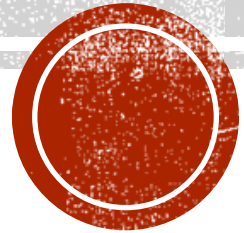
NETWORKING



By

Jitendra Singh Tomar || Jeetu

AGENDA

- Fundamentals Review
- Network Addressing Scheme
- Switching
- Router
- IP Routing
- IPv6
- WAN
- Crash-recovery(Router)
- SDN - Software Define Networking

INTRODUCTION TO NETWORKS

- Computer Network is a group of computers connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network.
- The aim of the computer network is the sharing of resources among various devices.
- A computer network consists of various kinds of nodes. Servers, networking hardware, personal computers, and other specialized or general-purpose hosts can all be nodes in a computer network.

WHAT IS A COMPUTER NETWORK?

- A computer network is a system that connects many independent computers to share information (data) and resources.
- The integration of computers and other different devices allows users to communicate more easily.
- A network connection can be established using either cable or wireless media.
- Hardware and software are used to connect computers and tools in any network.

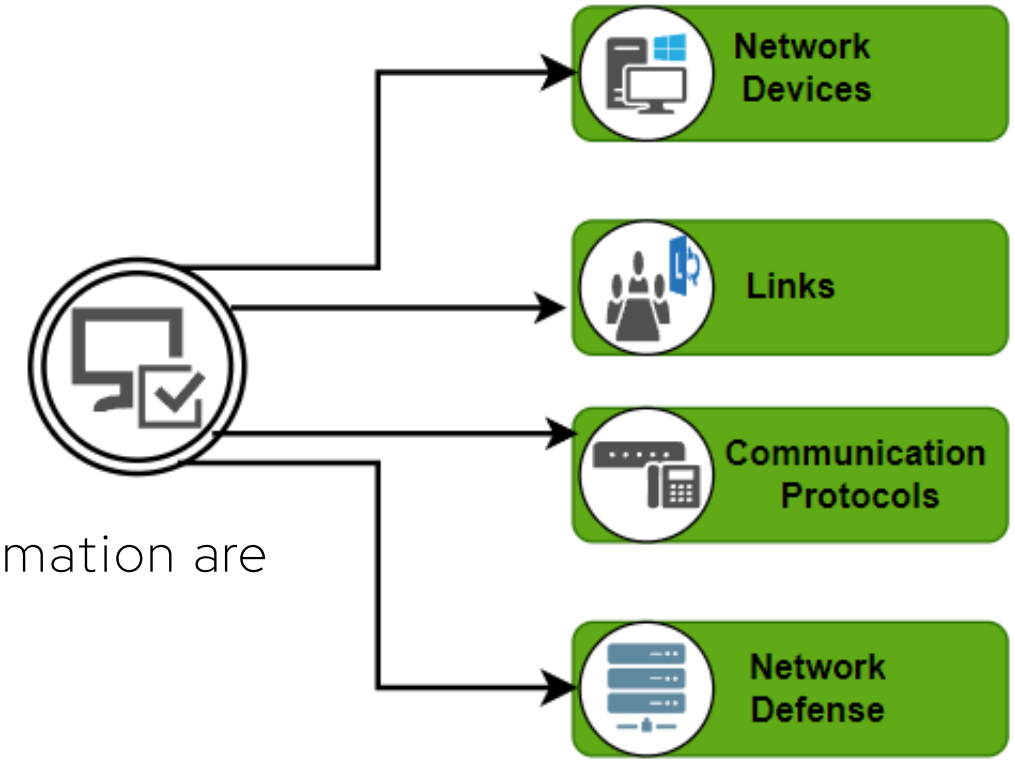
WHAT DO COMPUTER NETWORKS DO?

Computer Networks help in providing better connectivity that helps nowadays. Modern computer networks have the following functionality:

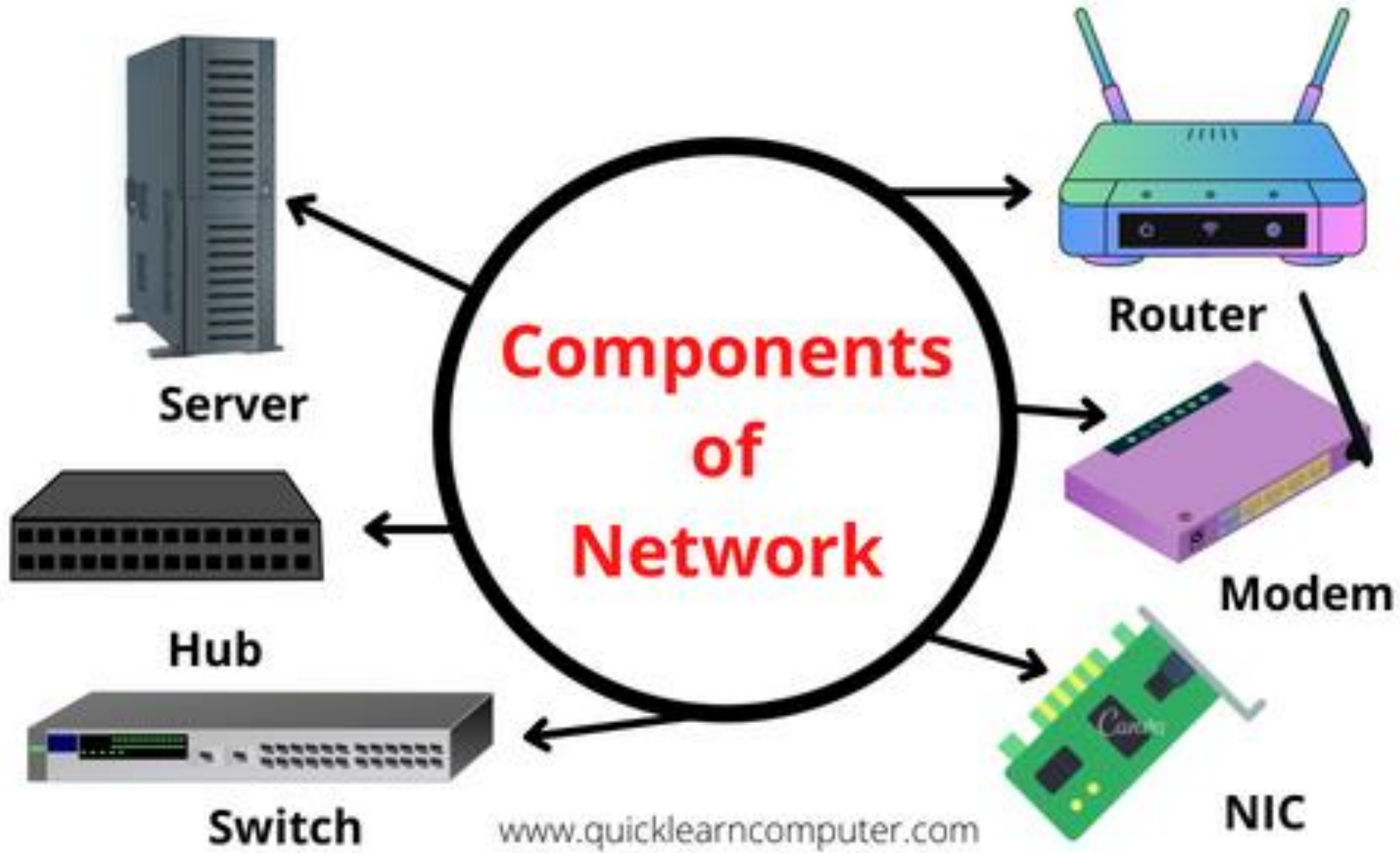
- Computer Networks help in operating virtually
- Computer Networks integrate on a large scale
- Computer Networks respond very quickly in case of conditions change
- Computer Networks help in providing data security

KEY COMPONENTS OF A COMPUTER NETWORK

- A computer network is made up of two main parts:
  - Devices (called nodes) &
  - Connections (called links)
- The links connect the devices to each other.
- The rules for how these connections send information are called communication protocols.
- The starting and ending points of these communications are often called ports.



COMPONENTS OF COMPUTER NETWORK



NETWORK DEVICES

- Network Interface Card (NIC)
- Repeater
- Hub
- Bridges
- Switches
- Routers
- Gateways

NETWORK INTERFACE CARD

- NIC is a hardware component, typically a circuit board or chip on a computer.
- A NIC provides a computer with a dedicated, full-time connection to a network.
- It implements the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi.
- Each card represents a device and can prepare, transmit and control the flow of data on the network.
- The NIC operates as a middleman between a computer and a data network.

TYPES OF NICS

- Wireless. NICs that use an antenna to provide wireless reception through radio frequency waves. Wi-Fi connections use wireless NICs.
- Wired. NICs that have input jacks made for cables. Ethernet is the most popular wired LAN technology.
- USB. NICs that provide network connections through a device plugged into the USB port.
- Fiber optics. NICs used as a high-speed support system for network traffic handling on server computers.

NIC COMPONENTS

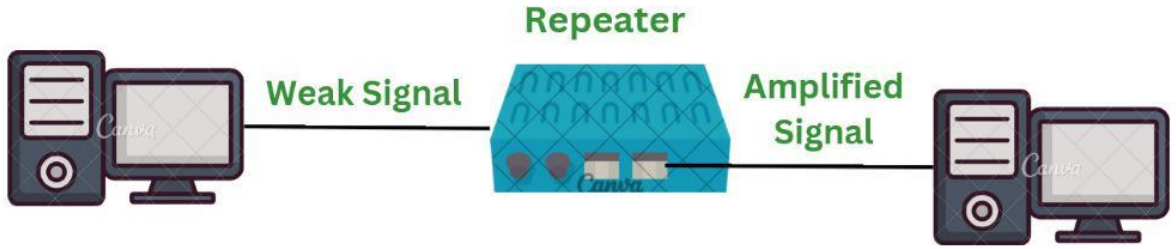
- Speed. All NICs have a speed rating in terms of *megabits per second* (Mbps) that determines the card's performance in a network. The average Ethernet NICs come in
  - 10 Mbps,
  - 100 Mbps,
  - 1000 Mbps and
  - 1 gigabits per second varieties.
- Driver. The required software that passes data between the computer's operating system and the NIC.

NIC COMPONENTS

- MAC address. Unique, unchangeable media access control addresses, also known as physical network addresses, are assigned to NICs. Router.
- LED indicator. Most NICs have an LED indicator integrated into the connector to notify the user when the network connects and data transmission occurs.
- Router. A router is sometimes needed to enable communication between a computer and other devices. In this case, the NIC connects to the router which is connected to the internet.

REPEATER

- Repeaters are defined as a networking device that is used to amplify and generate the incoming signal.



- The main aim of using a repeater is to increase the networking distance by increasing the strength and quality of signals.
- The major advantage of using a repeater is that it provides with transfer of data with more security and over a long distance.

FEATURES OF REPEATERS

- Repeater can regenerate the signal without modifying it.
- Repeaters can be used in analog signals and digital signals.
- Repeaters can extend the range of networks.
- Dynamic networking is supported by repeater.
- Use of Repeaters reduces error and loss of data.
- Power is required for working of repeaters.
- Using repeater can add complexity in the network.

TYPES OF REPEATERS

- According to the type of Signals.
  - *Analog Repeater* – Analog repeaters are used to amplify only the analog signals.
  - *Digital Repeater* – Digital repeaters are the type of repeaters that does not amplify digital signal but regenerates it directly.
- According to the type of Connected Network.
  - *Wired Repeaters* – Wired repeater receives the signal and repeats it within LAN.
  - *Wireless Repeaters* – Wireless repeaters are used in wireless Local Area Networks(LANs) and Cellular networks. A router connected in the network sends wireless signal to the repeater.

TYPES OF REPEATERS

- According to the Domain of LAN Networks.
  - *Local Repeaters*
    - Local Repeaters are used in Local Area Networks where the network is very small.
    - The distance between the devices connected in network is very small.
  - *Remote Repeaters*
    - Remote Repeaters are used in Local Area Networks where network is very large.
    - The distance between the devices connected in network is more.

TYPES OF REPEATERS

- Based on Technologies
  - *Microwave Repeater*
    - The use of microwave repeater depends upon the distance between two devices.
    - In microwave repeaters high power transmitters and sensitive receivers are used.
  - *Optical Repeater*
    - Optical repeaters are defined as a type of repeaters that are used for the communication of fiber optic communication systems.
    - Optical repeaters can amplify and reshape the operations before they are being transmitted.

TYPES OF REPEATERS

- Based on Technologies
  - *Radio Repeater*
    - Radio repeater is a type of repeater that transmits all the received data into radio signals.
    - Radio repeaters has two different ports namely radio receiver and radio transmitter.
  - *Telephone Repeater*
    - Telephone repeaters are type of repeaters used for long distance networks.
    - Amplifiers having transistors are used in telephone repeater.
    - Telephone repeaters are majorly used for communication in submarines.

ADVANTAGES & DISADVANTAGES OF REPEATER

Advantages

- Better Performance of Network
- Cost Effective
- Extends the network
- No Physical barriers
- Enhanced Signals

Disadvantages

- Network Traffic
- Network Segmentation
- Limited number of repeaters
- Collision Domain

HUB

- Hub in networking plays a vital role in data transmission and broadcasting.
- A hub is a hardware device used at the physical layer to connect multiple devices in the network.
- Hubs are widely used to connect LANs.
- A hub has multiple ports & cannot filter the data, i.e. it cannot identify the destination of the packet, So it broadcasts or sends the message to each port.

TYPES OF NETWORK HUBS

- Active Hub
  - They have a power supply for regenerating, and amplifying the signals.
  - When a port sends weak signaled 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.

TYPES OF NETWORK HUBS

- Passive Hub
  - Passive hubs are simply used to connect signals from different network cables as they do not have any computerized 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 amplify or strengthen the signal.

TYPES OF NETWORK HUBS

- Intelligent Hub
  - Intelligent hubs as the name suggests 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 analyzing and troubleshooting network problems. Intelligent hubs work similarly to active hubs but with some management features.
  - Like it can monitor the traffic of the network and the configuration of a port.

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 & DISADVANTAGES OF HUB

Advantages

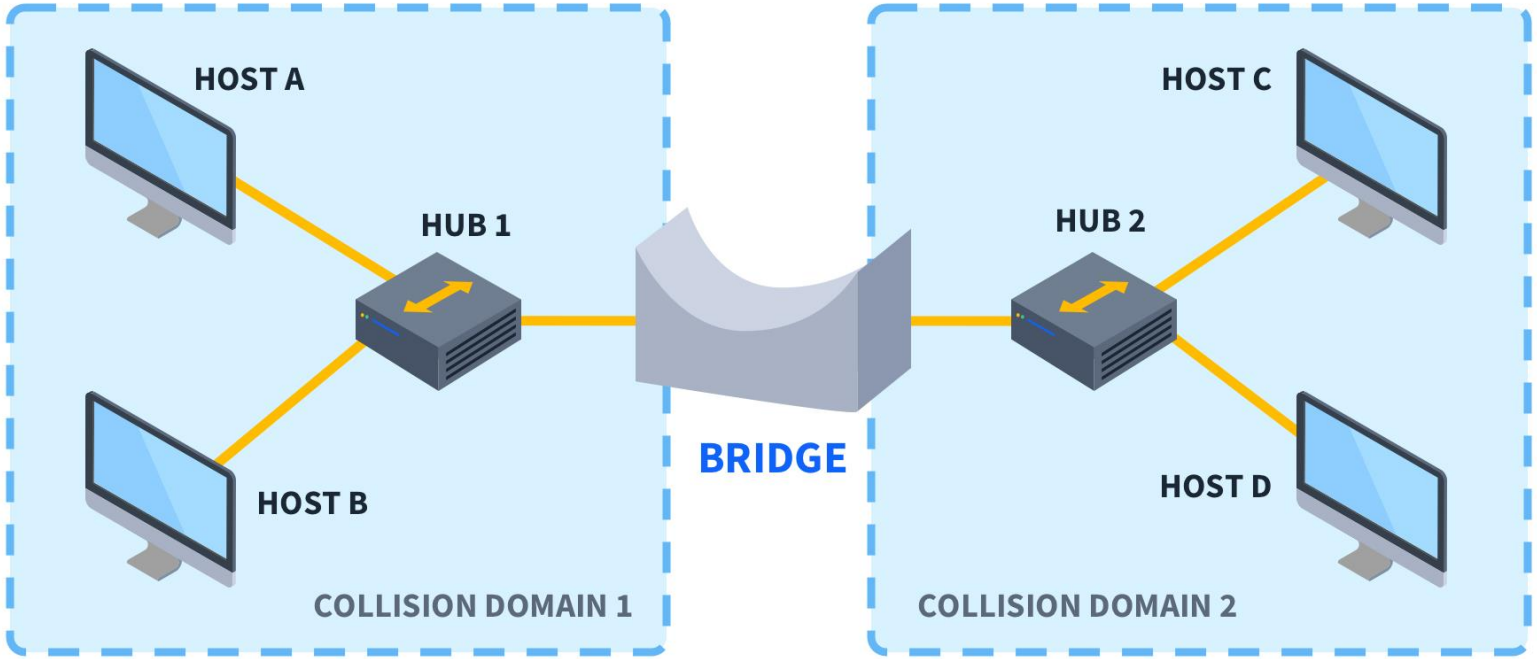
- It is less expensive.
- It does not impact network performance.
- Hub support different network media

Disadvantages

- 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.

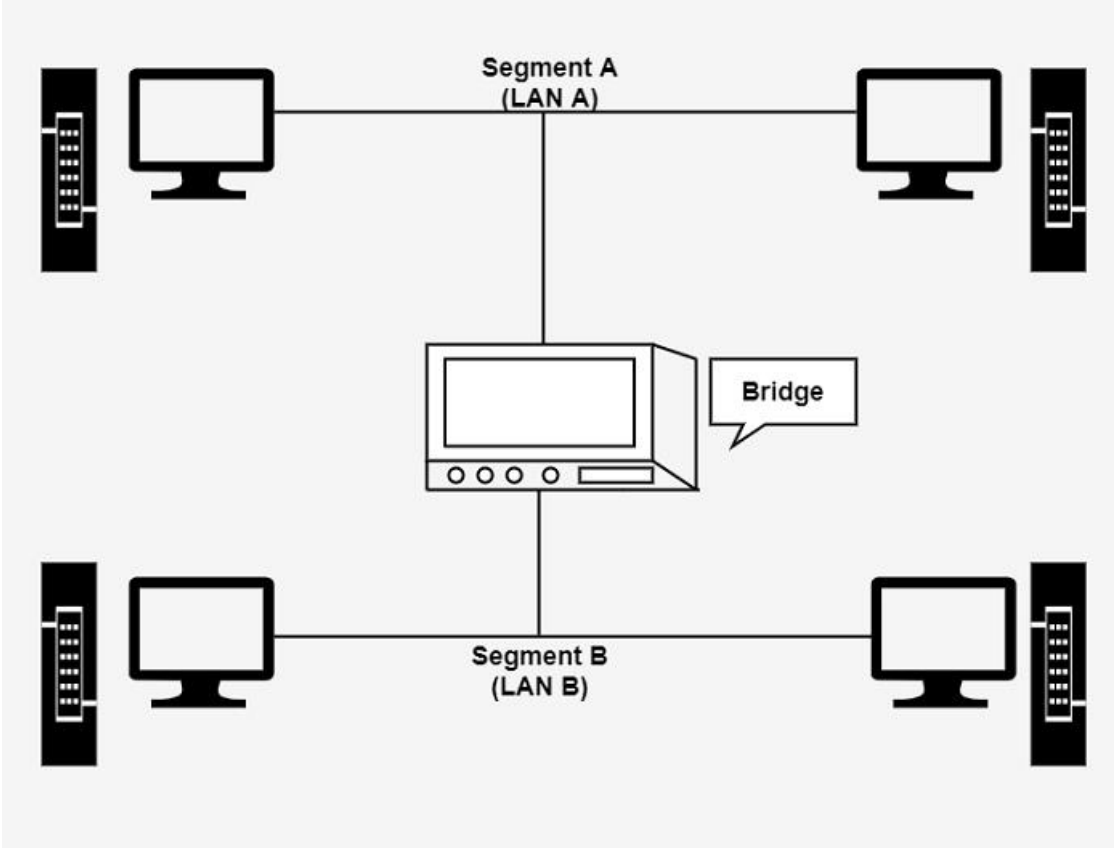
BRIDGES

- Bridges are used to connect two subnetworks that use interchangeable protocols.
- It combines two LANs to form an extended LAN.
- The main difference between the bridge and repeater is that the bridge has a penetrating efficiency.

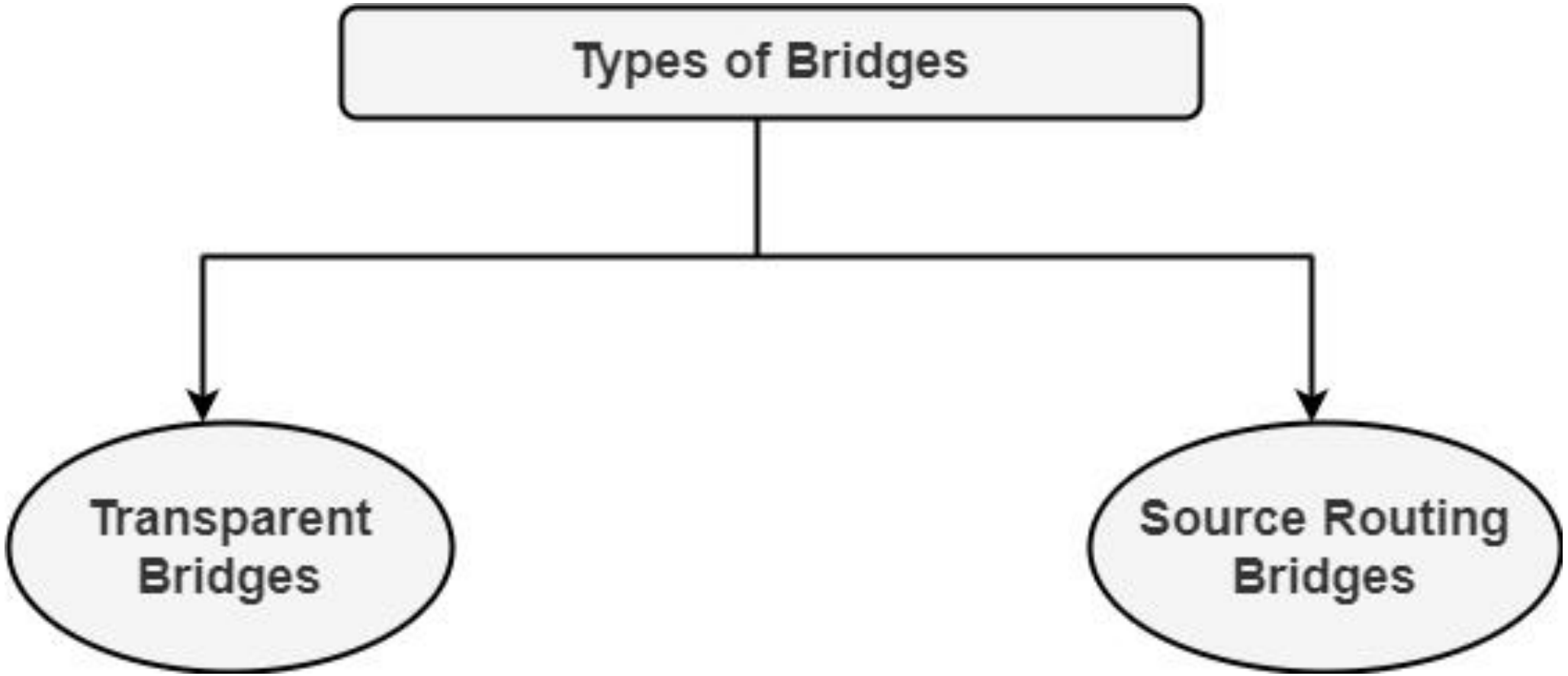


WORKING OF BRIDGES

- A bridge accepts all the packets and amplifies all of them to the other side.
- The bridges are intelligent devices that allow the passing of only selective packets from them.
- A bridge only passes those packets addressed from a node in one network to another node in the other network.



TYPES OF BRIDGES



TYPES OF BRIDGES

- Transparent Bridges
  - It is also called learning bridges.
  - Bridge construct its table of terminal addresses on its own as it implements connecting two LANs.
  - It facilitates the source location to create its table. It is self-updating. It is a plug and plays bridge.

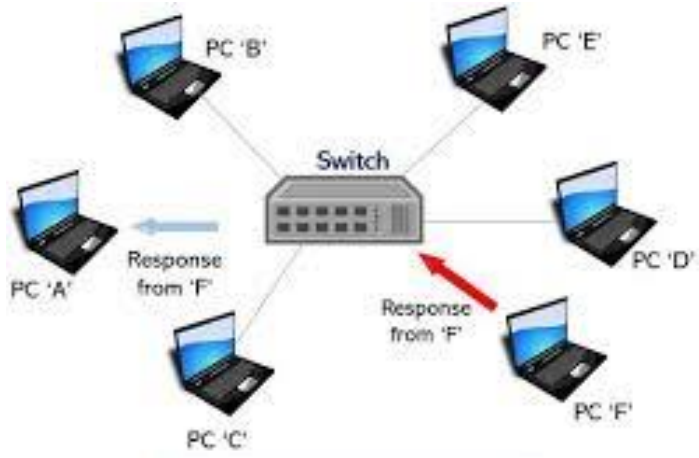
TYPES OF BRIDGES

- Source Routing Bridge
  - This sending terminal means the bridges that the frames should stay.
  - This type of bridge is used to prevent looping problem.

SWITCHES

- The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments.
- It is responsible for filtering and forwarding the packets between LAN segments based on MAC address.
- Switches have many ports, and when data arrives at any port, the destination address is examined first and some checks are also done and then it is processed to the devices.
- Different types of communication are supported here like unicast, multicast, and broadcast communication.

FEATURES OF NETWORK SWITCHES



- It operates in Data Link Layer in OSI Model.
- It performs error checking before forwarding data.
- It transfers the data only to the device that has been addressed.
- It allocates each LAN segment a limited bandwidth.
- Packet Switching techniques are used to transfer data packets from source to destination.
- Switches have a more significant number of ports.

WHY ARE NETWORK SWITCHES VALUABLE?

- Switches are having full-duplex communication which helps in making effective use of bandwidth.
- Switches help to provide a wired connection to printers, IoT devices, wireless points, and many more devices.
- IoT Devices send data through Network Switches that help in making smarter surroundings with the help of Artificial Intelligence.
- Network Devices are made with the help of Switches that carry a large number of traffic in telecommunication.

TYPES OF SWITCHES

- Virtual Switches: Virtual Switches are the switches that are inside Virtual Machine hosting environments.
- Routing Switches: These are the switches that are used to connect LANs. They also have the work of performing functions in the Network Layer of the OSI Model.
- Unmanaged Switches: Unmanaged Switches are the devices that are used to enable Ethernet devices that help in automatic data passing. These are generally used for home networks and small businesses.

TYPES OF SWITCHES

- Managed Switches: Managed Switches are switches having more complex networks. SNMP (Simple Network Management Protocol) can be used for configuring managed switches.
- LAN Switches: LAN (Local Area Network) Switches are also called ethernet switches or data switches. LAN switches always try to avoid overlapping of data packets in the network just by allocating bandwidth in such a manner.
- PoE Switches: Power over Ethernet(PoE) are the switches used in Gigabit Ethernets. PoE help in combining data and power transmission over the same cable so that it helps in receiving data and electricity over the same line.

TYPES OF SWITCHES

- Smart Switches: Smart Switches are switches having some extra controls on data transmissions but also have extra limitations over managed Switches. They are also called partially managed switches.
- Stackable Switches: Stackable switches are connected through a backplane to combine two logical switches into a single switch.
- Modular Switches: These types of switches help in accommodating two or more cards. Modular switches help in providing better flexibility.

NETWORK SWITCH VS ROUTER

Network Switch	Router
It works on Layer 2 of the OSI Model.	It primarily a device of Layer 3 of the OSI Model.
The resource is shared among multiple devices.	Data is moved between two or more computers.
Network switches uses data frames	Routers use data packets.
It works in a Wired network connection.	It works with both wired and Wifi networks.
Switches use MAC Addresses for transferring data.	Routers use IP Addresses

NETWORK SWITCHES

- Network switches help provide automatic link connections that remove time-consuming settings and provide easy access to network devices.
- Switches provide a better, more secure, reliable network having more control over data.
- Switches work in full duplex mode, which helps in continuous data transmission and that improves better connectivity.
- As MAC Address is used for the devices connected to it, that helps in the delivery of messages to only the required destination, not everywhere.
- Network Switches work for home networks or local networks where streaming works are performed regularly.

ADVANTAGES & DISADVANTAGES OF SWITCHES

Advantages

- Prevents traffic overloading in a network by segmenting the network into smaller subnets.
- Increases the bandwidth of the network.
- Less frame collision as the switch creates the collision domain for each connection.

Disadvantages

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

ROUTERS

- The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks.
- A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets.
- There are some popular companies that develop routers; such are
  - Cisco
  - 3Com
  - HP
  - Juniper
  - D-Link

ROUTERS

- A router is used in LAN (Local Area Network) and WAN (Wide Area Network) environments.
- It shares information with other routers in networking.
- It uses the *routing protocol* to transfer the data across a network.
- It is more expensive than other networking devices like switches and hubs.

ROUTING PROTOCOL

- A routing protocol is a set of rules that routers use to identify and forward packets across a network path.
- Routing protocols can be categorized into two main types:
  - *Interior gateway protocols*
    - Interior gateway protocols work best within an autonomous system, which is a network that's administratively controlled by a single organization.
  - *Exterior gateway protocols.*
    - Exterior gateway protocols are better for managing information transfer between two autonomous systems.

TYPES OF ROUTER

- Broadband routers
  - it is used to connect computers or it is also used to connect to the internet.
- Wireless routers
  - These routers are used to create a wireless signal in your office or home.
- Wired routers
  - It takes the transmission data from the modem and distribute it to a further network

TYPES OF ROUTER

- Edge routers
  - These are located at the edges usually connected to an Internet Service Provider, and distribute packets across multiple packets.
- Core routers
  - These routers distribute packets within the same network. The main task is to carry heavy data transfers.
- Virtual routers
  - They are implemented using a software on the virtual machine , and they are more flexible and scalable.

FUNCTIONS OF ROUTER

- Forwarding
- Routing
- Networking Address Translation (NAT)
- Security
- Quality of Service (QoS)
- Virtual Private Network (VPN) connectivity
- Bandwidth management
- Monitoring and diagnostics

ADVANTAGES & DISADVANTAGES OF ROUTER

Advantages

- Easier Connection
- Security
- NAT Usage
- Support Dynamic Routing
- Filtering of packets

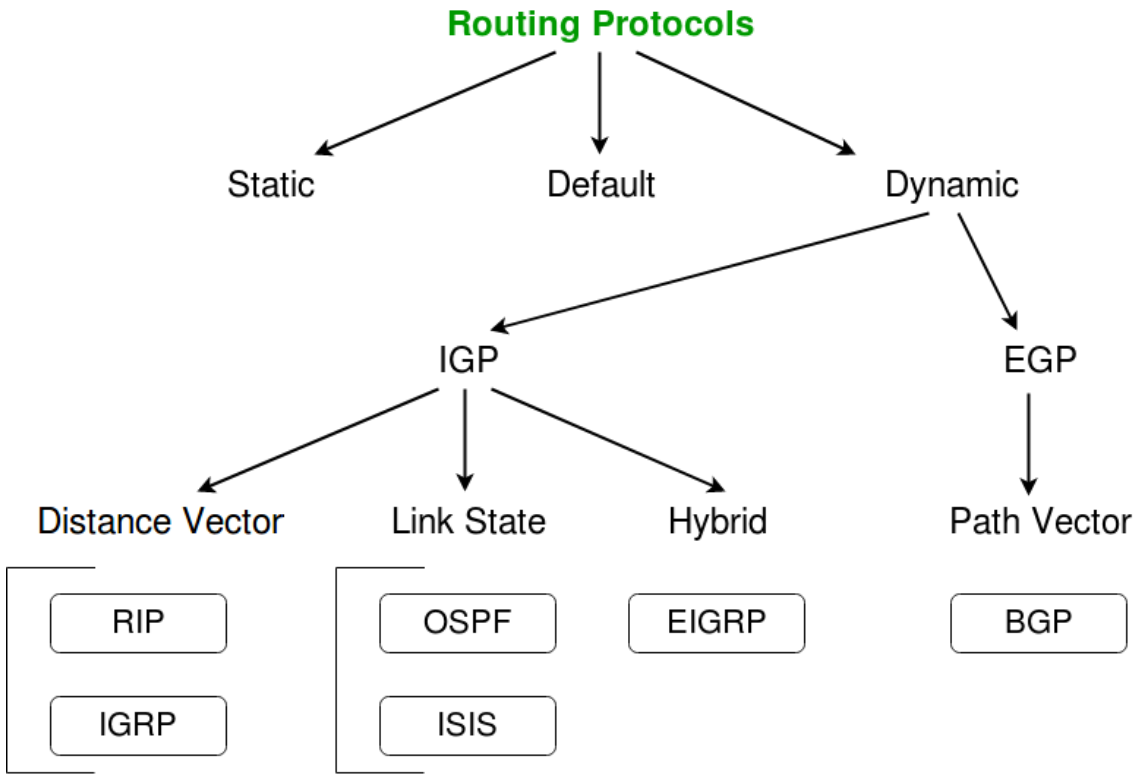
Disadvantages

- Slower
- High Cost
- Need for configuration
- Quality Issues
- Bandwidth shortages

ROUTING PROTOCOL

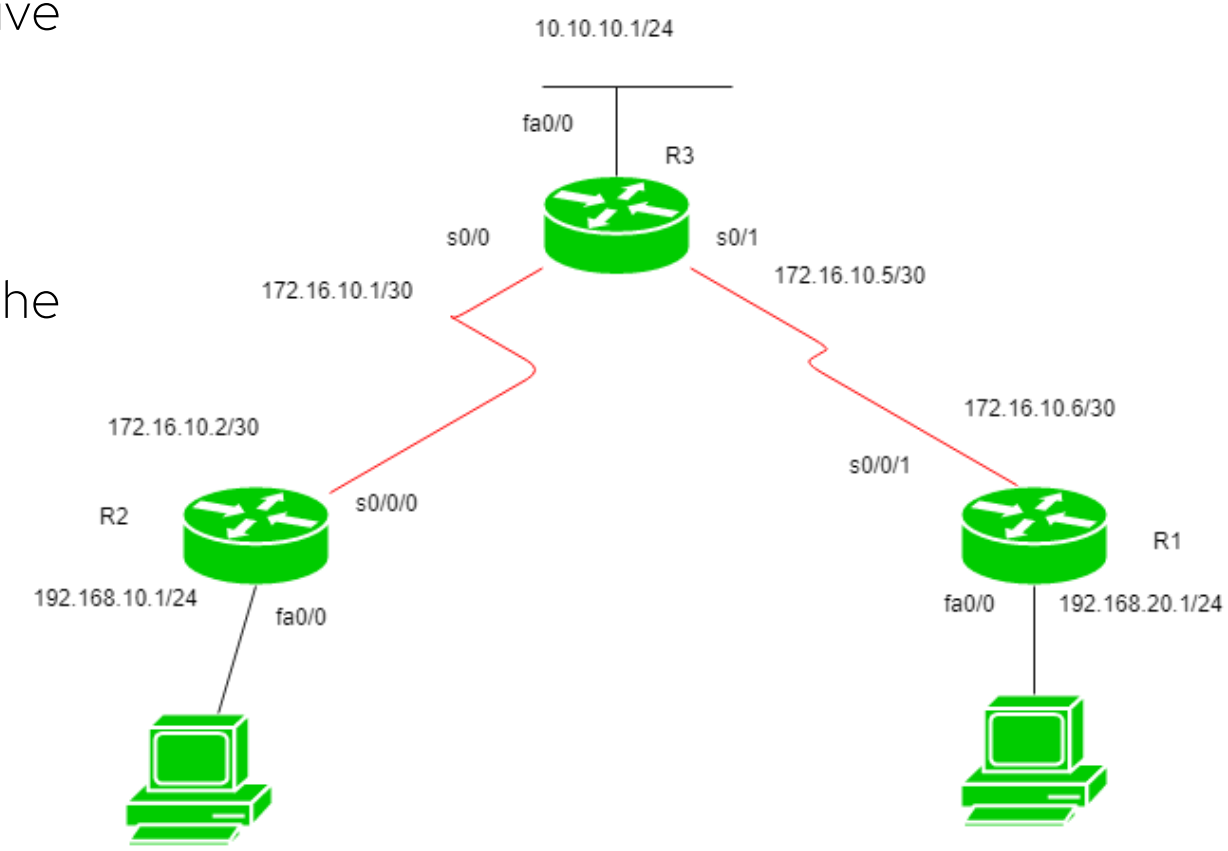
Routing is of 3 types:

- Static Routing
- Default Routing
- Dynamic Routing



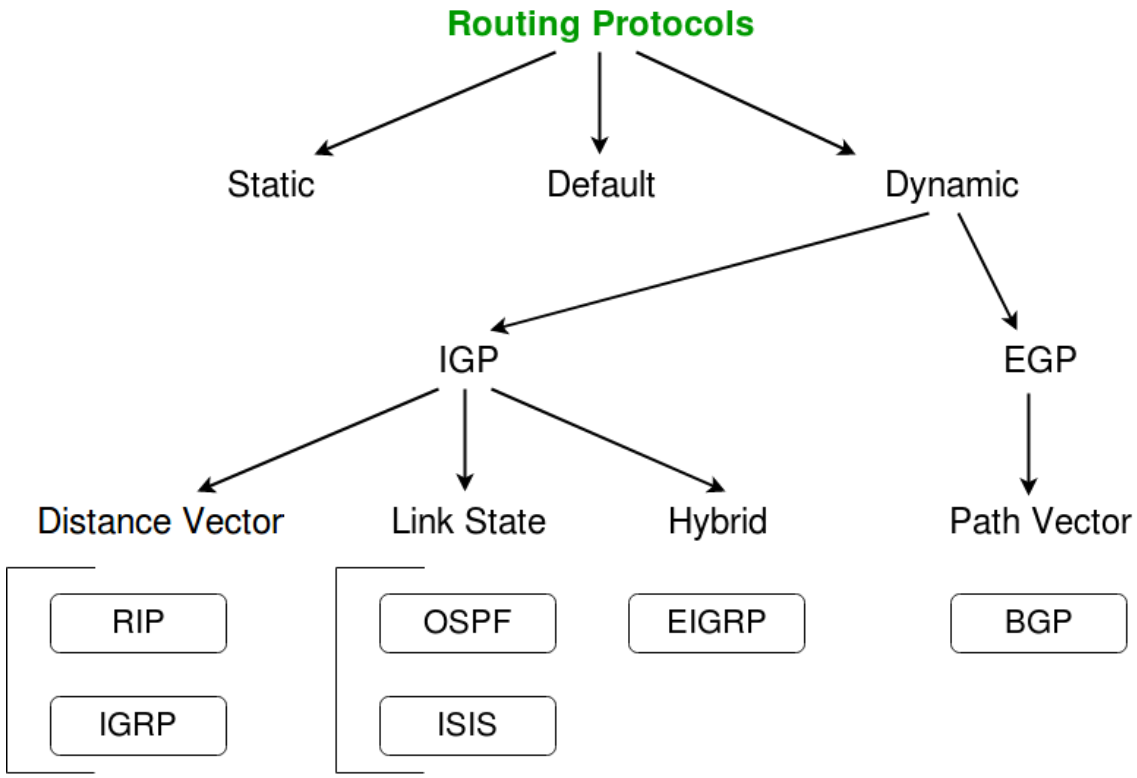
ROUTING PROTOCOL – STATIC ROUTING

- Static Routing is also called as “non-adaptive routing”.
- In this routing is done manually by the administrator.

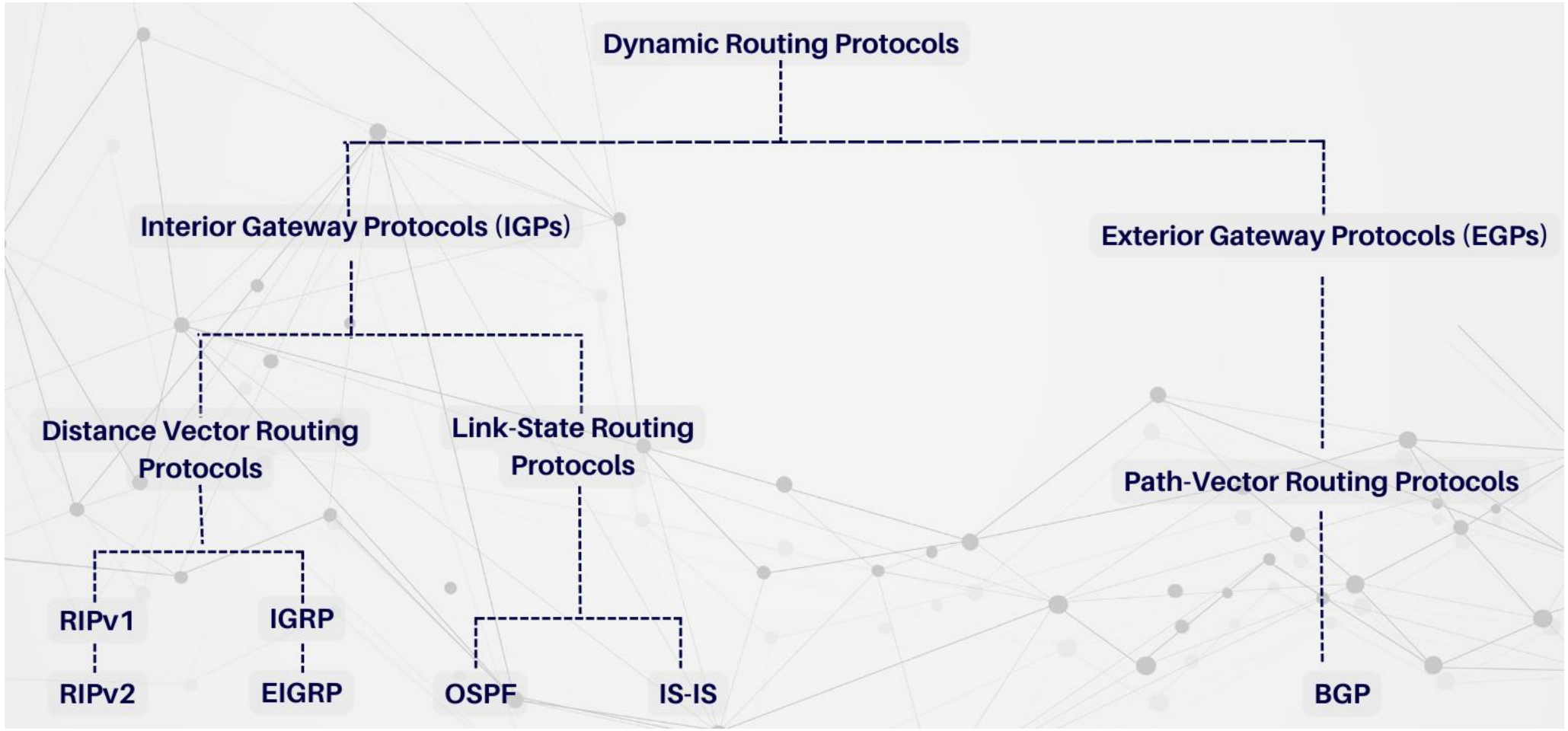


ROUTING PROTOCOL

- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)
- Interior Gateway Routing Protocol (IGRP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Exterior Gateway Protocol (EGP)



DYNAMIC ROUTING PROTOCOL



WHAT IS AN INTERNET PROTOCOL (IP) ADDRESS?

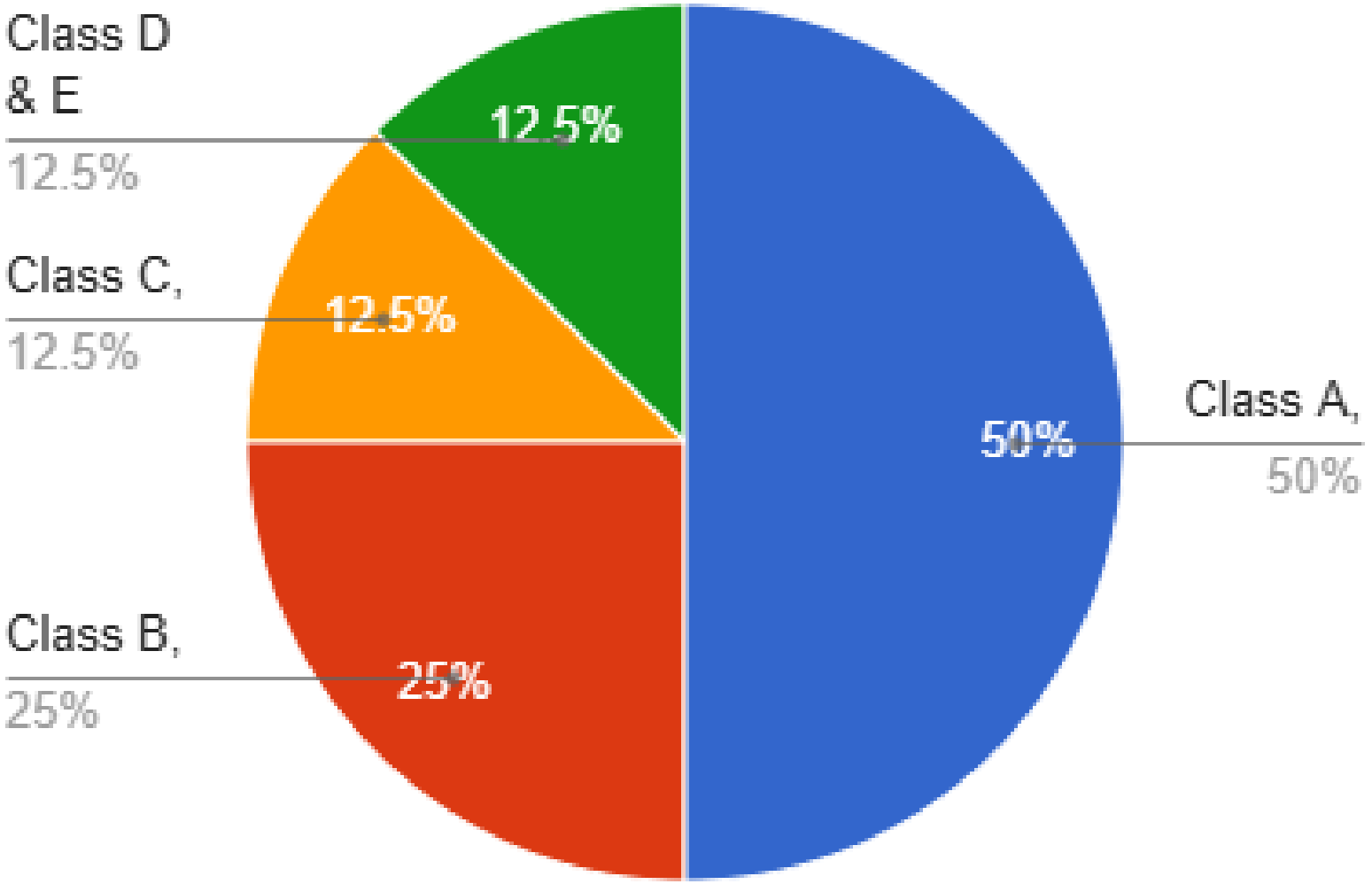
- An Internet Protocol (IP) address is a unique identifier assigned to each device connected to a network. This address enables devices to locate each other and communicate across networks, such as local area networks (LANs) and the internet.
- An IP address functions like a "home address" for each device, directing data to the correct destination.
- There are two main types of IP addresses in use today:
  - IPv4 (Internet Protocol version 4)
  - IPv6 (Internet Protocol version 6)

IPV4 ADDRESSES

- IPv4 is the older and more widely used IP addressing format. An IPv4 address is a 32-bit number divided into four 8-bit sections (octets), each separated by a dot.
- Each octet can hold a value between 0 and 255, resulting in an address structure like 192.168.1.1.

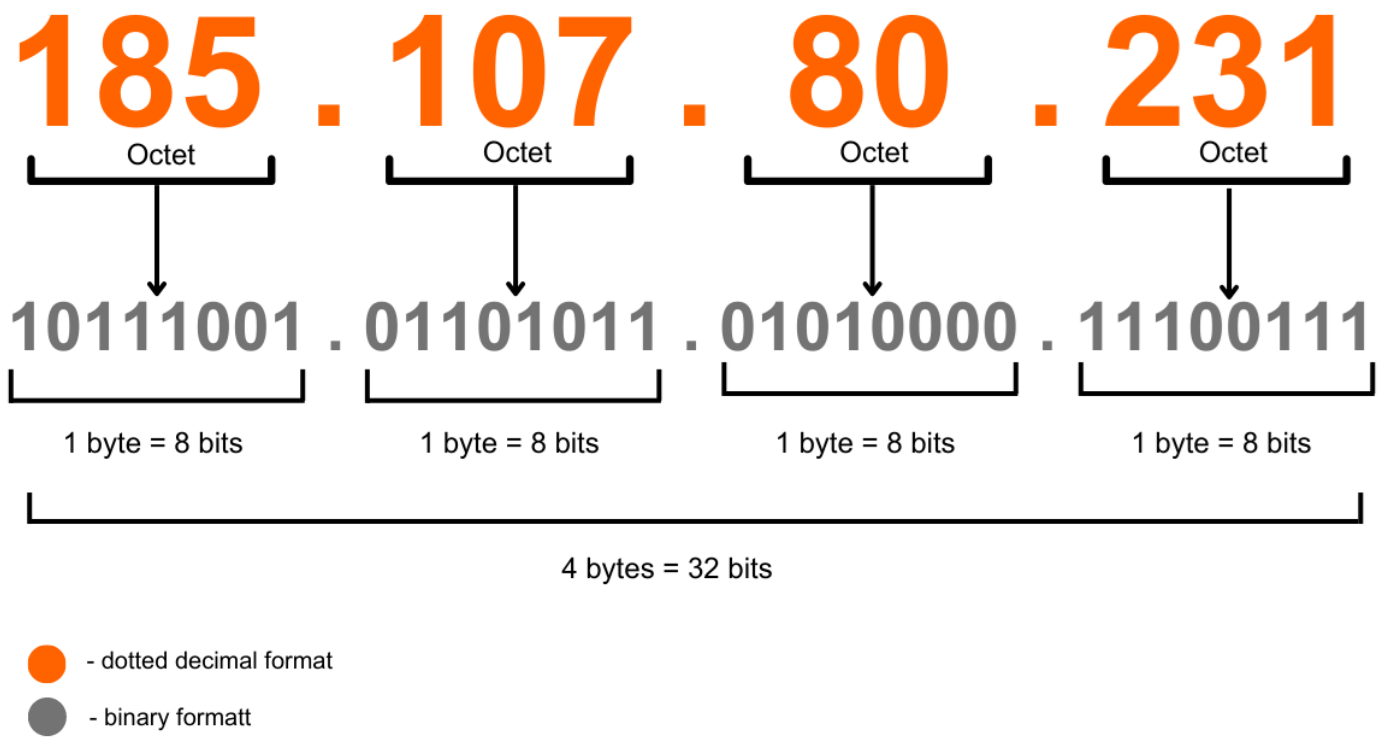
```
IPv4 Address: 192.168.0.1
Binary Format: 11000000.10101000.00000000.00000001
```

IPV4 ADDRESSES

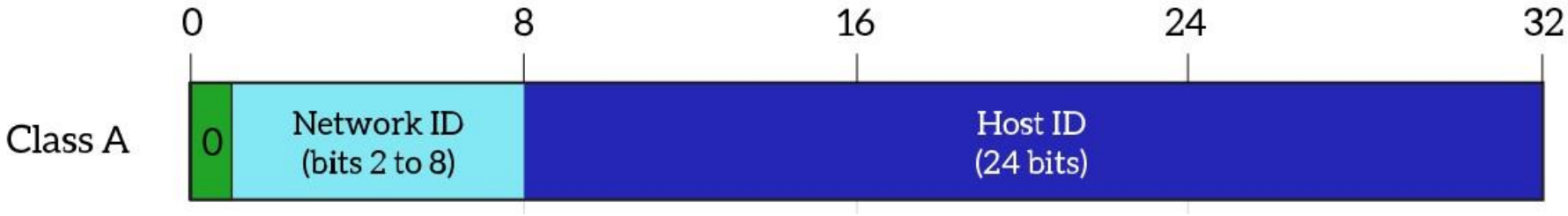


IP ADDRESS

- Internet Protocol Address.
- It is 32 Bits address.
- It's a logical address.
- IP must be unique & universal.
- 2 ways to display an IP address:
  - Binary Notation
  - Dotted-Decimal Notation

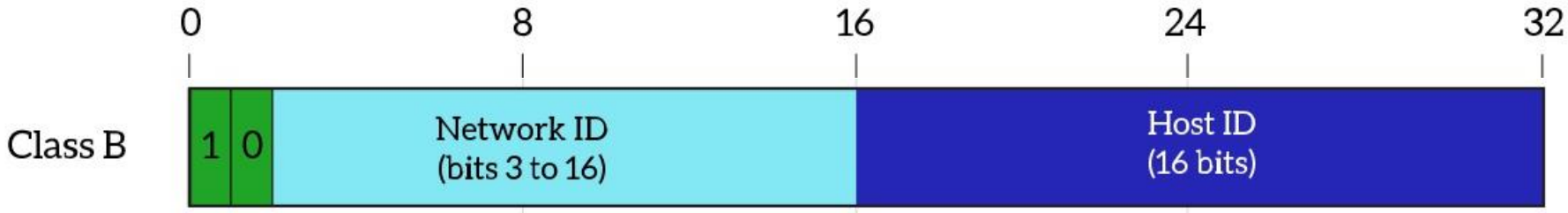


IP ADDRESS – CLASS "A"



- 1st Bit is reserved.
- Network ID = 8 bits
- Host ID = 24 bits
- 2 reserved IPs
  - 0.0.0.0 = Special purpose
  - 127.0.0.0 = Loopback address
- IP Range = 0 – 127
- Usage Networks IDs: $(2^7 - 2)$
- Total Hosts IDs: $(2^{24} - 2)$

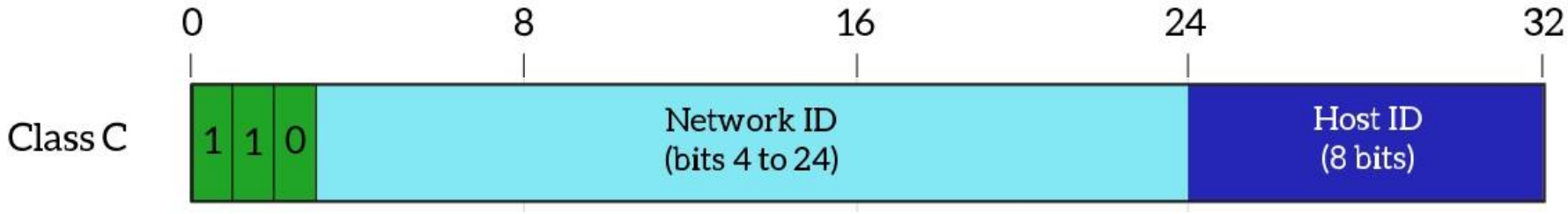
IP ADDRESS – CLASS "B"



- 1st 2 Bits (10) are reserved.
- Network ID = 16 bits
- Host ID = 16 bits
- 2 reserved bits
  - 1 = 1st bit
  - 0 = 2nd bit

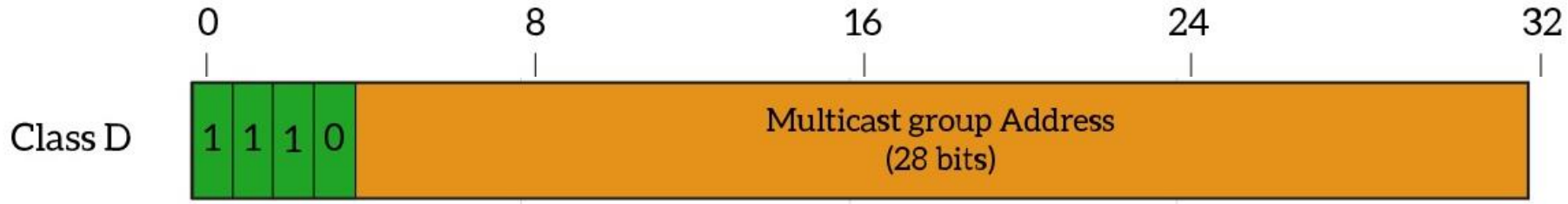
- IP Range = 128 - 191
- Usage Networks IDs: ($2^{16-2} = 2^{14} = 16{,}384$)
- Total Hosts IDs: ($2^{16} - 2 = 65{,}534$)

IP ADDRESS – CLASS "C"



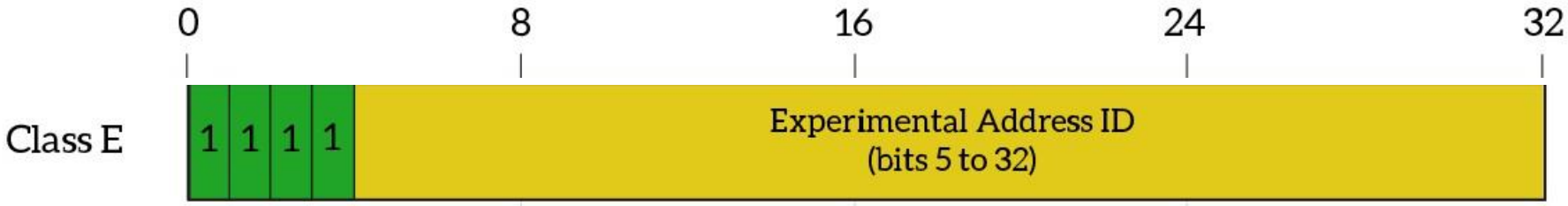
- 1st 3 Bits (110) are reserved.
- Network ID = 24 bits
- Host ID = 8 bits
- IP Range = 192 – 223
- Usage Networks IDs: ($2^{24-3} = 2^{21}$ = 20,97,152)
- Total Hosts IDs: ($2^{8} - 2$ = 254)

IP ADDRESS – CLASS "D"



- 1st 4 Bits (1110) are reserved.
- Used for multicasting
- IP Range = 224 – 239
- Class D IP addresses are reserved for multicasting.
- Class D IP addresses are reserved for multicasting

IP ADDRESS – CLASS "E"



- 1st 4 Bits (1111) are reserved.
- Reserved for experimental purposes by IETF (Internet Engineering Task Force).
- IP Range = 240 - 255
- These addresses are not allocated for use on the internet or any public networks..
- Class E addresses are not routable on the global internet

IPV6 ADDRESSES

- To address IPv4 limitations, IPv6 was introduced. IPv6 uses a 128-bit address format, which allows for an astronomically large number of unique addresses.
- Instead of the four-octet structure of IPv4, IPv6 addresses are written as eight groups of four hexadecimal digits separated by colons. This structure supports over 340 undecillion addresses.

```
IPv6 Address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

TYPES OF IP ADDRESSES: PUBLIC AND PRIVATE

- In addition to IPv4 and IPv6 differences, IP addresses are also classified as public or private:
  - Public IP Addresses are globally unique and accessible over the internet. They are assigned by the Internet Assigned Numbers Authority (IANA) and are used to identify devices on a wide-scale network, such as the internet.
  - Private IP Addresses are used within private networks (e.g., home or office networks). These addresses are not unique globally and are meant for devices within a single network to communicate without directly connecting to the internet.

ROLE OF IP ADDRESSES IN NETWORKING

- The IP address is vital for:
  1. Routing data between networks: Routers use IP addresses to forward packets to the correct destination.
  2. Identifying devices in a network: Each device on a network has a unique IP address, which is used to locate and communicate with other devices.
  3. Providing security and control: IP addresses allow network administrators to manage access, control routing, and set up security protocols.
- Each IP address consists of two parts:
  1. Network portion: Identifies the specific network.
  2. Host portion: Identifies the individual device within that network.

IP ADDRESS CLASSES (IPV4)

- Class A (1.0.0.0 to 126.0.0.0):
  - Supports large networks with millions of hosts.
  - Class A has a default mask of *255.0.0.0*
- Class B (128.0.0.0 to 191.255.0.0):
  - Designed for medium-sized networks.
  - Class B has a default mask of *255.255.0.0*
- Class C (192.0.0.0 to 223.255.255.0):
  - Ideal for small networks, supporting up to 254 hosts.
  - Class C has a default mask of *255.255.255.0*

PRIVATE IP ADDRESS RANGES

The private address ranges set by the Internet Engineering Task Force (IETF) for IPv4 are:

Class	Starting Address	Ending Address	Default Subnet Mask	Usage	Special Notes
A	0.0.0.0	127.255.255.255	255.0.0.0	Large networks	Includes `127.0.0.0/8` (reserved for loopback)
B	128.0.0.0	191.255.255.255	255.255.0.0	Medium-sized networks	N/A
C	192.0.0.0	223.255.255.255	255.255.255.0	Small networks	Commonly used for local area networks (LANs)
D	224.0.0.0	239.255.255.255	N/A	Multicasting	Used for sending data to multiple hosts simultaneously
E	240.0.0.0	255.255.255.255	N/A	Reserved for experimental purposes	Not used for general communication

IPV4 ADDRESS CLASSES

- Class A (1.0.0.0 to 126.0.0.0): Supports large networks with millions of hosts.
- Class B (128.0.0.0 to 191.255.0.0): Supports medium-sized networks.
- Class C (192.0.0.0 to 223.255.255.0): Ideal for small networks.
- Class D (224.0.0.0 to 239.255.255.255): Reserved for multicast.
- Class E (240.0.0.0 to 255.255.255.255): Reserved for experimental or research purposes.

IPV6 ADDRESS TYPES

- IPv6 addresses are also categorized by type, based on the intended application:
  - Unicast: Assigned to a single interface, allowing one-to-one communication.
  - Multicast: Intended for one-to-many communication.
  - Anycast: Assigned to multiple interfaces, with packets routed to the nearest device.
- IPv6 utilizes CIDR notation and prefixes to determine the address range:
  - Global Unicast Addresses: Range from 2000::/3, used for routing globally.
  - Link-Local Addresses: Range from fe80::/10, used within a single network segment.

UNICAST COMMUNICATION

- Unicast refers to one-to-one communication between a single sender and a single receiver.

  In unicast, data packets are sent from one device (source) to another specific device (destination), identified by a unique IP address.

- Example of Unicast in Networking:
  - When a user requests a webpage, the request and response between the client and the web server occur over a unicast channel. The server sends the requested content directly to the requesting client's IP address.

CHARACTERISTICS OF UNICAST

- One-to-One Communication: Only one sender and one receiver are involved.
- Direct Route: The data packet travels directly from source to destination, without involving other devices.
- Private and Personalized: The data transfer is intended only for the receiver, making it secure and private.
- Common in Client-Server Communication: Most internet traffic, such as web browsing, email, and file transfer, uses unicast communication.

MULTICAST COMMUNICATION

- Multicast is a form of communication where data packets are sent from one sender to multiple selected recipients.
- Unlike unicast, multicast allows for a one-to-many transmission without sending multiple copies of the same data.
- It's particularly useful in applications where data needs to reach multiple receivers but not the entire network.
- Example of Multicast in Networking:
  - Multicast is used in applications like IPTV (Internet Protocol Television) and video conferencing where one stream of data (like a live video feed) is transmitted to multiple recipients simultaneously.

CHARACTERISTICS OF MULTICAST:

- One-to-Many Transmission: Data is sent from one source to a selected group of devices.
- Efficient Use of Bandwidth: Only one copy of the data packet is sent, with routers replicating it as necessary to reach recipients in the multicast group.
- IP Multicast Addresses: Special IP addresses in the range of 224.0.0.0 to 239.255.255.255 are reserved for multicast traffic in IPv4, while IPv6 uses addresses starting with FF00::/8.

BROADCAST COMMUNICATION

- Broadcast is a method of data transmission where a message is sent from one sender to all devices on a network.
- In broadcast communication, data packets reach every connected device within a specific network or broadcast domain.
- This method is useful for sharing information that all devices in the network need, such as address resolution or network discovery.
- Example of Broadcast in Networking:
  - When a device needs to find the MAC address associated with an IP address, it sends an ARP request as a broadcast. All devices in the network receive the packet, but only the device with the matching IP address responds.

SUMMARY OF UNICAST, MULTICAST, AND BROADCAST

Transmission Type	Scope	IP Address Range	Use Case
Unicast	One-to-One	Specific IP address	Client-server interactions
Multicast	One-to-Many (group)	224.0.0.0 to 239.255.255.255	Streaming, conferencing
Broadcast	One-to-All	255.255.255.255 (IPv4)	Network discovery, ARP, DHCP

- Each data transmission method serves unique purposes:
  - Unicast for secure and direct communications.
  - Multicast for efficient data delivery to a group.
  - Broadcast for network-wide communication, often for discovery purposes.

RESERVED AND SPECIAL IP ADDRESS RANGES (IPV4)

- Private IP Ranges
  - Class A: 10.0.0.0 to 10.255.255.255
  - Class B: 172.16.0.0 to 172.31.255.255
  - Class C: 192.168.0.0 to 192.168.255.255
- Loopback Addresses (127.0.0.0 to 127.255.255.255) The loopback range is used for testing network interfaces on a local machine. 127.0.0.1 is commonly known as the "localhost" address, used to refer to the device itself.

RESERVED AND SPECIAL IP ADDRESS RANGES (IPV4)

- Link-Local Addresses (169.254.0.0 to 169.254.255.255) These addresses are automatically assigned when a device cannot obtain an IP from a DHCP server. Link-local addresses enable basic, limited communication within a local network.
- Multicast Addresses (224.0.0.0 to 239.255.255.255) Reserved for multicast groups, these addresses allow data to be sent to multiple recipients simultaneously.
- Broadcast Address (255.255.255.255) The broadcast address is used to send data to all devices on a network. For example, sending a packet to 255.255.255.255 reaches all devices within the network.

RESERVED AND SPECIAL IP ADDRESS RANGES (IPV6)

- IPv6 also reserves certain address ranges for specific purposes:
  - Link-Local Addresses (fe80::/10) Similar to IPv4 link-local addresses, IPv6 link-local addresses allow devices to communicate on the same local link without requiring a globally routable IP.
  - Multicast Addresses (ff00::/8) Multicast addresses in IPv6 are used for one-to-many communication, similar to IPv4's multicast function.
  - Loopback Address (::1) IPv6's loopback address, ::1, functions like IPv4's 127.0.0.1, allowing a device to test its own networking configuration.

CIDR (CLASSLESS INTER-DOMAIN ROUTING)

- CIDR is a method for more flexible IP address allocation and efficient routing.
- It came as a replacement for the *class-based IP addressing system* (Classes A, B, C).
- CIDR allows for subnetting and aggregation of IP addresses, making it crucial for efficient network management and mitigating IPv4 address exhaustion.
- CIDR addresses use variable-length subnet masking (VLSM), which allows network administrators to define IP addresses with varying subnet sizes, ensuring that IP addresses are allocated according to an organization's specific needs.

THE STRUCTURE OF CIDR NOTATION

- CIDR notation consists of an IP address followed by a slash (/) and a number that specifies the length of the network prefix.
- For example:
  - 192.168.1.0/24 means that the first 24 bits of the IP address are the network portion, and the remaining bits are available for host addresses.
  - 10.0.0.0/8 indicates that the first 8 bits are used for the network, allowing for a large range of host addresses within that network.

BENEFITS OF CIDR

- Efficient Use of IP Addresses: CIDR allows for custom subnet sizes, ensuring that IP addresses are assigned based on need.
- Reduced Routing Complexity: Aggregating IP addresses into supernets minimizes routing table entries, improving routing efficiency.
- Flexibility in Network Design: Networks can be structured to match organizational requirements without the constraints of traditional IP classes.
- Support for IPv6: CIDR seamlessly integrates with IPv6, providing a robust method for handling extensive address spaces.

COMMON CIDR NOTATIONS AND THEIR SUBNET SIZES

CIDR Notation	Subnet Mask	Total Addresses	Usable Addresses
/8	255.0.0.0	16,777,216	16,777,214
/16	255.255.0.0	65,536	65,534
/24	255.255.255.0	256	254
/26	255.255.255.192	64	62
/30	255.255.255.252	4	2

NETWORK ADDRESS

- The network address identifies a specific network or subnet within a larger network.
- It is the first IP address in any subnet and represents the network itself, not any individual device.
- The network address is often used by routers and other devices to recognize the starting point of a subnet, allowing them to route data correctly.
- Key Points about Network Address:
  - Indicates Network/Subnet: It identifies the network, not any host within it.
  - Cannot Be Assigned to Devices: The network address is reserved and not assigned to devices as it represents the subnet.
  - Calculation: In binary, the host portion of a network address is all 0s.

EXAMPLE OF NETWORK ADDRESS CALCULATION:

For the IP address 192.168.1.0/24:

- Convert to Binary: 192.168.1.0 in binary is 11000000.10101000.00000001.00000000.
- Subnet Mask in /24 Notation: 255.255.255.0, which translates to 11111111.11111111.11111111.00000000.
- Resulting Network Address: The network address is 192.168.1.0, and it represents the entire network of all devices connected to it.

BROADCAST ADDRESS

- The broadcast address is the last IP address in a subnet and is used to send data to all devices within that subnet.
- Any message sent to the broadcast address reaches every device in the subnet, making it useful for network-wide communications, such as ARP (Address Resolution Protocol) and DHCP (Dynamic Host Configuration Protocol) requests.
- Key Points about Broadcast Address:
  - One per Subnet: The broadcast address is unique to each subnet.
  - Reserved for Network-Wide Communications: Devices should not be assigned this address, as it is for broadcasting to all devices in the subnet.
  - Calculation: In binary, the host portion of the broadcast address is all 1s.

EXAMPLE OF BROADCAST ADDRESS CALCULATION:

Using the same network 192.168.1.0/24:

- Convert to Binary: 192.168.1.0 is 11000000.10101000.00000001.00000000.
- Host Portion as 1s: Changing the last 8 bits to 1s gives 11000000.10101000.00000001.11111111.
- Broadcast Address: Converting back to decimal, the broadcast address is 192.168.1.255.

VALID HOST ADDRESSES

- Valid host addresses are the IP addresses that can be assigned to devices within a subnet.
- These addresses fall between the network and broadcast addresses and can be allocated to individual hosts, such as computers, printers, and other devices.
- Key Points about Valid Host Addresses:
  - Range Between Network and Broadcast Addresses: Valid host IP addresses are those between the network and broadcast addresses.
  - Assignable to Devices: Any address between the network and broadcast address is assignable.
  - Number of Hosts Calculation: The number of valid hosts in a subnet is determined by the subnet mask, calculated as 2^N - 2, where N is the number of host bits.

EXAMPLE OF VALID HOST ADDRESS RANGE:

Using 192.168.1.0/24:

- Subnet Range: 192.168.1.0 to 192.168.1.255.
- Valid Hosts: From 192.168.1.1 to 192.168.1.254.
- Host Count: With 8 bits for hosts, 2^8 - 2 = 254 valid hosts.

WHAT IS A PUBLIC IP ADDRESS?

- A public IP address is a globally unique IP address assigned to devices for communication over the internet.
- These addresses are accessible from anywhere on the internet, meaning devices with public IPs can send and receive data from other public IP addresses worldwide.
- Public IP addresses are issued by Internet Service Providers (ISPs) and are required for devices that need direct, unrestricted internet access, such as web servers or routers in home networks.

CHARACTERISTICS OF PUBLIC IP ADDRESSES:

- Globally Unique: Each public IP address is unique across the internet, ensuring that data can reach the correct destination globally.
- Internet-Routable: Devices with public IPs can be reached from other devices over the internet.
- Assigned by ISPs: ISPs control and assign public IPs to customers, often with additional costs associated with static public IPs.

EXAMPLES OF PUBLIC IP USAGE:

- Web Servers: Websites, email servers, and cloud services use public IP addresses, allowing users worldwide to connect.
- Routers in Home Networks: Routers often have a public IP on their internet-facing side, enabling them to connect to the wider internet.

WHAT IS A PRIVATE IP ADDRESS?

- Private IP addresses are reserved for local network use only.
- They are not accessible from the public internet and are used within private networks like home, office, and corporate networks.
- Devices with private IP addresses can communicate with each other within the same network, but they cannot directly interact with devices on the internet without using a router or a Network Address Translation (NAT) service.

CHARACTERISTICS OF PRIVATE IP ADDRESSES:

- Local Use Only: Private IPs are meant for communication within a single network and are not routed on the internet.
- Reuse Across Networks: Private IP ranges are reserved, allowing them to be reused in multiple networks without conflict, as they do not interact directly with public IPs.
- NAT Required for Internet Access: For devices with private IPs to access the internet, routers use NAT to translate private IPs to a public IP.

PRIVATE IP ADDRESS RANGES:

The IPv4 private address ranges, as specified by the Internet Assigned Numbers Authority (IANA), are:

- Class A: 10.0.0.0 to 10.255.255.255
- Class B: 172.16.0.0 to 172.31.255.255
- Class C: 192.168.0.0 to 192.168.255.255

EXAMPLES OF PRIVATE IP USAGE:

- Home Networks: Devices such as computers, smartphones, and printers in a home network often use private IP addresses.
- Corporate Networks: In offices, private IPs are assigned to employees' devices, allowing for internal communication and security.

PUBLIC VS PRIVATE IP ADDRESSES

Feature	Public IP Address	Private IP Address
Scope	Global (internet-wide)	Local (restricted to a private network)
Uniqueness	Unique across the internet	Reusable within multiple networks
Assignment	Managed by ISPs	Assigned within a network by routers/DHCP
NAT Requirement	Not needed	Needed for internet access
Example	`8.8.8.8` (Google DNS)	`192.168.1.1` (local router IP)

NETWORK ADDRESS TRANSLATION (NAT)

- NAT is a technology that enables devices with private IPs to communicate over the internet by translating private IP addresses to a public IP address.
- Routers use NAT to map multiple private IP addresses to a single public IP, which conserves IP addresses and allows entire networks to share a single public IP for internet access.
- Types of NAT:
  - Static NAT: Maps a single private IP to a single public IP, often used for hosting services.
  - Dynamic NAT: Maps private IPs to a pool of public IPs dynamically.
  - Port Address Translation (PAT): Maps multiple private IPs to a single public IP using different ports, commonly used in home networks.

OVERVIEW OF IP ADDRESS CLASSES

Class	Range of First Octet	Default Subnet Mask	Number of Networks	Number of Hosts per Network	Usage
A	0 – 127	255.0.0.0	128	16,777,214	Large networks
B	128 – 191	255.255.0.0	16,384	65,534	Medium-sized networks
C	192 – 223	255.255.255.0	2,097,152	254	Small networks
D	224 – 239	Not applicable	Not applicable	Not applicable	Multicasting
E	240 – 255	Not applicable	Not applicable	Not applicable	Experimental and reserved

CLASS A IP ADDRESSES

- Class A addresses are designed for very large networks with millions of devices, such as multinational corporations, universities, and government agencies. Only the first octet represents the network portion, with the remaining three octets allocated to hosts.
  - Range: 0.0.0.0 to 127.255.255.255
  - Default Subnet Mask: 255.0.0.0
  - Network/Host Allocation: The first octet represents the network, while the remaining three octets are used for hosts.
  - Hosts per Network: Over 16 million addresses per network.
  - Example: 10.0.0.0 is a Class A network address, commonly used in private networks.
- Notable Feature:
  - The first bit in Class A addresses is always 0.
  - The IP address 127.x.x.x is reserved for loopback purposes, used for testing and diagnosing the local device.

CLASS B IP ADDRESSES

- Class B addresses are used by medium-sized networks, such as universities, large business networks, and sizable internet service providers. Class B splits the IP address into two octets for the network and two for the host.
  - Range: 128.0.0.0 to 191.255.255.255
  - Default Subnet Mask: 255.255.0.0
  - Network/Host Allocation: The first two octets represent the network portion, while the last two octets are allocated for hosts.
  - Hosts per Network: Around 65,000 hosts per network.
  - Example: 172.16.0.0 is a Class B address range, often used in private networks.
- Notable Feature:
  - The first two bits in Class B addresses are always 10.
  - Class B strikes a balance between network and host capacities, suitable for organizations that require a medium range of IP addresses.

CLASS C IP ADDRESSES

- Class C addresses are the most commonly used for small to medium-sized networks, such as small business networks or office LANs. Class C addresses allocate three octets for the network portion and only one for the host.
  - Range: 192.0.0.0 to 223.255.255.255
  - Default Subnet Mask: 255.255.255.0
  - Network/Host Allocation: The first three octets represent the network, and the last octet is for the host.
  - Hosts per Network: A maximum of 254 hosts per network.
  - Example: 192.168.1.0 is a Class C address often used for internal networks and home routers.
- Notable Feature:
  - The first three bits in Class C addresses are always 110.
  - Class C offers a large number of networks but a smaller number of hosts, making it ideal for smaller networks that don't require many devices.

CLASS D IP ADDRESSES (MULTICAST)

- Class D is reserved for multicasting. Unlike other IP classes, Class D addresses are not used for conventional device-to-device communication or for identifying unique hosts or networks. Instead, they are designed to send data to multiple devices simultaneously.
  - Range: 224.0.0.0 to 239.255.255.255
  - Default Subnet Mask: Not applicable (does not define a network/host structure).
  - Network/Host Allocation: Class D does not differentiate between network and host portions.
  - Usage: Multicasting, where one source can communicate with multiple recipients.
  - Example: 224.0.0.0 to 224.0.0.255 is reserved for local network multicast.
- Notable Feature:
  - The first four bits in Class D addresses are always 1110.
  - Common applications include video conferencing and streaming where data needs to be distributed to multiple users at once.

CLASS E IP ADDRESSES (EXPERIMENTAL)

- Class E addresses are reserved for experimental use and are not allocated for standard IP address allocation. This class is often used for testing new protocols and research.
  - Range: 240.0.0.0 to 255.255.255.255
  - Default Subnet Mask: Not applicable.
  - Network/Host Allocation: Class E does not differentiate between network and host portions.
  - Usage: Reserved for future use or experimental purposes; not assignable for general network use.
  - Example: Addresses in the range 240.0.0.0 to 255.255.255.254 are part of Class E.
- Notable Feature:
  - The first four bits in Class E addresses are always 1111.
  - Class E is generally unused in the public internet and private networks.

CLASSFUL VS. CLASSLESS ADDRESSING

- Classful Addressing: IP classes (A, B, and C) are considered classful as they follow predefined boundaries based on the first few bits of the address. While they simplify network design, they also limit flexibility and can lead to inefficient IP usage, as each class has a fixed number of hosts and network allocation.
- Classless Inter-Domain Routing (CIDR): CIDR was introduced to address the limitations of classful addressing. It allows networks to be defined by the subnet mask instead of the class, which conserves IP addresses by allocating them based on network needs rather than rigid class boundaries.

SUPERNETTING

- Supernetting is a technique used in computer networks to combine multiple smaller subnets (networks) into a larger address block.
- It is the inverse/opposite of subnetting.
- This approach simplifies routing and conserves address space, especially in scenarios where contiguous IP address blocks are available.

PURPOSE OF SUPERNETTING

- Reduce Routing Table Size: By aggregating several routes into a single entry, supernetting reduces the size of routing tables, improving router efficiency.
- Simplify Network Management: Fewer routes mean less administrative overhead.
- Optimize Address Allocation: Enables efficient use of IP address space.
- Support CIDR (Classless Inter-Domain Routing): Works with CIDR to allow flexible subnet masks instead of fixed class-based subnetting.