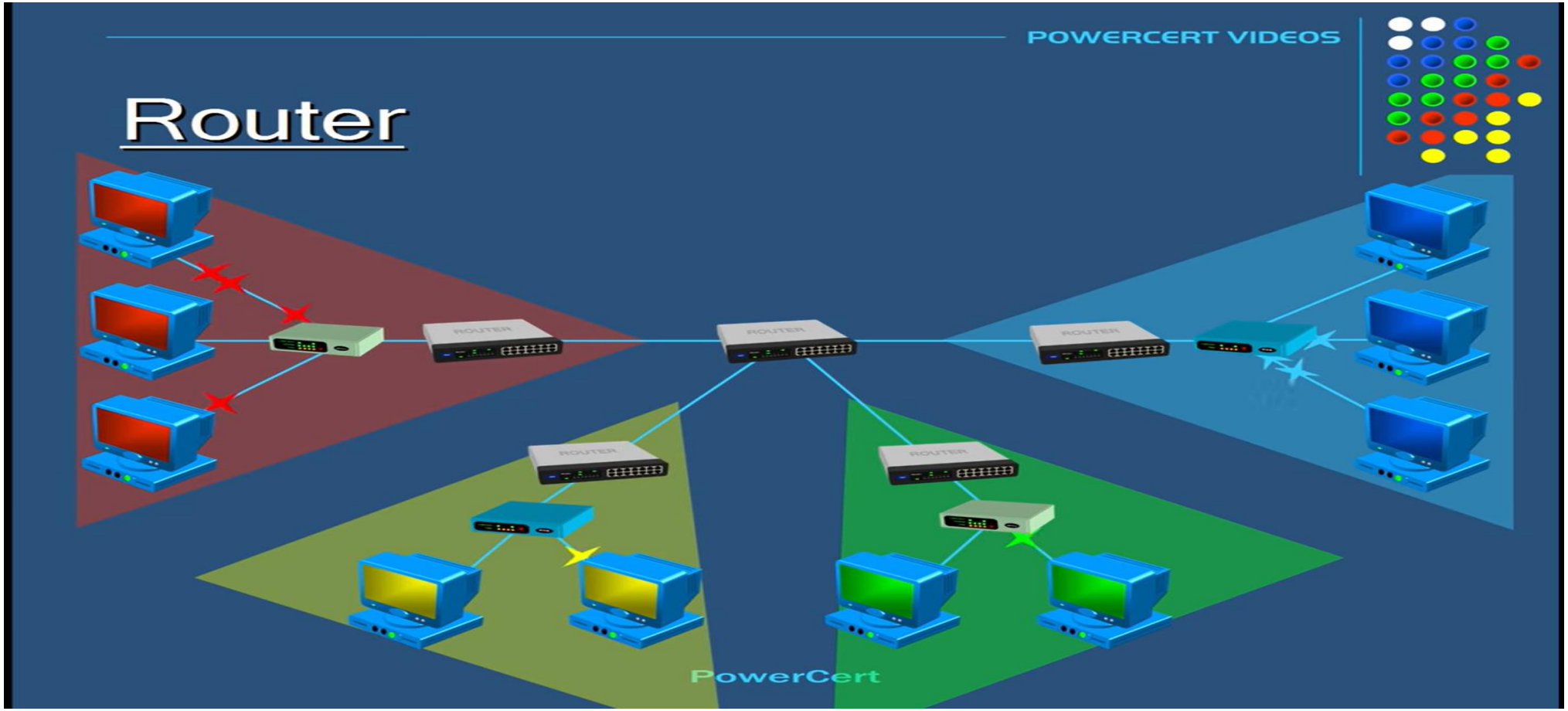
Routing table-route print

```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kirit>route print
===========================================================================
Interface List
 18...66 6c 80 2a c0 e7 ......Microsoft Wi-Fi Direct Virtual Adapter
 10...76 6c 80 2a c0 e7 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  7...64 6c 80 2a c0 e7 ......Qualcomm QCA61x4A 802.11ac Wireless Adapter
 14...64 6c 80 2a c0 e8 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.0.1    192.168.0.103     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link    192.168.0.103    306
    192.168.0.103  255.255.255.255         On-link    192.168.0.103    306
    192.168.0.255  255.255.255.255         On-link    192.168.0.103    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    192.168.0.103    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    192.168.0.103    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  7    306 fe80::/64                On-link
  7    306 fe80::e379:904a:1f6f:25d9/128
                                    On-link
  1    331 ff00::/8                 On-link
```

Working of Routers

- When a router receives a packet it determines the destination IP address by reading the header of the packet.
- Router searches this destination address in its routing table and determines how to reach the destination.
- The routing table contains information about which networks are directly connected to the router and which networks can be reached through other routers.

Working of Routers



Working of Routers

- Routers use a routing table to determine the best path for data packets to take between networks.
- And forward packet to the next hop on the route.
- Routing table very important and needs to be updated and completed.

Types of Routers :**Static Router:**

- If router uses static routing, the routing table information are updated manually.
- The administrator enter the route for each destination into the table manually.
- It can not updated automatically when there is change in internet.
- The router will always use same path to a destination even if it is not shortest and efficient.
- Static routing can be more secure than dynamic routing, as it does not rely on information from other routers that could be compromised or incorrect.

Dynamic Router:

- Dynamic routers automatically update their routing tables based on information they receive from other routers in the network.
- As routing table is automatically updated, it can save time and reduce the risk of errors.
- It can automatically find the shortest path between networks and avoid congestion.
- Dynamic routing can adapt to changes in the network topology and can handle larger networks more easily.

Advantages of Routers

- **Connectivity**: Routers allow multiple devices to connect to a network, including wired and wireless devices.
- **Routing**: Routers can be used to route traffic between networks, enabling devices on different networks to communicate with each other.
- **Network Address Translation (NAT):** Routers can use NAT to assign private IP addresses to devices on a local network and map them to a public IP address, which is used to communicate with devices outside of the local network.
- **Firewall:** Many routers have built-in firewalls, which can be configured to block incoming traffic that is not authorized.

Dis-advantages of Routers

- **Cost**: Routers can be more expensive than other networking devices, such as switches or hubs.
- **Configuration Complexity:** Routers can be more complex to configure than other networking devices, this can require additional training or expertise.
- **Single Point of Failure:** If a router fails, the entire network can be affected.

Router summary slide

- Router works at physical layer, data link layer, network layerIt is a layer 3 network device.

1. Packet Forwarding:
- Determines the best path for data packets to travel from the source to the destination.

2. Traffic Management:
- Controls and prioritizes network traffic to prevent congestion and ensure efficient data flow.

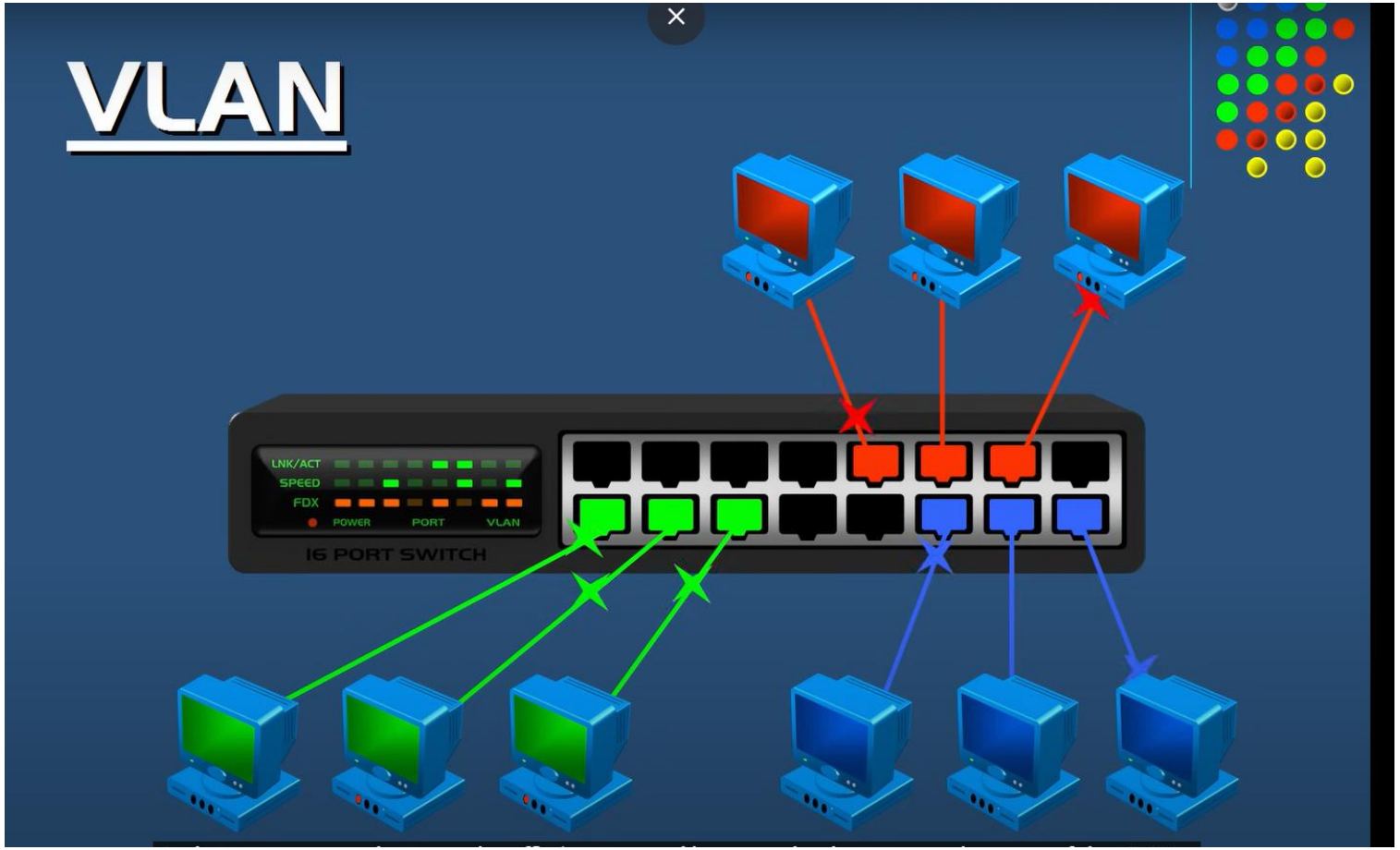
3. Network Address Translation (NAT):
- Converts private IP addresses to a public IP address, enabling multiple devices to share a single internet connection.

4. Dynamic Routing:
- Uses routing protocols (e.g., RIP, OSPF, BGP) to update and optimize network paths dynamically.

5. Firewall and Security:
- Provides basic security features by filtering traffic and blocking unauthorized access.

6. Connecting Different Networks:
- Links multiple networks together, such as LANs, WANs, and the internet.

VLAN



Layer-3 Switch

- **Definition:** A Layer 3 switch is a high-performance networking device that combines the functions of a switch and a router, operating at both Layer 2 (Data Link) and Layer 3 (Network) of the OSI model.
- **Functionality:** It performs switching (MAC-based forwarding) like a Layer 2 switch but also supports routing (IP-based forwarding) like a router.
- **Packet Forwarding**: Uses hardware-based switching to forward packets efficiently, unlike traditional routers that rely on software-based routing.
- **Routing Capabilities:** Supports routing protocols such as RIP, OSPF, and static routing for inter-VLAN communication.

Layer-3 Switch

- **Inter-VLAN Routing**: Enables communication between different VLANs without needing an external router, improving network performance.
- **Better than Layer 2 Switches**: Unlike Layer 2 switches, which only forward based on MAC addresses, Layer 3 switches can make forwarding decisions based on IP address.
- **Use Cases**: Used in large LANs, enterprise networks, and data centers where high-speed inter-VLAN routing is required.

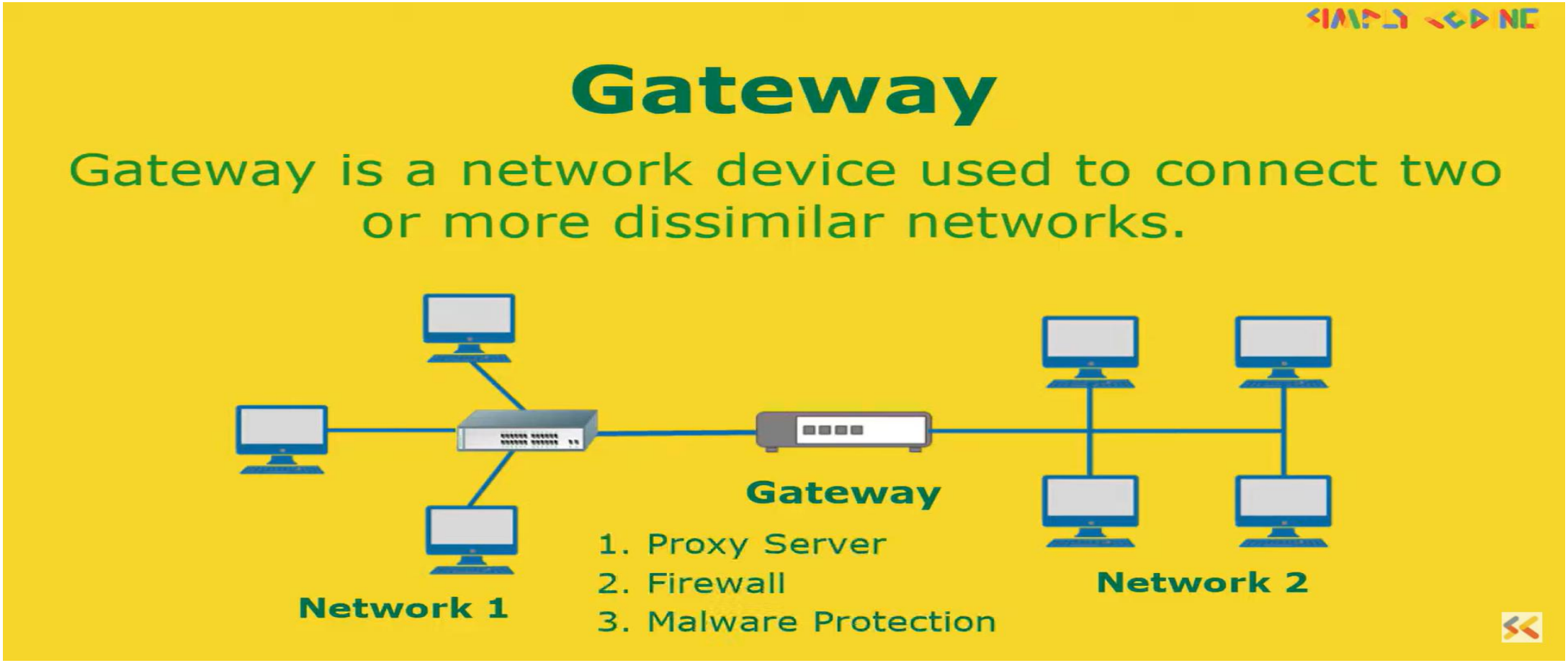
Difference Between Layer 2 and Layer 3 switch

Feature	Layer 2 Switch	Layer 3 Switch
OSI Layer	Works at Layer 2 (Data Link Layer)	Works at Layer 3 (Network Layer)
Packet Forwarding	Based on MAC addresses	Based on IP addresses
Switching Method	Uses MAC address table for switching	Uses routing table for forwarding packets
Inter-VLAN Communication	Requires an external router for inter-VLAN routing	Can perform inter-VLAN routing internally
Routing Functionality	No routing capability	Supports static and dynamic routing (OSPF, RIP etc.)
Speed	Faster for simple switching within a VLAN	Faster for inter-VLAN communication than routers
Cost	Cheaper	More expensive than Layer 2 switches but cost-effective compared to routers
Hardware	Uses switching fabric for MAC address-based forwarding	Uses ASIC hardware for both switching and routing

Gateway

- A Gateway is a device or hardware which acts like a “gate” among the networks.
- network device used to connect two or more dissimilar networks
- It acts as an entrance for the other nodes in the network.
- Operates at all layers of OSI .

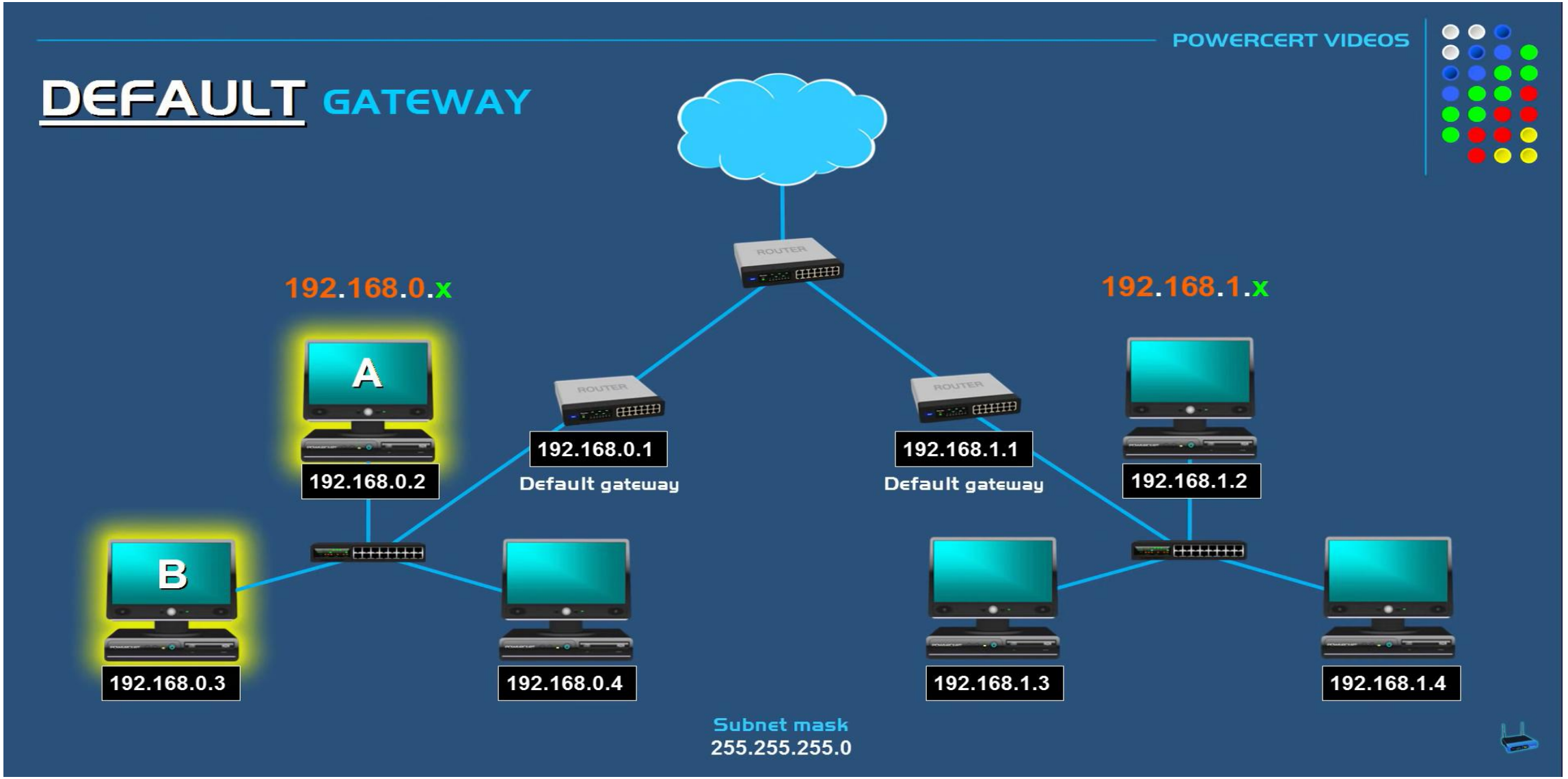
Gateway


Gateway
Gateway is a network device used to connect two or more dissimilar networks.
Gateway
1. Proxy Server
2. Firewall
3. Malware Protection
Network 1
Network 2

Gateway

- Responsible for enabling the traffic flow within the network.
- Gateway uses more than one protocol for communication thus its activities are much more complex than a switch or a router.
- device that is used for communication among the networks that have a different set of protocols and is responsible for the conversion of one protocol into the other.

Gateway

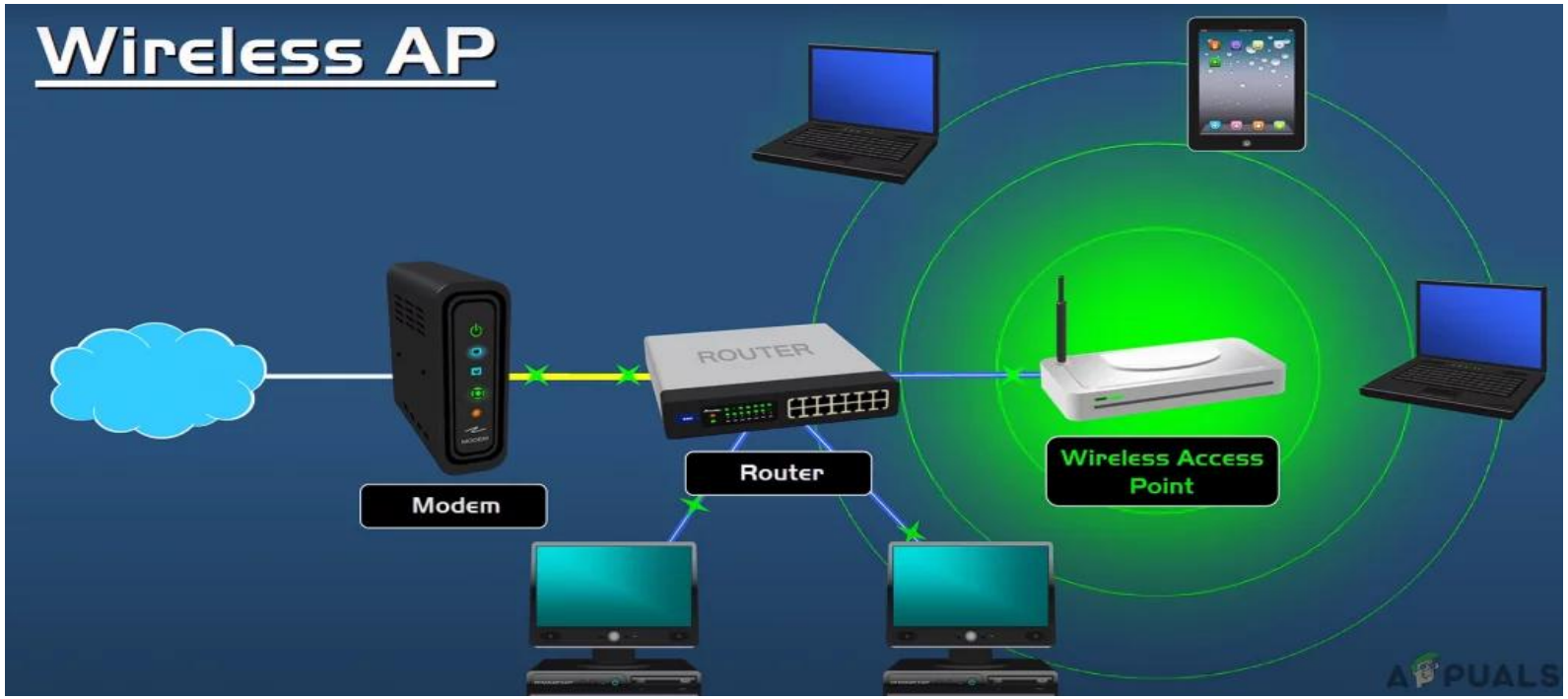

POWERCERT VIDEOS
DEFAULT GATEWAY
ROUTER
192.168.0.x
192.168.1.x
A
B
192.168.0.2
192.168.0.1
Default gateway
192.168.1.1
Default gateway
192.168.1.2
192.168.0.3
192.168.0.4
192.168.1.3
192.168.1.4
Subnet mask
255.255.255.0

Gateway

- Gate way is generally software installed within a router.
- For example: we can use two different kind of electronic mail system such as X.400 protocol mail system or SMTP mail system.
- Here SMTP and X.400 are emailing protocol but as both are different we need gateway to send and receive the mail.
- Gateways are costly than other network devices.
- It is also difficult to install and configure gateways

Access Point

- An access point (AP) in networking is a device that allows wireless devices to connect to a wired network.



Access Point

- Act as central Transmitter and receiver of WLAN radio signals.
- It acts as a bridge between wireless devices, such as laptops, smartphones, and tablets, and a wired network, such as a LAN (Local Area Network) or the Internet.
- An access point has an Ethernet port that connects to a wired network and antennas that broadcast wireless signals to allow devices to connect.
- Each access point can serve multiple users within a defined network area; as people move beyond the range of one access point, they are automatically handed over to the next one.

Access Point

- It acts as a bridge between wireless devices, such as laptops, smartphones, and tablets, and a wired network, such as a LAN (Local Area Network) or the Internet.
- An access point has an Ethernet port that connects to a wired network and antennas that broadcast wireless signals to allow devices to connect.
- Each access point can serve multiple users within a defined network area; as people move beyond the range of one access point, they are automatically handed over to the next one.

Access Point

- Provides a very long coverage area for both indoor and outdoor
- Provides MAC address filtering , leads to securing the network data.
- Also provides encrypted security.
- Modern access point can connect 200 wireless devices simultaneously