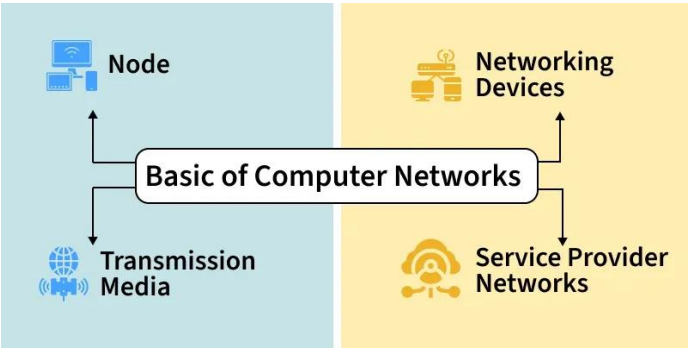
Lecture Notes For COMPUTER NETWORKS Prepared By PRANATI PATTNAIK

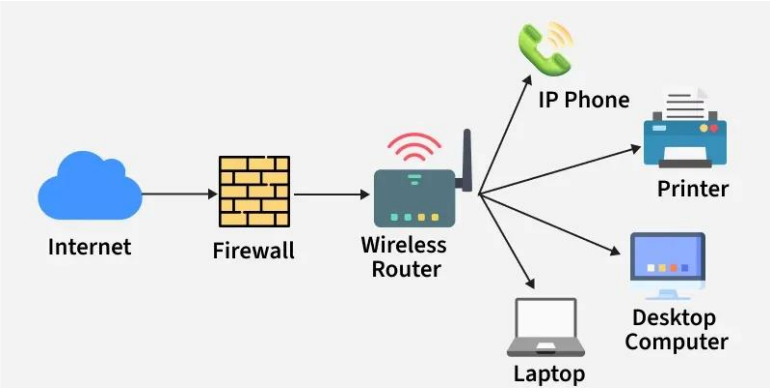
UNIT-1

A computer network is a collection of interconnected devices that share resources and information. These devices can include computers, servers, printers, and other hardware. Networks allow for the efficient exchange of data, enabling various applications such as email, file sharing, and internet browsing.



Network: A group of connected computers and devices that can communicate and share data.
Node: Any device that can send, receive, or forward data in a network. This includes laptops, mobiles, printers, earbuds, servers, etc.
Networking Devices: Devices that manage and support networking functions. This includes routers, switches, hubs, and access points.
Transmission Media: The physical or wireless medium through which data travels between devices.
Wired media: Ethernet cables, optical fibre.
Wireless media: Wi-Fi, Bluetooth, infrared
Service Provider Networks: Networks offered by external providers that allow users or organisations to lease network access and capabilities. This includes internet providers, mobile carriers, etc.
Working Of a Computer Network

The basic building blocks of a Computer network are Nodes and Links.
Network Node: Any device in a network, such as a modem, router, or computer, that sends or receives data.
Link: The medium that connects nodes, like cables, wires, or wireless signals.
Working: Networks use rules called protocols to send and receive data between devices. Each device is identified by a unique IP Address.
Firewall: A security tool (hardware or software) that monitors traffic. Based on set rules, it either allows, blocks, or drops data.



Types of Computer Network Architecture

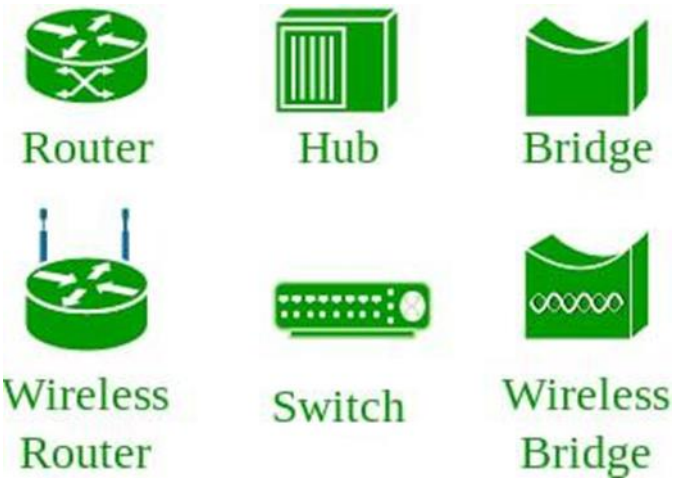
Computer Network falls under these broad Categories:

Client-Server Architecture: Client-Server Architecture is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behaviour.

Peer-to-Peer Architecture: In P2P (Peer-to-Peer) Architecture, there is not any concept of a Central Server. Each device is free for working as either client or server.

Network Devices

An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.



Various Network devices are:

1. Router
Connects multiple networks (like home network to the internet).
Directs data packets to their correct destination.

2. Switch
Connects devices within a network (like computers in an office).
Forwards data only to the specific device it is meant for.

3. Hub
Basic device that connects multiple devices in a network.
Sends data to all devices (less efficient than a switch).

4. Bridge
Connects and filters traffic between two networks or segments.
Helps reduce network traffic.

5. Gateway
Connects two different types of networks.
Translates data between different protocols.

6. Access Point (AP)
Provides wireless connectivity to devices.
Extends a wired network into a Wi-Fi network.

7. Modem
Converts digital data from a computer into signals for phone/cable lines and vice versa.
Provides internet access.
8. Firewall
Monitors and controls incoming and outgoing network traffic.
Provides security by blocking unauthorized access.

Goals of Networks
Convenience: Make computer use easier for users.
Efficiency: Manage hardware resources effectively for better performance.
Resource Management: Allocate CPU, memory, I/O, and storage fairly and efficiently.
Security & Protection: Protect data and resources from unauthorized access.
Reliability & Fault Tolerance: Ensure system runs smoothly and recovers from failures.
Scalability: Support growth in users, processes, and resources.

Uses of Computer Networks

Communication: Email, chat, and video conferencing.
Resource Sharing: Share printers, scanners, and files to save cost and effort.
Remote Access: Access data and systems from anywhere.
Collaboration: Work together on projects, share ideas, and review work.
E-commerce: Enable online shopping and secure payments.
Education: Support online learning, research, and student–teacher collaboration.

Characteristics of Computer Networks
1. Security
Protects data from unauthorized access, hacking, and viruses.
Uses tools like firewalls, encryption, and authentication to ensure safety.
2. Reliability
Ensures data and resources are always available.
Redundancy and backups keep the network running during failures.
3. Scalability
The ability to grow and handle more devices/users without performance loss.
Example: The internet supports millions of new users daily.
4. High Performance
Fast data transfer, low latency, and high throughput improve user experience.
Performance depends on bandwidth, response time, and processing power.
5. Quality of Service (QoS)
Prioritizes important data for faster delivery.
Ensures smooth communication, especially for streaming and video calls.

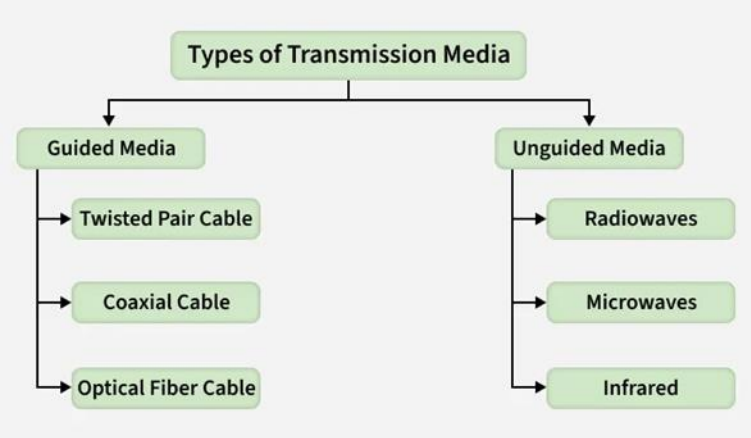
UNIT-2

Transmission Media in Computer Networks

Transmission media refers to the physical or wireless communication channel used to carry data signals from one device to another within a computer network. It forms the fundamental pathway through which information is transmitted, ensuring connectivity between networked devices.
The selection of a transmission medium depends on factors such as:

- Transmission distance
- Data transfer speed (bandwidth)
- Susceptibility to interference and noise
- Cost and installation requirements

Based on the nature of the transmission path, transmission media are broadly classified into two main types:



Guided Media

Guided Media also known as wired or bounded transmission media, refers to transmission media in which data signals are transmitted through a physical path using cables. The signal is confined and guided along a fixed route, providing controlled communication between network devices.

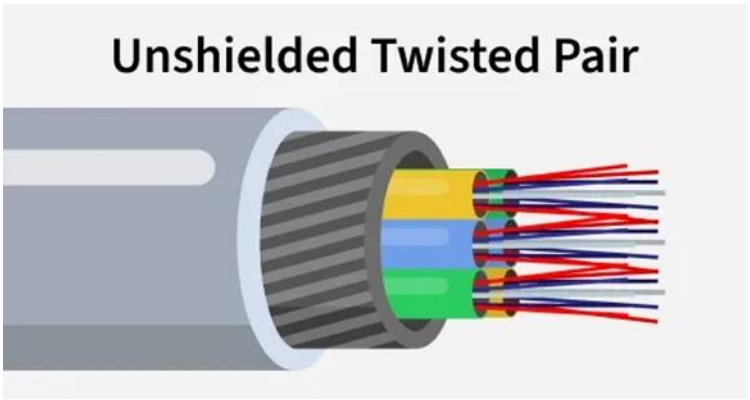
- Uses physical cables to transmit data signals.
- Provides dedicated and well-defined transmission paths.
- Major types of guided media included Twisted Pair Cables, Coaxial Cables and Optical Fiber Cables.
- Offers higher data transmission rates compared to most wireless media.
- Provides better security due to physical connectivity and limited signal leakage.
- Suitable for short to long-distance communication, depending on the cable type used.

1. Twisted Pair Cable

   A twisted pair cable consists of two individually insulated copper conductors twisted together in a helical pattern to minimize electromagnetic interference (EMI) and crosstalk between adjacent pairs. Multiple twisted pairs are typically enclosed within a protective outer sheath, making this cable one of the most commonly used and cost-effective guided transmission media.

- Twisting of conductors helps reduce interference and signal degradation.
- Multiple pairs can be bundled together within a single cable.
- Widely used due to low cost, flexibility, and ease of installation.
- Commonly used in telephone systems and local area networks (LANs).

(a) **Unshielded Twisted Pair (UTP):** UTP cable consists of twisted copper wire pairs without any additional metallic shielding. The twisting provides basic protection against interference, making UTP suitable for environments with moderate noise levels.



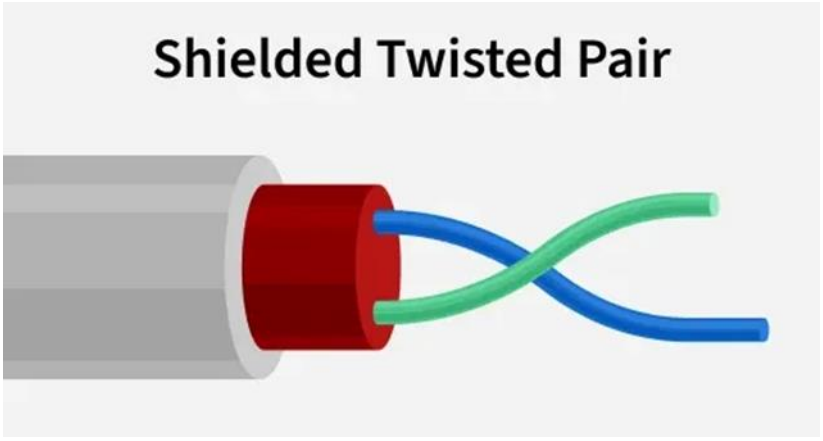
Advantages:

- Least expensive among guided transmission media.
- Easy to install and maintain due to its lightweight and flexible nature.
- Supports high data transmission rates over short distances.
- Widely used in Ethernet-based LANs and telephone networks.

Disadvantages:

- Lower performance and capacity compared to Shielded Twisted Pair (STP).
- Limited transmission distance due to signal attenuation.
- More susceptible to noise and electromagnetic interference.

(b) **Shielded Twisted Pair (STP):** Shielded Twisted Pair (STP) cable consists of twisted pairs of insulated copper conductors enclosed within an additional metallic shielding layer, such as a foil or braided shield. This shielding provides enhanced protection against external electromagnetic interference (EMI) and reduces crosstalk, resulting in more stable and reliable data transmission.



Shielded Twisted Pair

Advantages

Provides better performance at higher data transmission rates compared to UTP.

Significantly reduces electromagnetic interference and crosstalk. Ensures more reliable and stable communication, especially in noisy environments. Suitable for high-speed Ethernet networks and voice and data transmission systems.

Suitable for high-speed Ethernet networks and voice and data transmission systems.

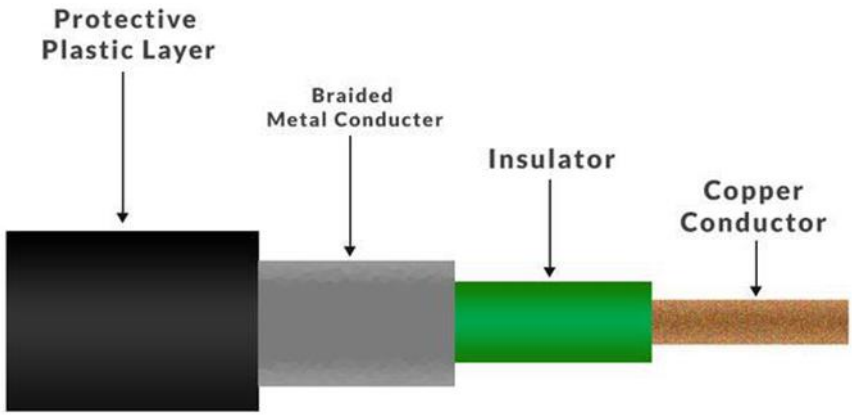
Disadvantages

- Higher cost compared to Unshielded Twisted Pair (UTP).
- More complex installation and termination due to shielding requirements.
- Bulkier and less flexible, making cable management more difficult.

2. Coaxial Cable

Coaxial Cable consists of a central copper conductor surrounded by a dielectric insulating layer, a metallic shielding layer, and an outer protective jacket. This structure allows signals to be transmitted with better protection against noise and interference compared to twisted pair cables.

- Supports data transmission in both baseband mode (single channel) and broadband mode (multiple channels).
- Provides higher bandwidth than twisted pair cables.
- Strong shielding makes it more resistant to noise, crosstalk, and electromagnetic interference (EMI).
- Commonly used in cable television (CATV), broadband networks, and analog television systems.
- More durable and reliable due to its layered construction.
- Easier to install and maintain compared to optical fiber cables.



Coaxial Cable

Advantages:

- Supports higher bandwidth than twisted pair cables.
- Offers better signal quality and reliability.
- Allows multiple channels using frequency division multiplexing (FDM).
- Less affected by external electromagnetic interference.

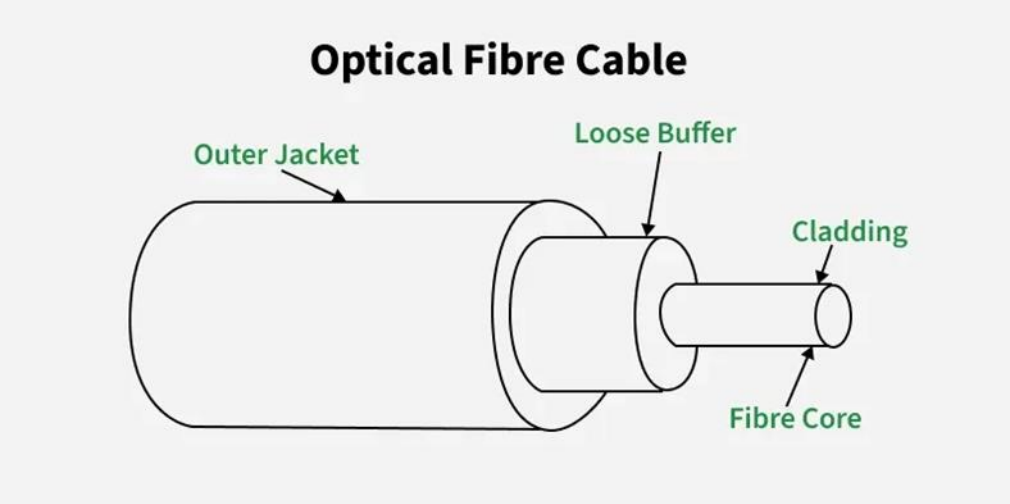
Disadvantages:

- More expensive than twisted pair cables.
- Requires proper grounding to ensure safety and minimize interference.
- Bulkier and less flexible due to multiple layers.
- More vulnerable to security breaches, as the cable can be physically tapped.

3. Optical Fiber Cable

Optical Fiber Cable is a guided transmission medium that transmits data in the form of light signals through a glass or plastic core using the principle of total internal reflection. The core is surrounded by a cladding layer with a lower refractive index, which confines the light within the core and enables high-speed, long-distance data transmission.

- Supports very large data volumes at extremely high speeds.
- Can operate in unidirectional or bidirectional communication modes.
- WDM (Wavelength Division Multiplexer) allows multiple light signals to be transmitted simultaneously over a single fiber.
- Widely used where high bandwidth, long distance, and low signal loss are required.



Advantages:

- Provides very high bandwidth and data-carrying capacity.
- Lightweight and compact, making installation easier over long distances.
- Exhibits low signal attenuation, suitable for long-distance communication.
- Immune to electromagnetic interference (EMI) and electrical noise.
- Resistant to corrosion and harsh environmental conditions.

Disadvantages:

- Complex installation and maintenance due to precise splicing and handling requirements.
- High initial installation and equipment cost.
- Fragile compared to copper cables and requires careful handling.

Applications:

- Medical: Used in endoscopy, imaging systems, and laser-based surgical procedures.
- Defense and Aerospace: Supports secure, high-speed, and interference-free communication.
- Communication: Widely used in internet backbone networks, undersea cables, and telecommunication systems.
- Industrial and Automotive: Used for sensing, lighting, data communication, and safety systems.

Single-Mode Fiber

SMF stands for single-mode fiber. It can transmit only one mode of light because of its small core diameter. Single-mode fibres are used in cable television and backbone networks. It is the best option for high-speed and data transmission over longer distances.

SMF transfers data up to 80 km at a speed of 100 gbps. Due to the small core diameter, it reduces signal attenuation and dispersion. SMF has the capacity to sustain signal integrity across long distances. SMF is frequently used in high- speed data transmission applications.

Multimode Fiber

- Multimode Fiber is also known as MMF. Multimode fiber can transfer the various light modes because its core diameter is larger; it is typically 50 or 62.5 microns. Multimode fiber is ideal for short-distance data transmission, such as within buildings or data centers, because it results in a lower bandwidth and shorter distances.
- Multimode fiber allows the propagation of many modes of light, which can be generated by LED or laser light sources, due to the larger core size.
- Multimode Fiber is commonly used in short-distance data transfer applications within buildings or data centers. It offers signal amplification-free data transfer across distances up to 550 metres at speeds up to 10 Gbps.
- Multimode fiber is less expensive than single-mode fiber, because, for manufacturing, it requires less accuracy, which is one of its main advantages. It is more suitable for short-distance installations since it is also simpler to terminate and splice.

Difference between Single-Mode Fiber and Multimode Fiber

Characteristics	Single-Mode Fiber	Multimode Fiber
Diameter of a Core	It has a small diameter core	It has a large diameter core
Source Optical	SMF is a type of laser.	Multimode is LED.
Bandwidth	The SMF bandwidth is more	The multimode fiber bandwidth is less
Fields	In telecom and CATV networks, SMF is preferred.	Multimode fibre is preferred in security systems and LANs.
Modal Dispersion	The single-mode fibre contains a narrower modal dispersion.	Multimode fibre has a wider range of modal dispersion.
Speed	It carries the signal with great speed	It transmits the signal slowly.
Cost	SMF is expensive.	Multimode fiber is low cost
Wavelength	The single-mode fibre wavelengths are 1310 nm and 1550 nm.	The multimode fibre wavelengths are 850 nm and 1300 nm.
Transmission Capactiy	SMF transmission capacity is less	Multimode fiber transmission capacity is more

Unguided Media

Unguided media, also known as wireless or Unbounded transmission media , uses electromagnetic waves to transmit data without any physical medium. Signals propagate through free space such as air or vacuum. The main types of unguided media are radio waves, microwaves, and infrared waves.

Features:

- Signals propagate through air or free space
- Less secure due to broadcast nature
- Suitable for long-distance communication

1.Radio Waves

Radio waves are a type of electromagnetic wave that can easily be generated and can propagate through buildings and other obstacles. They do not require line-of-sight between transmitting and receiving antennas, making them highly suitable for broadcast communication and wireless data transmission.

Frequency Range:

3 kHz – 300 GHz

Applications:

AM and FM radio broadcasting, television transmission, cordless phones, and wireless communication.

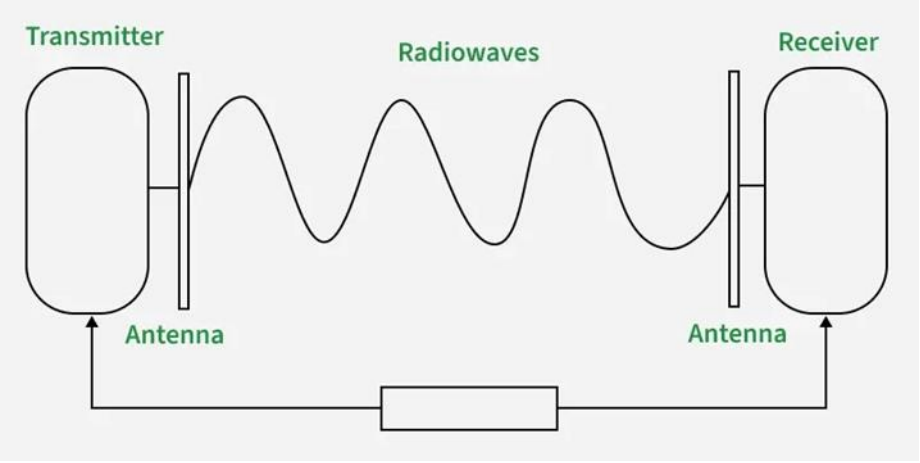
Types of Radio Waves:

- Shortwave: AM radio broadcasting
- VHF (Very High Frequency): FM radio and television
- UHF (Ultra High Frequency): Television and mobile communication

Components:

Transmitter: Generates and modulates the signal

Receiver: Receives and demodulates the signal



2. Microwaves

Micro waves are a form of unguided transmission media that use line-of-sight communication, where the transmitting and receiving antennas must be properly aligned. The transmission range depends on the height of the antennas. Microwaves operate in the frequency range of 1 GHz to 300 GHz and are widely used in mobile communication, satellite links, and television distribution.

Advantages:

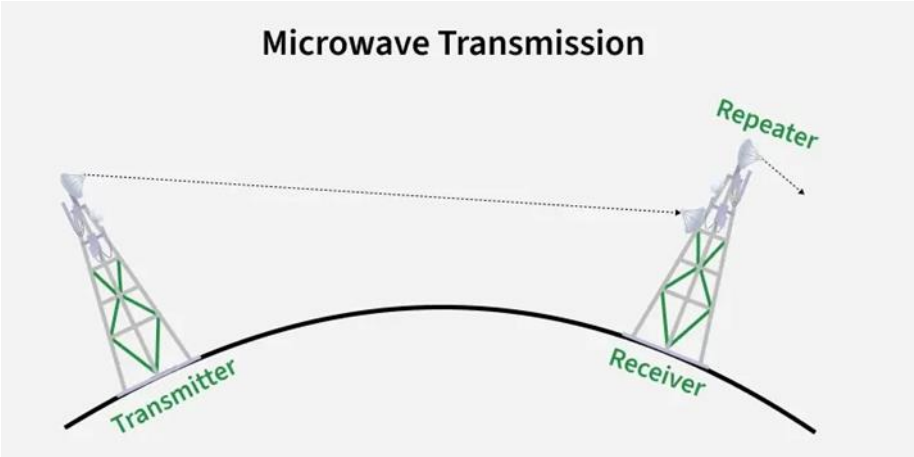
- Cost-effective compared to laying physical cables
- No need for land acquisition

- Suitable for communication over difficult terrains and oceans

Supports high data transmission rates

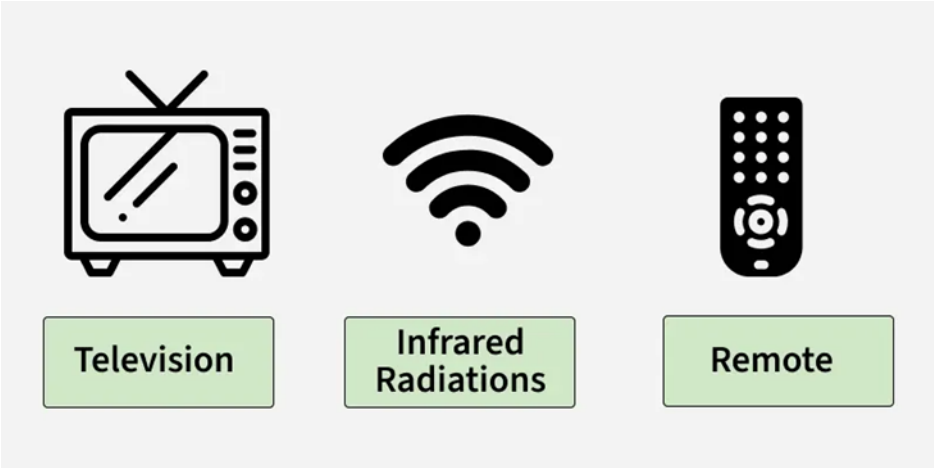
Disadvantages:

- Less secure without proper encryption
- Susceptible to weather conditions such as rain and fog
- Affected by obstacles due to line-of-sight requirement
- High cost of antenna design, installation, and maintenance



3. Infrared

Infrared waves are used for short-range wireless communication and operate in the frequency range of 300 GHz to 400 THz. They cannot penetrate solid obstacles, which limits their range but helps minimize interference between nearby systems. Infrared waves are commonly used in TV remote controls, wireless keyboards, mice, and printers.



Difference Between Radio Waves, Micro Waves, and Infrared Waves

Radio Waves	Microwaves	Infrared Waves
Omnidirectional in nature	Highly directional	Directional, requires line of sight (LOS)
Can penetrate buildings and obstacles easily due to low frequency	Poor penetration; line of sight required	Cannot penetrate obstacles
Frequency range: 3 kHz – 300 GHz	Frequency range: 1 GHz – 300 GHz	Frequency range: 300 GHz – 400 THz
Low security	Medium security (encryption possible)	Relatively high security but limited range
Moderate attenuation	Variable attenuation, depends on weather conditions	High attenuation
Some frequency bands require government licensing	Most frequency bands are licensed by the government	Generally unlicensed
Low to moderate cost	High cost	Low cost
Supports long-distance communication	Supports long-distance communication	Suitable only for very short-distance communication

Causes of Transmission Impairment

Transmission impairment refers to the loss or distortion of signals during data transmission, leading to errors or reduced quality in communication. Common causes include signal distortion, attenuation, and noise all of which can affect the clarity and reliability of transmitted data.

Attenuation: Loss of signal strength as the signal propagates over a transmission medium due to resistance and energy loss. In analog systems, amplifiers are used to increase signal strength, while in digital communication, repeaters or regenerators are used to restore the original signal.

Distortion: Occurs when the shape of the transmitted signal changes. This typically happens in composite signals where different frequency components travel at different speeds, causing phase shifts and timing differences at the receiver.

Noise: It refers to unwanted electrical or electromagnetic signals that interfere with the original signal, potentially corrupting data. Common types of noise include thermal noise, induced noise, crosstalk, impulse noise.

Factors Considered for Designing the Transmission Media

Bandwidth: It refers to the range of frequencies that a transmission medium can support.
Higher bandwidth allows higher data transmission rates, assuming other factors such as noise and attenuation remain constant.
Transmission Impairment : Transmission Impairment occurs when the received signal differs from the transmitted signal. Signal quality will be impacted as a result of transmission impairment.
Interference: It is the disturbance of a signal caused by the addition of unwanted signals from external sources such as electromagnetic radiation or neighbouring channels. It degrades signal clarity and may result in data corruption.

Ku-band (12–18 GHz) is a widely used microwave frequency range in satellite communication networks for high-speed data, VSAT services, and direct-to-home (DTH) television. Offering a balance between coverage and capacity, it enables smaller antenna sizes compared to C-band but is more susceptible to signal attenuation from heavy rain (rain fade).
Key Aspects of Ku-Band in Network Communication
Frequency Range: Operates within 12-18 GHz, which is part of the K-band spectrum (short for "K-under").
Primary Applications: Extensively used for Direct-to-Home (DTH) satellite TV, Very Small Aperture Terminal (VSAT) networks for enterprise data, and satellite backhaul for, for example, television networks.
Advantages:
Smaller Antennas: Due to higher frequencies, smaller dishes (typically 75 cm to 1.8 m) can be used, reducing installation costs and space requirements.
High Bandwidth: Suitable for high-speed data and video applications.
Less Interference: Less interference from terrestrial microwave links compared to C-band.

Disadvantages (Rain Fade): The 12-18 GHz frequency range is susceptible to significant signal attenuation during heavy rainfall, often known as "rain fade," which requires careful planning in tropical regions.
Network Role: Frequently used for connecting remote locations in TDMA satellite networks, SpaceX Starlink LEO satellites, and satellite communication in aerospace applications.

WIFI 802.11
802.11 is the IEEE standard for Wireless Local Area Networks (WLANs), commonly known as Wi-Fi, defining the rules for how devices connect and communicate wirelessly using radio waves for internet access and data exchange. It's a family of specifications (like 802.11a, b, g, n, ac, ax) developed by the Institute of Electrical and Electronics Engineers (IEEE) that evolve with amendments, improving speed, range, and efficiency, and forming the backbone of most home and office wireless networks.
Detailed Analysis of Standards

1. IEEE 802.11b (The Legacy Standard)
Frequency: 2.4 GHz.
Speed: Up to 11 Mbps.
Range: Approx 100 feet (30-35 meters) indoors.
Pros: Good range, cheap, low power consumption.
Cons: Very slow, prone to interference from microwaves and Bluetooth.
2. IEEE 802.11a (The Business Standard)
Frequency: 5 GHz.
Speed: Up to 54 Mbps.

Range: Short range (approx 25-30 meters).
Pros: Less interference (less crowded spectrum).
Cons: Higher cost, poor penetration through walls.

3. IEEE 802.11g (The Transition Standard)

Frequency: 2.4 GHz.
Speed: Up to 54 Mbps.
Pros: Combines speed of 'a' with range of 'b'.
Cons: Uses crowded 2.4 GHz, prone to interference.

4. IEEE 802.11n (Wi-Fi 4 - The MIMO Era)

Frequency: Dual-band (2.4 GHz and 5 GHz).
Speed: Theoretical 300-600 Mbps.
Key Technology: MIMO (Multiple-Input Multiple-Output) - Uses multiple antennas to send/receive data faster.
Range: Better range than previous standards due to stronger signals.

5. IEEE 802.11ac (Wi-Fi 5 - Gigabit Wi-Fi)

Frequency: Primarily 5 GHz (often combined with 2.4 GHz n-radio).
Speed: 400 Mbps up to 1300+ Mbps.
Key Technologies: Wider channels (80/160 MHz), MU-MIMO (Multi-User MIMO), Beam forming.
Pros: Very high speed, ideal for HD streaming and gaming.

Comparison Table

Standard	Generation	Frequency	Max Speed	Key Feature
802.11b	Wi-Fi 1	2.4 GHz	11 Mbps	Long Range
802.11a	Wi-Fi 2	5 GHz	54 Mbps	Less Interference
802.11g	Wi-Fi 3	2.4 GHz	54 Mbps	Compatibility
802.11n	Wi-Fi 4	2.4/5 GHz	600 Mbps	MIMO (Better Speed)
802.11ac	Wi-Fi 5	5 GHz	1300+ Mbps	Gigabit Speed

What is 2G (Second generation)?

2G mobile network is based on GSM(Global System for Mobile Communication). This technology was developed in Finland in 1991. Messages are encrypted in this technology. Digital signals used in this technology use less battery and hence lead to less power consumption. Also provided data services for mobile phones. Advanced versions are 2.5G and 2.75G.

What is 3G (Third generation)?

3G mobile network was developed in Japan in 2001 to achieve heights of speed which was lacking in 2G technology. The standards of this technology were set by the International Telecommunication Union(ITU). This technology provided users with services like GPS(Global Positioning System), video conferencing and mobile television.

Difference between 2G and 3G Cellular Network

Parameters	2G Network	3G Network
Introduction Year	Early 1990s	Early 2000s
Technology	GSM (Global System for Mobile Communications)	UMTS (Universal Mobile Telecommunications System)
Data Transfer Speed	Up to 50-100 kbps	Up to 2 Mbps, theoretically up to 14 Mbps
Voice Quality	Good, but with some limitations	Improved voice quality and clarity
Data Services	Basic SMS and limited data services	Enhanced data services including web browsing, video streaming, etc.
Network Bandwidth	Limited bandwidth	Higher bandwidth compared to 2G
Call Setup Time	Longer	Faster
Internet Browsing	Slow and basic web access	Faster web browsing and access to multimedia
Multimedia Support	Limited multimedia capabilities	Better support for multimedia applications
Latency	Higher latency	Lower latency
Network Coverage	Widely available in most regions	Coverage expanding but not as widespread as 2G
Frequency Bands	Operates in lower frequency bands (e.g., 900 MHz, 1800 MHz)	Operates in higher frequency bands (e.g., 1900 MHz, 2100 MHz)

Parameters	2G Network	3G Network
Standardization	Standardized for voice and basic data services	Standardized for improved data services and multimedia

Difference Between 4G and 5G

4G Technology	5G Technology
It stands for Fourth Generation technology	It stands for Fifth Generation technology
The maximum upload rate of 4G technology is 500 Mbps	While the maximum upload rate of 5G technology is 1.25 Gbps
The maximum download rate of 4G technology is 1 Gbps	While the maximum download rate of 5G technology is 2.5 Gbps.
The latency of 4G technology is about 50 ms	While the latency of 5G technology is about 1 ms
4G offers CDMA	While 5G offers OFDM, BDMA
4G can't differentiate between fixed and mobile devices	While 5G has the capability to differentiate between fixed a cognitive radio techniques to identify each device and offer the most appropriate delivery channel.
4G has the advantages of high speed handoffs, global mobility	While 5G has the advantages of extremely high speeds, low latency
4G can be used for high speed applications, mobile TV, wearable devices	While 5G can be used for high resolution video streaming, r robots and medical procedures

Cellular network generations (2G-5G) represent the evolution of mobile technology, significantly increasing data speeds, reducing latency, and improving capacity. 2G (GSM) introduced digital voice/SMS, 3G enabled mobile internet, 4G LTE allowed high-speed streaming, and 5G delivers near-instantaneous, high-capacity connectivity for IoT and advanced applications.

UNIT -3

Data Link Layer

The data link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model

- Responsible for the node-to-node delivery of data within the same local network.
- Major role is to ensure error-free transmission of information.
- Also responsible for encoding, decoding, and organizing the outgoing and incoming data.

The data link layer is further divided into two sub-layers.

Logical Link Control Sub-layer (LLC) –

Provides the logic for the data link, Thus it controls the synchronization, flow control, and error checking functions of the data link layer. Functions are -

- Error Recovery.
- It performs the flow control operations.
- User addressing.

Media Access Control Sub-layer (MAC) -

It is the second sub-layer of data-link layer. It controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. This layer is responsible for sending the data over the network interface card.

Functions are –

- To perform the control of access to media.
- It performs the unique addressing to stations directly connected to LAN.
- Detection of errors.

Data Link Layer Protocols

Key protocols include Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), and Frame Relay.

Key Data Link Layer Protocols

- **Ethernet (IEEE 802.3):** The most common protocol for wired Local Area Networks (LANs).
- **Wi-Fi (IEEE 802.11):** Protocols for wireless LANs.
- **Point-to-Point Protocol (PPP):** Used for direct connections between two nodes, commonly for router-to-router or client-to-ISP links.
- **High-Level Data Link Control (HDLC):** A bit-oriented protocol for communication over point-to-point and multipoint links.
- **Frame Relay:** A streamlined protocol for transmitting data over WANs.
- **ATM (Asynchronous Transfer Mode):** Used for high-speed switching of data, voice, and video.
- **Bluetooth/BLE:** Wireless PAN protocols used for short-range device communication.

Design issues with data link layer are :

The data link layer (Layer 2) ensures node-to-node data transfer, managing framing, physical addressing, error control, and medium access control (MAC). Key design issues include framing (delimiting data), flow control (preventing receiver overload), and error handling. Examples include Ethernet (wired), WLAN (wireless), and Bluetooth, each handling these issues differently.

The main functions and the design issues of this layer are

- Providing services to the network layer
- Framing
- Error Control
- Flow Control

The types of services provided can be of three types –

- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

Unacknowledged and connectionless services.

- Here the sender machine sends the independent frames without any acknowledgement from the sender.
- There is no logical connection established.

Acknowledged and connectionless services.

- There is no logical connection between sender and receiver established.
- Each frame is acknowledged by the receiver.
- If the frame didn't reach the receiver in a specific time interval it has to be sent again.
- It is very useful in wireless systems.

Acknowledged and connection-oriented services

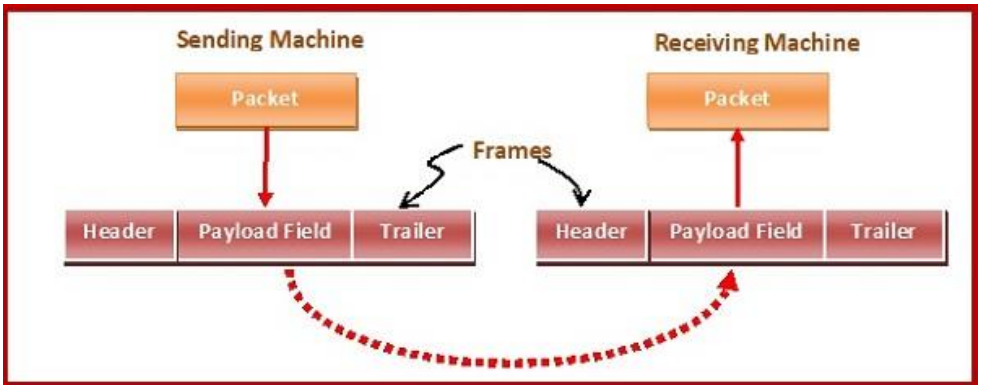
- A logical connection is established between sender and receiver before data is trimester.
- Each frame is numbered so the receiver can ensure

Framing

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely –

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer



Error Control

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are –

- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them
- Controlling access to shared channels in case of broadcasting

Flow Control

The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are –

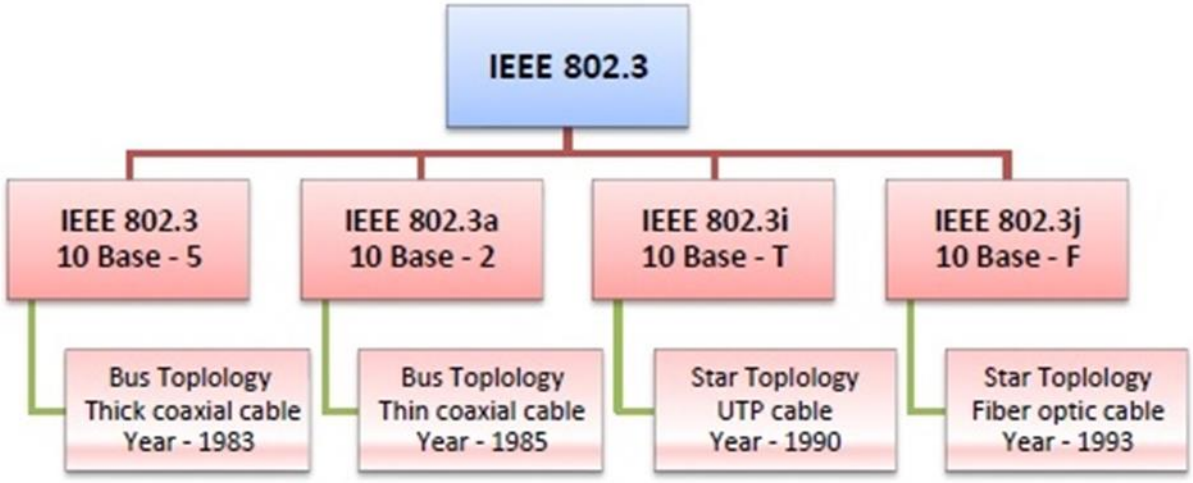
- Feedback based flow control
- Rate based flow control

Key Data Link Layer Protocols

- **Ethernet (IEEE 802.3):** Uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection) for wired networks to manage collisions. It provides unacknowledged, connectionless service.
  Ethernet is a set of technologies and protocols that are used primarily in LANs. There are a number of versions of IEEE 802.3 protocol. The most popular ones are –

- IEEE 802.3: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.

- IEEE 802.3a: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m .
- IEEE 802.3i: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium.
- IEEE 802.3i: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.



- **Wi-Fi (IEEE 802.11):** Protocols for wireless LANs. WLAN utilizes CSMA/CA (Collision Avoidance). Due to the high error rates in wireless, it often requires explicit link-layer acknowledgments (ACKs).
- **Bluetooth**

  It is a built-in platform support for Bluetooth Low Energy (BLE) in the central role and provides APIs that apps can use to discover devices, query for services, and transmit information.

  Common use cases include the following:
- Transferring small amounts of data between nearby devices.
- Interacting with proximity sensors to give users a customized experience based on their current location.

  In contrast to classic Bluetooth, BLE is designed for significantly lower power consumption. This allows apps to communicate with BLE devices that have stricter power requirements, such as proximity sensors, heart rate monitors, and fitness devices.

Switching techniques

Switching is a technique of transferring the information from one computer network to another computer network. The bandwidth of the network increases with the help of a switch.

Advantages

- It tries to reduce the workload on individual PCs because it always sends the information to specified addressed devices.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision because; switch creates the collision domain for each connection.

Disadvantages

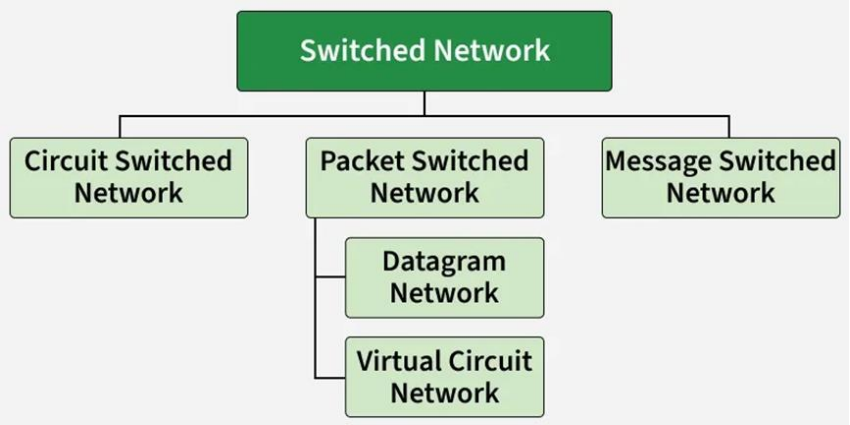
The disadvantages of switching are as follows −

- A Switch is more expensive than network bridges.

- It cannot determine the network connectivity issues easily.
- The proper designing and configuration of the switch are required to handle multicast packets.

Types of Switching

There are three types of switching methods:



Message Switching:

Message Switching is a switching technique where the entire message is sent as a single unit from one node to another without a dedicated path between the sender and receiver. Each intermediate node stores the message temporarily and then forwards it to the next node until it reaches its destination. Communication occurs hop by hop, with messages being the smallest unit of transfer.

Key Features of Message Switching

1. Store-and-Forward

- Each intermediate node must store the entire message before forwarding it.
- Transmission occurs only if the next link and node are available; otherwise, the message waits in storage until resources are free.

2. Message Delivery

- Messages are transmitted as complete units, with a header containing routing information (source and destination addresses).
- Communication is hop by hop until the message reaches its destination.

3. Network Components

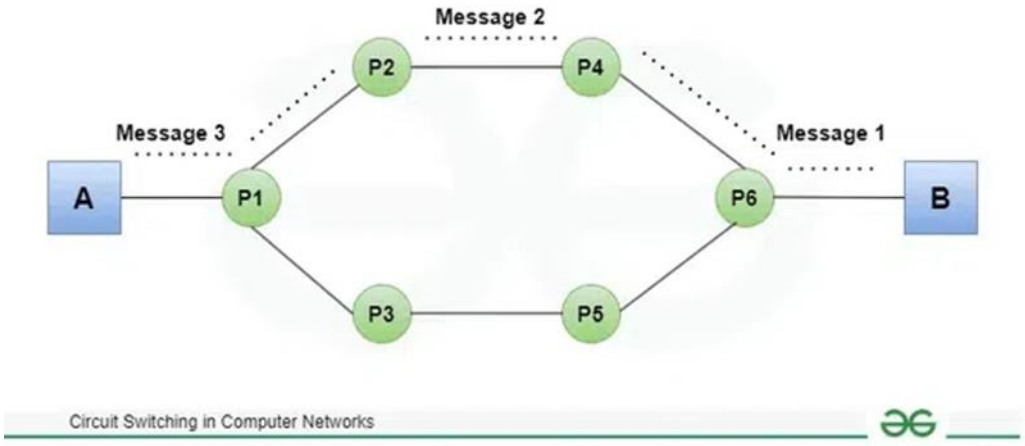
A message-switching network consists of:

- Transmission links (channels)
- Store-and-forward switching nodes
- End stations (source and destination devices)

Circuit Switching:

Circuit Switching establishes a dedicated path between sender and receiver before communication, using the full network bandwidth. Data flows without delay, and bit delay remains constant. While it guarantees a fixed data rate, it is costly and inefficient for high-traffic or large networks due to reserved resources.

- Bandwidth is divided into pieces.
- Bit delay is constant during communication.
- Data can flow without delay once the circuit is established.



The telephone system network is one of the examples of Circuit switching. FDM (Frequency Division Multiplexing) and TDM (Time Division Multiplexing) are two methods of multiplexing multiple signals into a single carrier.

1. **Frequency Division Multiplexing (FDM):**

- Divides total bandwidth into non-overlapping frequency bands.
- Each band carries a separate signal simultaneously.
- Used in radio, TV, and optical fiber for multiple independent signals.

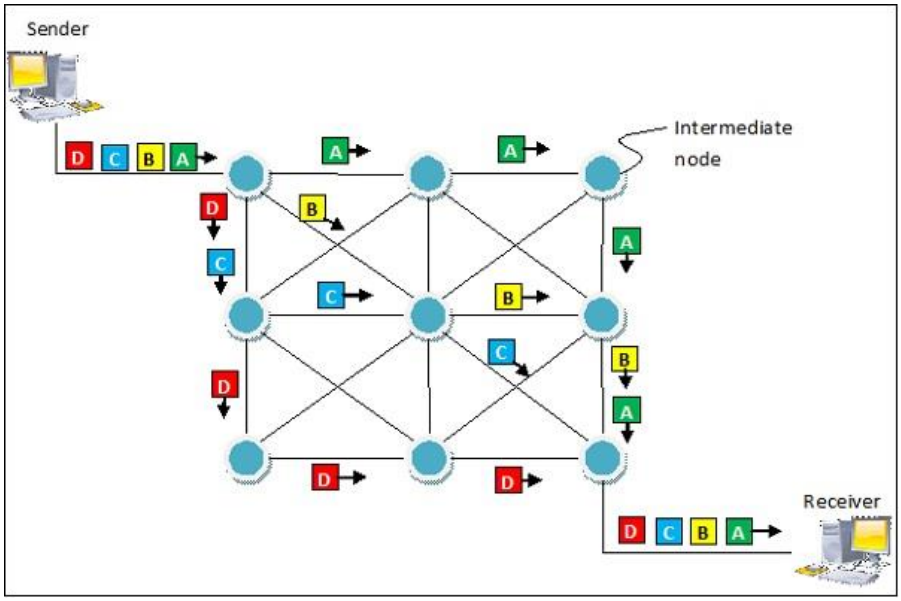
2. Time Division Multiplexing (TDM):

- Transmits multiple signals over the same channel at different time slots.
- Uses synchronized switches at both ends.
- Suitable for long-distance links with heavy data traffic.
- Also called a digital circuit switch

- **Packet Switching:**

Packet switching is the foundation of modern computer networks, including the Internet. Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication. In this method:

- Data is divided into small packets.
- Each packet carries a portion of the message and the destination address.
- Packets may travel through different paths in the network.
- At the destination, packets are reassembled to reconstruct the original message.

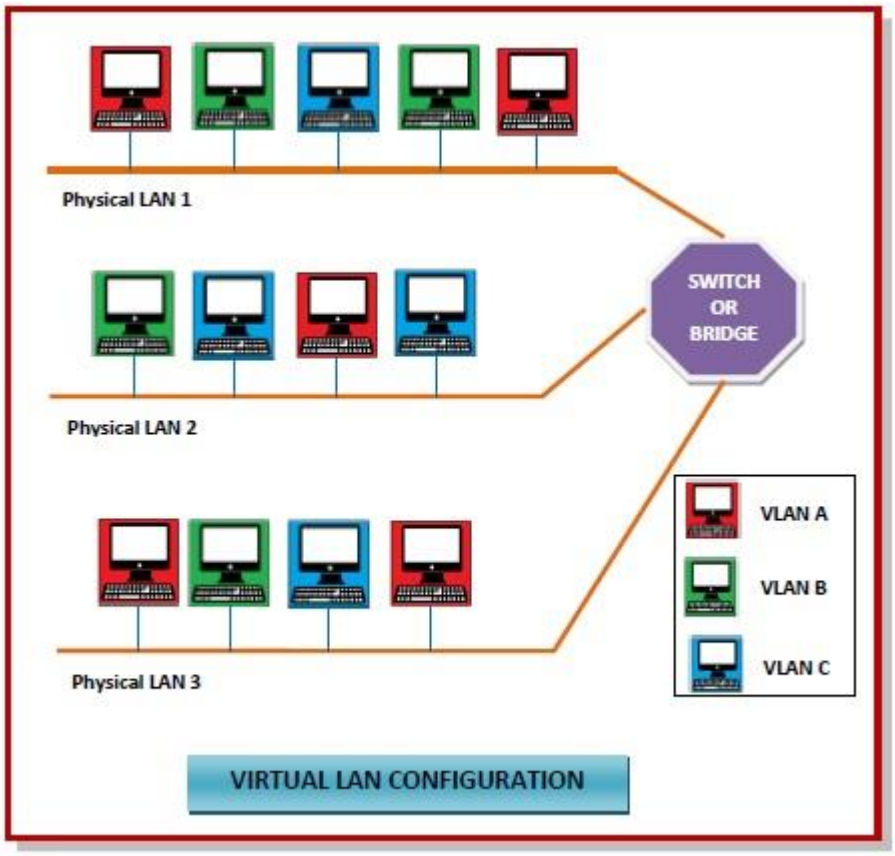


Message Switching	Circuit Switching	Packet Switching
No dedicated path; the entire message is stored and forwarded at each node.	A fixed, dedicated path is established before transmission.	Data is split into packets that follow dynamic or virtual paths.
Very inefficient due to full message storage and forwarding.	Inefficient because bandwidth remains reserved even when idle.	Highly efficient due to optimal bandwidth utilization.
High transmission delay.	Low delay after initial setup.	Delay varies based on network conditions.
Less reliable and obsolete.	Reliable with guaranteed connection.	Reliable with error control and retransmission.
Used in telegraph systems.	Used in traditional telephone networks.	Used in the Internet.

Virtual LAN (VLAN)

Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network. Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or

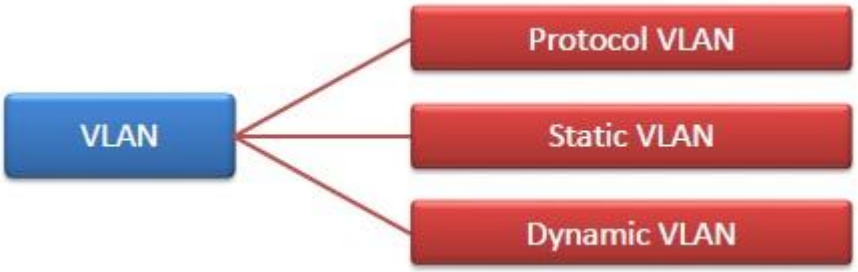
multiple switches or bridges. This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.



Features of VLANs

- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.
- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids is quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed.

Types of VLANs



- **Protocol VLAN** − Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.
- **Port-based VLAN** − This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.
- **Dynamic VLAN** − Here, the network administrator simply defines network membership according to device characteristics.

UNIT-4

Network Layer

Design Issues

The network layer or layer 3 of the OSI (Open Systems Interconnection) model is concerned delivery of data packets from the source to the destination across multiple hops or links.

The design issues can be elaborated under four heads –

- Store − and − Forward Packet Switching
- Services to Transport Layer
- Providing Connection Oriented Service
- Providing Connectionless Service

Store − and − Forward Packet Switching

The network layer uses store and forward packet switching. The node which has a packet to send, delivers it to the nearest router. The packet is stored in the router until it has fully arrived and its checksum is verified for error detection. Once, this is done, the packet is forwarded to the next router. Since, each router needs to store the entire packet before it can forward it to the next hop, the mechanism is called store − and − forward switching.

Services to Transport Layer

The network layer provides service its immediate upper layer, namely transport layer, through the network − transport layer interface. The two types of services provided are −

- Connection − Oriented Service − In this service, a path is setup between the source and the destination, and all the data packets belonging to a message are routed along this path.
- Connectionless Service − In this service, each packet of the message is considered as an independent entity and is individually routed from the source to the destination.

The objectives of the network layer while providing these services are –

- The services should not be dependent upon the router technology.
- The router configuration details should not be of a concern to the transport layer.
- A uniform addressing plan should be made available to the transport layer, whether the network is a LAN, MAN or WAN.

Providing Connection Oriented Service

In connection − oriented services, a path or route called a virtual circuit is setup between the source and the destination nodes before the transmission starts. All the packets in the message are sent along this route. Each packet contains an identifier that denotes the virtual circuit to which it belongs to. When all the packets are transmitted, the virtual circuit is terminated and the connection is released. An example of connection − oriented service is Multi Protocol Label Switching (MPLS).

Providing Connectionless Service

In connectionless service, since each packet is transmitted independently, each packet contains its routing information and is termed as datagram. The network using datagrams for transmission is called **datagram** networks or datagram subnets. No prior setup of routes are needed before transmitting a message. Each datagram belong to the message follows its own individual route from the source to the destination. An example of connectionless service is Internet Protocol or IP.

Internet Protocols

The Internet Protocol (IP) assigns a unique address to each device, enabling communication over the internet.

Internet Protocol Version 4 (IPv4)

IPv4, the earlier version, uses 32-bit addresses, providing about 4.3 billion unique addresses, which are now nearly exhausted due to the rapid growth of the internet and IoT devices.

- IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.
- IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into
- Class A - it uses first octet for network addresses and last three octets for host addressing
- Class B - it uses first two octets for network addresses and last two for host addressing
- Class C - it uses first three octets for network addresses and last one for host addressing
- Class D - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- Class E - It is used as experimental.

Drawbacks of IPv4

- Limited address space: The 32-bit IPv4 address space is insufficient for the growing number of connected devices.
- Complex configuration: IPv4 relies on manual setup or DHCP, which can lead to configuration errors.
- Inefficient routing: Variable and complex headers increase processing overhead.
- Lack of built-in security: Security features are not inherent and require additional mechanisms.
- Limited QoS support: Traffic prioritization is weak, affecting real-time applications.
- Router-based fragmentation: Packet fragmentation by routers reduces efficiency and may cause data loss.
- Broadcast traffic overhead: Broadcast communication increases unnecessary network traffic and degrades performance.

Internet Protocol Version 6 (IPv6)

- IPv6, the newer version, uses 128-bit addresses, offering a vastly larger address space to overcome IPv4 exhaustion and support future internet expansion.

- Pv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each

Difference Between IPv4 and IPv6

The following table summarizes the key differences between IPv4 and IPv6 addressing:

Pv4 (Internet Protocol Version 4)	**IPv6 (Internet Protocol Version 6)**
Encryption and authentication is not provided in IPv4 (Internet Protocol Version 4).	Encryption and authentication is provided in IPv6 (Internet Protocol Version 6)
Header of IPv4 is 20 – 60 bytes.	Header of IPv6 is fixed at 40 bytes
Checksum field is available in IPv4.	Checksum field is not available in IPv6.
Packet flow identification is not available in IPv4 (Internet Protocol Version 4).	Packet flow identification is available in IPv6. Flow label field is available in the header.
IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each	An IPv6 address is represented as eight groups of four hexadecimal digits, each

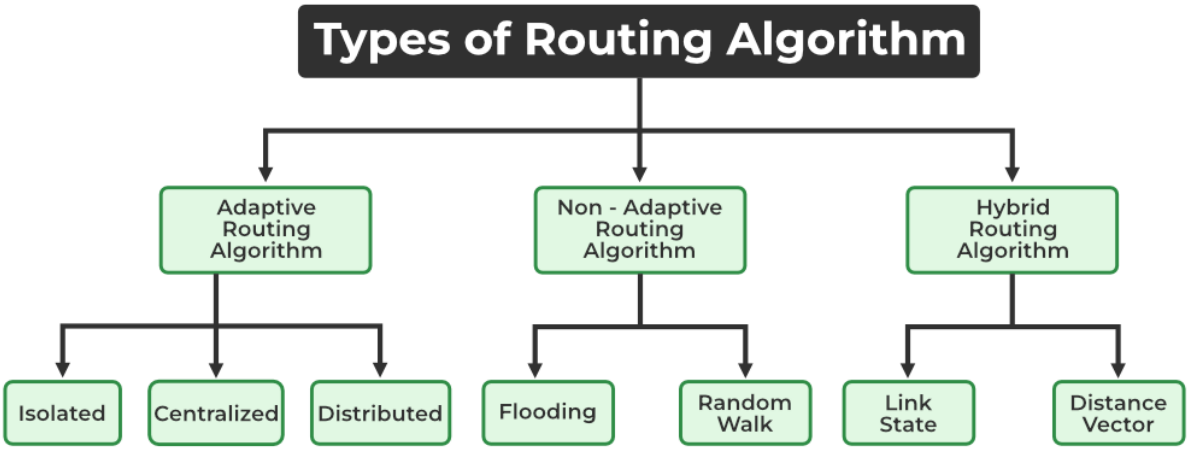
ranging from 0 to 255, separated by dots.	group representing 16 bits.
Sender and forwarding routers performs fragmentation in IPv4	Fragmentation is performed only by the sender in IPv6.
In IPv4, security features relies on application	In IPv6, there is an inbuilt security feature named IPSEC.
End to end connection integrity cannot be achieved in IPv4.	End to end connection integrity can be done in IPv6.
IPv4 supports DHCP and Manual address configuration	IPv6 supports renumbering and auto address configuration.
IPv4 addresses are 32-bit long	IPv6 addresses are 128 bits long.
The address space in IPv4 is 4.29 ×109	The address space in IPv6 is 3.4 ×1038
IPv4 has a broadcast message transmission scheme.	Multicast and Anycast message transmission scheme is available in IPv6.

Routing Algorithm

A routing algorithm is a procedure that lays down the route or path to transfer data packets from source to the destination. They help in directing Internet traffic efficiently. After a data packet leaves its source, it can choose among the many different paths to reach its destination. Routing algorithm mathematically computes the best path, i.e. least cost path that the packet can be routed through.

Types of Routing Algorithms

Routing algorithms can be broadly categorized into two types, adaptive and non adaptive routing algorithms. They can be further categorized as shown in the following diagram



Routing

Network routing is the process of selecting the best path for data to travel across one or more networks. It plays a vital role in the internet by ensuring that data packets reach their correct destination efficiently.

Routing in computer networks determines the optimal, lowest-cost path for data packets from source to destination using adaptive (dynamic) or non-adaptive (static) algorithms. Key principles include finding least-cost paths, maintaining routing table efficiency, and ensuring network stability, while major issues involve congestion, packet looping, scalability, and adapting to topological changes.

- Routing determines the path IP packets follow from source to destination.
- It is used in packet-switched networks like the Internet.
- Different routing methods are used to optimize speed, reliability, and performance.

Common Routing Protocols

- Distance Vector (e.g., RIP): Routers share their entire routing table with neighbors, leading to potential slow convergence.
- Link State (e.g., OSPF): Routers map the entire network topology to calculate the shortest path, offering faster convergence.

Distance Vector Routing (DVR) Protocol

In distance-vector routing (DVR), each router is required to inform the topology changes to its neighboring routers periodically.

How the DVR Protocol Works

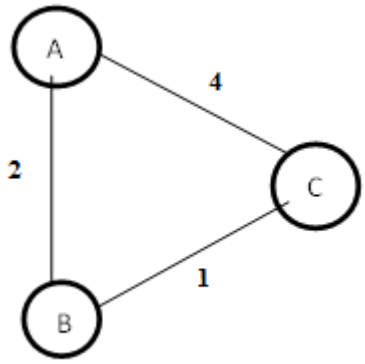
- In DVR, each router maintains a routing table. It contains only one entry for each router. It contains two parts − a preferred outgoing line to use for that destination and an estimate of time (delay). Tables are updated by exchanging the information with the neighbor's nodes. Ex − send echo request).
- Routers periodically exchange routing tables with each of their neighbors.

- It compares the delay in its local table with the delay in the neighbor's table and the cost of reaching that neighbor.
- If the path via the neighbor has a lower cost, then the router updates its local table to forward packets to the neighbor.

Example − Distance Vector Router Protocol

In the network shown below, there are three routers, A, B, and C, with the following weights − AB =2, BC =3 and CA =5.

Step 1 − In this DVR network, each router shares its routing table with every neighbor. For example, A will share its routing table with neighbors B and C and neighbors B and C will share their routing table with A.



Form A	A	B	C
A	0	2	3
B			
C			

Form B	A	B	C
A			
B	2	0	1
C			

Form C	A	B	C
A			
B			
C	3	1	0

Step 2 – If the path via a neighbor has a lower cost, then the router updates its local table to forward packets to the neighbor. In this table, the router updates the lower cost for A and C by updating the new weight from 4 to 3 in router A and from 4 to 3 in router C.

Form A	A	B	C
A	0	2	3
B			
C			

Form B	A	B	C
A			
B	2	0	1
C			

Form C	A	B	C
A			
B			
C	3	1	0

Step 3 – The final updated routing table with lower cost distance vector routing protocol for all routers A, B, and C is given below –

Router A

Form A	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

Router B

Form B	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

Router C

Form C	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

Link State Routing

Link state routing is a method in which each router shares its neighbourhoods knowledge with every other router in the internetwork. In this algorithm, each router in the network understands the network topology then makes a routing table depend on this topology. Each router will share data about its connection to its neighbour, who will, consecutively, reproduce the data to its neighbours,

In the Link - State Routing Protocol, the router attempts to construct its own internal map of the network topology. It provides the information about whether the link to reach the router is active or not.

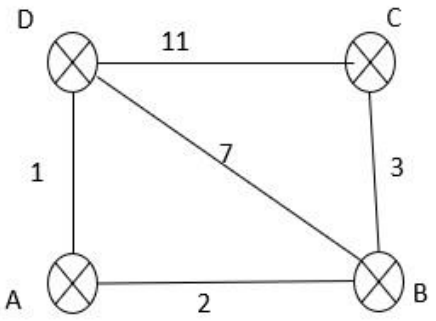
Every router will create something called Link state packets.

In the first round every node creates link state packets

Step 1 Prepare the link state packet at every router.

D	
Seq (a Sequence Number included)	
TTL (Time to Live)	
C	11
B	7
A	1

C	
Seq	
TTL	
D	11
B	3



A	
Seq	
TTL	
B	2
D	1

B	
Seq	
TTL	
A	2
D	7
C	3

Step 2 Every router flood the link state packets to every offer router

At A

Link state packet B, C, D

From B

A	2

C	3
D	7

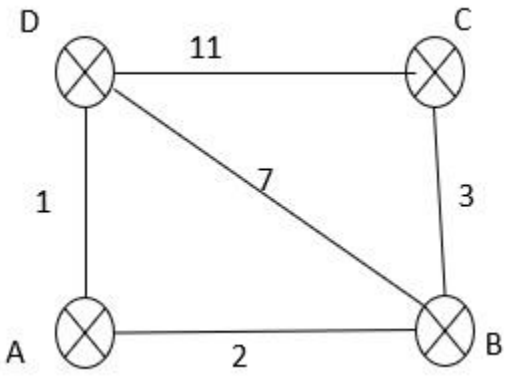
From C

B	3
D	11

From D

A	1
B	7
C	11

Now A can construct the entire graph using the received link protocol.



Like this, every node is able to construct the graph in its own memory. Every node has an entire graph. So every router can apply the Dijkstra algorithm to find the shortest path.

Advantages

- Fast Network Convergence: It is the main advantage of the link-state routing protocol. Because of receiving an LSP, link-state routing protocols immediately flood the LSP out of all interfaces without any changes except for the interface from which the LSP was received.
- Topological Map: Link-state routing uses a topological map or SPF tree for creating the network topology. Using the SPF tree, each router can separately determine the shortest path to every network.
- Hierarchical Design: Link-state routing protocols use multiple areas and create a hierarchical design to network areas. The multiple areas allow better route summarization.
- Event-driven Updates: After initial flooding of LSPs, the LSPs are sent only when there is a change in the topology and contain only the information regarding that change. The LSP contains only the information about the affected link. The link-state never sends periodic updates.

Disadvantages

- Memory Requirements The link-state routing protocol creates and maintains a database and SPF tree. The database and SPF tree required more memory than a distance vector protocol.
- Processing Requirements Link-state routing protocols also require more CPU processing because the SPF algorithm requires more CPU time than distance-vector algorithms just like Bellman-Ford because link-state protocols build a complete map of the topology.
- Bandwidth Requirements The link-state routing protocol floods link-state packet during initial start-up and also at the event like network breakdown, and network topology changes, which affect the available bandwidth on a network. If the network is not stable it also creates issues on the bandwidth of the network

Open Shortest Path First (OSPF) Protocol

Open Shortest Path First (OSPF) is a routing protocol for IP networks. It is used within a network or area. OSPF is an interior gateway protocol designed for a single autonomous system.

OSPF uses a link-state routing algorithm. Each router has information about every link and router in the network. It finds the shortest path to each destination. OSPF learns about all routers and subnets in the network to build a link-state database (LSDB). Routers exchange link-state advertisements (LSAs) to share information about routers, subnets, and more.

Basic Terms

- Link-state Description of a link between two routers, including its characteristics.
- SPF algorithm Computes shortest path from a source router to others.
- OSPF cost Metric representing the cost of using a link or path.
- Shortest path tree Shows the shortest path from a source router to all others.
- Areas Logical subdivisions of an OSPF network with similar characteristics.
- Border routers Connect different areas or external networks.
- Link-state packets Contain link-state advertisements and are sent by rout

OSPF Operation

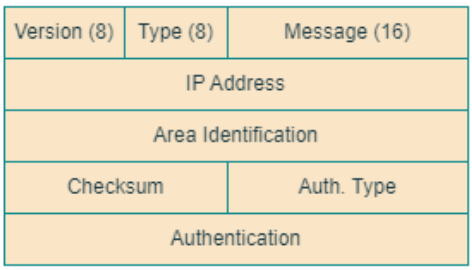
OSPF operates in three steps neighbor discovery, database exchange, and route calculation.

OSPF Steps

- Neighbor Discovery Routers find and communicate with neighbors on the same link.
- Database Exchange Routers exchange LSAs to learn about network topology.
- Route Calculation Routers use SPF algorithm to find the best paths.

OSPF Message Format

An OSPF message has different parts



OSPF Protocol

- Version A number that shows the version of OSPF being used.
- Type A number that tells the type of OSPF packet.
- Message The length of the whole message, including the header.

Other fields in the OSPF message

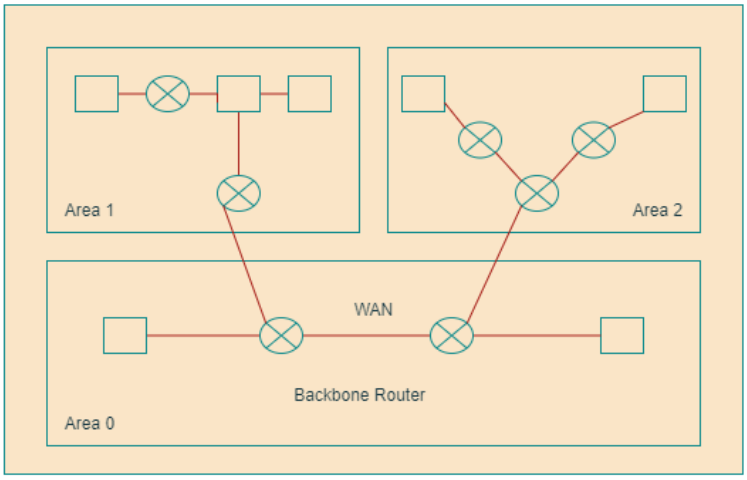
- Source IP address The address from which the packets are sent.
- Area identification The area where the routing happens.
- Checksum Used to find and fix errors in the message.
- Authentication type Two types - 0 means no authentication, 1 means password-based authentication.
- Authentication The actual authentication data in the message.

OSPF Design

- Divide network into areas for efficient routing.
- Use ABRs to connect and summarize routing info between areas.
- All areas connect to the backbone area (area 0) for network communication.

Areas in OSPF

There are different types of areas in OSPF, each with different characteristics and functions.



Types of OSPF Areas

Here are the different types of OSPF Areas

- Backbone area Central area (0) connecting all others and external networks.
- Standard area Non-backbone area connected to backbone. Supports all LSAs except 4 and 5.
- Stub area Non-backbone area not accepting external routes. Receives default route from ABRs.
- Totally stubby area More restrictive stub area, not accepting inter-area routes.
- Not-so-stubby area (NSSA) Special stub area allowing external routes with type 7 LSAs.
- Totally not-so-stubby area (NSSA) More restrictive NSSA, not accepting

Advantages of OSPF

- OSPF has many advantages over RIP. It is another interior gateway protocol based on a distance-vector routing algorithm. Advantages of OSPF are

- OSPF can handle variable length subnet masks (VLSM). It can support subnets of different sizes and optimize the use of IP address space.
- OSPF can support up to 65535 hops, while RIP has a limit of 15 hops. This makes OSPF more scalable and suitable for large networks.
- OSPF can perform route summarization and redistribution. It can reduce routing overhead and improve efficiency by aggregating routes and exchanging routes with other routing protocols.
- OSPF can use authentication to secure routing updates and prevent unauthorized or malicious changes to the network topology.
- OSPF can divide the network into areas and use different types of areas to reduce routing complexity and improve performance.

Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is designed to help routers determine the best path for sending data packets across a network. It uses hop count as its routing metric and is primarily used in small to medium-sized networks due to its scalability limitations.

- RIP operates at the Network Layer (Layer 3) of the OSI model and maintains routing tables on each router.
- Every 30 seconds, routers exchange their complete routing tables with neighbours using periodic updates.
- The hop count metric defines the number of routers a packet must pass through to reach its destination.

Note: RIP supports a maximum hop count of 15, which limits its use in larger networks. A hop count of 16 is considered unreachable.

Hop Count

Hop count is a routing metric that represents the total number of routers a data packet must pass through to travel from the source device to the destination device.

- Each router crossed by a packet is counted as one hop.
- Used by routing protocols like RIP to determine the best path.
- RIP selects the route with the lowest hop count as the optimal route.
- The maximum hop count in RIP is 15; a hop count of 16 is considered unreachable.
- Limiting the hop count helps prevent routing loops.
- This limitation reduces RIP's scalability, making it unsuitable for large networks.

Features of RIP

- Exchanges updates periodically (every 30 seconds).
- Broadcasts (RIPv1) or multicasts (RIPv2/RIPng) routing information.
- Sends entire routing tables in updates.
- Works on the principle of routing by rumour (trusting neighbours' information).

- Uses route poisoning and split horizon to avoid routing loops.

How RIP Works

Routing Information Protocol (RIP) is a distance-vector routing protocol that determines the best path to a destination network based on hop count.

- Each router maintains a routing table containing distances to all known networks.
- Routers periodically exchange routing information with neighboring routers.
- Every 30 seconds, routers broadcast or multicast their entire routing table.
- If a router learns a shorter path, it updates its routing table accordingly.
- If a route is not updated within 180 seconds, it is marked as invalid.
- If the route remains unused for 240 seconds, it is removed (flushed) from the routing table.
- These timers help maintain accurate routing information and prevent stale routes.

Benefits of RIP

- Easy to understand
- Feasible to configure
- Supported by all the routers
- Support load balancing

Versions of RIP

There are in total 3 versions of RIP:

- RIPv1
- RIPv2
- RIPng

Limitation of RIP

- The followings are the limitations/disadvantages of RIP
- Increased processing overheads when compared to static routing
- Not always loop-free
- Not so cost-effective in load balancing
- Pinhole congestion can occur
- Require large bandwidth
- Not suitable for the larger network as this leads to slow convergence
- Due to periodic checks on the routing table of neighbouring routers every 30 seconds, RIP tends to increase network traffic
- It only updates neighbouring routers, hence non-neighbouring routing updates can be forgotten since the information is not accessible immediately
- RIP enforces a maximum hop count limit as this restricts the usability of RIP to local networks only
- The shortest path is also not always guaranteed

Use of RIP

Routing Information Protocol (RIP) is used to transfer data packets from source to destination computer through the network with the help of routers.

The following are the usefulness of Routing Information Protocol (RIP)

- It is a fundamental protocol to connect users on the world wide web
- This helps easy and automatic configuration of routers among each other
- It helps with periodic network updates
- It helps routers on finding an effective path to establish communication between source and destination routers.

Where is RIP Used?

- Small to medium-sized networks with simple routing needs.
- Legacy networks that were built before OSPF/EIGRP became standard.
- Educational labs for training and learning routing basics.
- Backup routing protocol in case the primary protocol fails.

1. What is the difference between RIP and OSPF?

Unlike RIP, which requires routers to send routing table updates every 30 seconds, whereas OSPF (open shortest path first) sends the updated part of the routing table only when a change has to occur.

2. Is RIP a TCP and UDP?

RIP uses UDP (User Datagram Protocol) as the transport protocol.

Unit-5

Transport layer design issues

The primary design issues of the transport layer involve managing end-to-end reliability, flow control, congestion control, and connection management (establishment/termination). It must handle segmentation and reassembly of data, addressing (port mapping), and multiplexing to ensure data from multiple applications is delivered reliably and in order.

The Transport Layer in networking plays a critical role in ensuring reliable end-to-end communication between applications running on different hosts across a network. Its design involves addressing several key issues to achieve efficient and effective data transmission. Here are the design issues in detail:

1. Reliability:

Objective: Ensure that data delivered from the sender to the receiver is accurate and in the correct order, without errors or duplication.

- Techniques:
- Acknowledgment and Retransmission: Use of acknowledgments (ACKs) from the receiver to confirm receipt of data segments. If ACK is not received within a timeout period, the sender retransmits the segment.
- Sequence Numbers: Assign sequence numbers to data segments to ensure they are received in the correct order.
- Checksums: Include error-checking mechanisms (like CRC or checksums) to detect errors and corrupted data segments.

2. Flow Control:

- Objective: Regulate the amount of data sent by the sender to match the receiver's processing capability, preventing overflow and ensuring smooth transmission.
- Techniques:
- Sliding Window Protocol: Allows the sender to transmit multiple segments before receiving acknowledgments, optimizing throughput while adhering to the receiver's buffer capacity.
- Buffer Management: Manage buffer sizes at both sender and receiver ends to handle varying network conditions and traffic loads effectively.

3. Multiplexing and Demultiplexing:

- Objective: Enable multiple applications or services on the same host to communicate simultaneously over the network.
- Techniques:
- Port Numbers: Use port numbers to distinguish different communication streams (e.g., TCP/UDP ports like 80 for HTTP, 443 for HTTPS).
- Socket Pair: Combination of IP address and port number uniquely identifies a communication endpoint (socket) in a network.

4. Connection Management:

- Objective: Establish, maintain, and terminate logical connections between applications running on different hosts.
- Techniques:
- Connection-Oriented Protocols: Like TCP establish a reliable connection through a three-way handshake (SYN, SYN-ACK, ACK) before data exchange and tear down the connection gracefully.
- Connectionless Protocols: Like UDP do not establish a dedicated connection but simply send data packets independently.

5. Error Handling and Retransmission:

- Objective: Detect and recover from errors that occur during data transmission.
- Techniques:
- Selective Repeat and Go-Back-N: Two types of ARQ (Automatic Repeat reQuest) protocols used in sliding window mechanisms to handle lost or corrupted data segments.
- Timeouts: Set timers to wait for acknowledgments (ACKs). If an ACK is not received within the timeout period, the sender assumes the segment is lost and retransmits it.

6. Quality of Service (QoS):

- Objective: Prioritize traffic and allocate network resources based on application requirements (e.g., latency-sensitive applications like VoIP or video streaming).
- Techniques:
- Traffic Prioritization: Assign different priorities to data packets based on QoS parameters (e.g., delay, throughput, jitter).
- Congestion Control: Adjust transmission rates dynamically to avoid network congestion and ensure fair resource allocation among competing flows.

7. Segmentation and Reassembly:

- Objective: Divide large data units received from the upper layers into smaller segments for efficient transmission over the network.
- Techniques:
- Maximum Segment Size (MSS): Largest amount of data that TCP can send in one segment.
- Fragmentation: Splitting of data packets into smaller units to fit within the maximum transmission unit (MTU) size of the underlying network.

8. Security:

- Objective: Ensure data confidentiality, integrity, and availability during transmission.
- Techniques:
- Encryption: Use of cryptographic techniques (e.g., SSL/TLS for TCP) to encrypt data to protect against eavesdropping and unauthorized access.
- Authentication: Verification of identities using digital certificates or passwords to prevent unauthorized access or data tampering.

User Datagram Protocol

UDP is a connectionless, unreliable transport layer protocol that prioritizes speed and low latency over guaranteed delivery. It uses a minimal 8-byte header to send packets ("datagrams") independently without handshakes, making it ideal for real-time applications like video streaming, gaming, and VoIP.

Key Characteristics of UDP:

- Connectionless: No initial handshake is required before sending data, allowing for faster transmission.
- Unreliable: It does not guarantee delivery, packet ordering, or error correction (no retransmission of lost packets).
- Low Overhead: With a small 8-byte header, UDP is more efficient than TCP, resulting in higher speed.
- No Congestion/Flow Control: UDP sends data as fast as possible, which can cause packet loss in congested networks.
- Broadcast/Multicast Support: Suitable for sending data to multiple recipients.

Common Use Cases:

- Real-time Video/Audio Streaming: Occasional packet loss is acceptable, but latency must be low.
- Online Gaming: Requires fast, interactive, and quick data updates.
- VoIP (Voice over IP): Focuses on real-time conversation speed.
- DNS (Domain Name System): Requires quick queries and responses.
- DHCP and SNMP: Used for quick network management and IP configuration.

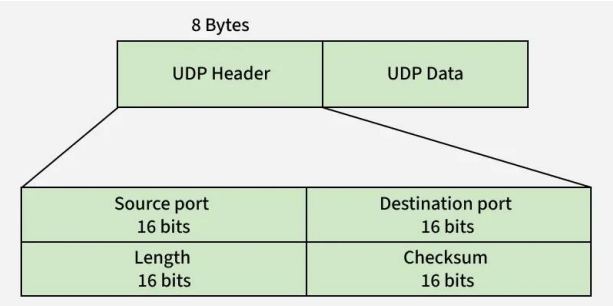
UDP Header Format:

The 8-byte header includes:

- Source Port (16 bits)
- Destination Port (16 bits)
- Length (16 bits)
- Checksum (16 bits - used for error detection)

User Datagram Protocol (UDP) is a Transport Layer protocol of the Internet Protocol (IP) that provides fast, connectionless, and lightweight communication between processes. It does not guarantee delivery, order, or error checking, making it suitable for real-time and time-sensitive applications such as video streaming, DNS, and VoIP. UDP Header

UDP header is 8 bytes long, followed by the data payload. It contains all the essential information needed for transmission. Each port number field is 16 bits, giving a range from 0 to 65535, where port 0 is reserved. Port numbers are used to identify and separate different user requests or processes.



Applications of UDP

UDP is preferred where low latency is crucial and occasional packet loss is acceptable:

- DNS uses UDP for fast query/response lookups since domain name queries are small and need quick replies.
- DHCP uses UDP to dynamically assign IP addresses to devices, where small control messages are exchanged.
- VoIP uses UDP for real-time voice communication, as it tolerates some packet loss but not delays.
- RIP uses UDP to send periodic routing updates between routers efficiently.
- NTP uses UDP to synchronize system clocks across networks with minimal overhead.

How UDP Interacts with IP

UDP operates on top of the Internet Protocol (IP) to enable communication between applications. Here's how data transmission takes place:

- The application provides the data along with destination details to UDP.
- UDP attaches its header, which includes the source port, destination port, length, and checksum.
- The UDP datagram is passed to the IP layer for addressing and routing.
- IP adds its own header and forwards the packet to the destination host.
- At the receiver's end, UDP removes its header and delivers the data to the target application.

Transmission Control Protocol (TCP)

TCP (Transmission Control Protocol) is a protocol that allows devices to communicate reliably over a network. It ensures that data reaches the destination correctly and in the right order, even if parts of the network are slow or unreliable.

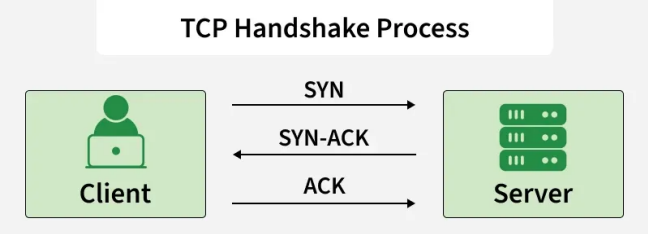
- It works at the Transport Layer (Layer 4) of the OSI model and is an essential part of the TCP/IP protocol suite used for Internet communication.
- TCP establishes a logical connection between the sender and receiver before data transmission begins.
- It ensures that data is delivered accurately and in the same order in which it was sent using acknowledgements and sequence numbers.
- TCP detects errors using checksums and retransmits lost or corrupted packets to maintain data integrity.
- It controls the data transmission rate to avoid overwhelming the receiver and adapts to network congestion for efficient communication.

Connection Establishment and Termination

Connection establishment and termination describe how two devices start and end a reliable communication session (mainly in TCP).

1. Connection Establishment (Three-Way Handshake)

TCP is connection-orientated, meaning a connection must be established before any data is sent. This is done using a three-way handshake:



- SYN (Synchronize): The sender sends a SYN segment to the receiver to request a connection.
- SYN-ACK (Synchronize-Acknowledge): The receiver responds with a SYN-ACK segment, acknowledging the request and agreeing to the connection.
- ACK (Acknowledge): The sender replies with an ACK, confirming the connection is established.
- This process ensures both sender and receiver are ready and synchronized, preventing lost or misordered data at the start.

2. Connection Termination (Four-Way Handshake)

Closing a TCP connection requires a four-step handshake to ensure both sides finish transmitting data safely:

- FIN (Finish): The sender who wants to close the connection sends a FIN segment to the receiver.
- ACK (Acknowledge): The receiver acknowledges the FIN with an ACK.
- FIN (Finish) from Receiver: The receiver then sends its own FIN when it is ready to close the connection.
- ACK (Acknowledge): The sender responds with an ACK, completing the termination.
- This ensures that all remaining data is transmitted before the connection is fully closed.

Working

1. Segmenting

When an application sends data (like an email or file), TCP breaks the data into smaller chunks called segments.

Each segment has a header containing information like sequence numbers, ports, and flags.

This makes it easier to send large amounts of data over the network reliably.

2. Routing via IP

Once TCP creates segments, they are handed to IP (Internet Protocol).

IP is responsible for delivering the segments from the sender to the receiver, possibly through multiple routers.

TCP doesn't care about the path—IP handles routing and addressing.

3. Reassembly at Receiver

Segments may arrive out of order because they can take different paths through the network.

TCP at the receiver uses sequence numbers to reassemble the segments into the correct order to reconstruct the original message.

4. Acknowledgments (ACKs)

The receiver sends an ACK for every segment (or group of segments) it receives correctly.

This tells the sender that the data has arrived safely.

If an ACK is not received, TCP assumes the segment was lost and triggers retransmission.

5. Retransmission

If the sender does not receive an acknowledgment within a certain time, it resends the missing segment.

This ensures no data is lost, making TCP reliable.

6. Flow & Error Control

Flow Control: TCP prevents the sender from sending too much data too quickly for the receiver to handle, using a sliding window mechanism.

Error Control: TCP checks for corrupted segments using checksums and requests retransmission if needed.

Together, these mechanisms ensure data is delivered reliably and efficiently, without overloading the network or the receiver.

Applications

1. Web Browsing (HTTP/HTTPS)

Websites send and receive data in small chunks called packets.

TCP ensures these packets arrive in order and completely, so pages load correctly without missing images or broken content.

HTTPS adds encryption, but TCP still handles reliability under the hood.

2. Email (SMTP, IMAP, POP3)

Sending and receiving emails requires all message data to arrive intact.

TCP ensures no part of the email is lost or corrupted, so attachments and text are received correctly.

3. File Transfer (FTP, SFTP)

Transferring files over a network involves large amounts of data.

TCP divides files into segments, reorders them at the destination, and retransmits lost segments, ensuring the file is received exactly as sent.

4. Remote Terminal Access (SSH, Telnet)

When you connect to a remote computer, you send commands and receive responses in real time.

TCP ensures that every keystroke or command is reliably transmitted and arrives in order, maintaining a stable connection for remote management.

Advantages

Error-Free Data Transfer: TCP detects errors during transmission and retransmits lost or corrupted data, ensuring accurate delivery.

Ordered Delivery: Data packets are received in the same sequence in which they were sent, maintaining data consistency.

Flow Control: Prevents the sender from overwhelming the receiver by controlling the rate of data transmission.

Congestion Control: Adjusts the sending speed based on network traffic conditions to reduce packet loss and congestion.

Reliable Communication: Ensures complete and dependable data transfer, making it suitable for critical applications.

Widely Supported and Standardized: TCP is a globally accepted protocol, supported by all major operating systems and network devices.

UNIT-6

Application layer design focuses on enabling user applications to interact with network services, primarily involving protocol selection, architectural style, and service optimization. Key issues include choosing between client-server or P2P, ensuring scalability, managing security, defining data formats, and handling application-specific synchronization to meet user requirements.

Key Application Layer Design Issues:

- Architecture Selection: Choosing between client-server (centralized, higher load) or peer-to-peer (P2P) systems, which impacts scalability and robustness.
- Protocol Design/Selection: Defining the syntax, semantics, and synchronization for application interactions (e.g., HTTP, FTP, SMTP, DNS).
- Performance and Scalability: Designing protocols to handle increasing loads without causing severe congestion, such as using efficient client-server, or, in some cases, decentralized P2P to avoid server saturation.
- Data Serialization and Security: Ensuring the structured format (syntax) of data is consistent across different platforms and implementing security protocols (e.g., encryption) for data integrity.
- Session Management & Synchronization: Managing dialog control (half-duplex/full-duplex) and adding checkpoints to data transfers to allow resumption of interrupted services.
- User-Network Interaction: Designing how user applications (browsers, email clients) communicate their needs to the underlying transport layer effectively.

Domain Name System (DNS)

DNS is a system that translates human-readable domain names into IP addresses so computers can communicate over the internet. It works in a hierarchical and distributed manner to efficiently resolve queries. DNS ensures users can access websites without remembering numeric IP addresses. It also improves performance using caching.

- Provides name-to-address resolution
- Uses a hierarchy (Root, TLD, Authoritative servers)
- Improves speed using caching mechanisms

Example: When you enter google.com in a browser, DNS converts it into an IP address (like 142.x.x.x), allowing your system to connect to the correct server.

Working

The DNS process can be broken down into several steps, ensuring that users can access websites by simply typing a domain name into their browser.

- User Input: The user enters a domain name (e.g., www.geeksforgeeks.org) in the browser.
- Local Cache Check: The browser or OS checks its cache for a stored IP address.
- DNS Resolver Query: If not found, the request is sent to a DNS resolver (usually by ISP).

- Root Server Query: The resolver queries a root server, which points to the correct TLD server.
- TLD Server Response: The TLD server directs the resolver to the domain's authoritative server.
- Authoritative Server Response: The authoritative server returns the actual IP address.
- Final Response: The resolver sends the IP back to the user, and the browser connects to the server.

Structure of DNS

The structure of DNS is hierarchical in nature, enabling scalable and organized domain name resolution across the global Internet.

1. Root:

The topmost level of the DNS hierarchy.

- Represented by a dot (.) at the end of a domain name
- Acts as the starting point of domain resolution

2. Top-Level Domains (TLDs):

The level directly below the root that defines domain extensions.

- Includes extensions like .com, .org, .net, .edu
- Helps categorize domains by purpose or region

3. Second-Level Domains:

The main domain name registered by an organization.

- Appears before the TLD (e.g., "example" in example.com)
- Uniquely identifies a domain under a TLD

4. Subdomains:

Extensions of the main domain used for organization.

- Examples: www, mail, blog
- Helps structure different parts of a website

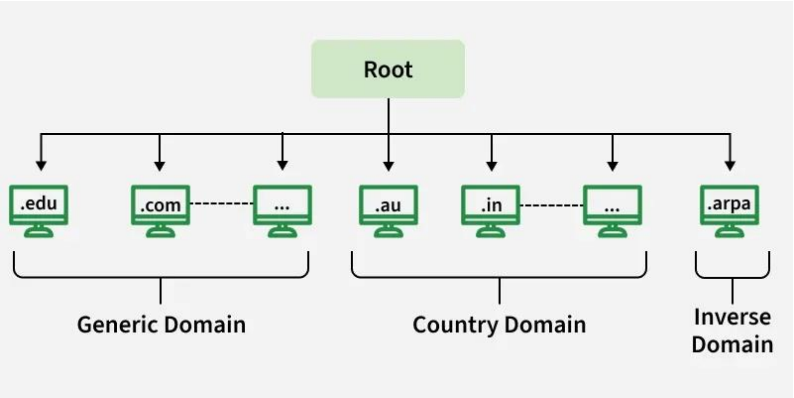
5. Hostnames:

Identifies specific servers or devices within a domain.

- Examples: web1, mailserver, ftp
- Maps to actual IP addresses using DNS records

Types of Domains

DNS categorizes domain names into different types to organize the global naming system and support both forward and reverse resolution



Types of Domains

1. Generic Domains (gTLDs):

These domains are used for general purposes and are not tied to any country.

- Include extensions like .com, .org, .net, .edu
- Not restricted to any specific country
- Used for commercial, organizational, and educational purposes

2. Country Code Domains (ccTLDs):

These domains represent specific countries or geographic regions.

- Examples: .in (India), .us (USA), .uk (UK), .jp (Japan)
- Managed by respective national authorities

3. Inverse Domains (Reverse DNS):

These domains are used to map IP addresses back to domain names.

- Used for reverse lookup (IP address → domain name)
- IPv4 uses in-addr.arpa
- IPv6 uses ip6.arpa
- Uses PTR (Pointer) records

Dynamic Host Configuration Protocol (DHCP)

DHCP is a network protocol that automatically gives devices an IP address and other network settings so they can connect and communicate on a network without manual configuration.

Assigns a unique IP address to each device.

Provides the subnet mask to define the local network range.

Configures the default gateway for communication outside the local network.

Supplies DNS server addresses for domain name resolution**.**

Components of DHCP

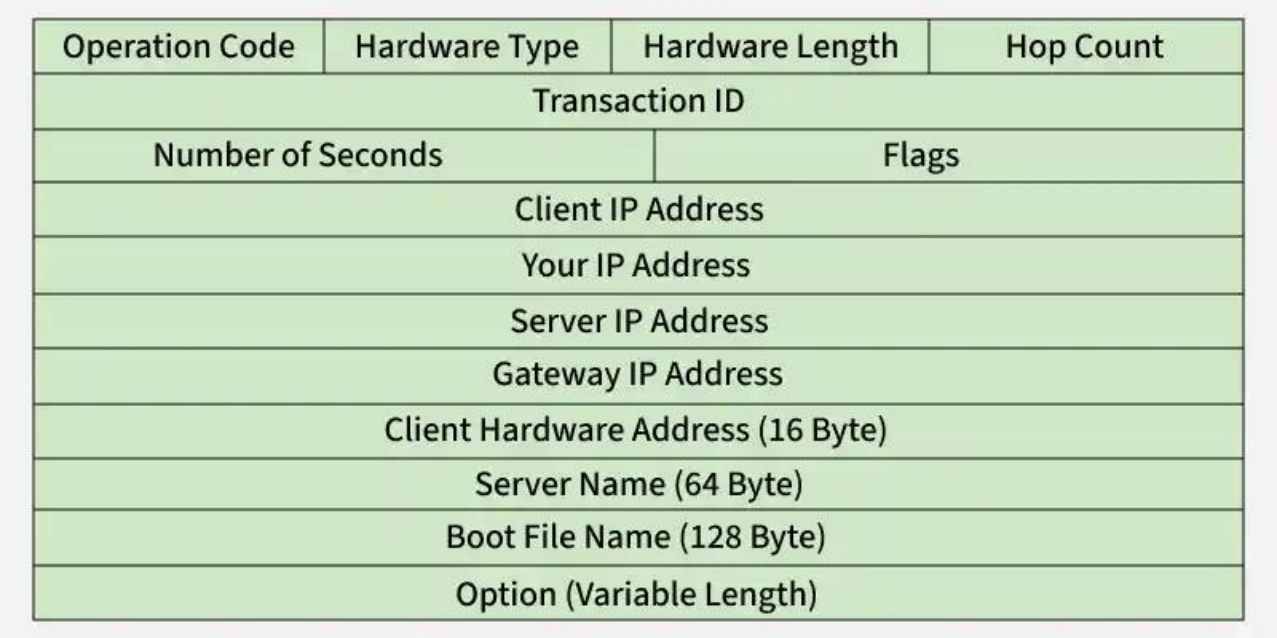
- DHCP works using a client–server model where the client requests network settings, the server allocates them from an address pool, and the settings are delivered as options for a fixed lease time. DHCP Server: The device (router/server) that manages the DHCP service, keeps the IP pool, and assigns IP addresses + configuration to clients.
- DHCP Relay: A router/switch feature that forwards DHCP requests and replies between clients and the server when they are in different networks (different subnets).
- DHCP Client: Any device (PC, mobile, printer, IoT) that requests an IP address and settings from the DHCP server.
- IP Address Pool: The range of IP addresses available for allocation to clients (often with exclusions/reservations).
- Lease: The time period for which an assigned IP address is valid; the client must renew the lease to keep using it.

- Default Gateway: The router IP given to the client so it can communicate outside the local network (reach the internet/other networks).
- DNS Servers: DNS addresses provided to the client so it can convert domain names (like google.com) into IP addresses.

DHCP Advanced Features

- Renewal: Client renews the lease early to keep the same IP and stay connected.
- Failover: Two DHCP servers share leasing; if one fails, the other continues service.
- Dynamic Updates: DHCP auto-updates DNS (A/PTR) when a client IP is assigned or changes.
- Audit Logging: Logs lease events (assign/renew/release) for tracking, troubleshooting, and audits.

DHCP Packet Format



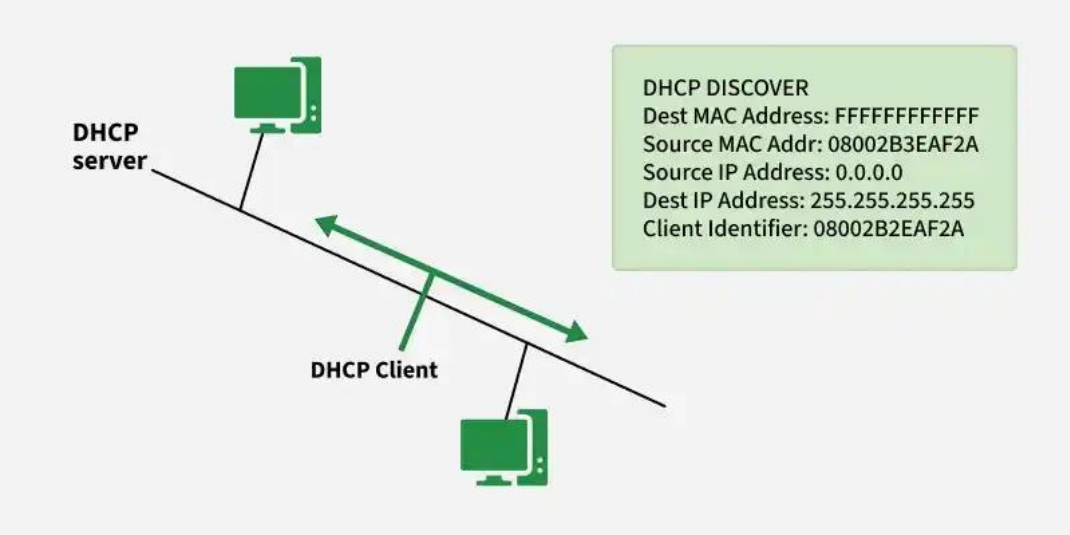
- Hardware Length (8 bits): Length of MAC address (e.g., 6 for Ethernet).
- Hop Count (8 bits): Maximum number of hops the packet can travel.
- Transaction ID (32 bits): Set by client, used to match requests and replies.
- Number of Seconds (16 bits): Time elapsed since the client started booting.
- Flags (16 bits): Leftmost bit indicates broadcast reply requirement.
- Client IP Address (4 bytes): Filled if the client already has an IP, else 0.
- Your IP Address (4 bytes): Client IP assigned by the server.
- Server IP Address (4 bytes): IP address of the responding DHCP server.
- Gateway IP Address (4 bytes): Router IP address (if applicable).
- Client Hardware Address: The device's MAC address.
- Server Name (64 bytes): Optional server hostname.
- Boot Filename (128 bytes): Pathname of boot file (for diskless clients).
- Options (variable): Vendor-specific or additional configuration.

Working of DHCP

DHCP operates at the Application Layer and uses UDP ports 67 (server) and 68 (client) to automatically assign network configuration through a client-server communication process called DORA (Discover, Offer, Request, Acknowledge).

1. DHCP Discover Message:

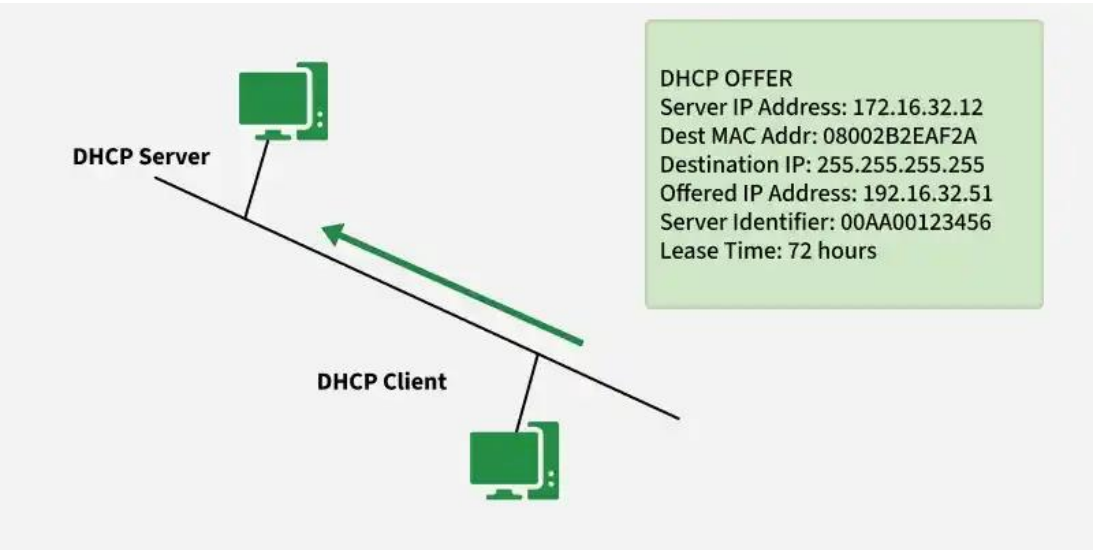
DHCP Discover is the first message sent by a DHCP client to check whether any DHCP server is available on the network and to start getting an IP address.



- Triggered when: A device connects to a network or boots up with no valid IP configuration.
- Transmission type: Broadcast, because the client does not know the DHCP server's address.
- Purpose: Identify DHCP server(s) capable of assigning an IP and network parameters.

2. DHCP Offer Message

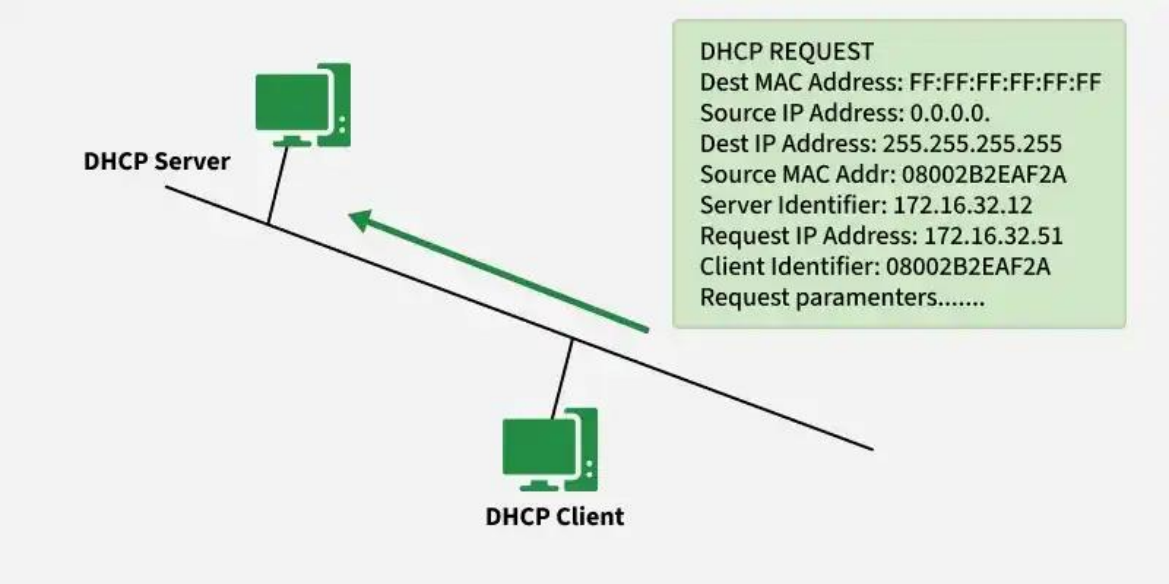
A DHCP server replies with an offer that includes an available IP address and configuration options (like subnet mask, gateway, DNS, and lease time).



- Can be broadcast or unicast (depends on client/network behavior)
- Includes Server Identifier so the client knows which server sent the offer
- The offered IP is carried in yiaddr ("your IP address" field)

3. DHCP Request Message

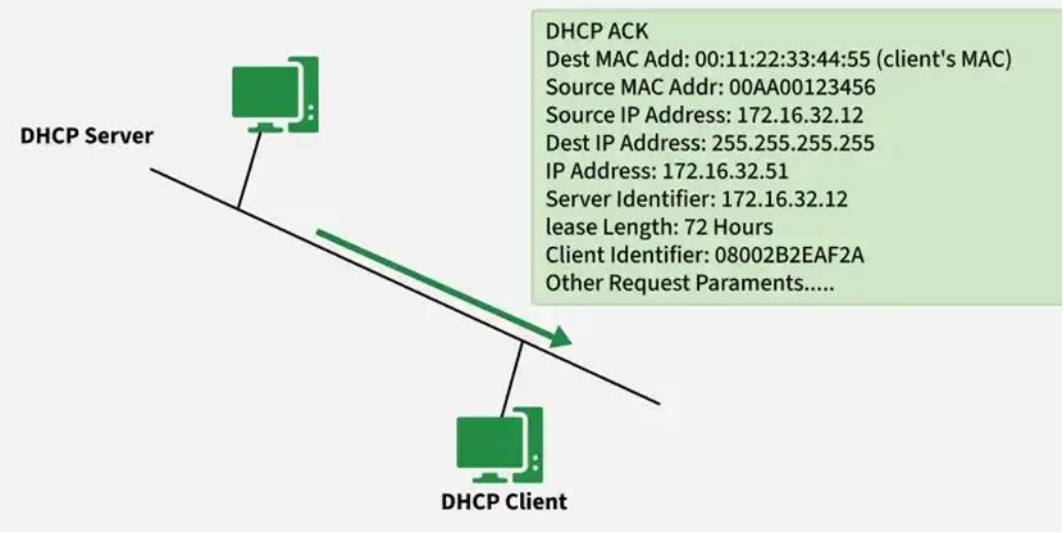
DHCP Request is the message where the client confirms one chosen offer and asks the selected DHCP server to allocate that IP officially. It also tells other DHCP servers not to keep their offered IP reserved.



- Sent by: DHCP client
- When it is sent: After the client receives one or more DHCP Offer messages
- It accept one offered IP address and identify the selected server
- Prevent multiple servers from assigning different IPs to the same client

4. DHCP Acknowledgment Message

DHCP ACK is the final confirmation sent by the selected DHCP server after it receives the client's DHCP Request. This message officially assigns the IP address to the client and provides the full set of network configuration parameters.



- **Sent by**: DHCP server
- **When it is sent**: After the server accepts the client's DHCP Request
- **Purpose:** Confirm the lease and deliver final configuration so the client can start network communication.

5. DHCP Negative Acknowledgment Message

- DHCP NAK is sent by the server to notify the client that the requested IP configuration is invalid and cannot be assigned.
- Sent by: DHCP server
- Purpose: Reject the client's DHCP Request
- Requested IP is outside the configured scope
- IP is already allocated to another device
- Client has moved to a different network
- Client must restart the DHCP process from Discover

6. DHCP Decline

- DHCP Decline is sent by the client when it detects that the offered IP address is already in use on the network.
- Sent by: DHCP client
- Purpose: Inform the server that the offered IP is not safe to use
- Typical trigger: Client detects an IP conflict using an ARP probe / gratuitous ARP
- Result: Server marks the IP as unavailable and selects another address for future allocation.

7. DHCP Release

- DHCP Release allows a client to return its assigned IP address to the server before the lease expires.

- Sent by: DHCP client
- Purpose: Free the IP for reuse
- Occurs when a device disconnects, shuts down, or disables the interface
- Helps maintain efficient IP address utilization

8. DHCP Inform

- DHCP Inform is used when a client already has a manually configured (static) IP but needs additional network settings from the DHCP server.
- Sent by: DHCP client
- Purpose: Request configuration parameters like DNS, domain name, NTP, etc., without obtaining a new IP.
- Server response: Sends a DHCP ACK containing only configuration options.
- Delivery: Typically unicast, since the client already has a valid IP.

Security Concerns with DHCP

DHCP has no built-in authentication, so attackers on the same LAN can misuse it to disrupt service or redirect traffic.

- DHCP Starvation (IP Pool Exhaustion): Floods DHCP requests with spoofed MACs to consume all available leases, blocking legitimate clients.
- Rogue DHCP Server: A fake server gives clients incorrect IP settings (gateway/DNS), taking control of their network path.
- Man-in-the-Middle: Done by pushing attacker-controlled gateway/DNS via rogue DHCP to intercept or alter traffic.
- DNS Misuse: Malicious DHCP options can point clients to unauthorized DNS servers for redirection/phishing.

Protection Against DHCP Attacks

- Enable DHCP Snooping on switches and allow DHCP replies only on trusted ports.
- Apply Port Security or rate-limiting to reduce spoofed requests and prevent starvation.
- Use IP/MAC filtering + monitoring/log analysis to detect and block abnormal lease activity

Simple Network Management Protocol (SNMP)

SNMP stands for Simple Network Management Protocol. It is an Internet-standard protocol for managing and monitoring devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, and network appliances. SNMP is primarily used in network management frameworks to monitor network-attached devices for conditions that require administrative attention.

Simple Network Management Protocol (SNMP) is an Internet Standard protocol used for managing and monitoring network-connected devices in IP networks. SNMP is an application layer protocol that uses UDP port number 161/162. SNMP is used to monitor the network, detect network faults, and sometimes even to configure remote devices **Architecture of SNMP**

There are mainly three main components in SNMP architecture:.

- SNMP Manager: It is a centralized system used to monitor the network. It is also known as a Network Management Station (NMS). A router that runs the SNMP server program is called an agent, while a host that runs the SNMP client program is called a manager.
- SNMP agent: It is a software management software module installed on a managed device. The manager accesses the values stored in the database, whereas the agent maintains the information in the database. To ascertain if the router is congested or not, for instance, a manager can examine the relevant variables that a router stores, such as the quantity of packets received and transmitted.
- Management Information Base:MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables. A MIB, or collection of all the objects under management by the manager, is unique to each agent. System, interface, address translation, IP, UDP , and EGP , ICMP , TCP are the eight categories that make up MIB. The MIB object is home to these groups.

SNMP Messages

- **GetRequest :** It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.
- **GetNextRequest :** To get the value of a variable, the manager sends the agent the GetNextRequest message. The values of the entries in a table are retrieved using this kind of communication. The manager won't be able to access the values if it doesn't know the entries' indices. The GetNextRequest message is used to define an object in certain circumstances.
- **SetRequest :** It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
- **Response :** When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.
- **Trap :** These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.
- **InformRequest :** It was added to SNMPv2c and is used to determine if the manager has received the trap message or not. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

Characteristics of SNMP

- SNMP is used to monitor network.
- It detects any network faults.
- It can also be used to configure remote devices.
- It allows a standardized way of collecting information about all kinds of devices from various manufacturers among the networking industry.

Advantages of SNMP

- It is easy to implement.
- Agents are widely implemented.
- Agent level overhead is minimal.
- It is robust and extensible.
- Polling approach is good forLAN based managed object.
- It offers the best direct manager agent interface.

Limitation of SNMP

- It does not scale well.
- There is no object orietned data view.
- It has no standard control definition.
- It has many implementation specific (private MIB) extensions.
- It has high communication overhead due to polling

Versions of SNMP

- SNMPv1:
- SNMPv2c:
- SNMPv3:

FTP (File Transfer Protocol) and TFTP (Trivial File Transfer Protocol)

FTP (File Transfer Protocol) and TFTP (Trivial File Transfer Protocol) are Application Layer protocols for file transfer. FTP is a complex, reliable, TCP-based protocol (ports 20/21) requiring user authentication, ideal for general file transfers. TFTP is a simple, UDP-based protocol (port 69) without authentication, used for booting, firmware updates, and local, small file transfers.

Key Differences:

- Transport Protocol: FTP uses TCP, providing reliable, connection-oriented transfer. TFTP uses UDP, providing unreliable, connectionless transfer.
- Authentication & Security: FTP supports username/password authentication. TFTP has no security or authentication, suitable only for trusted local networks.
- Connections: FTP uses two connections (port 21 for control, 20 for data). TFTP uses a single connection (port 69).
- Functionality: FTP allows directory listing, deleting, and renaming files. TFTP only supports reading and writing files.
- Use Cases: FTP is used for uploading website files, downloading data, and user-centric file transfers. TFTP is used for diskless workstation booting, network router configuration uploads, and firmware updates.

FTP Summary:

- Protocol: TCP (reliable).
- Ports: 21 (control), 20 (data).
- Authentication: Yes.
- Best for: General file transfer, remote server management.

TFTP Summary:

- Protocol: UDP (unreliable, faster).
- Port: 69.
- Authentication: No.
- Best for: Local area network file transfers, embedded system updates.

Difference Between FTP and TFTP

Feature	FTP	TFTP
Purpose	Transfer files between computers	Transfer files between computers
Connection	Establishes a connection between two computers, allowing for a more complex set of commands and options	Establishes a connection between two computers, but with a more limited set of commands and options
Authentication	Uses username and password for authentication	Does not support authentication

Feature	FTP	TFTP
Security	Encrypts data transfer	Does not encrypt data transfer
Error handling	Can recover from errors during transfer	Does not have error recovery
File transfer mode	Supports both ASCII and binary transfer modes	Only supports binary transfer mode
Transfer options	Supports resuming interrupted transfers and setting transfer mode, transfer type, and other options	Does not support any transfer options

Simple Mail Transfer Protocol (SMTP)

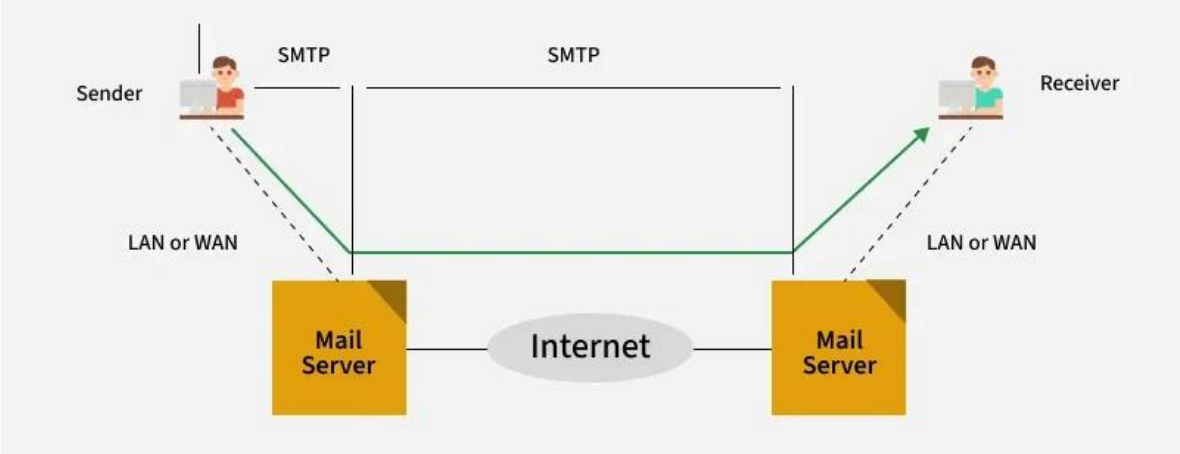
SMTP is an application-layer protocol used to send and transfer email between servers. It relies on a TCP connection to port 25 to reliably deliver messages from a client to an email server.

- Uses TCP for reliable message transmission
- Servers listen on port 25 for incoming email
- Client establishes a TCP connection before sending mail
- Core protocol for email delivery between mail servers

Types of SMTP Protocol

The SMTP model supports two types of email delivery methods: end-to-end and store-and-forward.

- End-to-end delivery is used between organizations. In this method, the email is sent directly from the sender's SMTP client to the recipient's SMTP server without passing through intermediate servers.
- Store-and-forward is used within organizations that have TCP/IP and SMTP-based networks. In this method, the email may pass through several intermediate servers (Message Transfer Agents, or MTAs) before reaching the recipient.



(SMTP)

- SMTP.com: Platform providing transaction email, relay, and delivery services at affordable prices.
- Industry Trust: Regarded as the most trusted sender by ISPs with decades of experience.
- Customer Base: Trusted by over 100,000 customers over the years.
- User-Friendly: Extremely intuitive and easy to set up for seamless integration.
- Business Integration: Seamlessly integrates into existing business systems.
- Easy Migration: Effortless migration from other email providers.

Features

The following are the key features of SMTP.com:

- Dedicated IP: Provides a unique sending IP to improve deliverability and maintain a strong sender reputation.
- Email API: Enables fast and seamless integration with detailed documentation, allowing businesses to connect in just minutes.
- 24/7 Customer Support: Offers round-the-clock human support across all plans, including website assistance and live chat for quick, reliable solutions.
- High-Volume Sending Solutions: Ideal for enterprises sending over 250 million emails monthly, with customized quotes and tailored infrastructure.
- Reputation Defender: An add-on service that automatically scans, cleans, and monitors email lists to maintain healthy sender reputation—no integration required.

Model of SMTP System

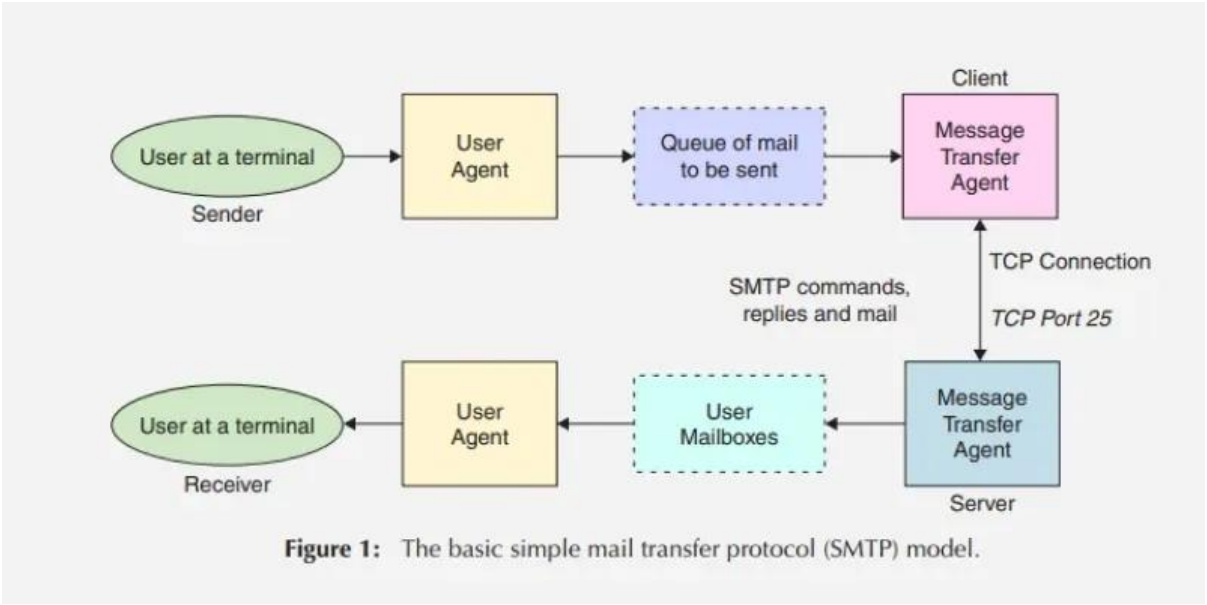
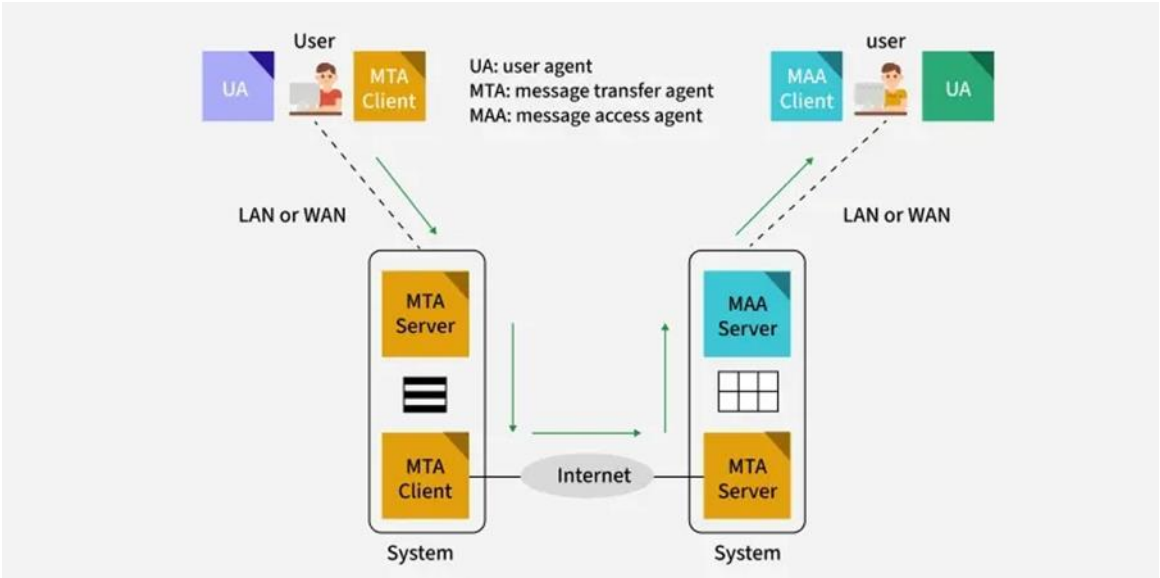


Figure 1: The basic simple mail transfer protocol (SMTP) model.

Components of SMTP

- Mail User Agent (MUA): It is a computer application that helps you in sending and retrieving mail. It is responsible for creating email messages for transfer to the mail transfer agent(MTA).
- Mail Submission Agent (MSA): It is a computer program that receives mail from a Mail User Agent(MUA) and interacts with the Mail Transfer Agent(MTA) for the transfer of the mail.
- Mail Transfer Agent (MTA): It is software that has the work to transfer mail from one system to another with the help of SMTP.
- Mail Delivery Agent (MDA): A mail Delivery agent or Local Delivery Agent is basically a system that helps in the delivery of mail to the local system.

How does SMTP Work?



1. Sending Email:
   - When a user wants to send an email, they use a User Agent (UA), like Outlook or Gmail.
   - The email is handed over to the MTA, which is responsible for transferring the email to the recipient's mail server.

2. SMTP Client and Server:
   - Sender-SMTP (Client): The email sender's MTA initiates the connection to the recipient's MTA (Receiver-SMTP).
   - Receiver-SMTP (Server): The receiving MTA listens for incoming connections and receives the email from the sender-SMTP.
   - This communication happens over TCP port 25.

3. Relays and Gateways:
   - Relays: In some cases, the email may pass through several intermediate MTAs before reaching the destination server. These MTAs act as relays.
   - Gateways: If the sending and receiving systems use different email protocols (e.g., SMTP and non-SMTP), an email gateway can convert the email to the appropriate format for delivery.

4. Email Delivery:
   - The sender's MTA sends the email to the receiver's MTA, either directly or through relays.
   - The MTA uses the SMTP protocol to transfer the message. Once it's delivered to the destination MTA, the email is placed in the recipient's mailbox.
   - The recipient's User Agent (UA) can then download the email.

SMTP Envelope

Purpose:
   - The SMTP envelope contains information that guides email delivery between servers.
   - It is distinct from the email headers and body and is not visible to the email recipient.

Contents of the SMTP Envelope
   - Sender Address: Specifies where the email originates.
   - Recipient Addresses: Indicates where the email should be delivered.
   - Routing Information: Helps servers determine the path for email delivery.

Comparison to Regular Mail
   - Think of the SMTP envelope as the address on a physical envelope for regular mail.
   - Just like an envelope guides postal delivery, the SMTP envelope directs email servers on where to send the email.

Advantages of SMTP
   - If necessary, the users can have a dedicated server.
   - It allows for bulk mailing.
   - Low cost and wide coverage area.
   - Offer choices for email tracking.
   - Reliable and prompt email delivery.

Disadvantages of SMTP
   - SMTP's common port can be blocked by several firewalls.
   - SMTP security is a bigger problem.

- Its simplicity restricts how useful it can be.
- Just 7-bit ASCII characters can be used.
- If a message is longer than a certain length, SMTP servers may reject the entire message.
- Delivering your message will typically involve additional back-and-forth processing between servers, which will delay sending and raise the likelihood that it won't be sent.

World Wide Web (WWW)

The World Wide Web (WWW) operates at the Application Layer (Layer 7 of the OSI model) as a client-server system, using HTTP/HTTPS protocols to request and transmit hyperlinked documents (HTML) between web browsers and servers. It acts as the user interface for network services, allowing users to access internet-based content.

Key Aspects of WWW in the Application Layer:

- Protocols (HTTP/HTTPS): The application layer uses HyperText Transfer Protocol (HTTP) and its secure version (HTTPS) to enable web browsers to send requests to web servers and receive HTML, CSS, images, and other resources in return.
- Client-Server Model: The web browser (e.g., Chrome, Firefox) serves as the client application that initiates communication by requesting specific content, while the web server stores and serves this content.
- User Interface (UI): The application layer enables end-user software to interact with the network. Browsers format HTML, images, and other data into a human-readable web page.
- Functionality: It manages user-entered URLs, handles requests for website data, and ensures the data received is properly interpreted and displayed.
- Underlying Components: While the user interacts with the web via browser, the application layer also utilizes protocols like DNS (Domain Name System) to translate human-readable names (e.g., google.com) into IP addresses for networking.

The WWW is just one of many applications (like email or FTP) that utilize the application layer to interact with the underlying transport and network layers.

Telnet and SSH (Secure Shell)

Both Telnet and SSH (Secure Shell) are [application layer protocols that enable remote access to network devices and systems. The primary distinction lies in their security: Telnet is unencrypted and transmits data in plain text, while SSH uses encryption for a secure connection.

Telnet (Telecommunications Network)

Telnet is an older, simple protocol that provides a virtual terminal connection to a remote system.

- Security: It is highly insecure because all information, including usernames, passwords, and commands, is sent as plain text, making it vulnerable to interception and eavesdropping via packet sniffing.
- Port: Operates on TCP port 23 by default.

- Usage: Primarily used in controlled, private, and trusted local area networks or for basic network diagnostics and interacting with legacy equipment where security is not a concern. It is now largely obsolete in modern environments.

SSH (Secure Shell)

- SSH was developed as a secure replacement for Telnet and other unsecure protocols like rsh. It provides a secure, encrypted channel over an insecure network.
- Security: All data transmitted over an SSH session is encrypted using cryptography (symmetric, asymmetric, and hashing), ensuring confidentiality and integrity. This protects sensitive data from being intercepted or read.
- Authentication: It uses strong authentication methods, including password-based authentication and more secure public-key cryptography.
- Port: Operates on TCP port 22 by default.
- Usage: It is the industry standard for secure remote administration of servers and network devices (routers, switches, etc.) over both private and public networks like the internet. It also supports secure file transfers through protocols like SFTP and SCP.

Summary of Differences

Feature	Telnet	SSH (Secure Shell)
Security	Transmits data in plain text (unencrypted)	Encrypts all data transmitted
Authentication	Basic, less secure authentication	Strong authentication with password or public key
Default Port	TCP Port 23	TCP Port 22
Network Type	Suitable only for secure private networks	Suitable for both private and public networks
Vulnerabilities	Susceptible to sniffing, IP spoofing, man-in-the-middle attacks	Designed to prevent sniffing and other attacks

For virtually all current networking applications, **SSH is the recommended protocol** due to its robust security features

UNIT-7

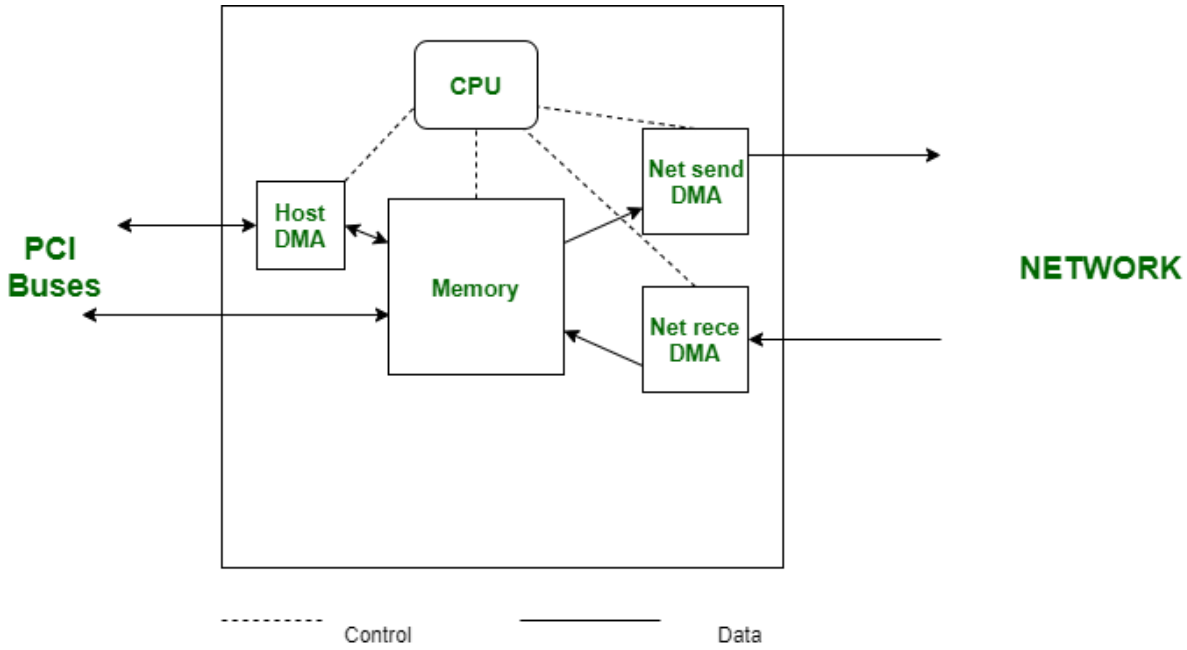
Network Interface Card (NIC):

A Network Interface Card (NIC) is a hardware component that enables a computer or any device to connect to a network. It acts as an interface between the device and the network, allowing communication by sending and receiving data. Every device that needs network connectivity must have a NIC, which may be built into the system or installed as a separate card. The NIC uses a MAC address to identify the device on a network.

- NIC stands for Network Interface Card.
- It is also known as a network card, network adapter, or Ethernet card (for wired networks).
- NIC is a major and essential component required to connect a device to a network.
- Network devices such as switches also contain NICs to connect to networks.
- A NIC can be a circuit board or an expansion card installed in a computer or PC.
- NIC operates at:

Physical Layer (Layer 1) – signal transmission
Data Link Layer (Layer 2) – framing and MAC addressing

- Each NIC has a unique MAC address used for identification.
- In wired networks, a NIC converts data into electrical signals and vice versa (Ethernet).
- In wireless networks, a NIC converts data into radio signals and vice versa (Wi-Fi).
- NIC requires drivers to communicate with the operating system



Characteristics of NIC

The main characteristics of a NIC describe how it identifies devices, connects to the network, and indicates network status.

1. Physical Network Address (MAC Address): Every NIC has a unique MAC address permanently assigned by the manufacturer. It is a 48-bit (6-byte) address used to uniquely identify a device on a network. The first half represents the vendor ID, and the second half uniquely identifies the device.
2. Network Connection Port: A NIC provides a network port to connect a device to the network medium, such as Ethernet or fiber. The port type must match the network cable being used.
3. Status Indicator Lights: NICs include LED indicators to show network status.
Link light confirms physical connection.
Activity light blinks during data transmission or reception.

Types of Network Interface Cards

There are two main types of NICs based on the type of network connection:

1. Wired NIC (Ethernet NIC): A wired NIC uses physical cables (such as Ethernet) to connect a device to a network. Wired NICs provide high-speed data transfer (up to 1 Gbps or more) and offer better security and stability compared to wireless connections. They are widely used in LAN, MAN and WAN networks, and are preferred for applications like gaming and video conferencing.

Examples: TP-Link TG-3468 Gigabit PCI Express Network Adapter, Integrated Ethernet NICs

2. Wireless NIC: A wireless NIC connects devices to a network using radio signals, commonly through Wi-Fi. These NICs provide mobility and portability and are often built into laptops, smartphones, and tablets. Wireless NICs can also be added externally using USB or internal adapter cards and support modern standards such as Wi-Fi 6.

Examples: Intel 3160 Dual-Band Wireless Adapter, Internal Wi-Fi Cards, USB Wi-Fi Adapters, Wi-Fi 6 Adapters

Wired Network Interface Card (NIC)	Wireless Network Interface Card (NIC)
A wired NIC connects a system to a network through physical Ethernet cables.	A wireless NIC connects a system to a network using radio-frequency signals (Wi-Fi).
It provides a highly stable and reliable network connection.	It offers comparatively lower stability due to signal interference.
Wired NICs support higher data transfer speeds.	Wireless NICs generally provide lower data transfer speeds.
Data transmission is more secure because access requires a physical connection.	Wireless transmission is more susceptible to security risks and relies on encryption for protection.

Wired Network Interface Card (NIC)	Wireless Network Interface Card (NIC)
It is commonly used in desktops, servers, and enterprise networks.	It is widely used in laptops, mobile devices, and portable systems.
Installation requires network cabling and dedicated ports.	Installation is simpler as no physical cabling is required.
Performance remains consistent regardless of distance within cable limits.	Performance decreases with increased distance and physical obstructions.
Wired NICs typically exhibit low latency.	Wireless NICs usually experience higher latency.
Example: TP-Link TG-3468 Gigabit PCI Express Network Adapter.	Example: Intel 3160 Dual-Band Wireless Adapter.

A Network Interface Card (NIC) provides high-speed network communication, often supporting data transfer rates in gigabits per second. It offers a reliable and stable connection, especially in wired networks. A NIC allows multiple peripheral devices to connect to a network through different ports and enables efficient sharing of large amounts of data among multiple users, making it suitable for organizational and enterprise networks.

Wired NICs lack portability and flexibility because they require physical cables, unlike wireless networking solutions. Proper network configuration is necessary to achieve optimal performance, which can increase setup complexity. Additionally, if appropriate security measures are not implemented, data transmission over a network may be vulnerable to unauthorized access.

Hub:

A hub is a multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. Hub does not have any routing table to store the data of ports and map destination addresses., the routing table is used to send/broadcast information across all the ports.

How Does a Network Hub Work?

A hub is a multiport device, which has multiple ports in a device and shares the data to multiple ports altogether. A hub acts as a dumb switch that does not know, which data needs to be forwarded where so it broadcasts or sends the data to each port.

Types of Network Hubs

Networks hubs are classified into three types:

1. Active Hub: They have a power supply for regenerating, and amplifying the signals. When a port sends weak signalled data, the hub regenerates the signal and strengthens it, then send it further to all other ports. Active hubs are expensive in costs as compared to passive hubs.
2. Passive Hub: Passive hubs are simply used to connect signals from different network cables as they do not have any computerised element. They simply connect the wires of different devices in the star topology. Passive hubs do not do any processing or signal regeneration and that's why do not require electricity the most they can do is they can copy or repeat the signal. It can't clean the message, and it can't amplify or strengthen the signal.
3. Intelligent Hub: Intelligent hubs are smarter than active and passive hubs. The intelligent hub comprises a special monitoring unit named a Management Information Base (MIB). This is software that helps in analysing and troubleshooting network problems. Intelligent hubs work similarly to active hubs but with some management features.

Features of Hubs

Hubs are the hardware device that operates in the physical layer of the OSI model.

- It supports half-duplex transmission
- It works with shared bandwidth and broadcasting.
- The hub can provide a high data transmission rate to different devices.
- It can detect collisions in the network and send the jamming signal to each port.
- Hub does not support Virtual LAN(VLAN) and spanning tree protocol.
- It is unable to filter the data and hence transmit or broadcast it to each port.
- It cannot find the best route/ shortest path to send any data, which makes it an inefficient device.

Advantages of Network Hubs

- It is less expensive.
- It does not impact network performance.
- Hub support different network media.

Disadvantages of Network Hubs

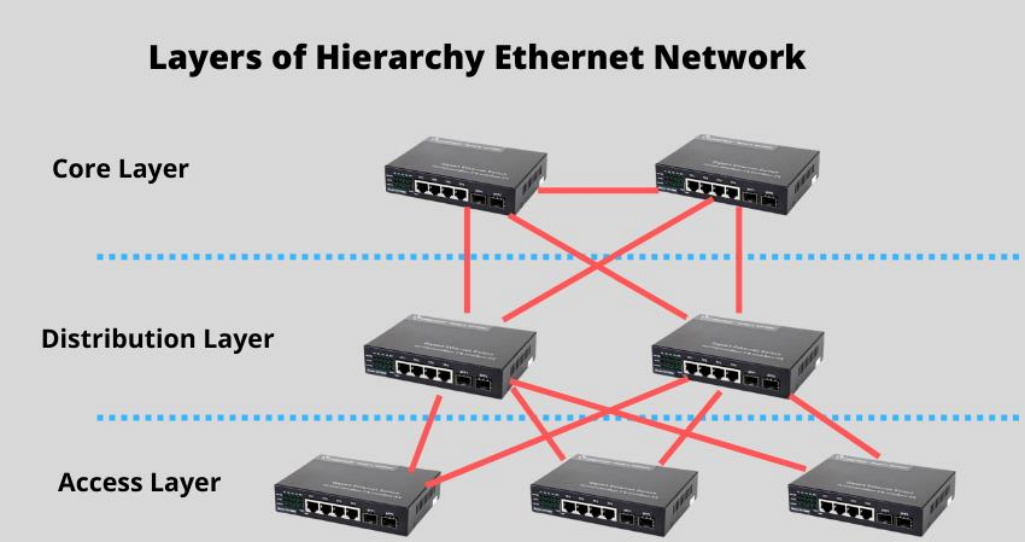
- It cannot find the best/ shortest path of the network.
- No mechanism for traffic detection.
- No mechanism for data filtration.
- Not capable of connecting to different network topologies like token ring, ethernet, etc.

Difference Between Network Hub And Switch

Hub	Switch
It works on the physical layer of the OSI model.	It works on the data link layer of the OSI model.
It performs frame flooding, which includes broadcast, multicast and unicast as well.	It mainly performs broadcasts and performs multicast, and unicast whenever required.
The transmission mode is half-duplex.	The transmission mode is full-duplex.
It cannot perform data filtering.	It can filter data and send the frame to the desired destination.
There is no spanning tree.	A switch may contain more than one spanning tree possible.
It can not store the MAC address of the ports and the destination address of the frame that arrived.	It can store the data in a routing table and it helps in further sending the data.
It is a passive device.	It is an active device.
Hub can operate at a speed of 10Mbps.	The switch can operate at a speed of 10-100Mbps and 1- 10 Gbps.

This white paper introduces the following three types of network switches and further discusses the selection criteria for each switch.

- Core Switch
- Distribution Switch
- Access Switch



Core switches

Core switches are the high-performance backbone of a network's core layer, responsible for fast, reliable, and efficient switching of traffic between different areas of a network or to the internet. Operating at the top tier of hierarchical network design, they aggregate data from distribution switches, offering massive bandwidth, redundancy, and minimal latency.

Key Aspects of Core Switches:

- **Purpose:** Act as the central backbone linking distribution switches in enterprise networks, data centers, and MANs/WANs.
- **Performance:** They focus on speed, handling high-volume traffic (e.g., 10/40/100G Ethernet) using robust hardware with advanced forwarding capabilities.
- **Redundancy:** Engineered for reliability, core switches often include redundant power supplies and links to ensure minimal downtime.
- **Functionality:** Unlike access switches that manage end-user connectivity, core switches prioritize packet transport, often limiting complex security protocols or QoS to maintain maximum speed.
- **Key Features:** High backplane bandwidth, large capacity, and high-density port resources.

Core switches differ from edge/access switches by prioritizing high-speed transport over user-level connectivity.

Distribution switch:

A distribution switch acts as the central intermediary in a network's three-layer architecture, sitting between access switches (end-user devices) and core switches (the backbone). It aggregates traffic from multiple access switches, performs routing (Layer 3) to enable inter-VLAN communication, and enforces security policies, ensuring efficient data flow and high availability.

Key Functions and Characteristics

- Aggregation: Connects multiple edge/access switches, reducing the number of direct links to the core layer.
- Layer 3 Routing: Handles inter-VLAN routing, allowing different network segments to communicate.

- Policy Enforcement: Implements security features such as Access Control Lists (ACLs), Quality of Service (QoS), and packet filtering.
- Redundancy and High Availability: Provides a bridge that connects the access layer to the core, offering multiple paths to ensure network continuity in case of failure.

Key Differences from Other Switches

- vs. Access Switch: Distribution switches have higher throughput, more bandwidth, and advanced routing capabilities compared to the Layer 2, end-user-focused access switches.
- vs. Core Switch: While core switches focus purely on speed for moving data across the backbone, distribution switches focus on "intelligence" (routing, security, policy).

Common Use Cases

- VLAN Segmentation: Aggregates and routes traffic between VLANs defined at the access layer.
- Campus Networks: Connects different buildings, with each building having its own distribution switch feeding into the main core.
- Traffic Management: Prioritizes sensitive traffic (like VoIP or video) over general traffic.

Access switches:

Access switches are Layer 2 networking devices situated at the edge of a network, serving as the primary connection point for end-user devices like computers, printers, IP phones, and Wi-Fi access points. They manage data traffic, improve efficiency via MAC address learning, and often support Power over Ethernet (PoE) to power devices.

Key Aspects of Access Switches:

- Purpose: Connect end devices to the network infrastructure.
- Location: Placed at the edge of the network (e.g., in office workstations or workgroup areas).
- Features: High port density (e.g., 24/48 ports), VLAN support for traffic segmentation, and port security features.
- Operation: Generally operate at Layer 2 (Data Link Layer) of the OSI model.
- Role in Hierarchy: Connect directly to distribution or core switches to transmit data into the wider network.

Common Uses:

- Office Networking: Linking PCs, printers, and phones to the LAN.
- Wireless Connectivity: Connecting wireless access points.
- Security & Surveillance: Connecting IP cameras and access control systems.

These switches are the most numerous type of switch in an enterprise network, focusing on cost-effective, high-port-density connectivity.

Core Switch vs. Distribution Switch vs. Access Switch:

Factors	Core Switch	Distribution Switch	Access Switch
Working layer	Core layer	Distribution layer	Access layer
Numbers of switches in a network	The least (normally one or two)	May comprise sum of the core layer and access layer switches	The most compare to c layer
Features	Layer 3 switches, highest reliability, functionality and throughput	Layer 3 switches, higher reliability, functionality and throughput	Layer 2 switches, relati lower reliabi functionality and throug
Supported functions	Very high forwarding rate, QoS, redundant components, etc.	Packet filtering, QoS, and application gateways, etc.	Port security, VLANs, Ethernet/Gigabit Ethe PoE, etc.
Cost	Highest	Higher	Relatively Lower

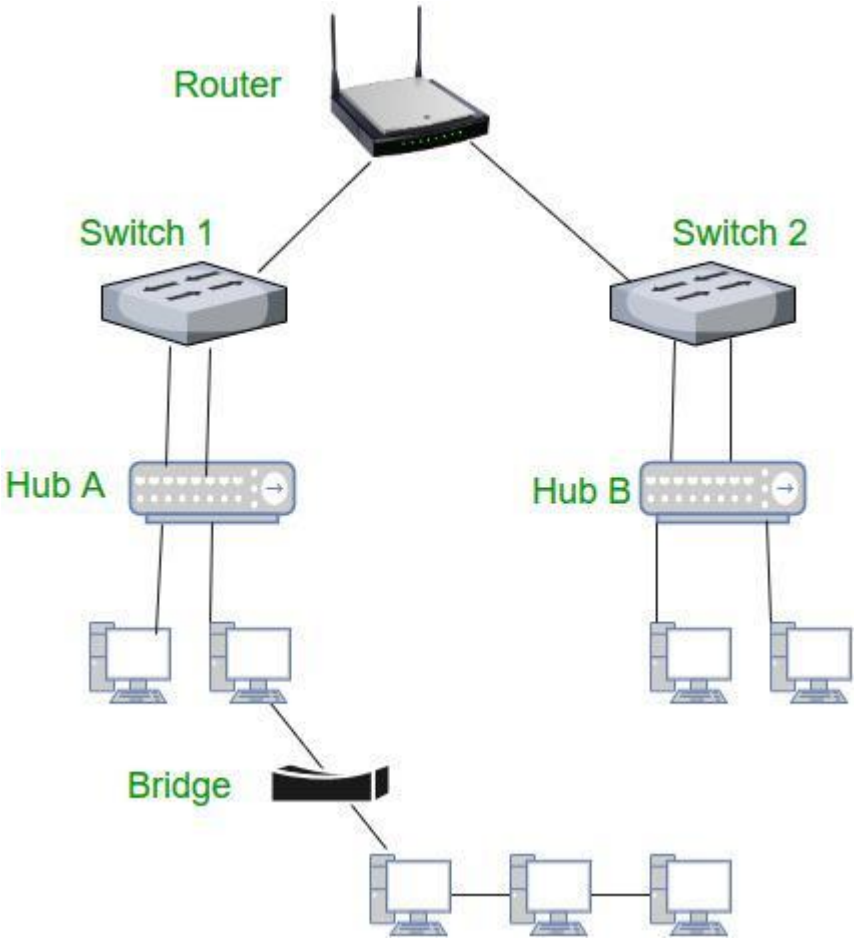
Router:

A router is a networking device that forwards data packets between different computer networks. It connects multiple packet-switched networks or subnetworks, managing traffic by directing packets to their intended IP addresses. Routers allow multiple devices to share an Internet connection efficiently.

How Does a Router Work?

Routers determine the path for a packet by examining its destination IP address and consulting the routing table, which contains information on network paths. They use a set of rules to identify the most efficient route for each packet.

- Static routing: Configured manually, suitable for small or stable networks.
- Dynamic routing: Automatically updated based on network activity, ideal for large or changing networks.



Functions of a Router

- Forwarding: Receives packets, examines headers, and forwards them to the correct output port.
- Routing: Determines the optimal path for packets using routing tables and algorithms.
- Network Address Translation (NAT): Translates private IPs to a public IP for Internet access.
- Security: Supports firewalls and other security measures.
- VPN Connectivity: Provides secure remote access to networks.
- Bandwidth Management: Controls data flow to prevent congestion.
- Monitoring & Diagnostics: Tracks traffic and helps troubleshoot network issues.

A typical router consists of:

- Input Port: Accepts packets, decapsulates them, and determines forwarding paths.
- Switching Fabric: The core of the router connecting input ports to output ports. Can be implemented via:

Memory switching: CPU copies packets to output ports.

Bus switching: Single bus transfers packets to the correct port.
Interconnection networks: Complex designs connecting multiple input/output ports.

- Output Port: Transmits packets to outgoing links, managing queuing and link-layer functions.
- Routing Processor: Executes routing protocols and algorithms, maintaining the forwarding table.

Common Routing Protocols

- Open Shortest Path First (OSPF): Determines the optimal path across networks.
- Border Gateway Protocol (BGP): Shares routing information between edge routers.
- Interior Gateway Routing Protocol (IGRP): Exchanges routing info within autonomous networks.
- Enhanced IGRP (EIGRP): Requests routing paths from neighbors if unknown.
- Exterior Gateway Protocol (EGP): Shares routing data between internet hosts.

Applications of Routers

- Connect remote servers, networks, and devices globally.
- Support wired and wireless communication, including high-speed data transfer.
- Used by ISPs to transmit audio, video, image, and email efficiently.
- Implement access control, enabling selective resource usage.

Types of Routers

1. Broadband Routers: Connect computers to the Internet and share the connection.
2. Wireless Routers: Create Wi-Fi networks in homes or offices.
3. Wired Routers: Connect multiple devices via Ethernet cables, common in schools and offices.
4. Edge Routers: Located at network boundaries, distributing packets to and from ISPs.
5. Core Routers: Operate within networks, handling heavy data traffic.
6. Virtual Routers: Software-based routers implemented on virtual machines for flexibility and scalability.
7. Portable Routers: Small devices creating private Wi-Fi for mobility.

WiFi Access Point (AP)

A WiFi Access Point (AP) is a hardware device that enables wireless devices (phones, laptops) to connect to a wired network, acting as a bridge. A Wireless LAN Controller (WLC) acts as the central brain, managing multiple APs simultaneously to streamline configuration, security, and roaming in large networks.

Key Differences and Functions:

Wireless Access Point (AP/WAP):

- Function: Takes bandwidth from a router (via Ethernet) and broadcasts it as Wi-Fi, expanding coverage.
- Role: Acts like a switch in a wired network but for wireless devices, allowing higher user density than a home router.
- Types: Standalone (independent) or Lightweight (controlled by a WLC).
- Features: Supports VLANs, multiple SSIDs (guest/secure), and QoS to prioritize traffic.

Wireless LAN Controller (WLC):

- Function: Centralizes control of multiple APs, acting as the "orchestra conductor" for the network.
- Role: Automates configuration, radio frequency management, security policies, and roaming (uninterrupted movement between APs).
- Usage: Crucial for large enterprise, corporate, or campus networks, whereas small offices may only use independent APs.

In modern, larger deployments, the WLC holds the intelligence, while APs become "lightweight" (LWAP), receiving configurations directly from the controller.