SINCE 1983

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

MIT-WPU
॥ विश्वशान्तिर्धुवं ध्रुवा ॥

Supported by
UNESCO
UNESCO Chair for
Human Rights, Democracy, Peace & Tolerance
World Peace Centre (Alandi) Pune, India

Chapter No. 2
Network Topologies and Networking Devices

Course Outcome

❖

Setup a computer network for specific requirement.

Content

➢ **Network Topologies –** Introduction, Definition, Selection Criteria. Type of Topology – Bus Topology, Ring Topology, Star Topology, Mesh Topology, Tree Topology, Hybrid Topology.

➢ **Network Control / Connecting Devices** -Need of Network Control Devices, Role of Network Control devices in a Network.

➢ **Network Connecting Devices:-** Passive & Active Hubs, Switches, Routers, Bridges, Repeaters, Gateways, Modems, wireless infrastructure components, Network Security Devices (firewalls , Proxy Server)
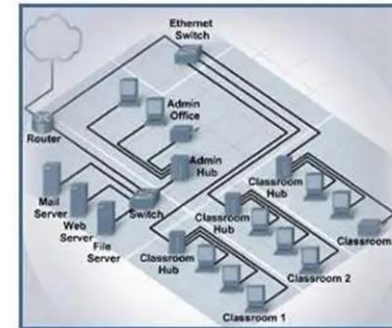
What is Network Topology?

- Geographical representation of the links.

- Topology is physical **layout** of **computers, cables and other connected devices** on a network.

- Topology defines the structure of the network of how all the components are interconnected to each other.

- Types

  1. **Physical Topology**
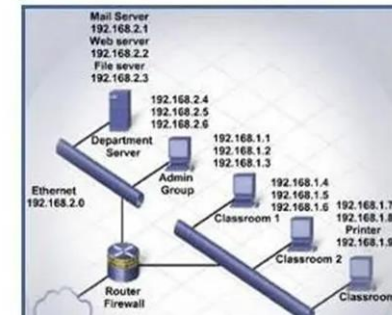
  2. **Logical Topology**

1. **Physical Topology**
- Actual layout of the computer cables and other network devices.
- It refers to the placement of the various network's components, including device location and cable installation

2. **Logical Topology**

- The way in which the network appears to the devices that use it.
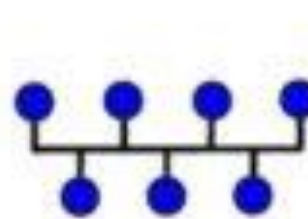- It shows how data flows within a network, regardless of its physical design.

Physical topology is the physical layout of the components on the network.

Logical topology determines how the hosts access the medium to communicate across the network.
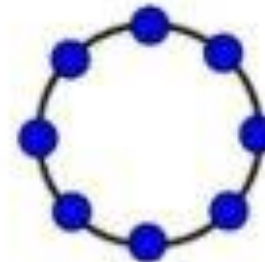
Selection Criteria

- **Size (no of node) of the system.**

- **Cost of the components and service required.**

- **Management of network.**

- **Architecture of network.**

- **Cable type.**

- **Expandability of the network.**

- **The desired performance.**

- **Reliability.**
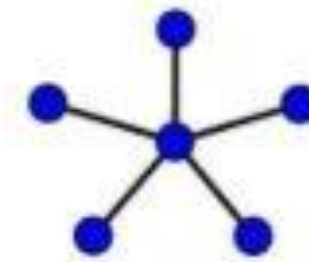
Types of Network Topology

SINCE 1983

Dr. Vishwanath Karad
MIT WORLD PEACE
UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

MIT-WPU

Supported by
UNESCO
UNESCO Chair for
Human Rights, Democracy, Peace & Tolerance
World Peace Centre (Alandi) Pune, India

❖Bus Topology
❖Star Topology
❖Ring Topology
❖Mesh Topology
❖Tree Topology
❖Hybrid Topology
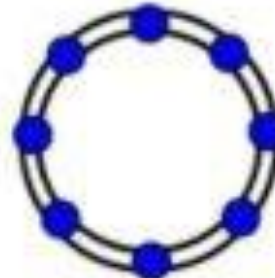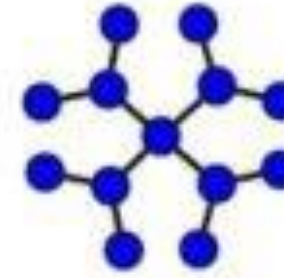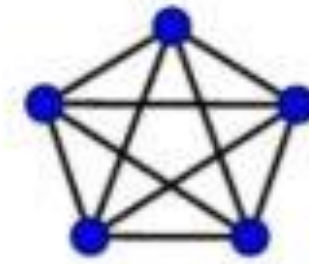
1. Bus Topology- Also Called as linear topology

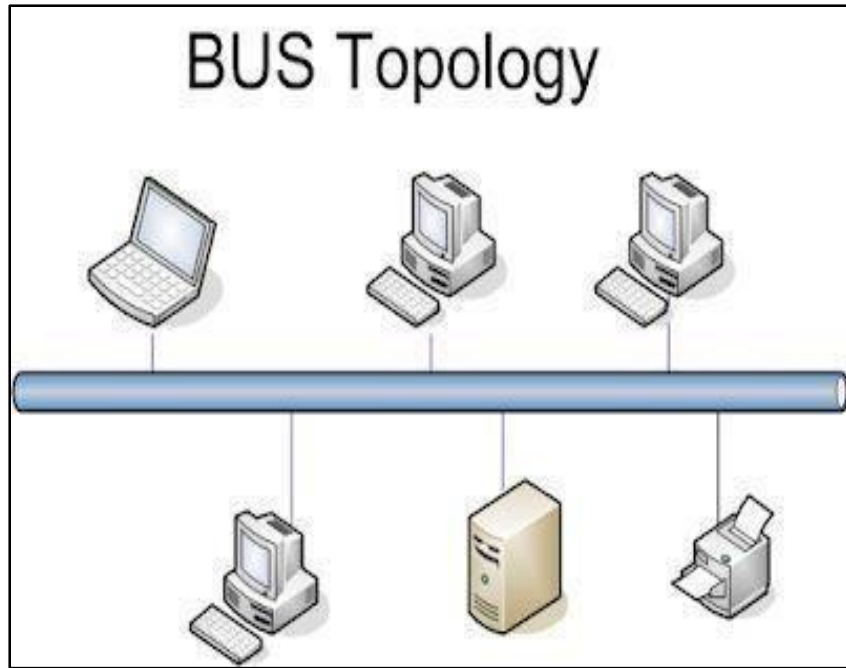**BUS Topology**

This allows only one device to transmit at a time.

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.

- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.

- When a node wants to send a message over the network, it puts a message over the network.

- All the stations available in the network will receive the message whether it has been addressed or not.

- If a device want to communicate with other device on the n/w, sends a **broadcast message** onto the wire all other devices receive the message.

- But only the intended devices accepts and process the message.

- Bus is passive topology.

- **Advantages:**

1. Ease of installation
2. Less cabling
3. Suitable for temporary and small networks.
4. Moderate data speeds: Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.

Application:
- Most computer motherboard.

- **Disadvantages:**

1. Difficult to add new devices.
2. If any fault in backbone can stops all transmission.
3. Only one computer can transmit at a time.
4. Limited cable length and number of stations.
5. Difficult to identify the problem if the entire network shuts down
6. It is slow when more devices are added into the network
7. If a main cable is damaged then network will fail or be split into two networks

2. Ring Topology

Computer

Flow of message

Computer

Computer

Computer
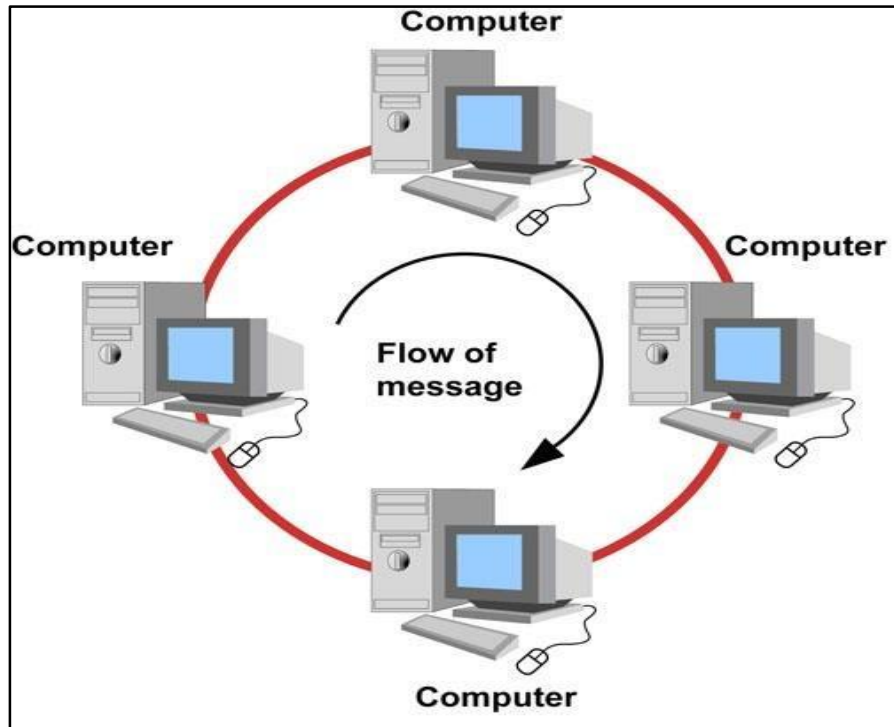
- Each packet is sent around the ring until it reaches its final destination.

- In Ring topology each node is connected to the two nearest nodes so the **entire network forms a circle**.

- The signal is passed in **one direction** from one device to another device until it reaches the destination.

- The data flows in a single loop continuously known as an endless loop.

Single Ring

Double Ring
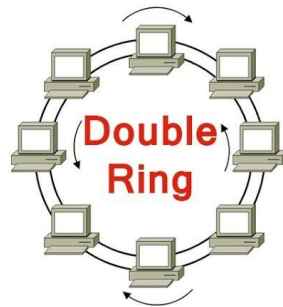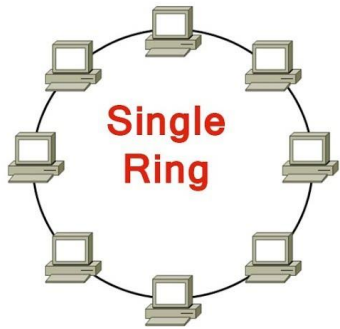
RING TOPOLOGY

- It has no terminated ends, i.e., each node is connected to other node and having no termination point.

- The data in a ring topology flow in a clockwise direction.

- Ring is the **Active Network**, because each computer retransmits what is receives from previous computer.

Working of Token passing:

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.

- The sender modifies the token by putting the address along with the data.

- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.

- In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.

- **Product availability:** Many hardware and software tools for network operation and monitoring are available.

- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.

- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.

- **Failure:** The breakdown in one station leads to the failure of the overall network.

- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.

- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Application

- Ring topologies are found in some office buildings or school campuses.

- Today high speed LANs made this topology **less popular.**

3. Star Topology
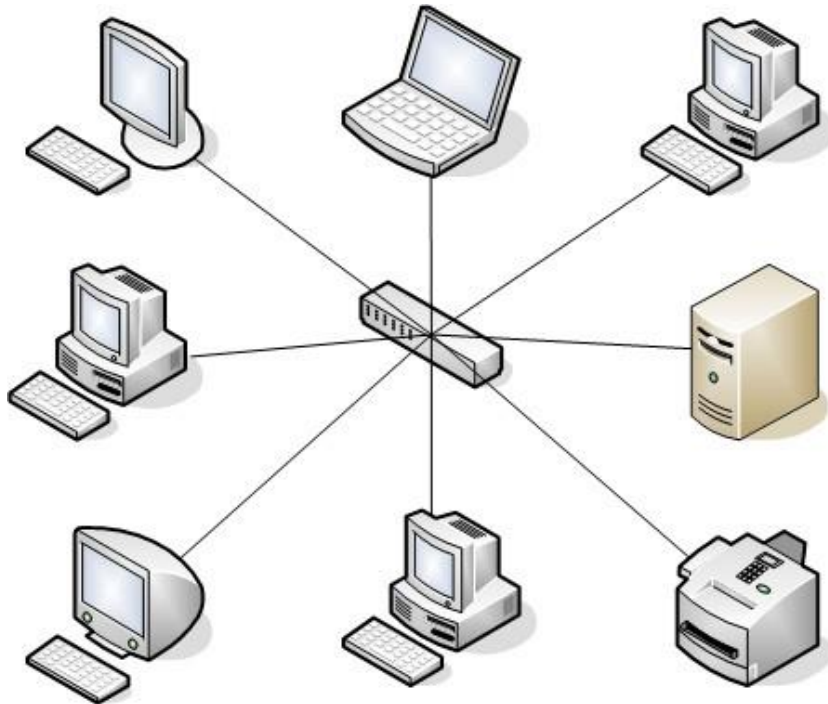
- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.

- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.

- Coaxial cable or RJ-45 cables are used to connect the computers.

- Hubs or Switches are mainly used as connection devices in a **physical star topology**.

- Star topology is the most popular topology in network implementation.

- **Advantages:**
- Easy to install and implement with wiring etc.

- Easy to troubleshoot and detect problems in the network.

- If one device fails, it does not affect the other devices in the network.

- You can easily add or remove devices without affecting the rest of the network.

- Centralized management and monitoring through the central switch/hub.

- **Disadvantages:**
- The main disadvantage of using this topology is that it has a single point of failure, i.e. when the central switch node is down, there will be a break in communication for all connected devices.

- More cabling is needed since you connect each individual devices to the central node.

- Performance of the whole network depends on the performance of the central node.

Application

- Star topology used in Local Area Networks (LANs).

- High speed LAN often use STAR.

Star Topology
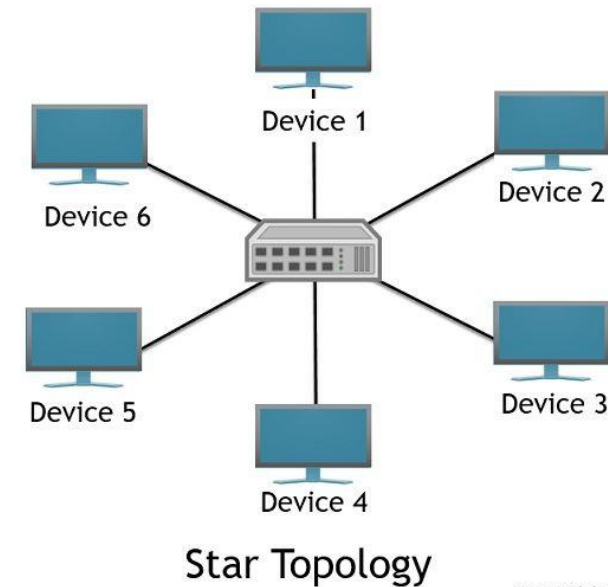
Circuit Globe

4. Mesh Topology

Computer

Computer

Computer

Computer

Computer

Computer
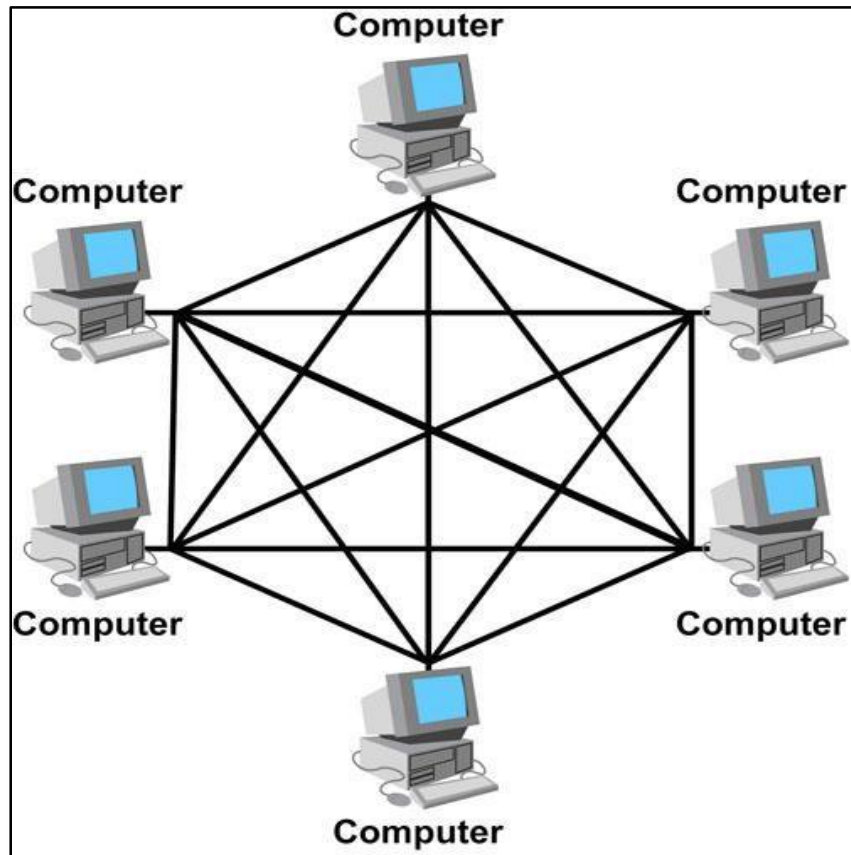
- Here every device has a **point to point** link to every other device.

- Node-1 must be connected with **n-1** nodes.

- A fully connected mesh can have **n(n-1)/2** physical channels to link n devices.

- It must have **n-1** input/output ports.

- **Advantages:**
- They use dedicated links so each link can only carry its own data load. So **traffic problem** can be avoided.

- **It is robust**. If **any one link get damaged** it cannot affect others.

- It gives privacy and security.(Message travels along a dedicated link)

- Fault identification and fault isolation are easy.

- **Disadvantages:**
1. **Cabling cost is high:** The **cabling** and **I/O ports** required are more, since every device is connected to each devices through dedicated link.

2. **Wiring is very complicated.**

3. Hardware required to connected each device is highly expensive.

4. Troubleshooting a failed cable is tricky.

Application

- Telephone Regional office.

- WAN.(Wide Area Network).
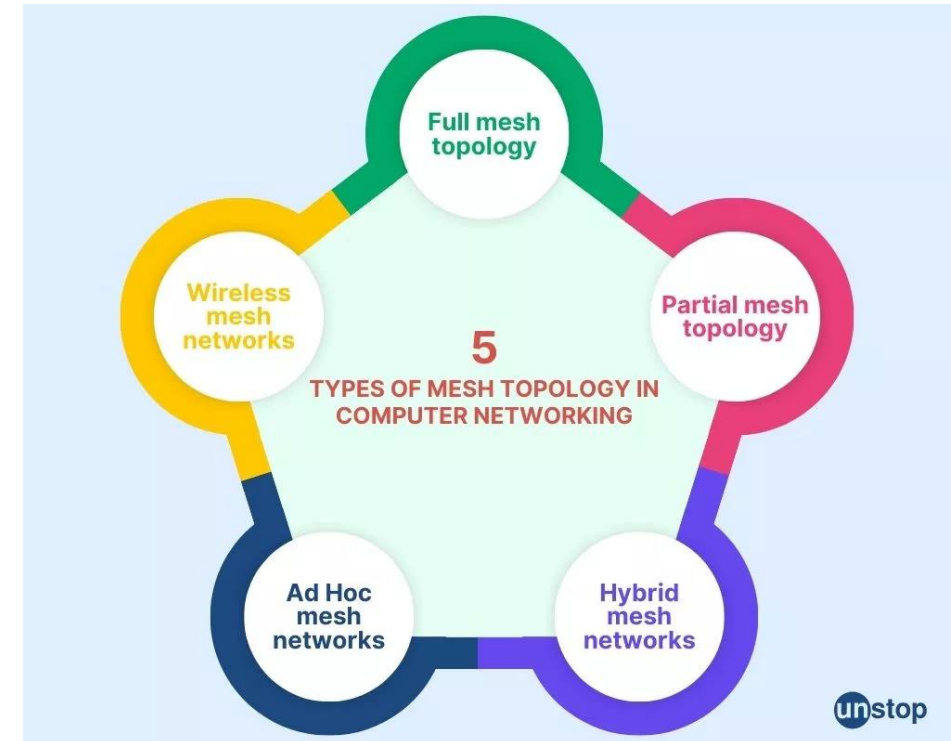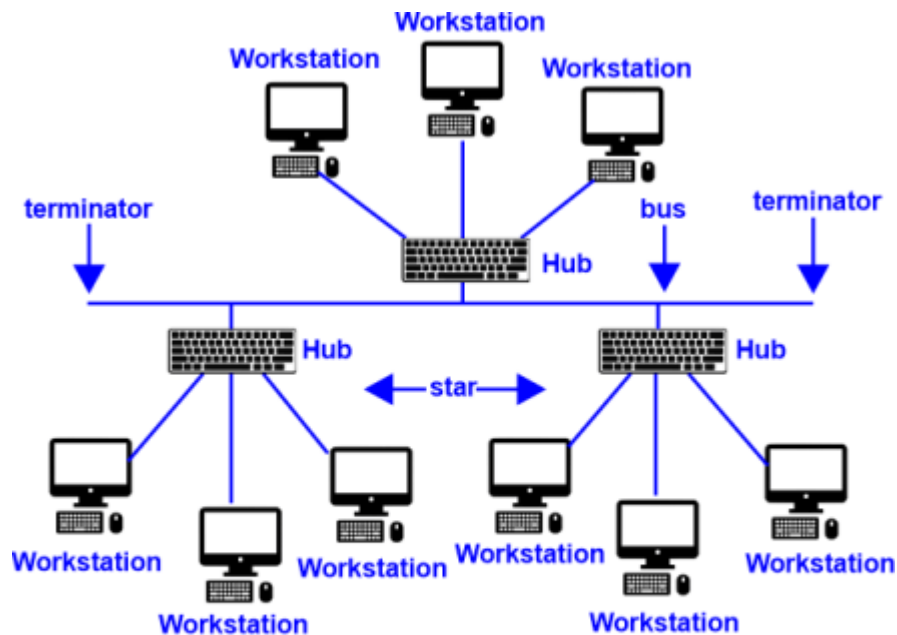
TREE TOPOLOGY

- Alternatively known as star bus topology

- This network topology is ideal for when you have a device acting as the root device on the network.

- Tree topology is one of the most common network setups that is similar to a bus topology and a star topology.

- A tree topology connects multiple star networks to other star networks.

Advantages:-

- Hierarchal Model

- Scalable

- Easy Implementation

- Easy Troubleshooting

Disadvantages:-

- Difficulty in maintenance and configuration
- Security threats
- Cost
- Maintenance
- Reliability
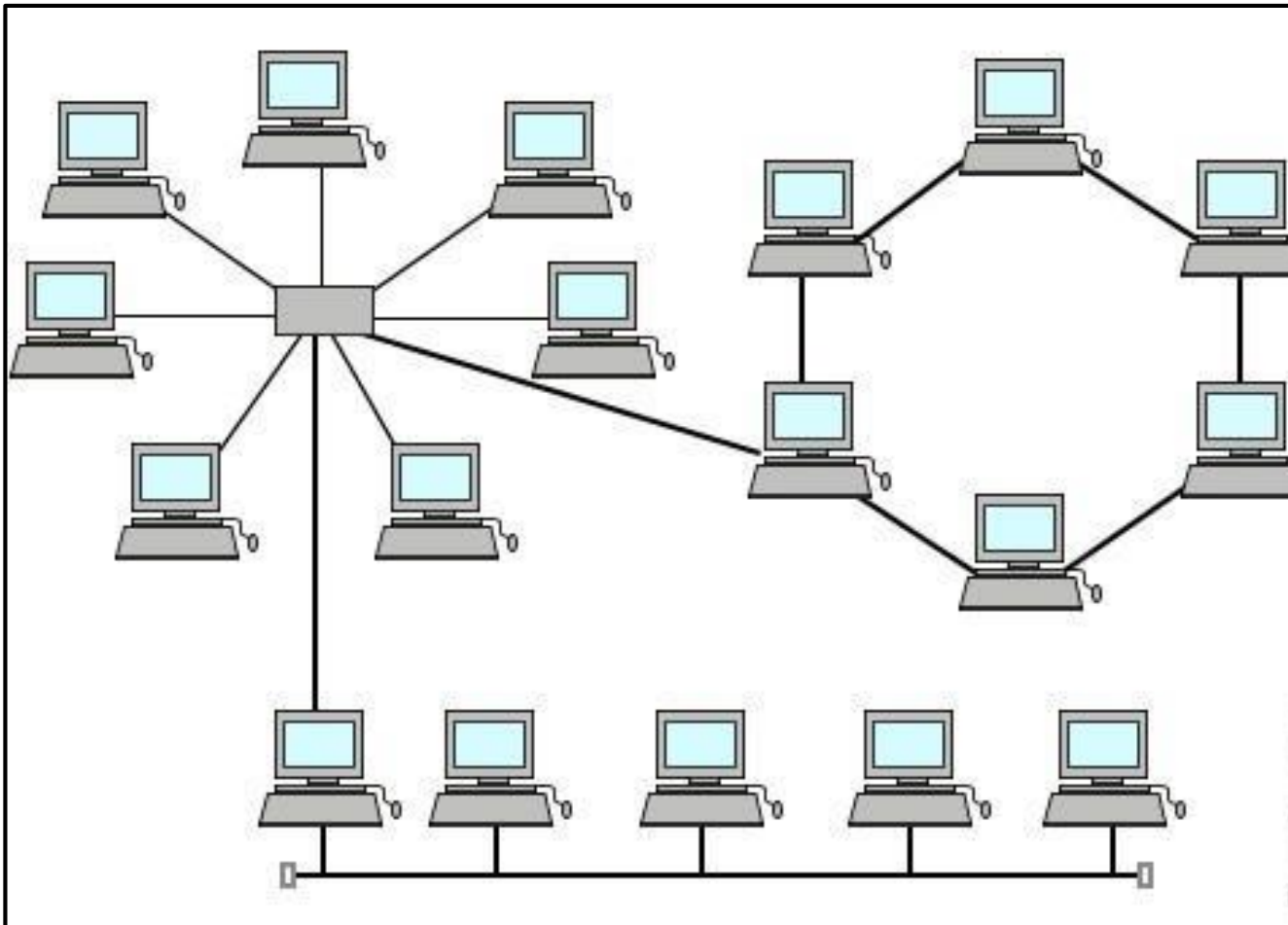
- A network which contain all type of physical structure and connected under a single backbone channel.

- This network topology is basically made up of several topologies i.e. a combination of two or more topologies, which could be bus, star, ring, etc.
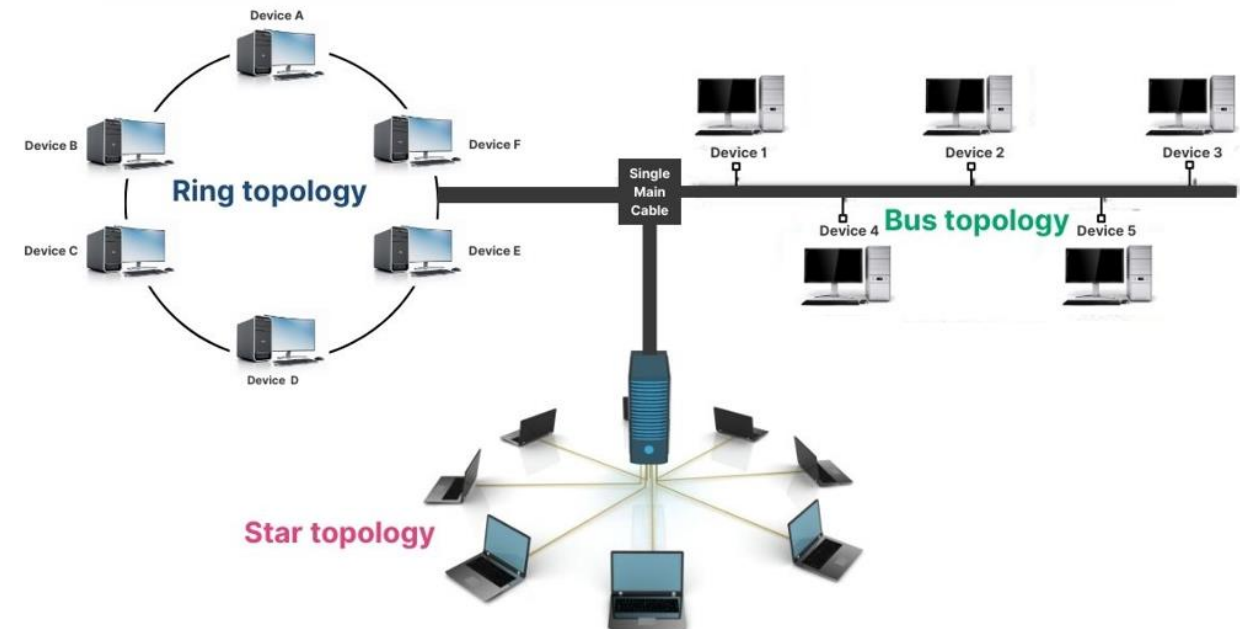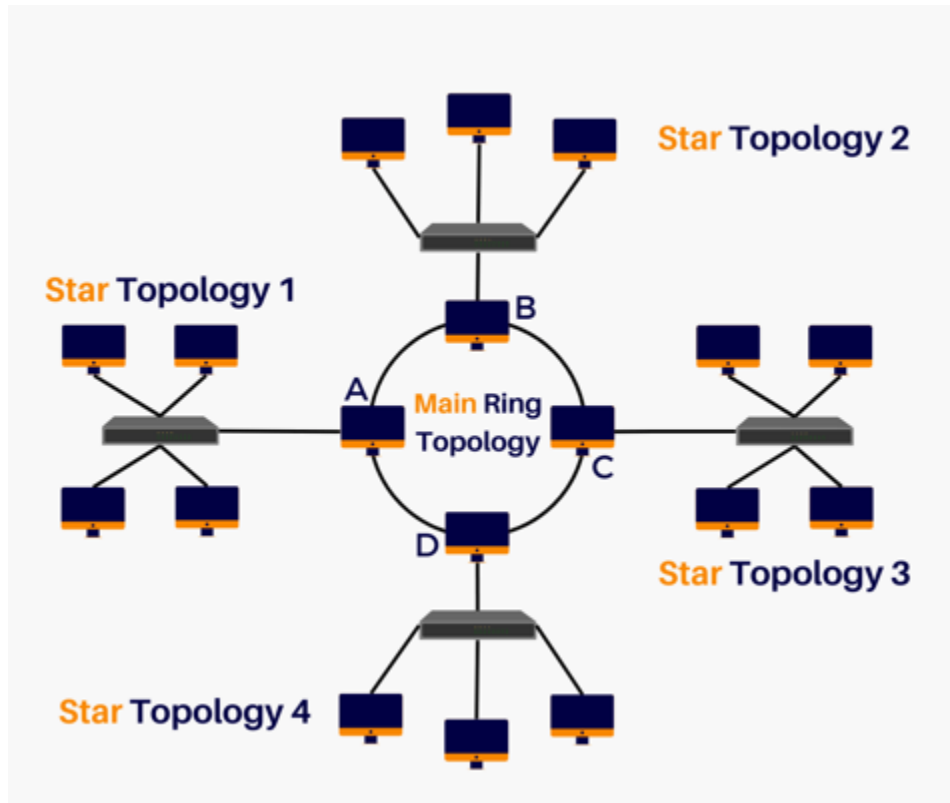
- **Advantages:**
- In terms of the advantages of using this kind of topology, we find that it has a high level of fault tolerance, which makes it reliable and flexible.

- Scalable as you can add new nodes easily.

- You can design it in such a way as to use the best features of various other topologies.

- **Disadvantages:**
- The disadvantages include things such as high cost and complexity of maintenance.

- This topology is used in real-life where scalability and high performance is important, for example Internet Service Providers.

- Costly infrastructure.

Network Control / Connecting Devices

- Network devices, or networking hardware, are physical devices that **are required for communication and interaction between hardware on a computer network**.

- Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called **network devices**.

- These devices transfer data in a fast, secure and correct way over same or different networks.

- Network devices may be inter-network or intra-network.

- Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc.

Network Connecting Devices

- Passive & Active Hubs

- Switches

- Routers

- Bridges

- Repeaters

- Gateways

- Modems

- Wireless infrastructure components

- Network Security Devices (firewalls , Proxy Server)

Network Connecting Devices

Repeaters

Matrox **Veos Repeater**

Repeater

Weak Signal — Amplified Signal
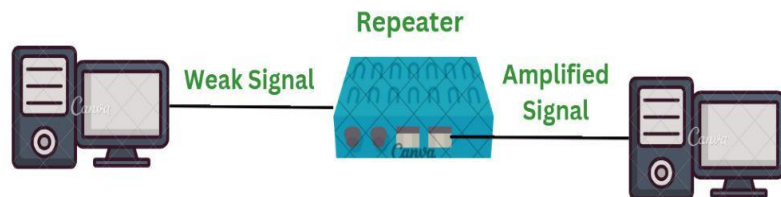
- 2 port device
- Forwarding
- No filtering
- Collision domain

- Network repeaters receive & retransmit incoming electrical, wireless or optical signals.

- A repeater operates at the physical layer.

- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted.

- An important point to be noted about repeaters is that they do not amplify the signal.

- When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.

Network Connecting Devices

Hub
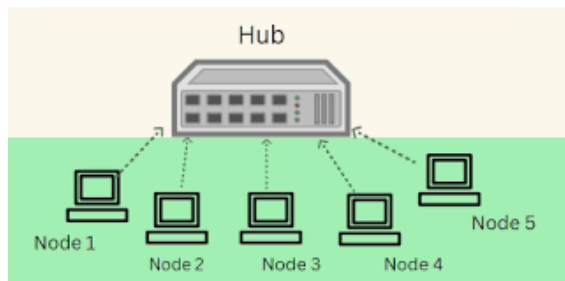
- Multiport repeater
- Forwarding
- No filter
- Collision domain

- A hub is basically a multiport 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.

- In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Network Connecting Devices:- Types of Hub

Active Hub:-
- These hubs have their own power supply and these hubs are used to clean, increase & transmit the signal using the network.
- It works as a wiring center & repeater.
- Active hubs play a key role in extending the distance between nodes.

Passive Hub :-
- These hubs collect wiring from the power supply and different nodes of an active hub.
- These hubs transmit the signals over the network without improving & cleaning them.
- These hubs are not suitable for extending the distance between nodes like an active hub.

Intelligent Hub :-
- It works like active hubs and includes remote management capabilities.
- They also provide flexible data rates to network devices.
- It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Network Connecting Devices

Bridge
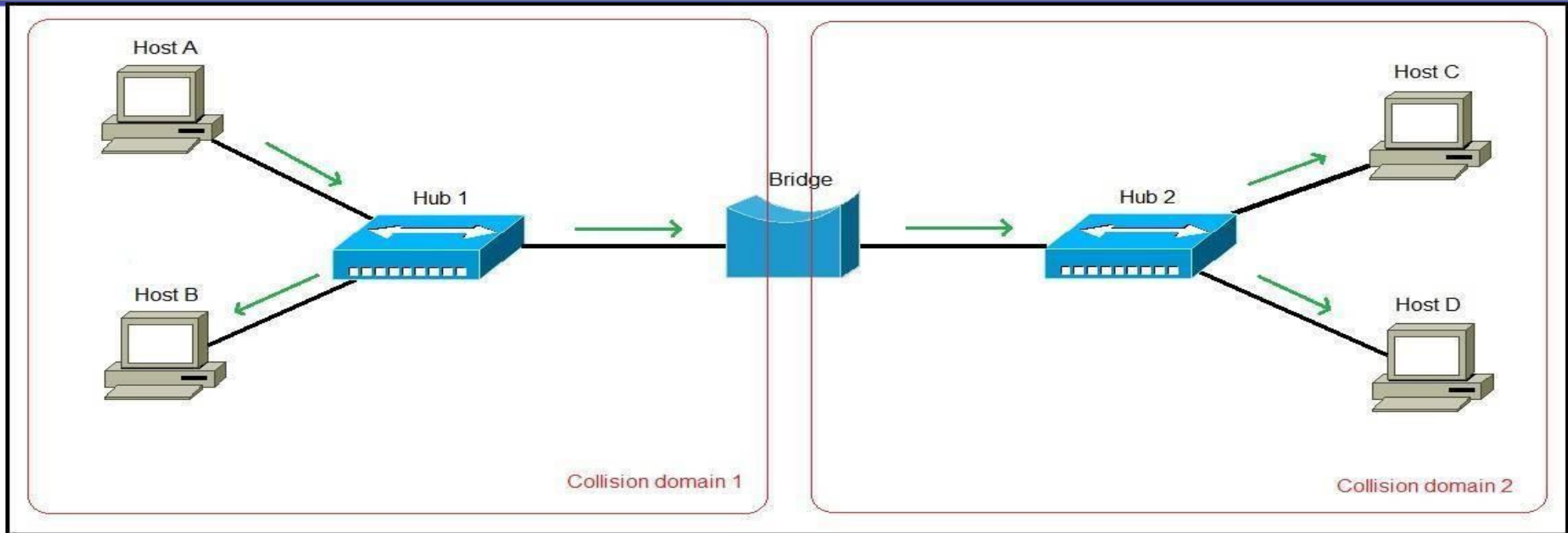
- Bridge operates at the data link layer and physical layer.
- Forwarding
- A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination.
- It is also used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, thus making it a 2 port device.

Network Connecting Devices

SINCE 1983
MIT-WPU
Dr. Vishwanath Kanad
MIT WORLD PEACE
UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

Bridge

Bridge In Computer Network

- Deals with Mac address of source and destination
- Filtering using Mac address which is not available in repeaters and hubs
- Static Bridge – manually maintains the table for port numbers and then forwarding/ filtering is done
- Network administrator has the task to manually maintain the table upon every change
- Dynamic Bridge – it learns the mac address as and when the packets are transmitted, then the table is populated every time for new source addresses
- So, first time broadcasting is done afterwards filtering is done
- To resolve looping it uses spanning tree protocol

Network Connecting Devices

Switch

- Works at data link layer
- Multiport bridge
- Full Duplex links
- Traffic minimal
- Collision domain zero – no collision

- Switch is more clever as compared with a hub.
- Different types of devices to be connected

- As the hub is used for data transferring, whereas a switch is used for filtering & forwarding the data.

- The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.

- In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.

Network Connecting Devices

SINCE 1983
Dr. Vishwanath Karad
MIT WORLD PEACE
UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS
MIT-WPU
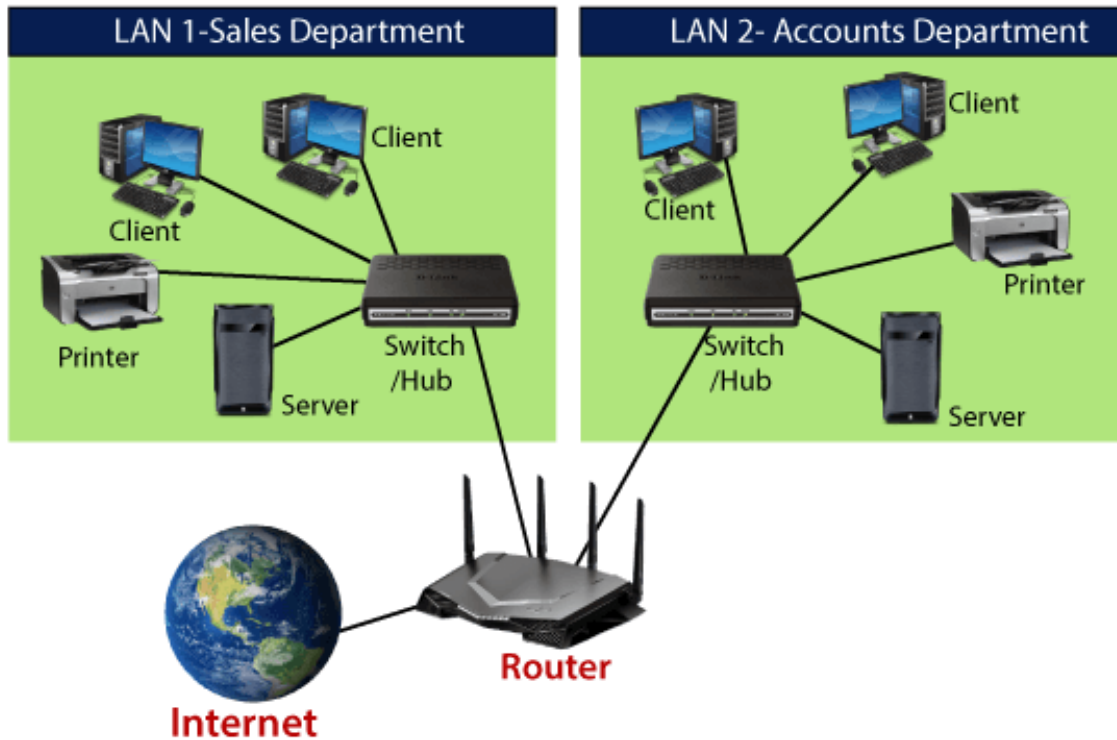
Routers

- Internet
- Works at Physical, data link and network layer
- A **router** is a **network layer** hardware device that transmits data from one LAN to another if both networks support the same set of protocols.
- It receives its data in the form of packets, which are data frames with their destination address added
- So, a router is typically connected to at least two LANs   and the internet service provider (ISP)
- Router also strengthens the signals before transmitting them
- A router reads its routing table to decide the best available route the packet can take to reach its destination quickly and accurately.

Network Connecting Devices
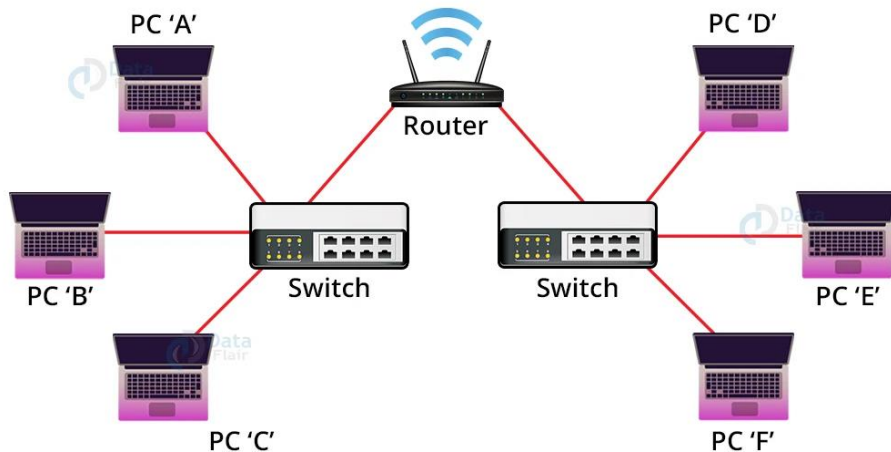
Routers

- Repeater –physical layer
- Switch, hubs – physical, data link layer
- Router – physical, data link, network layer
- Works with IP address
- Routing table is maintained to store address of all networks connected
- Forwarding done using routing table
- Flooding – kind of broadcasting in all directions if the packet can't be sent on desired location
- Filtering done - in case of ARP (address resolution protocol done within the same network)
- Store and forward method for routing so, no collision
- Collision domain zero

Network Connecting Devices

Routers

- A router reads its routing table to decide the best available route the packet can take to reach its destination quickly and accurately.
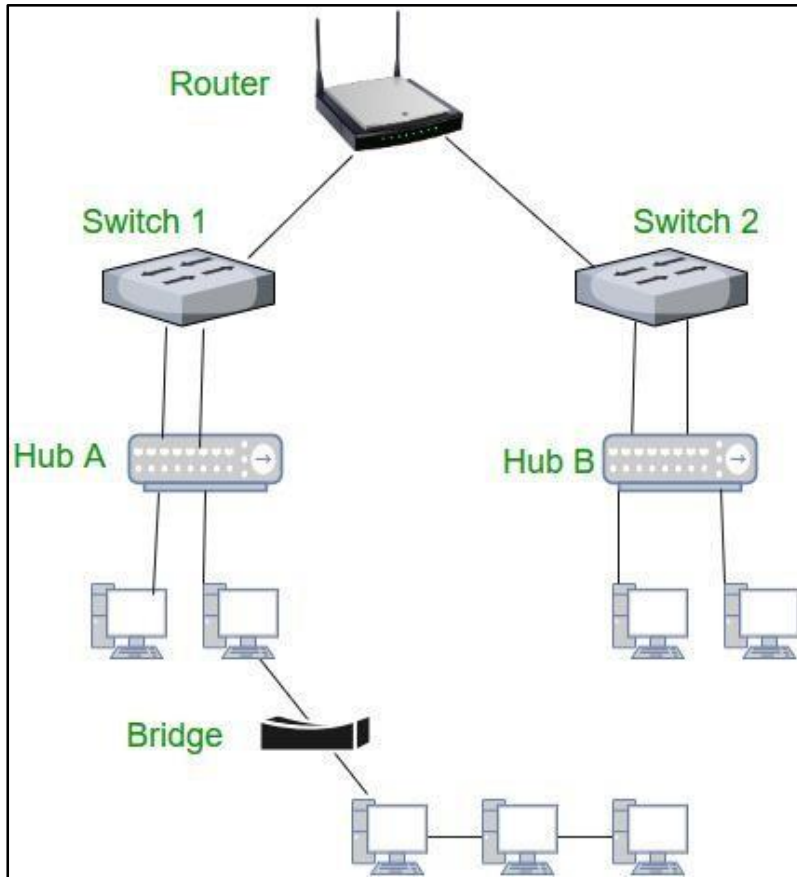- The routing table may be of these two types –

1. Static –
- In a static routing table the routes are fed manually.
- So it is suitable only for very small networks that have maximum two to three routers.

2. Dynamic –
- In a dynamic routing table, the router communicates with other routers through protocols to determine which routes are free.
- This is suited for larger networks where manual feeding may not be feasible due to large number of routers.

- *A modem is a device that modulates or demodulates the signal.*

- It maintains a dedicated connection with the ISP to get the internet connection for home or business.

- It acts as a bridge between the internet/telephone line and the computer.

- **The reason to use the modem for an internet connection is that both the internet and the computer take two different signals. It means that the internet sends the analog signal, but the computer system can only understand the digital signal. So, we need a device that can convert an analog signal to a digital signal and vice versa. To do this, we need a modem.**

- It modulates the incoming analog signal from the internet to digital signal and directs it to the computer, and vice versa.

What is Modulator demodulator?

MIT-WPU
Dr. Vishwanath Karad
MIT WORLD PEACE
UNIVERSITY | PUNE
SINCE 1983

Digital signal

Analog signal

Internet Service Provider

- The modem is placed between the telephone line and the computer system or router.
- It connects the devices with the ethernet port given in it.
- It connects the ISP(internet service provider) to the home network directly for the single PC. Or it is connected with the router to connect with multiple devices.
- This diagram is converting the incoming analog signal coming from telephone- lines/optical fiber to a digital signal and sending it to the PC.
- Without a modem, we cannot connect to the internet.

Modem or Router?
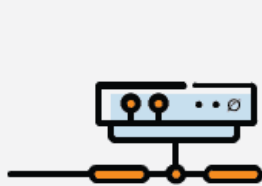
MODEM

A modem is the connection between your house and the internet.

A modem **does not** require a router to function.

ROUTER

A router is the connection between your modem and your wireless devices.

A router **does** need a modem to function.

Wireless Devices

How a modem and router work together

INTERNET

MODEM
Converts data to the Ethernet

Wi-Fi ROUTER
Connects to modem; the hub of your Wi-Fi connections

- **Router distributes or routes the internet connection from the modem to all the networking devices, either wired or wireless, such as PC, Laptop, Mobile phone, tablet, etc.**

Router vs Modem

Parameters	Modem	Router
Definition	A modem is a device that modulates and demodulates the electrical signal and maintains a dedicated connection between the internet and home/office network.	The router is a networking device that enables multiple devices to connect to wired or wireless networks.
Operating Layer of OSI model.	It works on **the data link** layer of the OSI model.	It works on the **physical, data-link, and network** layers of the OSI model.
Cable Used	RJ45 to connect with router, and RJ11 to connect with a telephone line.	RJ45 cable is used.
Security	The modem transmits the data without any authentication; hence it is not secure.	The router provides complete security with passwords and checks each data packet before transmitting it over a given network.

Router Vs Modem

Parameters	Modem	Router
Placed	A modem is placed between the telephone line and computer or router.	A router is placed between the modem and other networking devices.
Internet Access	It is essential to have a modem to access the internet as it connects the ISP to our PC.	We can access the internet without using a router.
Main Purpose	It takes the requested information from the internet to the computer.	It distributes the information from the modem to the given network.

Gateway

MIT-WPU
Dr. Vishwanath Karad
MIT WORLD PEACE
UNIVERSITY | PUNE
SINCE 1983
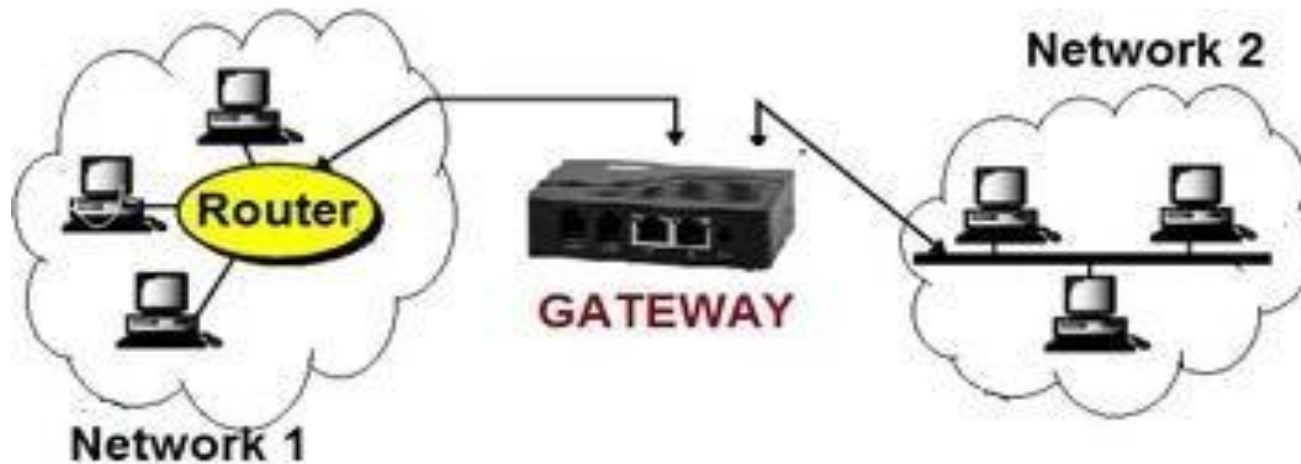
- Entry Exit point
- The gateway acts as a "Translator" in between two different systems that is used dissimilar communication protocols, data format or different architectures.
- It may be a server, router, firewall or other network device that allows to flow the traffic in and out of the network.

- Operates at all 7 layers of Osi Model
- A gateway usually is a computer with multiple **NICs** connected to different networks.
- A gateway can also be configured completely using software. As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network.
- **Gateway** uses **packet switching** technique to transmit data from one network to another.
- In this way it is similar to a **router**, the only difference being router can transmit data only over networks that use same protocols.

- **Access points**

  - Wireless devices can use access points to connect to a wired network.
  - It is easier to install access points within a wired network to connect all the computers or devices than to create connections using wires and cables.
  - Wireless access points are essential to enable wireless network connectivity. The type of access point an organization uses will depend on its specific needs.
  - For example:
    - On-premises access points are often the go-to option for businesses that have extensive security requirements and need to customize their wireless network infrastructure.

Wireless infrastructure components

- **Access points**

- **Wireless routers**

WRT300N
Wireless Router1

Laptop-PT
Laptop1

PC-PT
PC2

SMARTPHONE-PT
Smartphone0

TabletPC-PT
Tablet PC1

- A wireless router, or Wi-Fi router, combines the functions of a router and a wireless access point.
- Wireless routers are commonly used in smaller branch and home office networks, so workers in those locations can connect to the internet and the company network from one device in a small form factor.

Wireless infrastructure components

- **Wireless Gateway**
 - Gateway is network device that joins two networks.

- **Wireless NIC (Network Interface Card)**

- **Wireless LAN**
  - A wireless LAN is a wireless computer network that links two or more devices using wireless communication to form a local area network within a limited area such as a home, school, computer laboratory, campus, or office building.

Network Security Devices (Firewalls , Proxy Server)

- Network security is the security provided to a network from unauthorized access and risks.
- It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.
- **Types of Network Security Devices**
  - **Active Devices**
    These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.
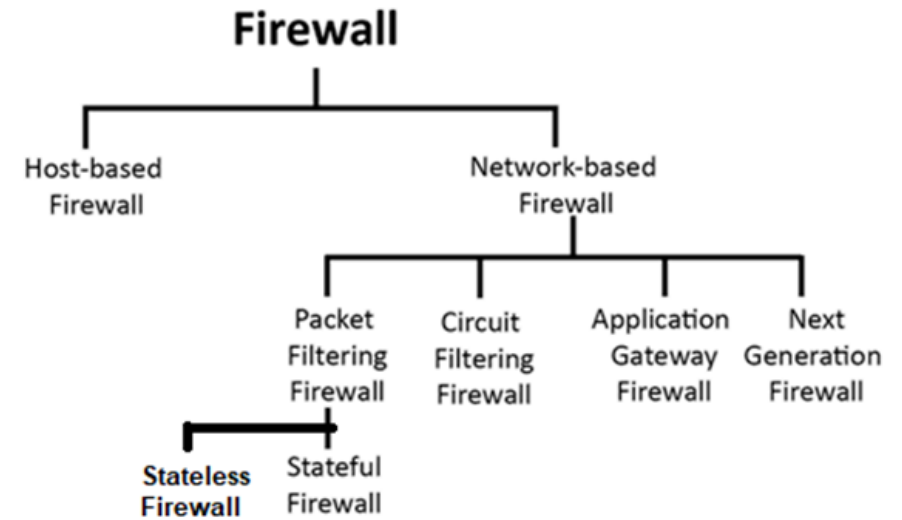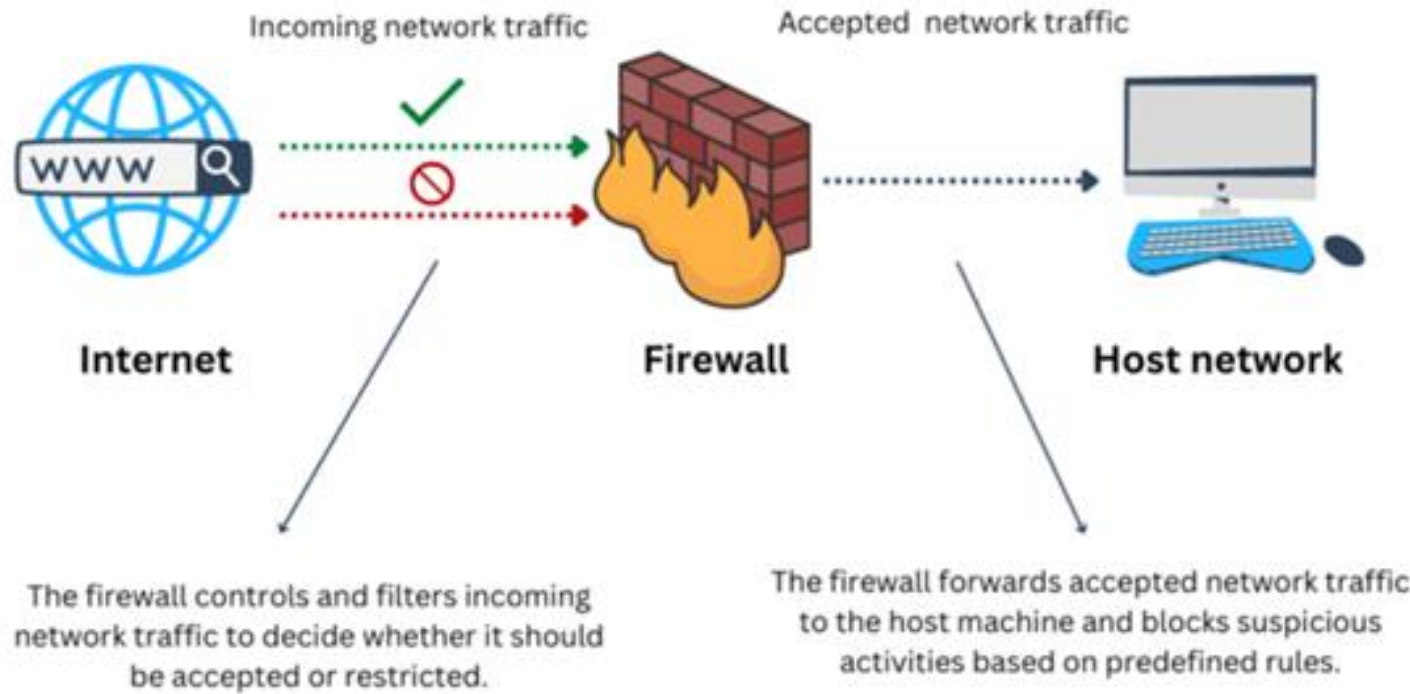 - **Passive Devices**
    These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

- **Firewalls**
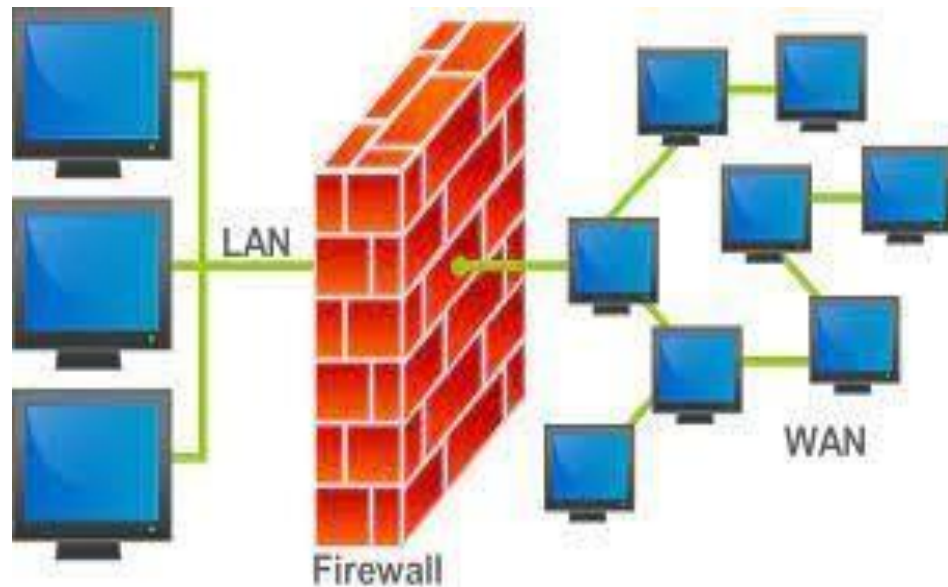
- A firewall is a network security system that manages and regulates the network traffic based on some protocols.
- A firewall establishes a barrier between a trusted internal network and the internet.
- Firewalls exist both as software that run on a hardware and as hardware appliances.
- Most personal computers use software-based firewalls to secure data from threats from the internet.
- Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet.
- Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

Firewall

Incoming network traffic

Accepted network traffic

Internet

Firewall

Host network

The firewall controls and filters incoming network traffic to decide whether it should be accepted or restricted.

The firewall forwards accepted network traffic to the host machine and blocks suspicious activities based on predefined rules.

Firewall

- Host-based Firewall
- Network-based Firewall
  - Packet Filtering Firewall
    - Stateless Firewall
    - Stateful Firewall
  - Circuit Filtering Firewall
  - Application Gateway Firewall
 - Next Generation Firewall

- **Antivirus**

  - An antivirus is a tool that is used to detect and remove malicious software.
  - It was originally designed to detect and remove viruses from computers.
  - Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc.
  - Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

- **Proxy Server**

  - Every computer that is connected to the network has an IP (Internet Protocol) address that identifies the device uniquely.
  - Similarly, the **proxy server** is a computer on the network that has its own IP address.
  - But sometimes, we want to access those websites or servers that are restricted and we do not want to show our identity (IP address).
  - In such a scenario, the **proxy server** comes into existence. We can achieve the same by using the **proxy server**.
  - It provides varying levels of functionality, security, and privacy that depend on the use case, needs, or policies of the company.

- **Proxy Server**
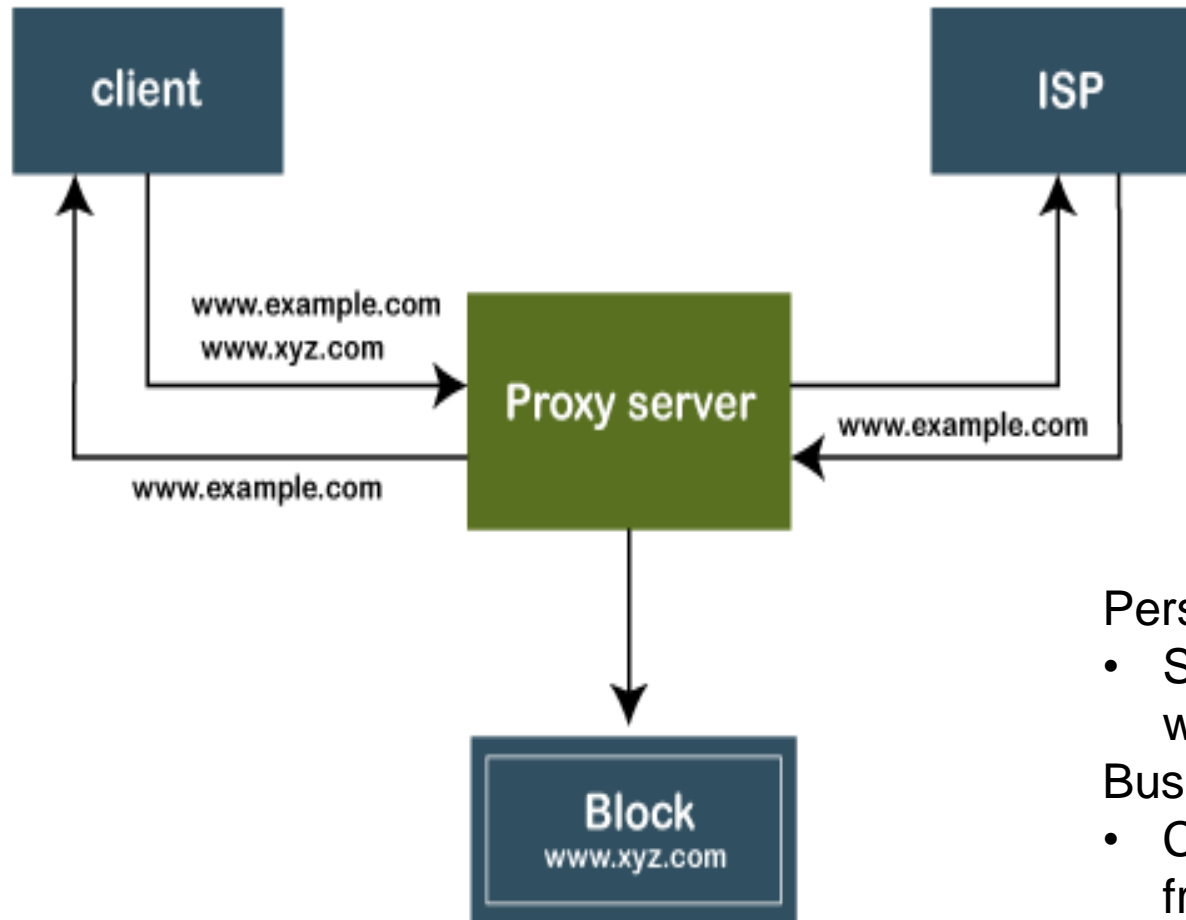
- Proxy server allows us to access any websites with a different IP address.
- It plays an intermediary role between users and targeted websites or servers.
- It collects and provides information related to user requests.
- The most important point about a proxy server is that it does not **encrypt traffic**.

Personal use
- Some people use proxy servers to hide their location while watching movies online

Business use
- Companies can use proxy servers to protect their networks from cyberattacks, phishing, and other malware attacks

- **Proxy Server**

  - **Advantages**

  - It improves the security and enhances the privacy of the user.

  - It hides the identity (IP address) of the user.

  - It controls the traffic and prevents crashes.

  - Protect our network from malware.

  - Allows access to the restricted content.

Thank You !!!