**Made by: Manthar Ali Sandano**

# **Networking history**

## **ARPANET the First Network(**Advanced Research Projects Agency Network)

In 1969, ARPANET, C computer network, was created by the US Department of Defense to ensure communication in case of a nuclear war. ARPANET initially connected four universities but grew to 40 machines by 1972. This system laid the foundation for the modern Internet.

## **Internet**

ARPANET grew to link US defense related universities and later included connections with the University College of London and Norway's Royal Radar Network. This global network of networks was named the "Internet" by Vinton Cerf, Yogen Dalal, and Carl Sunshine from Stanford University. They also developed the key protocols, like TCP, that are still used for communication on the Internet today.

## **What is computer networking?**

Computer networking refers to interconnected computing devices that can exchange data and share resources with each other.

## **communications protocols**

These networked devices use a system of rules, called communications protocols, to transmit information over physical or wireless technologies.

## **how computer network works?**

In a computer network, nodes follow rules called protocols to send and receive data. The network's design, including how its parts work and connect, is called the network architecture. It outlines the physical equipment, how everything is organized, and the rules and procedures for communication.

## **Modern computer networks:**

1. Operate Virtually: Create virtual networks over physical ones.

2. Integrate Large Networks: Connect and manage widespread networks efficiently.

3. Respond Quickly: Use software to adjust and manage traffic.

4. Ensure Security: Include built-in security and support extra protections.

## **Data communication (exchange the data [send and receive data])**

Transferring data over a transmission medium between two or more devices, systems, or places is known as data communication.

**Transmission**: It is part of Data communication sending data from one place to another place.

**Components of Data Communication:**

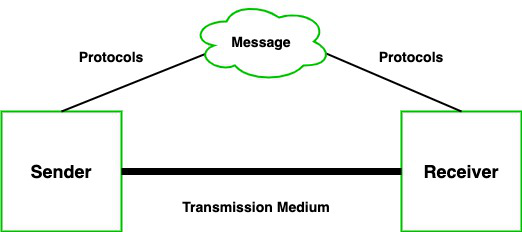
1. **Message:** The information being sent, like text, audio, or video.

2. **Sender:** The device that sends the message, such as a computer or phone.

3. **Receiver:** The device that gets the message, like a computer or phone.

4. **Transmission Medium / Communication Channels:** The way devices are connected, either through wired or wireless methods.

5. **Set of Rules (Protocol):** The guidelines that ensure the message is understandable to both sender and receiver, like language or internet protocols.



# **Types of Data Transmission:**

As we know data transmission is communication in which we can send or receive data from one device to another. The data communication is divided into two types:

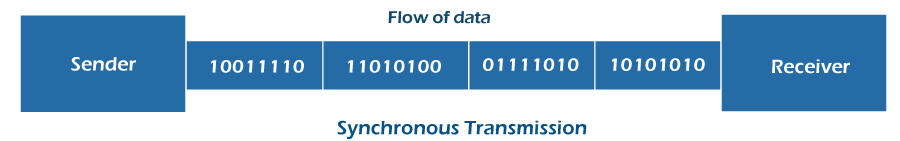
1. **Simplex(one way)**
   1. Simplex Communication: Oneway communication where one device only sends data and the other only receives. For example, using a keyboard or listening to music through speakers.
2. **duplex (two-way)**
   1. Half Duplex Communication: Twoway communication where devices can both send and receive data, but not at the same time. For example, walkietalkies.
   2. **Full Duplex Communication:** Twoway communication where devices can send and receive data simultaneously. For example, mobile phones and landlines.

## **Synchronous Transmission v/s Asynchronous Transmission**

Synchronous Transmission: Data flows continuously with timing signals to keep both sender and receiver in sync.

Advantage: Fast because data flows smoothly.

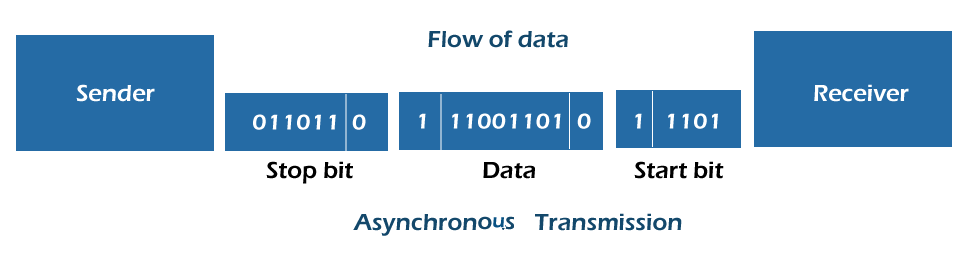
Disadvantage: Needs exact timing between sender and receiver.



Asynchronous Transmission: Data is sent in separate packets with start and stop signals, so sender and receiver don’t need to be in sync.

Advantage: Flexible and easy to set up.

Disadvantage: Slower due to extra signals.



## **Signal**

A data signal is an electrical or digital wave that carries information between devices.

That data consists of [binary code](https://www.computerhope.com/jargon/b/binary.htm) (0s and 1s) and is transmitted as electrical voltages, currents, or light pulses. The way data signals are transmitted and received depends on how the signals travel through the medium (copper wires, optical fibers, radio waves, etc.) and the [communication protocols](https://www.computerhope.com/jargon/c/comprot.htm) involved.

Analog Signal: A continuous wave that varies smoothly to represent information, like a radio wave.

Digital Signal: A series of discrete pulses or bits that represent information in binary form (0s and 1s).

**Analog signals reproduce real-world data, while digital signals convert this data into binary form.**

## **Protocols (set of rules)**

A network protocol is a set of rules that govern data communication between different devices in the network.

1. IP (Internet Protocol): Helps direct data packets to the right address on a network.

2. TCP/IP (Transmission Control Protocol/Internet Protocol): A set of protocols that work together to ensure data is sent and received correctly over the Internet.

3. FTP (File Transfer Protocol): Used to transfer files between computers over a network.

4. HTTP (Hypertext Transfer Protocol): Used for transferring web pages and data from the web to your browser.

5. ICMP (Internet Control Message Protocol): Used for sending error messages and operational information about network connections.

6. POP3 (Post Office Protocol version 3): A protocol for retrieving email from a server to your computer.

7. TCP (Transmission Control Protocol) breaks messages into smaller packets and puts them back together at the other end. It also makes sure the packets arrive in the right order and without errors.

**The key differences between \*\*IPv4\*\* (Internet Protocol version 4) and \*\*IPv6\*\* (Internet Protocol version 6) are related to their structure, capabilities, and how they address the growing demand for internet connectivity. Here are the main distinctions:**

**1. \*\*Address Length\*\***

**- \*\*IPv4\*\*: Uses a 32-bit address scheme. This allows for a total of about \*\*4.3 billion unique addresses\*\* (2³²).**

**- \*\*IPv6\*\*: Uses a 128-bit address scheme, providing \*\*3.4 x 10³⁸ unique addresses\*\* (2¹²⁸), vastly increasing the number of available IP addresses.**

**### 2. \*\*Address Notation\*\***

**- \*\*IPv4\*\*: Expressed in decimal format, separated by periods. Example: `192.168.0.1`**

**- \*\*IPv6\*\*: Expressed in hexadecimal format, separated by colons. Example: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`**

**### 3. \*\*Header Complexity\*\***

**- \*\*IPv4\*\*: Has a simpler header with 12 fields.**

**- \*\*IPv6\*\*: Has a more streamlined header with 8 fields, improving efficiency in routing and packet processing.**

**### 4. \*\*Address Space and Allocation\*\***

**- \*\*IPv4\*\*: Address exhaustion is a concern due to limited space; addresses are often reused through techniques like NAT (Network Address Translation).**

**- \*\*IPv6\*\*: Provides a significantly larger address space, eliminating the need for NAT and reducing the potential for address exhaustion.**

**### 5. \*\*Configuration\*\***

**- \*\*IPv4\*\*: Can be configured manually (static) or through DHCP (Dynamic Host Configuration Protocol).**

**- \*\*IPv6\*\*: Supports both stateful configuration (using DHCPv6) and stateless auto-configuration, where devices can automatically assign themselves an IP address.**

**### 6. \*\*Security\*\***

**- \*\*IPv4\*\*: Security features are optional and need to be implemented separately (e.g., IPsec).**

**- \*\*IPv6\*\*: Security (IPsec) is built-in as a mandatory feature, providing better security by default.**

**### 7. \*\*Broadcasting vs Multicasting\*\***

**- \*\*IPv4\*\*: Supports broadcasting, where a message is sent to all devices in a network.**

**- \*\*IPv6\*\*: No broadcasting; instead, it uses multicasting and "anycasting," where data is sent to the nearest node or to specific groups.**

**### 8. \*\*Packet Fragmentation\*\***

**- \*\*IPv4\*\*: Routers are responsible for fragmenting packets.**

**- \*\*IPv6\*\*: Hosts are responsible for fragmentation, simplifying the process for routers.**

**### 9. \*\*Transition Mechanism\*\***

**- \*\*IPv4\*\*: No transition needed (already in widespread use).**

**- \*\*IPv6\*\*: Several transition mechanisms like dual-stack (supporting both IPv4 and IPv6) and tunneling are used to ease the migration from IPv4 to IPv6.**

**### Summary**

**IPv4 is the older, widely used protocol, but it has limited address space. IPv6, the newer protocol, addresses the shortcomings of IPv4, particularly the address shortage, and offers improved security and efficiency. However, the transition from IPv4 to IPv6 is gradual and ongoing.**

**What is IP?**

**Why IP?**

**IP classes(classes)** **Find out network address, broadcast, subnet mask identify class., Ip types**

**Ipv4,ipv6**

## **How do Network Protocols Work?**

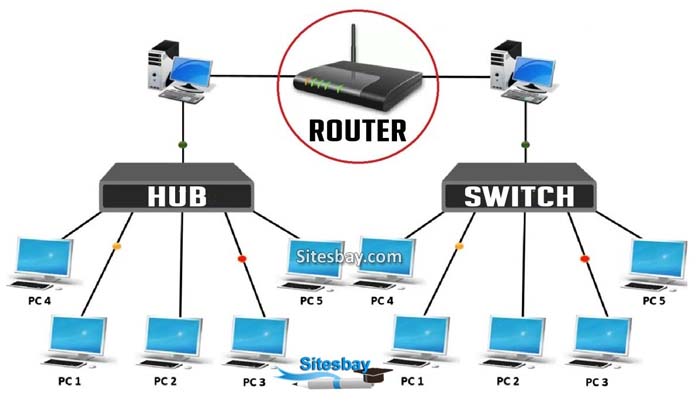
Network protocols help devices communicate over a network, and the OSI model is a common way to understand how this works. The OSI model has seven layers, each with its own job and protocols to handle different parts of the communication. For example, the Internet Protocol (IP) is a key protocol in the network layer that helps route data by managing the source and destination addresses of data packets. Each layer and protocol plays a specific role in making sure data travels correctly from one device to another.

## **Network connectivity devices**

Network connectivity devices and components are used for establishing and maintaining communication between devices on a network. Here’s a brief overview of some key devices and components:

1. **Router: Router layer 3 devices (IP address) (router inter-network communication device)**

: Connects different networks together, like a home network to the internet, and directs data between them.



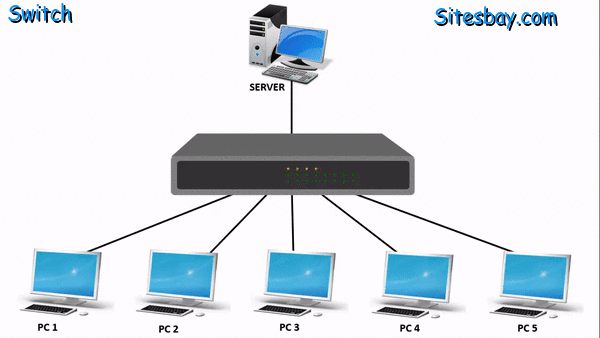
2. Switch (Intelligent, unicast work on layer 2 full duplex mac address: Connects multiple devices within the same network and directs data to the correct device by using MAC addresses.

When data is sent through a switch:

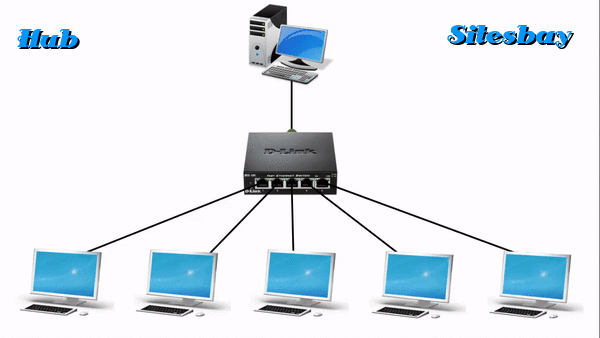
1. Data Arrives: A device sends data with its MAC address included.

2. Switch Learns: The switch records the MAC address and which port it came from.

3. Data Forwarded: The switch uses this information to send data only to the correct device on the right port.



3. Hub (No intelligent, broadcast collision domain, half duplex)D: Connects multiple devices in a network, but sends data to all devices, not just the intended one. It’s less efficient than a switch.



4. Modem: Converts digital data from a computer into a format suitable for transmission over telephone lines or cable and vice versa. It connects your network to the internet.

5. Access Point: Provides wireless connectivity to a wired network, allowing devices like laptops and smartphones to connect without cables.

6. Network Interface Card (NIC): A hardware component in a computer or device that allows it to connect to a network, either wired (Ethernet) or wireless (Wi-Fi).

7. Firewall: A security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules to protect the network.

8. Repeater: Amplifies signals to extend the range of a network, ensuring data can travel longer distances without degradation.

9. Bridge: A bridge in a computer network is a device used to connect multiple LANs together with a larger Local Area Network (LAN).

These devices and components work together to create, manage, and protect network connections, enabling effective communication and data transfer between devices.

**Broadcast vs Unicast**

In networking, "broadcast" and "unicast" are two different methods of sending data from one device to another. Here’s a simple comparison:

**Broadcast**

Definition: Sends data to all devices on a network segment or subnet.

Useful for messages that need to reach all devices, such as network discovery protocols (e.g., ARP Address Resolution Protocol).

Efficiency: Can be less efficient in large networks because it sends data to all devices, which can cause network congestion.

**Unicast**

Sends data from one device to a specific, single destination device.

Commonly used for direct communication between two devices, such as accessing a website or sending an email.

Efficiency: More efficient for targeted communication, as it reduces unnecessary data traffic to other devices.

## What is MAC Address(2nd layer)

A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. MAC address is 48 bit(8bytes) hexadecimal address. The format of a MAC address is MM:MM:MM:SS:SS:SS.

**A unique identifier for a network device, like a fingerprint.**

IEEE assigns MAC address blocks to manufacturers, while Aina (a hypothetical or real company) might use devices with those MAC addresses. They are related because IEEE provides the unique identifiers (MAC addresses) used in devices that companies like Aina produce or use.

1. ARP (Address Resolution Protocol):

The ARP (Address Resolution Protocol) is used to find the MAC address of a device when you only know its IP address.

Example: If a computer knows an IP address but needs to find the device’s MAC address to send data, it uses ARP.

2. RARP (Reverse Address Resolution Protocol):

Reverse Address Resolution Protocol (RARP) was used to find the IP address of a device when only its MAC address was known.

Example: A device with a known MAC address requests its IP address from a RARP server.

Classification of computer

## **There are two main types of computer network architecture:**

1. **Client-server Architecture:**

* Servers provide resources and manage tasks.
* Server nodes provide resources like memory, processing power, or data to client nodes.
* Clients request resources from servers but don’t share their own.
* Example: A company’s central server holds data that employees access.

2. **PeertoPeer (P2P) Architecture:**

* All computers have equal roles and can share resources with each other.
* Each peer may share some of its resources, like memory and processing power, with the entire computer network
* No central server is needed.
* Example: Multiple computers work together to handle tasks like 3D graphics rendering.

https://aws.amazon.com/whatis/computernetworking/#:~:text=Computer%20networking%20refers%20to%20interconnected,some%20common%20computer%20networking%20FAQs.

## **Types of Networks according to geographical coverage**

* PAN (Personal Area Network)
* LAN (Local Area Network)
* MAN (Metropolitan Area Network)
* WAN (Wide Area Network)

PAN (Personal Area Network): A small network typically used for connecting personal devices within a short range, usually within a few meters.

Example: Bluetooth connections between a smartphone and wireless headphones.

LAN (Local Area Network): A network that connects devices within a limited area, such as a home, office, or campus, allowing them to share resources and communicate.

Example: The network in an office building that connects computers, printers, and file servers.

MAN (Metropolitan Area Network): A network that covers a larger geographic area than a LAN but is smaller than a WAN, often spanning a city or a large campus.

Example: The network connecting multiple buildings of a university spread across a city.

WAN (Wide Area Network): A network that covers a broad geographic area, such as a country or continent, connecting multiple LANs and MANs.

Example: The internet, which connects various networks worldwide, or a company’s network linking offices in different cities or countries.

What is a network topology? A network topology is the physical and logical arrangement of nodes and connections...

Topology in the context of networks refers to the physical or logical arrangement of network devices and their connections. It defines how different network components, such as computers, routers, switches, and cables, are organized and connected to each other.

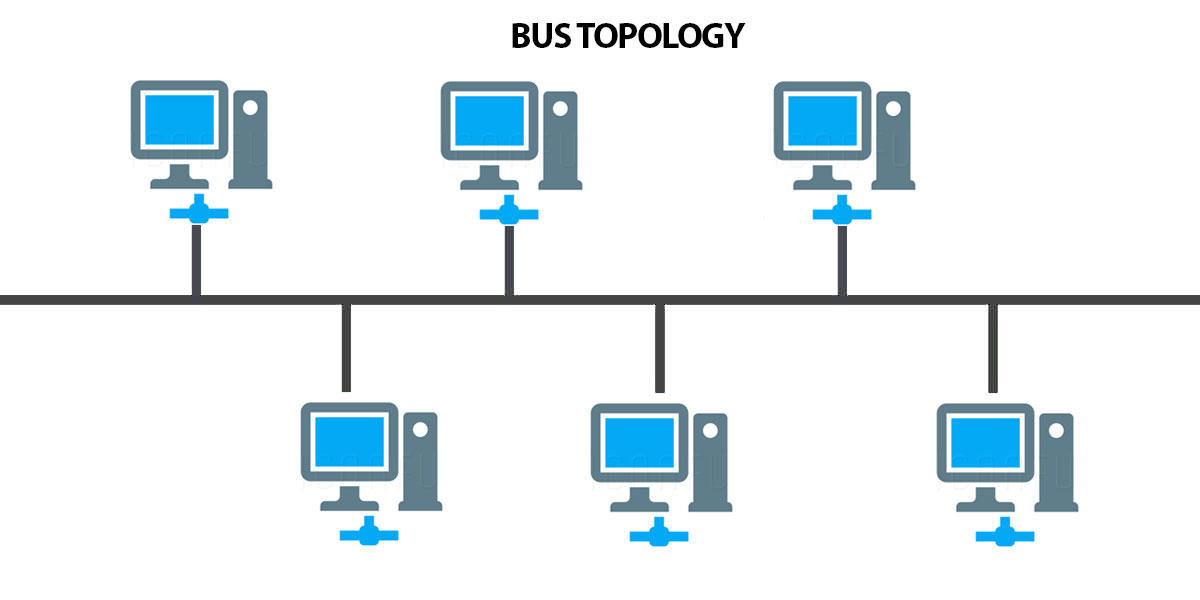
**Physical Topology:** Describes the actual physical layout of devices and cables in a network.

**Logical Topology:** Describes how data flows within a network and how devices interact from a data perspective, which may differ from the physical layout.

**Topology affects the network’s performance, reliability, and scalability.**

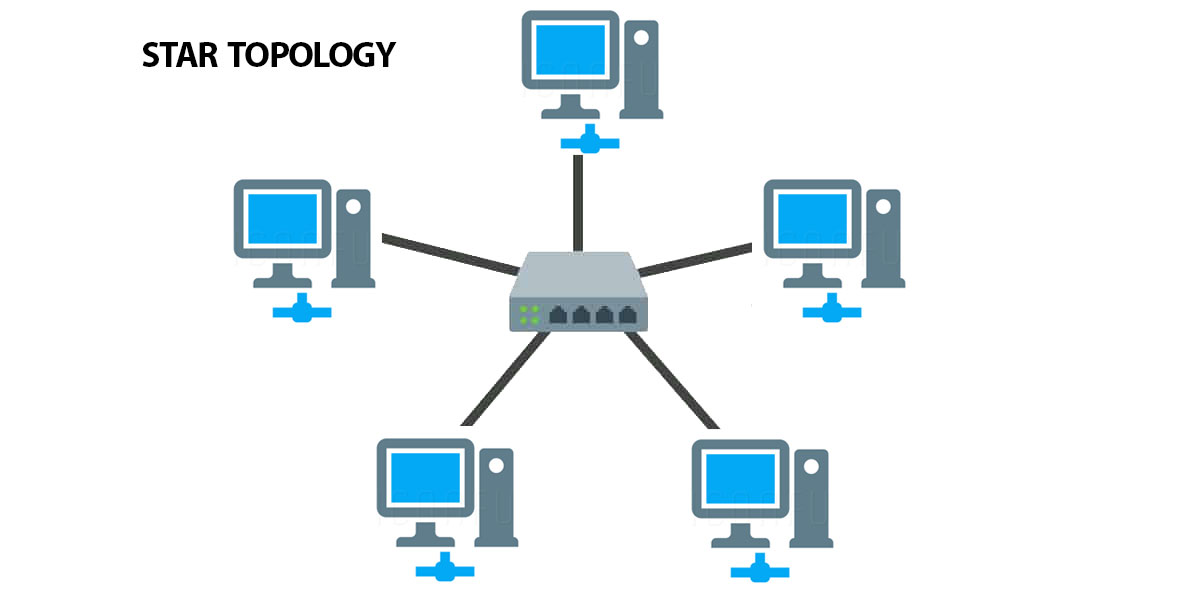
Bus Topology: A network layout where all devices are connected to a single central cable, known as the bus. Data sent by any device travels along the bus to all other devices.

Example: An older Ethernet network using coaxial cables.



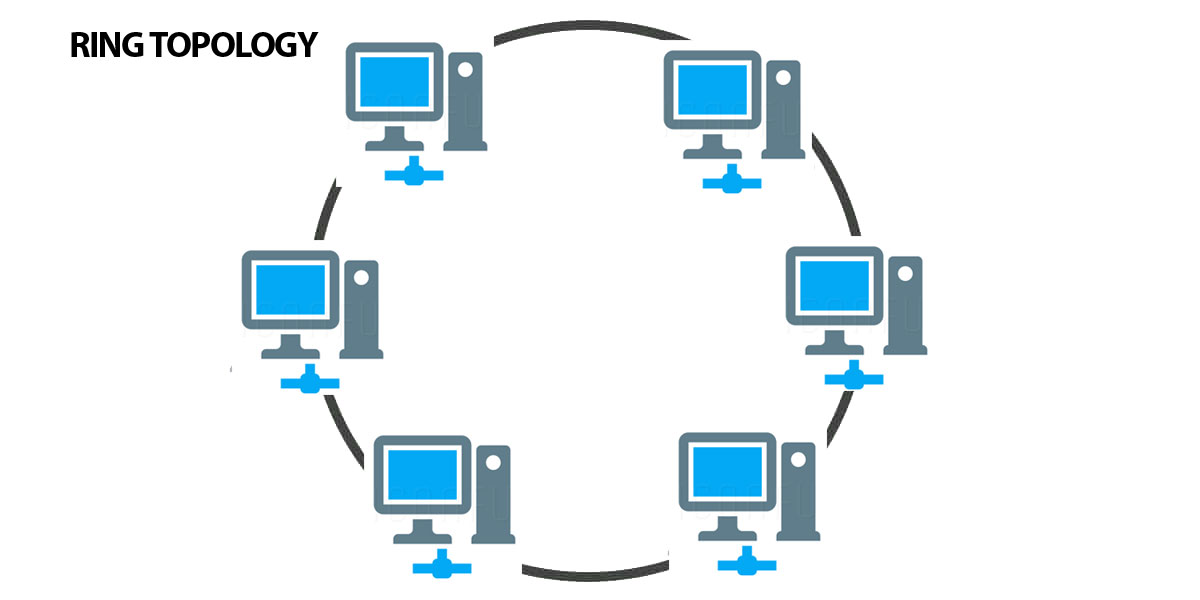
Star Topology: A network where each device is connected to a central hub or switch. The central hub manages and routes data between devices.

Example: Most modern office networks where computers and printers connect to a central switch or router.



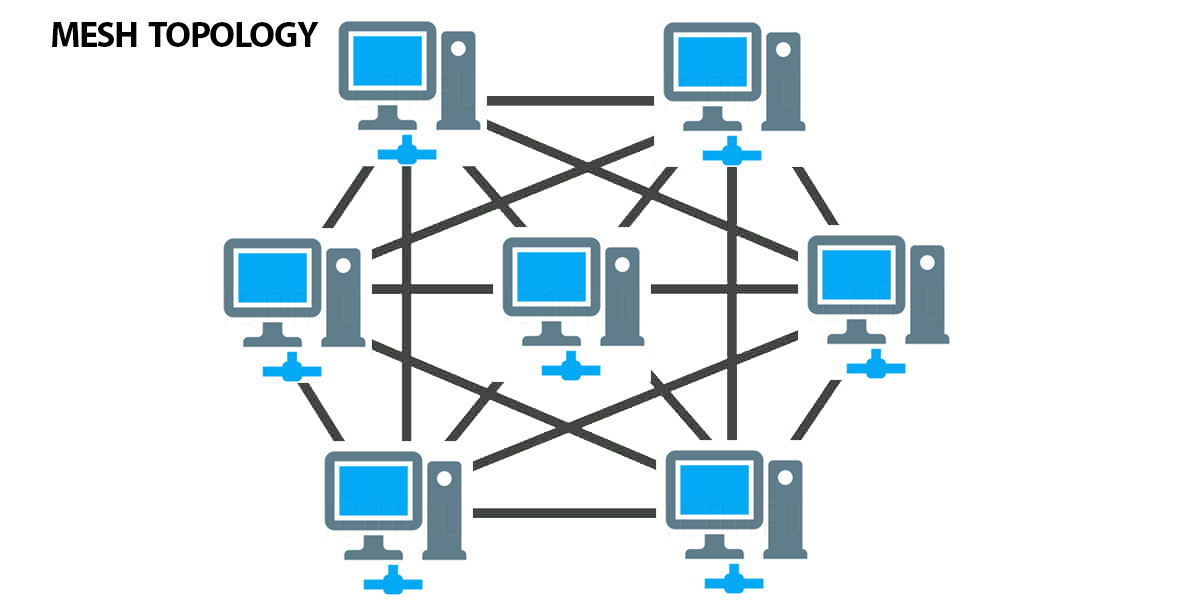
Ring Topology: A network where each device is connected to two other devices, forming a circular data path. Data travels in one direction (or both in a dual-ring setup).

Example: Token Ring networks where devices pass a token to control access to the network.



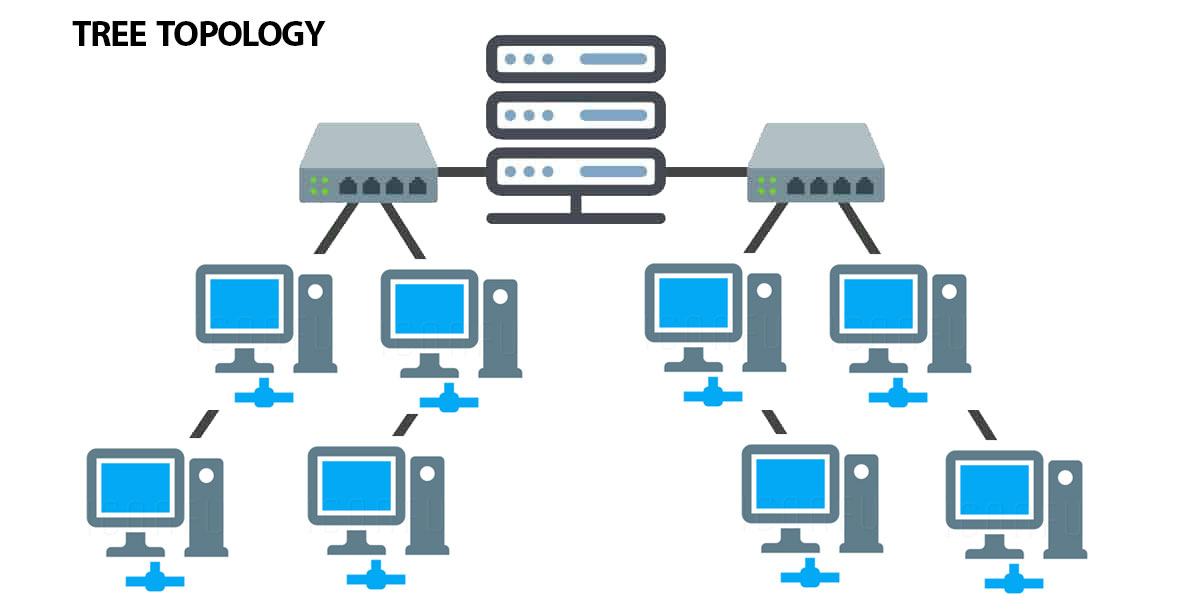
Mesh Topology: A network where devices are interconnected, allowing multiple paths for data to travel between devices. Can be fully (every device is connected to every other device) or partially meshed.

Example: The internet itself, where multiple redundant connections between routers ensure reliability.



Tree Topology: A hybrid topology that combines star and bus topologies. Devices are grouped into star-configured networks, which are then connected to a central bus or backbone.

Example: A large corporate network where departments have their own star networks connected to a central backbone.



Hybrid Topology: A network that combines two or more different topologies to leverage their benefits and address their limitations.

Example: A network that uses star topology within departments and connects these stars using a bus or ring topology for inter-department communication.

**Networking Addresses**

**There are two types of Addresses**

1. IP address (logical address)
2. Mac address (physical address)

**There are two types of IP**

* Public IP
* Private IP

**IP version 4 2^32 4 billion octal**

Router to router serial

Router to another device either net port

Ip v 6 128 bits 0-fff 2^128 (3 trillion)

16 bits one part(hexadecimal)

8 segments

DTE (Data Terminal Equipment): Devices that serve as endpoints in data communication networks, such as computers or printers. They generate or consume data and communicate through data interfaces.

DCE (Data Communication Equipment): Devices that facilitate data transmission between DTEs. Examples include modems, routers, and switches that provide communication services and convert data formats.

Routing: The process of selecting paths in a network to send data from a source to a destination.

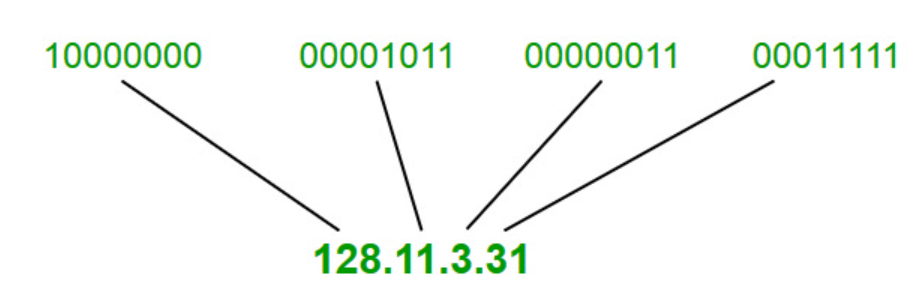
Dynamic Routing: A routing method where routes are automatically adjusted based on network changes using routing protocols (e.g., OSPF, BGP).

Static Routing: A routing method where routes are manually configured and do not change unless manually updated by the network administrator.

## What is an IPV4 Address?

An **IPv4 address** is a unique number assigned to every device that connects to the internet or a computer network. It’s like a home address for your computer, smartphone, or any other device, allowing it to communicate with other devices.

* **Format**: 192.168.1.1. Each number can range from 0 to 255.
* The [IPv4 address](https://www.geeksforgeeks.org/what-is-ipv4/) is divided into two parts: **Network ID** and **Host ID.**
* **Purpose**: The main purpose of an IPv4 address is to identify devices on a network and ensure that data sent from one device reaches the correct destination.
* **Example**: When you type a website address into your browser, your device uses the IPv4 address to find and connect to the server where the website is hosted.
* Host ID



## Need For **Classful Addressing**

Initially in 1980’s IP address was divided into two fixed part i.e., NID(Network ID) = 8bit, and HID(Host ID) = 24bit. So there are 28 that is 256 total network are created and 224 that is 16M Host per network.

There are one 256 Networks and even a small organization must buy 16M computer(Host) to purchase one network. That’s why we need classfull addressing.

**Note:**

* IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and Regional Internet Registries(RIR).

The 32-bit IP address is divided into five sub-classes. These are given below:

### Class A

* Range 1-126
* large number of hosts.
* The network ID is 8 bits long.
* The host ID is 24 bits long.
* IP addresses belonging to class a ranges from 1.0.0.0 – 126.255.255.255.

### Class B 128-191

* The network ID is 14 bits long.
* The host ID is 16 bits long.
* 2^14 = 16384 network address
* 2^16 – 2 = 65534 host address
* IP addresses belonging to class B ranges from 128.0.0.0 – 191.255.255.255.

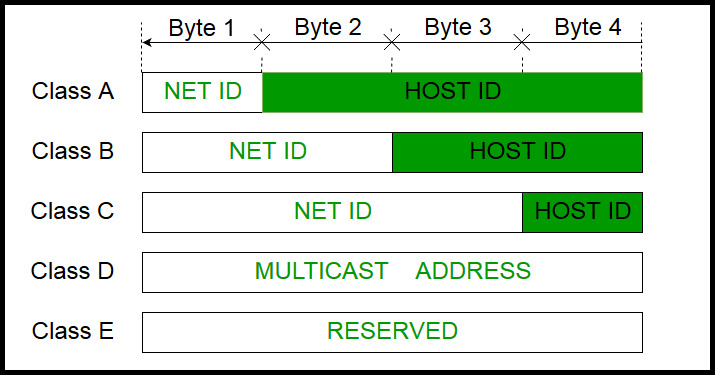
Class C 192-223

* IP addresses belonging to class C are assigned to small-sized networks.
* The network ID is 24 bits long.
* The host ID is 8 bits long.
* 2^21 = 2097152 network address
* 2^8 – 2 = 254 host address
* IP addresses belonging to class C range from 192.0.0.0 – 223.255.255.255.

Class D 224-239

Class E 240-255

Class is reserved for scientific purpose.

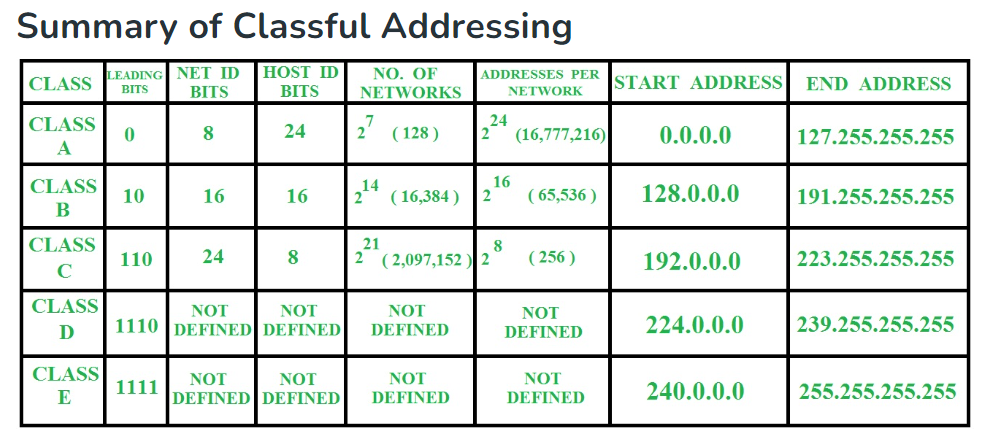
. 

Baseband one single channel at a time(signal).

Broadband multiple channel at a time(signal).

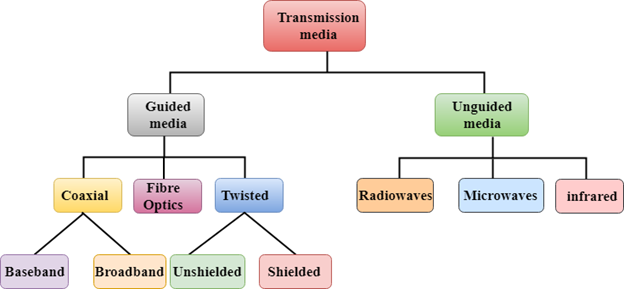
127 it is dedicated for loop back (some special cases, local server live server).

Sunbathing is the process of dividing a single IP



**Transmission media**

Transmission media are the means through which data is transmitted from one point to another. They include:



**Guided media:** In guided media, transmitted data travels through a cabling system that has a fixed path. For example, copper wires, fiber optic wires, etc.

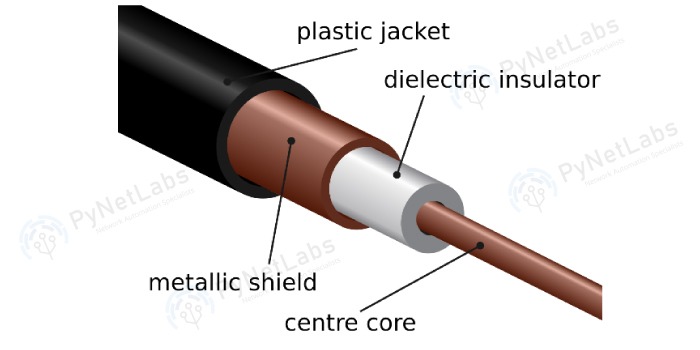
wired

**Unguided media**: In unguided media, transmitted data travels through free space in form of electromagnetic signal. For example, radio waves, lasers, etc.

wireless

Bandwidth: Amount of data that can travel through the cable in a unit period of time. Measure in kbps, Mbps, etc.

Coaxial Cable: A type of cable with a central conductor, an insulating layer, a metal shield, and an outer cover. It transmits data using electrical signals and is commonly used for cable TV and internet.



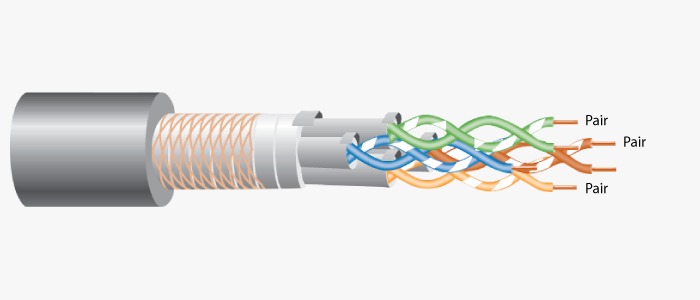
2. Twisted Pair Cable:

This cable has eight insulated wires. These are paired in groups of 2 and are twisted together based on a color code.

Two insulated wires twisted together to reduce interference. There are two types:

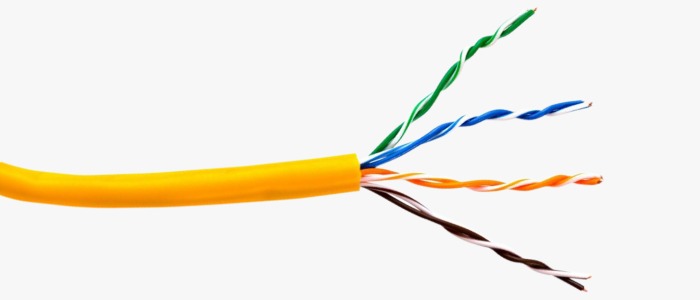
a. **Shielded twisted pair**

These twisted pair cables are covered in a braided shield which acts as a shield from outside interference.



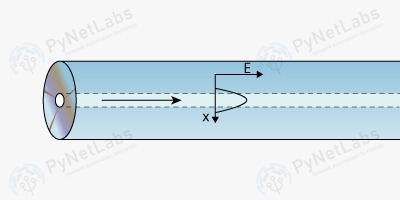
**Unshielded twisted pair**

These twisted pair cables do not have a braided shield. The 4 pairs are simply covered in a plastic insulator for safety.



Cat5, Cat6, Cat7: These are categories of twisted pair cables with increasing performance and speed. Cat5 is older and slower, while Cat7 is newer and faster.

Untwisted Pair Cable: Wires are not twisted; they're less effective at reducing interference compared to twisted pairs.

3. Fiber Optic Cable: A cable made of glass or plastic fibers that transmits data as light signals. It's used for high-speed internet and long-distance communication.

4. BNC(Bayonet Neill–Concelman) Connector: A type of connector used with coaxial cables. It’s often used in video and radio frequency applications.

5. T-Com Connector: A type of connector used with telephone lines, typically for connecting telephone equipment.

Satellite Microwaves: These microwaves are used for communication between the Earth and a satellite in orbit. It is crucial for global communication and broadcasting.

#### Uplink station sending data to Satellite Transponder which is 22,300 miles up, which forwards it to downlink

#### Infrared

#### Infrared waves are a type of energy that can travel through the air. Let’s discuss Infrared waves in detail.

**How it works?**

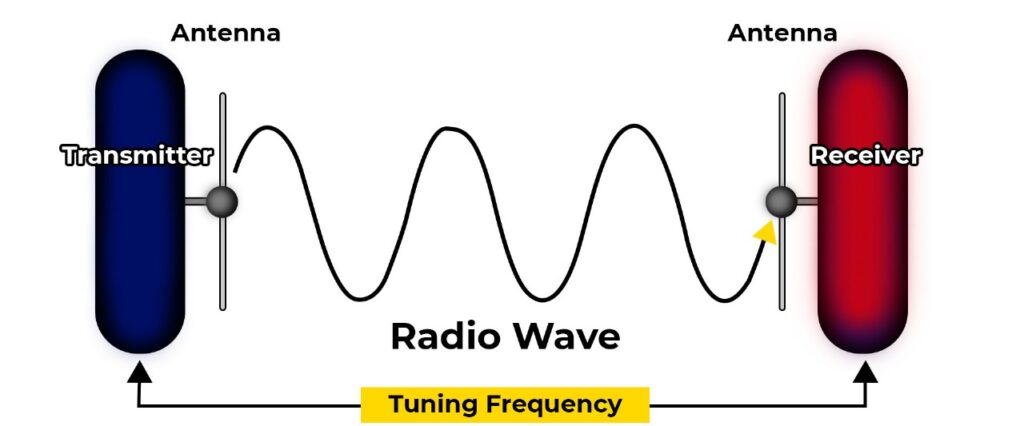
In order to send information with Infrared waves, we need special devices known as transceivers. These devices can send as well as receive infrared light.

Applications

* Wireless Keyboards and Mouse
* TV Remote Control
* Night Vision
* Weapon System
* Radio Waves: Electromagnetic waves used for wireless communication. They travel through the air and can carry signals like radio broadcasts, TV signals, and Wi-Fi.
* Example: When you listen to FM radio or use Wi-Fi on your phone, radio waves are transmitting the signal to and from your device.

**Role of Antenna**

* An antenna is a crucial component of radio wave transmission, which is responsible for converting electrical energy into radio waves.



Application

* Radio broadcasting
* Mobile communication
* Wireless networking
* Radar and navigation

Advantages

* Long-distance Communication
* Portable
* Reliable Communication
* Easy Installation

Disadvantages

* Prone to Interference
* Atmospheric Disturbances
* Limited Bandwidth
* Health Risks

#### Microwave Transmission

Microwave transmission is a method of transmitting data through high-frequency electromagnetic waves over long distances. Let’s understand in detail.

CIDR classless inter-domain 212.168.7.212/24

133.2.0.200

class b

133.2.0.0

133.2.255.255

255.255.0.0

191.15.0.12

class b

192.15.0.0

192.15.255.255

255.255.0.0

212.168.7.212

class c

212.168.7.0

212.168.7.255

255.255.255.0

17.0.0.244

class a

17.0.0.0

17.255.255.255

255.0.0.0

114.0.0.118

claas a

114.0.0.0

114.255.255.255

255.0.0.0

**OSI (open system interconnected) theoretical oriented model: is the benchmark of the network Invented by ISO (international standard organization).**

**Why OSI model?**

For example: you connected two computer and how they communicate with each other?

So OSI model describe how these computers can communicate with each other.

The OSI model can be seen as a universal language for computer networking.

* OSI model was introduced by IOS international standard organization in 1984.
* It has 7 layers and each layer has specific functionality.
* All these layers works combinely in order to transmit data from one network to another network.
* Physical Layer (hardware layer)
* Layer 1 is the physical layer and also the lowest layer of the OSI model. This layer transmits information in the form of bits (1s and 0s) from one node to the next. Components of the physical layer include cables, power plugs, connectors, network interface cards (NICs), and other hardware.
* Data-Link Layer(end to end error checking checksum)

Data framing

Data error checking

Data transfer rate is maintained

* Network Layer (Point to point error checking crc cyclic redundancy check)

The network layer is responsible for [routing data packets](https://www.enterprisenetworkingplanet.com/standards-protocols/network-routing/) from a source host to a destination host

Data is converted into packets

Sender and receivers IP

Routing

* Transport Layer ( end to end and error checking)

Data is converted into segments

TCP (feedback: either receiver receives data or not) and UDP (No feedback: either receiver receives data or not) works here

* Session Layer

It establish session connection between sender and receiver.

* Presentation Layer

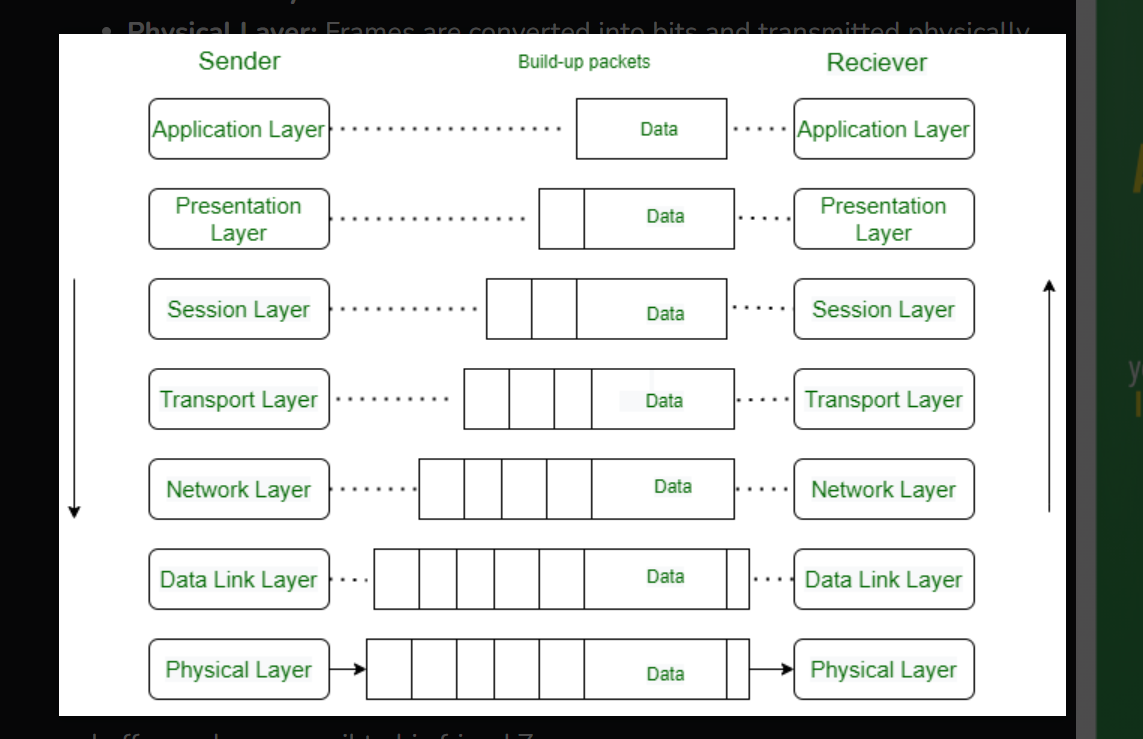
Translation

Encryption and decryption

Data compression

* Application Layer (software layer)

It provides interface trough which we can interact with applications and protocols (http,https,ftp,stmp) works here.



End to end checksum

Lan communication model

### **Advantages of OSI Model**

**The OSI model helps users and operators of computer networks:**

* Determine the required hardware and software to build their network.
* Understand and communicate the process followed by components communicating across a network.
* Perform troubleshooting, by identifying which network layer is causing an issue and focusing efforts on that layer.

**Real life Example:**

**Luffy sends an e-mail to his friend Zoro.**

Step 1: Luffy interacts with e-mail application like Gmail , outlook , etc. Writes his email to send. (This happens in Layer 7: Application layer )

Step 2: Mail application prepares for data transmission like encrypting data and formatting it for transmission. (This happens in Layer 6: Presentation Layer )

Step 3: There is a connection established between the sender and receiver on the internet. (This happens in Layer 5: Session Layer )

Step 4: Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information. (This happens in Layer 4: Transport Layer )

Step 5: Addressing of packets is done in order to find the best route for transfer. (This happens in Layer 3: Network Layer )

Step 6: Data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection. (This happens in Layer 2: Data Link Layer )

Step 7: Lastly Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.

After the email reaches the receiver i.e. Zoro, the process will reverse and decrypt the e-mail content. At last, the email will be shown on Zoro’s email client.

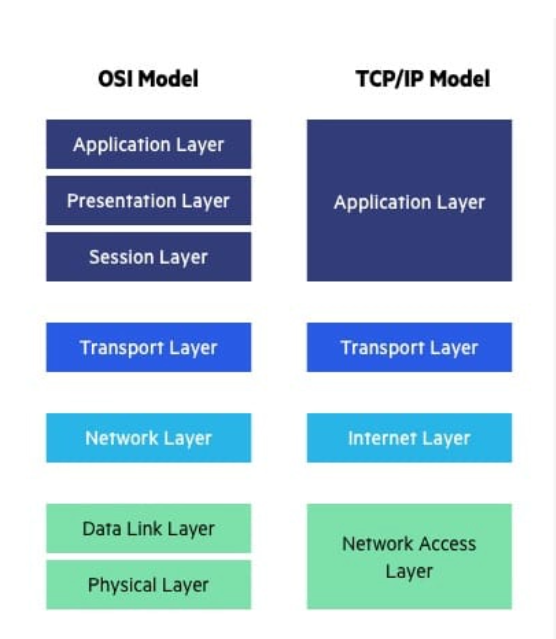
TCP/IP model Arpanet practical oriented model.

Application layer

Transport layer

Network layer

The [Transfer Control Protocol/Internet Protocol](https://www.imperva.com/learn/application-security/tcp-transmission-control-protocol/) (TCP/IP) is older than the OSI model and was created by the US Department of Defense (DoD). A key difference between the models is that TCP/IP is simpler, collapsing several OSI layers into one:

* OSI layers 5, 6, 7 are combined into one Application Layer in TCP/IP
* OSI layers 1, 2 are combined into one Network Access Layer in TCP/IP – however TCP/IP does not take responsibility for sequencing and acknowledgement functions, leaving these to the underlying transport layer.
* 

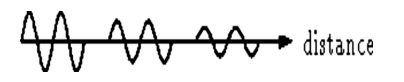
**Impairment causes in the network**

Signals travel through transmission media, which are not perfect

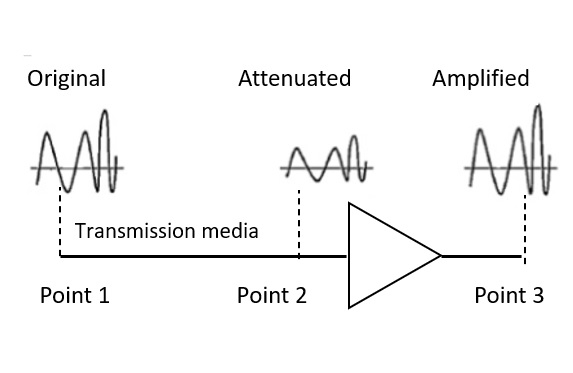
This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received.

* 1. **Attenuation (long distance +weak signal+ amplifier)**

Attenuation happens when a signal loses strength as it travels through the environment, making it harder to receive clearly at the other end.

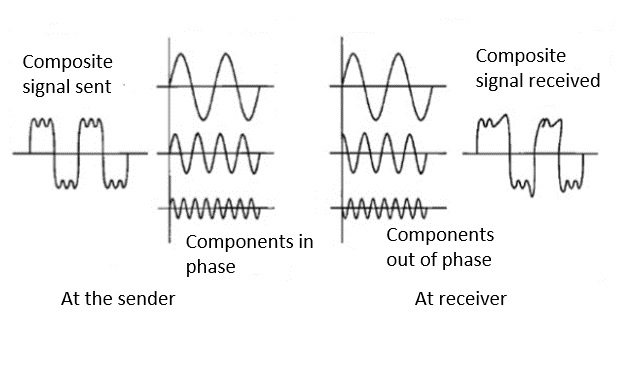


The above picture shows that the signal loses power at its travels time.



* 1. **Distortion(major impact)**

**Distortion** means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies.



* 1. **Noise** is another cause of impairment.

Noise is any unwanted signal that mixes with the transmitted signal, making it hard to get a clear message.

**Thermal noise:** Thermal noise is the random motion of electrons in a wire, which creates an extra signal not originally sent by the transmitter.

**Induced noise:** Induced noise comes from sources such as motors and appliancses. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.

**Crosstalk:** Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.

**Impulse noise**, may corrupt the signal.

Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

hub switches use IOS (internet operating system) operating system.

**Spanning Tree Protocol (STP)**

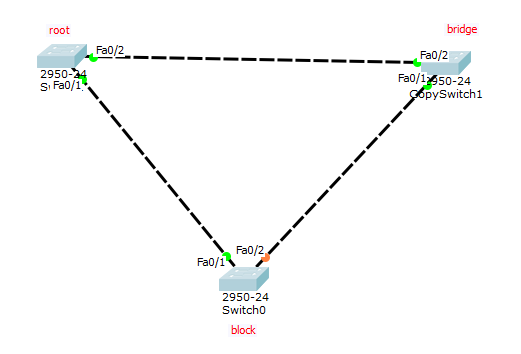
STP is a network protocol that prevents loops in Ethernet networks. It identifies and disables redundant paths in a network topology, ensuring there is only one active path between any two network devices. This helps maintain a loop-free network and improves reliability.

It decide on mac address which switch has to be root, bridge and block.

S1 mac largest block

S2 mac smallest root

S3 mac middle bridge



**Time to Live (TTL)**

TTL is a field in IP packets that determines how long a packet can exist in a network before being discarded. Each time a packet is routed through a device, its TTL value is decremented by one. When TTL reaches zero, the packet is dropped. This helps prevent packets from circulating indefinitely in case of routing loops.

**Lab networking**

There are two ways to give ip address

Static customize

Dynamic (IP is assigned automatically) DHCP(dynamic host configuration protocol).

<https://www.sitesbay.com/computer-network/cn-what-is-router>  
link for OSI Model

Router>EN

Router#config t

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 16.0.0.100 255.0.0.0

Router(config-if)#no shut

**Ip route network address of receiver subnet mask serial port address of receiver**

[What Is the OSI Model? | IBM](https://www.ibm.com/think/topics/osi-model)

link for OSI Model