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.

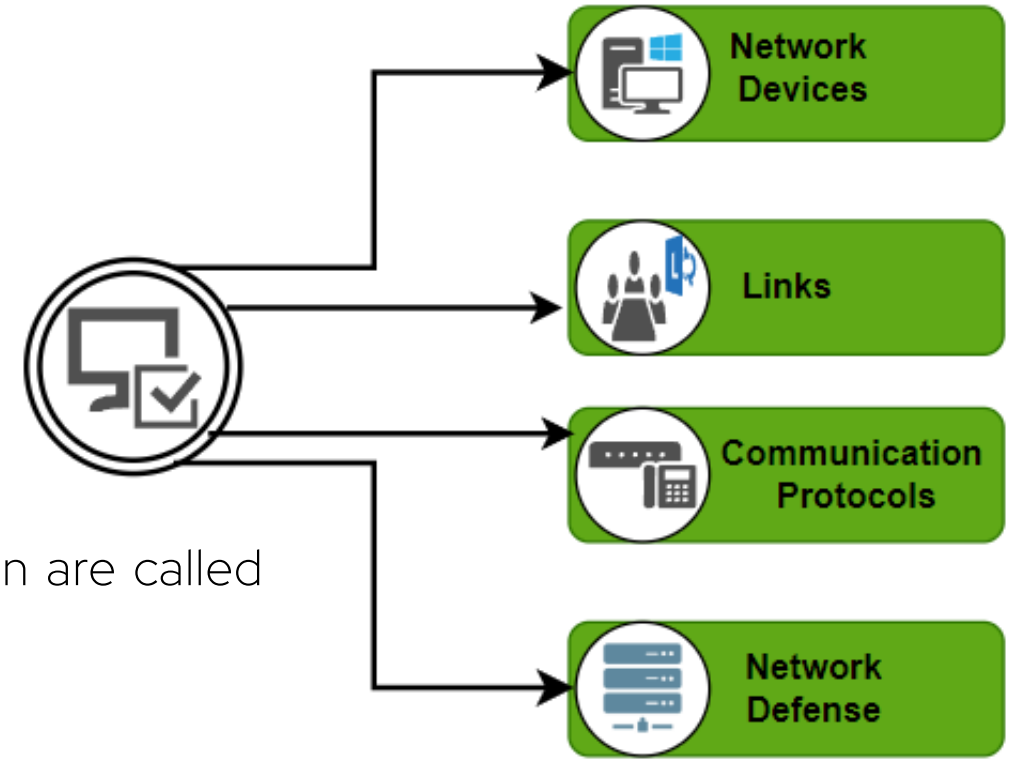
WHAT DO COMPUTER NETWORKS DO?

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

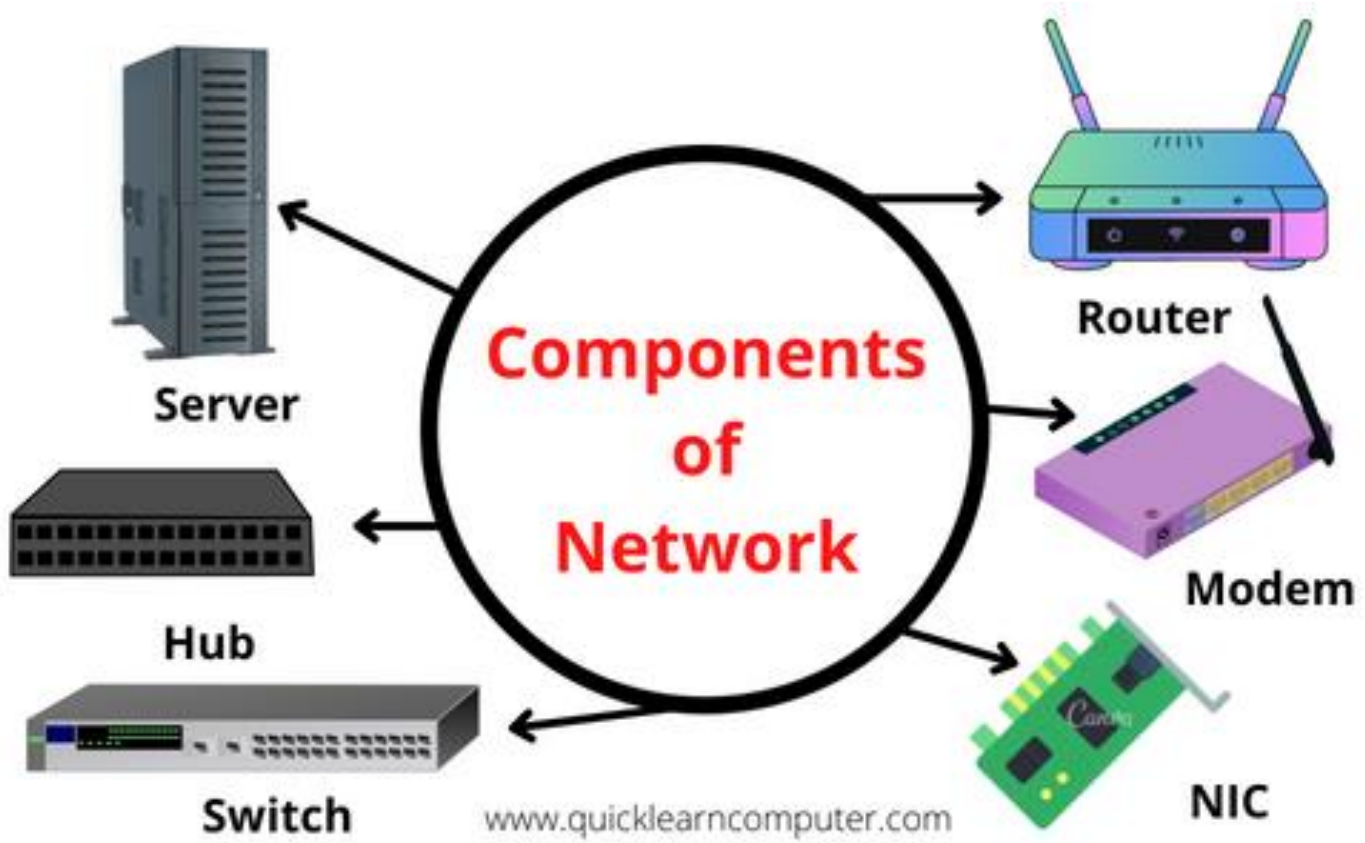
- Computer Networks help in operating virtually
- Computer Networks integrate on a large scale
- Computer Networks respond very quickly in case of conditions change
- Computer Networks help in providing data security

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

Types of NICs include the following:

- 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

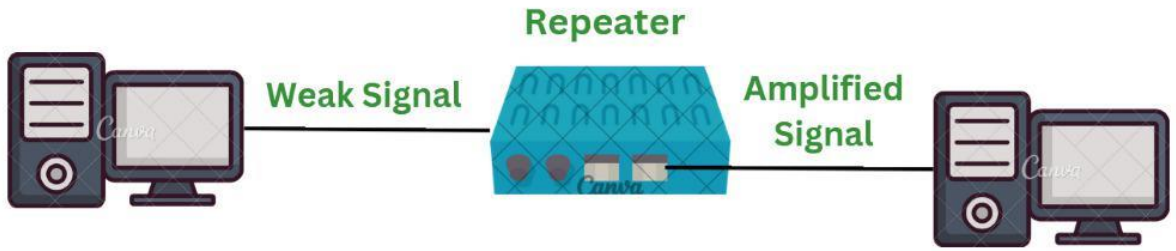
- Speed. All NICs have a speed rating in terms of megabits per second (Mbps) that determines the card's performance in a network. The average Ethernet NICs come in
  - 10 Mbps,
  - 100 Mbps,
  - 1000 Mbps and
  - 1 gigabits per second varieties.
- Driver. The required software that passes data between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

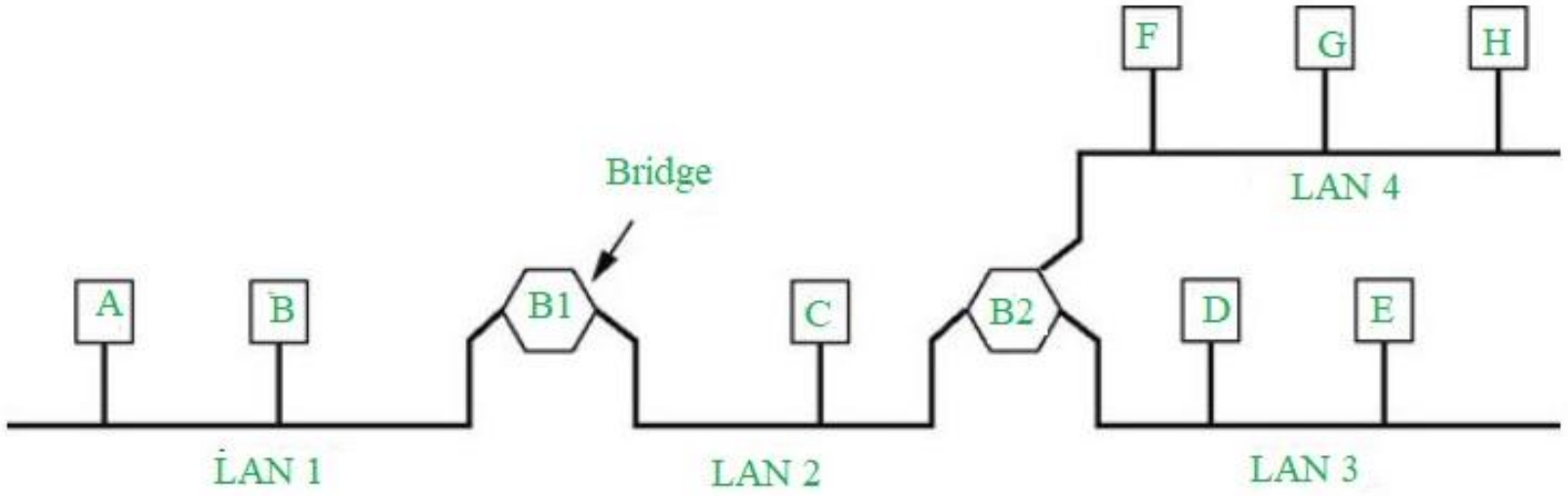
- It is less expensive.
- It does not impact network performance.
- Hub support different network media

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.

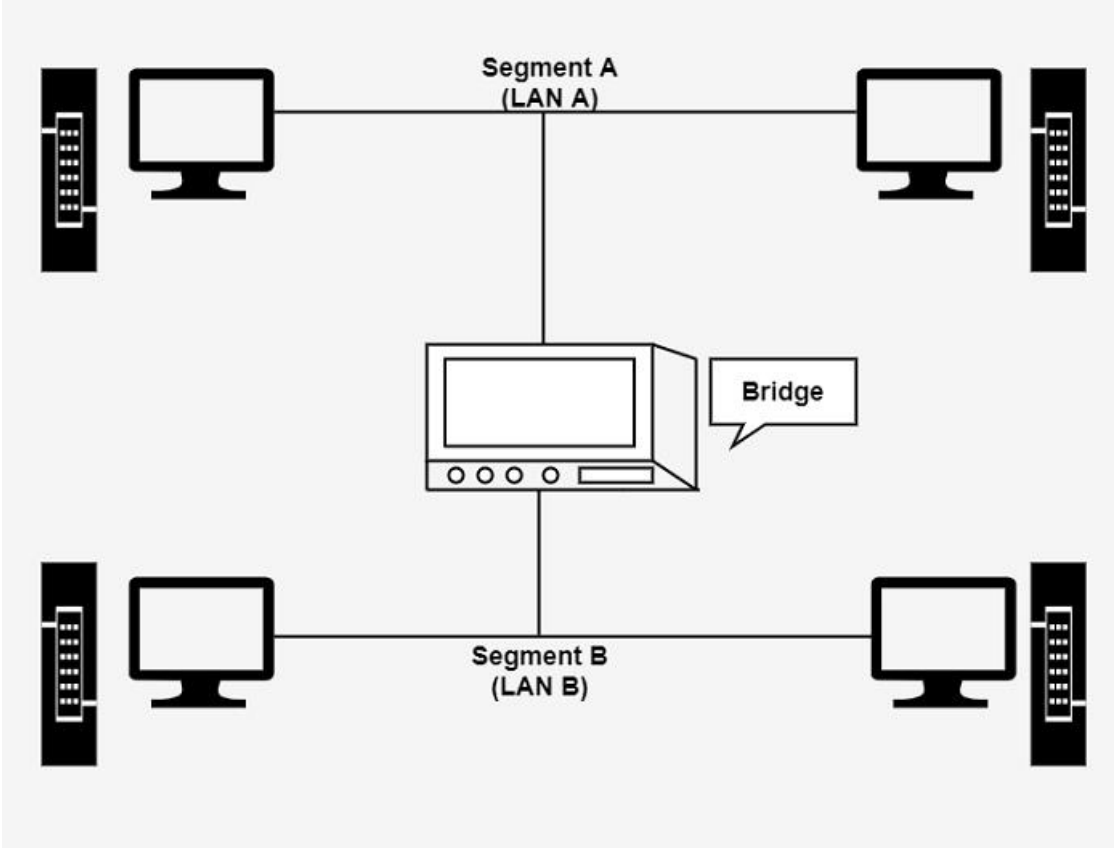
BRIDGES

- 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.

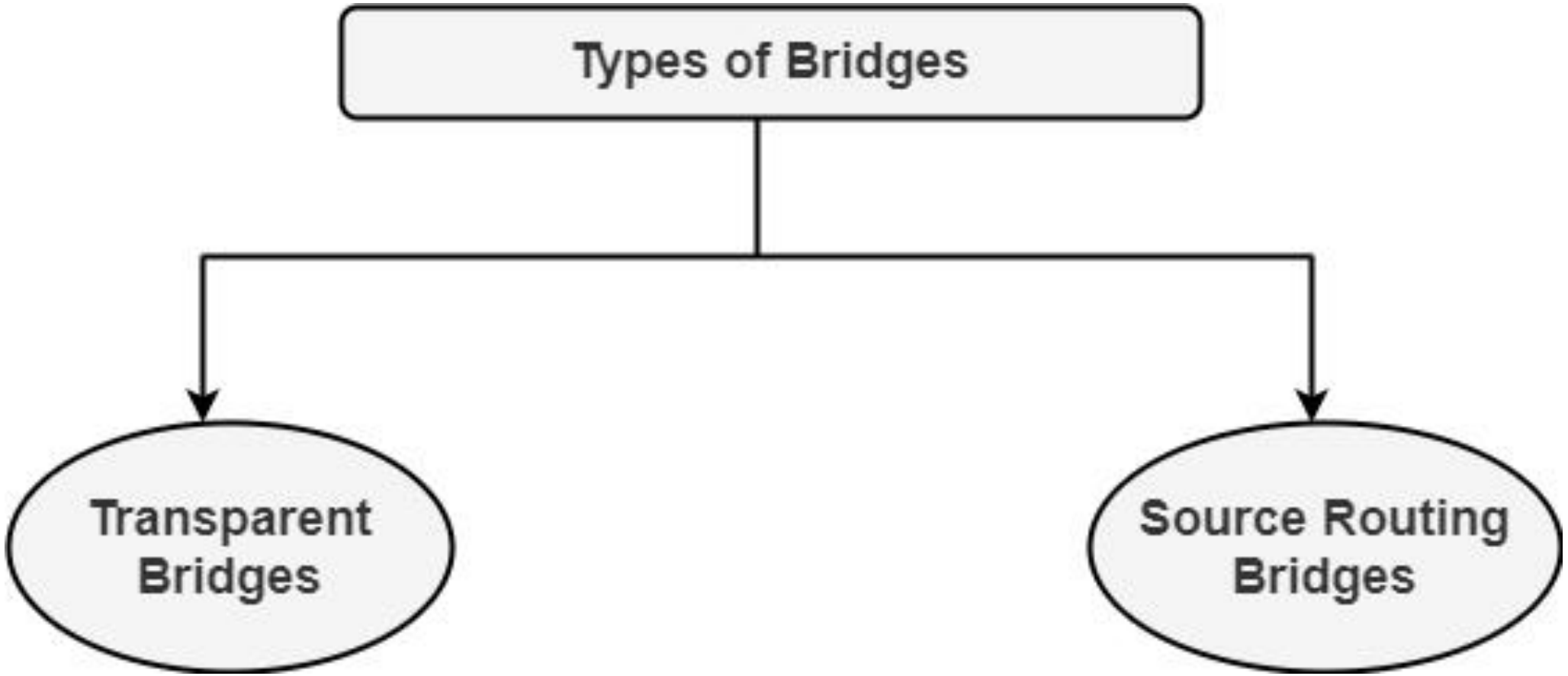


WORKING OF BRIDGES

- 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

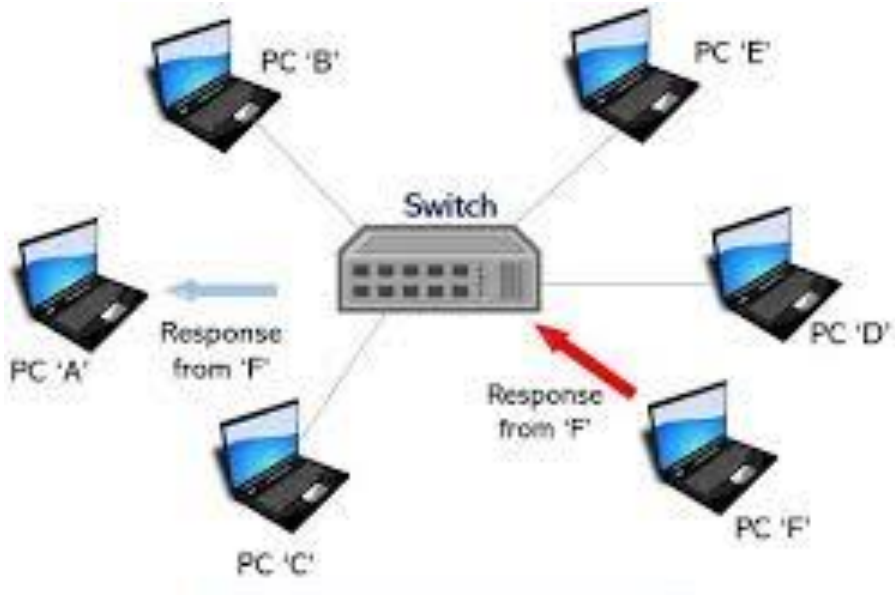
- Source Routing Bridge
  - This sending terminal means the bridges that the frames should stay.
  - This type of bridge is used to prevent looping problem.

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.



- It uses Unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all) transmission modes.
- 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

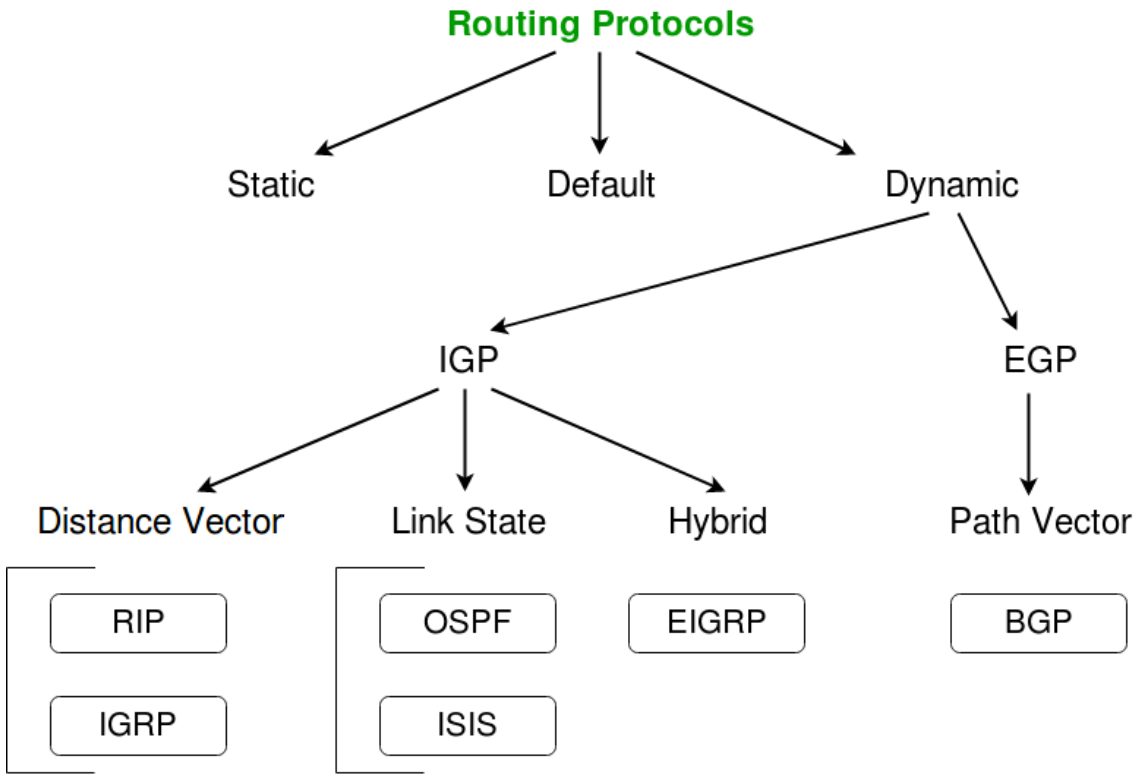
- Easier Connection
- Security
- NAT Usage
- Support Dynamic Routing
- Filtering of packets

Disadvantages

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

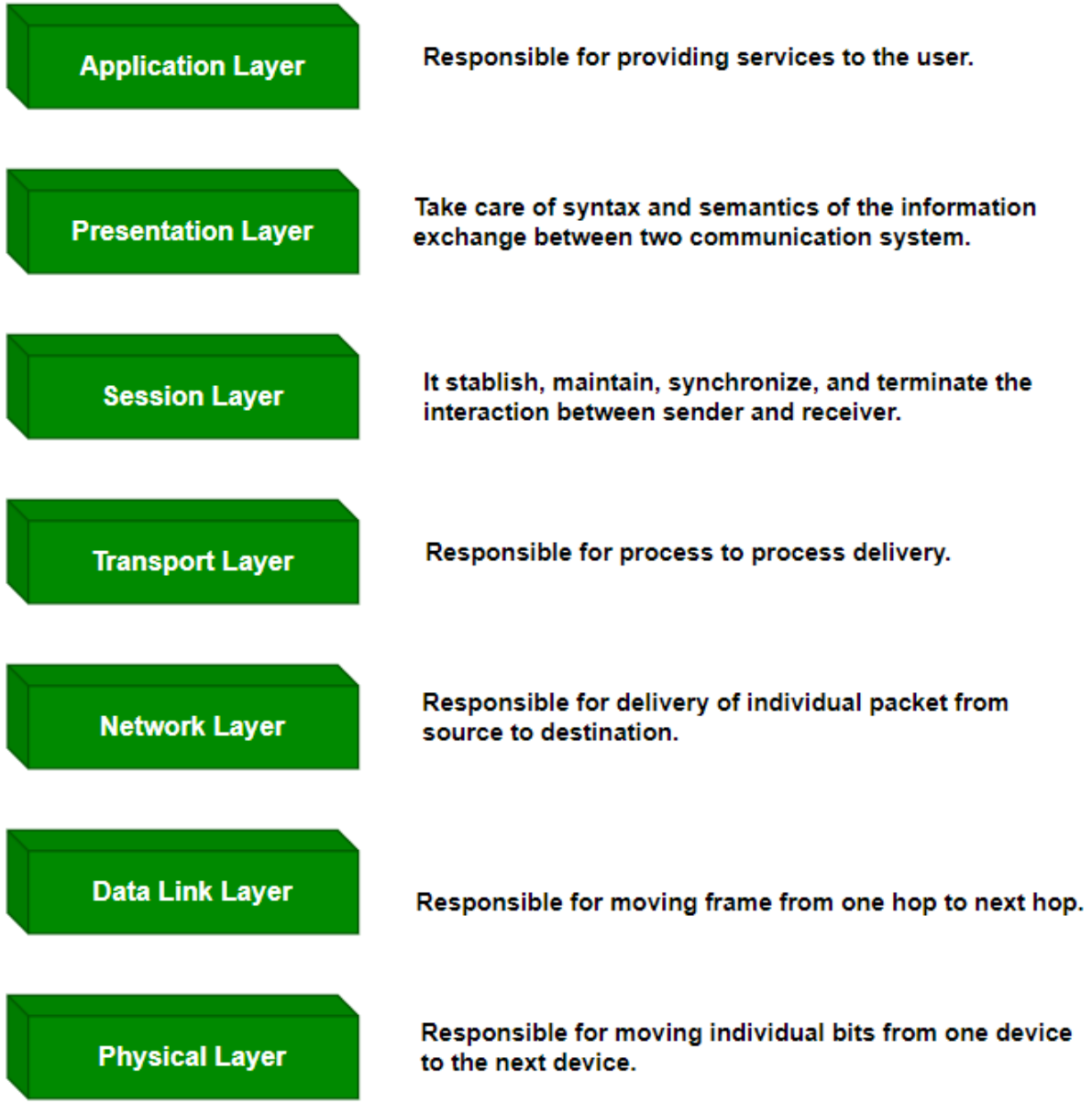
ROUTING PROTOCOL

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



OSI LAYERS

- The OSI model is a reference framework that explains the process of transmitting data between computers. It is divided into seven layers that work together to carry out specialized network functions, allowing for a more systematic approach to networking.



OSI LAYERS

- Application Layer: Applications create the data.
- Presentation Layer: Data is formatted and encrypted.
- Session Layer: Connections are established and managed.
- Transport Layer: Data is broken into segments for reliable delivery.
- Network Layer: Segments are packaged into packets and routed.
- Data Link Layer: Packets are framed and sent to the next device.
- Physical Layer: Frames are converted into bits and transmitted physically.