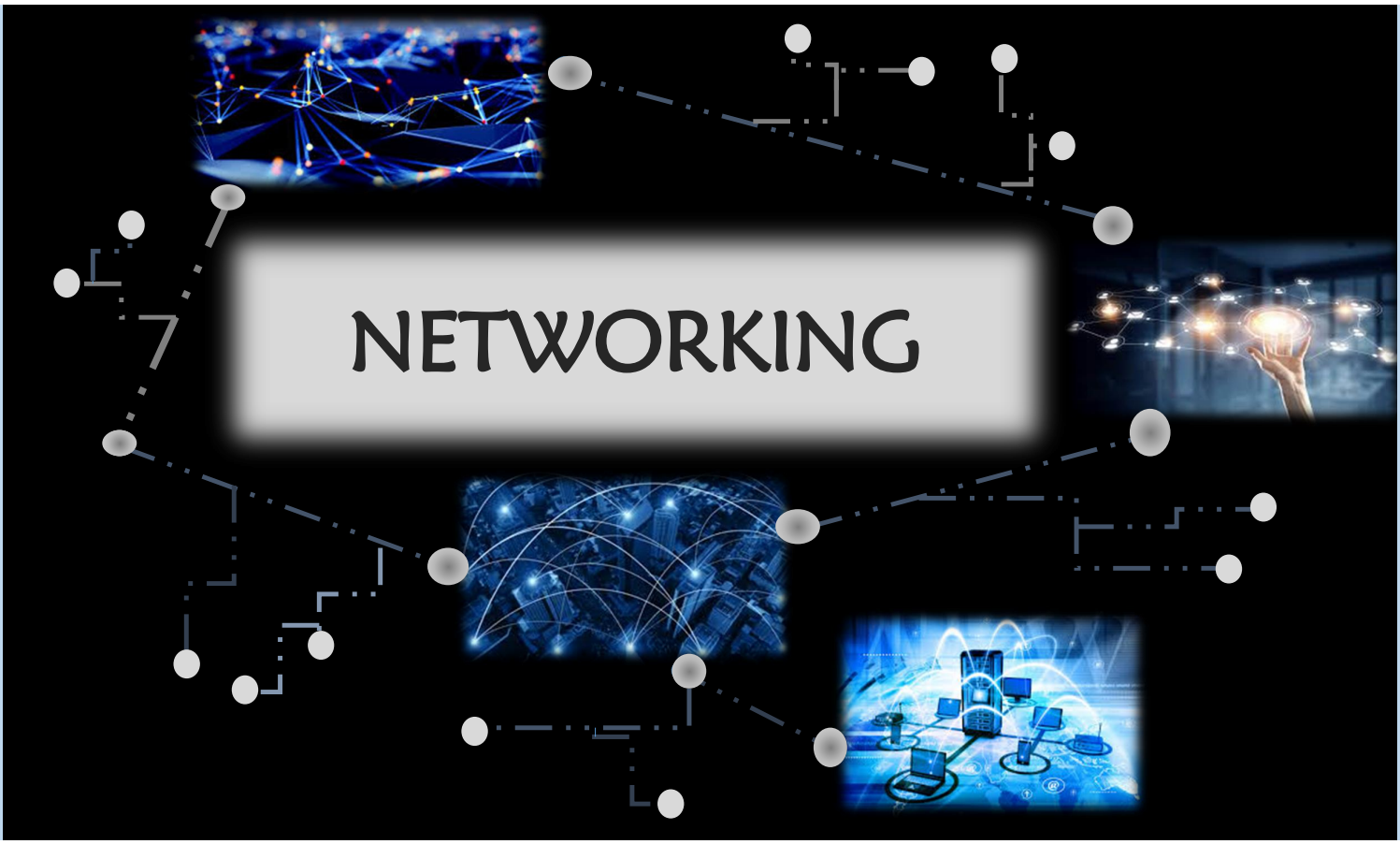
Chapter 16:

COMMUNICATION & NETWORKING CONCEPTS (A)

Index



Communication & Networking Concepts

NETWORK :

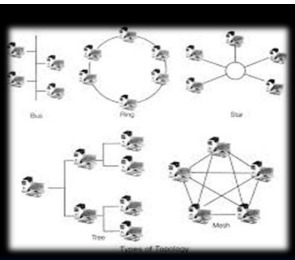
A network is an interconnected collection of autonomous computers. Two computers are said to be interconnected if they are capable of exchanging information.

NETWORK GOALS:

Resource Sharing- programs, data and peripherals are made available to all.
Reliability- A file can have copies on two or three different machines, so if one is unavailable other copies can be used.
Cost Factor- personal computers have better price/performance ratio than micro computers.
Communication Media- using networks people working far apart can have better co-operation among them as changes made at one end can be immediately noticed at another end.

EVOLUTION OF NETWORKING

In 1969 U.S. Department of Defence sponsored a project named ARPANET (Advanced Research Projects Agency Network). The goal of the project was to connect various universities and US Defence. In mid 80's National Science Foundation created a new high capacity network called NSFnet, which was more powerful than ARPANET. In 1990 the Internet came into picture.



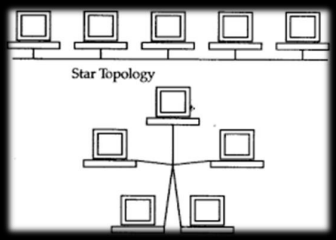
Wired Technologies (Guided Media)
When the computers in a network are interconnected through a wire or cable, then such a medium is categorised as:-
1. Ethernet Cable It is also known as twisted pair cable. There are two identical wires wrapped together and twisted around each other.

2. Co-axial Cable It consists of a solid core wire surrounded by foil shield, each separated by some insulator. The inner solid core wire carries the signal through the network and the shield is used to provide earthing or ground..

3. Optical Fiber It consists of thin strands of extruded glass silica or plastic, slightly thicker than human hair, which are capable of carrying light signals from a source at one end to another end. An optical fiber cable contain s: Core it is the innermost part, which is made up of glass or plastic through which the light signals travels ; Cladding covers the core and reflects the light beam back into the core ;
Protective Coating is outside the cladding for the protection of the optical fiber.

Types of Network
On the basis of coverage or geographical spread, a network can be divided into following types:
1. Local Area Network (LAN) When the network of computer is confined to a small or localised area such as school, office or building, it is known as Local Area Network (LAN).
2. Metropolitan Area Network (MAN) A metropolitan area network is the network which is spread over a city. The functions of a MAN is similar to LAN.
3. Wide Area Network (WAN) the network of computers which is spread across the countries probably over the entire world is known as a Wide Area Network (WAN).

4. Personal Area Network (PAN) The PAN refers to a computer network, which is used for communication among computer devices spread over a few meters. Bluetooth personal area network (PAN) is also called a picante. It can be composed of unto eight devices in a master slave relationship. The first Bluetooth device is master and other devices are acting as slaves.



Star Topology In star topology, there is a direct and dedicated connection of every . node of the network with the central node or server. In star topology, the server is directly connected with each and every node in the network via a hub.
Advantages of Star Topology
The star topology is the most reliable as there is a direct connection of every node in the network with the central node or server.
If there is any problem in connection with any node, other nodes in the network are not affected.
Disadvantages of Star Topology
Since, every node is directly connected with the central node or the server, so a large quantity of the cable is required.
There is dependency on the central node. If there are some problems with the central node, entire network stops functioning.

Advantages of Optical Fiber
It is immune to electrical and magnetic interference i.e. noise in any form cannot harm the data because, the information is travelling on a modulated light beam.
It is highly suitable for rigid industrial environments.
Optical fiber cables can be used for broadband transmission, where several channels (i.e. frequency bands of) are handled in parallel and there is possibility of mixing up of data transmission channels with other channels.
Disadvantages of Optical Fibber
Connecting either two fibres together or a light source to a fibre is a difficult process. Because of noise immunity, optical fibres are virtually impossible to tap. In order to intercept the signal, the fibre must be cut and a detector must be inserted which is not possible.
Optical fibre cables are more difficult to scolding (joint of one or more cable).

Internet
The Internet has gained popularity and emerged as an important and efficient means of communication. The Internet is world wide network of networks.
Through Internet, computers become able to exchange information with each other and find diverse perspective on issue from a global audience. **Wi-Fi** is a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access. *Wi-Fi* is a trademark of the non-profit Wi-Fi Alliance, which restricts the use of the term *Wi-Fi Certified* to products that successfully complete interoperability certification testing. As of 2017, the Wi-Fi Alliance consisted of more than 800 companies from around the world. As of 2019, over 3.05 billion Wi-Fi enabled devices are shipped globally each year. Devices that can use Wi-Fi technologies include personal computer desktops and laptops, smartphones and tablets, smart TVs, printers, smart speakers, cars, and drones.

We can booked tickets for airlines and trains or even we can book a room in a hotel at any destination by a network.

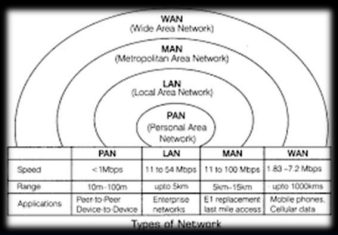
Communication Media

Communication media of a network refer to the connecting media, through which different computers in a network are interconnected together. The communication media can also be referred as communication channels.

Communication In a network environment, communication between different users or computers is possible. By which we can send messages, documents (text), data files, graphics, videos, images or an e-mail to different users over the network.

Accessing Remote Database We can access the remote database and retrieve information according to our requirement in a network.

- **Applications of Network** some of the applications of network are discussed below:
- Sharing of Information In a network, the users can share information, data and text easily to other users. Different users can share the same database, having different levels of access control.
- Sharing of Peripherals the computers, in a network, can share common peripherals, e.g. one highly speed common printer can be used for all computers in a network.



	PAN	LAN	MAN	WAN
Speed	< 1Mbps	11 to 54 Mbps	11 to 100 Mbps	1.83 -7.2 Mbps
Range	10m-100m	upto 5km	5km-15km	upto 1000kms
Applications	Peer to Peer Device to Device	Enterprise networks	E1 replacement last mile access	Mobile phones, Cellular data

Types of Network

Network Topologies

Ring Topology In ring or circular topology, the nodes are connected in a circular way. In such arrangement, each node is connected to exactly with its two neighbouring nodes.

Advantages of Ring Topology

Short cable length is required for connecting the nodes together.

The architecture of network is simple and easy to maintain.

Disadvantages of Ring Topology

In ring topology, each node is connected in a circular way with its two neighbouring nodes, so when there is transmission problem anywhere in the network, entire network stops functioning.

Fault diagnosis is very difficult in a network formed using ring topology

Bus Topology Bus topology is also referred as linear topology. Under this arrangement, all nodes in the network are connected by a single length of transmission medium, which is normally a co-axial cable. Both ends of the cable are terminated by terminators. Data transmission from any workstation can travel in both directions.

Advantages of Bus Topology

In bus topology, all nodes are connected through a single length of cable, so very short cable length is used.

Extension of network is very easy in bus topology. We can connect new nodes along its length.

Disadvantages of Bus Topology

When there is any problem in data communication with any node, whole network stops functioning.

In case of any fault in data transmission, fault isolation is very difficult. We have to check the entire network to find the fault.

.

Mesh Topology A network set-up where each computer and network device is interconnected with one another to provide an alternative route in case of the host is down or busy.

Advantages of Mesh Topology

Excellent for long distance networking.

Communication is also possible through the alternate route, if one path is busy.

Disadvantages of Mesh Topology

Long wire/cable length, hence increase in the cost of installation and maintenance

There are high chances of redundancy in many of the network connections.

Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

2. Infrared In this type of transmission, infrared light signals are used. Infrared signal are used in TV remotes, infrared wireless speakers, etc., as a mode of transmission.
In infrared transmission, signals are transmitted through the air but these signals cannot penetrate the walls.
Short range: performance d (i.e. able to see each other) to communicated drops off with longer distances.
3. Microwave In this type of transmission, signals are transmitted in the same way as the radio and television transmission. The requirement for microwave transmission is transmitter, receiver and the atmosphere. Under this mode of transmission parabolic antennas are mounted on the towers. These antennas send the signals in the atmospheric air. These signals are received by the receiver.

Radio Link When two terminals are connected by using radio frequencies, then such type of communication is referred as radio wave transmission or radio link. Any radio transmission set-up has two parts viz., the transmitter and the receiver. Both the transmitter and the receiver use antennas to send and receive the radio signals.
Satellite In this type of communication, data are transmitted through satellite. Under this arrangement, there is an earth station and a satellite placed in the stationary orbit, which is about 22300 miles above the earth's surface. In satellite communication, the earth station transmits data towards the satellite and the satellite accepts these signals, amplifies them and then retransmits them towards the earth. These signals are captured by the receiver.

Network Devices
Network devices are the components used to connect computer and other electronic devices together, so that they can share files or resources like printers or fax machines. The most common type of network devices used by the public to set-up a Local Area Network (LAN) are hub, switch, repeater and if online access is desired, a high-speed modem.
1. Modem (Modulator/Demodulator) Modem is a device that converts digital signal to analog signal (modulator) at the sender's site and converts back analog signal to digital signal (demodulator) at the receiver's end, in order to make communication possible via telephone lines.
Functions of Modem The essential function of a modem is to create an easily transmitted and decode signal. Modem divides the information into packets called frames. They minimise the error that occur while the transmission of signals.
Modems are of two types:
Internal Modem It refers to the modem that is fixed within a computer, e.g. dial-up and wireless.
External Modem **A modem that resides in a self-contained box outside the computer system, e.g. USB modem, Cable** modem.

Hub - Hub is a device used to connect several computers together. It provides a centralised connection to several computers with the central node or server.
It is multi-slot device in which multi-port cards can be inserted to provide access to computers in the network.
Switch The switch is a hardware device used to divide or segment the network into smaller subnets or LAN segments. The main purpose of segmenting a large network into smaller segments is to prevent the traffic overloading in a network.
.

Repeater The repeater is a hardware device used in a network to amplify the weak signals, when they are transported over long distances. When the signal is transmitted over a line, then due to resistance and other causes it accumulates noise. Due to this noise, the quality of signal degrades. So, to improve the quality of signals, repeaters are needed to be installed **Gateway** The gateway is a network device which is used to connect dissimilar networks. The gateway establishes an intelligent connection between a local network and external networks, which are completely different in

structure**.**

Network Protocols
Protocol refers to the set of rules and regulations applicable for a network. The protocol defines standardised format for the data packet to be transmitted through the network, techniques for detecting the errors whenever they arise and methods to correct these errors and so on.
Some of the commonly used protocols are as follows:
1. HTTP (Hypertext Transfer Protocol)
HTTP is an application level protocol and it is widely used for viewing information of a web page over Internet. It is a generic, stateless and object oriented protocol.
HTTP consists of a set of requests from the browser of a local computer to the web server and a set of responses going back to the other way.
Though HTTP is designed for the use in the web application but it has scope to be used in future object oriented applications.

4. PPP (Point-to-Point Protocol) The PPP is used with dial-up Internet connections including ISDN. It is a layered protocol, which is used for transmitting the data over usual telephone lines. It can provide connection authentication, transmission, encryption and compression.

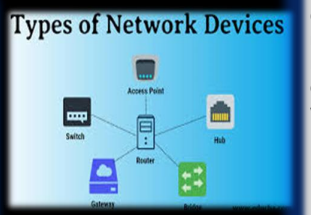
FTP (File Transfer Protocol)
FTP is designed to transfer files from one system to another. Using FTP, different people locating in different geographical locations can cooperate and work on a common project. FTP is designed to promote sharing of files and to encourage the indirect use of remote computers. Using FTP, any type of file can be transferred from one computer to another. Though for transferring files, we have to specify whether the file is in ASCII format or in binary format.

3. TCP/IP (Transmission Control Protocol/Internet Protocol) TCP/IP is a set of two protocols, i.e. TCP and IP. The Internet Protocol (IP) tells how packets of information are sent out over networks. IP has a packet addressing method that lets any computer on the Internet forward a packet to another computer that is a step closer to the packet's recipient. The Transmission Control Protocol (TCP) ensures the reliability of data transmission across Internet connected networks. TCP checks packets for errors and submits requests for retransmission if errors are found.

MAC Address (Media Access Control Address)
The MAC address refers to unique physical address assigned to a Network Interface Card (NIC). Every workstation or device which is connected with the network has unique node address. The MAC address is a 6 byte (48 bit) address. Each byte in this address is separated by a colon. There are hexadecimal numbers from 00 to FF (i.e. 0 – 255) in each byte, e.g. 05 : C2: 04 : 59 : 2F: BC is a MAC address.

.

Basic Components for the Working of Internet
Here, we are discussing some basic yet essential components of a network which are very much required for the proper functioning of the Internet.
IP Address
An IP address is an identifier for a computer or device on a TCP/IP network. It is a way to measure a user's unique identity. The traditional IP Addresses (IPv4) uses a 32-bit numeric format and it defines both network and host address. But now-a-days a new version of the IP protocol (IPv6) has been invented to offer virtually limitless number of unique addresses. An IP address can be static or dynamic. A static IP address will never change and it is a permanent Internet address. A dynamic IP address is a temporary address that is assigned to any computing device to access the Internet. An example of IPv4 address is 216.3.128.12. Each number can be from zero to 255.



Domain Name Resolution
Domain name resolution refers to the process of getting the corresponding IP address from a domain name. Infact the content of a website is stored on some server anywhere in the world and to access the information or content the IP address is required. Thereafter, the operating system searches the host file in which IP address of some domains are stored. If the corresponding domain name was not found there, then request is forwarded to Domain Name Servers (DNS). The DNS maintains a directory of all domain names and corresponding IP addresses registered on the Internet. When the IP address is required, it is provided to the browser. The browser can access the information from the respective website using the IP address.

Domain Name
Domain name is a unique name or identification that helps to create the path to open a particular website. All the domain names have IP addresses. IP address can be remembered by the computer, but it is difficult to remember for a human being. If you know that URL (Uniform Resource Locator) of a website, you can access it. The URL is actually the domain name of website, so the domain name is unique name of a website. Every time we enter a domain name it will be converted into an IP address and the website will be opened, e.g. www.Mybook.com A domain name contains three parts:
Host name as, www
Name describing the website purpose as, Mybook
Top level domain as .com, .net, .edu, etc

Network Security Concepts

Cookies
It is also known as browser cookies or tracking cookies. Cookies are small, often encrypted text files, located in browser directories. They are used by web developers to help users navigate their websites efficiently and perform certain functions

Hacker
A hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hacking is the practices of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose

Firewall
A system based on software or hardware designed to prevent unauthorised access to or from a private network. Firewalls may be combination of hardware and software. A firewall establishes a barrier between a trusted, secure internal network (private network) and another network that is not assumed to be secure and' trusted.

Cracker
A cracker is also called black hat hacker. A cracker is an individual with extensive computer knowledge whose purpose is to breach or bypass Internet security or gain access to the software without paying royalties. The general view is that, while hackers build things, crackers break things. Cracker is the name given to hackers who break into computers for criminal gain.

Cyber Law
Cyber law is a term that encapsulates legal issues related to the use of Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of rules and regulations. Some leading topics include Internet access and usage, privacy, freedom of expression and jurisdiction.

Trojan
A Trojan, or Trojan Horse, is a non-self-replicating type of malware which appears to performs a desirable function but instead facilitates unauthorised access to the user's computer system.
e.g. Beast, Sub7.Zeus, Zero Access Rootkit, etc.

NETWORKING DEVICES

Networking Devices are components used to connect computer or other electronic devices together so that they can share resources like printers, fax etc.

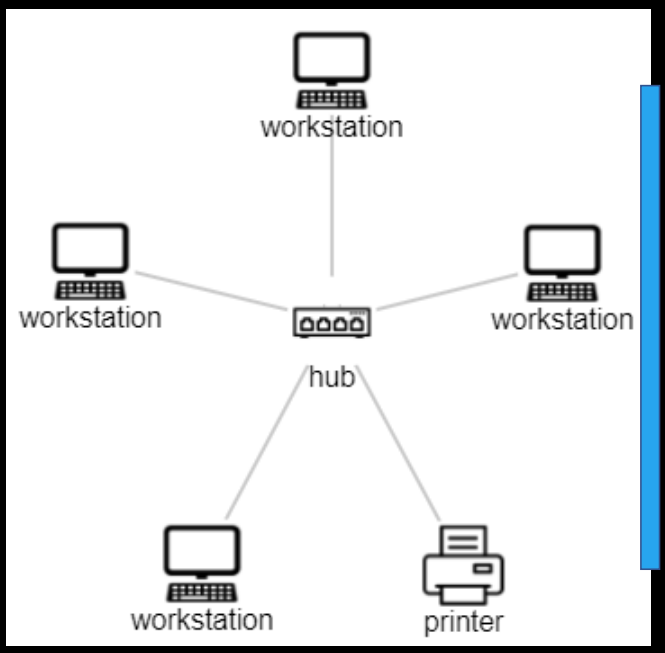
Types of Devices

- Hub
- Switch
- Gateway
- Bridge
- Router

1.

Hub

- Hub is a common connection point for devices in a network.
- Commonly used to connect segments of a LAN.
- Consists of multiple ports.
- When a packet arrives at one port, it is copied to all other ports to make it viewable to the entire LAN.



Hub

Structure of a Hub

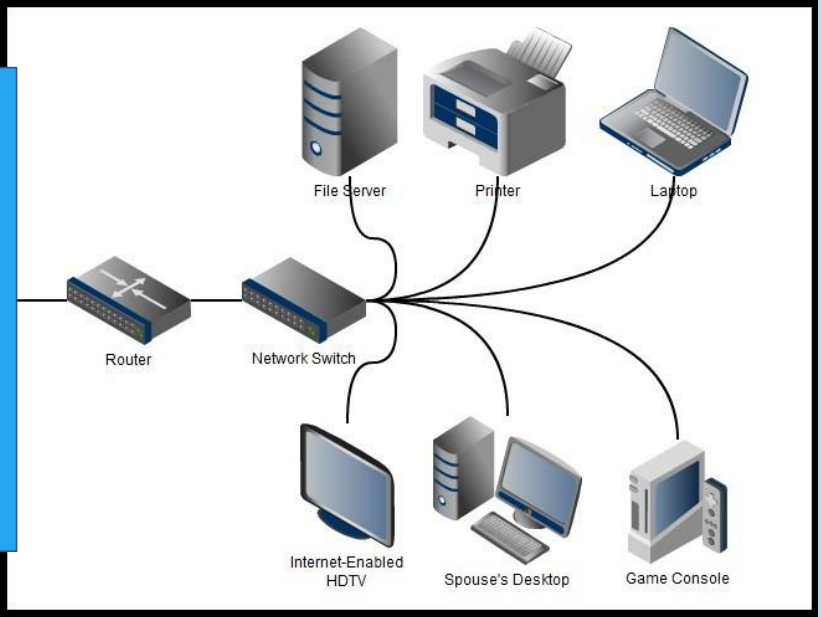
2.

Switch

- A network switch (also called switching hub, bridging hub and MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.
- A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches

Switch

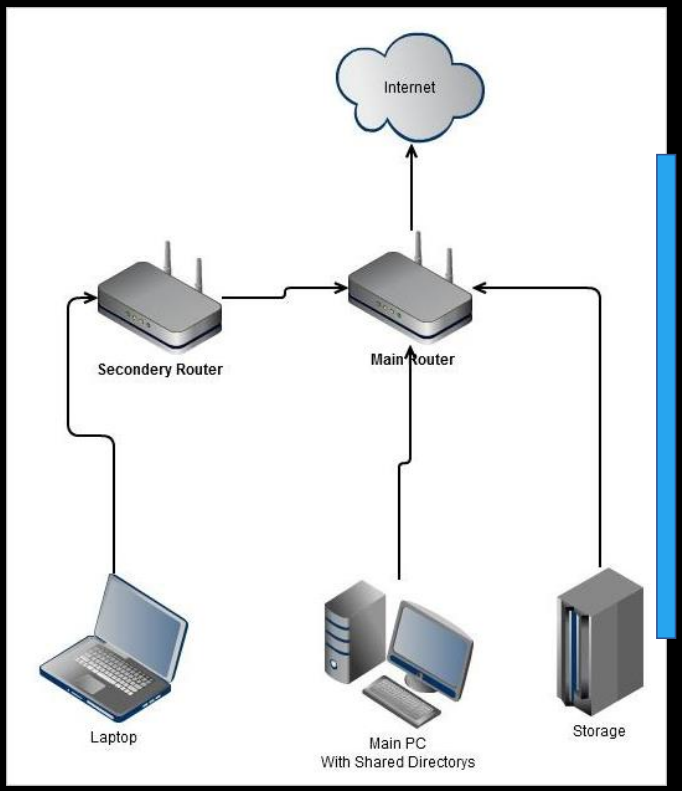
Structural diagram of a switch



3.

Gateway

A gateway is a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another. Gateways are distinct from routers or switches in that they communicate using more than one protocol to connect a bunch of networks and can operate at any of the seven layers of the open systems interconnection model (OSI).



Gateway

Structure of a Gateway

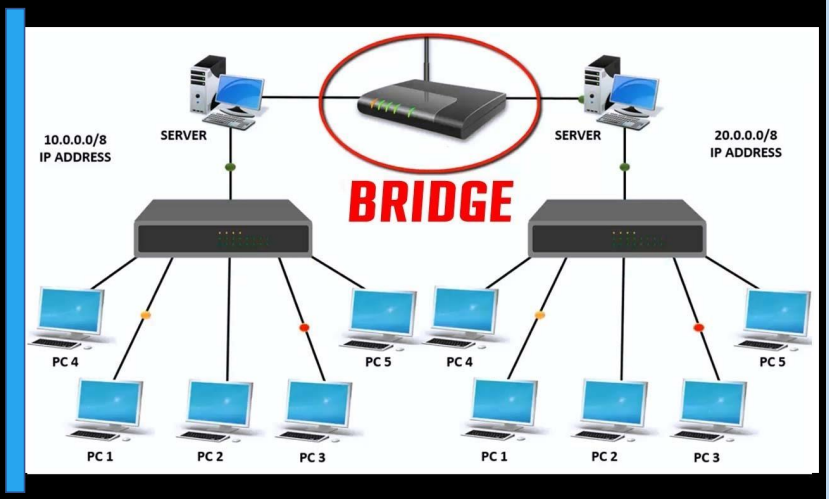
4.

Bridge

A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments. This function is called network bridging. In the OSI model, bridging is performed in the data link layer (layer 2). If one or more segments of the bridged network are wireless, the device is known as a wireless bridge.

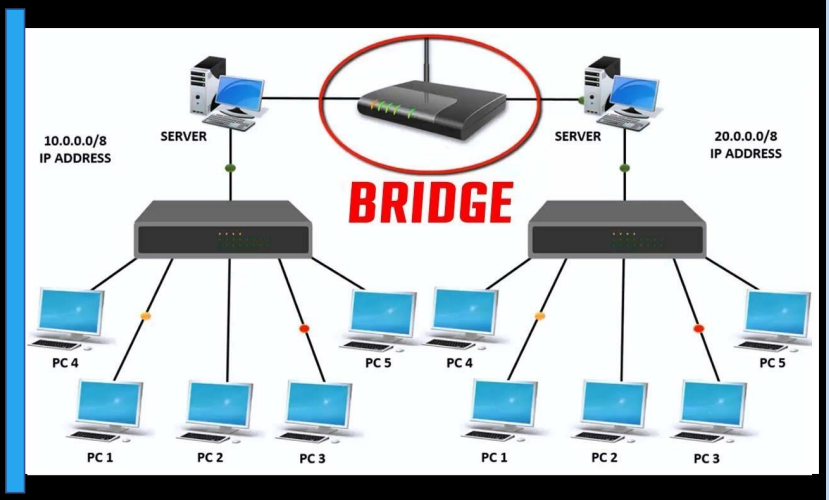
Bridge

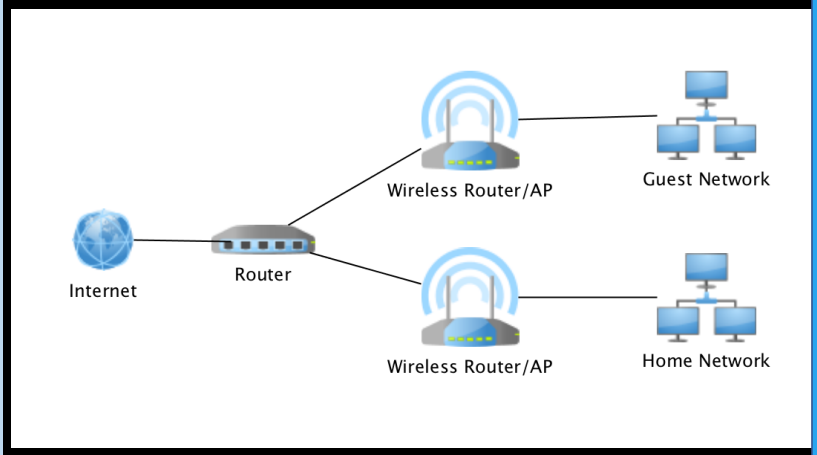
Structural diagram of a bridge



Bridge

Structural diagram of a bridge





Router

Structure of a Router