RESEARCH INNOVATION DISCOVERY

RID संस्था समस्या का समाधान

RUN BY TWKSAA WELFARE FOUNDATION

Reg.No: 048884
Foundation Day
05-09-2024

Computer Network

E-Book

Er. Rajesh Prasad(B.E, M.E)
Founder: TWF & RID Org.

- **RID ORGANIZATION** यानि **Research, Innovation Discovery** संस्था जिसका मुख्य उदेश्य हैं आने वाले समय में सबसे पहले **NEW (RID, PMS & TLR)** की खोज, प्रकाशन एवं उपयोग भारत की इस पावन धरती से भारतीय संस्कृति, सभ्यता एवं भाषा में ही हो |
- देश, समाज, एवं लोगों की समस्याओं का समाधान **NEW (RID, PMS & TLR)** के माध्यम से किया जाये इसके लिए ही मैं राजेश प्रसाद **इस RID संस्था** का स्थपना किया हूँ |
- Research, Innovation & Discovery में रूचि रखने वाले आप सभी विधार्थियों, शिक्षकों एवं बुधीजिवियो से मैं आवाहनं करता हूँ की आप सभी **इस RID संस्था** से जुड़ें एवं अपने बुध्दि, विवेक एवं प्रतिभा से दुनियां को कुछ नई **(RID, PMS & TLR)** की खोजकर, बनाकर एवं अपनाकर लोगों की समस्याओं का समाधान करें |

"त्वक्सा कंप्यूटर नेटवर्क के इस ई-पुस्तक में आप कंप्यूटर नेटवर्क से जुड़ी सभी बुनियादी अवधारणाएँ सीखेंगे। । मुझे आशा है कि इस ई-पुस्तक को पढ़ने के बाद आपके ज्ञान में वृद्धि होगी और आपको कंप्यूटर विज्ञान के बारे में और अधिक जानने में रुचि होगी"

"In this E-Book of Computer Network you will learn all the basic concepts related to computer Network. I hope after reading this E-Book your knowledge will be improve and you will get more interest to know more thing about computer Science".

RID हमें क्यों करना चाहिए ?

(Research)

अनुसंधान हमें क्यों करना चाहिए ?

Why should we do research?

1. नई ज्ञान की प्राप्ति (Acquisition of new knowledge)
2. समस्याओं का समाधान(To Solving problems)
3. सामाजिक प्रगति (To Social progress)
4. विकास को बढ़ावा देने(To promote development)
5. तकनीकी और व्यापार में उन्नति(To advances in technology & business)
6. देश विज्ञान और प्रौद्योगिकी के विकास(To develop the country's science & technology)

(Innovation)

नवीनीकरण हमें क्यों करना चाहिए ?

Why should we do Innovation?

1. प्रगति के लिए(To progress)
2. परिवर्तन के लिए(For change)
3. उत्पादन में सुधार(To Improvement in production)
4. समाज को लाभ(To Benefit to society)
5. प्रतिस्पर्धा में अग्रणी (To be ahead of competition)
6. देश विज्ञान और प्रौद्योगिकी के विकास। (To develop the country's science & technology)

(Discovery)

खोज हमें क्यों करना चाहिए?

Why should we do Discovery?

1. नए ज्ञान की प्राप्ति(Acquisition of new knowledge)
2. अविष्कारों की खोज(To Discovery of inventions)
3. समस्याओं का समाधान(To Solving problems)
4. ज्ञान के विकास में योगदान(Contribution to development of knowledge)
5. समाज के उन्नति के लिए (for progress of society)
6. देश विज्ञान और तकनीक के विकास (To develop the country's science & technology)

❖ Research(अनुसंधान):

- अनुसंधान एक प्रणालीकरण कार्य होता है जिसमें विशेष विषय या विषय की नई ज्ञान एवं समझ को प्राप्त करने के लिए सिद्धांतिक जांच और अध्ययन किया जाता है। इसकी प्रक्रिया में डेटा का संग्रह और विश्लेषण, निष्कर्ष निकालना और विशेष क्षेत्र में मौजूदा ज्ञान में योगदान किया जाता है। अनुसंधान के माध्यम से विज्ञान, प्रोधोगिकी, चिकित्सा, सामाजिक विज्ञान, मानविकी, और अन्य क्षेत्रों में विकास किया जाता है। अनुसंधान की प्रक्रिया में अनुसंधान प्रश्न या कल्पनाएँ तैयार की जाती हैं, एक अनुसंधान योजना डिज़ाइन की जाती है, डेटा का संग्रह किया जाता है, विश्लेषण किया जाता है, निष्कर्ष निकाला जाता है और परिणामों को उचित दर्शाने के लिए समाप्ति तक पहुंचाया जाता है।

❖ Innovation(नवीनीकरण): -

- Innovation एक विशेषता या नई विचारधारा की उत्पत्ति या नवीनीकरण है। यह नए और आधुनिक विचारों, तकनीकों, उत्पादों, प्रक्रियाओं, सेवाओं या संगठनात्मक ढंगों का सृजन करने की प्रक्रिया है जिससे समस्याओं का समाधान, प्रतिस्पर्धा में अग्रणी होने, और उपयोगकर्ताओं के अनुकूलता में सुधार किया जा सकता है।

❖ Discovery (आविष्कार):

- Discovery का अर्थ होता है "खोज" या "आविष्कार"। यह एक विशेषता है जो किसी नए ज्ञान, अविष्कार, या तत्व की खोज करने की प्रक्रिया को संदर्भित करता है। खोज विज्ञान, इतिहास, भूगोल, तकनीक, या किसी अन्य क्षेत्र में हो सकती है। इस प्रक्रिया में, व्यक्ति या समूह नए और अज्ञात ज्ञान को खोजकर समझने का प्रयास करते हैं और इससे मानव सभ्यता और विज्ञान-तकनीकी के विकास में योगदान देते हैं।

नोट : अनुसंधान विशेषता या विषय पर नई ज्ञान के प्राप्ति के लिए सिस्टमैटिक अध्ययन है, जबकि आविष्कार नए और अज्ञात ज्ञान की खोज है।

सुविचार:

1.	**समस्याओं का समाधान करने का उतम मार्ग हैं |**	→ शिक्षा ,RID, प्रतिभा, सहयोग, एकता एवं समाजिक-कार्य
2.	**एक इंसान के लिए जरूरी हैं |**	→ रोटी, कपड़ा, मकान, शिक्षा, रोजगार, इज्जत और सम्मान
3.	**एक देश के लिए जरूरी हैं |** -	→ संस्कृति-सभ्यता, भाषा, एकता, आजादी, संविधान एवं अखंडता
4.	**सफलता पाने के लिए होना चाहिए |**	→ लक्ष्य, त्याग, इच्छा-शक्ति, प्रतिबद्धता, प्रतिभा, एवं सतता
5.	**मरने के बाद इंसान छोडकर जाता हैं |**	→ शरीर, अन-धन, घर-परिवार, नाम, कर्म एवं विचार
6.	**मरने के बाद इंसान को इस धरती पर याद किया जाता हैं उनके**	

➔ नाम, काम, दान, विचार, सेवा-समपर्ण एवं कर्मो से...

आशीर्वाद (बड़े भैया जी)

Mr. RAMASHANKAR KUMAR

मार्गदर्शन एवं सहयोग

Mr. GAUTAM KUMAR

...सोच है जिनकी नई कुछ कर दिखाने की, खोज है रीड संस्था को उन सभी इंसानों की...

"अगर आप भी **Research, Innovation and Discovery** के क्षेत्र में रूचि रखतें हैं एवं अपनी प्रतिभा से दुनियां को कुछ नया देना चाहतें एवं अपनी समस्या का समाधान **RID** के माध्यम से करना चाहतें हैं तो **RID ORGANIZATION (रीड संस्था)** से जरुर जुड़ें" || **धन्यवाद** || **Er. Rajesh Prasad (B.E, M.E)**

Topic Name	Page No:
Computer network overview	4
What is computer network?	5
Types of networks	11
Computer network architecture	16
Network topology	21
Network device	26
Network protocol	48
Port number	53
Transmission mode	11
Digital transmission	56
Osi model	62
Tcp/ip model	80
Tcp vs udp	83
Osi model vs tcp/ip	84
IP address (IPV4, IPV4,SUBNET,SUBNETTING,)	87
MAC (media access control)	99
Domain name and dns	103
Uniform resource locator (url)	107
Domain name system (dns)	108
Internet	112
World wide web (www)	123
Search engine	130
Server	135
Web server	145
Http/https	150
Computer malware(virues, antivirues)	157
Cyber attacks	160
How a web application works.	165
Dynamic host configuration protocol (dhcp) & smtp	166
Ftp, sftp & tftp	167
Pop3 and imap protocols	168
What is RID ?	169

CONTENT

↕

SEARCH ENGINE

↕

BROWSERS

↕

WEB (WWW)

↕

INTERNET

↕

NETWORK

↕

COMPUTER

Definition: - Network is a group of computers which are connected to each other.

Discover: - US DOD, ARPANET (advance Research projects agency networks) in late 1960s & early 1970s

Use: - sharing data from one device to another device. or one place to another place.

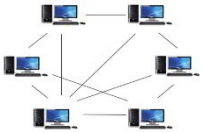
Types: - 1.PAN 2.LAN 3.MAN 4.WAN 5.GAN

Device: - Hardware devices are used to connect or make a network.

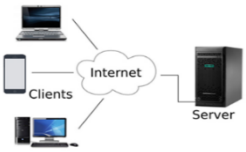
Architecture: - It is physical & logical design of the software, hardware, & protocols.

Types: - 1. Peer-To-Peer network 2. Client/Server network.

Peer-To-Peer network: - all the computers are linked together with equal privilege and responsibilities for processing the data.



Client/server network: - these types of networks are designed for end users called clients, to access the resources from a central computer known as Server.



Components: - NIC, switch, cable, hub, router, and modem.

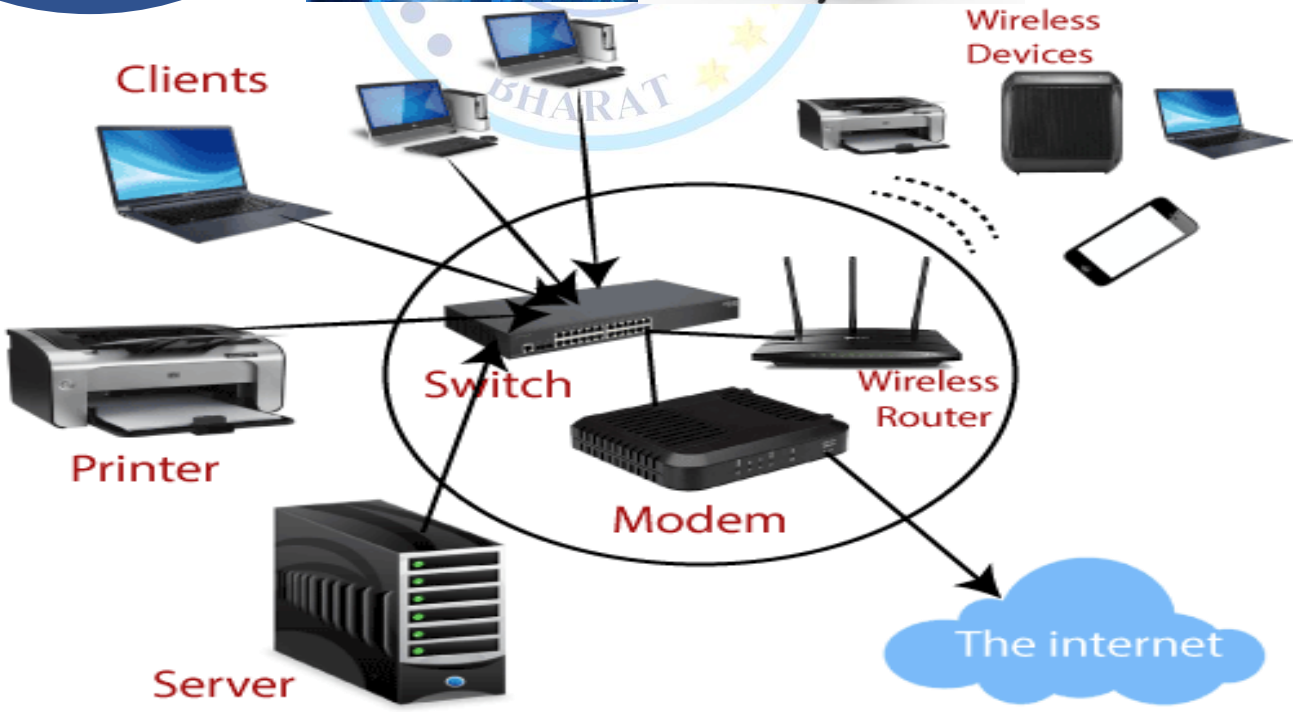
Features: - Data Sharing, Communication Speed, Backup, Scalability, Reliability, & Security

Internet: -it is network of network. Or global System of interconnected computer networks.

Server: - it is a main computer of computer network Or Centralised system, a piece of computer hardware or software program.

NETWORK

"RID संस्था"



Computer network

❖ What is computer network?

- In general, Computer Network is a collection of two or more computers.
- Computer Networking is connecting computers together to enable communication and data exchange between them.

❖ How Does a Computer Network Work?

- A computer network is a system that allows multiple computers to communicate and share resources with each other. Here's a simplified breakdown of how it works:

1. Hardware Components:

- **Nodes:** These are the devices connected to the network, such as computers, printers, servers, routers, switches, etc.
- **Network Interface Cards (NIC):**These are hardware components installed in each device that enable them to connect to the network. NICs provide a unique address called a MAC (Media Access Control) address.
- **Cables or Wireless Connections:** Networks can be wired (using Ethernet cables) or wireless (using technologies like Wi-Fi or Bluetooth) to facilitate communication between devices.

2. Data Transmission:

- Data is transmitted across the network in the form of packets. These packets contain the information being sent, along with addressing information
- When a device wants to send data to another device on the network, it encapsulates the data into packets. These packets are then transmitted through the network.

3. Network Protocols:

- Protocols are a set of rules and conventions that govern how data is transmitted and received over the network. They define things like how data is formatted, addressed, transmitted, routed, and received.

- Common network protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol), HTTP (Hypertext Transfer Protocol), FTP.

4. Network Devices:

- **Routers:**These devices connect multiple networks together and route data between them. They use IP addresses to determine the best path for data to travel.
- **Switches:**Switches are used to connect multiple devices within a single network. They use MAC addresses to determine where to forward data within the network.
- **Hubs:**Hubs are older devices that simply repeat incoming data to all other ports, regardless of the destination. They are not as efficient as switches.
- **Firewalls:**Firewalls are used to enforce security policies by filtering incoming and outgoing network traffic based on predefined rules.

5. Network Topologies:

- Network topology refers to the physical or logical layout of the network. Common topologies include bus, star, ring, mesh, and hybrid topologies.

6. Data Exchange:

- Once the data reaches its destination, it is decapsulated, and the receiving device processes it accordingly. This could involve displaying a web page, printing a document, saving a file, etc.

❖ Basic Terminologies of Computer Networks:

1. **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
2. **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and other devices.
3. **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.
4. **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. common network topologies include bus, star, ring, mesh, and tree.
5. **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
6. **IP Address:** An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
7. **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names into IP addresses that computers can understand.
8. **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

History of computer network

1. Early Networking (1950s-1960s):

- The earliest form of computer networking emerged in the 1950s with the development of mainframe computers. These early networks were primarily used within organizations to facilitate the sharing of computing resources.
- In the 1960s, projects such as the Advanced Research Projects Agency Network (ARPANET) in the United States laid the foundation for modern computer networking. ARPANET, funded by the U.S. Department of Defense, aimed to create a decentralized communication network resilient to nuclear attacks.

2. TCP/IP and Internet (1970s-1980s):

- The 1970s saw the development of key networking protocols, including TCP/IP (Transmission Control Protocol/Internet Protocol), which became the foundation of the internet.
- ARPANET successfully implemented TCP/IP in 1983, marking a significant milestone in evolution of computer networking. This event is often considered the birth of the modern internet.The National Science Foundation Network (NSFNET), established in the mid-1980s, expanded the internet's infrastructure and facilitated academic and research collaboration.

3. Commercialization and World Wide Web (1990s):

- The 1990s witnessed the commercialization and widespread adoption of the internet. The advent of dial-up internet access, broadband technologies, and internet service providers (ISPs) allowed individuals and businesses to connect to the internet.
- Tim Berners-Lee's invention of the World Wide Web in 1989 revolutionized the internet, making it accessible and user-friendly. The web browser, along with technologies such as Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP), enabled easy access to information and services on the internet.

4. Broadband and Wireless Networking (2000s):

- The 2000s saw the proliferation of broadband internet access, offering faster and more reliable connections to users worldwide. Technologies such as Digital Subscriber Line (DSL), cable modem, and fiber-optic internet became prevalent.
- Wireless networking technologies, including Wi-Fi, Bluetooth, and mobile data networks (3G, 4G), experienced significant growth, enabling users to access the internet from a variety of devices, including smartphones, tablets, and laptops.

5. Cloud Computing and Internet of Things (2010s-Present):

- The rise of cloud computing in the 2010s transformed how computing resources are provisioned and accessed. Cloud services offer scalable storage, processing power, and software applications over the internet. The Internet of Things (IoT) emerged as a significant trend, connecting everyday objects and devices to the internet, enabling communication and data exchange between them.
- Networking technologies continue to evolve, with developments in areas such as software-defined networking (SDN), 5G mobile networks, and edge computing shaping the future of computer networking.

❖ What was the main purpose behind the discovery and development of computer networks?

- The main purpose behind the discovery and development of computer networks was to facilitate communication and resource sharing between computers.

1. **Resource Sharing:** One of the primary motivations for creating computer networks was to enable multiple users to share computing resources such as data, storage, and processing power. By connecting computers together, organizations could optimize resource utilization and reduce costs.
2. **Communication:** Computer networks allowed users to communicate with each other, either within organizations or across different locations. Email, instant messaging, and collaborative tools became possible with the advent of computer networks, enhancing communication efficiency and productivity.
3. **Remote Access:** Networks enabled remote access to computing resources and services, allowing users to access information and applications from anywhere with an internet connection. This capability revolutionized the way people work and interact, enabling remote work, telecommuting, and online collaboration.
4. **Data Transfer and Distribution:** Networks facilitated the transfer and distribution of data and information between computers and across geographical locations. This capability is crucial for activities such as file sharing, content distribution, and data synchronization.
5. **Centralized Management:** Networks provided a platform for centralized management of computing resources and services. Administrators could monitor and control network activity, enforce security policies, and perform maintenance tasks more efficiently.
6. **Facilitating Research and Innovation:** Computer networks, such as ARPANET, played a significant role in fostering research and innovation in the field of computing and technology. They provided a platform for collaboration among researchers, leading to the development of new technologies and protocols.
7. **Scalability and Growth:** Networks allowed organizations to scale their computing infrastructure to accommodate growth and changing business needs. With the ability to add more devices and expand network capacity, organizations could adapt to evolving requirements and remain competitive.

- Overall, the main purpose behind the discovery and development of computer networks was to **create a scalable, efficient, and interconnected infrastructure** that enables communication, collaboration, and resource sharing in various domains, including business, education, research, and government.

Advantages, Disadvantages and Uses of Computer Networks

❖ Advantages of Computer Networks:

1. **Resource Sharing:** Users can share hardware devices like printers and storage devices, as well as software applications and data, leading to cost savings and improved efficiency.
2. **Communication:** Networks facilitate seamless communication through email, instant messaging, video conferencing, and collaborative tools, enabling quick and efficient exchange of information.
3. **Centralized Data Management:** Centralized data storage and management simplify data access, backup, and security measures, ensuring consistency and integrity of information.
4. **Remote Access:** Users can access network resources and services from remote locations, enabling flexible work arrangements such as telecommuting and remote collaboration.
5. **Cost Efficiency**: Sharing resources and infrastructure reduces overall costs compared to individual systems, as it eliminates redundancy and optimizes resource utilization.
6. **Scalability:** Networks can easily scale to accommodate growth and changing needs by adding or upgrading hardware components and expanding network capacity.

❖ Disadvantages of Computer Networks:

1. **Security Risks:** Networks are susceptible to security threats such as unauthorized access, data breaches, malware, and phishing attacks.
2. **Dependency on Infrastructure:** Network downtime or failures can disrupt operations and productivity, highlighting the importance of reliable infrastructure and backup systems.
3. **Complexity and Maintenance:** Managing and maintaining network infrastructure requires specialized knowledge and skills, as well as ongoing maintenance & troubleshooting efforts.
4. **Privacy Concerns:** Data transmitted over networks may be intercepted or compromised, raising privacy concerns and necessitating encryption and other security measures.
5. **Bandwidth Limitations:** Network performance may be affected by bandwidth limitations, especially in high-traffic environments, leading to slow data transfer speeds and congestion.
6. **Compatibility Issues:** Ensuring compatibility & interoperability between different hardware & software components can be challenging, particularly in heterogeneous network.

❖ Uses of Computer Networks:

1. **Businesses:** Networks are widely used in businesses for communication, collaboration, resource sharing, and centralized data management, improving efficiency and productivity.
2. **Education:** Educational institutions use networks for online learning, research collaboration.
3. **Government:** Governments use networks for communication, information sharing.
4. **Healthcare:** Networks enable electronic health records (EHRs), telemedicine, medical imaging, and healthcare information exchange.
5. **Entertainment:** Networks support online gaming, streaming media, social networking.
6. **Research and Development:** Networks facilitate collaboration among researchers, scientists, and innovators, enabling data sharing, computational resources access, and collaborative research projects.

TYPES OF NETWORK

- **There are following types of networks.**
  1. LAN(Local Area Network)
  2. PAN(Personal Area Network)
  3. MAN(Metropolitan Area Network)
  4. WAN(Wide Area Network)
  5. GAN(Global Area Network)

1. PAN (Personal Area Network):

- PAN is a network that connects devices within the immediate vicinity of an individual, typically covering an area of a few meters.
- It includes personal devices like smartphones, tablets, laptops, and wearable gadgets.
- PANs often use short-range wireless technologies like Bluetooth or Infrared to enable communication and data exchange between devices.

➢ **Example:** Bluetooth Network

❖ Advantages:

- **Personal connectivity:** PANs provide a convenient way to connect personal devices such as smartphones, tablets, and laptops for data sharing and communication.
- **Mobility:** PANs enable users to maintain connectivity and access resources while on the move, without the need for physical cables.

❖ Disadvantages:

- **Limited range:** PANs have a short-range coverage area, typically a few meters, which restricts their use to close proximity communication.
- **Interference:** PANs may experience interference from other wireless devices operating in the same frequency range, affecting reliability.

❖ **Use:** PANs are used for connecting personal devices like smartphones, tablets, and wearable gadgets, enabling data sharing, wireless audio streaming, and peripheral connectivity.

2. LAN (Local Area Network):

- LAN is a network that connects devices within a limited geographical area, such as a single building, office, or campus.
- It typically uses wired (Ethernet) or wireless (Wi-Fi) technology to facilitate communication and resource sharing among connected devices.
- LANs are commonly used in homes, offices, schools, and small businesses to enable local communication and resource sharing.

➢ **Example:** Office Network

❖ Advantages:

- **High-speed communication:** LANs typically offer fast data transfer speeds, making them suitable for applications like file sharing, video conferencing, and real-time collaboration.
- **Resource sharing:** LANs allow for the centralized sharing of resources such as printers, scanners, and internet connections among multiple users.
- **Easy management:** LANs are relatively easy to set up and manage, especially in small to medium-sized environments.

❖ Disadvantages:

- **Limited coverage:** LANs are restricted to a specific geographic area, typically a single building or campus, which can limit connectivity for remote users or branch offices.
- **Security concerns:** LANs may be susceptible to security threats such as unauthorized access and data breaches if proper security measures are not implemented.

❖ **Use:** LANs are commonly used in homes, offices, schools, and small businesses to facilitate local communication, resource sharing, and internet access.

3. MAN (Metropolitan Area Network):

- MAN is a network that spans a larger geographical area than a LAN but smaller than a WAN, typically covering a city or metropolitan area.
- It provides high-speed connectivity between different locations within the same city, enabling organizations, institutions, and government agencies to share resources and services over a wider area.

Example: Citywide Wi-Fi Network

❖ Advantages:

- **Extended coverage:** MANs cover larger geographic areas than LANs, providing connectivity across cities or metropolitan regions.
- **High-speed communication:** MANs offer fast data transfer speeds, making them suitable for applications like video surveillance, traffic management, and city-wide internet access.

❖ Disadvantages:

- **Cost:** Setting up and maintaining MAN infrastructure can be expensive due to the need for extensive cabling, networking equipment, and infrastructure deployment.
- **Complexity:** MANs require sophisticated network planning, management, and maintenance to ensure reliable operation across multiple locations.

❖ **Use:** MANs are used by telecommunications companies, government agencies, and large organizations to provide city-wide internet access, interconnect branch offices, and support applications like traffic management and public safety.

4. WAN (Wide Area Network):

- WAN is a network that covers a large geographical area, such as a country, continent, or multiple continents.
- It connects LANs, MANs, and other smaller networks over long distances using various communication technologies like leased lines, fiber optics, and satellite links.
- WANs enable organizations and individuals to communicate, access centralized resources, and connect to the internet on a global scale.

➢ **Example:** Internet

❖ Advantages:

- **Global connectivity:** WANs provide connectivity over large geographic areas, allowing organizations to establish communication links between geographically dispersed locations.

- Scalability: WANs can scale to accommodate growing network requirements and support a large number of users and devices.

❖ Disadvantages:

- **Latency:** WANs may experience higher latency compared to LANs due to the longer distances data must travel, impacting real-time communication and application performance.
- **Reliability:** WANs may be prone to connectivity issues, outages, and disruptions caused by factors such as network congestion, equipment failures, and environmental conditions.

❖ Use:

WANs are used by multinational corporations, internet service providers, and telecommunications companies to connect branch offices, data centers, and remote sites, and provide global internet connectivity.

5. GAN (Global Area Network):

- GAN is a network infrastructure that spans across multiple countries or continents, providing connectivity on a global scale.
- It extends its coverage worldwide, enabling seamless communication and data exchange across vast distances.
- GANs incorporate high-speed communication technologies, interconnect various WANs and telecommunications networks, and support access to internet and cloud services on a global scale.

➢ **Example:** Global Satellite Communication Network

❖ Advantages:

- **Worldwide connectivity:** GANs offer global connectivity, allowing seamless communication and data exchange across multiple countries or continents.
- **Access to global resources:** GANs provide access to global resources, services, and information available on the internet, cloud platforms, and international networks.

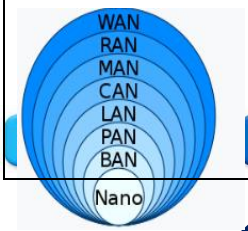
❖ Disadvantages:

- **Complexity:** GANs are complex to design, implement, and manage due to the diverse technologies, protocols, and infrastructure involved in global connectivity.
- **Security challenges:** GANs face significant security challenges, including data privacy, authentication, and protection against cyber threats, given the global scope and interconnected nature of the network.

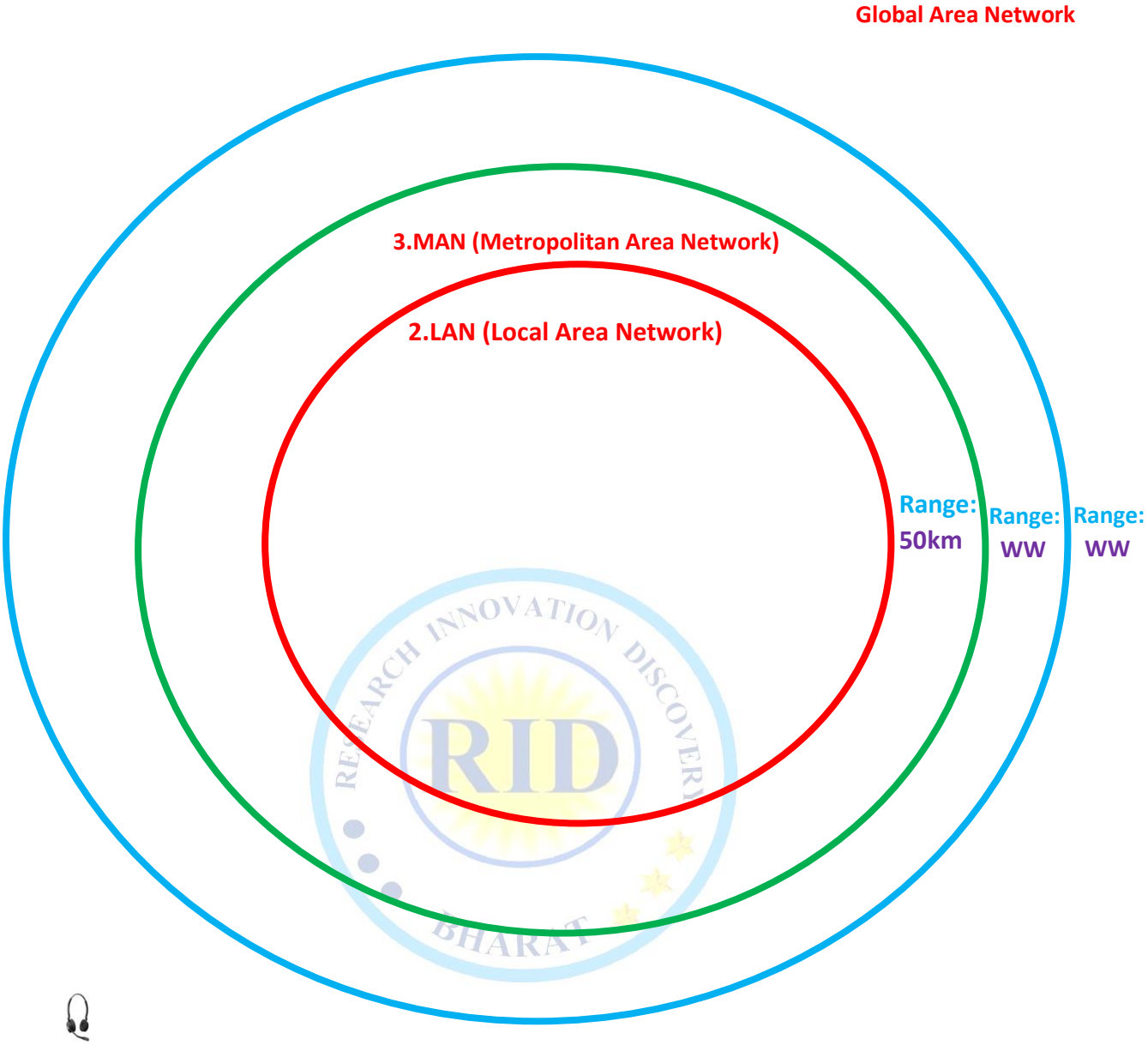
❖ Use:

GANs are used by multinational corporations, global enterprises, research institutions, and internet backbone providers to establish worldwide communication links, support global business operations, and enable international collaboration and data sharing.

❖ Diagram:

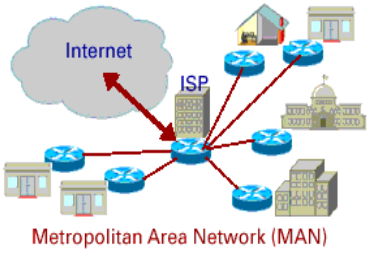


4.WAN (World Area Network)




Personal Area Network

Local Area Network



Metropolitan Area Network (MAN)

World Area Network

Note:

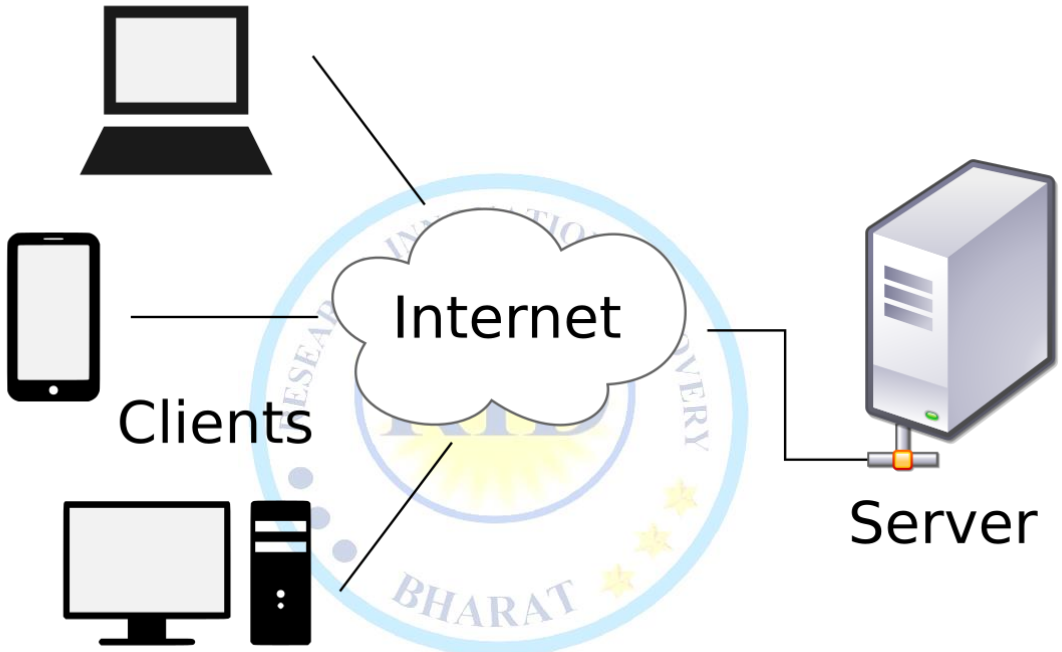
- **Campus Area Network (CAN):** Connects multiple LANs within a university campus, corporate campus, or large office complex. Similar to a MAN but limited to a specific campus area.

- **Storage Area Network (SAN):** Dedicated network that provides access to storage devices like disk arrays and tape libraries to multiple servers. Used for centralized storage management in data centers.
- **Virtual Private Network (VPN):** Secure network connection established over a public network, typically the internet. Used to provide remote access to corporate resources and ensure data privacy and security.
- **Wireless Local Area Network (WLAN):** LAN that uses wireless communication technologies like Wi-Fi to connect devices within a limited area. Provides flexibility and mobility without the need for physical cables.
- **Cellular Network:** Mobile network infrastructure that enables wireless communication between mobile devices and base stations. Used for voice and data communication over large geographic areas.
- **Satellite Network:** Utilizes communication satellites to relay signals between ground stations, providing coverage over wide geographic areas, including remote and rural regions.
- **Intranet:** Private network infrastructure used within an organization to facilitate internal communication, collaboration, and information sharing. Accessed only by authorized users.
- **Extranet:** Extension of an intranet that allows authorized external users, such as business partners or customers, to access specific resources or services over the internet.

COMPUTER NETWORK ARCHITECTURE

- Computer network architecture refers to the layout or structure of a network and how its components are organized and interconnected. There are several types of network architectures.
    1) Client-Server Architecture
    2) Peer-to-Peer (P2P) Architecture
    3) Hierarchical Architecture
    4) Centralized Architecture:
    5) Distributed Architecture

❖ **Diagram:**



- **Example:** A web server hosting a website accessed by multiple clients (web browsers).

❖ **Use:** Commonly used for internet services like email servers, file servers, web servers, and database servers. Provides centralized control, resource management, and security.

❖ Advantages:

- ✓ Centralized management and administration.
- ✓ Scalability and resource sharing.
- ✓ Enhanced security through centralized control.

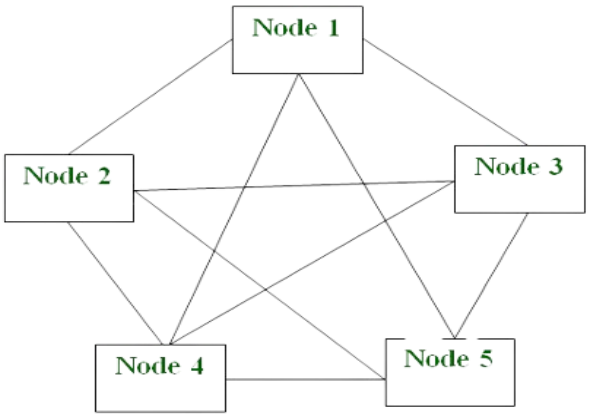
❖ Disadvantages:

- ✓ Dependency on server availability.
- ✓ Potential performance bottlenecks.
- ✓ Higher infrastructure and maintenance costs.

1. Peer-to-Peer (P2P) Architecture:

- In a peer-to-peer network, all devices, or peers, have equal status and can act as both clients and servers.
- Peers communicate directly with each other to share resources, such as files, printers, and internet connections, without the need for a centralized server.
- Each peer contributes its resources to the network and can request resources from other peers.

❖ Daigram:



P2P Architecture

➢ **Example:** File-sharing networks like BitTorrent, where peers directly exchange files without a central server.

❖ Use:

Suitable for decentralized applications such as file sharing, collaborative computing, and distributed content delivery. Enables resource sharing and collaboration among peers without relying on centralized infrastructure.

❖ Advantages:

- ✓ Decentralized architecture with no single point of failure.
- ✓ Scalability and flexibility.
- ✓ Lower infrastructure costs compared to client-server networks.

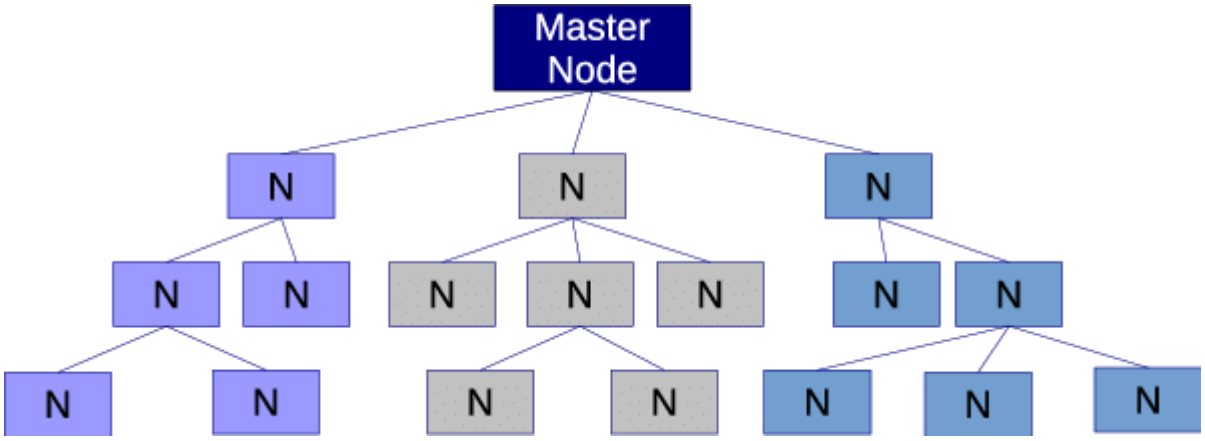
❖ Disadvantages:

- ✓ Lack of centralized management and control.
- ✓ Security concerns due to the difficulty in enforcing access controls.
- ✓ Performance may degrade as the number of peers increases.

2. Hierarchical Architecture:

- Also known as tiered architecture, this design organizes network components into multiple layers or tiers based on their functions and responsibilities.
- Each layer performs specific tasks, such as data transmission, routing, and application services, and communicates with adjacent layers.
- Common hierarchical models include the OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model.

❖ Diagram:



➢ **Example:** The OSI (Open Systems Interconnection) model or TCP/IP (Transmission Control Protocol/Internet Protocol) model, which organize network functions into layers.

❖ **Use:** Provides a structured approach to network design, management, and troubleshooting. Facilitates interoperability, scalability, and modularity in complex network environments.

❖ **Advantages:**

- ✓ Simplified design and management.
- ✓ Modular structure facilitates scalability and flexibility.
- ✓ Clear separation of concerns improves troubleshooting and maintenance.

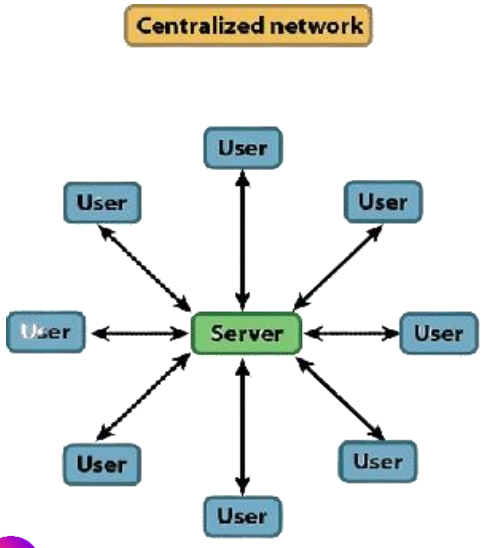
❖ **Disadvantages:**

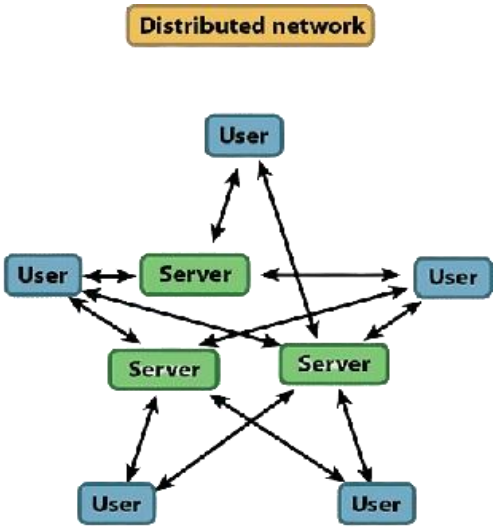
- ✓ Overhead introduced by additional layers.
- ✓ Potential for bottlenecks and latency at layer boundaries.
- ✓ Complexity increases with the number of layers.

3. Centralized Architecture:

- In a centralized network architecture, all network resources and services are hosted on a single central server or mainframe.
- Clients connect to the central server to access resources and perform tasks, such as file storage, processing, and data management.
- This architecture is common in small-scale networks or legacy systems with limited requirements.

❖ **Diagram:**





- **Example:** A small business network with all resources and services hosted on a single central server.

❖ **Use:** Suitable for small-scale environments where simplicity and centralized control are prioritized. Commonly used in legacy systems and basic network setups.

❖ **Advantages:**

- ✓ Simplified management and administration.
- ✓ Control over resource allocation and access.
- ✓ Reduced network complexity.

❖ **Disadvantages:**

- ✓ Single point of failure.
- ✓ Scalability limitations.
- ✓ Performance may degrade as the number of clients increases.

4. Distributed Architecture:

- In a distributed network architecture, network resources and services are distributed across multiple interconnected nodes or servers.
- Each node performs specific tasks independently, and communication between nodes occurs through message passing or distributed protocols.
- Distributed architectures are scalable, fault-tolerant, and resilient to failures, making them suitable for large-scale and mission-critical applications.

- **Example:** Cloud computing platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), where resources are distributed across multiple data centers.

❖ **Use:** Ideal for large-scale applications requiring scalability, fault tolerance, and geographic distribution. Enables efficient resource utilization, high availability, and on-demand scalability.

❖ **Advantages:**

- ✓ Scalability and fault tolerance.
- ✓ Enhanced performance through parallel processing and distributed computing.
- ✓ Geographic distribution improves availability and responsiveness.

❖ **Disadvantages:**

- ✓ Complexity of design and implementation.
- ✓ Increased network traffic and communication overhead.
- ✓ Security challenges in managing distributed resources and data.

Definition: - it is layout of computer. it is show how device and cables are connected to each other.

Types: - 1. Bus 2. Ring 3. Star 4. Mesh 5. Hybrid 6. Tree

1. Bus Topology: - All Nodes/Computer are connected to a single cable.

2. Ring Topology: - Nodes are connected to two or more nodes & thus forming a single continues path for the data transmission.

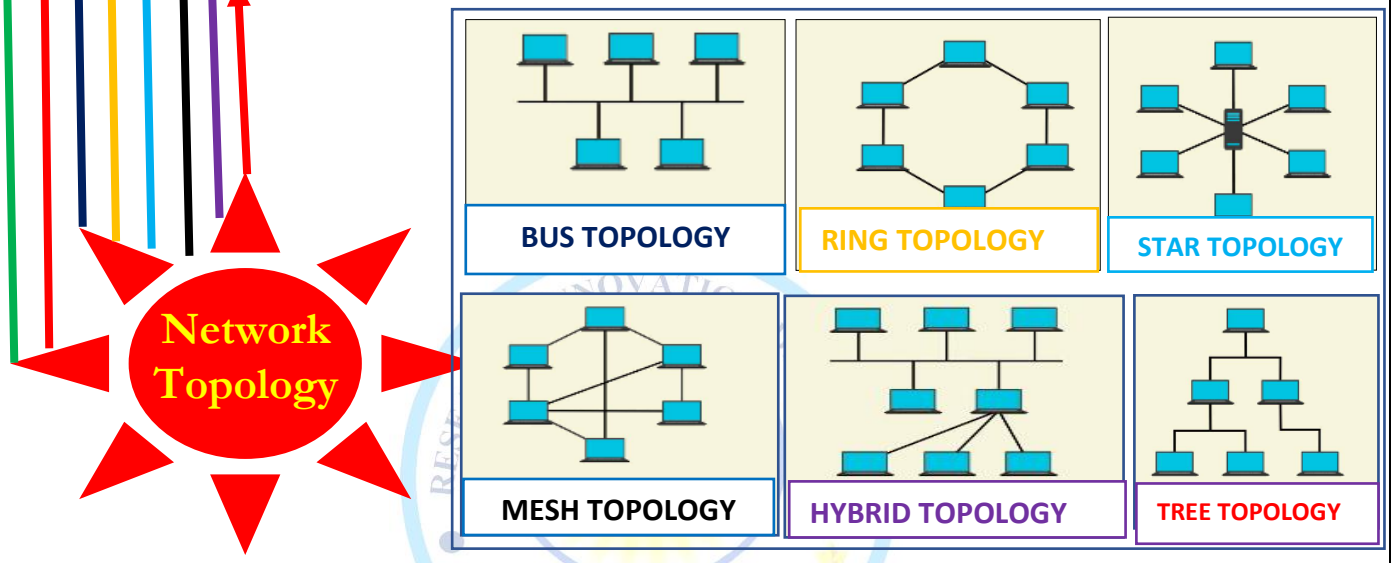
3. Star Topology: - ALL Nodes are connected to a single device known as a central device.

4. Mesh Topology: - ALL Nodes are individually connected to other nodes.

Types: - 1. fully connected 2. Partially connected

5. Hybrid Topology: - Combination of various different topology.

6. Tree Topology: - All the branch of tree are combination of Bus and star topology.



NETWORK TOPOLOGY

➢ **Definition:** Network topology refers to the physical or logical layout of a computer network. It defines how devices are connected and how data flows between them. Network topology describes the arrangement of nodes, links, and communication paths in a network.

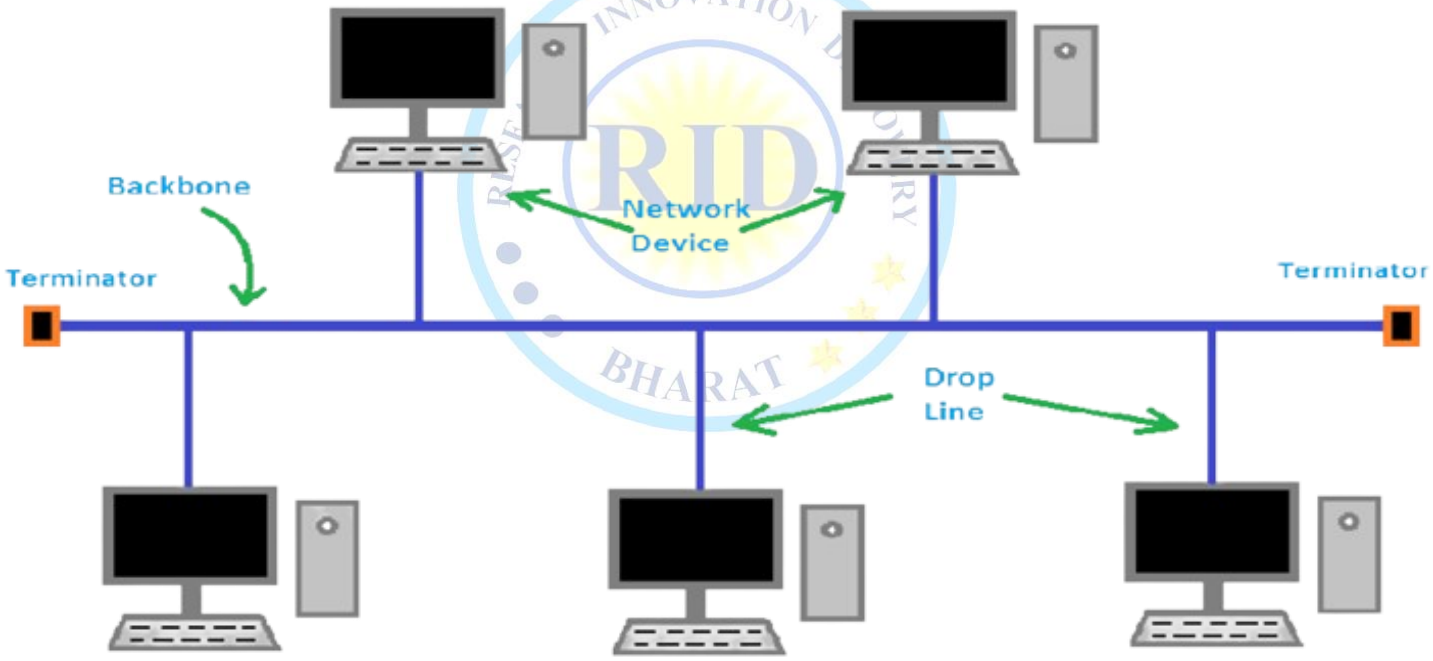
❖ Types of Network Topology:

1) Bus Topology
2) Star Topology
3) Ring Topology
4) Mesh Topology
5) Hybrid Topology

1). Bus Topology:

- In a bus topology, all devices are connected to a single communication line, known as bus.

❖ Diagram:



❖ Advantages:

- ✓ Simple and inexpensive to implement.
- ✓ Requires less cabling than a star topology.
- ✓ Easy to add or remove devices.

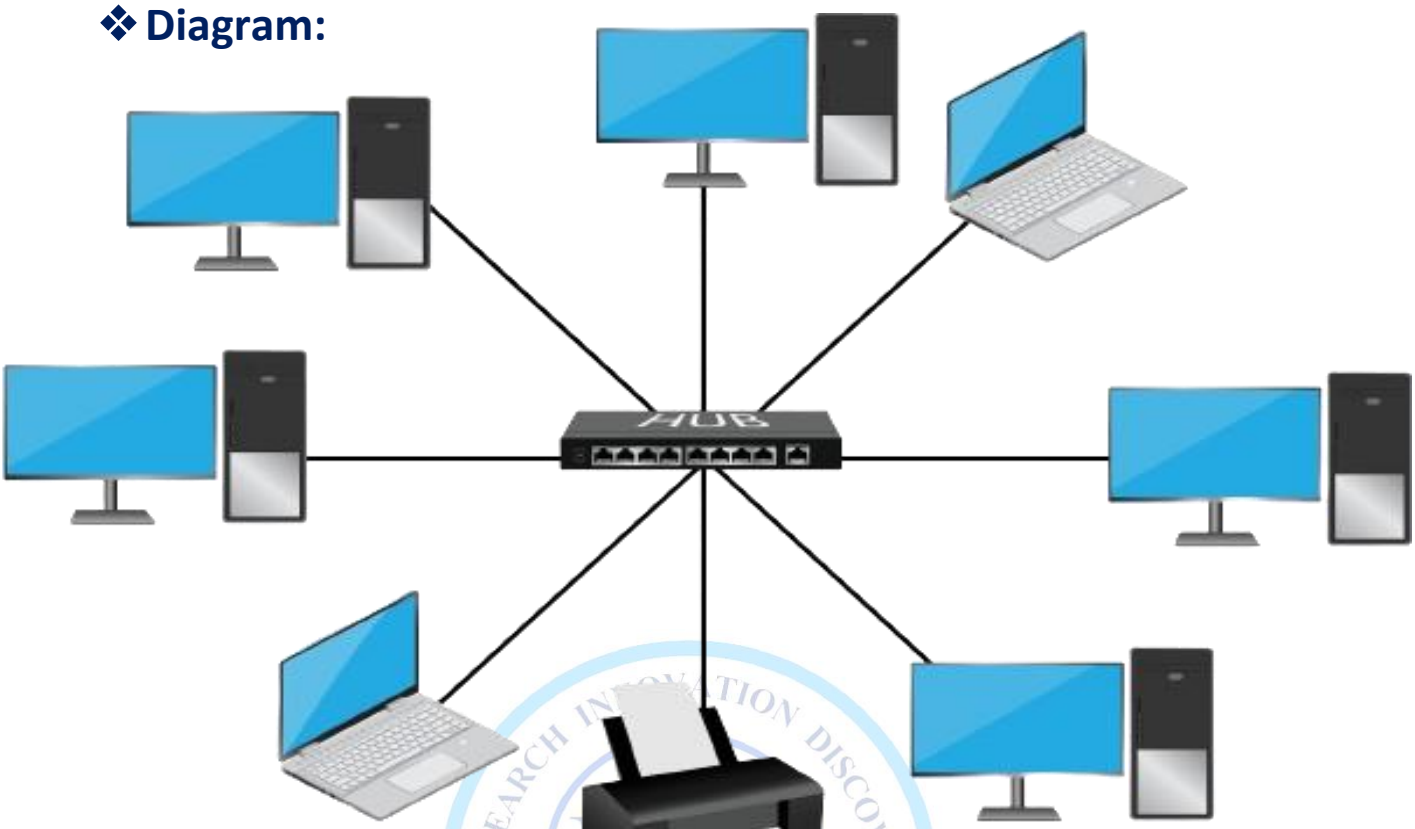
❖ Disadvantages:

- ✓ Single point of failure – failure of the bus disrupts the entire network.
- ✓ Limited scalability.
- ✓ Network performance decreases as more devices are added.

2). Star Topology:

- In a star topology, all devices are connected to a central hub or switch.

❖ Diagram:



❖ Advantages:

- ✓ Easy to set up and manage.
- ✓ Fault isolation – failure of one device does not affect others.
- ✓ Scalable – additional devices can be easily added.

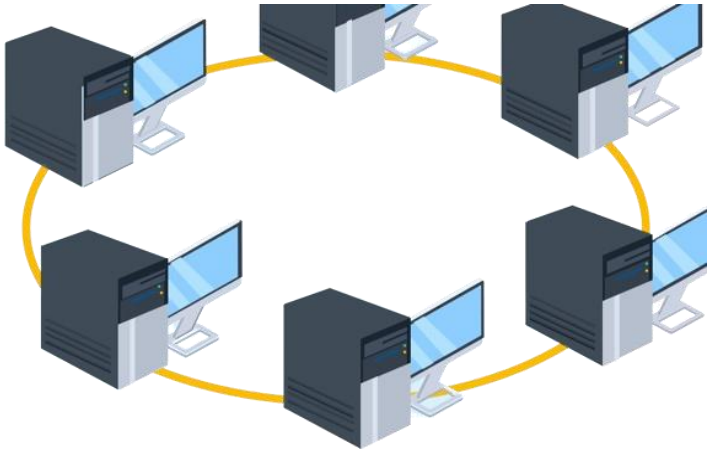
❖ Disadvantages:

- ✓ Dependency on the central hub – failure of the hub disrupts the entire network.
- ✓ Requires more cabling than some other topologies.

3). Ring Topology:

- In a ring topology, each device is connected to exactly two other devices, forming a closed loop.

❖ Diagram:



❖ Advantages:

- ✓ Equal access to resources for all devices.

- ✓ No collisions in data transmission.
- ✓ Easy to install and configure.

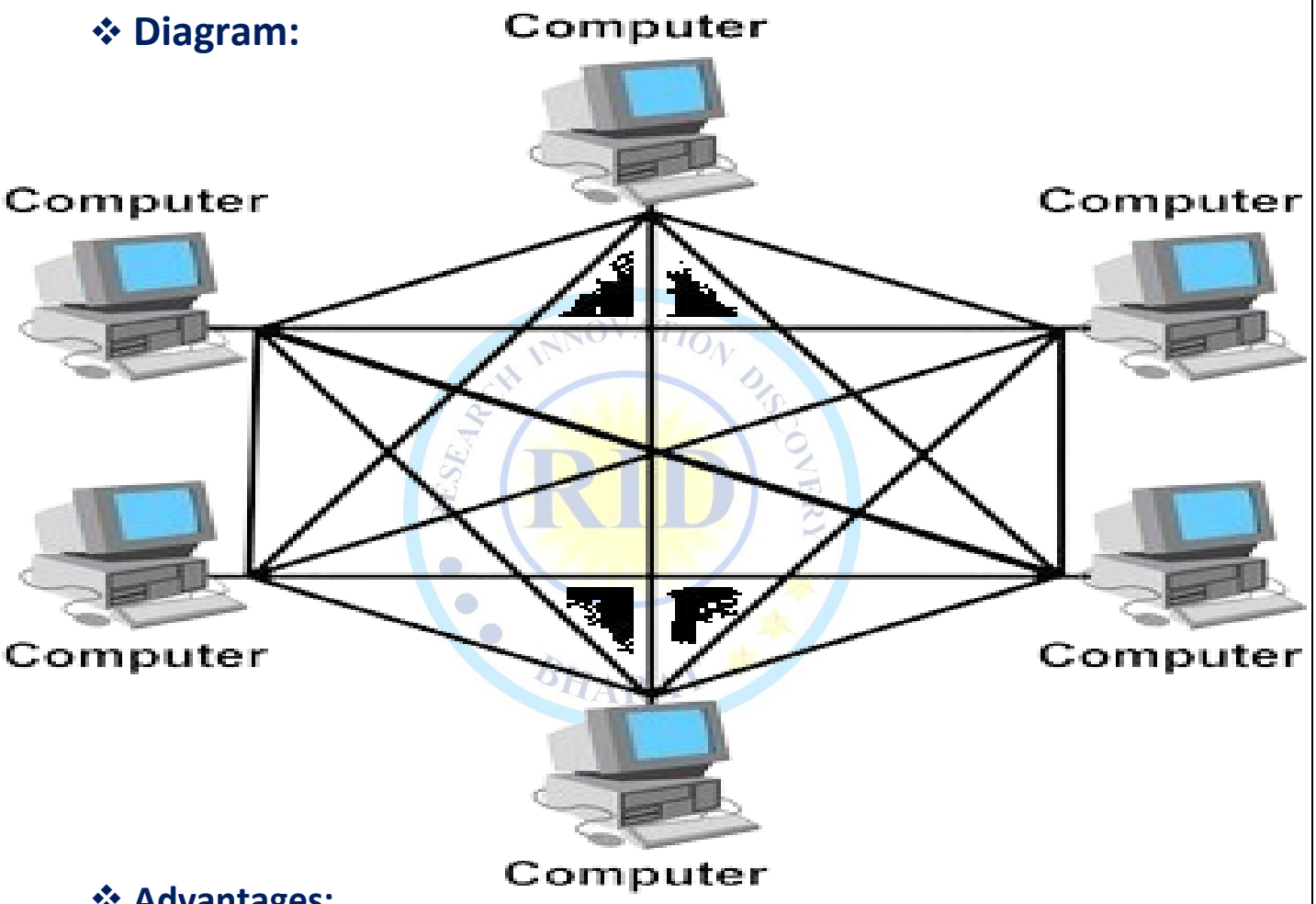
❖ Disadvantages:

- ✓ Single point of failure – failure of one device disrupts the entire network.
- ✓ Limited scalability.
- ✓ Complex to reconfigure or add/remove devices.

4). Mesh Topology:

- In a mesh topology, every device is connected to every other device in the network.

❖ Diagram:



❖ Advantages:

- ✓ Redundancy – multiple paths for data transmission increase reliability.
- ✓ Fault tolerance – failure of one link does not necessarily disrupt communication.
- ✓ Scalability – can easily accommodate additional devices.

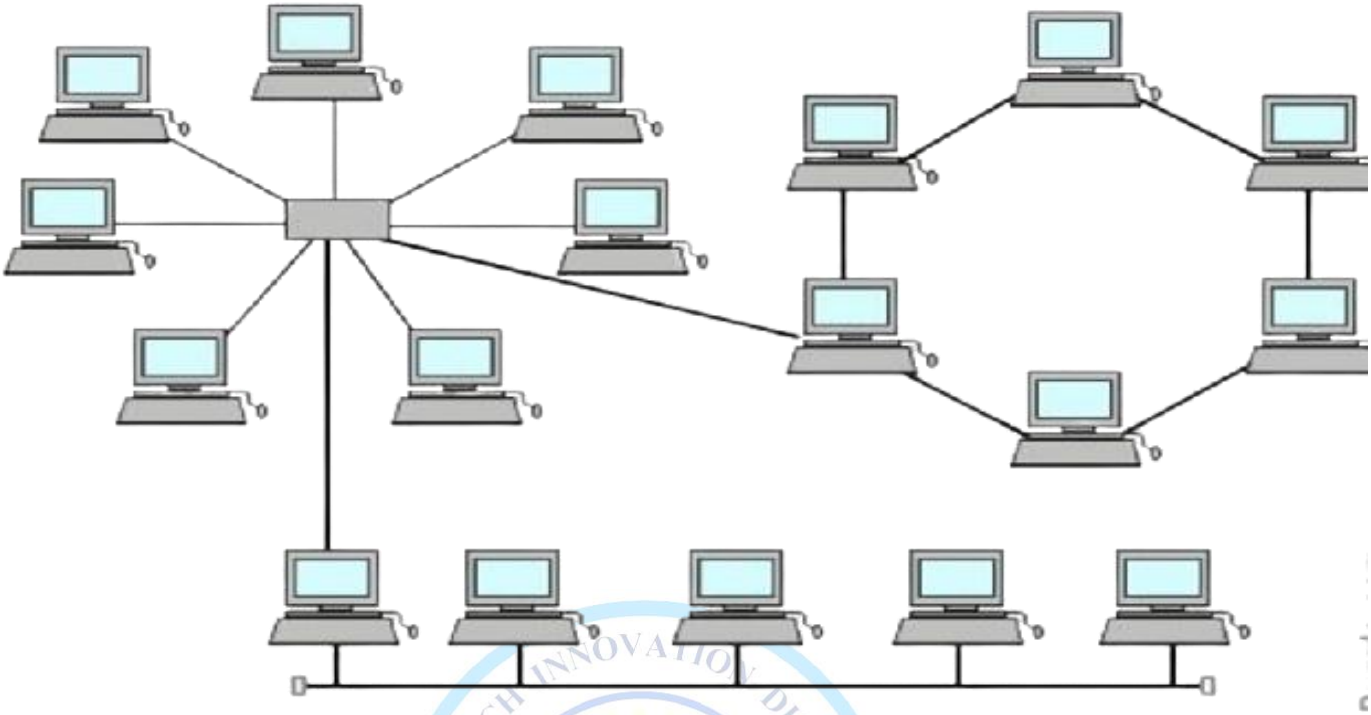
❖ Disadvantages:

- ✓ Expensive to implement due to the large number of connections required.
- ✓ Complex to manage and configure.
- ✓ High maintenance costs.

5). Hybrid Topology:

- A hybrid topology combines two or more basic topologies, such as star-bus, star-ring, or mesh-bus.

❖ Diagram:



❖ **Advantages** and **disadvantages** vary depending on the specific combination of topologies used.

❖ Use:

- Network topology selection depends on factors such as the size of the network, the types of devices connected, communication requirements, scalability needs, budget constraints, and reliability considerations.
- Different topologies are suitable for different scenarios. For example, star topologies are commonly used in small office/home office (SOHO) networks, while mesh topologies are often found in large-scale enterprise networks.

Definition: - Network devices, or networking hardware, are physical devices

use: - Making a Network or it is used to connect to two or more computer.

Ex: - NIC, switch, cable, hub, router, Repeater, Bridge Gateway and modem.

Cable: - it is transmission media used for transmitting a signal.

Types: - 1. Twisted pair cable 2. Coaxial cable 3. Fibre-optic cable

Hub: -it is hardware device that divides network connection among multiple devices.

Types: 1. Active Hub (need Electricity) 2. Passive Hub (Not need electricity)

Features.: - LAN Device, less intelligence (Not Store MAC), Broadcast, port, single Collision Domain, Half-Duplex. Layer-1.

Repeater: - It is a network device. used to Boost up the weak

Bridge: - It is a network device. used to separate LAN into number of sections. Or used to connect multiple LAN network

Features: LAN Device, Intelligent (check source & destination MAC Adress), Filter data Traffic, Reduce Traffic (by separate LAN), Port Number, Bridge Table (port & mac) 2 collision Domain, Half Duplex, First Broadcast then Multicast, Layer-2.

Switch (Multiport Bridge): - it is network device that connects multiple devices on a computer network.

Features: - LAN device, Full duplex mode, Intelligence (Using Port number (8/24/48), MAC address,), CAM Table (Content Accessible Memory), First Broadcast then unicast and multicast (Private Message), Multiple collision Domain, slow [10mbps (Wireless), 100mbps(wired)], Layer-2

Router: - it is an internetworking device which is used to connect both LAN & WAN with an internet connection.

Features: - full-Duplex, No Broadcast, Highly Intelligence [Routing Table [Port Number (2/4/8) & Network ID {Use IP Address}], Works as a traffic Controller, choose congestion free path, connect two dis-similar networks, speed: - Fast 10mbps/100mbps/1gbps/100gbps, Layer-3

Gateway: - It is an interworking network device. used to connect two Dissimilar networks. (Enter Exit Point), Layer Application Layer (OSI Layer:4,5,6)

Modem: - It stands for Modulator/Demodulator. **Modulator**: - Convert Digital to Analog signal **Demodulator**: - Convert Analog to Digital signal

NETWORK DEVICE
"RID संस्था"

NIC

HUB

SWITCH

CABLE

ROUTER

BRIDGE

REPEATER

GATEWAY

NETWORK DEVICE

- Network devices are physical devices that allow hardware on a computer network to interact and communicate with one device to another device. Or
- A network device is any hardware or software component that enables communication between devices in a computer network.

1. Hubs
2. Bridges
3. Repeaters
4. Switches
5. Routers
6. Modems
7. Network Interface Cards (NICs)
8. Wireless Access Points (WAPs)
9. Firewalls
10. Load Balancers
11. Gateways
12. Proxies
13. Network Attached Storage (NAS) devices
14. Network Print Servers
15. Network Cameras
16. Network Switching Fabric
17. Network Taps
18. Network Analyzers
19. Content Delivery Network (CDN) servers
20. Ethernet Extenders

Note: Cables themselves are not considered network devices. Instead, they are the physical medium that facilitates the transmission of data between network devices.

1) **Hubs:** Hubs are basic networking devices that connect multiple Ethernet devices together. They operate at the physical layer of OSI model and broadcast data to all devices connected to them. **Example:** Ethernet hub.
2) **Bridges:** Bridges are devices that connect two separate network segments and manage traffic between them. They operate at the data link layer (Layer 2) of the OSI model. **Example:** Wireless bridge.
3) **Repeaters:** Repeaters are devices used to regenerate and retransmit signals to extend the reach of a network. They amplify signals to compensate for attenuation over long distances. **Example:** Wi-Fi range extender.
4) **Switches:** Switches are devices that connect multiple devices within a local area network (LAN) and intelligently forward data only to the intended recipient based on MAC addresses. They operate at the data link layer (Layer 2) of the OSI model. **Example:** Ethernet switch.
5) **Routers:** Routers are devices that connect multiple networks together and determine the optimal path for data packets to reach their destination across interconnected networks based on IP addresses. They operate at the network layer (Layer 3) of the OSI model. **Example:** Wireless router.
6) **Modems:** Modems are devices that convert digital data from a computer into analog signals for transmission over analog communication lines (such as telephone lines) and vice versa. **Example:** Cable modem.

7) **Network Interface Cards (NICs):** NICs are hardware devices that allow computers and other network-enabled devices to connect to a network. They translate data between the computer's internal bus and the network's transmission medium. Example: Ethernet network adapter.
8) **Wireless Access Points (WAPs):** WAPs are devices that enable wireless devices to connect to a wired network using Wi-Fi technology. They transmit data wirelessly to Wi-Fi-enabled devices. **Example:** Wi-Fi access point.
9) **Firewalls:** Firewalls are security devices that control and monitor incoming and outgoing network traffic based on predetermined security rules to protect networks from unauthorized access and threats. **Example:** Hardware firewall appliance.
10) **Load Balancers:** Load balancers distribute incoming network traffic across multiple servers or network resources to ensure optimal utilization, reliability, and performance. **Example:** Application delivery controller (ADC).
11) **Gateways:** Gateways are devices that connect different types of networks together and facilitate communication between them by converting data formats or protocols. **Example:** Internet gateway.
12) **Proxies:** Proxies are intermediary servers that act on behalf of clients to access resources from other servers. They can provide security, anonymity, and caching benefits. **Example:** Web proxy server.
13) **Network Attached Storage (NAS) devices:** NAS devices are dedicated file storage devices that provide centralized data storage and file sharing services to network users and devices. **Example:** Synology DiskStation.
14) **Network Print Servers:** Print servers are devices that manage and facilitate printing tasks on a network by connecting printers to the network and processing print jobs. **Example:** HP Jetdirect print server.
15) **Network Cameras:** Network cameras, also known as IP cameras, are surveillance cameras that transmit video and audio data over a network, allowing for remote monitoring and recording. **Example:** Axis Communications network camera.
16) **Network Switching Fabric:** Network switching fabric refers to the internal architecture of a network switch that handles the forwarding of data packets between ports efficiently. **Example:** Cisco Nexus series switches.
17) **Network Taps:** Network taps are passive monitoring devices that capture and copy network traffic flowing between network devices for analysis and monitoring purposes. **Example:** Gigamon G-TAP.
18) **Network Analyzers:** Network analyzers are software or hardware tools used to capture, analyze, and troubleshoot network traffic to diagnose network performance issues and security threats. **Example:** Wireshark.
19) **Content Delivery Network (CDN) servers:** CDN servers are distributed network infrastructure that delivers web content to users based on their geographic location, reducing latency and improving website performance. **Example:** Akamai CDN.
20) **Ethernet Extenders:** Ethernet extenders are devices used to extend Ethernet connections beyond the standard distance limitations by utilizing existing copper wiring infrastructure. **Example:** Patton Ethernet extender.

HUB

- A hub is a basic network device that connects multiple Ethernet devices within a local area network (LAN). It operates at the physical layer (Layer 1) of the OSI model and simply broadcasts data received from one port to all other ports.
- Hubs are considered outdated technology and have largely been replaced by switches, which offer better performance and efficiency.

❖ Types of Hubs:

- There are following types of Hubs.
    1) Passive Hub.
    2) Active Hub
    3) Intelligent Hub

1. **Passive Hub:** Also known as a non-powered hub, it simply serves as a connection point for devices without any signal regeneration. Data received on one port is broadcasted to all other ports without any amplification.
2. **Active Hub:** Also called a powered hub, it regenerates signals before transmitting them to all connected ports. This helps in overcoming signal degradation and extending the network distance.
3. **Intelligent Hub:** It works like an active hub 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.

❖ Features of Hub:

1) **LAN Device:** Hubs are used within Local Area Networks (LANs) to connect multiple devices together, such as computers, printers, and servers.
2) **Less Intelligence (Not Store MAC):** Hubs operate at a basic level and do not possess the intelligence to store MAC addresses or make decisions based on them. They simply forward incoming data to all connected devices.
3) **Broadcast:** Hubs broadcast data packets to all connected devices indiscriminately, regardless of whether the data is intended for a specific device or not.
4) **Port:** A hub typically has multiple ports (e.g., 4, 8, 16 ports) to connect multiple devices. Each port functions as a connection point for a network device.
5) **Single Collision Domain:** Hubs create a single collision domain, meaning that all devices connected to the hub share the same network bandwidth and collisions can occur if multiple devices attempt to transmit data simultaneously.
6) **Half-Duplex:** Hubs operate in half-duplex mode, which means that data transmission can occur in only one direction at a time. Devices connected to a hub cannot transmit and receive data simultaneously.
7) **Layer-1:** Hubs operate at the physical layer (Layer 1) of the OSI model, primarily dealing with the transmission of raw data signals over the physical medium (such as Ethernet cables).

❖ Advantages of Hubs:

- ✓ **Simple Setup:** Hubs are easy to install and require minimal configuration.
- ✓ **Inexpensive:** Hubs are usually cheaper than switches, making them a cost-effective option for small networks.
- ✓ **No Addressing Required:** Since hubs broadcast data to all connected devices, there's no need for MAC address tables or packet forwarding logic.

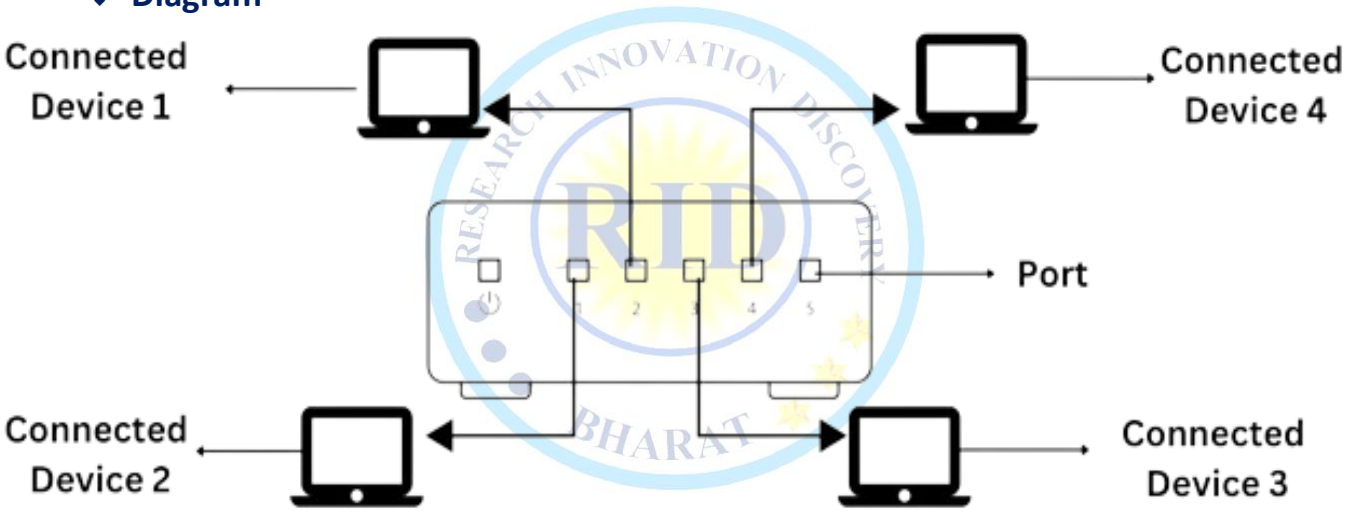
❖ Disadvantages of Hubs:

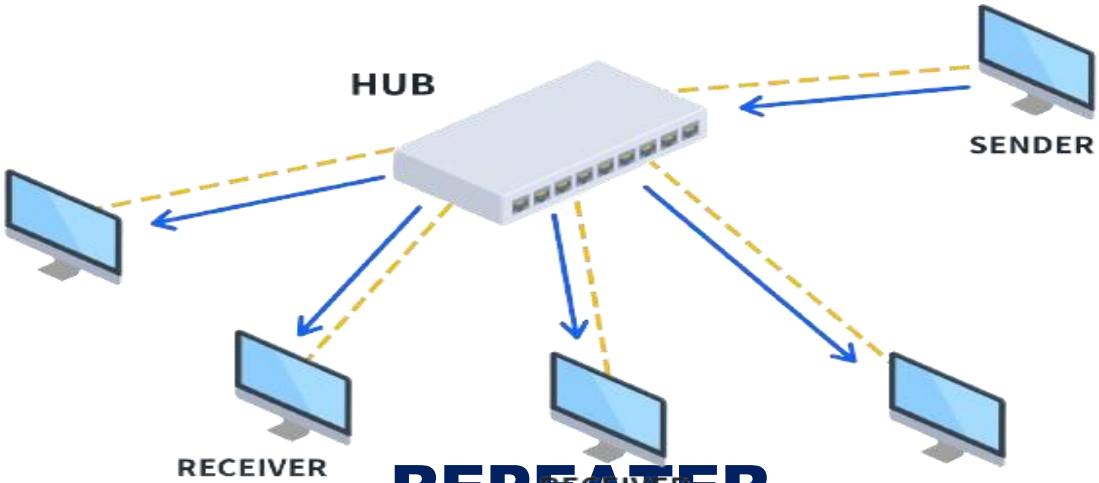
- ✓ **Limited Bandwidth:** Hubs share the total available bandwidth among all connected devices, leading to congestion and reduced network performance as the number of devices increases.
- ✓ **High Collision Rate:** In shared Ethernet networks, collisions occur when two devices transmit data simultaneously, leading to data retransmissions and decreased network efficiency.
- ✓ **Security Risks:** Since data is broadcasted to all devices, it's easier for attackers to capture sensitive information by sniffing network traffic.
- ✓ **Limited Scalability:** Hubs cannot segment network traffic like switches, leading to broadcast storms and network congestion as the network grows larger.

❖ Uses and Examples of Hubs:

- ➢ Hubs are rarely used in modern networking environments due to their limitations. However, they may still be found in legacy systems or in specific scenarios where simplicity and cost are prioritized over performance and security.
- ❖ **Example:** of a hub is the "NETGEAR FS105 5-Port Fast Ethernet Unmanaged Switch". This is a simple 5-port hub that provides basic connectivity for small networks or home setups. It operates at 10/100 Mbps and does not offer any advanced features like VLAN support or QoS (Quality of Service).

❖ Diagram





REPEATER

➢ A repeater is a network device used to extend the reach of a network by regenerating and retransmitting signals. It operates at the physical layer (Layer 1) of the OSI model and is primarily used to compensate for signal attenuation over long distances in wired communication systems.

❖ Definition:

- A repeater is a simple networking device that receives signals from one network segment, amplifies them, and retransmits them to another network segment. Its primary function is to regenerate the original signal to maintain its strength and quality over extended distances.

❖ Types of Repeaters:

- There are two main types of repeaters:
  1. **Analog Repeaters:** Analog repeaters regenerate analog signals by amplifying them to compensate for signal loss over long distances. They are commonly used in analog communication systems such as telephone networks.
  2. **Digital Repeaters:** Digital repeaters regenerate digital signals by reshaping and retransmitting them. They are used in digital communication systems such as Ethernet networks.

❖ Advantages:

- ✓ **Signal Regeneration:** Repeaters regenerate signals, ensuring that they maintain their strength and quality over long distances.
- ✓ **Simple Operation:** Repeaters are simple devices with no configuration required, making them easy to install and maintain.
- ✓ **Cost-Effective:** Repeaters are often more cost-effective than alternative solutions for extending network reach over long distances.

❖ Disadvantages:

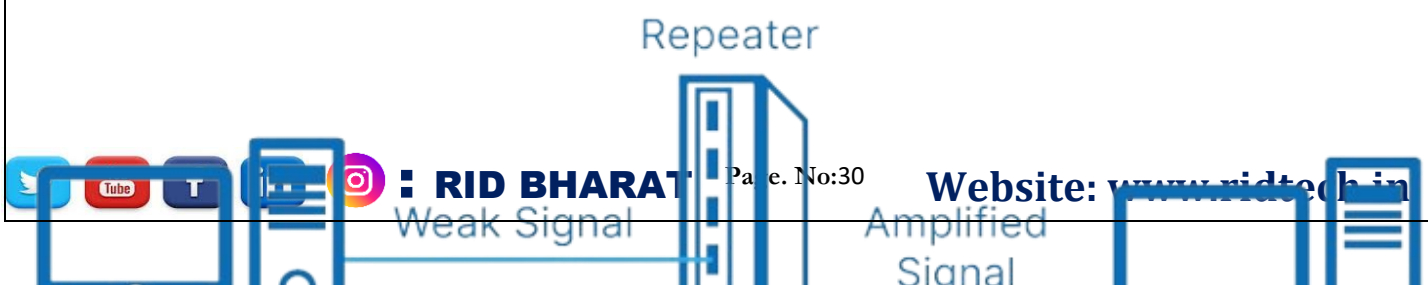
- ✓ **Limited Range:** Repeaters can only extend the reach of a network to a certain extent and are limited by factors such as signal degradation and noise.
- ✓ **Signal Amplification Only:** Repeaters amplify both the signal and any noise present in the network, which can degrade signal quality if excessive noise is present.
- ✓ **Not Suitable for All Situations:** Repeaters are not suitable for all network scenarios, particularly in environments with high levels of interference or where longer distances need to be covered.

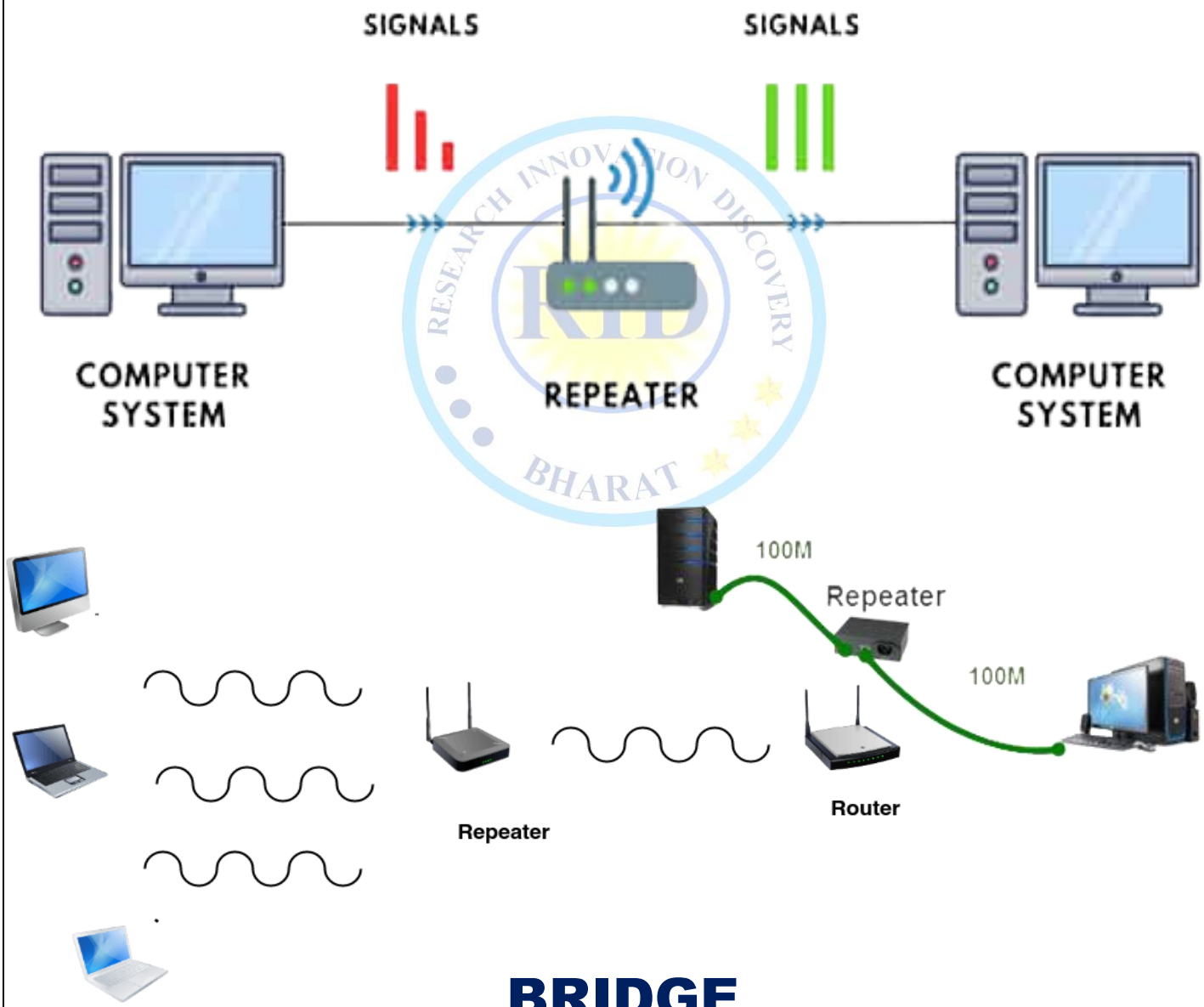
❖ Uses:

- **LAN Extensions:** Repeaters are commonly used to extend the reach of local area networks (LANs) beyond the standard distance limitations of Ethernet cables.
- **Telecommunications:** Repeaters are used in telecommunications networks, such as telephone systems, to amplify signals for transmission over long distances.
- **Fiber Optic Networks:** Repeaters are used in fiber optic networks to regenerate optical signals for long-distance transmission.

❖ Example:

- Example of a repeater is the Cisco RE1000 Range Extender, which is used to extend the range of wireless networks by receiving and retransmitting Wi-Fi signals. It operates by amplifying the signals received from the wireless router and rebroadcasting them to areas with weak or no coverage, effectively extending the reach of the wireless network.

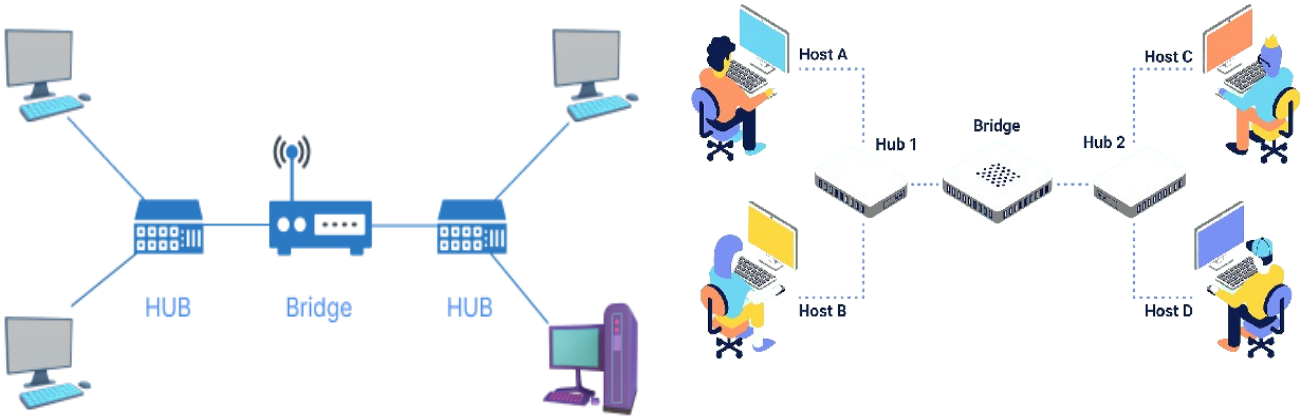



SIGNALS
SIGNALS
COMPUTER SYSTEM
REPEATER
COMPUTER SYSTEM
100M
Repeater
100M
Repeater
Router

BRIDGE

- A bridge is a network device that connects multiple network segments or LANs (Local Area Networks) together and forwards traffic between them based on MAC (Media Access Control) addresses. It operates at the Data Link layer (Layer 2) of the OSI model and makes forwarding decisions by examining the destination MAC address of each incoming frame.

❖ Diagram:



❖ Features of Bridge:

- There are following features of bridg.

1. LAN Device:

- Bridges are LAN devices that operate at the Data Link layer (Layer 2) of the OSI model.
- They connect multiple LAN segments together to form a single logical network.
- Intelligent (Check Source & Destination MAC Address):
- Bridges are intelligent devices that examine the source and destination MAC addresses of incoming frames.
- They use this information to make forwarding decisions and selectively forward frames to the appropriate network segment.

2. Filter Data Traffic:

- Bridges filter out unnecessary data traffic by examining the destination MAC address of each frame.
- They forward frames only to the network segment where the destination device resides, reducing unnecessary transmission.
- Reduce Traffic (by Separate LAN):
- Bridges help reduce network congestion and improve overall network performance by dividing a large network into smaller LAN segments.
- Each LAN segment has its own collision domain, reducing the likelihood of collisions and improving data transmission efficiency.

3. Port Number:

- Bridges have multiple ports, each connected to a separate LAN segment.
- Ports allow bridges to receive and transmit data frames between different network segments.
- Bridge Table (Port & MAC):
- Bridges maintain a bridge table, also known as a MAC address table, that maps MAC addresses to the corresponding port on the bridge. This table is used to make forwarding decisions and determine the appropriate port for transmitting frames.

4. Collision Domain:

- Bridges create separate collision domains for each LAN segment connected to them.
- This helps reduce collisions and network congestion, improving overall network performance.

5. Half Duplex:

- Bridges operate in half-duplex mode, meaning they can either transmit or receive data at any given time, but not both simultaneously.
- This mode of operation helps avoid collisions and ensures smooth data transmission.

6. First Broadcast then Multicast:

- Bridges initially broadcast incoming frames to all network segments except the one they were received on.
- Once the destination MAC address is learned, subsequent frames destined for the same device are forwarded only appropriate segment, reducing unnecessary broadcast traffic.

7. Layer-2:

- Bridges operate at the Data Link layer (Layer 2) of the OSI model.
- They forward frames based on MAC addresses and do not inspect higher-layer protocol information.

❖ Advantages:

- ✓ Segmentation: Bridges divide large networks into smaller segments, improving overall network performance and reducing collision domains.
- ✓ Traffic Control: Bridges effectively control network traffic by forwarding frames only to the relevant segments, optimizing bandwidth usage.
- ✓ Improved Reliability: Bridges enhance network reliability by isolating network segments, reducing the impact of failures or network congestion.
- ✓ Scalability: Bridges can be easily added to expand network capacity without disrupting existing network infrastructure.

❖ Disadvantages:

- ✓ Limited Coverage: Bridges operate at the Data Link layer and can only connect LANs within the same broadcast domain.
- ✓ Configuration Complexity: Managing bridges and ensuring proper configuration across multiple network segments can be complex.
- ✓ Potential Bottlenecks: In large networks, bridges may become bottlenecks if not properly managed, leading to performance issues.
- ✓ Single Point of Failure: A bridge failure can disrupt communication between network segments connected through it.

❖ Use and Example:

- Use: Bridges are commonly used in Ethernet networks to connect LAN segments and extend network coverage.

➢ **Example:** In a corporate office building, separate LAN segments may be set up on each floor. Bridges can connect these segments, allowing devices on different floors to communicate while keeping local traffic contained within each floor's segment.

❖ Types of Bridge:

- Bridges can be classified into different types based on various factors such as their functionality, deployment, and implementation.

1. Transparent Bridge:

- Transparent bridges are the most common type of bridge used in Ethernet networks.
- They operate transparently and make forwarding decisions based on MAC addresses without requiring any configuration.
- Transparent bridges dynamically learn MAC addresses by examining source addresses in incoming frames and maintain a bridge table to facilitate forwarding.

2. Source-Route Bridge (SRB):

- Source-Route Bridges are older bridge models primarily used in Token Ring networks.
- They use source routing information contained within data frames to determine the path a frame should take through the network.
- Unlike transparent bridges, SRBs rely on explicit routing information specified within the frame headers.

3. Remote Bridge:

- Remote bridges connect LAN segments located at geographically distant locations.
- They extend network connectivity over long distances, typically using telecommunications links such as leased lines or broadband connections.
- Remote bridges facilitate communication between remote LANs, enabling users in different locations to access shared resources and services.

4. Wireless Bridge:

- Wireless bridges, also known as wireless LAN (WLAN) bridges or wireless access points, connect wired and wireless network segments.
- They enable wireless devices to communicate with devices on the wired network and vice versa.
- Wireless bridges use radio frequency signals to transmit data between network segments, providing flexibility and mobility.

5. Managed Bridge:

- Managed bridges are equipped with management features and capabilities for configuration, monitoring, and control.
- They allow network administrators to centrally manage and optimize bridge operation, monitor network performance, and troubleshoot issues.
- Managed bridges often support features such as VLAN (Virtual LAN) configuration, spanning tree protocol (STP), and quality of service (QoS) settings.

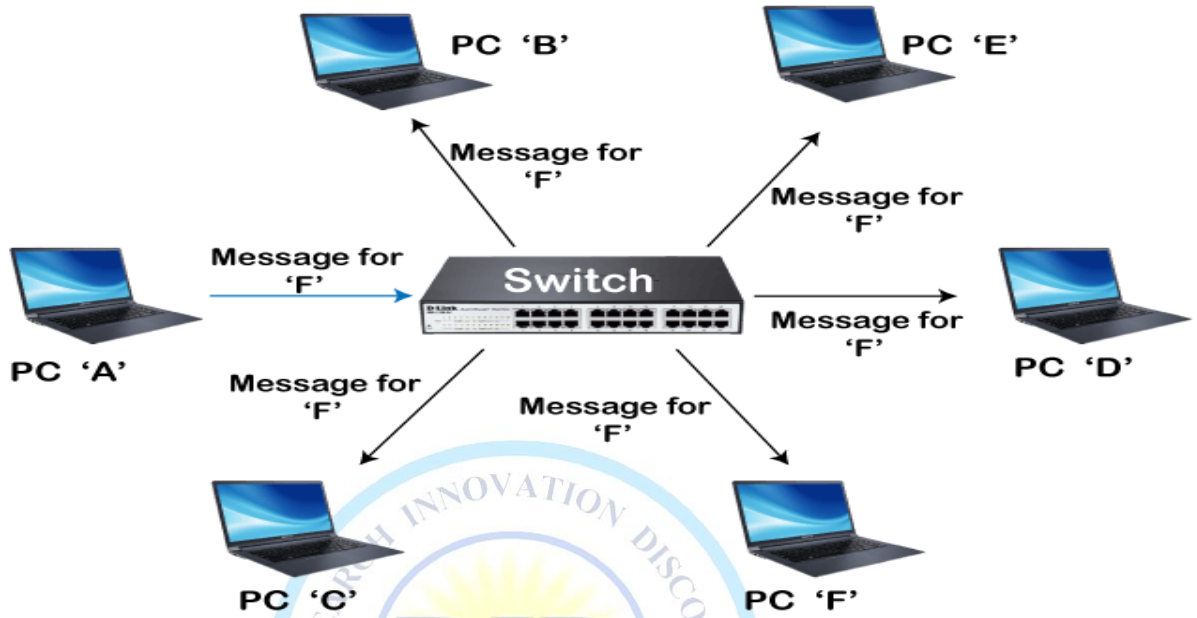
6. Software Bridge:

- Software bridges are implemented in software and run on general-purpose computing devices such as servers or routers.
- They use software-based algorithms to forward traffic between network segments, typically within the same device.
- Software bridges are commonly used in virtualized environments, where they facilitate communication between virtual machines (VMs) or network segments hosted on the same physical server.

SWITCH

- A switch is a networking device that connects multiple devices on a Local Area Network (LAN) and forwards data packets between them based on their Media Access Control (MAC) addresses. It operates at the Data Link layer (Layer 2) of the OSI model and uses MAC address tables to make forwarding decisions, enabling efficient communication within a network.

❖ Diagram:



❖ Features of switch:

1. LAN Device:

- A switch is a Local Area Network (LAN) device used to connect multiple devices within a network.
- It serves as a central point of connectivity, allowing devices such as computers, printers, servers, and other networking equipment to communicate with each other.

2. Full Duplex Mode:

- Switches operate in full-duplex mode, enabling simultaneous transmission and reception of data on each port.
- In full-duplex mode, devices can send and receive data at the same time, effectively doubling the available bandwidth and reducing latency compared to half-duplex communication.

3. Intelligence (Using Port Number, MAC Address):

- Switches are intelligent devices that use port numbers and Media Access Control (MAC) addresses to make forwarding decisions.
- Each port on a switch is assigned a unique number, and the switch maintains a table associating MAC addresses with their corresponding port numbers.
- By examining the destination MAC address of incoming frames, the switch determines the appropriate outgoing port to forward the data packet.

4. CAM Table (Content Addressable Memory):

- The Content Addressable Memory (CAM) table, also known as the MAC address table, is a critical component of a switch's operation.
- It stores MAC address/port mappings, allowing the switch to quickly look up the destination port for incoming data packets.

- The CAM table is dynamically updated as devices communicate on the network, ensuring accurate and efficient packet forwarding.

5. First Broadcast then Unicast and Multicast (Private Message):

- Upon receiving a broadcast frame, switches forward the frame to all ports except the incoming port.
- Once the source MAC address is learned, subsequent frames destined for the same device are forwarded only to the appropriate port, reducing unnecessary broadcast traffic.
- Unicast and multicast frames are forwarded directly to the intended destination port, optimizing network bandwidth and efficiency.

6. Multiple Collision Domains:

- Switches create separate collision domains for each port, isolating collisions to individual segments of the network.
- By segmenting the network into multiple collision domains, switches minimize network congestion and improve overall performance.

7. Speed Options (10Mbps for Wireless, 100Mbps for Wired):

- Switches support different speed options to accommodate the varying requirements of connected devices.
- Wireless connections typically operate at slower speeds, such as 10Mbps, while wired Ethernet connections offer faster speeds, typically up to 100Mbps or higher.
- The choice of speed depends on factors such as network topology, device capabilities, and performance requirements.

8. Layer-2 Functionality:

- Switches operate at the Data Link layer (Layer 2) of the OSI model, where they forward data frames based on MAC addresses.
- They do not inspect the contents of higher-layer protocols (e.g., IP addresses), focusing solely on efficient packet forwarding within the local network segment.

❖ Types of switch:

1. Unmanaged Switch:

- Unmanaged switches are basic switches that operate without any configuration or management capabilities.
- They are plug-and-play devices, making them easy to install and use.
- Unmanaged switches are suitable for small-scale deployments or home networks where simplicity and cost-effectiveness are prioritized.

2. Managed Switch:

- Managed switches offer advanced management features and capabilities, allowing network administrators to configure, monitor, and optimize network performance.
- They provide granular control over network traffic, Quality of Service (QoS) settings, VLAN configuration, and security features.

❖ Advantages:

1. Efficient Data Transmission:

- Switches use MAC address tables to forward data packets directly to the intended destination device, reducing unnecessary broadcast traffic and improving overall network efficiency.

2. Scalability:

- Switches support multiple ports, allowing them to accommodate a growing number of network devices and users.
- They offer flexibility for network expansion and can be easily upgraded or replaced to meet evolving business needs.

3. **Segmentation:**
   - Switches divide the network into multiple collision domains, preventing collisions and congestion and improving data transmission performance.
   - VLANs can be configured on managed switches to further segment network traffic and enhance security and performance.
4. **Increased Bandwidth:**
   - Switches provide dedicated bandwidth to each connected device, allowing simultaneous communication between multiple devices without affecting network performance.
   - This results in higher throughput and faster data transfer rates compared to shared-media networks like hubs.
5. **Improved Security:**
   - Managed switches offer security features such as access control lists (ACLs), port security, and MAC address filtering to control access to the network and protect against unauthorized access and attacks.

❖ Disadvantages:

1. **Cost:**
   - Managed switches are generally more expensive than unmanaged switches due to their advanced features and capabilities.
   - The initial investment and ongoing maintenance costs may be prohibitive for small businesses or home users.
2. **Complexity:**
   - Managed switches require configuration and management by skilled network administrators.
   - The complexity of configuring VLANs, QoS settings, and security features may pose challenges for inexperienced users.
3. **Single Point of Failure:**
   - Like any network device, switches are susceptible to hardware failures or software glitches.
   - A failure in a critical switch can disrupt communication within the network until the issue is resolved or the switch is replaced.

❖ Use and Example:

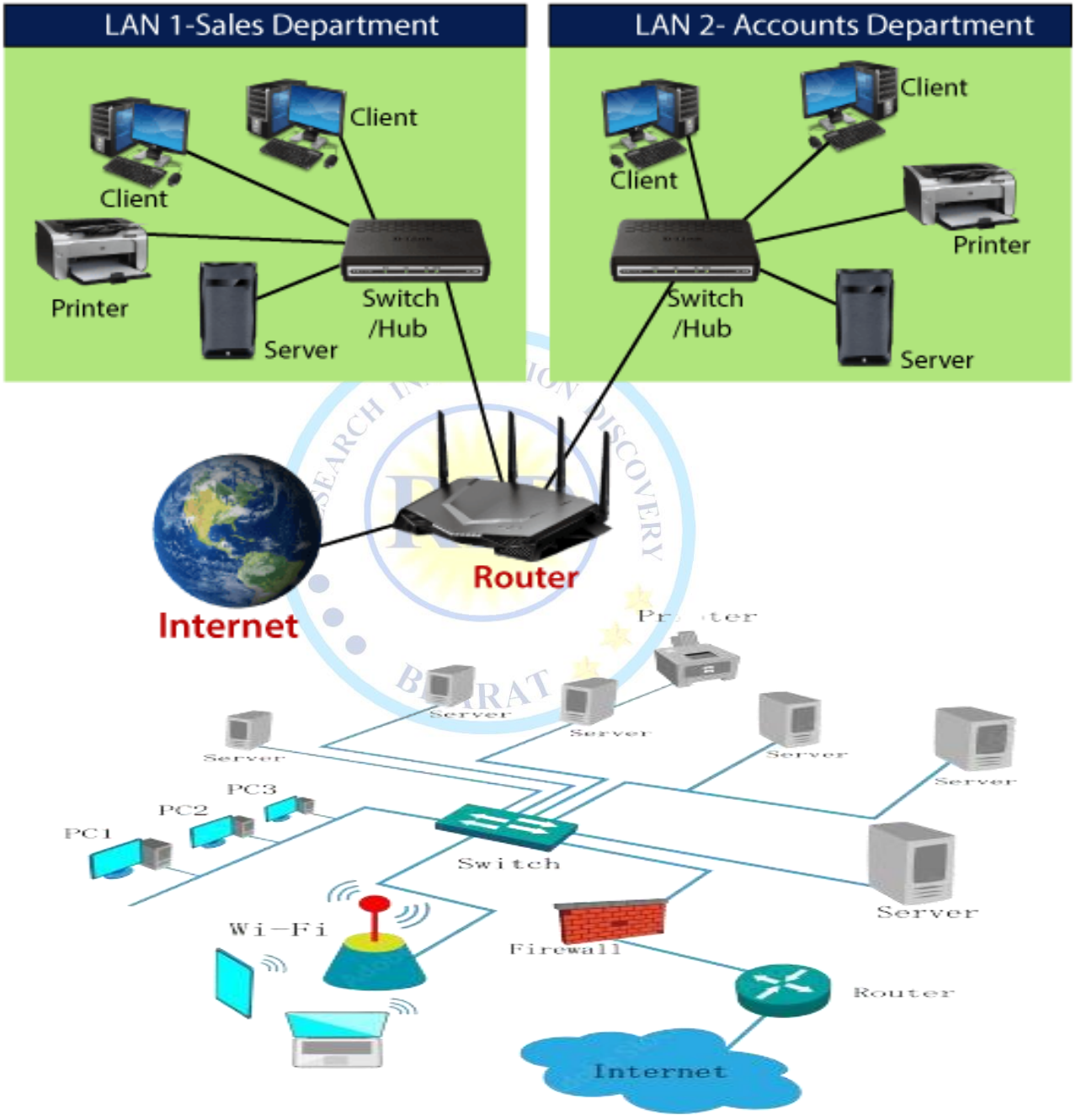
- **Use:** Switches are used in LAN environments to connect computers, printers, servers, and other network devices and facilitate communication between them.
- **Example:** In an office network, a managed switch is deployed to interconnect various departments and provide reliable connectivity for employees to access shared resources such as files, applications, and printers.

ROUTER

➢ A router is a networking device that connects multiple networks together and routes data packets between them based on IP addresses.

- It operates at the Network layer (Layer 3) of the OSI model and uses routing tables to determine the best path for forwarding packets.
- In simpler terms, a router acts as a traffic cop for data traveling between different networks. It receives data packets from one network, examines the destination IP address, and then decides where to send the packets next based on routing protocols and configurations.

❖ Diagram:



Features of Router:

1. **Full-Duplex:**
   - Routers operate in full-duplex mode, allowing simultaneous transmission and reception of data on each interface.

- This means that routers can send and receive data simultaneously, maximizing the utilization of network bandwidth and improving overall performance.

2. **No Broadcast:**
   - Unlike switches, routers do not forward broadcast packets to all connected interfaces.
   - Routers use routing tables to determine the best path for forwarding packets based on destination IP addresses, reducing unnecessary broadcast traffic and conserving network resources.
3. **Highly Intelligent:**
   - Routers are highly intelligent devices capable of making complex routing decisions based on routing protocols and routing tables.
   - They maintain routing tables containing information about network topology, available paths, and optimal routes to destination networks.
   - Routers use this information to determine the most efficient path for forwarding data packets, taking into account factors such as network congestion, link quality, and administrative preferences.
4. **Routing Table:**
   - Routing tables contain entries that map destination IP addresses to the next-hop router or outgoing interface.
   - They also include information about the network ID, subnet mask, and associated interface or port number. Routing tables enable routers to make forwarding decisions and determine the best path for routing packets to their destination.
5. **Works as a Traffic Controller:**
   - Routers act as traffic controllers, directing data packets between different networks and ensuring that they reach their intended destination.
   - They examine the destination IP address of incoming packets and use routing algorithms to determine the optimal path for forwarding traffic.
6. **Choose Congestion-Free Path:**
   - Routers dynamically adjust their routing decisions to avoid congested or unreliable network paths.
   - They use routing metrics such as hop count, bandwidth, delay, and reliability to select congestion-free paths and optimize network performance.
7. **Connect Two Dissimilar Networks:**
   - Routers can connect networks with different architectures, protocols, and technologies.
   - They serve as gateways between dissimilar networks, such as connecting Ethernet LANs to the Internet or linking IPv4 and IPv6 networks.
8. **Speed Options:**
   - Routers support a wide range of speeds, from Fast Ethernet (10Mbps) to Gigabit Ethernet (1Gbps) and beyond.
   - The choice of speed depends on factors such as network topology, device capabilities, and performance requirements.
9. **Layer-3 Functionality:**
   - Routers operate at the Network layer (Layer 3) of the OSI model, where they route data packets based on destination IP addresses.
   - They use IP routing protocols such as OSPF, EIGRP, and BGP to exchange routing information and build routing tables.
   - Layer-3 functionality enables routers to interconnect multiple networks and facilitate end-to-end communication across heterogeneous network environments.

❖ Types of Routers:

1. **Wired Routers:**

- Wired routers are traditional routers that use physical Ethernet connections to connect devices within a network.
- They typically have multiple Ethernet ports for connecting to local area network (LAN) devices and a wide area network (WAN) port for connecting to the Internet or another network.

2. **Wireless Routers:**
   - Wireless routers incorporate Wi-Fi functionality, allowing devices to connect to the network wirelessly using Wi-Fi technology.
   - They provide both wired and wireless connectivity options and often include built-in access points for wireless communication.
3. **Core Routers:**
   - Core routers are high-performance routers used in the backbone of large-scale networks, such as Internet Service Provider (ISP) networks.
   - They handle a significant volume of traffic and are optimized for fast packet forwarding and routing between different network segments.
4. **Edge Routers:**
   - Edge routers are deployed at the edge of a network, where they connect to end-user devices or smaller networks. They often provide additional features such as firewall capabilities, network address translation (NAT), and virtual private network (VPN) support for securing and managing network traffic.

❖ Advantages:

1. **Interconnectivity:**
   - ✓ Routers enable connectivity between different networks, allowing devices from one network to communicate with devices on another network.
   - ✓ This facilitates data sharing, collaboration, and resource access across distributed network environments.
2. **Routing and Forwarding:**
   - ✓ Routers use routing algorithms and tables to determine the best path for forwarding data packets between networks.
   - ✓ They optimize packet delivery by selecting the most efficient route based on factors such as network congestion, link quality, and cost.
3. **Network Segmentation:**
   - ✓ Routers can divide a large network into smaller subnetworks or segments, known as network segmentation.
   - ✓ Network segmentation enhances security, performance, and manageability by isolating traffic and limiting the scope of network issues.
4. **Network Address Translation (NAT):**
   - ✓ Many routers support NAT functionality, which allows multiple devices within a private network to share a single public IP address.
   - ✓ NAT enhances security and conserves IP address space by masking internal IP addresses from external networks.
5. **Security Features:**
   - ✓ Routers often include built-in firewall capabilities and access control features to protect against unauthorized access, intrusion attempts, and malicious traffic.
   - ✓ They can enforce security policies, filter incoming and outgoing traffic, and provide secure remote access via VPNs.

❖ Disadvantages:

1. **Complexity:**
   - ✓ Routers can be complex to configure and manage, especially for large-scale networks with intricate routing requirements.
   - ✓ Proper configuration and maintenance require expertise in networking concepts, protocols, and technologies.
2. **Cost:**
   - ✓ High-performance routers with advanced features can be expensive to purchase and deploy, particularly for organizations with budget constraints.
   - ✓ Additionally, ongoing maintenance costs, software licensing fees, and hardware upgrades may contribute to the total cost of ownership.
3. **Single Point of Failure:**
   - ✓ Routers serve as critical network infrastructure components, and a failure in a router can result in network downtime and disruption of communication.
   - ✓ Redundancy measures such as backup routers and failover mechanisms are necessary to mitigate the risk of a single point of failure.

❖ Use and Example:

- **Use:** Routers are used in various networking scenarios, including home networks, corporate networks, Internet service provider (ISP) networks, and data center environments.
- **Example:** In a corporate network, a router serves as the gateway between the internal LAN and the external Internet. It routes data packets between internal devices, such as computers and servers, and external destinations on the Internet, enabling employees to access online resources, communicate with clients, and conduct business operations.

INTERNET GATEWAY

- An Internet gateway is a networking device or software application that serves as the entry and exit point for data traffic between a local network and the Internet. It enables communication between devices within the local network and external resources on the Internet, such as websites, servers, and other online services.

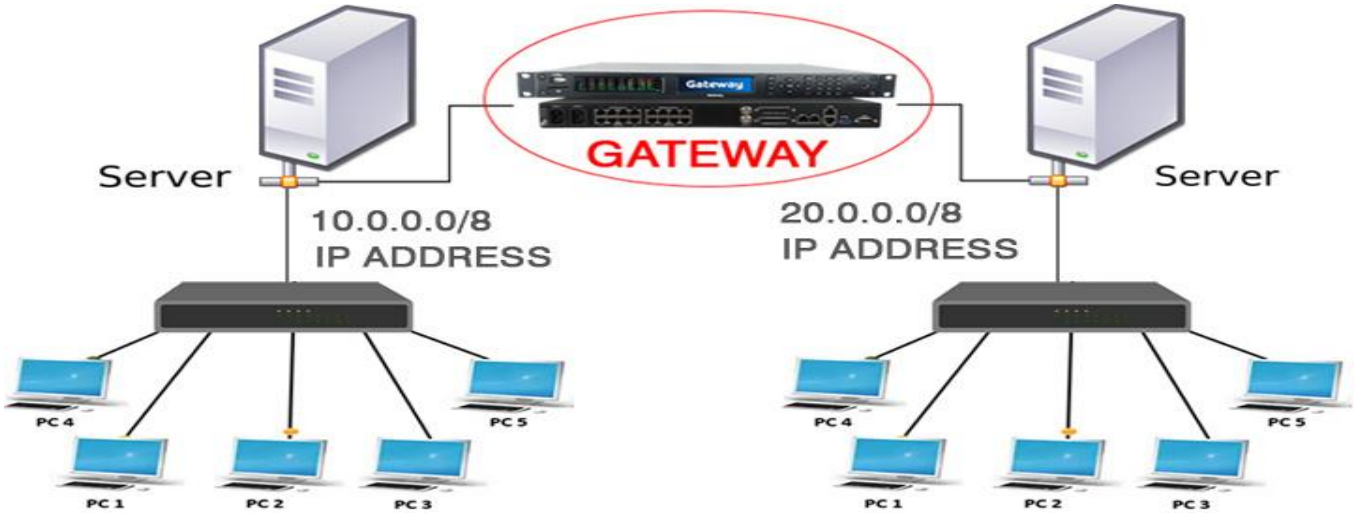
❖ Definition:

- An Internet gateway is a specialized networking device or software component that provides connectivity, routing, and security services to facilitate communication between a local network (such as a home network, corporate network, or campus network) and the Internet. It acts as a bridge between the internal network and external networks, enabling data exchange and access to Internet resources.

❖ Key Functions:

1. **Connectivity:** The primary function of an Internet gateway is to establish and maintain connectivity between devices within the local network and external resources on the Internet. It provides the necessary infrastructure for data transmission between the two networks.
2. **Routing:** The gateway routes data packets between the local network and the Internet based on destination IP addresses. It uses routing protocols and tables to determine the best path for forwarding packets, ensuring efficient and reliable data transmission.
3. **Address Translation:** Internet gateways often perform Network Address Translation (NAT) to map internal IP addresses to external public IP addresses. This allows multiple devices within the local network to share a single public IP address when accessing the Internet, enhancing security and conserving IP address space.
4. **Firewall and Security:** Internet gateways typically include firewall capabilities to protect the local network from unauthorized access, malicious attacks, and unwanted traffic from the Internet. They enforce security policies, filter incoming and outgoing traffic, and monitor network activity to detect and prevent security threats.
5. **Proxy Services:** Some Internet gateways offer proxy services to cache and optimize web content, reduce bandwidth usage, and improve browsing performance for users within the local network. Proxies can also enhance privacy and security by masking the identities of internal devices from external servers.

❖ Diagram:



- Hardware Gateways: Physical networking devices, such as routers, switches, and dedicated gateway appliances, designed specifically for Internet connectivity and security.

- Software Gateways: Software applications or services installed on servers or dedicated computing platforms to provide gateway functionality, often used in virtualized or cloud-based environments.

❖ Use Cases:

- **Home Networks:** Internet gateways are commonly used in home networks to provide broadband Internet access to multiple devices, such as computers, smartphones, tablets, and smart home devices.
- **Corporate Networks:** In corporate environments, Internet gateways serve as the central point of connectivity for employees to access the Internet, corporate resources, and cloud-based services securely.
- **Educational Institutions:** Universities, schools, and colleges deploy Internet gateways to provide Internet access to students, faculty, and staff while enforcing security policies and content filtering.
- **Public Wi-Fi Hotspots:** Public venues, such as airports, coffee shops, and hotels, use Internet gateways to offer Wi-Fi connectivity to guests and patrons, often with captive portals for authentication and access control.

❖ Features of Internet gateway:

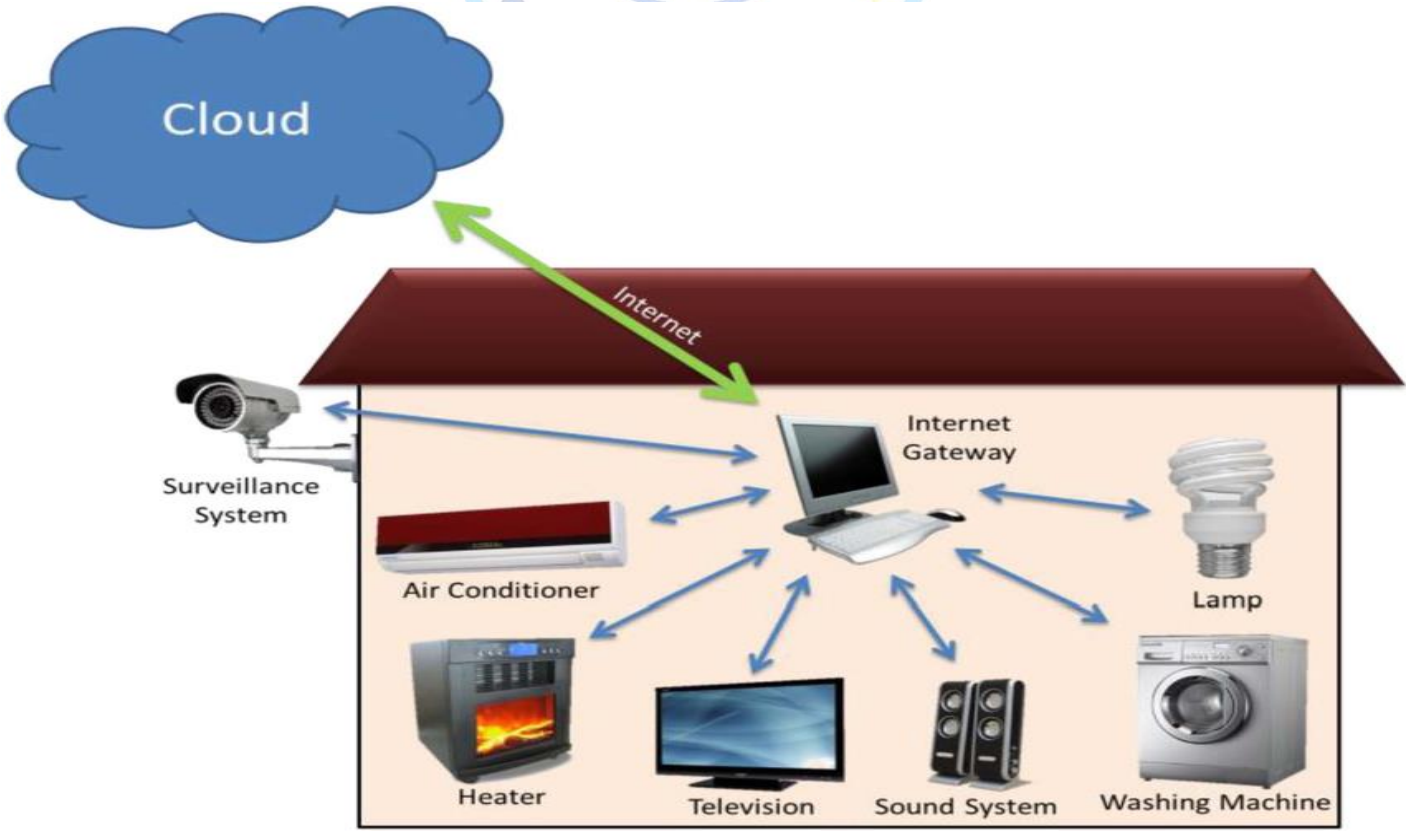
- **Connectivity:** Enables communication between local networks and the Internet.
- Routing: Routes data packets between the local network and the Internet based on destination IP addresses.
- **Address Translation:** Performs Network Address Translation (NAT) to map internal IP addresses to external public IP addresses.
- **Security:** Enforces firewall policies to protect against unauthorized access and malicious attacks.
- **Proxy Services:** Offers proxy services to optimize web content, reduce bandwidth usage, and enhance privacy.
- **Quality of Service (QoS):** Prioritizes certain types of traffic for optimal performance.
- **Traffic Management:** Manages network traffic to minimize congestion and ensure efficient data transmission.
- **Monitoring and Logging:** Provides monitoring and logging capabilities to track network activity and security incidents.
- **Remote Management:** Supports remote configuration, monitoring, and troubleshooting.
- **Redundancy and High Availability:** Offers failover mechanisms and redundant connectivity options for uninterrupted service.
- **Scalability:** Scales to accommodate growing network requirements, supporting a large number of users and devices.

❖ Advantages of Internet Gateway:

- ✓ **Connectivity:** Internet gateways provide seamless connectivity between local networks and the Internet, enabling users to access online resources, communicate with external parties, and utilize cloud-based services.
- ✓ **Routing and Traffic Management:** Gateways route data packets between networks, ensuring efficient and reliable transmission by selecting the best path for data delivery. They also manage network traffic, prioritize packets, and optimize bandwidth utilization.
- ✓ **Security:** Internet gateways offer robust security features such as firewall protection, intrusion detection and prevention, content filtering, and virtual private network (VPN) support. These features safeguard the local network from unauthorized access, malicious attacks, and data breaches.
- ✓ **Address Translation:** Gateways perform Network Address Translation (NAT) to map internal IP addresses to external public IP addresses, allowing multiple devices within the local network to share a single public IP address.
- ✓ **Proxy Services:** Some gateways provide proxy services to cache and optimize web content, reduce bandwidth consumption, and improve browsing performance.

❖ Disadvantages of Internet Gateway:

- ✓ **Complexity:** Configuring and managing an Internet gateway can be complex, especially for non-technical users or organizations lacking IT expertise. Proper setup and maintenance require knowledge of networking concepts, protocols, and security practices.
- ✓ **Cost:** High-performance Internet gateway hardware and software solutions can be expensive to purchase, deploy, and maintain.
- ✓ Single Point of Failure: Internet gateways serve as critical network infrastructure components, and a failure in the gateway can result in network downtime and disruption of communication.
- ✓ **Performance Limitations:** Inadequate bandwidth, processing power, or memory capacity in the gateway can lead to performance limitations, such as network congestion, latency, and reduced throughput.



- A modem, short for modulator-demodulator, is a device used in computer networks to modulate and demodulate digital data into analog signals for transmission over analog communication channels, such as telephone lines or cable systems. It serves as an interface between digital devices.

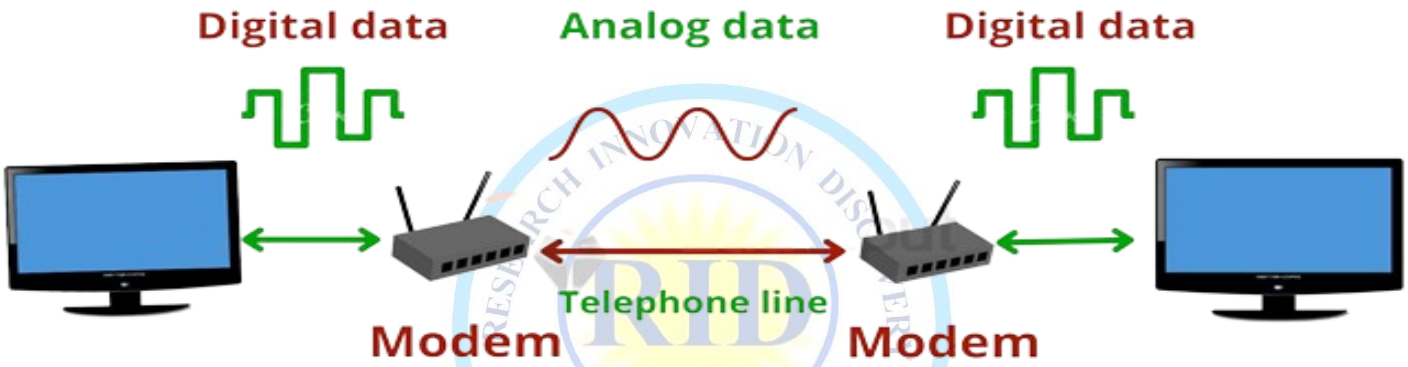
❖ Modulation:

- The modem's modulator component converts digital data generated by computers into analog signals suitable for transmission over analog communication lines. Modulation techniques vary depending on the communication medium used, such as amplitude modulation (AM), frequency modulation (FM), or phase modulation (PM).

❖ Demodulation:

- On the receiving end, the modem's demodulator component extracts digital data from incoming analog signals. Demodulation reverses the modulation process, converting analog signals back into digital data that computers can understand and process.

❖ Diagram:



❖ Types of Modems:

1. **Analog Modems:** Traditionally used for dial-up Internet connections, analog modems operate over standard telephone lines and support data transfer rates up to 56 Kbps.
2. **Digital Modems:** Used for high-speed Internet access, digital modems operate over digital communication channels, such as cable or DSL (Digital Subscriber Line), and support higher data transfer rates.
3. **Wireless Modems:** Wireless modems, also known as cellular modems or mobile hotspots, provide Internet connectivity over cellular networks, allowing devices to access the Internet wirelessly.

❖ Types of Connections:

1) **Dial-up:** Analog modems establish connections over telephone lines by dialing a phone number and establishing a connection with a remote modem.
2) **DSL:** Digital Subscriber Line (DSL) modems use existing telephone lines to provide high-speed Internet access.
3) **Cable:** Cable modems connect to cable television lines to provide broadband Internet access.
4) **Wireless:** Wireless modems connect to cellular networks to provide Internet access to devices wirelessly.

❖ Features of Modem:

1. **Modulation and Demodulation:** Converts digital signals to analog for transmission and vice versa.
2. **Connection Types:** Supports various connections like dial-up, DSL, cable, and wireless.
3. **Compatibility:** Works with different communication channels and standards.

4. **Data Transfer Rates:** Offers variable speeds from low to high, depending on technology.
5. **Portability:** Wireless modems provide mobility within coverage areas.
6. **Security:** Some modems include built-in firewall features for protection.
7. **Reliability:** Includes error correction and data retransmission mechanisms.
8. **Ease of Use:** Generally easy to install and configure for users.
9. **Scalability:** Can accommodate multiple users and devices.
10. **Cost-Effectiveness:** Provides affordable Internet access options.
11. **Voice and Fax Support:** Some modems offer voice and fax capabilities.

❖ Advantages:

- ✓ Widely available: Modems are compatible with various types of communication channels, making them suitable for different environments.
- ✓ Cost-effective: Analog modems provide affordable Internet access, especially in areas where broadband services are limited.
- ✓ Portable: Wireless modems allow users to access the Internet from anywhere within cellular coverage areas.

❖ Disadvantages:

- **Limited speed:** Analog modems have slower data transfer rates compared to broadband technologies like DSL or cable.
- **Signal quality:** Analog modems may experience signal degradation or interference, affecting data transmission quality.
- **Dependency on infrastructure:** Modem performance may be affected by the condition and quality of communication lines or cellular network coverage.

❖ Use Cases:

- Home Internet access: Analog or digital modems are used to provide Internet connectivity to households, either through dial-up, DSL, cable, or wireless connections.
- Business connectivity: Modems are used in businesses to establish network connections, access online services, and facilitate communication with remote offices or clients.

❖ Examples:

- A dial-up modem used to connect a computer to the Internet via a telephone line.
- A cable modem installed in a household to provide high-speed Internet access over a cable television network.
- A wireless modem or mobile hotspot used to access the Internet on smartphones, tablets, or laptops while on the go.

Definition: -it is a set of rules. use: - used for digital communication, formatting and processing the data
Type: -TCP, UDP, IP, HTTP, FTP, SMTP, DHCP, ICMP, POP, IMAP, ARP, RIP, NFS, FMTP, SNMP etc…
Application Layer Protocols: - HTTP: -- Hypertext Transfer Protocol, **DNS: -** Domain Name System,
FTP: - File Transfer Protocol, **Telnet, SMTP: -** Simple Mail Transfer Protocol, **SNMP: -** Simple Network Time p.

Presentation Layer Protocols: - SSL, HTTP/ HTML (agent), FTP AppleTalk Filing Protocol, Telnet

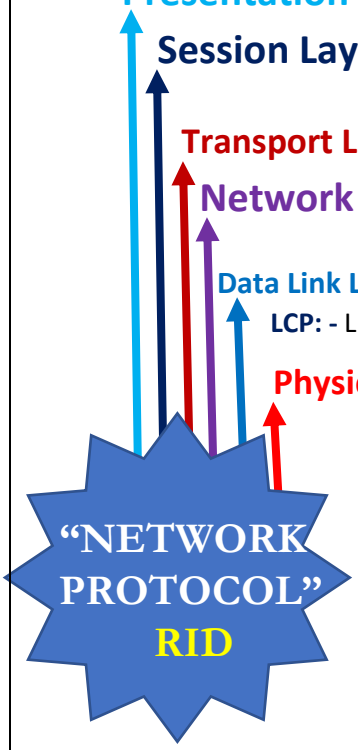
Session Layer Protocols: - RPC: - Remote Procedure Calls **PPTP: -** Point-to-Point Tunnelling P **SCP:-** Secure Copy Protocol. **SDP:-** Session Description Protocol etc..

Transport Layer Protocols: - TCP: - Transmission Control Protocol **UDP: -** User Datagram Protocol

Network Layer Protocols: - IP: -Internet protocol, **ICMP: -**Internet Control Message Protocol **ARP: -**Address Resolution Protocol

Data Link Layer Protocols: - SDLC: - Synchronous Data Link Protocol, **PPP: -** Point to Point Protocol **LCP: -** Link Control Protocol **LAP: -** Link Access Procedure **SLIP: -** Serial Line Interface Protocol

Physical Layer Protocols: - Physical layer provides an electrical, mechanical, and procedural interface to the transmission medium.



Application Layer Protocols: - HTTP :-- Hypertext Transfer Protocol**, HTTPS:- Hypertext Transfer Protocol secure DNS:-** Domain Name System, **FTP:-** File Transfer Protocol , **Telnet, SMTP:-** Simple Mail Transfer Protocol , **SNMP:-** Simple Network Time protocol DHCP:- Dynamic host configuration Protocol LDAP:-Lightweight Directory Access Protocol MGCP:- Media Gateway control protocol MQTT:- Lightweight protocol OSPF:- open shortest path first IMAP:- internet message access protocol BGP:-BORDER Gateway Protocol IRC:- Internet relay chat pop:- post office protocol PTP:- Precision Time protocol NTP:- Network time protocol; RTP:- Real time transport RIP:- routing information protocol SIP :- Session initiation protocol SSH:- Secure shell Protocol SSL:- Secure Socket Layer RTSP:- real time streaming protocol ONC/RPC:- open network computing
RPC: - remote procedure call.

Transport Layer Protocols: - TCP: - Transmission Control Protocol **UDP: -** User Datagram Protocol
DCCP: - Datagram congestion control Protocol SCTP: -Stream Control Transmission Protocol

Network/ Internet Layer Protocols or: - IP: -Internet protocol, **ICMP: -**Internet Control Message Protocol **ARP: -**Address Resolution Protocol IGMP: - Internet group management Protocol ECN: - Explicit Congestion Notification NDP: - Neighbour Discovery Protocol

NETWORK PROTOCOL

- A network protocol is a set of rules and conventions that govern how data is exchanged between devices on a computer network. These protocols define the format, timing, sequencing, error control, and security aspects of communication, enabling devices to communicate effectively and reliably across diverse network environments.

  Purpose: Network protocols provide a standardized framework for communication between devices, ensuring compatibility and interoperability across heterogeneous network infrastructures.

❖ Components of protocol:

1. **Packet Format:** Defines the structure of data packets exchanged between devices, specifying fields such as headers, payloads, and checksums.
2. **Addressing:** Determines how devices are identified and addressed on the network, such as using IP addresses in Internet Protocol-based networks.
3. **Routing:** Specifies the paths that data packets take through the network from source to destination, involving protocols like Routing Information Protocol (RIP) or Border Gateway Protocol (BGP).
4. **Flow Control:** Manages the rate of data transmission to prevent congestion and ensure efficient use of network resources, employing mechanisms such as sliding window protocols.
5. **Error Control:** Detects and corrects errors in transmitted data packets, utilizing techniques such as cyclic redundancy check (CRC) or error detection and retransmission.
6. **Security:** Implements mechanisms for authentication, encryption, and access control to protect data and network resources from unauthorized access and malicious attacks.
7. **Session Management:** Facilitates the establishment, maintenance, and termination of communication sessions between devices, handling tasks like session initialization, negotiation, and termination.
8. **Application Support:** Provides protocols tailored to specific applications or services, such as File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), or Hypertext Transfer Protocol (HTTP), enabling interoperability between different software applications.

❖Types of protocols:

1. Communication Protocols:

- These protocols are essential for network functioning. They define rules and formats for data transfer, handling aspects like syntax, semantics, error detection, synchronization, and authentication.

a. **Hypertext Transfer Protocol (HTTP):** A layer 7 protocol for transferring hypertext (web pages) between systems. Most web data sharing occurs via HTTP.
b. **Transmission Control Protocol (TCP):** Reliable, connection-oriented protocol that establishes a connection before data transfer. Used for emails, FTP, streaming media, etc.
c. **User Datagram Protocol (UDP):** Connectionless protocol for faster data transmission (used in real-time applications).
d. **Simple Mail Transfer Protocol (SMTP):** Handles email transmission between servers.

2. Network Management Protocols:

- These focus on managing network devices, monitoring performance, and ensuring efficient operation. Administrators use them for maintenance and troubleshooting.

a. **Simple Network Management Protocol (SNMP):** Monitors and manages network devices (routers, switches, etc.).

b. **Internet Control Message Protocol (ICMP):** Reports errors and provides status updates.
c. **Network Time Protocol (NTP):** Synchronizes clocks across devices.
d. **Dynamic Host Configuration Protocol (DHCP):** Assigns IP addresses dynamically.

3. Network Security Protocols:

- Enhance network security by ensuring data confidentiality, integrity, and authentication.

a. **Secure Sockets Layer (SSL) / Transport Layer Security (TLS):** Encrypts data during transmission (e.g., HTTPS for secure web browsing).
b. **IPsec (Internet Protocol Security):** Provides secure communication over virtual private networks (VPNs).
c. **Firewall Rules (e.g., Circuit-Level Gateway):** Control access to network resources.
d. **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** Detect and prevent unauthorized access.

4. Data Transmission Protocols:

- These protocols govern the transmission of data over the network, ensuring reliable delivery and error detection.

a. **Ethernet:** Defines standards for wired local area network (LAN) communications, including protocols for data framing and packet delivery.
b. **Wi-Fi (IEEE 802.11):** Wireless communication protocol for local area networks, enabling devices to connect and exchange data wirelessly.

5. Routing Protocols:

- These protocols determine the optimal paths for data packets to travel through the network.

a. **Border Gateway Protocol (BGP):** A routing protocol used to exchange routing information between different autonomous systems on the internet.
b. **Open Shortest Path First (OSPF):** Interior gateway routing protocol used within an autonomous system for efficient routing.

6. Voice over Internet Protocol (VoIP) Protocols:

- These protocols enable voice communication over the internet, facilitating services like internet telephony and video conferencing.

a. **Session Initiation Protocol (SIP):** A signaling protocol used for initiating, maintaining, and terminating multimedia sessions over the internet.
b. **Real-time Transport Protocol (RTP):** Transports audio and video data in VoIP communications, ensuring timely delivery and synchronization.

7. File Transfer Protocols:

- These protocols facilitate the transfer of files between devices or systems.

a. **File Transfer Protocol (FTP):** Standard network protocol used to transfer files between a client and server on a computer network.
b. **Secure File Transfer Protocol (SFTP):** Secure version of FTP that encrypts data during transmission, providing enhanced security.

8. Domain Name System (DNS):

- This protocol translates domain names into IP addresses, enabling users to access websites using human-readable addresses.

a. **Domain Name System (DNS):** Hierarchical decentralized naming system for computers, services, or other resources connected to the internet or a private network.

❖ Advantages of protocol:

- ✓ **Interoperability:** Allows devices from different vendors to communicate seamlessly.
- ✓ **Scalability:** Supports networks of varying sizes, from small local networks to global internetworks.
- ✓ **Reliability:** Ensures reliable data transmission through error detection and correction mechanisms.
- ✓ **Security:** Provides mechanisms for securing data and network resources against unauthorized access and attacks.
- ✓ **Efficiency:** Optimizes network performance by managing data flow, congestion, and resource utilization.

❖ Disadvantages of protocol:

- ✓ **Complexity:** Implementing and managing network protocols can be complex and require specialized knowledge and expertise.
- ✓ **Overhead:** Some protocols introduce additional overhead in terms of bandwidth and processing resources, impacting network performance.
- ✓ **Vulnerabilities:** Protocol implementations may contain vulnerabilities that can be exploited by attackers to compromise network security or disrupt services.
- ✓ **Compatibility Issues:** Incompatible or outdated protocols may hinder interoperability and limit the functionality of network devices and applications.

❖ Example of protocols:

- HTTP (Hypertext Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- FTP (File Transfer Protocol)
- TCP (Transmission Control Protocol)
- DNS (Domain Name System)
- SSH (Secure Shell)
- SNMP (Simple Network Management Protocol) etc.

❖ Use of protocols:

1. **HTTP (Hypertext Transfer Protocol):**

➢ **Use:** HTTP is used for accessing and retrieving web pages and resources from web servers. It facilitates communication between web clients (such as browsers) and web servers.

2. **SMTP (Simple Mail Transfer Protocol):**

➢ **Use:** SMTP is used for sending and receiving email messages between email clients and mail servers. It handles the transmission of emails over the internet.

3. **FTP (File Transfer Protocol):**

➢ **Use:** FTP is used for transferring files between a client and a server on a computer network. It allows users to upload, download, and manage files on remote servers.

4. **TCP (Transmission Control Protocol):**

➢ **Use:** TCP is a core protocol used in internet communications for reliable, connection-oriented data transmission. It ensures that data packets are delivered reliably and in the correct order.

5. **DNS (Domain Name System):**

- **Use:** DNS is used to translate human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) that computers use to identify and communicate with each other over the internet.

6. SSH (Secure Shell):

- **Use:** SSH is used for secure remote access to computer systems and for executing commands remotely. It provides encrypted communication between a client and a server, making it suitable for tasks like remote administration and file transfer.

7. SNMP (Simple Network Management Protocol):

- **Use:** SNMP is used for managing and monitoring network devices, such as routers, switches, and servers. It allows administrators to gather information about the health and performance of network devices and to configure them remotely.

8. POP3 (Post Office Protocol version 3):

- **Use:** POP3 is used by email clients to retrieve email messages from a mail server. It enables users to download emails from the server to their local devices for reading and storage.

9. IMAP (Internet Message Access Protocol):

- **Use:** IMAP is another protocol used by email clients for accessing and managing email messages on a remote mail server. It allows users to view, organize, and manipulate emails stored on the server without downloading them to their local devices.

10. DHCP (Dynamic Host Configuration Protocol):

- **Use:** DHCP is used for dynamically assigning IP addresses and other network configuration parameters to devices on a network. It automates the process of IP address allocation, making it easier to manage and scale large networks.

11. NTP (Network Time Protocol):

- **Use:** NTP is used for synchronizing the time of computer systems on a network. It ensures that all devices maintain accurate and consistent time settings, which is crucial for various network applications and services.

12. LDAP (Lightweight Directory Access Protocol):

- **Use:** LDAP is used for accessing and managing directory services, such as user authentication and authorization information, on a network. It provides a standardized way to interact with directory servers and perform directory operations.

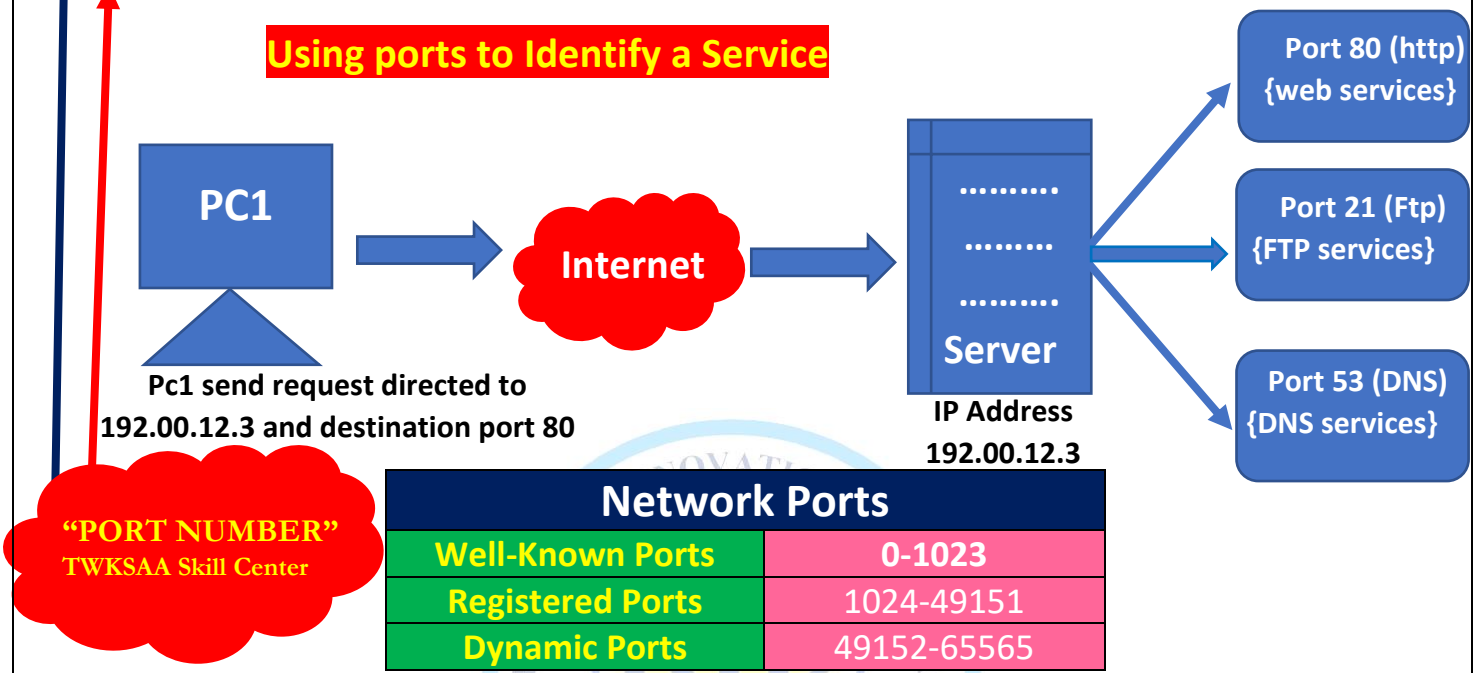
Definition: - Port Number is assigned to uniquely identify a connection endpoint and to direct data Specific Service. it is logical Number that identifies a specific process or a type of network service. Manged by (IANA)

Port Number is a 16-Bits, Port is connection on computer to peripheral Devices.

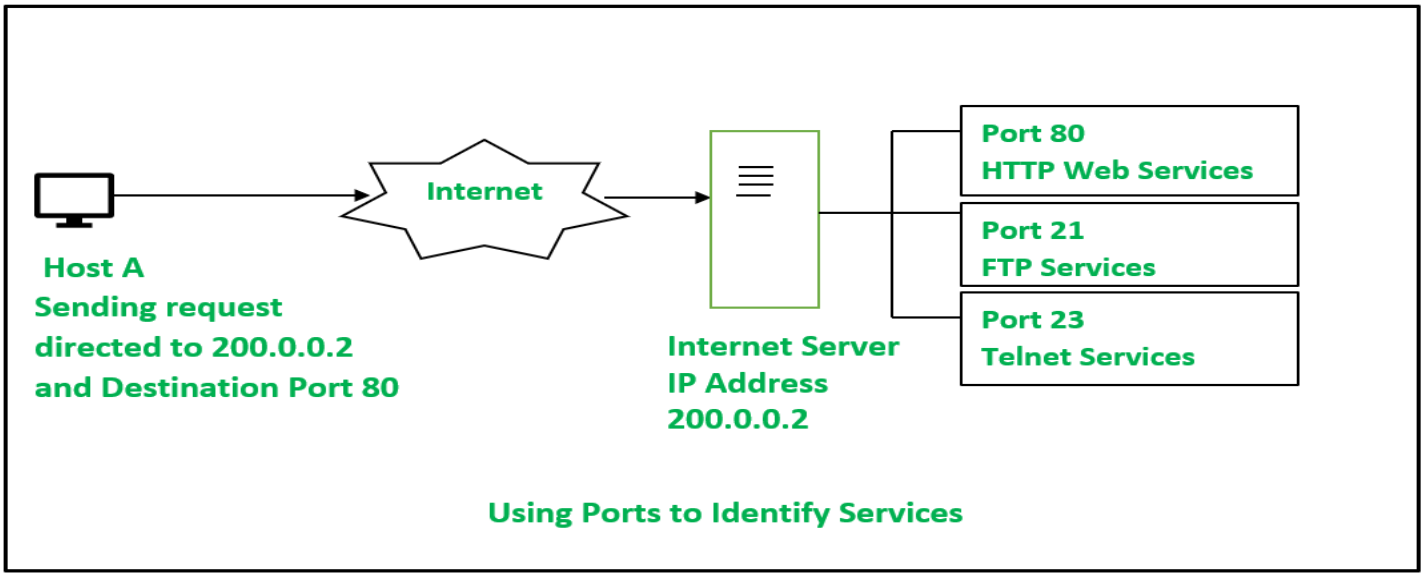
Range: - (0-65535) 1). Well-Know Ports (System Port) {0-1023} 2). Registered Ports {1024-49151} 3). Dynamic or Private Ports (49152-65535)

Service	DNS	HTTP	HTTPS	FTP	SSH	TALNET	SMTP	DHCP	POP3
Port Number	53	80	443	20 &21	22	23	25	67 & 68	110

Types: - 1). Serial Port: - Interface to connect using serial port 2). Parallel Port: - Used Parallel Port



Network Ports	
Well-Known Ports	0-1023
Registered Ports	1024-49151
Dynamic Ports	49152-65565



- Transmission mode, also known as data transmission mode or communication mode, refers to the method by which data is transmitted between devices in a computer network. It defines how data is transferred between the sender and receiver and the direction of data flow.
- There are three main transmission modes:

1. Simplex Mode:

- In simplex mode, communication is unidirectional, similar to a one-way street. Only one of the two devices on a link can transmit data, while the other can only receive.

❖ **Examples of simplex mode:**

- ✓ Keyboard and traditional monitors: The keyboard can only introduce input, and the monitor can only display output.

❖ **Advantages:**

- ✓ Simplex mode is the easiest and most reliable mode of communication.
- ✓ It is cost-effective, requiring only one communication channel.
- ✓ No coordination between transmitting and receiving devices is needed.
- ✓ Useful for scenarios where feedback or response is not required (e.g., broadcasting or surveillance).

❖ **Disadvantages:**

- ✓ Only one-way communication is possible.
- ✓ No way to verify if transmitted data has been received correctly.
- ✓ Not suitable for bidirectional communication needs.

2. Half-Duplex Mode:

- In half-duplex mode, each station can both transmit and receive, but not simultaneously. When one device is sending, the other can only receive, and vice versa.

❖ **Examples of half-duplex mode:**

- Walkie-talkies: Messages are sent one at a time, allowing bidirectional communication.

❖ **Advantages:**

- ✓ Allows bidirectional communication.
- ✓ More efficient than simplex mode.
- ✓ Less expensive than full-duplex mode.

❖ **Disadvantages:**

- ✓ Less reliable than full-duplex mode.
- ✓ Delay between transmission and reception can cause issues.
- ✓ Requires coordination between transmitting and receiving devices.

3. Full-Duplex Mode:

- In full-duplex mode, both stations can transmit and receive simultaneously. Signals going in one direction share the channel capacity with signals going in the opposite direction.

❖ **Examples of full-duplex mode:**

- Telephone conversations: Both parties can talk and listen simultaneously.

❖ **Advantages:**

- ✓ Enables simultaneous bidirectional communication.
- ✓ Efficient use of channel capacity.
- ✓ Suitable for applications requiring real-time interaction.

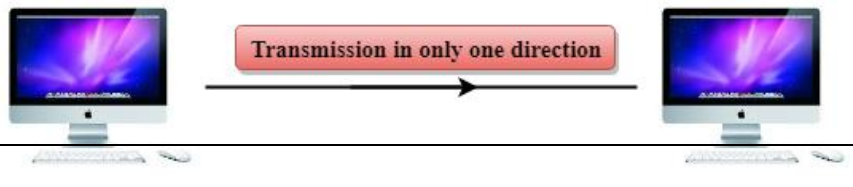
❖ **Disadvantages:**

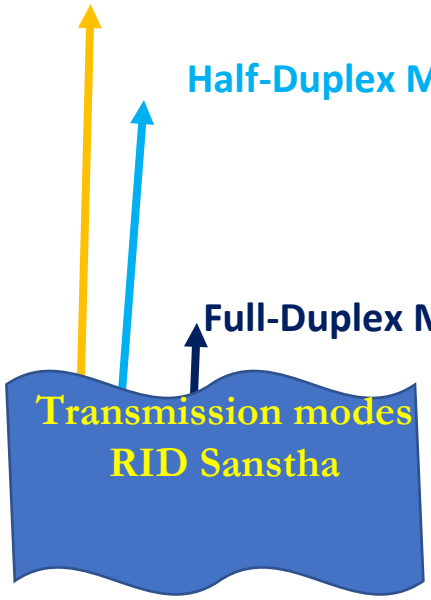
- ✓ More complex than half-duplex mode.
- ✓ Requires specialized hardware for simultaneous transmission and reception.

Definition: -The way in which data is transmitted from one device to another device is known as transmission mode. It is also known as Communication Mode

Type: - 1. Simplex mode 2. Half-duplex mode 3. Full-duplex mode

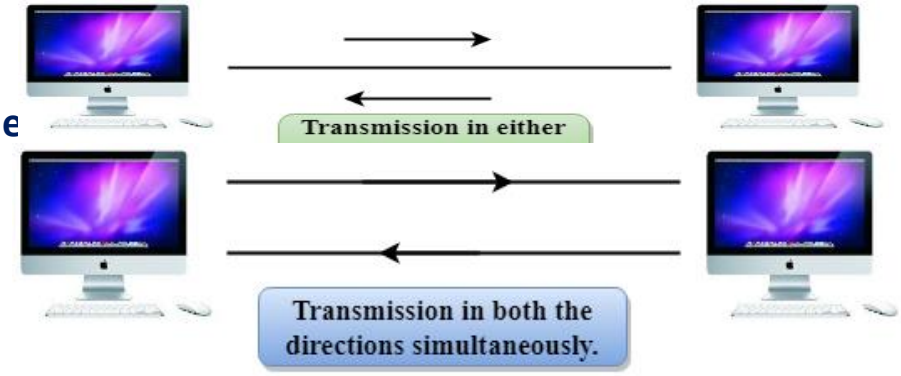
Simplex mode: -

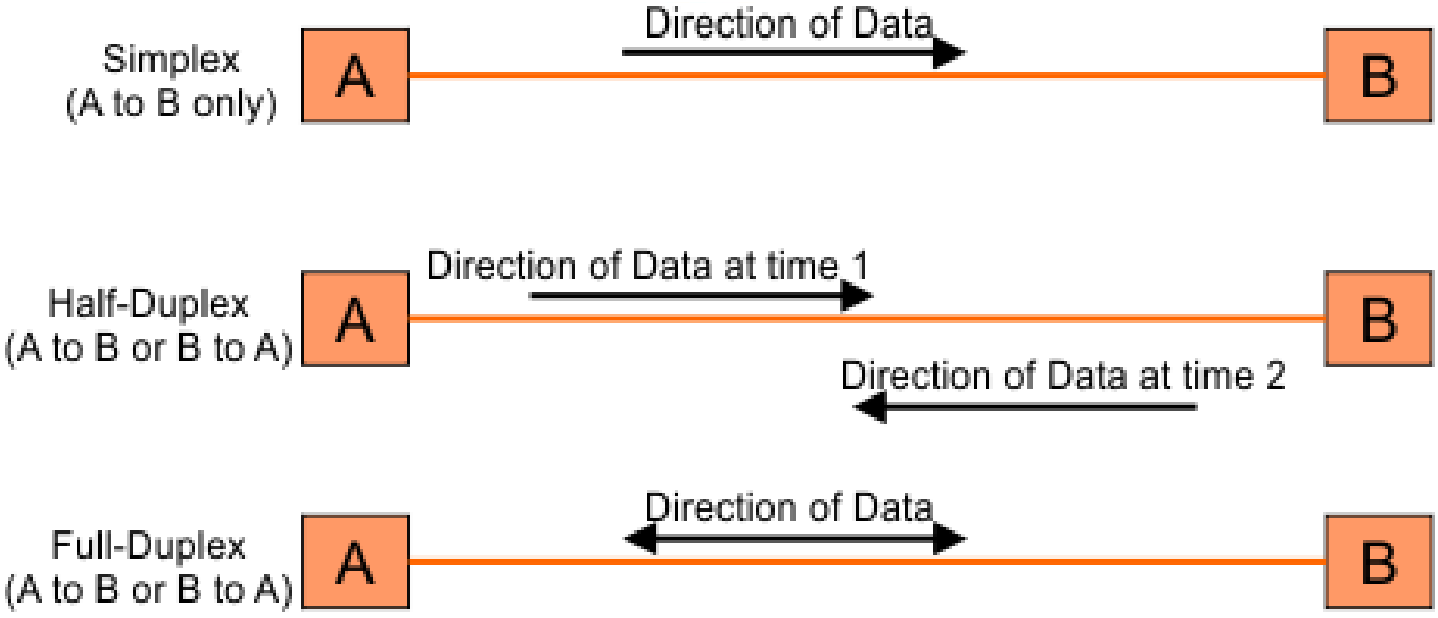




Half-Duplex Mode: - Messages flow in both the directions, but not at the same time.

Full-Duplex Mode





DIGITAL TRANSMISSION

- Digital transmission refers to the process of transferring data in the form of digital signals—a series of binary bits (0s and 1s)—over a communication channel. Unlike analog transmission, which sends data as a continuous signal, digital transmission encodes data into discrete signals.

❖ **Data Encoding:**

- Information (whether text, voice, or video) is converted into binary format for transmission.
- Binary signals represent discrete values, making them suitable for communication over networks, the Internet, cellular systems, and digital broadcasting.

❖ **Signal Transmission:**

- These binary signals are then transmitted over various communication channels, such as:
  - **Copper cabling:** Voltage variations represent the binary data.
  - **Fiber-optic cabling or wireless communication:** Intensity variations or other physical quantities convey the information.

❖ **Error Detection and Correction:**

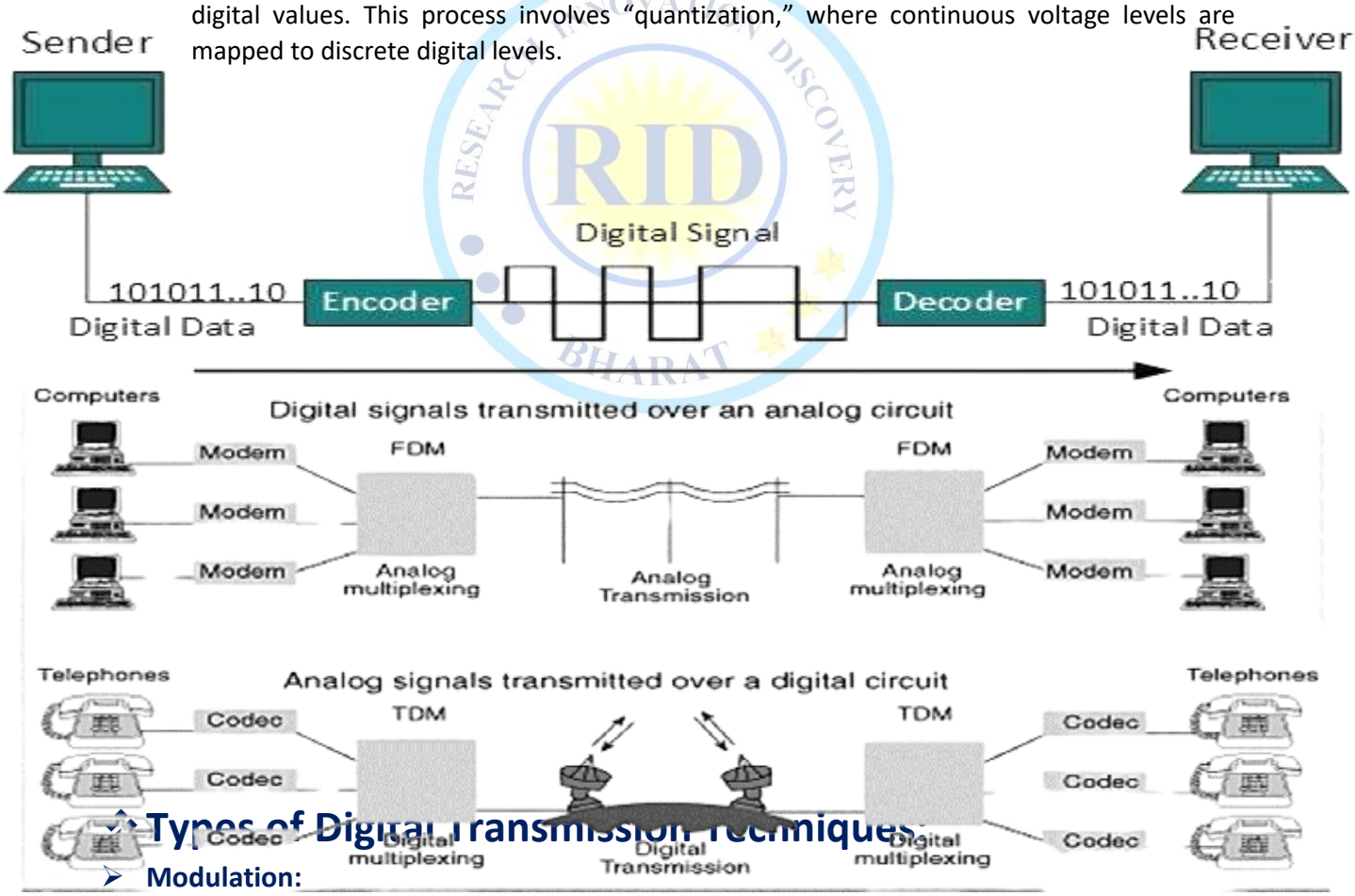
- Digital transmission often includes mechanisms for detecting and correcting errors that may occur during transmission. These error-checking techniques enhance data integrity.

❖ **Differentiating from Analog Transmission:**

- The opposite of digital transmission is analog transmission, where information is transmitted as a continuously varying quantity. Analog signals can be converted to digital signals using devices like an analog-to-digital converter and vice versa using a digital-to-analog converter.

➢ **How it works:**

- ADCs (Analog-to-Digital Converters): Convert varying AC voltages (analog signals) to stepped digital values. This process involves "quantization," where continuous voltage levels are mapped to discrete digital levels.



❖ **Types of Digital Transmission Techniques:**

➢ **Modulation:**

- Modulation converts digital signals into a form suitable for the transmission medium.
- Common types of digital modulation include:
  - ✓ **Amplitude Shift Keying (ASK):** Modulates the amplitude of the carrier signal.
  - ✓ **Frequency Shift Keying (FSK):** Modulates the carrier frequency.

- ✓ **Phase Shift Keying (PSK):** Modulates the phase of the carrier signal.

❖ Why Digital Transmission Matters:

- **Efficiency:** Digital transmission allows efficient use of bandwidth and resources.
- **Reliability:** Digital signals are less susceptible to noise interference, leading to better error detection and correction.
- **Ubiquity:** It underpins modern communication systems, including the Internet, mobile networks, and digital broadcasting.
- **Advancements:** Ongoing technological progress continues to expand the possibilities of digital communication.

❖ Types of transmission Media:

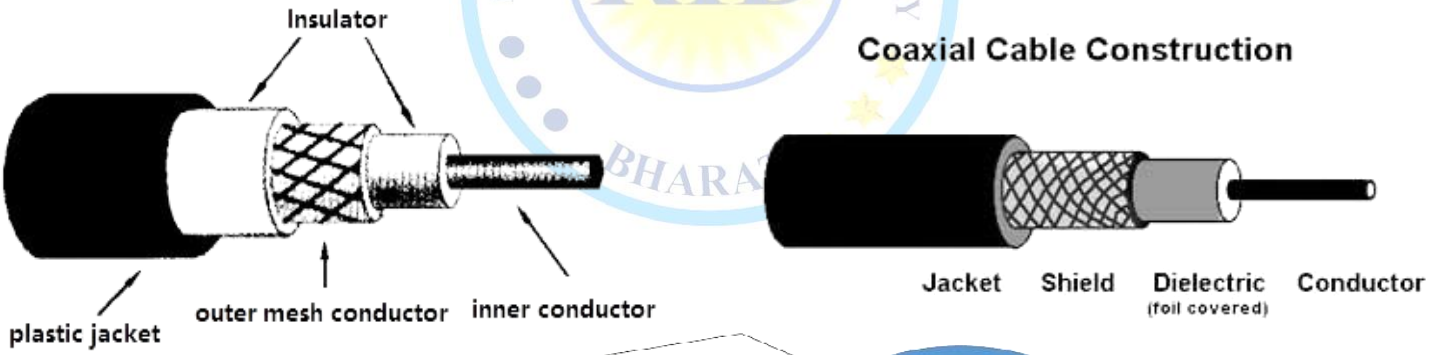
1. Guided Media (Wired Transmission):

➢ It is, also known as bounded or wired media, are physical cables that guide electromagnetic signals along a specific path. They provide a physical conduit for transmitting data signals.

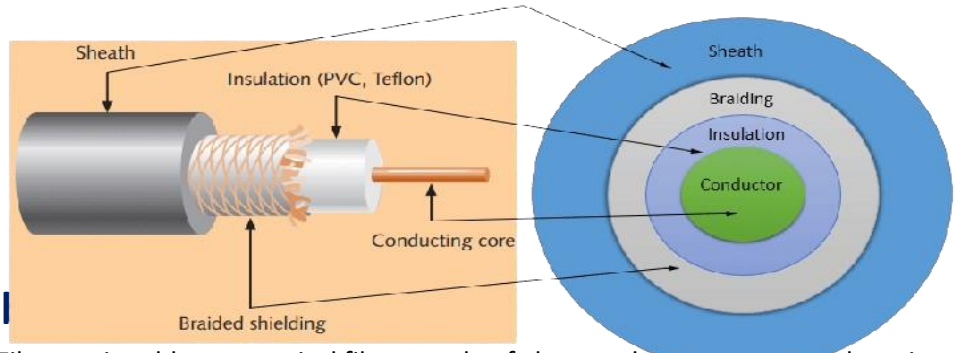
a. Coaxial Cable:

- It consists of a central conductor, an insulating layer, a metallic shield, and an outer insulating layer. It is commonly used for transmitting cable television signals and networking data.
  1. **Baseband:** In baseband transmission, the entire bandwidth of the cable is used to transmit a single digital signal.
  2. **Broadband:** In broadband transmission, the cable's bandwidth is divided into multiple channels, allowing for simultaneous transmission of multiple signals.

- **Applications:** Cable TV, analog television networks, digital audio (S/PDIF), Ethernet, and radio transmitters/receivers.

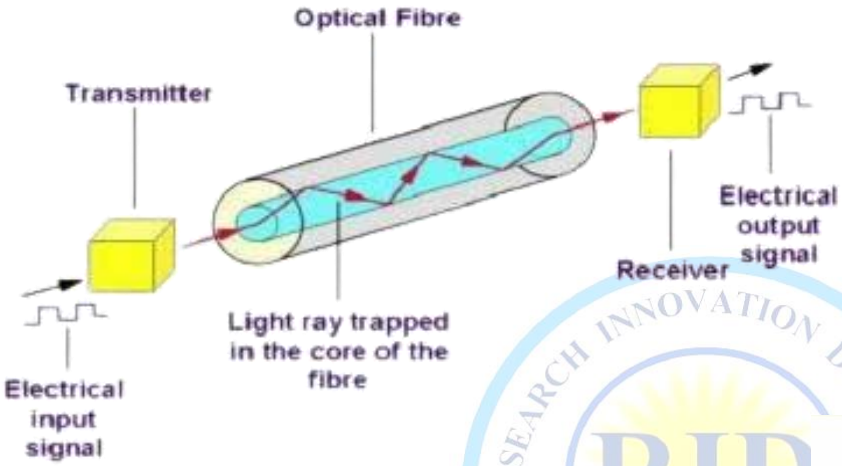


b. Fil



- Fiber optic cables use optical fibers made of glass or plastic to transmit data signals using light pulses. These cables are known for their high bandwidth, low attenuation, and immunity to electromagnetic interference.
- Fiber optic cables are widely used in telecommunications networks, internet infrastructure, and high-speed data transmission applications.

Light Ray



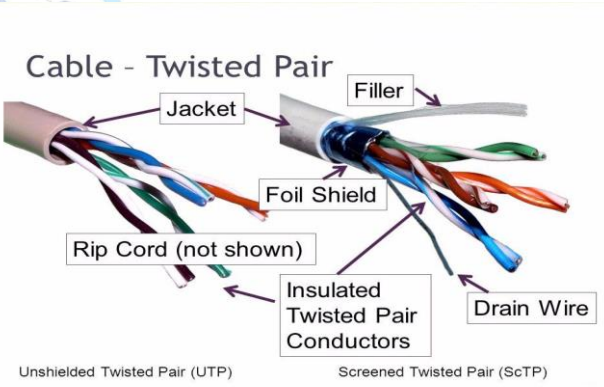
Advantages:

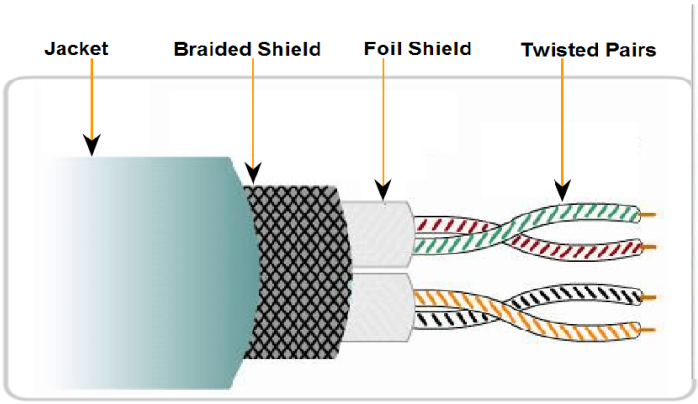
- ✓ High bandwidth.
- ✓ Better noise immunity.
- Easy to install and expand

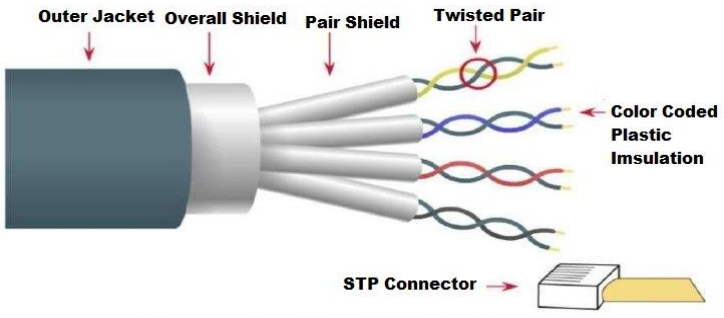
Applications: Transmitting data over long distances, high-speed internet, telecommunication networks.

C. Twisted Pair Cable:

- **Description:** Twisted pair cables consist of two separately insulated conductor wires wound around each other. Several pairs are often bundled together in a protective sheath.







:

- Used for telephonic applications.
- Doesn't rely on a physical shield to block interference.

Advantages:

- ✓ Least expensive.
- ✓ Easy to install.

- ✓ High-speed capacity.

Disadvantages:

- ✓ Susceptible to external interference.
- ✓ Lower capacity compared to Shielded Twisted Pair (STP).
- ✓ Short-distance transmission due to attenuation.

2. **Shielded Twisted Pair (STP):** Contains a special jacket (copper braid or foil shield) to block external interference. Used in fast-data-rate Ethernet and voice/data channels.

Advantages:

- ✓ Better performance at higher data rates than UTP.
- ✓ Eliminates crosstalk. And Faster.

Disadvantages:

- ✓ More difficult to install and manufacture.
- ✓ More expensive and Bulky.

- **Applications:** Telephone connections, LAN networks.

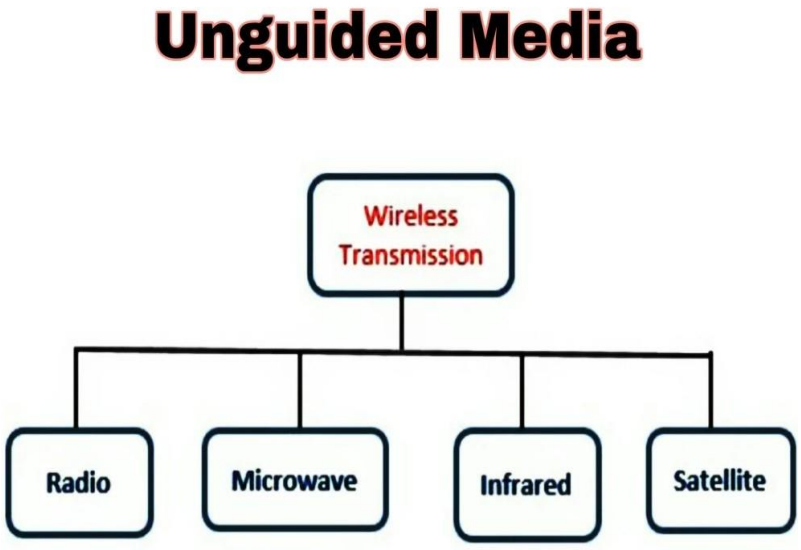
2.Unguided Media (Wireless Transmission):

➢ Unguided media transport electromagnetic waves without using a physical conductor. It is also known as unbounded or wireless media, and does not rely on physical pathways to transmit signals. Instead, they use wireless communication methods to propagate signals through the air or free space.

❖ Types of Unguided Media:

➢ There are following types of unguided media or wireless transmission.

➢



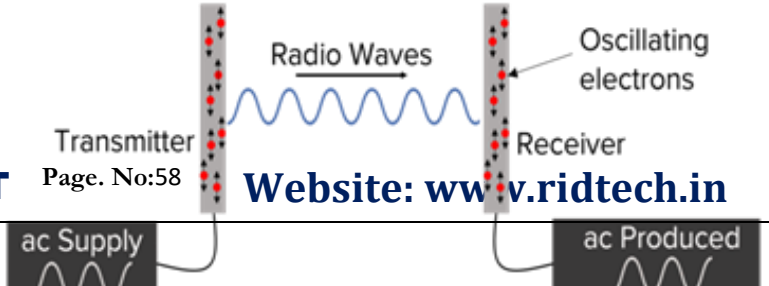
1. Radio Waves:

➢ Radio waves are a type of electromagnetic radiation with the lowest frequencies and the longest wavelengths in the electromagnetic spectrum

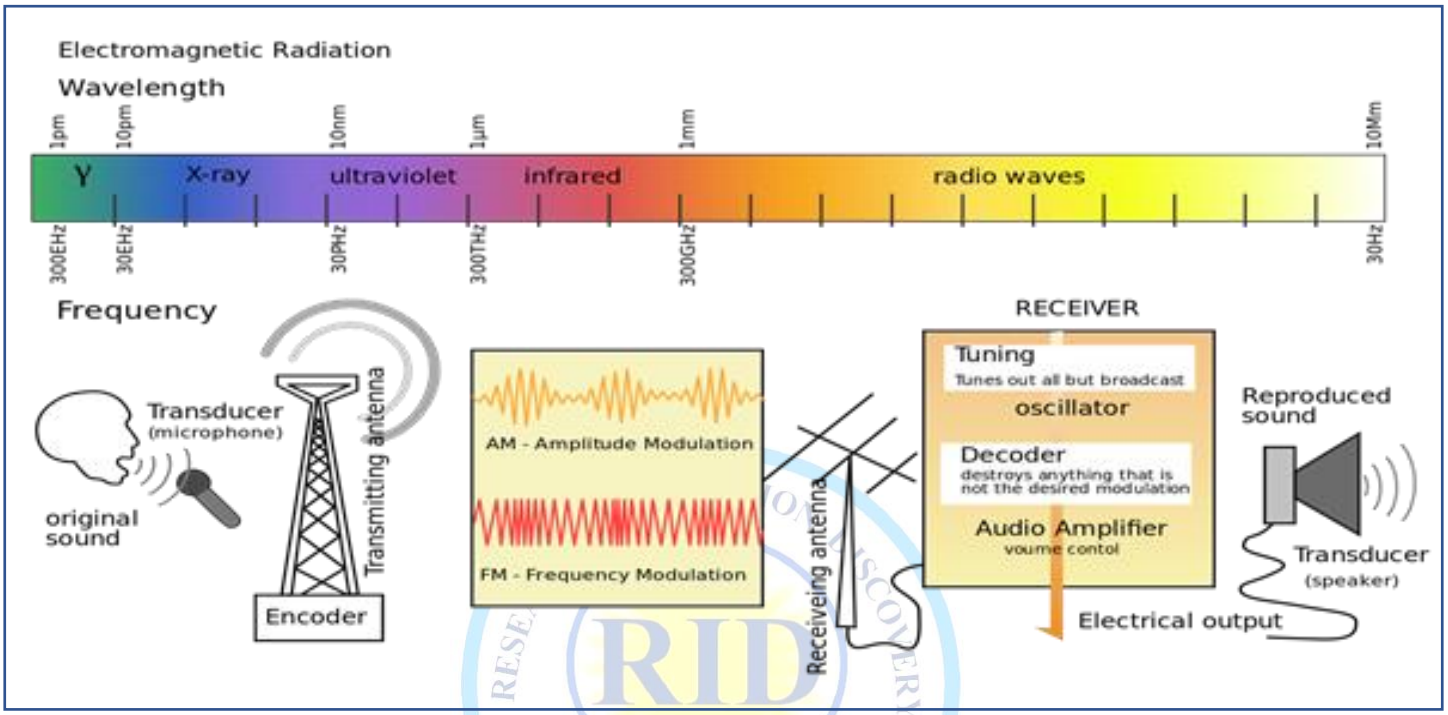
➢

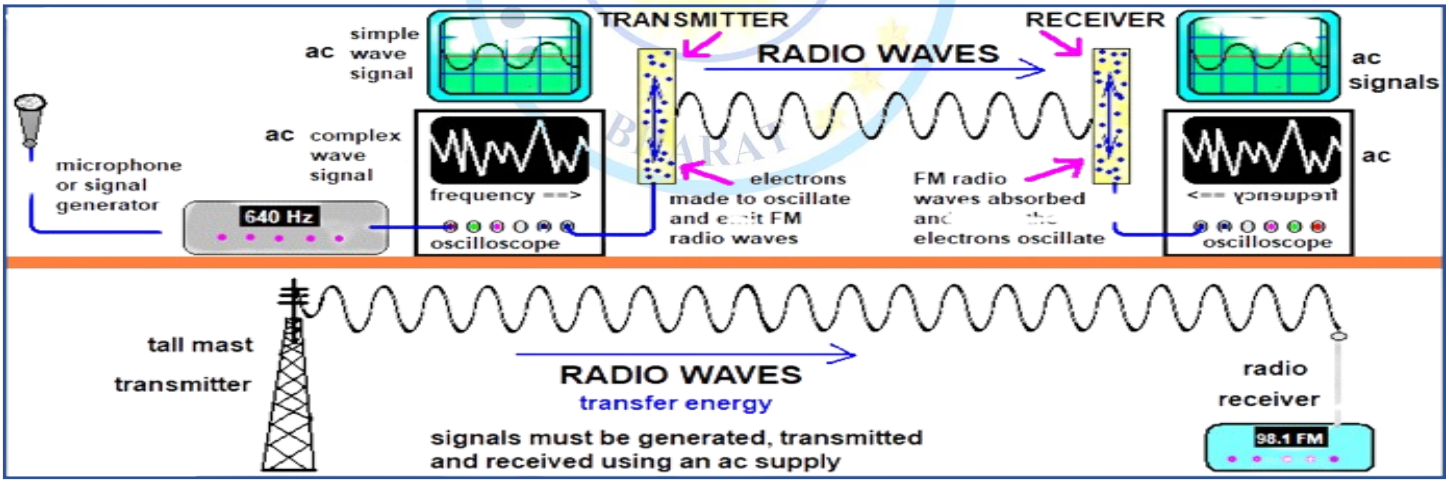
➢ Electromagnetic signals used for Wi-Fi, Bluetooth, and radio broadcasting. Frequency range: 3 kHz to 1 GHz.

➢



- **Characteristics:**
  - Omni-directional (propagated in all directions).
  - Susceptible to interference.
- **Applications:** AM/FM radio, television, cordless phones.





2.Microwaves:

- Microwave is a form of electromagnetic radiation with wavelengths shorter than other radio waves (as originally discovered) but longer than infrared waves.
- Electromagnetic waves with frequencies between 1 and 300 GHz.

- **Characteristics:**
  - Unidirectional (sending and receiving antennas must be aligned).
- **Applications:** Microwave communication, satellite communication.

3.Infrared:

- Infrared is electromagnetic radiation (EMR) with wavelengths longer than that of visible light but shorter than microwaves.
- Frequencies from 300 GHz to 400 THz (short-range communication).

❖ **Applications:** Remote controls, short-range data transfer.

"Digital Transmission"

Definition: - Conversation of Data from Analog to Digital is known as Digital Transmission.

Transmission Media: - communication channel that carries information from sender to receiver.

Why Need: - Because Computer store data in Digital Form.

- carry the information in the form of bits. It's support Physical Layer, OSI Model
- Data is transmitted through the electromagnetic
- It is a physical path between transmitter and receiver.

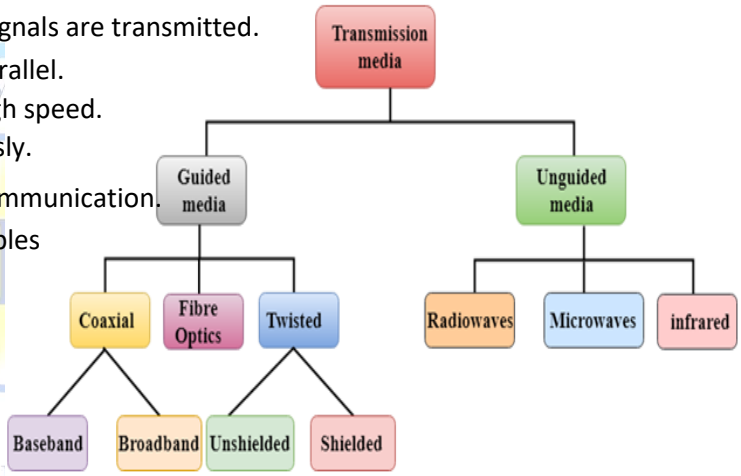
❖ Guided Media is physical medium through which the signals are transmitted.

- Coaxial cable is TV wire it contains two conductors parallel.

1.Baseband: - process of transmitting a single signal at high speed.
2.Broadband: - Transmitting multiple signals simultaneously.

- Fibre optic is a cable that uses electrical signals for communication.
- Twisted pair is physical media made up of a pair of cables

1. unshielded is widely used in telecommunication.
2. shielded is a cable that contains mesh surrounding wire that allows higher transmission rate.



❖ unguided Media transmits electromagnetic waves without using any physical medium. (wireless)

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Microwaves are of two types:

1. Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
2. satellite is a physical object that revolves around the earth at a known height.

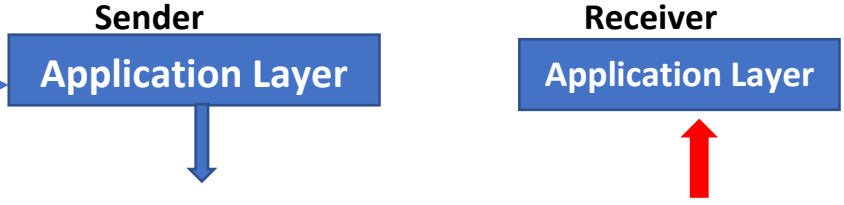
- infrared transmission is a wireless technology used for communication over short ranges.

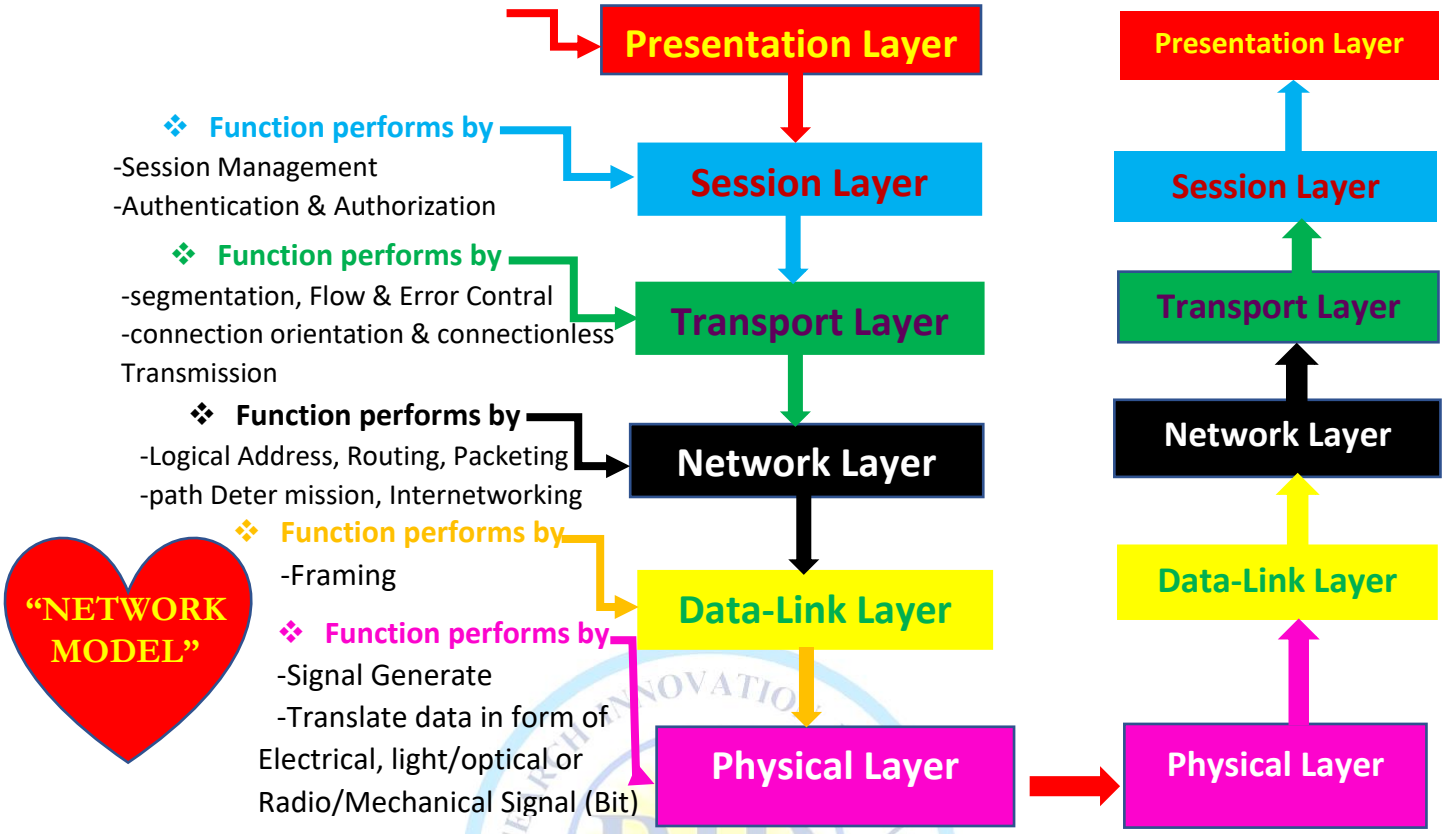
OSI MODEL

OSI Model: - Open System Interconnection Model. OSI model was developed by the International Organization for Standardization (ISO) in 1984, it is a reference model.

❖ **Function performs by**
-Used by computer application
-Application layer Protocols
(HTTPS, FTP, SMTP TALENT etc.

❖ **Function performs by**
-Data translation & compression
-Data encryption & decryption





- **OSI (Open Systems Interconnection)** model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers. Each layer in the OSI model represents a specific function necessary for network communication, and these layers work together to enable data transmission between devices on a network.
- First developed in **1978** by **French software engineer** and **pioneer**, Hubert Zimmermann, The **OSI Model** has become widely adopted by all major computer and telecommunication companies since its inception in **1984.** It belongs to the **International Organization for Standards (ISO)** and its identification is ISO/IEC 7498–1.
- **International Organization for Standardization (ISO)** is an independent, non-governmental international organization that develops and publishes voluntary international standards. **ISO was founded in 1947** and is headquartered in **Geneva, Switzerland**.
- **ISO develops** standards in a wide range of areas, including technology, manufacturing, healthcare, agriculture, and services. These standards provide specifications and guidelines to ensure consistency, quality, safety, and efficiency in products, processes, and services. ISO standards cover diverse fields such as **quality management (ISO 9001),** environmental management **(ISO 14001)**, **information security (ISO 27001)**, and many others.

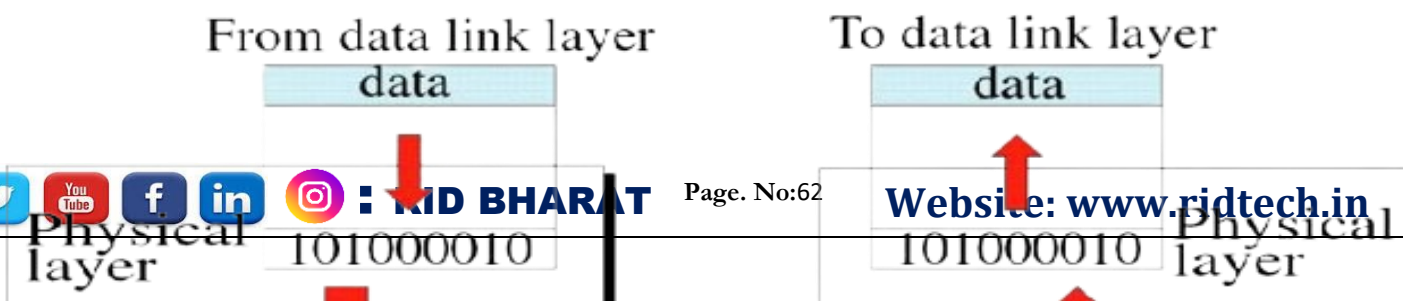
➢ OSI model consists of seven layers.

1. **Physical Layer**
2. **Data Link Layer**
3. **Network Layer**
4. **Transport Layer**
5. **Session Layer**
6. **Presentation Layer**
7. **Application Layer**

1. Physical Layer:

1.PHYSICAL LAYER

- Physical Layer is the bottom-most layer in the Open System Interconnection (OSI) Model which is a physical and electrical representation of the system. It consists of various network components such as power plugs, connectors, receivers, cable types, etc.
- Physical layer sends data bits from one device(s) (like a computer) to another device(s). The physical Layer defines the types of encoding (that is how the 0's and 1's are encoded in a signal). The physical Layer is responsible for the communication of the unstructured raw data streams over a physical medium.



❖ Function of physical layer:

1. Data Rate Maintenance:

- The Physical Layer ensures the data rate at which a sender can transmit bits per second.
- It manages the flow of data between devices.

2. Bit Synchronization:

- Achieves synchronization by ensuring that receiver's clock is aligned with sender's clock.
- This synchronization prevents data loss or corruption during transmission.

3. Transmission Medium Decisions:

- Determines the direction of data transfer (simplex, half-duplex, or full-duplex).
- Considers factors like unidirectional or bidirectional communication.

4. Physical Topology Decisions:

➢ Helps choose the appropriate physical topology for connecting devices:

- **Mesh Topology:** Each device has a dedicated point-to-point connection with every other device, ensuring data security.
- **Star Topology:** Devices connect to a central controller or hub, making installation and reconnection easier.
- **Bus Topology:** Multiple devices share a single cable with tap and drop lines.
- **Ring Topology:** Devices form a circular ring connected by repeaters.

5. Physical Medium and Interface Decisions:

- Selects the physical medium (e.g., copper cables, fiber optics) for data transmission.
- Defines the interface between devices (PCs or computers) and the transmission medium.

6. Configuration Types:

➢ Provides two types of configurations:

- **Point-to-Point:** Direct connection between two devices.
- **Multi-Point:** Multiple devices share a common communication channel.

7. Modulation:

- Converts data into radio waves by adding information to an electrical or optical nerve signal. Essential for wireless communication.

8. Switching Mechanism:

- Enables data packets to be forwarded from one port (sender port) to the destination port.
- Devices like hubs and Ethernet switches operate at this layer.

❖Examples of physical Layer Protocols:

1. Fiber Optic Cables:

- These use light signals to transmit data over long distances.

- High bandwidth, low attenuation, and immunity to electromagnetic interference.
- Commonly used in high-speed internet connections and long-haul networks.

2. Integrated Services Digital Network (ISDN):

- Provides digital communication over traditional telephone lines.
- Supports voice, data, and video transmission.
- Used for video conferencing, remote access, and digital subscriber lines (DSL).

3. Ethernet:

- A widely used protocol for local area networks (LANs).
- Defines how data packets are placed on the network medium (e.g., twisted-pair cables).
- Variants include 10BASE-T, 100BASE-TX, and 1000BASE-T.

4. Bluetooth:

- Enables wireless communication between devices over short distances.
- Used for connecting headphones, speakers, smartphones, and smartwatches.
- Bluetooth versions include Bluetooth 4.0, Bluetooth 5.0, and newer iteration

5. Wi-Fi (IEEE 802.11):

- Wi-Fi is a wireless networking technology based on the IEEE 802.11 standards.
- It operates at both the Physical and Data Link layers of the OSI model and defines protocols for wireless communication, including modulation techniques, frequency bands, and channel access methods.

6. Universal Serial Bus (USB):

- Used for connecting devices like keyboards, mice, printers, and external drives.
- Provides a common interface for data transfer and power supply.
- USB versions include USB 2.0, USB 3.0, and USB-C.

7. Controller Area Network (CAN):

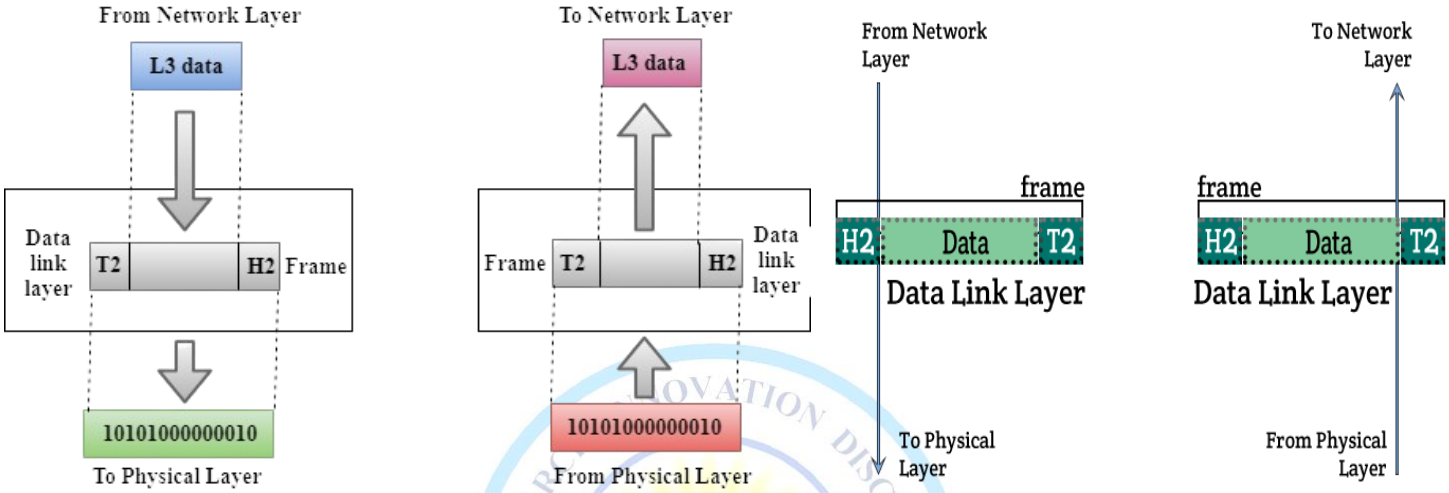
- Primarily used in automotive applications for communication between electronic control units (ECUs).
- Supports real-time data exchange and fault tolerance.
- Ensures reliable communication in vehicles.

❖ Key Points about Physical Layer:

1) The physical layer maintains the data rate (how many bits a sender can send per second).
2) It performs the Synchronization of bits.
3) It helps in Transmission Medium decisions (direction of data transfer).
4) It helps in Physical Topology (Mesh, Star, Bus, Ring) decisions (Topology through which we can connect the devices with each other).
5) It helps in providing Physical Medium and Interface decisions.
6) It provides two types of configuration Point Point configuration and Multi-Point configuration.
7) It provides an interface between devices (like PCs or computers) and transmission medium.
8) It has a protocol data unit in bits.
9) Hubs, Ethernet, etc. device is used in this layer.
10) This layer comes under the category of Hardware Layers (since the hardware layer is responsible for all the physical connection establishment and processing too).
11) It provides an important aspect called Modulation, which is the process of converting the data into radio waves by adding the information to an electrical or optical nerve signal.
12) It also provides a Switching mechanism wherein data packets can be forwarded from one port (sender port) to the leading destination port.

2.DATA LINK LAYER

- The Data Link Layer is the second layer of the OSI (Open Systems Interconnection) model, residing just above the Physical Layer. It is responsible for the reliable transfer of data between adjacent nodes on the same network segment. The Data Link Layer ensures that data packets are delivered error-free and in the correct order.



1. Purpose and Responsibilities:

- The Data Link Layer facilitates node-to-node communication within a network segment.
- Its primary responsibilities include error-free transmission, framing, addressing, and flow control.
- DLL ensures that data frames are correctly transmitted between adjacent devices.

2. Sub-Layers of the Data Link Layer:

- The DLL is further divided into two sub-layers:

a. Logical Link Control (LLC):

- Manages multiplexing (sharing the communication channel among different applications).
- Handles flow control and provides error messages and acknowledgments.

b. Media Access Control (MAC):

- Manages device interactions and controls physical media access.
- Responsible for addressing frames and handling collision avoidance.

3. Functions of the Data Link Layer:

a. Framing:

- DLL receives packets from the Network Layer and divides them into smaller frames.
- Each frame contains data along with special bits (for error control and addressing).

b. Addressing:

- The DLL encapsulates the source and destination MAC addresses in the frame header.
- MAC addresses are unique hardware addresses assigned during device manufacturing.

c. Error Control:

- Detects and corrects errors in transmitted data using error detection and correction techniques.

- Adds error detection bits to the frame header.

d. Flow Control:

- Synchronizes sender and receiver speeds to prevent buffer overflow.
- Ensures efficient data transfer without loss.

e. Access Control:

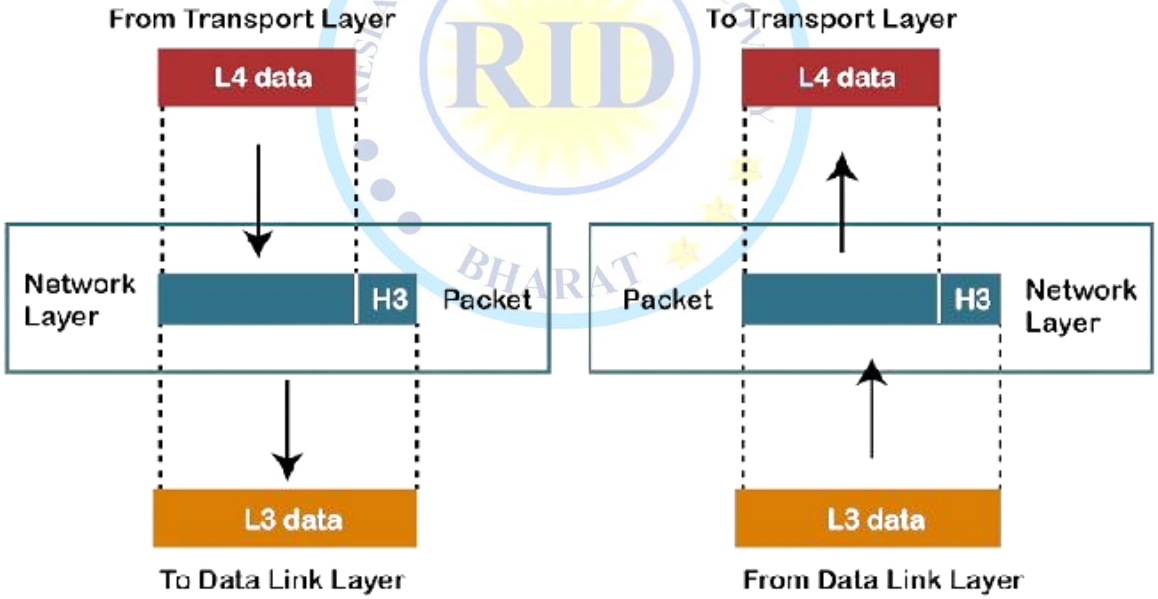
- Manages shared communication channels to avoid collisions.
- Techniques like CSMA/CD (Carrier Sense Multiple Access with Collision Detection) and CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) are used.

4. Examples of Data Link Layer Devices and Protocols:

- **Switches:** Operate at this layer, forwarding frames based on MAC addresses.
- **Bridges:** Connect separate LAN segments, filtering traffic based on MAC addresses.
- **Network Interface Cards (NICs):** Hardware components that enable devices to connect to a network.
- **Ethernet:** A widely used protocol for LANs, defining frame structure and addressing

3.NETWORK LAYER

➢ Network Layer is the third layer of the OSI (Open Systems Interconnection) model, responsible for routing data packets between different networks to reach their intended destinations. It provides logical addressing, routing, and path determination functions to enable end-to-end communication across interconnected networks.



1. Function or Responsibilities of Network Layer:

a. Packet Forwarding: The Network Layer is responsible for forwarding data packets from the source to the destination, even when they need to traverse multiple networks.

b. Packet Switching: The Network Layer supports packet-switched networks, where data is divided into smaller packets for transmission. These packets are independently routed through the network and reassembled at the destination.

c. Routing: It determines the optimal path for data packets to reach their destination. This involves making decisions based on network topology, addressing, and routing algorithms.

d. **Path Determination:** Network Layer determines specific path that data packets will take to reach their destination. This involves selecting intermediate routersalong the route and establishing logical connections between them to forward packets toward the destination.
e. **Logical Addressing:** The Network Layer assigns logical addresses (such as IP addresses) to devices. These addresses help identify the source and destination of data packets.
f. **Fragmentation and Reassembly:** When data packets are too large to fit within the maximum transmission unit (MTU) of a network segment, the Network Layer breaks them into smaller fragments for transmission. At the destination, it reassembles these fragments into the original packets.
g. **Error Handling:** The Network Layer detects and handles errors in data transmission. If a packet encounters issues during its journey, the Network Layer can request retransmission or take corrective actions.
h. **Congestion Control:** Congestion control mechanisms regulate the flow of data through the network to prevent network congestion and packet loss. The Network Layer monitors network

2. Key Components of the Network Layer:

a. **IP Addresses:** The Network Layer uses IP addresses (IPv4 or IPv6) to uniquely identify devices on a network. These addresses are essential for routing and forwarding.
b. **Routers:** Routers operate at the Network Layer. They examine packet headers, make routing decisions, and forward packets between different networks.
c. **Subnetting:** The Network Layer allows for subnetting, which involves dividing a large network into smaller subnetworks. Each subnetwork has its own unique address range.

3. Examples of Network Layer Protocols:

a. **Internet Protocol (IP):** The most prominent protocol at this layer. It provides logical addressing and routing.
b. **Internet Control Message Protocol (ICMP):** Used for error reporting and diagnostics
c. **Internet Group Management Protocol (IGMP):** Facilitates multicasting within IP networks.
d. **Routing Protocols:** Examples include RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol).

4. Network Layer Devices:

a. **Routers:** As mentioned earlier, routers operate at this layer. They connect different networks and make intelligent routing decisions.
b. **Layer 3 Switches:** These devices combine features of switches (Data Link Layer) and routers (Network Layer) to improve network performance.

5. Advantages of Network Layer Services:

- ✓ Packetization service in the network layer provides ease of transportation of the data packets.
- ✓ Packetization also eliminates single points of failure in data communication systems.
- ✓ Routers present in the network layer reduce network traffic by creating collision and broadcast domains.
- ✓ With the help of Forwarding, data packets are transferred from one place to another in the network.

6. Disadvantages of Network Layer Services:

- ✓ There is a lack of flow control in the design of the network layer.

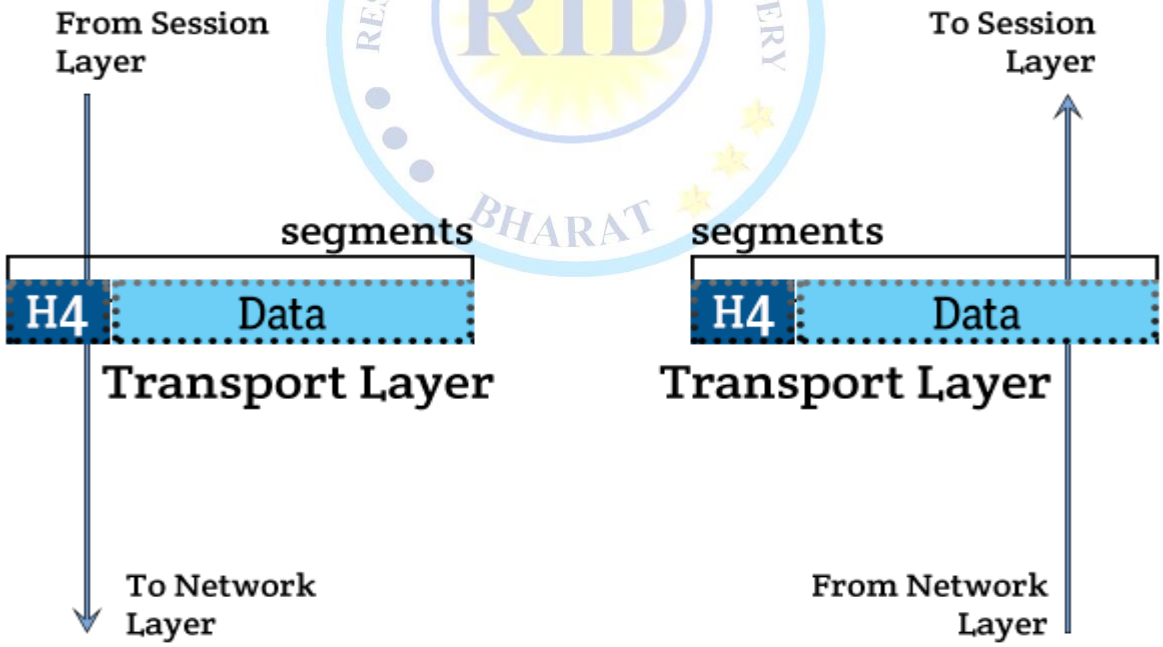
- ✓ Congestion occurs sometimes due to the presence of too many datagrams in a network that is beyond the capacity of the network or the routers. Due to this, some routers may drop some of the datagrams, and some important pieces of information may be lost.
- ✓ Although indirect error control is present in the network layer, there is a lack of proper error control mechanisms as due to the presence of fragmented data packets, error control becomes difficult to implement.

Note:

- Network Layer plays a crucial role in enabling end-to-end communication across interconnected networks, ensuring that data packets are routed efficiently and reliably from the source to the destination. It forms the backbone of the internet and other wide-area networks, facilitating global connectivity and information exchange.

4.TRANSPORT LAYER

➢ Transport Layer is the fourth layer of the OSI (Open Systems Interconnection) model, situated above the Network Layer and below the Session Layer. It is responsible for providing reliable, end-to-end communication between processes running on different hosts across a network. The Transport Layer ensures that data is delivered accurately, efficiently, and in the correct order.



❖ Working of Transport Layer:

➢ transport layer takes services from the Application layer and provides services to Network layer.

1. **sender's side:** The transport layer receives data (message) from the Application layer and then performs Segmentation, divides the actual message into segments, adds the source and destination's port numbers into the header of the segment, and transfers the message to the Network layer.

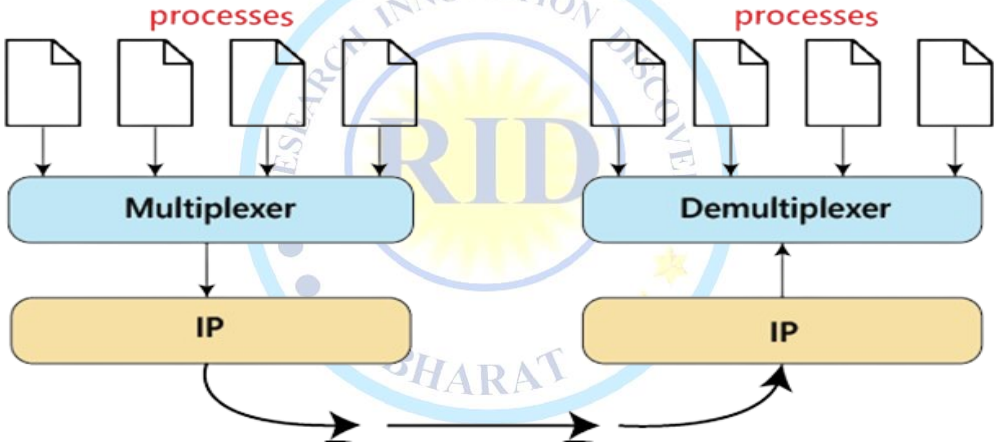
2. **receiver's side:** The transport layer receives data from the Network layer, reassembles the segmented data, reads its header, identifies the port number, and forwards the message to the appropriate port in the Application layer.

❖ Responsibilities of a Transport Layer:

1. The Process to Process Delivery
2. End-to-End Connection between Hosts
3. Multiplexing and Demultiplexing
4. Congestion Control
5. Data integrity and Error correction
6. Flow control

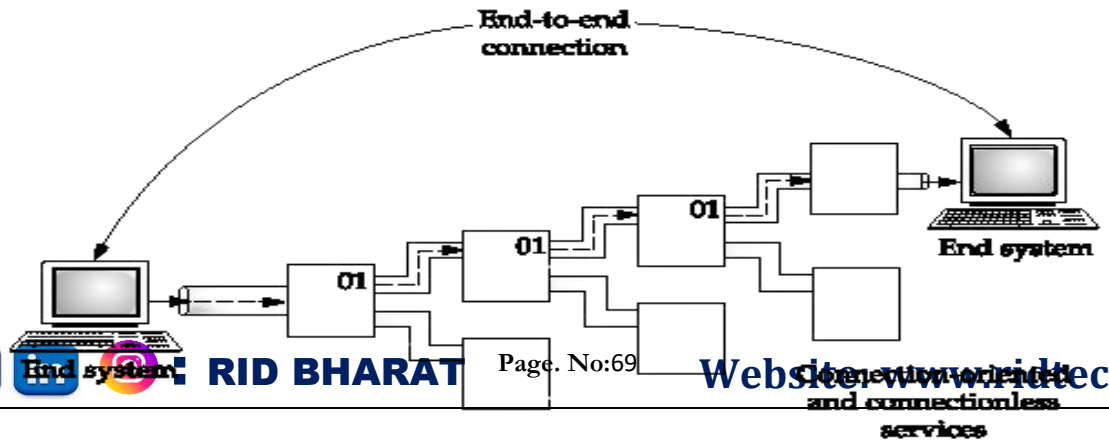
1. The Process-to-Process Delivery:

- While Data Link Layer requires the MAC address (48 bits address contained inside the Network Interface Card of every host machine) of source-destination hosts to correctly deliver a frame and the Network layer requires the IP address for appropriate routing of packets, in a similar way Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A port number is a 16-bit address used to identify any client-server program uniquely.



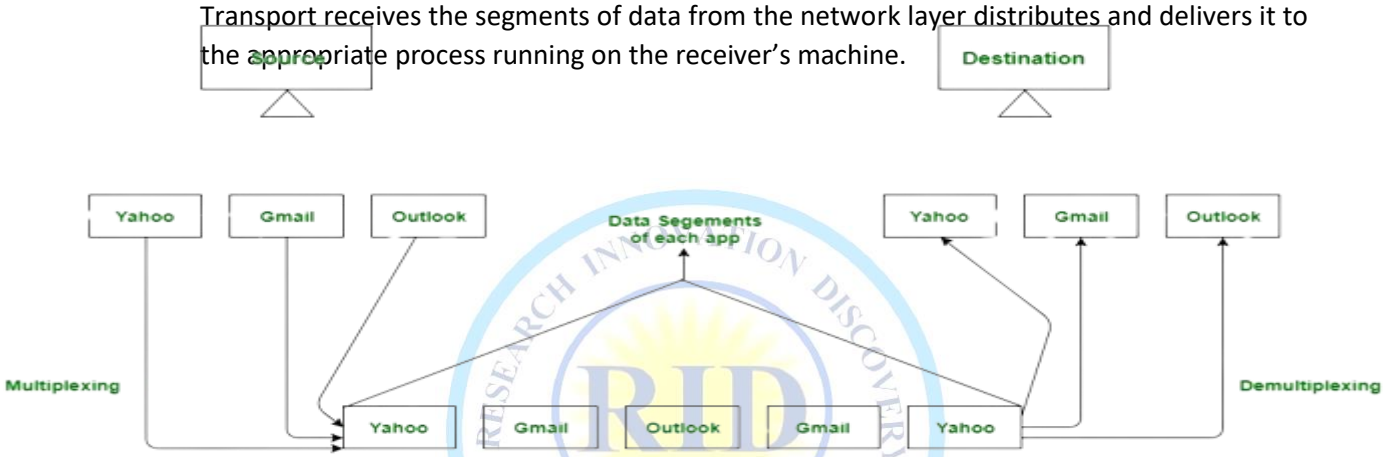
2. End-to-end Connection between Hosts:

- The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection-orientated protocol that uses a handshake protocol to establish a robust connection between two end hosts. TCP ensures the reliable delivery of messages and is used in various applications. UDP, on the other hand, is a stateless and unreliable protocol that ensures best-effort delivery. It is suitable for applications that have little concern with flow or error control and requires sending the bulk of data like video conferencing. It is often used in multicasting protocols.



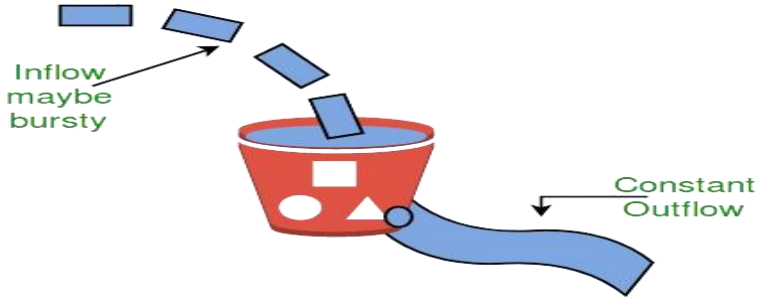
3. Multiplexing and Demultiplexing:

- Multiplexing(many to one) is when data is acquired from several processes from the sender and merged into one packet along with headers and sent as a single packet. Multiplexing allows the simultaneous use of different processes over a network that is running on a host. The processes are differentiated by their port numbers. Similarly, Demultiplexing(one to many is required at the receiver side when the message is distributed into different processes. Transport receives the segments of data from the network layer distributes and delivers it to the appropriate process running on the receiver's machine.



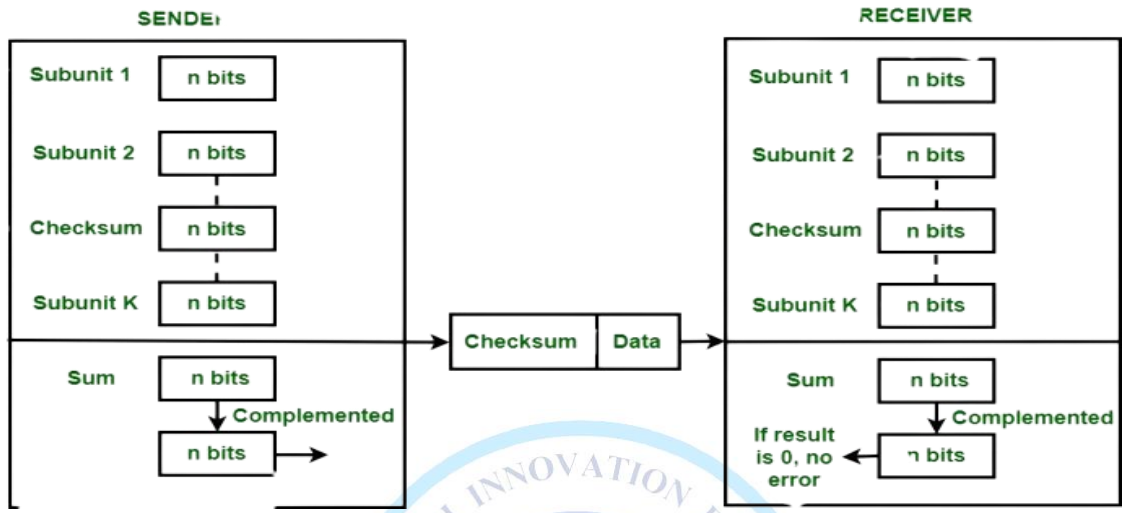
4. Congestion Control:

- Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occurs. As a result, the retransmission of packets from the sources increases the congestion further. In this situation, the Transport layer provides Congestion Control in different ways. It uses open-loop congestion control to prevent congestion and closed-loop congestion control to remove the congestion in a network once it occurred. TCP provides AIMD – additive increases multiplicative decrease and leaky bucket technique for congestion control.



5. Data integrity and Error Correction:

- The transport layer checks for errors in the messages coming from the application layer by using error detection codes, and computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.



6. Flow Control:

- The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

❖ Protocols of Transport Layer:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Stream Control Transmission Protocol (SCTP)
- Datagram Congestion Control Protocol (DCCP)
- AppleTalk Transaction Protocol (ATP)
- Fibre Channel Protocol (FCP)
- Reliable Data Protocol (RDP)
- Reliable User Data Protocol (RUDP)
- Structured Steam Transport (SST)
- Sequenced Packet Exchange (SPX)

❖ **TCP (Transmission Control Protocol):** Provides reliable, connection-oriented communication. It ensures data integrity, sequencing, and flow control.

❖ **UDP (User Datagram Protocol):** Offers connectionless communication. It's faster but doesn't guarantee reliability. Commonly used for real-time applications like streaming and VoIP.

❖ Key Points:

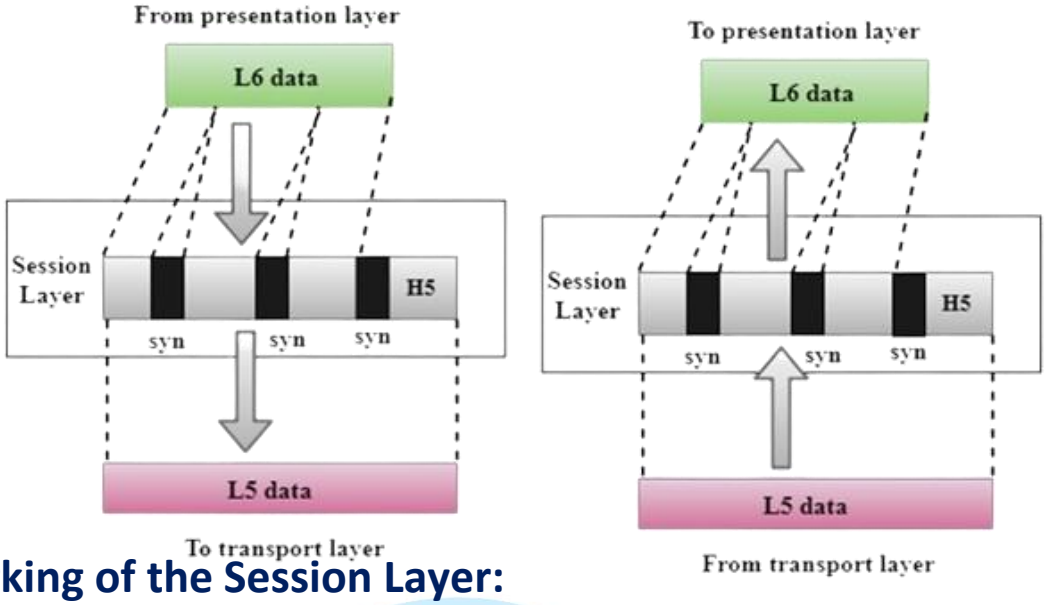
1) **Segmentation and Reassembly:** Segmentation involves breaking down data from the higher layers into smaller units called segments for transmission over the network. Reassembly is the process of reconstructing the original data stream from received segments at the destination.

2) **Connection-Oriented vs. Connectionless Communication:** Connection-oriented communication establishes a logical connection between sender and receiver before data exchange, ensuring reliable delivery and sequencing of data. Connectionless communication does not require prior setup and simply sends data without guaranteeing delivery or ordering.
3) **Protocols:** TCP (Transmission Control Protocol) is a connection-oriented protocol that provides reliable, ordered delivery of data packets. UDP (User Datagram Protocol) is a connectionless protocol that offers lightweight, best-effort delivery without reliability guarantees.
4) **Reliable Data Delivery:** Reliable data delivery ensures that data packets are delivered accurately and in the correct order. TCP achieves reliability through acknowledgment, sequencing, and retransmission mechanisms to detect and recover from lost or corrupted packets.
5) **Error Detection:** Error detection involves identifying errors, such as transmission errors or data corruption, that may occur during data transmission. TCP and UDP use checksums to detect errors in data packets.
6) **Flow Control:** Flow control regulates the flow of data between sender and receiver to prevent data overflow and ensure that the receiver can handle incoming data at a manageable rate. TCP uses a sliding window mechanism for flow control.
7) **Congestion Control:** Congestion control manages network congestion and prevents packet loss by adjusting transmission rate based on network conditions. TCP implements congestion avoidance algorithms to dynamically adjust the transmission window size and avoid overwhelming network.
8) **Multiplexing and Demultiplexing:** Multiplexing combines multiple data streams into a single transmission stream, while demultiplexing separates incoming data streams and directs them to the appropriate receiving processes based on port numbers or identifiers.
9) **Port Addressing:** Port addressing uses port numbers to identify the source and destination processes running on a host. Port numbers are included in the transport layer header of data packets and allow multiple applications to share the same network interface.
10) **Socket Programming:** Socket programming enables communication between processes running on different hosts using network sockets. Applications interact with the Transport Layer through socket APIs to establish connections, send and receive data, and manage communication sessions.

5.SESSION LAYER

- Session Layer is the fifth layer of the OSI (Open Systems Interconnection) model, situated above the Transport Layer and below the Presentation Layer. It is responsible for establishing, managing, and terminating communication sessions between processes running on different hosts across a network.

- The Session Layer provides services that enable reliable and orderly communication between applications, including session establishment, maintenance, synchronization, and termination.



❖ Working of the Session Layer:

- Session Layer uses services provided by Transport Layer to enable applications to establish and maintain sessions and synchronize them. To establish a session connection, several steps are followed:
  1. **Mapping Session Address:** The session address is mapped to the shipping address.
  2. **Selecting Quality of Service (QoS):** Required transport quality of service parameters are chosen.
  3. **Negotiating Session Parameters:** Negotiations occur between session parameters.
  4. **Transmitting Limited Transparent User Data:** Data is transmitted transparently.
  5. **Monitoring Data Transfer:** Proper monitoring during the data transfer phase is essential.

❖ functions of Session Layer:

- **Dialog Controller:** It allows systems to communicate in either half-duplex or full-duplex mode.
- **Token Management:** Prevents simultaneous access to critical operations by two users.
- **Synchronization:** Adds checkpoints (synchronization points) to data streams.
- **Session Checkpointing and Recovery:** Ensures session integrity.
- Opening, Closing, and Managing Sessions: Between end-user application processes.
- **RPCs (Remote Procedure Calls):** Services offered by the Session Layer are often implemented using RPCs.
- **Synchronizing Information:** Handles synchronization from different sources.
- **Controlling Connections:** Manages single or multiple connections for each end-user application.
- Session Layer works as a dialog controller through which it allows systems to communicate in either half-duplex mode or full duplex mode of communication.
- This layer is also responsible for token management, through which it prevents two users to simultaneously access or attempting the same critical operation.
- This layer allows synchronization by allowing the process of adding checkpoints, which are considered as synchronization points to the streams of data.
- This layer is also responsible for session checkpointing and recovery.
- This layer basically provides a mechanism of opening, closing and managing a session between the end-user application processes.
- The Session Layer is also responsible for synchronizing information from different sources.

- This layer also controls single or multiple connections for each-end user application and directly communicates with both Presentation and transport layers.

❖ Examples of Session Layer Protocols:

- NetBIOS: Used for session establishment in Windows networking.
- PPTP (Point-to-Point Tunneling Protocol): Establishes and manages VPN sessions.
- SMB (Server Message Block): Used for file and printer sharing.

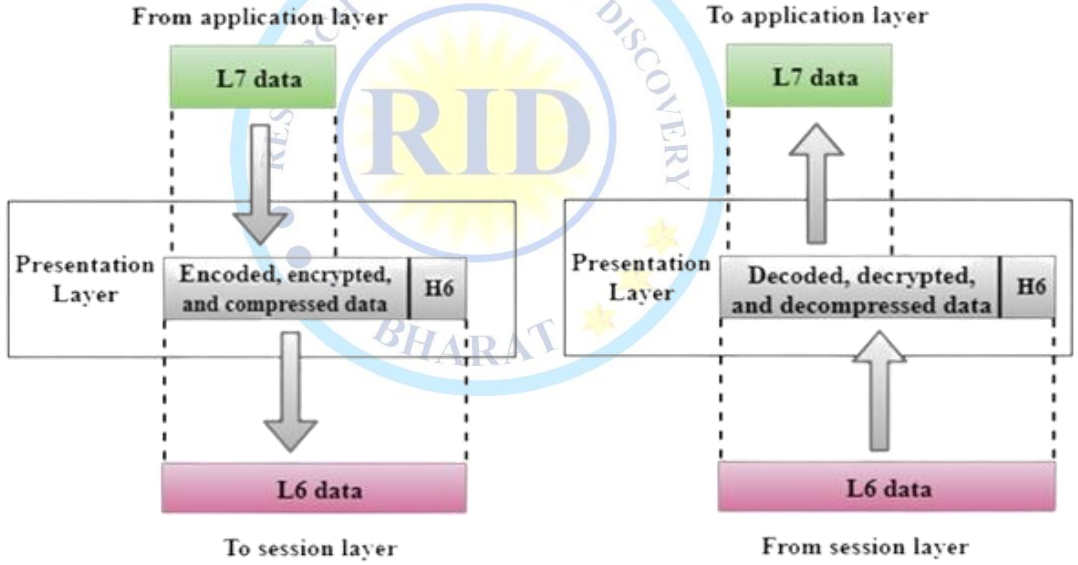
❖ Devices Associated with the Session Layer:

- **Routers:** Although primarily operating at the Network Layer, routers may inspect transport-layer headers for routing decisions.
- **Firewalls:** Examine transport-layer information for security enforcement

6.PRESENTATION LAYER:

➢ Presentation Layer is the sixth layer of the OSI (Open Systems Interconnection) model, situated above the Session Layer and below the Application Layer. It is responsible for ensuring that data exchanged between applications is presented in a format that is understandable and usable by the receiving application.

➢ The Presentation Layer provides services related to data translation, encryption, compression, and formatting to facilitate interoperability and compatibility between different systems.



❖ Responsibilities of the Presentation Layer:

1) **Data Format Translation:** The Presentation Layer takes data received from the Application Layer and manipulates it into the required format for transmission over the network. It ensures that the receiver can efficiently interpret and utilize the data.
2) **Abstract Data Structures:** This layer manages abstract data structures, allowing high-level data (such as banking records) to be defined and exchanged.
3) **Encryption and Decryption:** The Presentation Layer handles encryption at the transmitter and decryption at the receiver. It ensures data security during transmission.
4) **Data Compression:** To optimize bandwidth usage, the Presentation Layer performs data compression, reducing the number of bits transmitted.
5) **Interoperability:** Different computers use varying encoding methods. The Presentation Layer ensures interoperability by handling encoding differences.

6) **String Representation:** It deals with issues related to string representation in data.
7) **Standardization:** The Presentation Layer integrates various formats into a standardized format for efficient communication.
8) **Syntax and Semantics:** Ensures that messages presented to upper and lower layers adhere to accurate and standardized formats.
9) **Serialization:** Converts data structures into a format suitable for storage or transmission.

❖ Examples of Presentation Layer Tasks:

- **File Format Conversion:** The Presentation Layer translates different file formats, allowing two systems to communicate effectively.
- **Data Compression:** Reduces the bandwidth required for data transmission.
- **Encryption:** Ensures data privacy and security.
- **String Handling:** Deals with character encoding and representation.
- **Standardization:** Converts user-dependent formats to a common format for communication between dissimilar systems.

❖ Devices Associated with the Presentation Layer:

- **Routers:** Although routers primarily operate at the Network Layer, they may inspect transport-layer headers for routing decisions.
- **Firewalls:** Examine transport-layer information for security enforcement.

❖ Function of Presentation Layer:

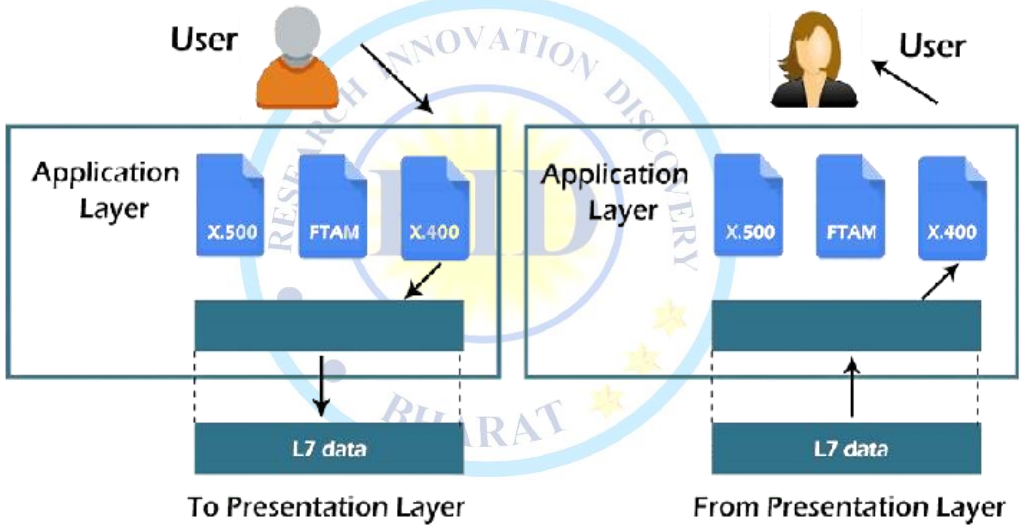
- Presentation layer format and encrypts data to be sent across the network.
- This layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data efficiently and effectively.
- This layer manages the abstract data structures and allows high-level data structures (example- banking records), which are to be defined or exchanged.
- This layer carries out the encryption at the transmitter and decryption at the receiver.
- This layer carries out data compression to reduce the bandwidth of the data to be transmitted (the primary goal of data compression is to reduce the number of bits which is to be transmitted).
- This layer is responsible for interoperability between encoding methods as different computers use different encoding methods.
- This layer basically deals with the presentation part of the data.
- Presentation layer, carries out the data compression (number of bits reduction while transmission), which in return improves the data throughput.
- This layer also deals with the issues of string representation.
- The presentation layer is also responsible for integrating all the formats into a standardized format for efficient and effective communication.
- This layer encodes the message from the user-dependent format to the common format and vice-versa for communication between dissimilar systems.
- This layer deals with the syntax and semantics of the messages.
- This layer also ensures that the messages which are to be presented to the upper as well as the lower layer should be standardized as well as in an accurate format too.
- This layer also performs serialization (process of translating a data structure or an object into a format that can be stored or transmitted easily).

❖ Working of Presentation Layer in the OSI model :

- Presentation layer in the OSI model, as a translator, converts the data sent by the application layer of the transmitting node into an acceptable and compatible data format based on the applicable network protocol and architecture. Upon arrival at the receiving computer, the presentation layer translates data into an acceptable format usable by the application layer. Basically, in other words, this layer takes care of any issues occurring when transmitted data must be viewed in a format different from the original format. Being the functional part of the OSI mode, the presentation layer performs a multitude (large number of) data conversion algorithms and character translation functions. Mainly, this layer is responsible for managing two network characteristics: protocol (set of rules) and architecture.

6.APPLICATION LAYER:

- Application Layer is the topmost layer of the OSI (Open Systems Interconnection) model, situated above the Presentation Layer. It is responsible for providing network services directly to end-users or applications and enabling communication between applications running on different hosts across a network.
- The Application Layer encompasses a wide range of protocols, services, and applications that facilitate user interaction, data exchange, and distributed computing.



❖ Functions of the Application Layer:

1. **Data Format Translation:** The Application Layer ensures that data exchanged between different systems is correctly understood. It handles data format translation.
2. **User Interaction:** Users directly interact with the software applications at this layer. It provides a bridge between the user and the network.
3. **Email Services:** Application Layer allows users to forward emails and provides storage facilities.
4. **File Management:** Users can access, retrieve, and manage files on remote computers.
5. **Remote Login:** Users can log in to remote hosts.
6. **Global Information Access:** Provides access to global information services.
7. **Protocols for Data Exchange:** Offers protocols for sending and receiving information.
8. **Network Transparency:** Ensures seamless communication across different networks.
9. **Resource Allocation:** Handles issues related to resource allocation.
10. **Host Initialization:** Prepares hosts for communication.
11. **Interacting with Operating Systems:** The Application Layer interacts with the OS to preserve data in a suitable manner.
12. **Synchronization and Identification:** Helps identify communication partners and synchronizes communication.

❖ Features provided by Application Layer Protocols:

- To ensure smooth communication, application layer protocols are implemented the same on source host and destination host.
- The following are some of the features which are provided by Application layer protocols-
- The Application Layer protocol defines process for both parties which are involved in communication.
- These protocols define the type of message being sent or received from any side (either source host or destination host).
- These protocols also define basic syntax of the message being forwarded or retrieved.
- These protocols define the way to send a message and the expected response.
- These protocols also define interaction with the next level.

❖ **Application Layer Protocols:** The application layer provides several protocols which allow any software to easily send and receive information and present meaningful data to its users.

➢ The following are some of the protocols which are provided by the application layer.

1) **TELNET:** Telnet stands for Telecommunications Network. This protocol is used for managing files over the Internet. It allows the Telnet clients to access the resources of Telnet server. Telnet uses port number 23.
2) **DNS:** DNS stands for Domain Name System. The DNS service translates the domain name (selected by user) into the corresponding IP address. For example- If you choose the domain name as www.abcd.com, then DNS must translate it as 192.36.20.8 (random IP address written just for understanding purposes). DNS protocol uses the port number 53.
3) **DHCP:** DHCP stands for Dynamic Host Configuration Protocol. It provides IP addresses to hosts. Whenever a host tries to register for an IP address with the DHCP server, DHCP server provides lots of information to the corresponding host. DHCP uses port numbers 67 and 68.
4) **FTP:** FTP stands for File Transfer Protocol. This protocol helps to transfer different files from one device to another. FTP promotes sharing of files via remote computer devices with reliable, efficient data transfer.
5) **SMTP:** SMTP stands for Simple Mail Transfer Protocol. It is used to transfer electronic mail from one user to another user. SMTP is used by end users to send emails with ease. SMTP uses port numbers 25 and 587.
6) **HTTP:** HTTP stands for Hyper Text Transfer Protocol. It is the foundation of the World Wide Web (WWW). HTTP works on the client server model. This protocol is used for transmitting hypermedia documents like HTML. This protocol was designed particularly for the communications between the web browsers and web servers,HTTP uses port number 80.
7) **NFS:** NFS stands for Network File System. This protocol allows remote hosts to mount files over a network and interact with those file systems as though they are mounted locally.
8) **SNMP:** SNMP stands for Simple Network Management Protocol. This protocol gathers data by polling the devices from the network to the management station at fixed or random intervals, requiring them to disclose certain information.

❖ Working of Application Layer in the OSI model :

- In the OSI model, this application layer is narrower in scope. The application layer in the OSI model generally acts only like the interface which is responsible for communicating with host-based and user-facing applications.
- This is in contrast with TCP/IP protocol, wherein the layers below the application layer, which is Session Layer and Presentation layer, are clubbed together and form a simple single layer

which is responsible for performing the functions, which includes controlling the dialogues between computers, establishing as well as maintaining as well as ending a particular session, providing data compression and data encryption and so on.

TCP/IP Model

Transmission Control Internet Protocol

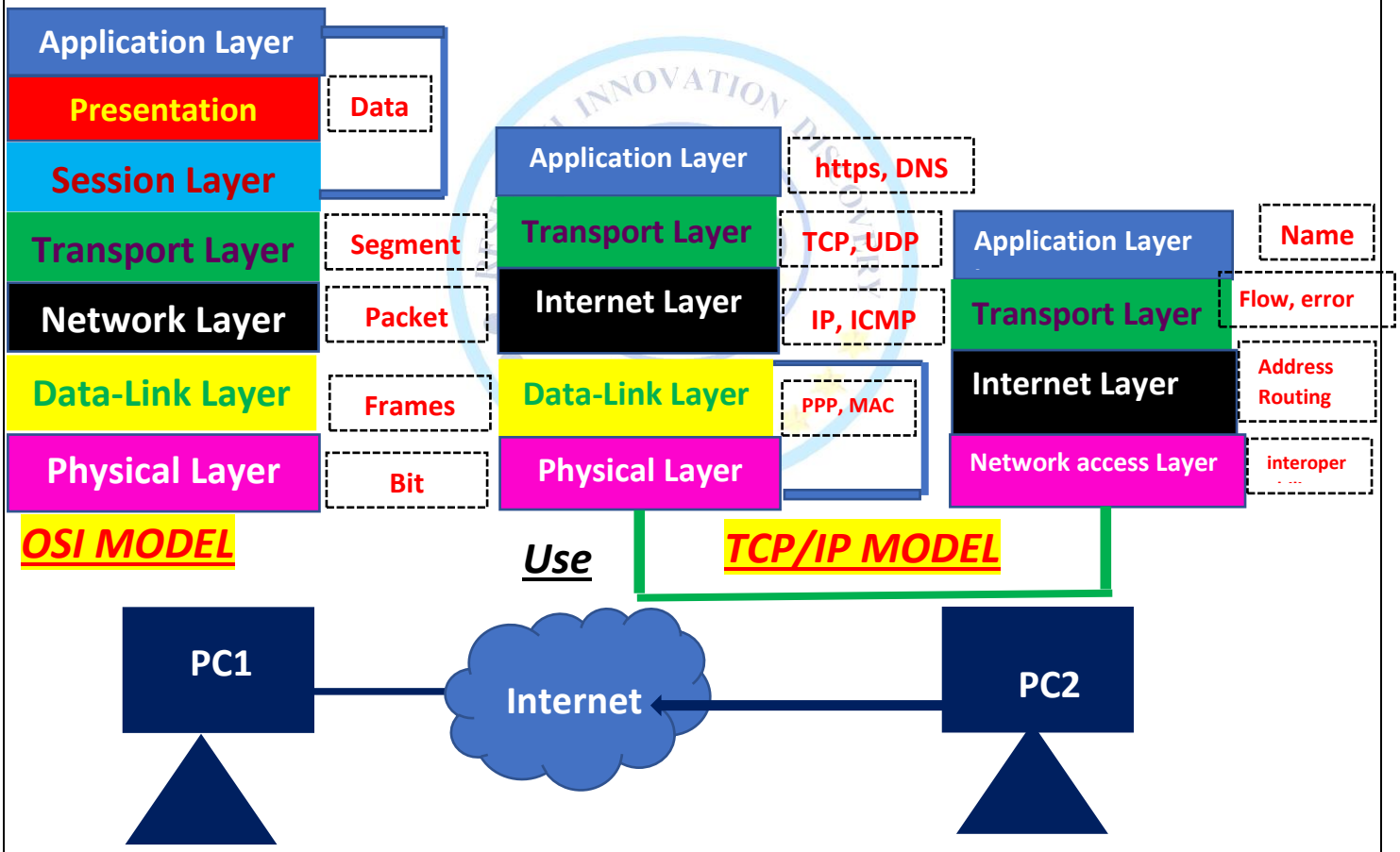
- TCP/IP model developed by American DOD (Defence of Department) in flag day 1-jan-1983. It is practical Model.

❖ what was Problem?

1. How data transmitted across a network. &
2. How data should be formatted so other network system can understand.

❖ **TCP/IP Model Features: -** 1. End Node Verification & 2. Dynamic Routing

TCP/IP Model Layers



Protocols

1. Application Layer (Protocols): - HTTP/HTTPS: - Hypertext Transfer Protocol, **DNS: -** Domain Name System, **FTP: -** File Transfer Protocol HTTPS, DNS, FTP, DHCP, IMCP, IRC, NTP, POP, RTP, SSL, SSH, SMTP etc.

2. Transport Layer (Protocols): - TCP: - Transmission Control Protocol **UDP: -** User Datagram Protocol - TCP, UDP, DCCP, SCTP, RSVP, QUIC etc.

3. Internet Layer (Protocols): - IP: -Internet protocol, **ICMP: -**Internet Control Message Protocol **ARP: -**Address Resolution P IP, ICMP, NDP, ECN, IGMP, IPSEC etc.

4. Data Link Layer (Protocols): - SDLC: - Synchronous Data Link Protocol, **PPP: -** Point to Point Protocol **LCP, IAP, SLIP NCP,MAC** etc.

- The TCP/IP model, also known as the Internet Protocol Suite, is a conceptual framework used for understanding and designing network communication protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model consists of four layers:
  - **Application Layer:** This layer provides interfaces for software applications to communicate over the network. It includes protocols like HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and DNS (Domain Name System).
  - **Transport Layer:** The transport layer is responsible for end-to-end communication between the source and destination hosts. It ensures that data packets are delivered reliably and in order. The two main protocols in this layer are TCP (Transmission Control Protocol), which provides reliable, connection-oriented communication, and UDP (User Datagram Protocol), which provides connectionless, unreliable communication.
  - **Internet Layer:** This layer handles the transmission of data packets across different networks. It is primarily concerned with routing packets from the source host to the destination host. The main protocol in this layer is IP (Internet Protocol), which provides the addressing and routing functions necessary for data transmission across the internet.
  - **Link Layer:** Also known as the Network Interface Layer or Network Access Layer, this layer deals with the physical and data link aspects of network communication. It includes protocols and technologies specific to the physical network medium, such as Ethernet, Wi-Fi, and PPP (Point-to-Point Protocol).
- TCP/IP model is the foundational framework that underpins the functioning of the internet and many other computer networks. It is a standardized model that allows diverse computer systems to communicate.

❖ History of TCP/IP Model:

- The TCP/IP model was developed during the 1970s by researchers at the Defense Advanced Research Projects Agency (DARPA) in the United States. It was created to enable communication between different types of computer systems on diverse networks, including military and academic networks. Initially, it was designed to meet the communication needs of ARPANET, which was the precursor to the modern internet.
- The TCP/IP model was refined and standardized over time, with key contributions from researchers such as Vint Cerf and Robert Kahn. In 1983, TCP/IP became the standard protocol suite for ARPANET, replacing the earlier NCP (Network Control Program) protocol.

❖ How TCP/IP Works:

- TCP/IP works by breaking data into segments (TCP), attaching addressing information (IP), routing data across networks, reassembling segments at the destination, and delivering it to the application. TCP ensures reliability by acknowledging data receipt and requesting retransmission if needed. IP handles addressing and routing, ensuring data reaches the correct destination. Routers forward data between networks based on IP addresses. Overall, TCP/IP enables communication between devices on different networks reliably and efficiently.

❖ IP Routing Basics:

- IP routing determines the shortest path for data to travel from one computer to another, whether within the same network or across different networks.

- It involves forwarding data packets via routers, which examine the destination address and decide where to send the packet next.
- The process aims to minimize cost and deliver data in the quickest time possible.

❖ Routing Terminology:

- Autonomous System (AS): A collection of networks managed by a single entity.
- Router: The device responsible for forwarding data across multiple networks.
- Routing Table: A table in the router that stores routing information.

❖ Types of Routing:

1. **Static Routing:**
   - Network administrators manually update the routing table.
2. **Dynamic Routing:**
   - Routing tables are automatically updated using routing protocols.
3. **Default Routing:**
   - Configured to send all data toward a specific router (often used with stub routers).
4. **IP Routing Process:**
   - When data is sent from the source to the destination:
   - The TCP and other protocols form an IP packet.
   - This packet traverses multiple routers to reach the destination.
5. **Each router:**
   - Extracts the destination address from the packet.
   - Consults its routing table to identify the next router.
   - Considers factors like cost and other necessary information.
   - Makes a routing decision using routing protocols.

❖ What is the Difference between TCP and IP?

- TCP and IP are different protocols of Computer Networks. The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP. This is the basic difference between TCP and IP.

TCP and UDP in Transport Layer

- Layer 3 or the Network layer uses IP or Internet Protocol which being a connection less protocol treats every packet individually and separately leading to lack of reliability during a transmission. For example, when data is sent from one host to another, each packet may take a different path even if it belongs to the same session. This means the packets may/may not arrive in the right order. Therefore, IP relies on the higher layer protocols to provide reliability.

❖ TCP (Transmission Control Protocol):

➢ TCP is a layer 4 protocol which provides acknowledgement of the received packets and is also reliable as it resends the lost packets. It is better than UDP but due to these features it has an additional overhead. It is used by application protocols like HTTP and FTP.

❖ UDP (User Datagram Protocol):

➢ UDP is also a layer 4 protocol but unlike TCP it doesn't provide acknowledgement of the sent packets. Therefore, it isn't reliable and depends on the higher layer protocols for the same. But on the other hand it is simple, scalable and comes with lesser overhead as compared to TCP. It is used in video and voice streaming.

TCP Vs UDP

1. **Session Multiplexing:**
   - A single host with a single IP address is able to communicate with multiple servers. While using TCP, first a connection must be established between the server and the receiver and the connection is closed when the transfer is completed. TCP also maintains reliability while the transfer is taking place.
   - UDP on the other hand sends no acknowledgement of receiving the packets. Therefore, provides no reliability.
2. **Segmentation:**
   - Information sent is first broken into smaller chunks for transmission.
   - Maximum Transmission Unit or MTU of a Fast Ethernet is 1500 bytes whereas the theoretical value of TCP is 65495 bytes. Therefore, data has to be broken into smaller chunks before being sent to the lower layers. MSS or Maximum Segment Size should be set small enough to avoid fragmentation. TCP supports MSS and Path MTU discovery with which the sender and the receiver can automatically determine the maximum transmission capability.
   - UDP doesn't support this; therefore it depends on the higher layer protocols for data segmentation.
3. **Flow Control:**
   - If sender sends data faster than what receiver can process then the receiver will drop the data and then request for a retransmission, leading to wastage of time and resources. TCP provides end-to-end flow control which is realized using a sliding window. The sliding window sends an acknowledgement from receiver's end regarding the data that the receiver can receive at a time.
   - UDP doesn't implement flow control and depends on the higher layer protocols for the same.
4. **Connection Oriented:**
   - TCP is connection oriented, i.e., it creates a connection for the transmission to take place, and once the transfer is over that connection is terminated.
   - UDP on the other hand is connectionless just like IP (Internet Protocol).
5. **Reliability:**
   - TCP sends an acknowledgement when it receives a packet. It requests a retransmission in case a packet is lost.
   - UDP relies on the higher layer protocols for the same.
6. **Headers:**
   - The size of TCP header is 20-bytes (16-bits for source port, 16-bits for the destination port, 32-bits for seq number, 32-bits for ack number, 4-bits header length)
   - The size of the UDP header is 8-bytes (16-bits for source port, 16-bits for destination port, 16-bits for length, 16-bits for checksum); it's significantly smaller than the TCP header

OSI MODEL VS TCP/IP

1. Number of Layers:

- **OSI Model:** The OSI model consists of seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
- **TCP/IP Model:** TCP/IP model consists of four layers: Application, Transport, Internet, and Link.

2. Layer Structure:

- **OSI Model:** Each layer in the OSI model has a specific function and communicates with adjacent layers only. The layers are more strictly defined, with clear separation of concerns.
- **TCP/IP Model:** The TCP/IP model has fewer layers, and there is often overlap in functionality between layers. For example, the TCP/IP model combines the session, presentation, and application layers of the OSI model into a single application layer.

3. Development History:

- **OSI Model:** The OSI model was developed by the International Organization for Standardization (ISO) in the late 1970s and early 1980s as an abstract framework for network protocols.
- **TCP/IP Model:** The TCP/IP model was developed by researchers at DARPA in the United States during the 1970s to facilitate communication between different types of computer systems on diverse networks, including ARPANET.

4. Protocol Suites:

- **OSI Model:** The OSI model is a theoretical framework and has not been widely implemented in practice. However, it has influenced the development of network protocols and standards.
- **TCP/IP Model:** The TCP/IP model is the basis for the modern internet and is widely implemented in networking hardware and software. It is the de facto standard for communication on the internet and many other computer networks.

5. Flexibility:

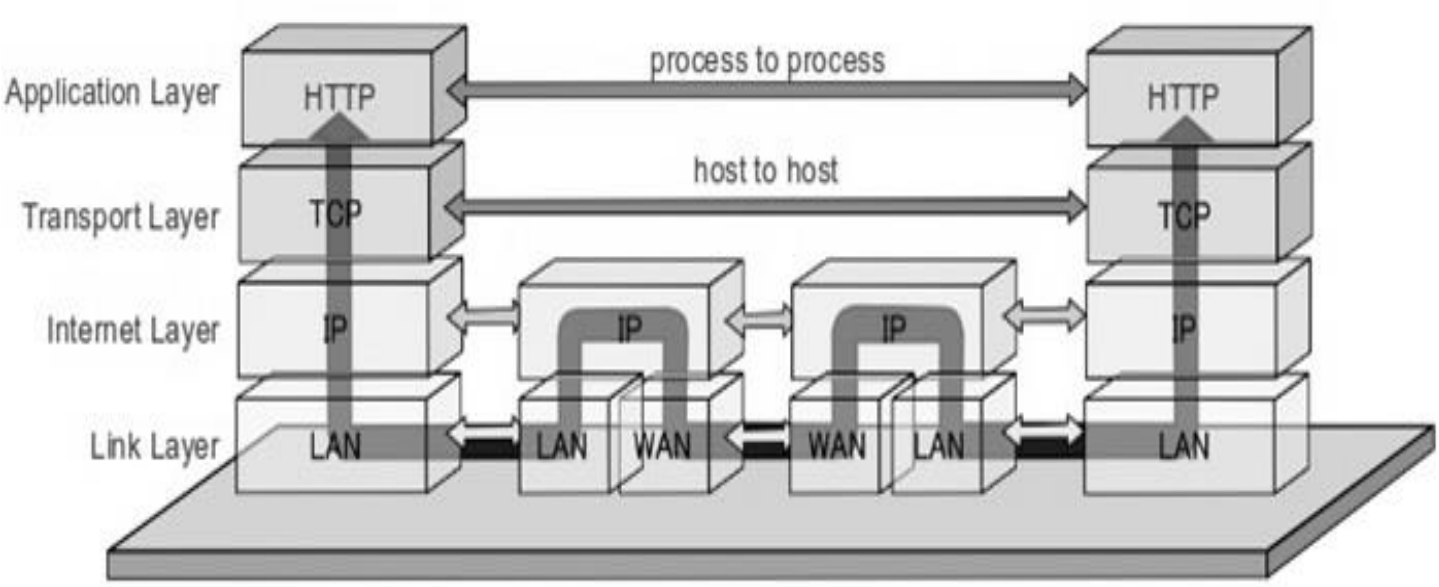
- **OSI Model:** The OSI model is more flexible and modular, making it easier to understand and implement new protocols.
- **TCP/IP Model:** The TCP/IP model is more streamlined and efficient, making it well-suited for the practical requirements of internet communication.

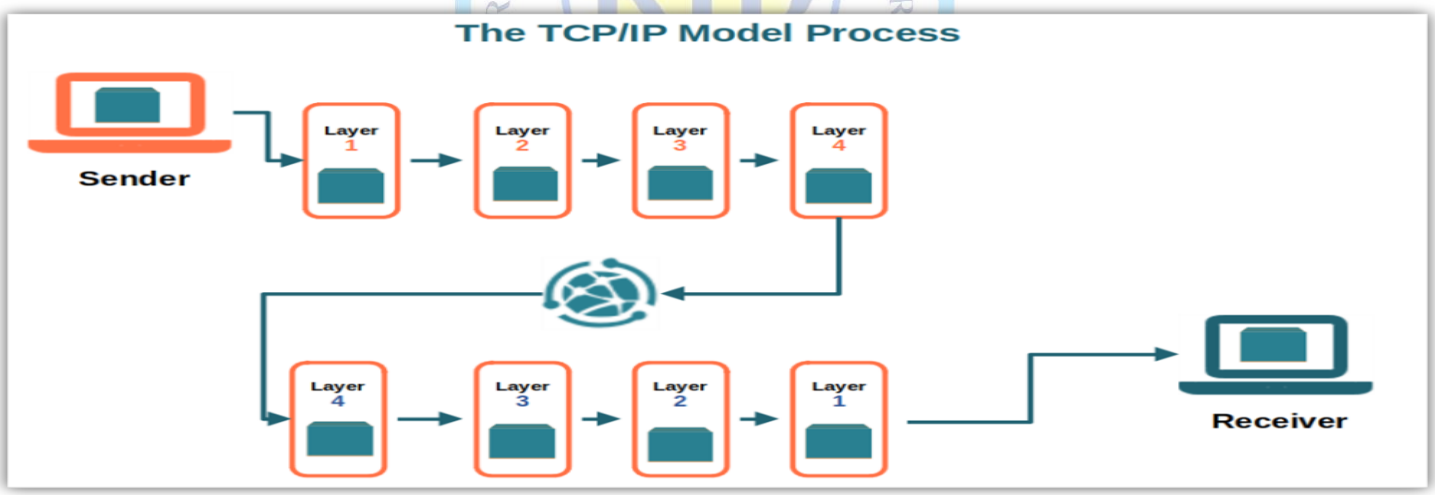
USE OF TCP/IP MODEL

1) **Internet Communication:** The TCP/IP model serves as the foundation for communication on the internet. It enables devices connected to the internet to exchange data packets reliably and efficiently, regardless of the underlying hardware and software differences.
2) **Networking Protocols:** The TCP/IP model provides a standardized set of protocols for various networking functions, such as addressing, routing, data transmission, and error detection. These protocols include IP (Internet Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), and others.
3) **Network Administration and Management:** TCP/IP protocols are used for network administration tasks such as configuring IP addresses, managing routing tables, monitoring network performance, and diagnosing network issues. Tools and utilities built on TCP/IP protocols facilitate network management tasks.
4) **Application Development:** Many software applications, including web browsers, email clients, file transfer programs, and messaging apps, rely on TCP/IP protocols for communication over networks. Developers use TCP/IP APIs (Application Programming Interfaces) to integrate networking capabilities into their applications.
5) **Interoperability:** The TCP/IP model promotes interoperability among diverse computer systems and networks. It enables devices running different operating systems and using different network technologies to communicate with each other seamlessly, fostering a connected global network.
6) **Cloud Computing and Virtualization:** TCP/IP protocols are essential for cloud computing and virtualization environments, where virtual machines and cloud services communicate over

networks. TCP/IP ensures reliable and secure data transmission between virtualized resources and client devices.

7) **Internet of Things (IoT):** As the IoT ecosystem expands, TCP/IP protocols play a crucial role in connecting and managing a wide array of IoT devices, sensors, and actuators. TCP/IP enables data exchange between IoT devices and centralized servers or cloud platforms.
8) **Security and Encryption:** TCP/IP protocols support security mechanisms such as SSL/TLS (Secure Sockets Layer/Transport Layer Security) for encrypting data transmitted over networks. These security features help protect sensitive information from interception and unauthorized access.





Def: - it is a unique physical or logical address that identifies a network node or device over a Network or Internet.

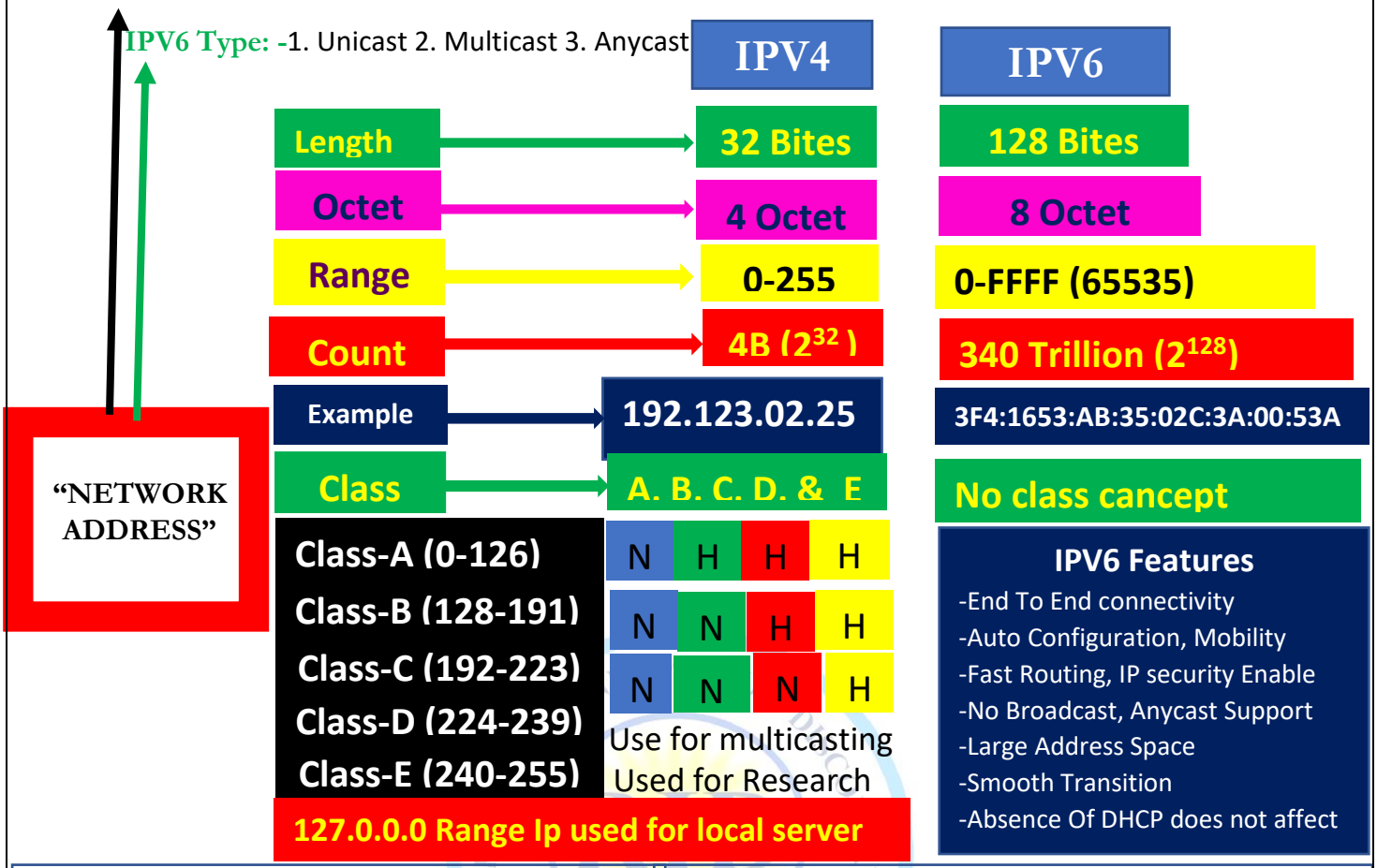
Type: - 1. IP Address or Logical Address 2.MAC Address or Physical Address.

IP Address: Internet Protocol is a unique address that is used to identify computers on the internet.

IP ADDRESS = NETWORK ID(1) + HOST ID(0)

IP ADDRESS

IPV4 Type: -1. Private IP & 2. Public IP



❖ **ICANN (Internet Corporation for Assigned Names and Numbers):**

- **Foundation Day:** 30-Sept-1998
- **HQ:** Los Angeles, California, USA
- **Purpose:** Manages DNS and IP address allocation, facilitates policy development, promotes competition in domain name marketplace.
- **Role in New Technology Development:** Supports deployment of new Internet technologies

❖ **IANA (Internet Assigned Numbers Authority):**

- **Foundation Day:** December, 1988
- **HQ: Los Angeles USA**
- **Purpose:** Manages and coordinates IP addresses, ASNs, protocol parameters, and DNS root zone.
- **Role in New Technology Development:** Supports deployment of new Internet technologies by managing allocation of protocol numbers and IP addresses.
- **Note: IANA** is a one Dept of ICANN

❖ **IETF (Internet Engineering Task Force):**

- **Foundation Day:** 1986
- **HQ:** Decentralized, Postal address: Washington DC USA
- **Purpose:** Develops and promotes Internet standards and protocols
- **Role in New Technology Development:** Drives innovation and evolution of the Internet.

❖ **IEEE (Institute of Electrical and Electronics Engineers):**

- **Foundation Day:** 1963
- **HQ:** New York City, USA
- **Purpose:** Advances technology for benefit of humanity
- **Role in New Technology Development:** Sets technical standards, fosters innovation, and promotes knowledge exchange across various engineering fields.

IP (INTERNET PROTOCOL) ADDRESS

➢ IP (Internet Protocol) address, also known as a logical address, is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. IP addresses serve two primary purposes:

1. **Identification:** IP addresses uniquely identify devices on a network. Just like a home address helps mail carriers deliver mail to specific houses, an IP address enables routers and other network devices to route data packets to the correct destination device.

2. **Location Addressing:** IP addresses are used for location addressing, allowing devices to communicate with each other across networks. When a device sends data over a network, it includes the IP address of the destination device so that routers can forward the data packets to the correct destination.

❖ Types of IP Address:

➢ There are primarily two types of IP addresses: IPv4 addresses and IPv6 addresses. Here's a brief overview of each:

1. IPv4 Addresses:

- IPv4 (Internet Protocol version 4) addresses are 32-bit numerical addresses expressed in dotted-decimal notation (e.g., 192.0.2.1).
- The address space of IPv4 is limited to approximately 4.3 billion unique addresses, which has led to address exhaustion in many regions.
- IPv4 addresses are divided into classes, including Class A, Class B, and Class C, based on the number of bits used for network and host portions.
- To alleviate address exhaustion, techniques such as Network Address Translation (NAT) and the use of private IP address ranges have been employed.

2. IPv6 Addresses:

- IPv6 (Internet Protocol version 6) addresses are 128-bit hexadecimal addresses separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- The address space of IPv6 is significantly larger than IPv4, allowing for approximately 340 undecillion unique addresses (3.4 x 10^38).
- IPv6 addresses are divided into multiple sections, with each section separated by colons. Leading zeros in each section can be omitted, and consecutive sections of zeros can be represented with a double colon (::).
- IPv6 adoption is increasing to accommodate the growing number of internet-connected devices and to provide a solution to the limitations of IPv4.

IPV4 ADDRESS

➢ IPv4 (Internet Protocol version 4) is the fourth revision of the Internet Protocol (IP), which serves as the foundation for communication on the Internet and many other computer networks.

1. Address Format:

- IPv4 addresses are 32-bit binary numbers, divided into four octets (groups of 8 bits) and expressed in dotted-decimal notation for readability (e.g., 192.0.2.1).
- Each octet can represent values from 0 to 255, providing a total of approximately 4.3 billion unique addresses (2^32).

- The address is divided into two parts: the network portion and the host portion. The division between these parts is determined by the subnet mask, which specifies how many bits are used for the network and how many for the host.

2. Classes of IPv4 Addresses:

- IPv4 addresses are historically classified into five classes: A, B, C, D, and E.
- Classes A, B, and C are used for addressing networks, while classes D and E have specific purposes and are not commonly used for network addressing.
- Each class has a different range of valid addresses and a different default subnet mask:
- Class A: 1.0.0.0 to 126.255.255.255 (with a default subnet mask of 255.0.0.0)
- Class B: 128.0.0.0 to 191.255.255.255 (with a default subnet mask of 255.255.0.0)
- Class C: 192.0.0.0 to 223.255.255.255 (with a default subnet mask of 255.255.255.0)

3. Subnetting:

- Subnetting allows a network administrator to divide a single Class A, B, or C network into multiple smaller subnetworks (subnets).
- This is achieved by borrowing bits from the host portion of the address to create additional subnets, resulting in a custom subnet mask.
- Subnetting helps optimize network efficiency, manage network traffic, and improve security by logically separating different parts of a network.

4. Private IP Addresses:

- IPv4 reserves certain address ranges for private use within internal networks, which are not routable over the public Internet.
- These private address ranges include:
- 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

➢ Network Address Translation (NAT) allows devices with private IP addresses to communicate with devices on the public Internet by translating their private addresses to a single public IP address.

5. IPv4 Address Exhaustion:

- The rapid growth of the Internet and the proliferation of connected devices have led to IPv4 address exhaustion, particularly in regions with high internet penetration.
- IPv4 address exhaustion has necessitated the adoption of IPv6, which provides a significantly larger address space to accommodate the growing number of internet-connected devices.

❖ Types of IpV4:

➢ IPv4, addresses are broadly categorized into two types based on their visibility and routability on the Internet: private IP addresses and public IP addresses.

1. Private IP Addresses:

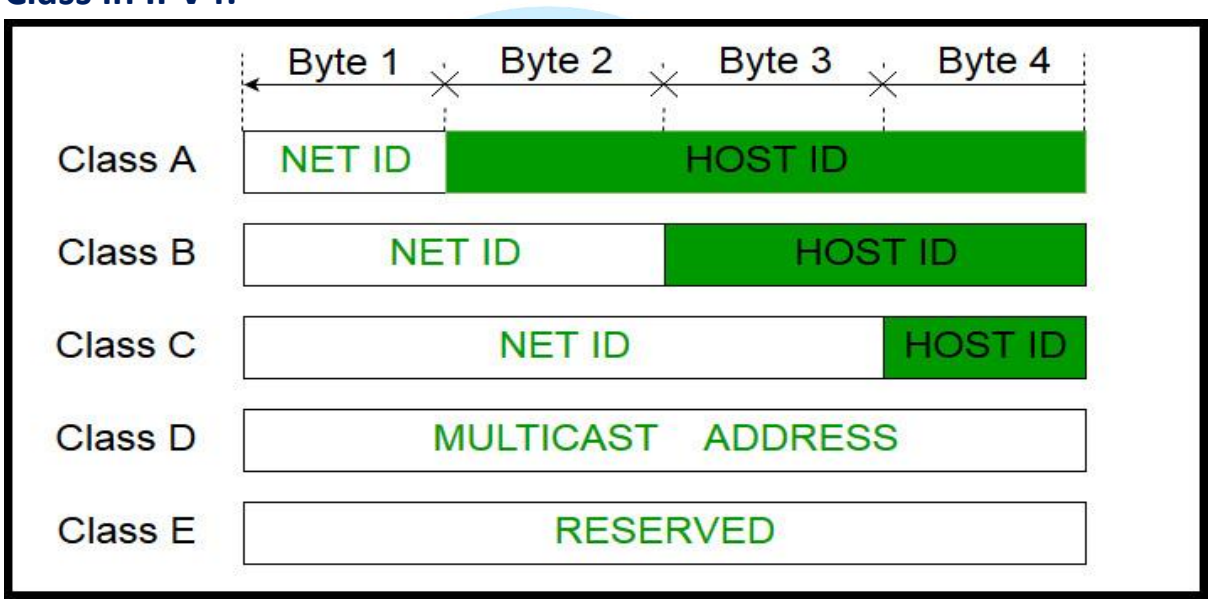
- Private IP addresses are reserved for use within private networks and are not routable over the public Internet. They are commonly used for internal communication within organizations, homes, or other closed networks.
- Private IP addresses are specified in RFC 1918 and are divided into three blocks:
- Class A Private Addresses: 10.0.0.0 to 10.255.255.255 (CIDR notation: 10.0.0.0/8)

- Class B Private Addresses: 172.16.0.0 to 172.31.255.255 (CIDR notation: 172.16.0.0/12)
- Class C Private Addresses: 192.168.0.0 to 192.168.255.255 (CIDR notation: 192.168.0.0/16)
- Private IP addresses can be freely used within private networks without requiring coordination with Internet authorities like ICANN (Internet Corporation for Assigned Names and Numbers).

2. Public IP Addresses:

- Public IP addresses are globally unique addresses assigned to devices connected to the public Internet. They are used for communication between devices across different networks and are routable over the Internet.
- Public IP addresses are managed and allocated by regional Internet registries (RIRs) such as ARIN (American Registry for Internet Numbers), RIPE NCC (Réseaux IP Européens Network Coordination Centre), APNIC (Asia-Pacific Network Information Centre), and others.
- Public IP addresses are obtained from ISPs (Internet Service Providers) and are assigned to routers, servers, and other network devices that require direct communication over the Internet.
- Public IP addresses must be unique to ensure proper routing and delivery of data packets across the global Internet infrastructure.

❖ Class in IPV4:



❖ Network ID:

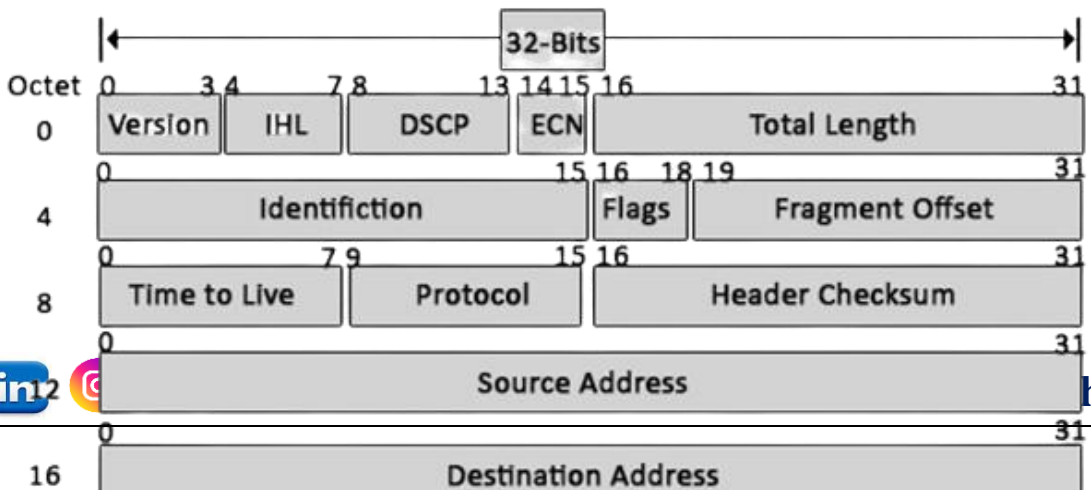
- The network ID represents the portion of the IP address that identifies the network to which a device belongs.
- In IPv4 addresses, the network ID is determined by the class of the IP address or by subnetting within a classful address range.
- For Class A, B, and C addresses, the network ID is the portion of the address that is fixed and identifies the network. The rest of the address is used to identify hosts within that network.
- Network IDs are used by routers to determine the path that data packets should take to reach their destination network.

❖ Host ID:

- The host ID represents the portion of the IP address that identifies a specific device (host) within a network.
- In IPv4 addresses, the host ID is the portion of the address that uniquely identifies a device on the network.
- For Class A, B, and C addresses, the host ID portion can vary and is used to distinguish individual devices within the same network.
- Host IDs are used by devices within a network to communicate with each other directly.

1. **Class A:**
   - Public IP Range: 1.0.0.0 to 127.0.0.0
   - Private IP Range: 10.0.0.0 to 10.255.255.255
   - Subnet Mask: 255.0.0.0 (8 bits)
   - Number of Networks: 126
   - Maximum Hosts per Network: Approximately 17 million
   - Usage: Class A addresses are suitable for networks with a large number of total hosts.
2. **Class B:**
   - Public IP Range: 128.0.0.0 to 191.255.0.0
   - Private IP Range: 172.16.0.0 to 172.31.255.255
   - Subnet Mask: 255.255.0.0 (16 bits)
   - Number of Networks: 16,382
   - Maximum Hosts per Network: Approximately 65,000
   - Usage: Class B addresses are designed for medium to large-sized networks.
3. **Class C:**
   - Public IP Range: 192.0.0.0 to 223.255.255.0
   - Private IP Range: 192.168.0.0 to 192.168.255.255
   - Subnet Mask: 255.255.255.0 (24 bits)
   - Number of Networks: Approximately 2 million
   - Maximum Hosts per Network: 254
   - Usage: Class C addresses are commonly used in small local area networks (LANs).
4. **Class D:**
   - Range: 224.0.0.0 to 239.255.255.255
   - Usage: Class D addresses are reserved for multicast groups and special purposes.
5. **Class E:**Range: 240.0.0.0 to 255.255.255.255
   - Usage: Class E addresses are reserved for experimental purposes and are not typically used in practical networks.

❖ IPV4 Header:



1. **Version (VER):**
   - A 4-bit field indicating the IP protocol version. For IPv4, this value is always 4.
   - The header length is specified in 32-bit words, so the minimum value for this field is 5 (indicating a 20-byte header), and the maximum is 15 (for a 60-byte header).
2. **Header Length (HLEN):**
   - A 4-bit field representing the number of 32-bit words in the header.
   - The actual header length is calculated by multiplying the value in this field by 4.
   - The minimum header length is 20 bytes (5 words), and the maximum is 60 bytes (15 words).
3. **Type of Service (TOS):**
   - An 8-bit field that specifies the quality of service requested for the packet.
   - It includes subfields for low delay, high throughput, and reliability.
4. **Total Length:**
   - A 16-bit field indicating the total length of the datagram (header + data) in bytes.
   - The maximum value is 65,535 bytes.
5. **Identification:**
   - A 16-bit field used for fragmentation and reassembly of datagrams.
   - Helps identify related fragments of a larger packet.
6. **Flags and Fragmentation Offset:**
   - The 3-bit Flags field is used for fragmentation control:
   - Bit 0: Reserved (always set to 0)
   - Bit 1: Don't Fragment (DF) flag
   - Bit 2: More Fragments (MF) flag
   - The 13-bit Fragmentation Offset field indicates the position of the fragment within the original datagram.
7. **Time-to-Live (TTL):**
   - An 8-bit field representing the maximum number of hops (routers) the packet can traverse before being discarded.
   - Prevents packets from circulating indefinitely.
8. **Protocol:**
   - An 8-bit field specifying the transport layer protocol (e.g., TCP, UDP, ICMP) to which the datagram should be delivered.
9. **Header Checksum:**
   - A 16-bit checksum calculated over the entire header.
   - Used for error detection during transmission.
10. **Source IP Address:**
    - A 32-bit field identifying the sender's IP address.
    - Destination IP Address:

- A 32-bit field identifying the intended recipient's IP address.

11. Options and Padding:

- Optional fields that may be present in the header.
- Used for specific purposes (e.g., timestamping, security).
- If not used, padding fills the remaining space.

SUBNET

➢ In IPv4 addressing, a subnet refers to a logical subdivision of a larger IP network. It allows network administrators to divide a single IP network into smaller, more manageable segments. Each subnet functions as an independent network with its own unique range of IP addresses. Subnetting helps optimize network performance, improve security, and conserve IP address space.

Example:

➢ Consider a Class C IPv4 network with the default subnet mask of 255.255.255.0. This provides a total of 256 IP addresses, ranging from 192.168.1.0 to 192.168.1.255. Now, let's subnet this network into smaller subnets to accommodate multiple departments within an organization.

- **Subnet 1:** Department A
- **IP Range:** 192.168.1.0 - 192.168.1.63
- **Subnet Mask:** 255.255.255.192 (/26)
- **Subnet 2:** Department B
- **IP Range:** 192.168.1.64 - 192.168.1.127
- **Subnet Mask:** 255.255.255.192 (/26)
- **Subnet 3:** Department C
- **IP Range:** 192.168.1.128 - 192.168.1.191
- **Subnet Mask:** 255.255.255.192 (/26)
- **Subnet 4:** Department D
- **IP Range:** 192.168.1.192 - 192.168.1.255
- **Subnet Mask:** 255.255.255.192 (/26)

➢ By subnetting the Class C network, we've created four smaller subnets, each with its own range of IP addresses to accommodate different departments or segments within the organization.

➢

SUBNETTING

- Subnetting: Subnetting is the process of dividing a large network into smaller, more manageable sub-networks (subnets). It helps improve network efficiency, security, and organization.

➢ **Why Subnet?:** Subnetting allows efficient use of IP addresses, reduces broadcast traffic, and enhances network performance.

Example:

➢ Consider a Class C IP address 193.1.2.0 with a subnet mask of 255.255.255.128.

➢ We divide it into two subnets:

Subnet 1: Range from 193.1.2.0 to 193.1.2.127

- Subnet ID: 193.1.2.0
- Broadcast ID: 193.1.2.127

- Total usable hosts: 126
- Subnet mask: 255.255.255.128

Subnet 2: Range from 193.1.2.128 to 193.1.2.255

- Subnet ID: 193.1.2.128
- Broadcast ID: 193.1.2.255
- Total usable hosts: 126
- Subnet mask: 255.255.255.128

❖ Subnet Mask:

- Subnet Mask: A subnet mask defines the network portion and host portion of an IP address. It consists of 32 bits (usually represented in decimal-dotted notation).
- Example: A subnet mask of 255.255.255.0 means the first 24 bits represent the network, and the remaining 8 bits represent the host.

❖ CIDR (Classless Inter-Domain Routing)

- CIDR: CIDR is a method for allocating and routing IP addresses based on their network prefix rather than their class (Class A, B, C, etc.).
- CIDR Notation: CIDR addresses are represented using slash notation (e.g., 192.168.1.0/24). The number after the slash specifies the length of the network prefix.

Example:

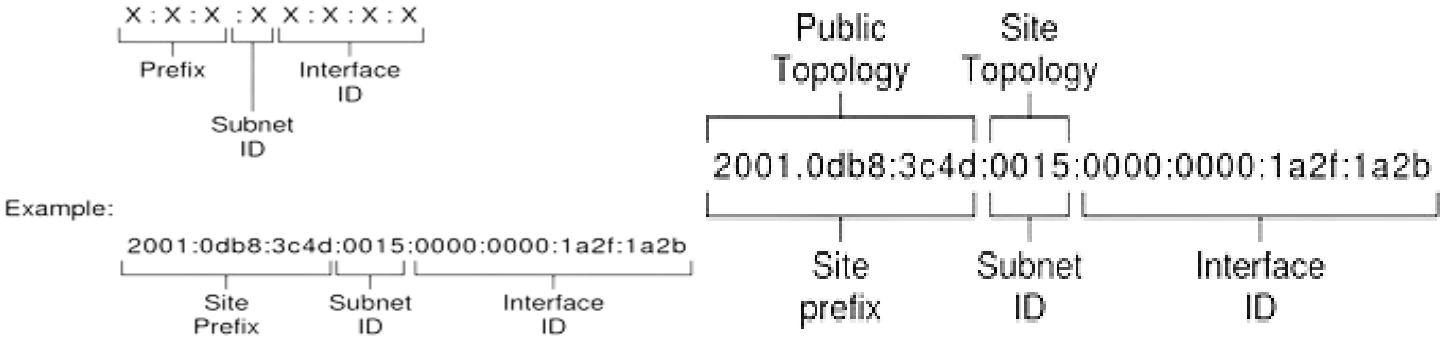
- 192.168.1.0/24 means the first 24 bits are the network prefix, and the remaining 8 bits are for hosts.
- IP Classes (Classful Addressing)
  - Class A: Range: 1.0.0.0 to 126.255.255.255. Supports 16 million hosts per network.
  - Class B: Range: 128.0.0.0 to 191.255.255.255. Supports 65,000 hosts per network.
  - Class C: Range: 192.0.0.0 to 223.255.255.255. Supports 254 hosts per network.
  - Class D: Reserved for multicast groups.
  - Class E: Reserved for experimental purposes.
- Remember, CIDR allows for more efficient IP address allocation and better routing, while subnetting enhances network organization and performance.

IPV6 ADDRESS

- IPv6 (Internet Protocol version 6) is the most recent version of the Internet Protocol (IP) that is designed to succeed IPv4. IPv4, which has been the primary Internet protocol for decades, uses 32-bit addresses, limiting the number of possible unique addresses to around 4.3 billion. With the rapid growth of internet-connected devices, the available IPv4 addresses are running out, necessitating the transition to IPv6.
- IPv6 addresses are 128 bits in length, allowing for a vastly larger number of possible unique addresses—approximately 340 undecillion (3.4 × 10^38).
- IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a 128-bits address having an address space of 2128, which is way bigger than IPv4. IPv6 use Hexa-Decimal format separated by colon (:).

❖ Components in Address format:

- There are 8 groups and each group represents 2 Bytes (16-bits).
- Each Hex-Digit is of 4 bits (1 nibble)
- Delimiter used – colon (:)



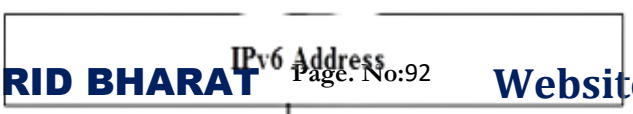
1. **Format:** IPv6 addresses are typically represented as eight groups of four hexadecimal digits separated by colons (:). For example, an IPv6 address might look like this: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
2. **Zero Compression**: Leading zeros within each group can be omitted, and consecutive groups of zeros can be replaced with a double colon (::). However, you can only use the double colon once in an IPv6 address to avoid ambiguity. For example, 2001:0db8::8a2e:0370:7334.
3. **Address Space Allocation:** The address space is divided into different blocks for various purposes, such as global unicast addresses, link-local addresses, multicast addresses, and others.
4. **Global Unicast Addresses:** These are equivalent to public IPv4 addresses and are routable on IPv6 internet. Global unicast addresses are used to uniquely identify devices on global internet.
5. **Link-Local Addresses:** These addresses are used for communication within a single network segment (link). They are equivalent to IPv4's Automatic Private IP Addressing (APIPA) addresses. Link-local addresses always start with the prefix fe80.
6. **Special Addresses:** IPv6 reserves certain addresses for special purposes, such as loopback (::1) and unspecified address (::).
7. **IPv6 Prefix:** Similar to IPv4 subnet masks, IPv6 uses prefixes to define network segments. The prefix length indicates the number of bits used for the network portion of the address.

❖ Address Structure:

- IPv6 addresses consist of 128 bits, which is a significant increase compared to the 32-bit addresses used in IPv4.
- Each IPv6 address is represented as a series of eight groups, separated by colons. Each group contains four hexadecimal digits.
- **Example of IPV6:**
  2001:0db8:85a3:0000:0000:8a2e:0370:7334.

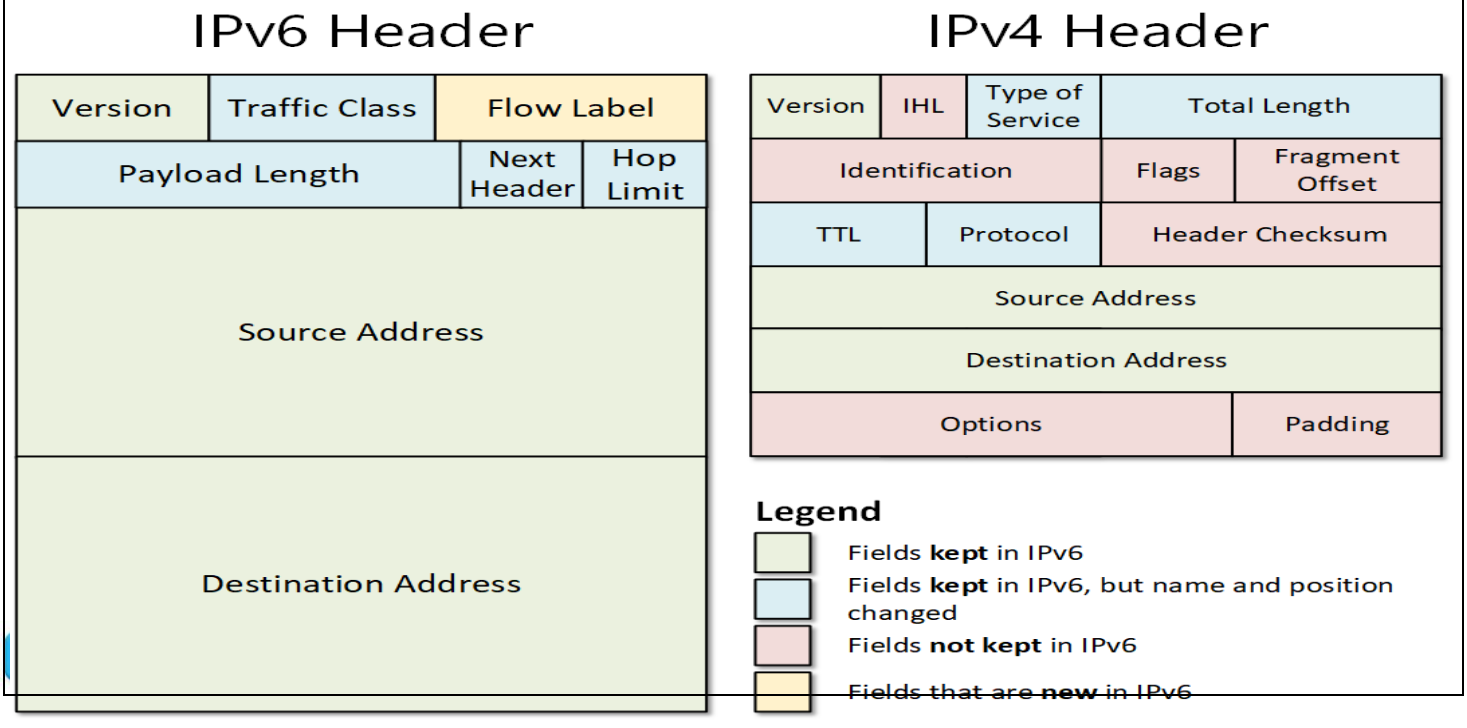
❖ Address Types: IPv6 addresses can be classified into three main types:

- **Unicast:** An address identifying a single network interface. Packets sent to a unicast address are delivered to that specific interface.
- **Multicast:** An address used to deliver packets to multiple interfaces. Packets sent to a multicast address are delivered to all interfaces identified by the multicast address.
- **Anycast:** An address assigned to multiple interfaces, with packets sent to the nearest interface (according to routing protocols).



❖ No Broadcast in IPv6:

- Unlike IPv4, which uses broadcast addressing, IPv6 does not have broadcast. Instead, it relies on multicast for similar purposes.
- The all-nodes link-local multicast group (ff02::1) serves a similar role as broadcast but is not recommended for general use.



- The IPv6 header is a fundamental part of the IPv6 protocol suite and is used to encapsulate data packets for transmission across networks. It contains essential information required for routing and delivery of packets between source and destination nodes.

1. **Version (4 bits):** Indicates the version of the IP protocol being used. For IPv6, this field is set to 6.
2. **Traffic Class (8 bits):** This field is used for traffic classification and prioritization. It replaces the Type of Service (ToS) field in IPv4. It can be used for Quality of Service (QoS) purposes to prioritize certain types of traffic over others.
3. **Flow Label (20 bits):** Intended to provide special handling for certain flows of data, such as real-time multimedia streams or high-priority traffic. It allows routers to identify and process packets belonging to the same flow consistently.
4. **Payload Length (16 bits):** Indicates the length of the payload (data) in the packet, measured in octets (bytes). This includes the entire payload, including any extension headers that may follow the IPv6 header.
5. **Next Header (8 bits):** Specifies the type of the header that immediately follows the IPv6 header. It can indicate either another IPv6 extension header or the upper-layer protocol (e.g., TCP, UDP, ICMPv6) that is being used to carry the payload data.
6. **Hop Limit (8 bits):** Similar to the Time-to-Live (TTL) field in IPv4, this field specifies the maximum number of hops (routers) that a packet can traverse before being discarded. Each router decrements this value by one when forwarding the packet, and if it reaches zero, the packet is discarded.
7. **Source Address (128 bits):** Specifies the IPv6 address of the packet's source node. It uniquely identifies the sender of the packet on the IPv6 network.
8. **Destination Address (128 bits):** Specifies the IPv6 address of the packet's intended destination node. It uniquely identifies the recipient of the packet on the IPv6 network.

❖ Advantages of IPv6:

1. **Vast Address Space:** IPv6 provides a significantly larger address space compared to IPv4, allowing for an almost limitless number of unique addresses. This abundance of addresses ensures that every device can have its own globally unique IP address.
2. **Efficient Routing:** IPv6 simplifies the routing process by reducing the size of routing tables and enabling more efficient routing algorithms. This efficiency improves network performance and scalability.
3. **Auto-configuration:** IPv6 supports stateless address auto-configuration, allowing devices to automatically configure their own IPv6 addresses without the need for DHCP servers. This simplifies network management and reduces administrative overhead.
4. **Enhanced Security:** IPv6 includes built-in support for IPsec (Internet Protocol Security), providing end-to-end encryption and authentication for network communications. This enhances security and privacy for network traffic.
5. **Improved Quality of Service (QoS):** IPv6 introduces flow labeling, which enables routers to classify and prioritize traffic based on specific flows. This helps to ensure better quality of service for critical applications, such as real-time multimedia streaming.

❖ Disadvantages of IPv6:

1. **Compatibility Issues:** The transition from IPv4 to IPv6 involves compatibility challenges, as not all network infrastructure, applications, and devices fully support IPv6. This can lead to interoperability issues and need for dual-stack deployment (supporting both IPv4 and IPv6).
2. **Network Infrastructure Upgrades:** Implementing IPv6 may require significant upgrades to network infrastructure, including routers, switches, and other networking equipment. This can be costly and time-consuming for organizations, especially those with large and complex networks.
3. **Learning Curve:** IPv6 introduces new concepts and addressing schemes that may require training and expertise for network administrators and IT professionals. learning curve associated with IPv6 deployment can pose challenges for organizations transitioning from IPv4.
4. **Potential Security Risks:** While IPv6 offers enhanced security features, the complexity of IPv6 deployments and the lack of widespread expertise in IPv6 security may introduce new security vulnerabilities. Organizations need to carefully assess and mitigate potential risks associated with IPv6 adoption.

❖ Uses of IPv6:

1. **Internet Connectivity:** IPv6 is essential for providing internet connectivity to the growing number of devices, including smartphones, IoT devices, and other connected gadgets. As IPv4 addresses become scarce, IPv6 enables continued expansion of the internet and supports the proliferation of new technologies and services.
2. **Enterprise Networks**: Many organizations are deploying IPv6 within their internal networks to support the increasing number of devices and applications. IPv6 enables efficient addressing and routing within enterprise networks and facilitates seamless communication between different network segments.
3. **Mobile Networks:** Mobile operators are adopting IPv6 to accommodate the explosive growth of mobile devices and data traffic. IPv6 enables efficient use of address space and improves network performance for mobile users, particularly in densely populated areas.
4. **Cloud Services:** Cloud service providers are embracing IPv6 to ensure scalability and support the diverse needs of their customers. IPv6 enables cloud-based applications and services to reach a broader audience and provides a foundation for future growth and innovation.

IPV4 VS IPV6

1. **Address Length:**
   - **IPv4 addresses** are 32 bits long, allowing for approximately 4.3 billion unique addresses.
   - **IPv6 addresses** are 128 bits long, providing a vastly larger address space with approximately 340 undecillion unique addresses.
2. **Address Representation:**
   - **IPv4 addresses** are represented in decimal format separated by periods (e.g., 192.0.2.1).
   - **IPv6 addresses** are represented in hexadecimal format separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
3. **Address Configuration:**
   - **IPv4 addresses** can be configured manually, dynamically using DHCP (Dynamic Host Configuration Protocol), or automatically using APIPA (Automatic Private IP Addressing).
   - **IPv6 addresses** support stateless address auto-configuration, where devices can generate their own addresses based on the network prefix and interface identifier.
4. **Header Size:**

- **IPv4 headers** are typically 20 bytes in size, not including any options.
- **IPv6 headers** are fixed at 40 bytes in size, not including any extension headers.

5. **Header Fields:**
   - **IPv4 headers** include fields such as Version, Header Length, Type of Service (TOS), Total Length, Identification, Flags, Fragment Offset, Time to Live (TTL), Protocol, Header Checksum, Source Address, and Destination Address.
   - **IPv6 headers** include fields such as Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address, and Destination Address.
6. **Fragmentation:**
   - **IPv4** routers are responsible for fragmenting packets that are too large to traverse a network link.
   - **IPv6** routers typically do not perform fragmentation, and end-to-end fragmentation is discouraged. Instead, hosts are expected to perform Path MTU Discovery to determine the maximum transmission unit (MTU) size.
7. **Security Features:**
   - **IPv4** does not have built-in support for IPsec (Internet Protocol Security) but can be implemented as an optional extension.
   - **IPv6** includes built-in support for IPsec, providing end-to-end encryption, authentication, and data integrity for network communications.
8. **Options and Extension Headers:**
   - **IPv4** options, such as timestamp, record route, and strict source routing, are included in the main header.
   - **IPv6** options, such as hop-by-hop options, routing, fragmentation, authentication, and encapsulating security payload, are implemented as separate extension headers.
9. **Protocol Support:**

   IPv4 is widely supported by networking equipment, operating systems, and applications, but the available address space is becoming increasingly limited.

IPv6 adoption is growing steadily, and support is becoming more widespread among networking equipment, operating systems, and applications, especially as IPv4 address

MAC (MEDIA ACCESS CONTROL)

Definition: - **it is a Globally unique physical and Permanent address that identifies device over a Network.**

- **MAC address also known as Physical address or Hardware Address or BIA(Burnt-in) address.**

Length=48 Bits

48bits = 24bits + 24bits

MAC address= Organization + Device

MAC address= OUI + Vendor Specific

MAC Address Representation: it is represented as hexadecimal format

- 12 Hexadecimal (0-9, A, B, C, D, E, F)

Format

mm: mm: mm: ss: ss: ss

mm-mm-mm-ss-ss-ss

mmm. mmm. sss. sss

- MM=Organisation (OUI {organization unique identifier}) Ss=device Model

Ex: - Dell=AE: 40: FF: 00: 00: 01

aB-df-2b-33-39-3a

a4c.def.34a.bc6

MAC Address: 00:1A:2B:3C:4D:5E

1. First three octets 00:1A:2B represent the **OUI** (Organizationally Unique Identifier) assigned to the manufacturer.
2. Last three octets 3C:4D:5E represent the unique identifier assigned to the specific network interface controller by the manufacturer.

- **OUI (Organizationally Unique Identifier)** is provided by the IEEE (Institute of Electrical and Electronics Engineers)

❖ IEEE (Institute of Electrical and Electronics Engineers):

- **Foundation Day:** Founded on May 13, 1884.
- **HQ:** Located in New York City, USA.
- **Purpose:** To advance technology for the benefit of humanity.
- **Fields:** Covers various disciplines within electrical engineering, electronics, and related fields, including telecommunications, computer science, biomedical engineering, and more.
- **Role in New Technology Development:** IEEE plays a crucial role in developing and promoting standards, protocols, and best practices in emerging technologies. It facilitates collaboration among industry professionals, researchers, and academics to drive innovation and ensure interoperability in areas such as wireless communications, power systems, internet protocols, and beyond.
  - MAC (Media Access Control) address is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. It's a hardware address associated with a network adapter (NIC - Network Interface Controller) and is assigned by the manufacturer during production. MAC addresses are essential for communication within a local network and are used by devices to identify and communicate with each other.

  1. **Format:** MAC addresses are typically represented as six groups of two hexadecimal digits separated by colons or hyphens. For example, a MAC address might look like this: 00:1A:2B:3C:4D:5E.
  2. **Uniqueness:** MAC addresses are intended to be globally unique. Manufacturers are assigned ranges of MAC addresses by the IEEE (Institute of Electrical and Electronics Engineers), ensuring that no two network devices have the same MAC address.
  3. **Structure:** The MAC address is divided into two parts:
     - **OUI (Organizationally Unique Identifier):** The first three octets (or 24 bits) of the MAC address represent the manufacturer's unique identifier. This portion is assigned by the IEEE to device manufacturers and is unique to each manufacturer.
     - **NIC-specific Identifier:** The last three octets (or 24 bits) of the MAC address represent the specific identifier assigned to the network interface controller by the manufacturer.
  4. **Role in Networking:**

- **Address Resolution Protocol (ARP):** MAC addresses are used in ARP to map IP addresses to MAC addresses within a local network. When a device needs to communicate with another device on the same network, it sends out an ARP request to obtain the MAC address corresponding to the destination IP address.
- **Switching and Forwarding:** MAC addresses are used by network switches to forward data packets within a local network. Switches maintain a MAC address table, also known as a MAC address forwarding table, which maps MAC addresses to the physical ports on the switch. This table is used to efficiently forward packets to their intended destinations.
- **Ethernet Frames:** MAC addresses are included in the headers of Ethernet frames, which are used to encapsulate data packets for transmission over Ethernet networks. The source and destination MAC addresses in the Ethernet frame header identify the sending and receiving devices, respectively.

5. **Privacy Concerns:**

- Since MAC addresses are unique identifiers that can be used to track devices on a network, there are privacy concerns associated with their use. In some cases, techniques such as MAC address randomization are employed to enhance privacy and prevent tracking of devices.

Example: MAC Address: 00:1A:2B:3C:4D:5E

1. First three octets 00:1A:2B represent the **OUI** (Organizationally Unique Identifier) assigned to the manufacturer.
2. Last three octets 3C:4D:5E represent the unique identifier assigned to the specific network interface controller by the manufacturer.

- **OUI (Organizationally Unique Identifier)** is provided by the IEEE (Institute of Electrical and Electronics Engineers)

❖ IEEE (Institute of Electrical and Electronics Engineers):

- **Foundation Day:** Founded on May 13, 1884.
- **HQ:** Located in New York City, USA.
- **Purpose:** To advance technology for the benefit of humanity.
- **Fields:** Covers various disciplines within electrical engineering, electronics, and related fields, including telecommunications, computer science, biomedical engineering, and more.
- **Role in New Technology Development:** IEEE plays a crucial role in developing and promoting standards, protocols, and best practices in emerging technologies. It facilitates collaboration among industry professionals, researchers, and academics to drive innovation and ensure interoperability in areas such as wireless communications, power systems, internet protocols.

❖ Advantages of MAC Addresses:

- Unique identifiers for network interfaces
- Stable and remain constant
- Used for device identification and network security
- Enable quality of service management
- Suitable for local network communication

❖ Disadvantages of MAC Addresses:

- Limited to local network use
- Vulnerable to spoofing and cloning
- Not easily transferable between devices
- Complexity in managing large networks
- Potential for vendor lock-in

❖ Uses of MAC Addresses:

- ✓ Device identification on local networks
- ✓ Access control via MAC address filtering
- ✓ Network troubleshooting and diagnostics
- ✓ Quality of service management on switches
- ✓ Device authentication for network security.

❖ How to Find the MAC address:

➢ Mobile Devices (e.g., smartphones, tablets):

1. Android Devices:

- Open the "Settings" app.
- Navigate to "About phone" or "About device."
- Select "Status" or "Status information."
- Look for "Wi-Fi MAC address" or "Ethernet MAC address" to find MAC address of your device.

2. iOS Devices (iPhone, iPad):

- Go to the "Settings" app.
- Tap on "General."
- Select "About."
- Scroll down and find the "Wi-Fi Address" to view the MAC address of your iOS device.

3. Other Mobile Devices (e.g., Windows Phone, BlackBerry):

➢ The steps may vary depending on the device manufacturer and operating system. Generally, you can find the MAC address in the device settings under the network or status information section. Computers (e.g., Windows PC, Mac):

1. Windows PC:

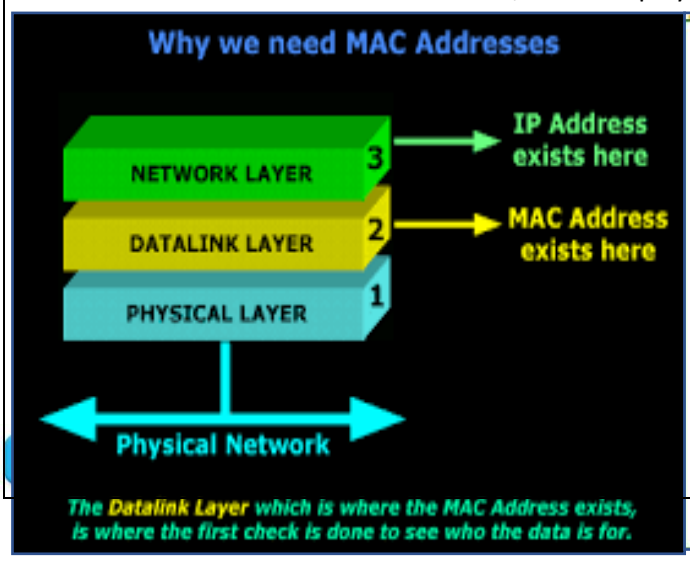
- Open the Start menu and type "cmd" to open the Command Prompt.
- In the Command Prompt window, type "ipconfig /all" and press Enter.

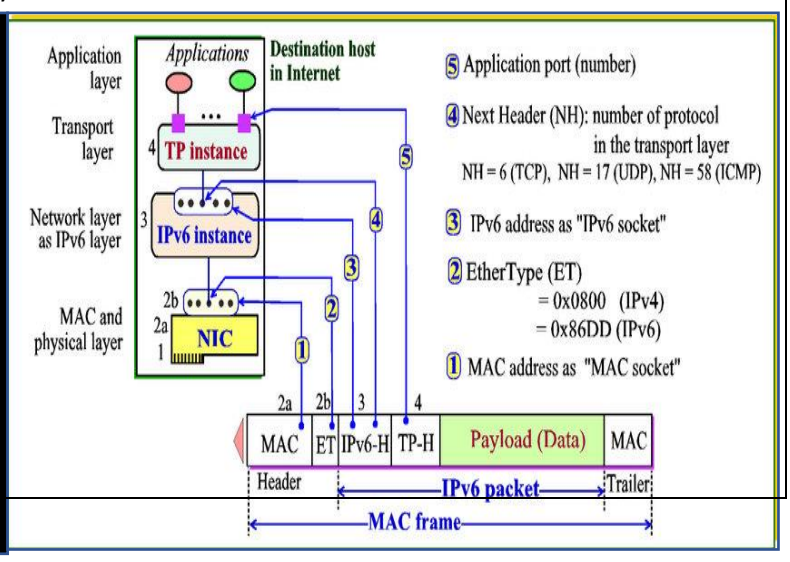
2. Mac (macOS):

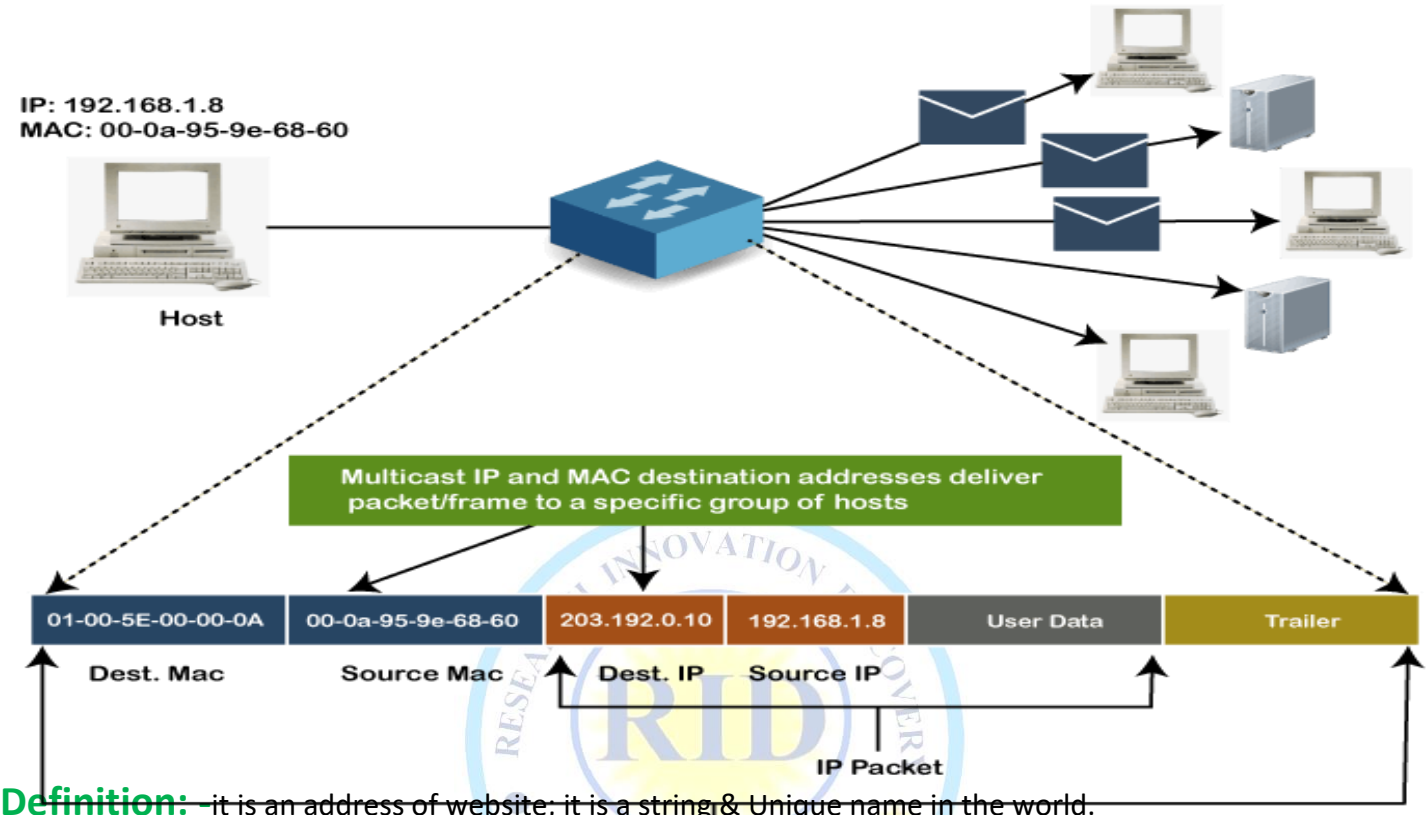
- Click on the Apple menu and select "System Preferences."
- Choose "Network" or "Network & Internet" depending on your macOS version.
- Select the network connection (e.g., Wi-Fi or Ethernet) from the left sidebar.
- Click on the "Advanced" button.
- Go to the "Hardware" tab, where you'll find the MAC address listed as "Wi-Fi Address" for wireless connections or "Ethernet ID" for wired connections.

3. Linux:

- Open a terminal window.
- Type the command "ifconfig" and press Enter.
- Look for the network interface you're interested in (eth0 for Ethernet or wlan0 for Wi-Fi).
- Find the "HWaddr" field, which displays the MAC address of the network interface.







Definition: - it is an address of website; it is a string & Unique name in the world.

Use: -it is used to identify services provided the internet such as website, email. Networking Contexts, application specific naming and addressing purpose identify domain or Ip resources.

Types: -1. Top-level Domain **(TLD)** 2. Second & low-level Domain (SLD)

TLD: - It is two types 1. Generic TLD**(GTLD)** 2. Country Code TLD **(CCTLD)**

GTLD: - .com, .net, .org, .edu, .mil, .int, .biz, & .gov,

CCTLD: - .IN, .US, .CN, .PK, etc.

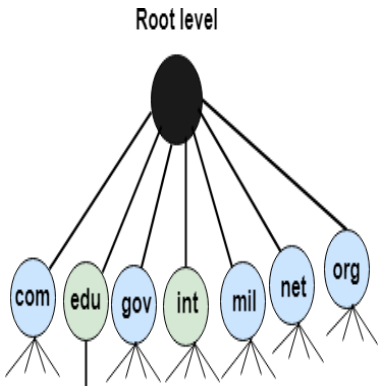
SLD: - ex:- www.twksaa.ra.org where .ra is SLD

Fully Qualified Domain Name: - www.twksaa.org.in.

Partially Qualified Domain Name: - www.twksaa.org.in

1st Domain Name: - Symolics.com in 15.03.1985

1st Edu Domain Name: - Berkeley.edu in 24.04.1985



DNS: - Domain Name System is a host name (Domain name) Ip address translation service.

Use: - it is used to Translate Domain name to Ip address vice-versa. DNS was introduced on ARPANET in1983 and Published by Internet Engineering Task Force (IETF). Managed BY ICANN (Internet Corporation for Assigned Names and Numbers)

Name Space: - 1). Flat Name Space 2). Hierarchy Name Space

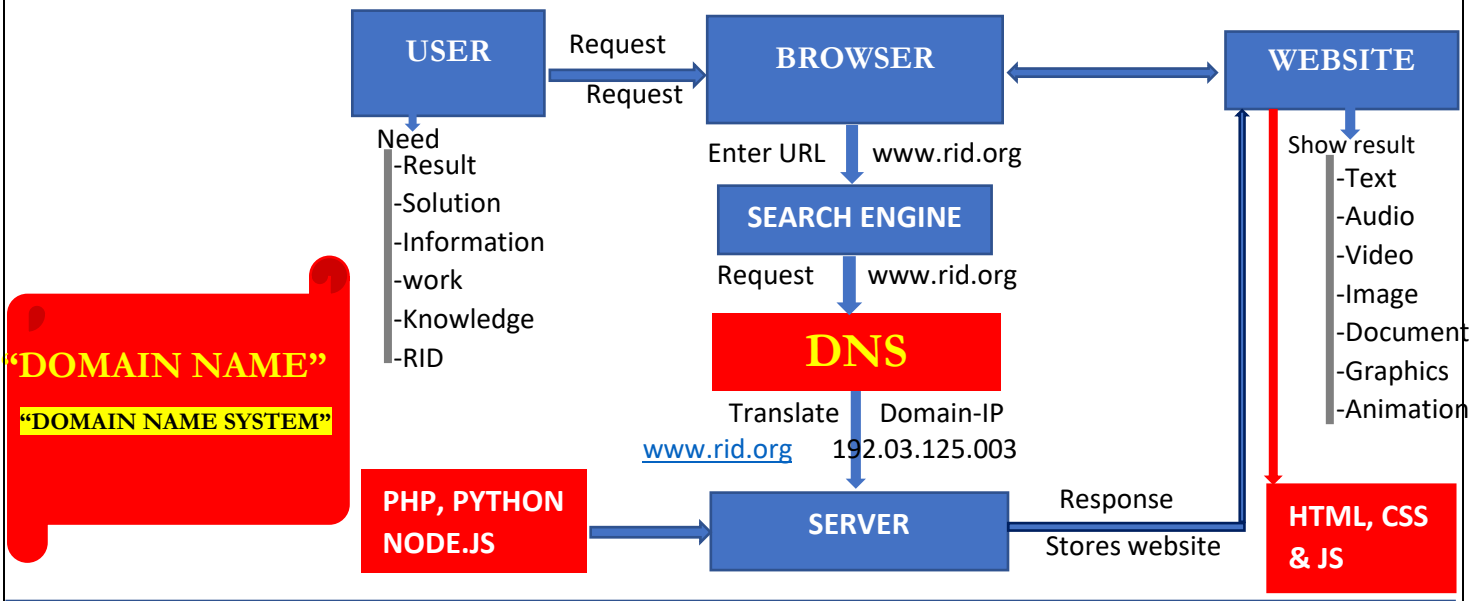
Flat DNS Name Space: - Name is assigned Sequence of character without any Structure.

Hierarchy DNS Name Space: - Name Space can be decentralised Hierarchy of Name Servers a).Root name server b).Top-level Server c).Authoritative Name Server.

DNS Resolver Method: - 1) Iterative Method 2). Recursive Method

Iterative Method: -Root name server involved at a single time.

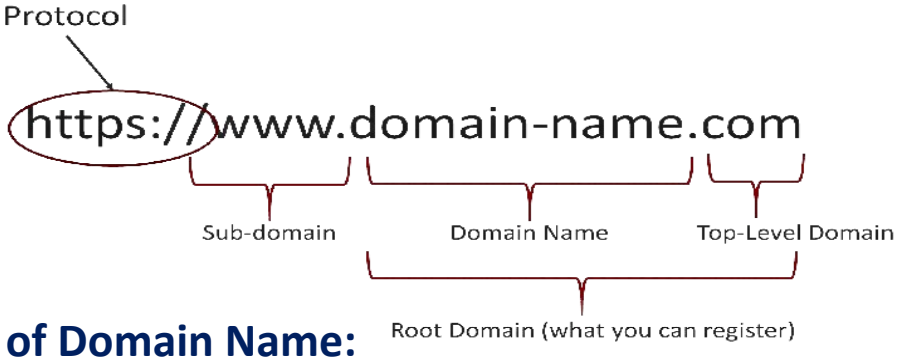
Recursive Method: - Root name server involved from starting to end (Request-Response)



- Domain names is managed by domain name registrars, which are accredited by the **Internet Corporation for Assigned Names and Numbers (ICANN)**.
- Registrars are responsible for facilitating the registration, renewal, and management of domain names on behalf of individuals, businesses, and organizations.
- **ICANN (Internet Corporation for Assigned Names and Numbers):**
- **Foundation Day:** ICANN was founded on September 18, 1998.
- **Purpose: ICANN** is a non-profit organization responsible for coordinating and overseeing the global **Domain Name System (DNS)** and **Internet Protocol (IP)** address allocation. Its mission is to ensure the stable and secure operation of the **Internet's unique identifier systems**. ICANN coordinates the assignment of domain names, IP addresses, and other **Internet protocol parameters**, as well as the management of the DNS root zone.

❖ Domain Name:

- Domain name is a human-readable label used to identify and locate resources on the Internet.
- Domain names are organized in a hierarchical structure and are part of the Domain Name System (DNS), which translates domain names into numerical IP addresses used by computers to communicate over the Internet.



❖ Use of Domain Name:

1. **Website Addressing:** They provide a human-readable way to access websites, replacing the need to remember complex IP addresses.
2. **Email Addressing:** Domain names identify the domain associated with an email account, such as "example.com" in "user@example.com."
3. **Branding and Brand Recognition:** Unique domain names help establish a strong online presence and differentiate brands from competitors.

4. **Online Identity and Reputation:** They contribute to establishing credibility and trustworthiness for organizations and individuals online.
5. **Marketing and Promotion:** Memorable domain names drive traffic to websites, promote products/services, and enhance brand visibility through marketing campaigns.
6. **E-commerce and Online Transactions:** Domain names provide secure platforms for conducting online transactions and interacting with customers.
7. **SEO (Search Engine Optimization):** Relevant domain names can improve search engine rankings, impacting a website's visibility in search results.
8. **Content Hosting and Distribution:** They are used to host and distribute various types of online content, facilitating sharing and accessibility across the web.

❖ Types of Domain Name:

1. Top-Level Domains (TLDs):

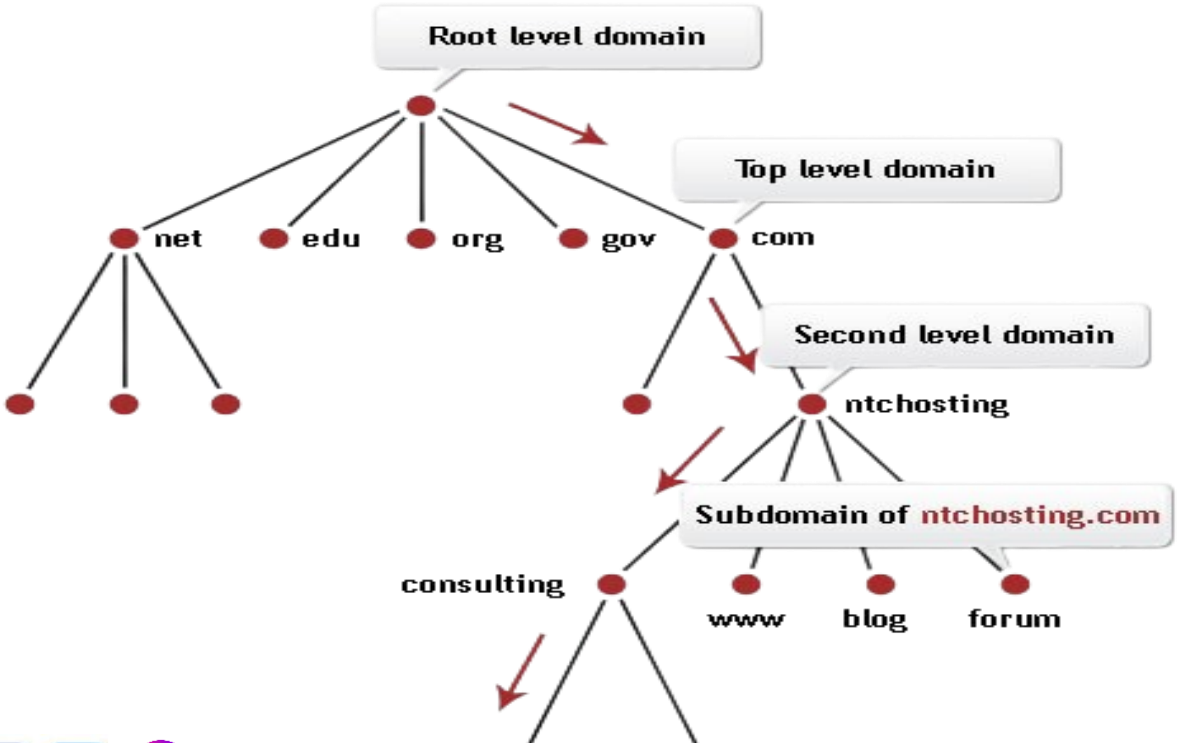
- **Generic Top-Level Domains (gTLDs):** These are general-purpose domain extensions that are not tied to any specific country or region. Examples: .com, .org, .net, .info, and .biz.
- **Country-Code Top-Level Domains (ccTLDs):** These domain extensions are associated with specific countries or territories. Examples: .in(India) .us (United States), .uk (United Kingdom), .ca (Canada), and .de (Germany).

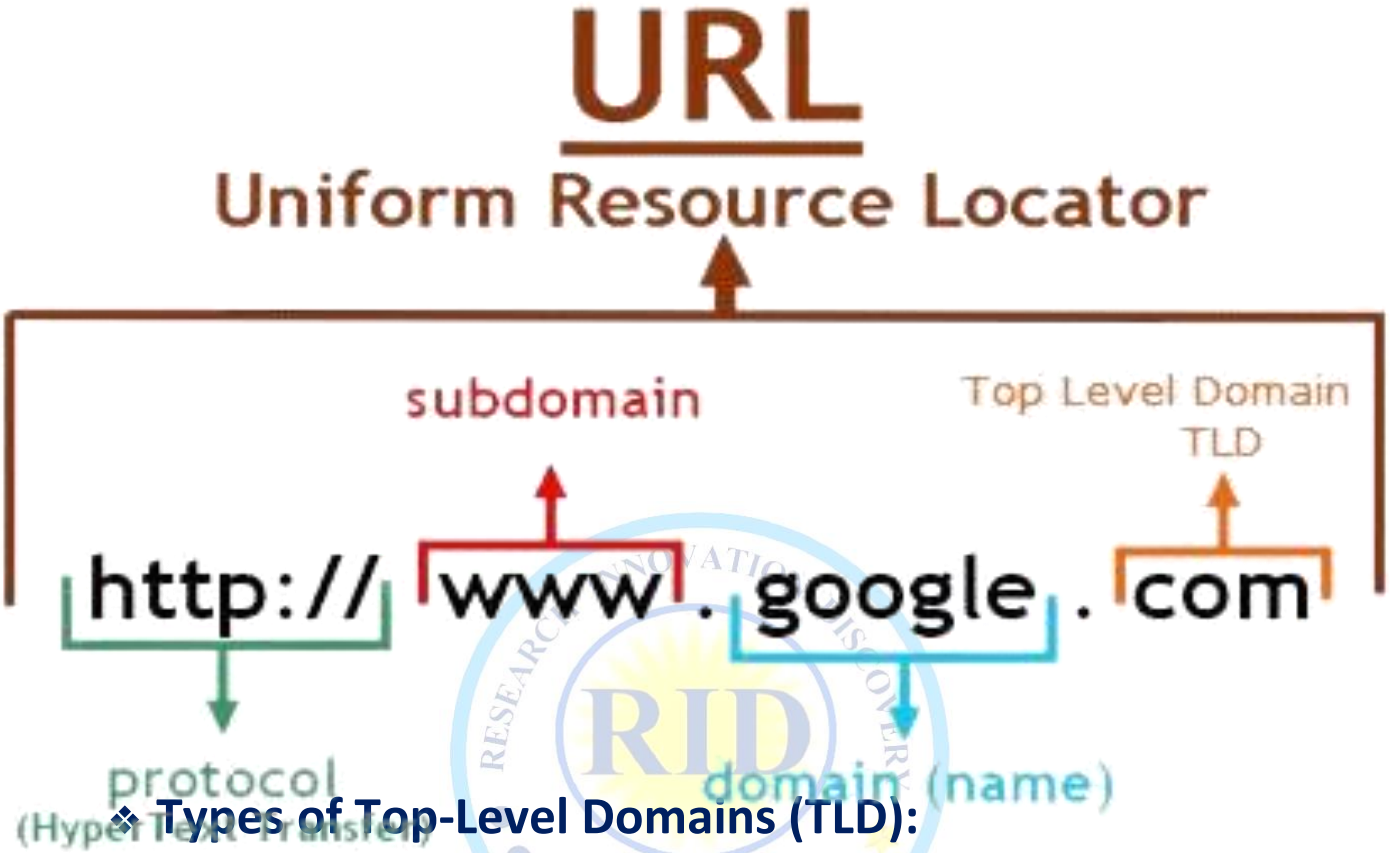
2. Second-Level Domains (SLDs):

- These are part of the domain name that appears directly to the left of the top-level domain. For example, in the domain name "example.com," "example" is the second-level domain.
- Second-level domains can be further categorized based on their purpose or function. For instance, commercial organizations often use .com, while educational institutions use .edu.

3. Subdomains:

- Subdomains are additional labels added to the front of a domain name, separated by periods. They can be used to create separate sections or branches within a main domain.
- Examples include "blog.example.com" and "shop.example.com," where "blog" and "shop" are subdomains of the main domain "example.com."





❖ Types of Top-Level Domains (TLD):

- Top-Level Domains (TLDs) are the highest level in the hierarchical Domain Name System (DNS). There are several types of TLDs, each serving different purposes and categories of websites. Here are the main types of TLDs.
- There are following types of TLD:

1. Generic Top-Level Domains (gTLDs):

- These are general-purpose domain extensions that are not tied to any specific country.

Examples:

- .com - Originally intended for commercial entities but now used by a wide range of websites.
- .org - Intended for non-profit organizations.
- .net - Originally intended for network infrastructure but now used by various types of websites.
- .info - Intended for informational websites.
- .biz - Intended for businesses and commercial use.
- .name - Intended for personal websites.

2. Country-Code Top-Level Domains (ccTLDs):

- These domain extensions are associated with specific countries or territories.They are two-letter codes based on ISO 3166-1 country codes.

Examples:

- .in- India
- .us - United States

- .uk - United Kingdom
- .ca - Canada
- .de - Germany
- .fr - France
- .jp - Japan

3. Sponsored Top-Level Domains (sTLDs):

- These are specialized domain extensions sponsored by specific organizations or communities.
- They serve specific industries, interest groups, or communities.

Examples:

- .edu - Intended for educational institutions in the United States.
- .gov - Restricted to U.S. government agencies.
- .mil - Restricted to U.S. military organizations.
- .int - Reserved for international organizations established by treaty.
- .aero - Intended for the aviation industry.
- .museum - Intended for museums and related organizations.

4. Infrastructure Top-Level Domains:

- These TLDs are used for infrastructure purposes and are not typically available for public registration.

Examples: .arpa - Used for the Address and Routing Parameter Area, primarily for technical infrastructure purposes.

URL

Uniform Resource Locator

Definition: - URL is a web address or location that pointing to a specific website.

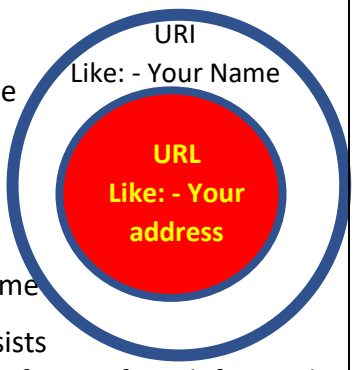
Use: it is used to describe the identify of resource on internet. URL is a type of URI (Uniform Resource Identifier. It is used only for locating web pages.)

History: - URL introduced by time Berners lee in 1991 **Example: -** https://www.twksaa.org

Component's: - path, domain, hash, string query & protocols

URL Contains: - 1. Port Number 2. Protocols 3. address 4. Location of service 5. Fragment 6. Directory Structure of server

URL Located: - Address bar or search bar at the top of the Browser

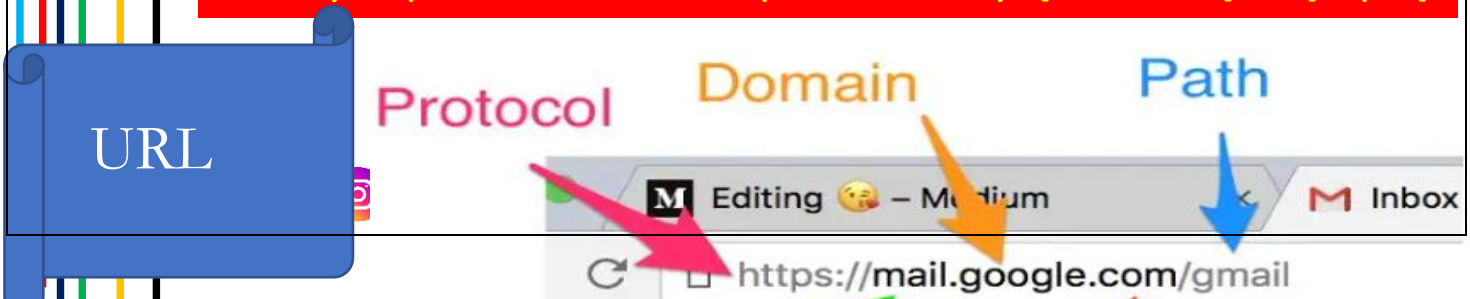


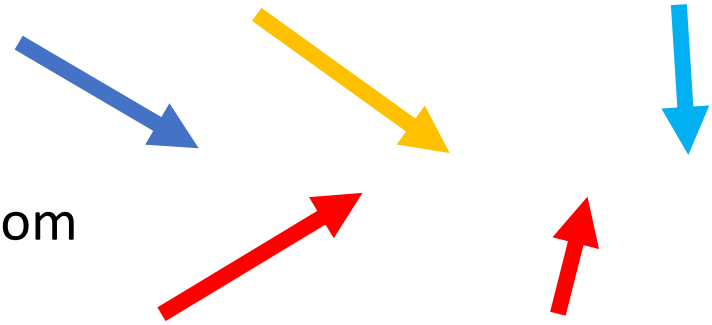
Format: - Combines the pre-existing system of domain name with file path. syntax //: - Slashes are used to separate directory and filename

HTTP URL conforms to syntax of a generic URI. URI generic syntax consists of five components organized hierarchically in order of decreasing significance from left to right

URI = scheme ":" ["//" authority] path ["?" query] ["#" fragment]

authority component consists of subcomponents: authority = [userinfo "@"] host [":" port]





DOMAIN NAME SYSTEM (DNS)

- Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network. It serves as the "phone book" of the Internet, translating human-readable domain names into numerical IP addresses and vice versa. This translation is crucial for enabling users to access websites, send emails, and perform other online activities using domain names.

1. **Domain Name:** A domain name is a human-readable label used to identify and locate resources on the Internet. Domain names consist of multiple parts separated by periods (dots), with the rightmost part indicating the top-level domain (TLD), such as .com, .org, .net, or a country-code TLD like .us or .uk. Examples of domain names include "example.com" and "google.com."
2. **DNS Resolver:** A DNS resolver is a client-side software or service responsible for initiating and processing DNS queries on behalf of users or applications. When a user enters a domain name into a web browser or other network application, the DNS resolver translates the domain name into an IP address by querying DNS servers.
3. **DNS Server:** A DNS server is a specialized computer or network device that stores DNS records and responds to DNS queries from DNS resolvers. DNS servers are organized into a hierarchical distributed network,with different types of DNS servers serving specific roles in resolution process.
4. **DNS Hierarchy:** The DNS hierarchy consists of multiple levels, each responsible for a specific portion of the DNS namespace. At the top of the hierarchy are the root DNS servers, which store information about the authoritative DNS servers for the TLDs (.com, .org, .net, etc.). Beneath the root servers are the authoritative DNS servers for each domain, which store DNS records (such as A, AAAA, MX, CNAME records) for the domain's subdomains and associated resources.

5. **DNS Record Types:** DNS records are data entries stored in DNS servers that provide information about domain names and their associated resources. Common types of DNS records include:
   - A (Address) Record: Maps a domain name to an IPv4 address.
   - AAAA (IPv6 Address) Record: Maps a domain name to an IPv6 address.
   - MX (Mail Exchange) Record: Specifies the mail servers responsible for receiving email messages for a domain.
   - CNAME (Canonical Name) Record: Alias for another domain name (canonical name).
   - TXT (Text) Record: Stores arbitrary text data associated with a domain name, often used for SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) records for email authentication.

❖ **DNS Resolution Process:** The DNS resolution process begins when a user or application sends a DNS query to a DNS resolver. The resolver first checks its local cache to see if it has a cached copy of the requested DNS record. If the record is not found in the cache, the resolver sends a recursive query to a series of DNS servers, starting with the root DNS servers and proceeding down the DNS hierarchy until it reaches the authoritative DNS servers for the requested domain.

❖ **Use: -** it is used to Translate Domain name to Ip address vice-versa. DNS was introduced on ARPANET in1983 and Published by Internet Engineering Task Force (IETF). Managed BY ICANN (Internet Corporation for Assigned Names and Numbers)

1. **Hostname Resolution:** Translates domain names to IP addresses, making it easier for users to access websites and services.
2. **Website Access:** Allows users to access websites by converting domain names entered into web browsers into IP addresses.
3. **Email Delivery:** Maps domain names to mail servers' IP addresses, ensuring email messages are delivered correctly.
4. **Application Connectivity:** Helps applications connect to servers, databases, and other resources by resolving domain names to IP addresses.
5. **Load Balancing:** Distributes network traffic across multiple servers to enhance performance and scalability.
6. **Failover and Redundancy:** Redirects traffic to backup servers or alternate IP addresses in case of failures, minimizing downtime.
7. **Content Delivery Networks (CDNs):** Improves content delivery by directing users to optimal server locations based on factors like geographic location.
8. **Security:** Supports various security mechanisms, including domain validation and threat detection, to protect against malicious activities.

❖Name Space:

- Name spaces are organizational structures used in various contexts, including computer systems and networking, to manage and organize names or identifiers. Two common types of name spaces are flat name space and hierarchy name space.

❖ Types Name Space:

1). Flat Name Space 2). Hierarchy Name Space

1. Flat Name Space:

- In a flat name space, all names or identifiers exist at the same level without any hierarchical structure.

- Each name is unique within the name space but does not have any relationship or hierarchy with other names.
- Examples of flat name spaces include some file systems where files are organized in a single directory without any subdirectories.
- In a flat name space, resolving conflicts or ensuring uniqueness of names may require additional mechanisms, such as appending numbers or random strings to duplicate names.

2. Hierarchy Name Space:

- In a hierarchy name space, names are organized in a hierarchical or tree-like structure, with parent-child relationships between names.
- Each name in the hierarchy is part of a larger structure and can have one or more subnames (children) and a parent name (except for the root).
- Hierarchy name spaces allow for logical organization and categorization of names, making it easier to manage and navigate large sets of names.
- Examples of hierarchy name spaces include the Domain Name System (DNS) used on the Internet, where domain names are organized in a hierarchical structure consisting of levels such as top-level domains (TLDs), second-level domains (SLDs), and subdomains.
- In a hierarchy name space, resolving names involves traversing the hierarchy from the root to the desired name, following a specific path based on the structure of the name space.

❖ DNS Resolver Method:

- DNS resolver method refers to how DNS queries are processed by DNS resolvers, which are client-side software or services responsible for initiating and handling DNS queries on behalf of users or applications. There are two main methods used by DNS resolvers to resolve DNS queries: iterative method and recursive method.

❖ Types of DNS Resolver Method:

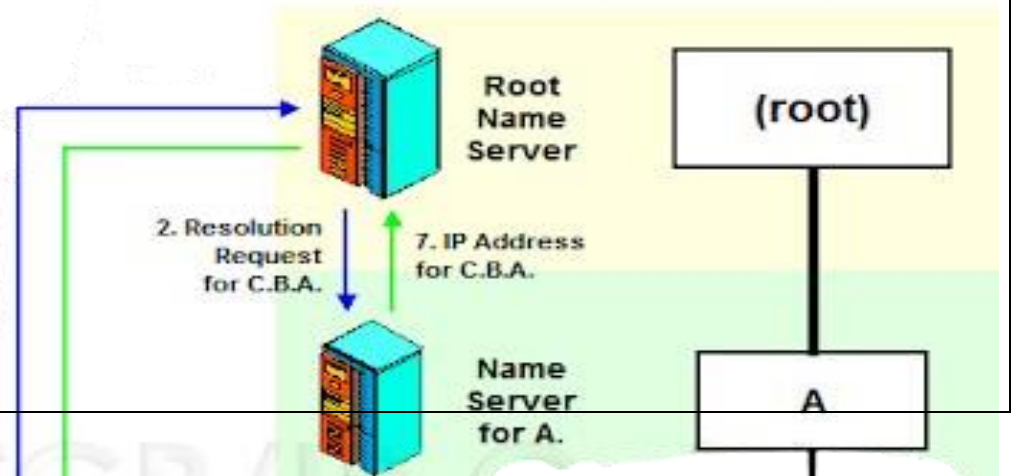
1) Iterative Method 2). Recursive Method

1. Iterative Method:

- In the iterative method, the DNS resolver sends a query to a DNS server and expects either a response with the requested information or a referral to another DNS server.
- The DNS server receiving the query may not have the requested information but can provide a referral to another DNS server that may have more specific information or be closer to the requested domain in the DNS hierarchy.
- If the DNS server has the requested information, it returns a response with the corresponding DNS records to the resolver. However, if it doesn't have the information, it returns a referral to the resolver, indicating the next DNS server to contact.
- The resolver then sends subsequent queries to the referred DNS server, continuing the process until it receives a response with the requested information or reaches the authoritative DNS server for the domain.
- The iterative method allows the resolver to interact with multiple DNS servers, making multiple queries and receiving referrals until it obtains the desired DNS records. It puts the burden of resolving the query on the resolver, which must follow referrals and continue the process until the end.

2. Recursive Method:

- In the recursive method, the DNS resolver sends a query to a DNS server and expects the server to handle the entire resolution process on its behalf.
- The DNS server receiving the query either has the requested information in its cache or contacts other DNS servers to resolve the query recursively.
- If the DNS server has the requested information in its cache or can resolve the query without further queries, it returns a response with the corresponding DNS records to the resolver.
- If the DNS server doesn't have the information in its cache, it contacts other DNS servers on behalf of the resolver, following referrals and resolving the query recursively until it obtains the requested information.
- Once the DNS server has resolved the query, it returns a complete response with the DNS records to the resolver, which then passes the information to the requesting application or user.
- The recursive method simplifies the resolution process for the resolver, as it delegates the entire process to DNS servers. The resolver only sends a single query and receives a complete response, without needing to interact with multiple servers or follow referrals.



Definition: - it is network of network. Or the global System of interconnected computer networks

use: - it is used to communicate between network & device by using the suite of network Protocols.

Discover: - US DOD, ARPA (advance Research projects agency) in 1969 1st Internet ARPANE

How it's Work: - 1. Packets & 2. Protocols

ICANN: - Internet Corporation for Assigned Names and Numbers "Organisation" responsibl (Domain names, IP addresses, application port numbers & other parameters.

ISP: Internet service Provider, it's provide internet **1). Tier-1** {Globally} **2).Tier-2** {Countries wise} **3).Tier-3** {Local}

IPS: - Internet Protocals Suite **1). TCP/IP** Model **2). OSI** (opent System Interconection) Model

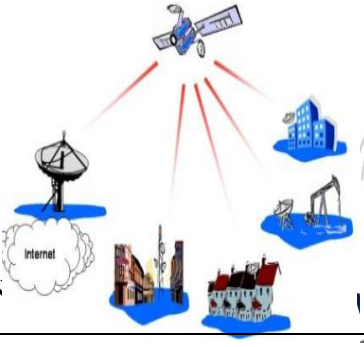
RIR: - Regional Internet registries established five regions of the world for assign IP address & other Internet parameters. **1. AfriNIC:**-African Network Information Center **for Africa**, **2.ARIN:**-American Registry Internet Numbers **for North America** **3.APNIC:**-Asia-Pacific NIC **for Asia** **4. LACNIC:**for Latin America &**5. RIPE NCC:**-Réseaux IP Européens – Network Coordination Centre **for Europe**

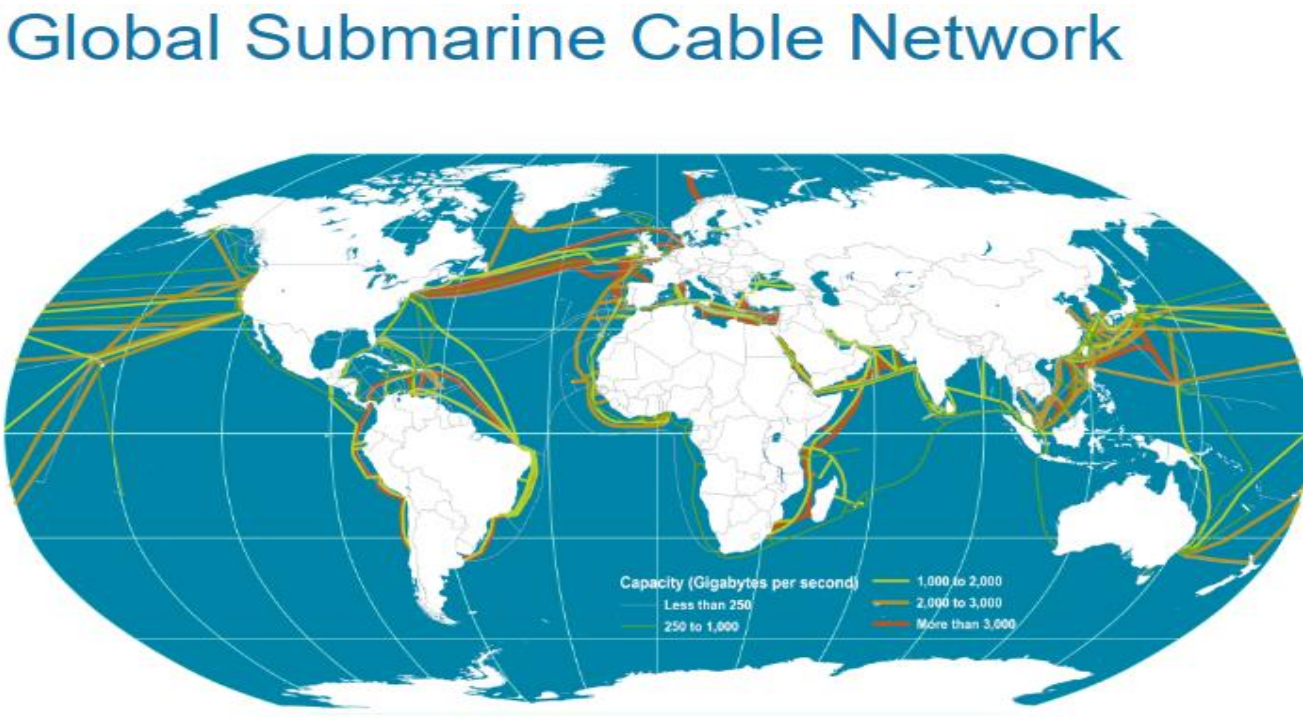
Parameter's: 1). Network 2).IP Address 3). Protocols 4).Domain Name 5).Port Number & 6).ISP

Access: 1).Cellular telephone (3G,4G, 5G, …) 2).Wi-fi 3).Satellite 4).Fibber Optics 5).Coaxial cable 6).Copper wire 7).DSL(Digital Subscriber Line) 8). BPL (Broadband over powerless 9).DLL

Application: - www, Social Media, Mobile Application, mail, File Transfer, Online work etc…

Internetworking Device: - Router, Switch, Internet Gateway etc..





services through a vast collection of private, public, business, academic, and government networks. It serves as a virtual infrastructure that links millions of computers and electronic devices worldwide, allowing users to exchange information seamlessly.

- The Internet is a global network of billions of computers and other electronic devices. By connecting a computer to the Internet (also known as going online), you gain access to almost any information and the ability to communicate with people worldwide.
- internet, often referred to simply as "the Net," is a global network of interconnected computer networks that utilize standardized communication protocols to link devices worldwide.
- internet serves as a global information superhighway, connecting billions of users worldwide and facilitating the exchange of knowledge, ideas, and experiences on an unprecedented scale. Its profound impact on society, economy, and culture continues to shape the modern world, driving innovation, connectivity, and digital transformation across industries.

❖ History of Internet:

➢ The history of the internet is a fascinating journey that spans several decades and involves numerous technological advancements, pioneering initiatives, and key milestones.

1) **Early Beginnings (1960s):** The internet's origins can be traced back to the 1960s, with the development of ARPANET (Advanced Research Projects Agency Network) by the United States Department of Defense. ARPANET was created to connect computers at various research institutions and enable them to share resources and communicate with each other.
2) **ARPANET and TCP/IP (1970s):** ARPANET grew steadily throughout the 1970s, expanding its network of interconnected computers. During this time, the TCP/IP (Transmission Control Protocol/Internet Protocol) suite was developed, providing a standardized set of protocols for transmitting data across networks. TCP/IP laid the groundwork for the modern internet's communication architecture.

3) **Commercialization and Expansion (1980s):** The 1980s saw the commercialization of the internet, as more organizations and institutions began to connect to ARPANET. The National Science Foundation (NSF) established NSFNET, a network backbone that significantly expanded the internet's reach and capabilities.
4) **World Wide Web (1990s):** The invention of the World Wide Web in the early 1990s revolutionized the internet. Tim Berners-Lee, a British computer scientist, developed the concept of the WWW, which allowed users to access and navigate interconnected web pages using hyperlinks. The introduction of web browsers, such as Mosaic and later Netscape Navigator, made the WWW accessible to the general public, sparking a surge in internet usage and online activity.
5) **Dot-Com Boom (late 1990s):** The late 1990s saw the rise of the dot-com boom, characterized by a rapid growth of internet-based companies and investments in the burgeoning online market. E-commerce, social networking, and digital content distribution became increasingly prominent, reshaping industries and economies worldwide.
6) **Broadband and Mobile Internet (2000s):** The 2000s witnessed the widespread adoption of broadband internet connections, which offered faster speeds and greater bandwidth compared to dial-up connections. Additionally, advancements in mobile technology, such as smartphones and wireless networks, led to the proliferation of mobile internet usage, allowing users to access the internet anytime, anywhere.
7) **Cloud computing Origins (2000s):** Cloud computing emerged in the mid-2000s as a response to the increasing demand for scalable and flexible computing resources. Companies like Amazon, Google, and Salesforce pioneered the concept, offering services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
8) **Social Media and Web 2.0 (2000s-2010s):** The rise of social media platforms, such as Facebook, Twitter, and YouTube, transformed the internet into a social and interactive medium. Web 2.0 technologies enabled user-generated content, collaboration, and community-building, empowering individuals to create and share content online.
9) **Internet of Things (IoT) and Future Trends (2010s-present):** In recent years, the internet has continued to evolve with the emergence of new technologies such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain. These innovations are driving the development of smart connected devices, autonomous systems, and decentralized applications, shaping the internet's future trajectory.

❖ Use of internet:

- **Access Information:** Instantly retrieve vast amounts of information on virtually any topic through websites, search engines, and online databases.
- **Communication:** Connect with others worldwide via email, instant messaging, social media platforms, and video conferencing tools.
- **Entertainment:** Stream videos, music, and games, access digital libraries, and participate in online forums and communities.
- **Commerce:** Conduct online shopping, banking, and financial transactions, as well as engage in e-commerce activities such as buying and selling goods and services.
- **Education:** Access online courses, tutorials, and educational resources, facilitating distance learning and self-directed study.
- **Work and Collaboration:** Collaborate on projects, share documents, and communicate with colleagues remotely through cloud-based productivity tools and platforms.

- **Research and Innovation:** Facilitate research and development across various disciplines, fostering innovation, collaboration, and knowledge exchange.
- **News and Information:** Stay updated on current events, trends, and developments through news websites, blogs, and online publications.

❖ Characteristics of the internet:

1. **Global Connectivity:** The internet connects devices and users worldwide.
2. **Decentralization:** It operates without a single point of control, distributed across interconnected devices.
3. **Interoperability:** Standardized protocols enable seamless communication between diverse systems and platforms.
4. **Scalability:** Capable of accommodating large numbers of users and devices while maintaining performance.
5. **Accessibility:** Available to a broad audience through various means, including wired and wireless connections.
6. **Information Exchange:** Facilitates the exchange of data and content through various applications and services.
7. **Openness:** Fosters collaboration, innovation, and freedom of expression across diverse communities.
8. **Security and Privacy:** Incorporates measures to protect data and users from cyber threats and breaches.
9. **Evolutionary:** Continuously evolves to adapt to technological advancements and societal needs.

❖ Accessing the Internet:

➢ Accessing the internet involves connecting a device, such as a computer, smartphone, or tablet, to the global network of interconnected computers and servers. This connection is typically established through an internet service provider (ISP) using various means, including:

1. **Wired Connections:** Through Ethernet cables or fiber optic lines connected to a modem or router.
2. **Wireless Connections:** Using Wi-Fi technology, which allows devices to connect to a local network wirelessly, typically within range of a router.
3. **Mobile Networks:** Accessing the internet through cellular data networks provided by mobile carriers, using devices equipped with cellular connectivity.

❖ How internet works:

1. Packets:

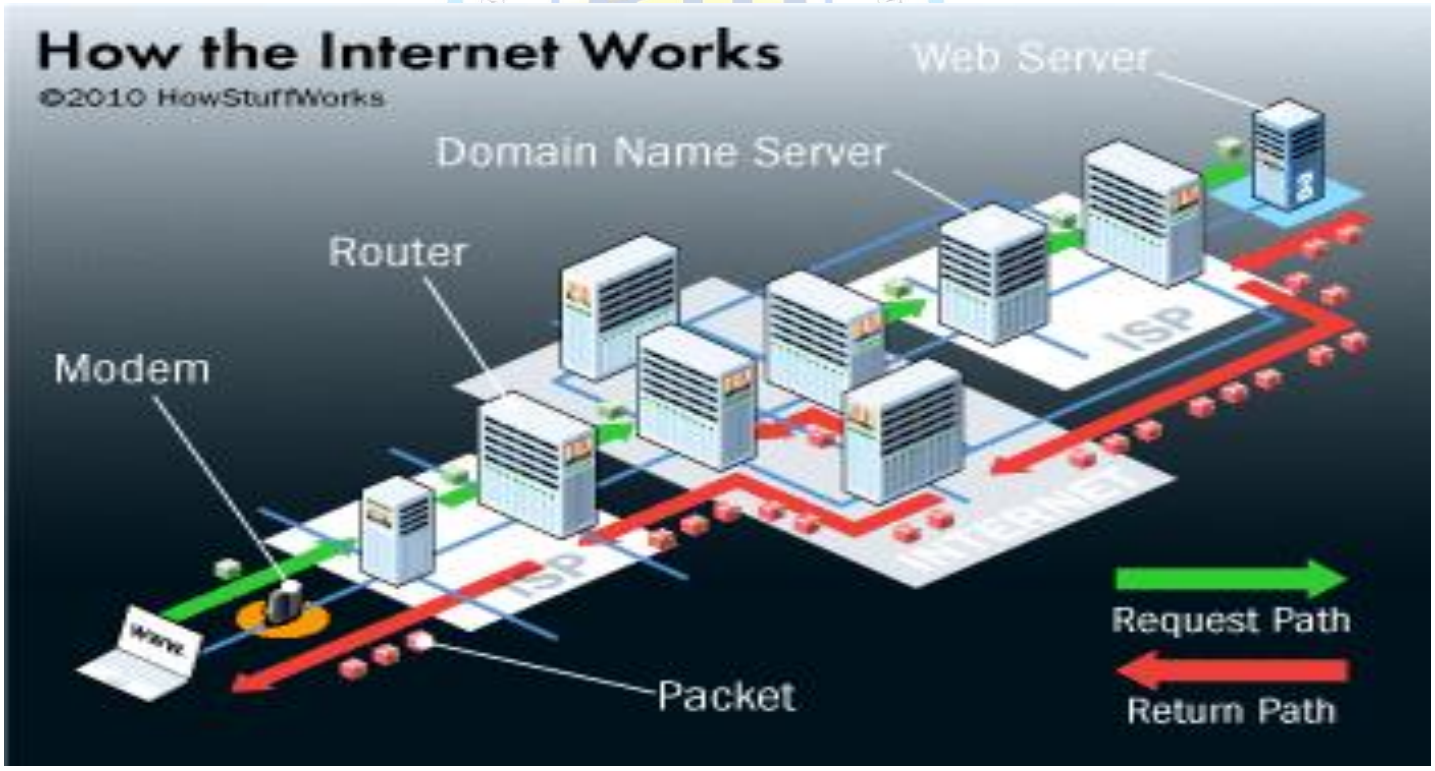
➢ **What are Packets?**

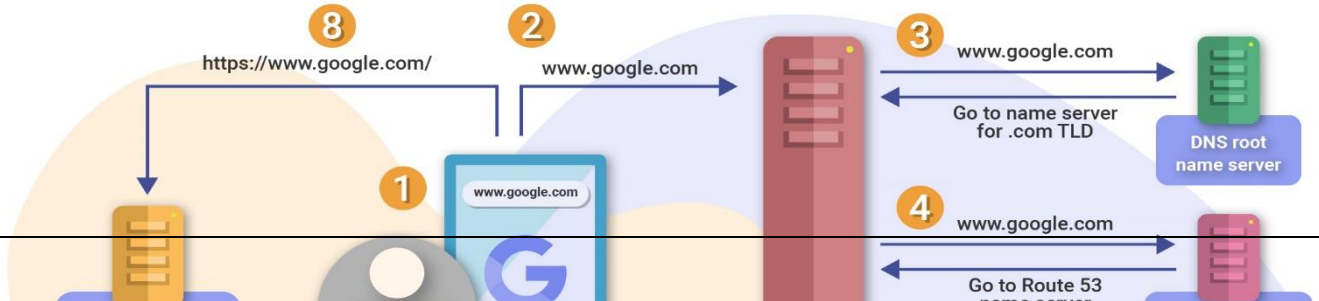
- Packets are units of data that are transmitted over a network. When data is sent over the internet, it is broken down into smaller packets for efficient transmission. Each packet contains a portion of the original data, along with additional information such as the source and destination addresses.

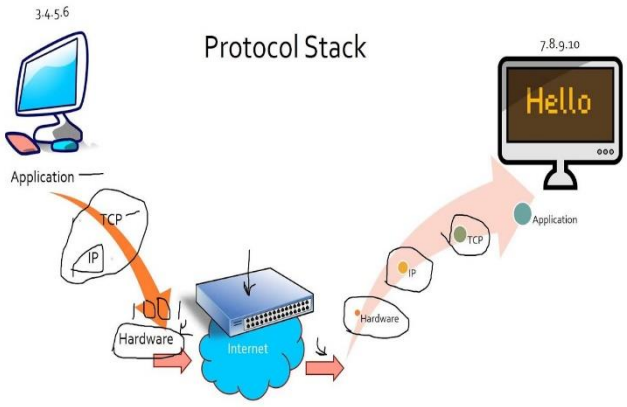
➢ **Packet Structure:**

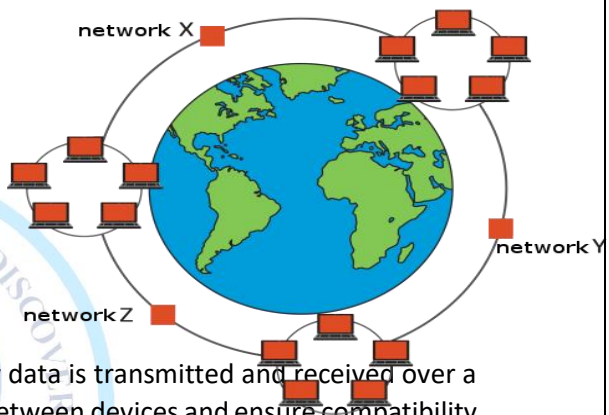
- Each packet consists of a header and a payload. The header contains essential information needed for routing and delivery, including the source and destination IP addresses, packet sequence number, and protocol information. The payload contains the actual data being transmitted, such as a portion of a file, a web page, or an email message.

- **Packet Switching:**
  - Packet switching is a fundamental principle of how data is transmitted over the internet. Instead of sending data in a continuous stream, it is broken down into packets, which are then routed independently across the network. This allows for more efficient use of network resources and enables data to take different paths to reach its destination.
- **Routing:**
  - Routers are devices that play a crucial role in packet switching. They examine the destination address in each packet's header and use routing tables to determine the best path for forwarding the packet towards its destination. Routers may employ various algorithms to select the most efficient route based on factors.
- **Transmission:**
  - Once a packet reaches its destination, it is reassembled into the original data stream. This process occurs at the receiving device, which uses the information in the packet headers to reconstruct the data in the correct order.









that govern how data is transmitted and received over a communication between devices and ensure compatibility and interoperability between different systems and platforms.

- **Internet Protocol (IP):**
  - The Internet Protocol (IP) is a fundamental protocol that provides the addressing scheme used to identify devices on the internet. IP addresses uniquely identify each device connected to the network and are used to route packets between them.
- **Transmission Control Protocol (TCP) and User Datagram Protocol (UDP):**
  - TCP and UDP are transport layer protocols responsible for establishing connections, breaking data into packets, and ensuring reliable and efficient communication between devices. TCP provides a connection-oriented communication channel, guaranteeing that data is delivered in the correct order and without errors. UDP, on the other hand, is connectionless and lightweight, suitable for applications that prioritize speed and efficiency over reliability, such as real-time streaming and online gaming.
- **HTTP and HTTPS:**
  - Hypertext Transfer Protocol (HTTP) is a protocol used for transmitting web pages and other hypertext documents on the World Wide Web. HTTPS (HTTP Secure) adds an extra layer of security by encrypting data exchanged between the client and server, ensuring confidentiality and integrity.
- **Domain Name System (DNS):**
  - The Domain Name System (DNS) translates human-readable domain names (e.g., www.example.com) into numerical IP addresses that computers use to locate servers on the internet. DNS servers maintain a distributed database of domain names and their

corresponding IP addresses, allowing users to access websites using familiar and easy-to-remember URLs.

❖ Types of internets:

1. Dial-Up:

- Dial-up Internet became commercially available in the 1990s.
- Users purchased modems from telephone service providers, with the most common being the 56K modem (maximum speed of 56 kbit/s).
- A limitation was that the Internet couldn't be used while someone was on the phone, as both services shared a single telephone line.
- Surprisingly, dial-up is still in use today, especially in remote areas and third-world countries where Internet access is scarce or nonexistent1.

2. DSL (Digital Subscriber Line):

- DSL broadband Internet followed dial-up.
- Known as ADSL (Asymmetrical Digital Subscriber Line), it operated through a telephone network.
- Unlike dial-up, DSL allowed simultaneous voice calls and Internet usage.
- Download speeds ranged from 256 Kbit/s to around 100 Mbit/s, with common speeds around 6 Mbit/s to 8 Mbit/s1.

3. Cable:

- Cable Internet access is widely used today.
- It operates over cable television lines, providing faster speeds than DSL.
- Cable Internet remains the most commonly used form of the Internet in 2020

4. Wireless:

- Wireless Internet uses radio waves or microwaves for communication.
- Wi-Fi networks fall under this category, allowing devices to connect without physical cables.
- Wi-Fi hotspots, mobile data, and wireless routers enable wireless Internet access.

5. Satellite:

- Satellite Internet relies on communication satellites orbiting Earth.
- It's useful in remote areas where other forms of Internet infrastructure are unavailable.
- However, latency can be higher due to the signal traveling to and from space.

6. Cellular:

- Cellular networks provide Internet access via mobile devices.
- 3G, 4G, and now 5G networks offer varying speeds and coverage.

7. Fiber Optic:

- Fiber-optic cables transmit data using light signals.
- They offer incredibly high speeds and low latency.
- Fiber-optic Internet is becoming more widespread in urban areas.

8. ISDN (Integrated Services Digital Network):

- ISDN was popular in the past but has largely been replaced by newer technologies.
- It provided digital voice and data services over traditional telephone lines.

❖ Advantages and Disadvantage of internet:

Advantages:

1) **Access to Information:** The internet provides access to a vast amount of information on virtually any topic, allowing users to educate themselves, conduct research, and stay informed about current events.
2) **Communication:** The internet facilitates communication and collaboration through email, instant messaging, social media, and video conferencing tools, enabling individuals and businesses to connect with others worldwide.
3) **Convenience:** With the internet, tasks such as shopping, banking, and paying bills can be done conveniently from the comfort of home, saving time and effort.
4) **Entertainment:** The internet offers a wide range of entertainment options, including streaming movies and music, playing online games, and accessing digital content.
5) **E-commerce:** The internet has revolutionized commerce, enabling businesses to reach a global audience and customers to shop online anytime, anywhere, fostering economic growth and innovation.
6) **Education:** Online courses, tutorials, and educational resources available on the internet make learning accessible and convenient, allowing individuals to acquire new skills.
7) **Social Connection:** Social media platforms and online communities allow people to connect with friends, family, and like-minded individuals, fostering social interaction.

Disadvantages:

1) **Information Overload:** The abundance of information on the internet can be overwhelming, making it difficult to discern credible sources from misinformation or fake news.
2) **Privacy Concerns:** The internet raises concerns about privacy and data security, as personal information shared online can be vulnerable to hacking, surveillance, and misuse by third parties.
3) **Cybersecurity Threats:** The internet is susceptible to various cybersecurity threats, including malware, phishing scams, identity theft, and cyberattacks, posing risks to individuals and organizations.
4) **Digital Divide:** Not everyone has equal access to the internet due to factors such as geography, socioeconomic status, and infrastructure limitations, exacerbating inequalities and disparities in access to information and opportunities.
5) **Addiction and Distraction:** Excessive internet usage, especially on social media and gaming platforms, can lead to addiction, compulsive behavior, and reduced productivity, impacting mental health and well-being.
6) **Online Harassment and Bullying:** The anonymity of the internet can facilitate harassment, cyberbullying, and trolling, causing emotional distress and harm to individuals, particularly vulnerable populations such as children and teenagers.
7) **Dependency:** Dependency on the internet for essential tasks such as communication, information access, and commerce can lead to reliance issues and difficulties functioning without internet connectivity in case of outages or disruptions.

❖ ICANN:

- ICANN, the Internet Corporation for Assigned Names and Numbers, is the organization responsible for coordinating and managing various key aspects of the internet's infrastructure. Here's what ICANN oversees:

1. **Domain Names:** ICANN is responsible for overseeing the domain name system (DNS), which involves managing domain name registration and allocation. This includes the assignment of top-level domains (TLDs), such as .com, .org, and country-code TLDs like .uk and .jp.
2. **IP Addresses:** ICANN plays a role in the allocation and administration of IP addresses, which are numerical identifiers assigned to devices connected to the internet. While the Internet Assigned Numbers Authority (IANA) is responsible for the overall allocation of IP address blocks, ICANN helps manage the policies and procedures related to IP address distribution.
3. **Application Port Numbers:** ICANN is involved in the coordination of application port numbers, which are used to identify specific services or processes running on devices connected to the internet. Port numbers facilitate communication between devices and applications by specifying the destination for data packets.
4. **Other Parameters:** In addition to domain names, IP addresses, and application port numbers, ICANN is involved in managing other parameters related to internet infrastructure and standards. This may include protocols, technical standards, and policy development related to internet governance.

❖ internet Service Providers (ISPs):

➢ internet Service Providers (ISPs) play a crucial role in providing individuals and organizations with access to the internet. ISPs can be categorized into different tiers based on their network infrastructure and the scope of their operations:

1) Tier-1 ISPs (Globally):

- Tier-1 ISPs operate at the highest level of the internet hierarchy. These ISPs have vast networks and infrastructure that span across multiple continents and regions. They have direct connections to other Tier-1 ISPs, allowing them to exchange internet traffic without having to pay for transit services. Tier-1 ISPs serve as the backbone of the internet, handling a significant portion of global internet traffic.

2) Tier-2 ISPs (Country-wise):

- Tier-2 ISPs operate at a regional or national level within specific countries or regions. While they may have extensive networks and infrastructure within their respective territories, Tier-2 ISPs typically rely on transit agreements with Tier-1 ISPs to connect to the rest of the internet. They serve as intermediaries between Tier-1 ISPs and Tier-3 ISPs, providing internet connectivity to local ISPs and end-users.

3) Tier-3 ISPs (Local):

- Tier-3 ISPs are local or regional providers that offer internet services to end-users within specific communities or areas. They typically lease network infrastructure from Tier-1 or Tier-2 ISPs and focus on providing internet access to residential and small business customers. Tier-3 ISPs may offer a range of internet connectivity options, including dial-up, DSL, cable, fiber-optic, and wireless broadband services.

❖ Internet Protocol Suite (IPS):

➢ Indeed, the Internet Protocol Suite (IPS) encompasses the foundational protocols used for communication over the internet. Let's briefly explore the two primary models within the IPS:

1. TCP/IP Model:

➢ The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a conceptual framework used to describe the protocols and functions involved in internet communication.

➢ It consists of four layers:

1. **Application Layer:** This layer includes protocols like HTTP, FTP, SMTP, and DNS, which facilitate communication between applications running on different devices.
2. **Transport Layer:** The TCP and UDP protocols operate at this layer, providing reliable, connection-oriented communication (TCP) and unreliable, connectionless communication (UDP) between devices.
3. **Internet Layer:** The Internet Protocol (IP) operates at this layer, handling the routing and forwarding of data packets between networks.
4. **Link Layer:** This layer encompasses the protocols and technologies used for local network communication, such as Ethernet, Wi-Fi, and PPP.

2. OSI Model (Open Systems Interconnection):

- OSI model is a conceptual framework developed by International Organization for Standardization (ISO) to standardize the communication process between different computer systems.

➢ It consists of seven layers:

1. **Application Layer:** Provides network services directly to end-users and application programs.
2. **Presentation Layer:** Handles data formatting, encryption, and compression to ensure that data exchanged between systems can be interpreted correctly.
3. **Session Layer:** Manages communication sessions and establishes, maintains, and terminates connections between devices.
4. **Transport Layer:** Ensures reliable data transmission between devices and handles error detection and correction.
5. **Network Layer:** Responsible for routing and forwarding data packets between networks based on logical addresses (e.g., IP addresses).
6. **Data Link Layer:** Handles the transmission of data frames over the physical network medium and provides error detection and flow control.
7. **Physical Layer:** Deals with the physical transmission of data over the network medium, including specifications for cables, connectors, and transmission rates.

❖ RIR: - Regional Internet registries established five regions of the world for assign IP address & other

- Regional Internet Registries (RIRs) are organizations responsible for the allocation and management of IP address space and related internet resources within specific geographic regions. Here's an overview of the five RIRs and their respective regions:

1. AfriNIC (African Network Information Center):

- Responsible for the allocation and management of IP address space and ASNs (Autonomous System Numbers) in Africa and the surrounding regions.
- Headquartered in Ebene, Mauritius, AfriNIC serves the African continent and parts of the Indian Ocean region.

2. ARIN (American Registry for Internet Numbers):

- Responsible for allocation and management of IP address space and ASNs in North America, including the United States, Canada, and several Caribbean and North Atlantic islands. Headquartered in Chantilly, Virginia, ARIN serves the North American region.

3. APNIC (Asia-Pacific Network Information Centre):

Responsible for the allocation and management of IP address space and ASNs in the Asia-Pacific region, encompassing East Asia, Southeast Asia, South Asia, and Oceania. Headquartered in Brisbane, Australia, APNIC serves the Asia-Pacific region.

4. LACNIC (Latin America and Caribbean Network Information Centre):

- Responsible for the allocation and management of IP address space and ASNs in Latin America and the Caribbean region.
- Headquartered in Montevideo, Uruguay, LACNIC serves Latin American and Caribbean region.

5. **RIPE NCC (Réseaux IP Européens – Network Coordination Centre):**
   - Responsible for the allocation and management of IP address space and ASNs in Europe, the Middle East, and Central Asia. Headquartered in Amsterdam, Netherlands, RIPE NCC serves the European and surrounding regions.

❖ **Parameter's:** 1). Network 2).IP Address 3). Protocols 4).Domain Name 5).Port Number & 6).ISP

1. Network:

- A network is a collection of devices, such as computers, servers, printers, and other hardware, connected together to share resources and communicate with each other. Networks can be classified based on their geographical scope (LAN, WAN, MAN) and their connection method (wired or wireless).

2. IP Address:

- An IP (Internet Protocol) address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. IP addresses serve two primary functions: host or network interface identification and location addressing. There are two versions of IP addresses in use today: IPv4 (32-bit) and IPv6 (128-bit).

3. Protocols:

- Protocols are a set of rules and conventions that govern the exchange of data between devices on a network. They define the format, timing, sequencing, and error control of data transmission. Examples of network protocols include TCP (Transmission Control Protocol), UDP (User Datagram Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol).

4. Domain Name:

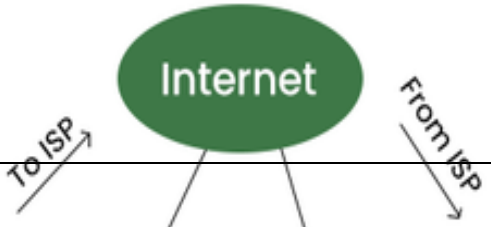
- A domain name is a human-readable label that serves as an easy-to-remember alias for the numerical IP address of a server hosting a website or other internet services. Domain names are organized hierarchically and consist of two main parts: the top-level domain (TLD) and the second-level domain (SLD). For example, in the domain name "example.com," ".com" is the TLD, and "example" is the SLD.

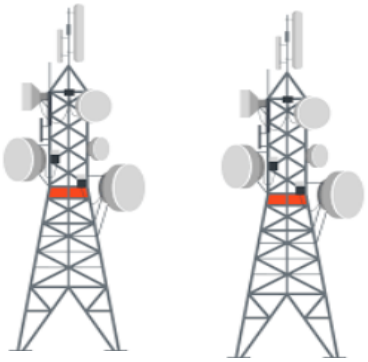
5. Port Number:

- A port number is a numerical identifier used by network protocols to distinguish between different services or processes running on a single device. Ports allow multiple services to operate concurrently on the same device without interfering with each other. Well-known port numbers are reserved for specific services, such as port 80 for HTTP (web browsing) and port 25 for SMTP (email).

6. ISP (Internet Service Provider):

- An Internet Service Provider (ISP) is a company that provides individuals and organizations with access to the internet. ISPs offer various types of internet connections, such as dial-up, DSL, cable, fiber-optic, and wireless broadband. They typically charge subscription fees for internet access and may also provide additional services such as email, web hosting, and online storage.





Definition: - www is a global collection of documents and other resources linked by hyperlink and URLs.it is known as web, it is an information system technology enabling.

History: - computer scientist "Tim Berners Lee" at CERN {(European Organization for nuclear Research) it is a Intergovernmental org. established in 1954)} invented in1989.1st proposal was written & working system implemented by end of 1990 including www Browser & http server.

Function: - 1).HTML 2). Linking 3). www prefix 4). Scheme specifiers 5). Web Page 6). Website 7). Browser 8). Search Engine 9). Server 10). Cookie 11). Deep web 12). Caching 13). Security 14). Privacy 15). Standards

HTML: - Hypertext Markup Language it used for Creating Web page & Web Application.

Linking: - it is interconnecting the web page via Hyperlinks.

www prefix: -it is like .com, .org, .net etc. **Scheme specifiers: -** http:// or https://

Browser: - it is a software responsible for open the website

Web Page: - A webpage is an HTML document on the WWW. **Website: -** it is a collection of web page.

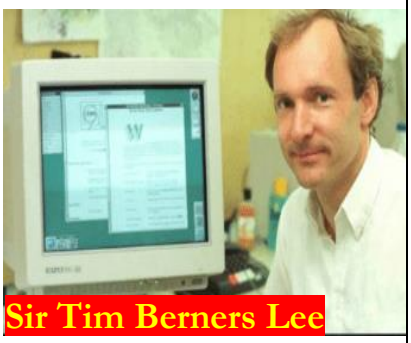
Search Engine: - it is a software program/system Software Desigen to carry out the web search.

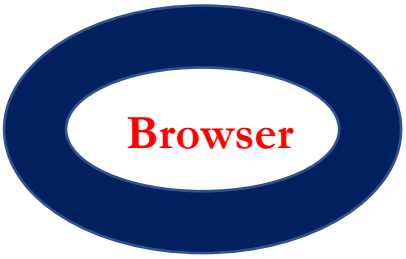
Server: - it is a software or hardware device that accept & respond to request made over a network.

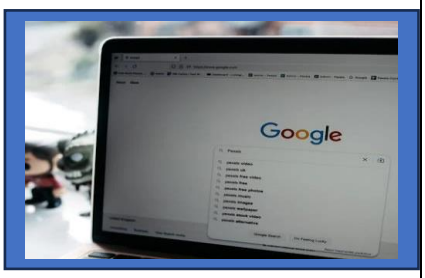
Cookie: - it is a small piece of data sent from the website and stored on the user's computer by the web browser while user is browsing. It is stateful

Deep web: - it is an invisible web or hidden web are parts of www whose contents are not indexed by standard web search engine. Computer scientist "Michael K. Bergman" is credited with deep web in 2001

Caching: - A web cache is a server computer located on the public internet. It is stores recently accessed web page to improve response time for user's







Definition: - Browser is an application software or a software Program.

Use: - Browser is used for accessing websites fetch content from the www or from local storage and display on the user's Device

History: - www was the 1st Browser created in 1990 by sir Tim Berner Lee Mosaic-1993 Netscape-1994 Internet Explorer-1995 Opera-1995 Mozilla Firefox-2004 Safari-2003 Chrome-20008 Edge-

Features: - Automatically log user's Browsing history, set Book Marks, Customize Browser with Extensions, User password, Sync Service, Web Accessibility, open Multiple Pages, Back & forward Bottoms, Refresh, Reload Stop, Home bottom, Address Bar to IP URLs and security etc.

❖ World Wide Web (WWW):

- The World Wide Web (WWW) is a global information system comprised of interconnected documents and resources, accessible via hyperlinks and Uniform Resource Locators (URLs). Commonly referred to as the "web," it's a fundamental component of the internet infrastructure, facilitating the dissemination and retrieval of information across various devices and platforms.
- The web enables users to navigate between web pages, access multimedia content, engage with interactive applications, and communicate with others worldwide. It serves as a cornerstone of modern information technology, revolutionizing how individuals, businesses, and organizations access and share information on a global scale.

❖ History of WWW:

- In 1989, computer scientist Tim Berners-Lee, working at CERN (European Organization for Nuclear Research), proposed the concept of the World Wide Web (WWW) as a means to facilitate the sharing and retrieval of scientific information among researchers. By the end of 1990, he had not only written the first proposal for the WWW but also developed a working system that included a web browser (the WorldWideWeb browser) and a Hypertext Transfer Protocol (HTTP) server.
- This groundbreaking invention laid the foundation for the modern internet, revolutionizing communication, collaboration, and information dissemination on a global scale. CERN, established in 1954, is an intergovernmental organization dedicated to nuclear research and is headquartered in Geneva, Switzerland.

❖ Function of WWW:

- 1).HTML 2). Linking 3). www prefix 4). Scheme specifiers 5). Web Page 6). Website 7). Browser 8). Search Engine 9). Server 10). Cookie 11). Deep web 12). Caching 13). Security 14). Privacy 15). Standards

1. HTML (Hypertext Markup Language):

- HTML is the standard markup language used to create and structure web pages. It consists of elements and tags that define the structure, content, and layout of web documents.

2. Linking:

- Linking involves connecting different web pages or resources together using hyperlinks. Hyperlinks allow users to navigate between pages, access related content, and explore the web.

3. www Prefix:

- The "www" prefix in a URL (Uniform Resource Locator) stands for "World Wide Web" and is commonly used to identify web pages or resources accessible via the internet.

4. Scheme Specifiers:

- Scheme specifiers, such as "http://" or "https://", indicate the protocol used to access a web resource. For example, "http://" denotes the Hypertext Transfer Protocol, while "https://" denotes the secure version, HTTPS.

5. Web Page:

- A web page is a single document or file accessible via the World Wide Web. It typically contains text, images, multimedia elements, and hyperlinks, designed to be viewed in a web browser.

6. Website:

- A website is a collection of related web pages hosted on a web server and accessible via the internet. Websites often have a common theme or purpose and may include multiple web pages, subpages, and multimedia content.

7. Browser:

- A web browser is a software application used to access and view web pages on the internet. Popular web browsers include Chrome, Firefox, Safari, and Edge.

8. Search Engine:

- A search engine is a web-based tool that allows users to search for information on the internet. Search engines index and catalog web pages, enabling users to find relevant content based on keywords or phrases.

9. Server:

- A server is a computer or system that hosts web resources and delivers them to clients, such as web browsers, upon request. Servers store web pages, databases, and other files, making them accessible to users over the internet.

10. Cookie:

- A cookie is a small piece of data stored on a user's device by a website. Cookies are used to track user preferences, store login information, and personalize the browsing experience.

11. Deep Web:

- The deep web refers to content on the internet that is not indexed by search engines and is not easily accessible through standard web browsers. It includes databases, private networks, and other resources that require specific access credentials or permissions.

12. Caching:

- Caching involves storing copies of web resources, such as web pages and images, on local servers or devices to improve performance and reduce load times. Cached content can be retrieved more quickly, especially for frequently accessed resources.

13.Security:

- Security measures are protocols, technologies, and practices implemented to protect web resources, users' data, and communications from unauthorized access, data breaches, and cyberattacks.

14.Privacy:

- Privacy concerns the protection of individuals' personal information and data privacy rights while using the internet. Privacy measures aim to ensure that users have control over their personal data and how it is collected, stored, and used by websites and online services.

15.Standards:

- Standards refer to established guidelines, protocols, and specifications that ensure interoperability, compatibility, and reliability of web technologies. Standards organizations, such as the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF), develop and maintain standards for web development, networking, and internet protocols.

❖ Working of WWW:

➢ The World Wide Web (WWW) works through a combination of client-server architecture, protocols, and technologies that enable the sharing and retrieval of information across the internet. Here's an overview of how the WWW works:

1. Client-Server Model:

- The WWW operates on a client-server model. Clients, such as web browsers, request web resources from servers, which store and deliver those resources upon request.

2. HTTP Protocol:

- The Hypertext Transfer Protocol (HTTP) is the primary protocol used for communication between clients and servers on the WWW. It defines how messages are formatted and transmitted, allowing clients to request web resources (e.g., web pages, images, files) from servers.

3. Web Addresses (URLs):

- Web resources are identified by Uniform Resource Locators (URLs), which consist of a scheme specifier (e.g., "http://" or "https://"), a domain name (e.g., "example.com"), and a path to the specific resource on the server.

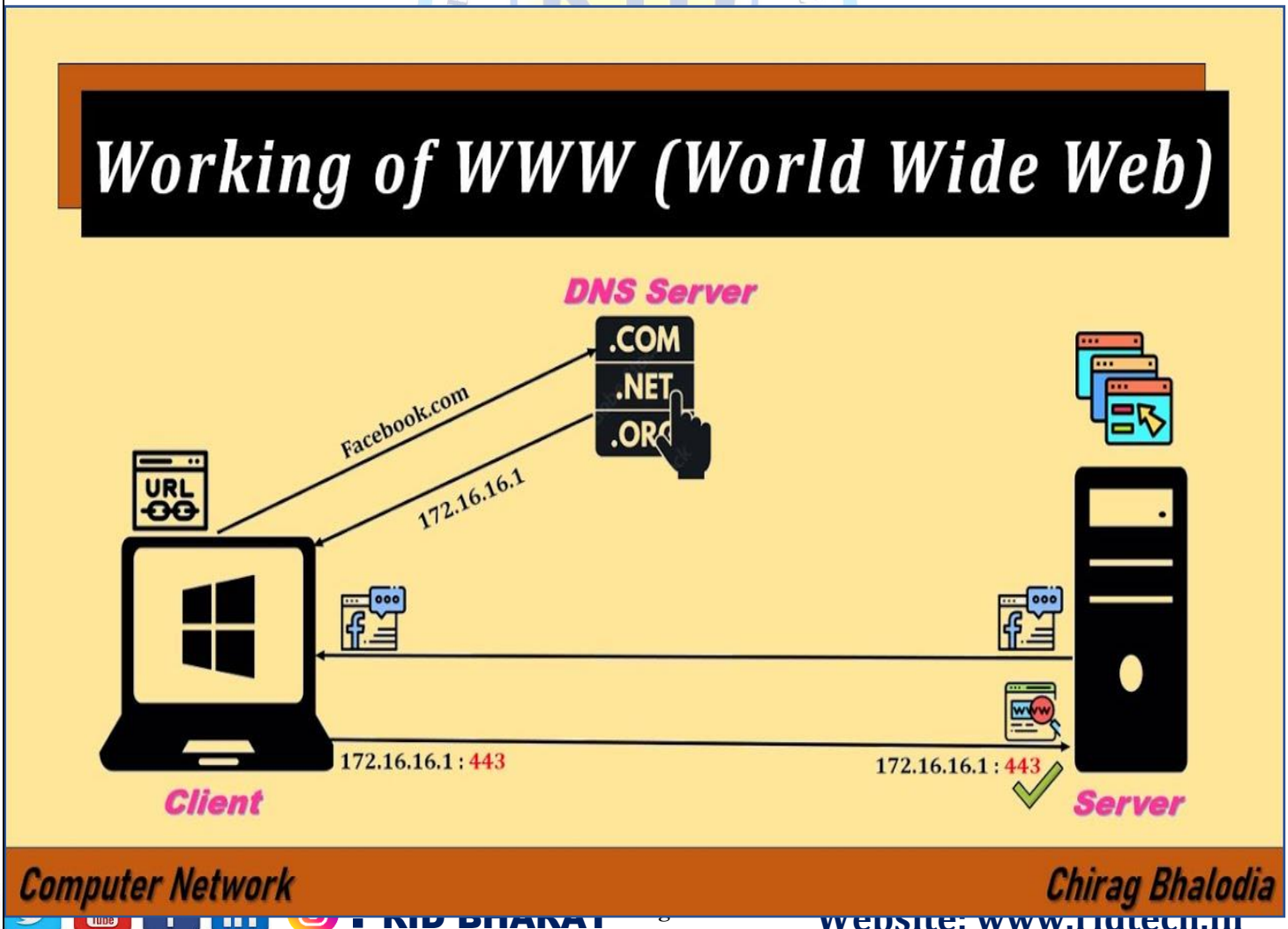
4. DNS Resolution:

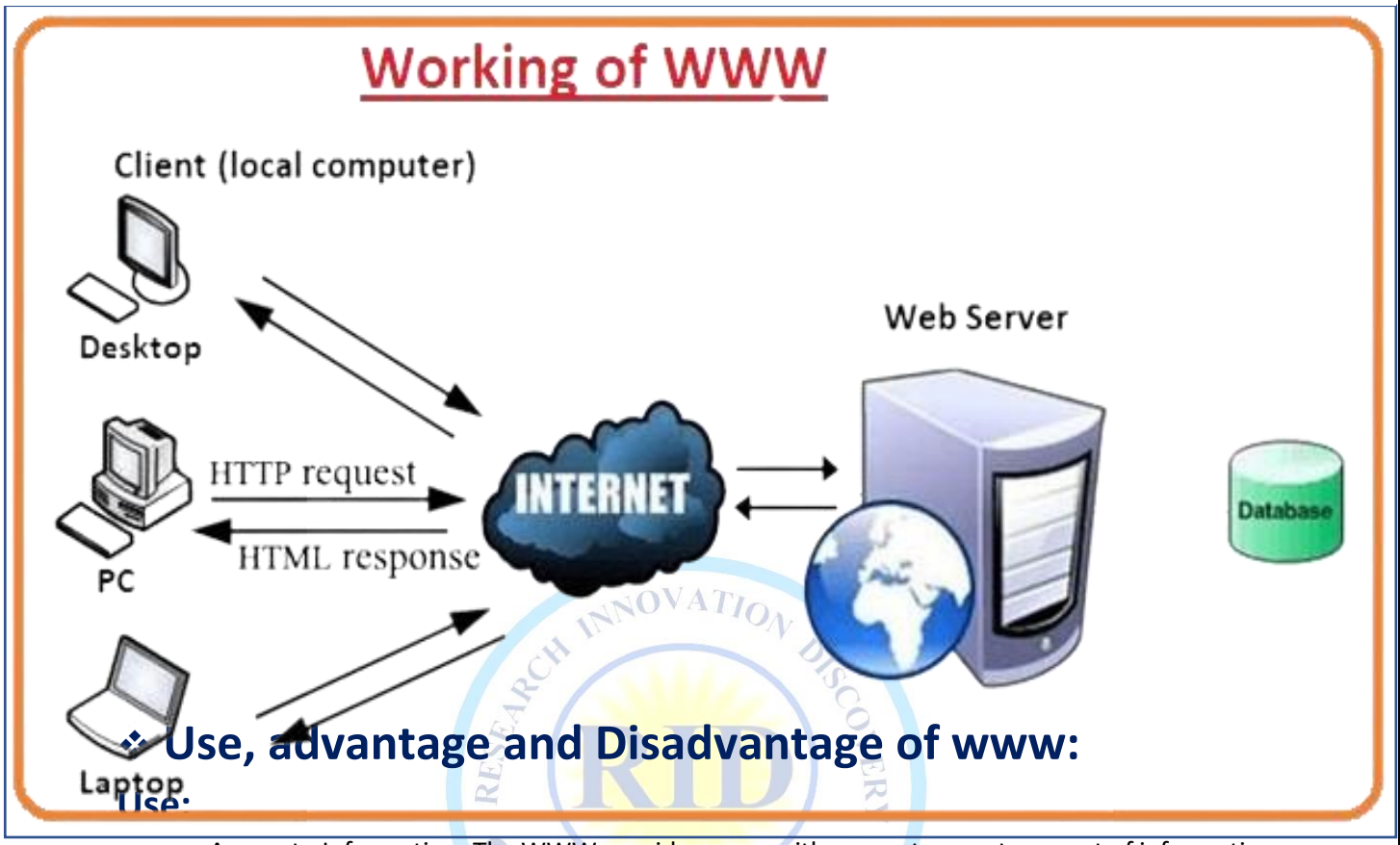
- When a user enters a URL into a web browser, the browser sends a Domain Name System (DNS) query to resolve the domain name to an IP address. DNS servers translate human-readable domain names into numerical IP addresses, allowing clients to locate servers on the internet.

5. Request-Response Cycle:

- Once the browser has resolved the domain name to an IP address, it sends an HTTP request to the server for the requested resource. The server processes the request and responds with the requested resource, typically in the form of an HTML document.

6. **HTML Rendering:**
   - The browser receives the HTML document from the server and parses it to render the web page in the browser window. The HTML document may include references to additional resources, such as images, stylesheets, and scripts, which the browser requests from the server using additional HTTP requests.
7. **Hyperlinks:**
   - Web pages often contain hyperlinks, which are clickable elements that allow users to navigate between pages and access related content. Hyperlinks specify the target URL of the linked resource, enabling users to explore the web by following links to other pages and websites.
8. **Cookies and Sessions:**
   - Web servers may use cookies to store information on the client's device, such as user preferences, session identifiers, and authentication tokens. Cookies enable personalized browsing experiences and help track user interactions across multiple pages and sessions.
9. **Security Measures:**
   - To ensure the security and privacy of web communications, HTTPS (HTTP Secure) encrypts data exchanged between clients and servers using SSL/TLS encryption protocols. HTTPS
   -
   - protects sensitive information, such as login credentials and financial transactions, from eavesdropping and tampering by unauthorized parties.





❖ Use, advantage and Disadvantage of www:

Use:

- Access to Information: The WWW provides users with access to a vast amount of information on virtually any topic, including news, research, educational resources, and entertainment.
- Communication: It enables communication and collaboration through email, messaging platforms, social media, and online forums, connecting individuals and organizations worldwide.
- E-commerce: The WWW facilitates online shopping and commerce, allowing businesses to sell products and services to customers globally through websites and e-commerce platforms.
- Entertainment: It offers a wide range of entertainment options, including streaming movies, music, videos, and online gaming.
- Education: Educational institutions use the WWW to deliver online courses, tutorials, and educational resources, making learning accessible and convenient.
- Social Interaction: Social media platforms and online communities provide opportunities for social interaction, networking, and sharing of ideas and experiences.
- Research and Innovation: Researchers and innovators use the WWW to collaborate, share findings, and access scientific literature, contributing to advancements in various fields.

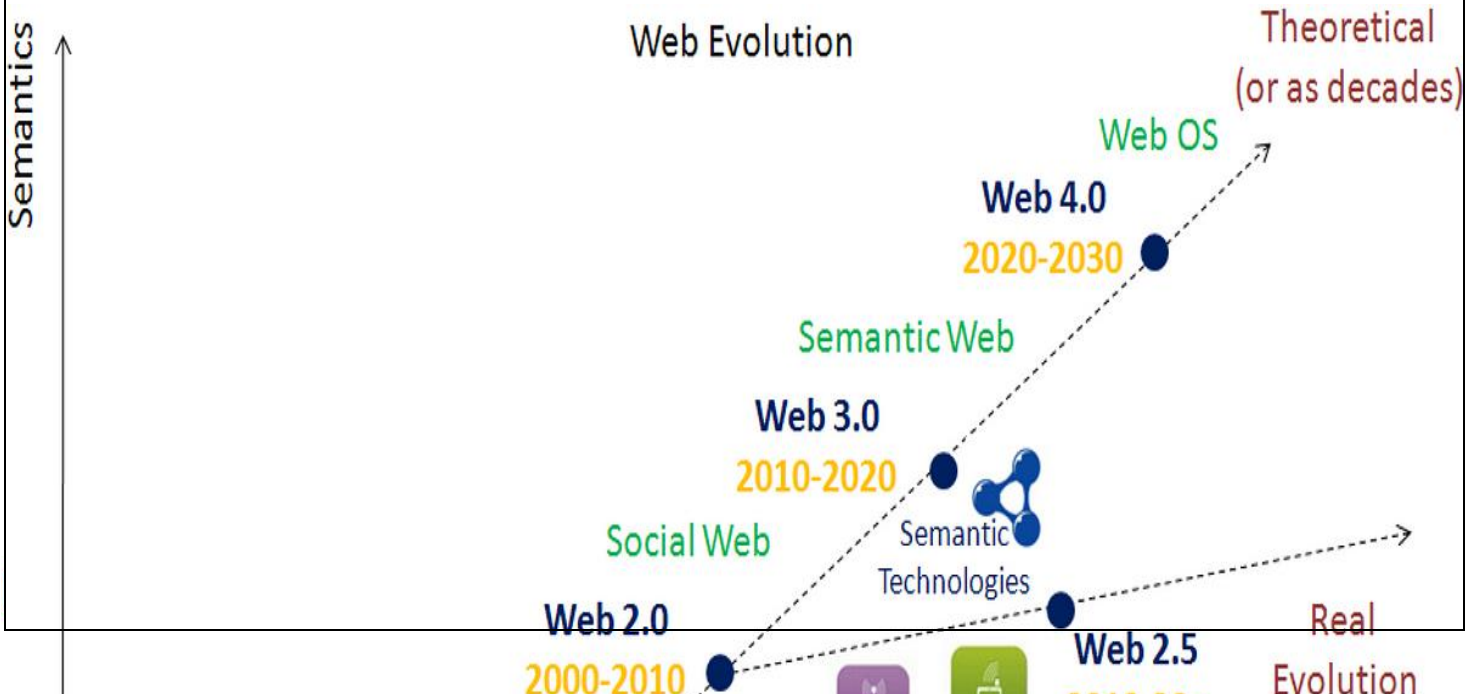
Advantages:

- Global Access: The WWW is accessible to anyone with an internet connection, enabling users to access information and services from anywhere in the world.
- Convenience: It offers convenient access to a wide range of resources and services, allowing users to perform tasks such as shopping, banking, and communication from the comfort of their homes.

- Information Sharing: The WWW facilitates the sharing and dissemination of information, knowledge, and ideas across geographical and cultural boundaries, fostering collaboration and innovation.
- Economic Opportunities: It creates economic opportunities through e-commerce, online advertising, digital marketing, and freelance work, contributing to economic growth and job creation.
- Education and Learning: The WWW provides access to educational resources and online courses, empowering individuals to acquire new skills, knowledge, and qualifications.
- Social Connectivity: Social media platforms and online communities enable individuals to connect with friends, family, and like-minded individuals, fostering social interaction and support networks.
- Innovation and Creativity: The WWW provides a platform for creativity, innovation, and expression, allowing individuals and businesses to showcase their talents, ideas, and products to a global audience.

Disadvantages:

- Information Overload: The abundance of information on the WWW can lead to information overload and difficulties in finding accurate, relevant, and trustworthy information.
- Privacy Concerns: The WWW raises concerns about privacy and data security, as personal information shared online can be vulnerable to surveillance, data breaches, and misuse by third parties.
- Cybersecurity Risks: It is susceptible to various cybersecurity threats, including malware, phishing scams, identity theft, and cyberattacks, posing risks to individuals and organizations.
- Digital Divide: Not everyone has equal access to the WWW due to factors such as geographical location, socioeconomic status, and technological infrastructure, exacerbating inequalities in information access and digital literacy.
- Online Addiction: Excessive use of the WWW, especially on social media and gaming platforms, can lead to addiction, compulsive behavior, and negative impacts on mental health and well-being.
- Misinformation and Fake News: The WWW facilitates the spread of misinformation, fake news, and propaganda, which can influence public opinion, undermine trust in institutions, and lead to societal divisions and conflicts.
- Dependency: Dependency on the WWW for essential tasks such as communication, information access, and commerce can lead to reliance issues and difficulties functioning without internet connectivity in case of outages or disruptions.



Definition: - A search engine is a software system designed to carry out web searches. Or it is set of Program.

use: - it is used to search www in a systematic way for particular information specified in a textı

History: - 10 sept 1990 is D.O.B of 1st Search Engine "Archie" by Alan Emtage (note: - note index Concept) 1st Popular Search Engine was Yahoo! (Founded by Yang and David Filo in 1994) Google Search Engine (Founded by Lary Page & Sergey Brin in 1998) used Page Rank Algorithm, Indexing & Hyperlinks

Example: - Google, Bing, Yahoo, Baidu, DuckDuckGo, Yandex, Ask.com, AOL Search, Ecosia, Qwant etc.

Types: - 1. Conventional 2. Text-Based 3. Voice-Based 4. Multimedia Search 5. Q/A 6. Clustering 7. Research System

Conventional (Library CatLog): - Search by keyword title, Author etc.

Text-based & Voice-based: - Google, Bing & Yahoo! Search by keyword

Multimedia Search: - (QBIC, Web seek, safe) Search by visual Appearance (Shapes, colours)

Q/A: - Stack Exchange, NSIR search in (Restricted) Natural Language.

Clustering: - Vivisimq, clustery **Research System: -** Lemur, Nutch

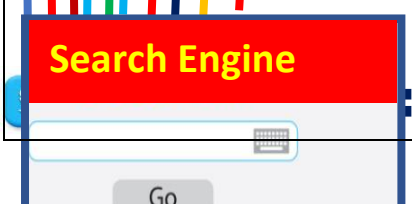
How Search Engine work

Crawling: - also known as Spider or Spider Bot it is internet bot that systematically browses the www and that is typically operated by search engine for the purpose of web indexing.

Indexing: - Collecting, Parsing and Storing of Data

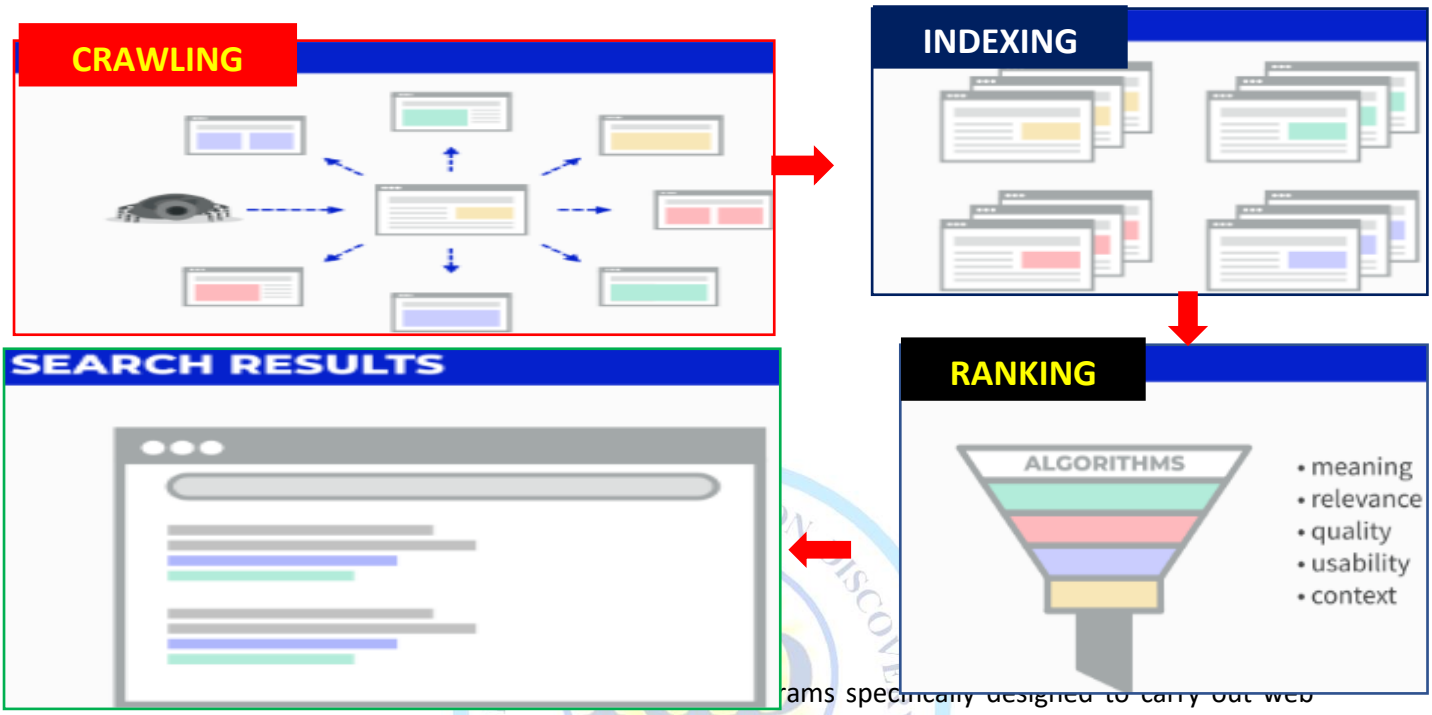
Ranking: - position a website or webpage holds within a specific search engine results page.

Search Results: - it is a query that a user enters into a "web search engine "to satisfy the information needs



TWKSAA

TWKSAA



rams specifically designed to carry out web searches efficiently. It systematically indexes information available on the **World Wide Web** and provides users with a way to search for specific content, websites, or information by entering keywords or phrases.

- The search engine then retrieves relevant results from its index and presents them to the user in a structured manner, usually in the form of a list of links, along with brief descriptions or snippets..

❖ Use of Search Engine:

- The primary use of a search engine is to systematically search the World Wide Web for specific information specified in a textual web search query. Users input keywords or phrases related to the information they are seeking, and the search engine scours its indexed database to retrieve relevant results..

• Search engines serve various purposes, including:

1. **Information Retrieval:** Users can quickly find information on a wide range of topics, from academic research to news articles, product reviews, and general knowledge.
2. **Navigation:** Search engines help users navigate the vast expanse of the internet by providing links to relevant websites and online resources.
3. **Problem Solving:** Users can use search engines to find solutions to specific problems or queries, such as troubleshooting issues, DIY projects, or technical support.
4. **Research:** Search engines are valuable tools for conducting research, allowing users to explore different perspectives, gather data, and access scholarly articles and academic resources.
5. **Shopping:** Many search engines offer specialized features for shopping, enabling users to compare prices, read reviews, and find products and services from various online retailers.

6. **Entertainment:** Users can use search engines to discover multimedia content, including videos, images, music, and games, for entertainment purposes.

❖ History of Search Engine:

➢ The history of search engines marks significant milestones in the development of information retrieval systems on the internet. Here's a brief overview:

- **Archie (1990):** Considered the first search engine, Archie was developed by Alan Emtage, a student at McGill University in Montreal, Canada. Archie was a simple tool designed to index and retrieve files from FTP (File Transfer Protocol) sites. It operated by creating a searchable index of directory listings from FTP servers.
- **Yahoo! (1994):** Founded by Jerry Yang and David Filo, Yahoo! began as a directory of websites organized into categories. It quickly became one of the most popular search engines of its time, providing users with a curated selection of websites and resources. While it started as a directory, Yahoo! later incorporated search functionality, making it one of the first comprehensive search engines on the web.
- **Google (1998):** Founded by Larry Page and Sergey Brin, Google revolutionized the search engine landscape with its innovative approach to indexing and ranking web pages. Google's PageRank algorithm, developed by Page and Brin while they were students at Stanford University, evaluated the importance of web pages based on the number and quality of links pointing to them. This algorithm, along with efficient indexing and analysis of hyperlinks, enabled Google to deliver more relevant search results compared to its predecessors.
- Google's clean interface, fast search speed, and accurate results quickly propelled it to dominance in the search engine market. Over the years, Google has continuously refined its search algorithms and introduced new features to improve the user experience, such as personalized search, knowledge graphs, and voice search.
- These **early search engines** laid the foundation for the sophisticated information retrieval systems we rely on today. From basic directory listings to complex algorithms analyzing billions of web pages, search engines have become indispensable tools for accessing information on the internet.

❖ Example: - Google, Bing, Yahoo, Baidu, DuckDuckGo, Yandex, Ask.com, AOL Search.

❖ Types of search engine:

1. Conventional Search Engines:

- **Example:** Google, Bing, Yahoo!
- **Description:** Conventional search engines crawl and index web pages across the internet, allowing users to search for information using keywords or phrases.

2. Text-Based Search Engines:

- **Example:** Google, Bing
- **Description:** Text-based search engines primarily focus on indexing and retrieving textual content from web pages. Users input text queries, and the search engine returns relevant text-based results.

3. Voice-Based Search Engines:

- **Example:** Google Voice Search, Apple Siri, Amazon Alexa

- **Description:** Voice-based search engines allow users to perform searches using voice commands instead of typing. These systems utilize natural language processing to interpret spoken queries and retrieve relevant information.

4. Multimedia Search Engines:

- **Example:** Google Images, YouTube, Flickr
- **Description:** Multimedia search engines specialize in indexing and retrieving multimedia content such as images, videos, and audio files. Users can search for specific multimedia content using keywords, tags, or visual recognition technology.

5. Question-Answering (Q/A) Search Engines:

- **Example:** Quora, Yahoo! Answers
- **Description:** Q/A search engines allow users to ask questions in natural language, and the system retrieves relevant answers from a database of user-generated content or curated knowledge sources.

6. Clustering Search Engines:

- **Example:** DuckDuckGo, Yippy
- **Description:** Clustering search engines organize search results into meaningful categories or clusters to help users navigate and refine their search queries more efficiently. These engines aim to provide a structured and organized presentation of search results.

7. Research Systems:

- **Example:** Google Scholar, PubMed
- **Description:** Research systems are specialized search engines designed for accessing academic and scholarly content. They index research papers, journals, conference proceedings, and other scholarly publications, providing researchers with access to authoritative and peer-reviewed information.

❖ How Search Engine Works:

1. Crawling:

- Crawling is the process by which search engines discover and retrieve web pages from World Wide Web. This is done by specialized programs called crawlers, spiders, bots.
- These bots systematically browse the internet, following links from one web page to another. They start from a list of known web pages (seed URLs) and continuously navigate through links, discovering new pages along the way.
- As the bots crawl the web, they gather information about each page they visit, including its URL, content, metadata, and links to other pages.

2. Indexing:

- ➢ Once a web page is crawled, the search engine indexes the information it collects. Indexing involves organizing and storing the data in a structured format that can be quickly retrieved when a user performs a search.
- ➢ The indexing process includes:
- **Collecting Data:** The search engine parses the content of the web page, extracting text, images, metadata, and other relevant information.

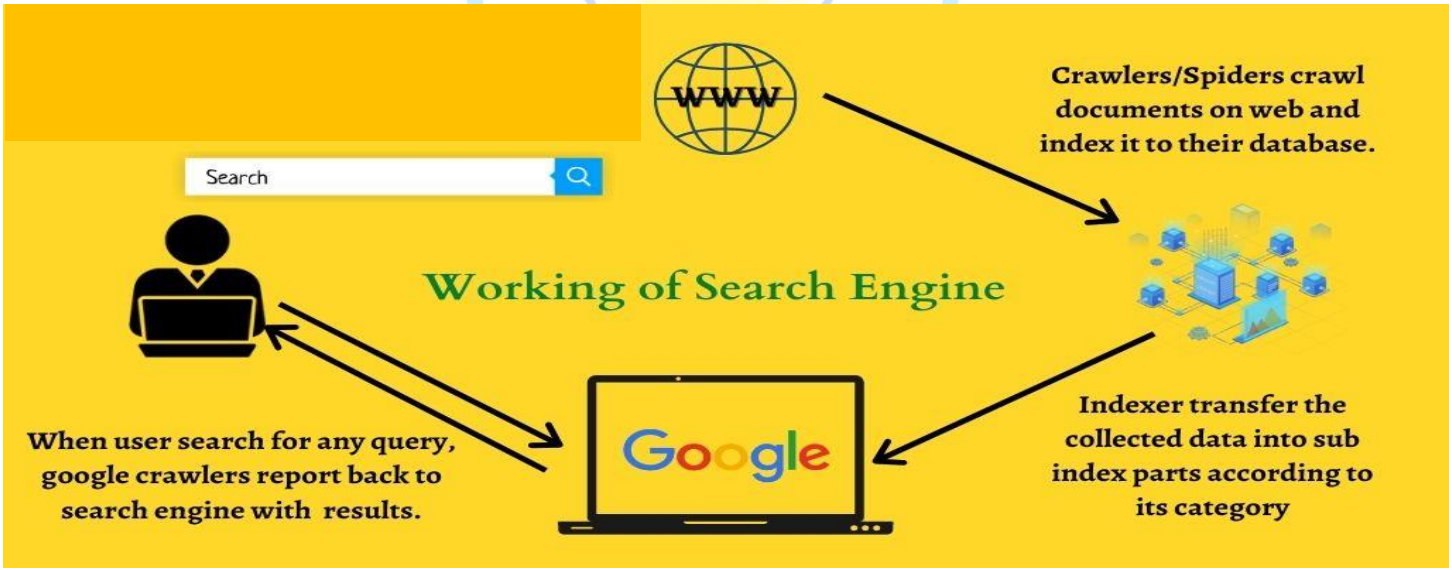
- **Parsing:** The data is then parsed and analyzed to identify keywords, phrases, and other elements that can be used to match search queries.
- **Storing Data:** The indexed data is stored in a massive database, often referred to as an index. This allows the search engine to quickly retrieve relevant information in response to user queries.

3. Ranking:

- When a user enters a search query, the search engine retrieves relevant pages from its index and ranks them based on their relevance to the query.
- The ranking algorithm evaluates various factors to determine the relevance and importance of each page. This may include factors such as keyword density, the quality and quantity of inbound links, user engagement metrics.
- One of the most well-known ranking algorithms is Google's PageRank, which analyzes the link structure of the web to determine the importance of web pages.

4. Search Results:

- Finally, the search engine presents the search results to the user in the form of a search engine results page (SERP). This page typically includes a list of web pages that are deemed relevant to the user's query.
- Each search result is accompanied by a title, URL, and brief snippet of the page's content. The search results are often ranked in order of relevance, with the most relevant pages appearing at the top of the list.
- Users can then click on a search result to visit the corresponding web page and find the information they are looking for.



❖ Advantage and Disadvantage of Search Engine:

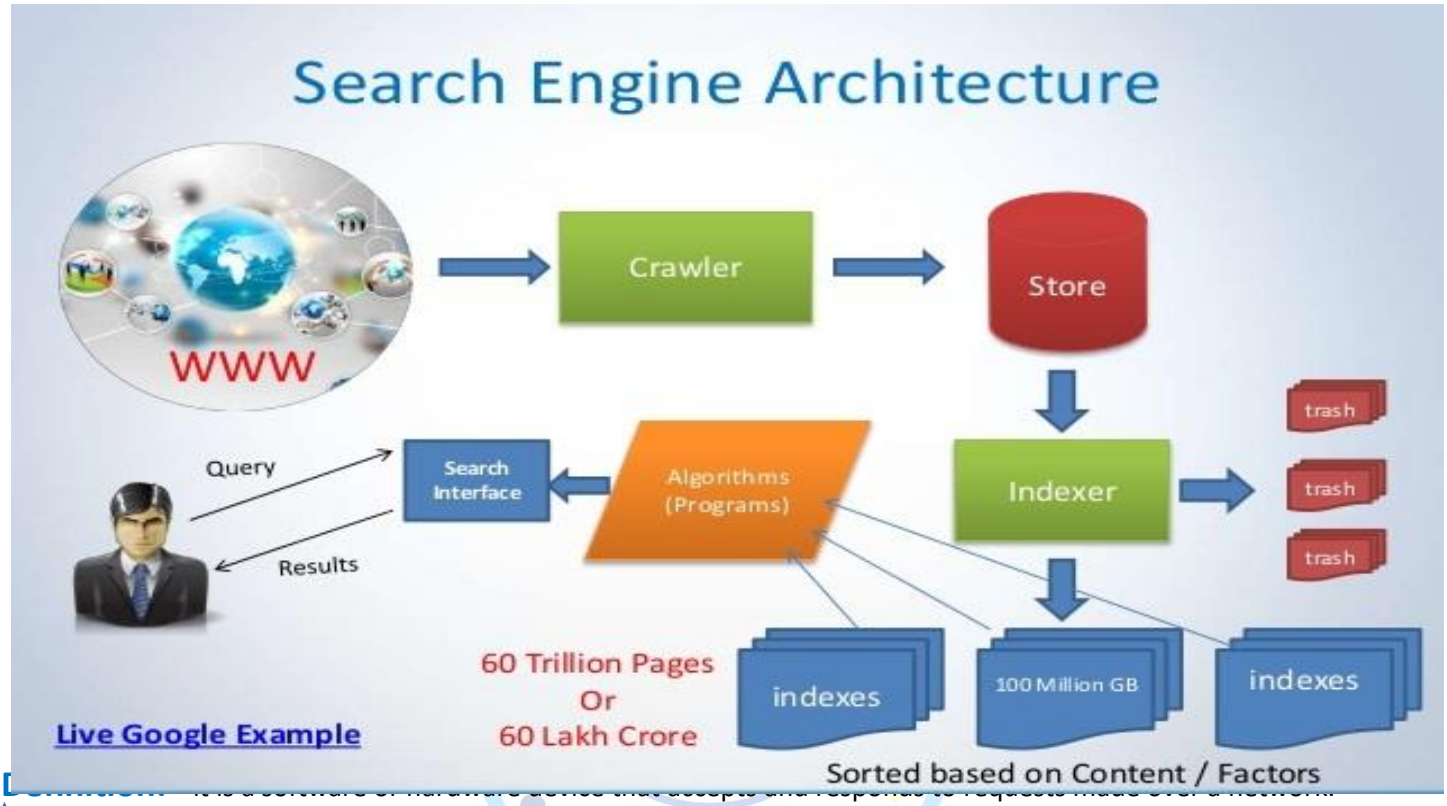
Advantages:

1. **Access to Vast Information:** Search engines provide access to a vast amount of information available on the World Wide Web. Users can easily find relevant content on a wide range of topics with just a few clicks.
2. **Convenience and Efficiency:** Search engines offer a convenient and efficient way to find information. Users can quickly search for specific topics, products, or services without having to browse through numerous websites manually.
3. **Timely and Up-to-Date Information:** Search engines continuously crawl and index new web pages, ensuring that users have access to the latest and most up-to-date information available on the internet.
4. **Customization and Personalization:** Many search engines offer customization features such as personalized search results, search history, and saved preferences, allowing users to tailor their search experience to their specific needs and preferences.
5. **Multi-Platform Accessibility:** Search engines are accessible across various devices and platforms, including desktop computers, laptops, smartphones, and tablets, making it easy for users to search for information anytime, anywhere.

Disadvantages:

1. **Information Overload:** The vast amount of information available on the internet can lead to information overload, making it challenging for users to sift through search results and find relevant content.
2. **Quality and Relevance of Results:** Search engine algorithms may not always prioritize quality and relevance, leading to irrelevant or low-quality search results. Users may need to refine their search queries or use advanced search techniques to find the information they need.
3. **Privacy Concerns:** Search engines collect and store user data, including search history, IP addresses, and other personal information, raising concerns about privacy and data security.

4. **Bias and Manipulation:** Search engine rankings may be influenced by various factors, including search engine optimization (SEO) techniques, advertising, and paid placements, leading to biased or manipulated search results.
5. **Dependency and Reliability:** Users may become overly reliant on search engines for accessing information, leading to a lack of critical thinking and research skills. Additionally, search engines may experience downtime or technical issues, impacting their reliability.



use: - it is used for store, send, & receive data. Responsible for Client/user, Http/Https Request & Response.

Types: - web server, application server, mail server, FTP server, real-time communication server, & virtual server.

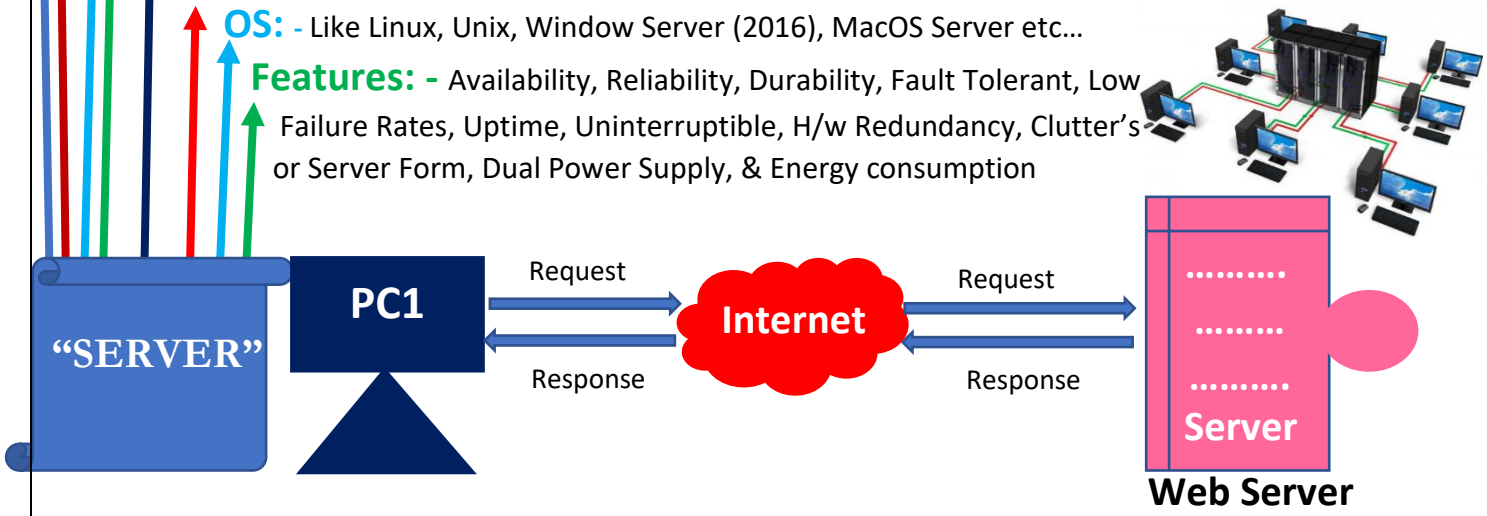
World 1st web server CERN httpd (later renamed to W3C httpd) was invented in 1989 by Tim Berners-Lee.

Parameter's: - Network, Internet, Data Centre, Host, Port, Protocol, Hardware, O.S, &Power.

Hardware: - RAID (Redundant array of independent) Disk, ECC (Error Correction Code) Memory,

OS: - Like Linux, Unix, Window Server (2016), MacOS Server etc…

Features: - Availability, Reliability, Durability, Fault Tolerant, Low Failure Rates, Uptime, Uninterruptible, H/w Redundancy, Clutter's or Server Form, Dual Power Supply, & Energy consumption



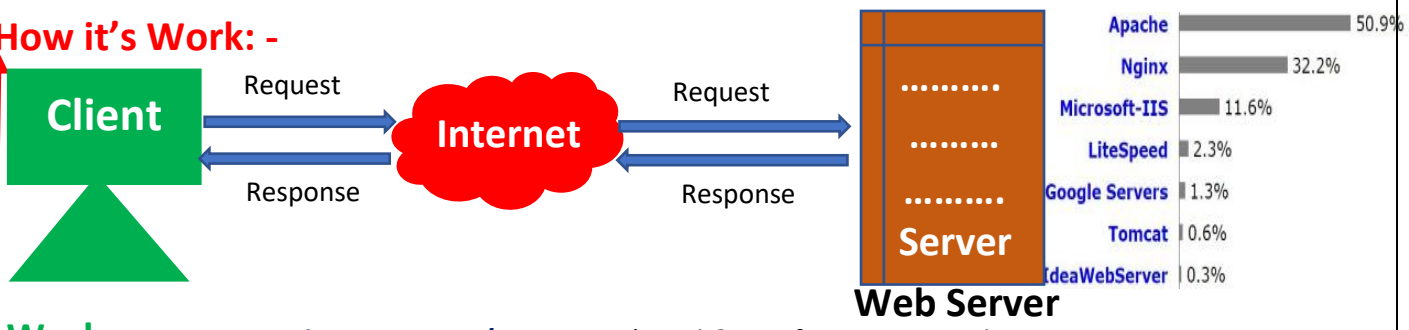
WEB SERVER

Definition: - web server is computer software and hardware that accepts requests via HTTPS (IP created to distribute web content). A web server is a dedicated computer responsible for running websites.

use: - it is used to process and manage HTTP/HTTPS requests and responses from the client system. A web server Store and protect website data.

Example: - Apache (Http server project), Microsoft IIS, Nginx, Apache Tomcat etc.

How it's Work: -



Work: - 1. Receive Client Request/Response (Read & Verify, URL-Normalization, URL Mapping, URL Path Redirections) **2. Executes or refuse HTTP Request Method** (URL Authorization, URL Redirection, Directory Index File Regular Files) **3. Response/Replies** (HTTP Response, Logs)

"WEB SERVER"

Features: - 1. Static Content serving 2. HTTP/HTTPS 3. Logging 4. Dynamic Content Serving 5. Virtual Hosting 6. Authorization 7. Content Cache 8. Large file Support 9. Bandwidth throttling 10. Rewrite Engine 11. Custom Error Page 12. Security

❖ Server:

- A server is a software or hardware device that accepts and responds to requests made over a network. It serves data, applications, or services to other devices, known as clients, within the network. Servers are designed to handle specific tasks or functions, such as hosting websites, storing and managing files, providing email services, or running applications.
- They operate continuously, ready to process incoming requests and deliver responses to clients efficiently and reliably. Servers can range from simple software programs running on standard computer hardware to complex, specialized hardware systems designed for high-performance computing and large-scale data processing.

❖ Use of Server:

1. **Data Storage:** Servers are used to store large amounts of data, including files, documents, multimedia content, and databases. They provide centralized storage that can be accessed and managed by multiple users or clients within a network.
2. **Data Transfer:** Servers facilitate the transfer of data between clients within a network or over the internet. They manage data transmission protocols and ensure reliable and efficient communication between clients.
3. **Email Services:** Email servers are responsible for sending, receiving, and storing email messages. They handle tasks such as message routing, storage, and retrieval, allowing users to send and receive emails seamlessly.

4. **Web Hosting:** Web servers host websites and web applications, making them accessible to users over the internet. They respond to HTTP and HTTPS requests from web browsers, serving web pages, multimedia content, and dynamic web applications.
5. **File Sharing:** File servers allow users to share and access files and documents within a network. They provide centralized storage for files, enabling users to collaborate on projects, share resources, and access files remotely.
6. **Application Hosting:** Application servers host and run software applications, providing access to application functionality and data over a network. They handle tasks such as application logic, data processing, and user authentication, allowing clients to access and interact with applications remotely.
7. **Database Management:** Database servers store and manage databases, allowing users to store, retrieve, and manipulate data efficiently. They handle tasks such as data storage, retrieval, indexing, and querying, enabling users to access and manage large volumes of data.
8. **Authentication and Authorization:** Authentication servers verify the identity of users and grant access to resources based on predefined permissions and privileges. They ensure secure access to network resources and protect sensitive data from unauthorized access.
9. **Backup and Recovery:** Backup servers are used to create and store backups of critical data and systems, ensuring data integrity and facilitating disaster recovery in case of data loss or system failure.
10. **Remote Access:** Servers can provide remote access services, allowing users to connect to a network or access resources from remote locations. Remote access servers facilitate secure and reliable connections, enabling users to work remotely and access network resources from anywhere in the world.

❖ Types of Servers:

1. Web Server:

- **Description:** Web servers are specialized servers that host websites and web applications. They handle HTTP and HTTPS requests from clients (web browsers) and serve web pages, multimedia content, and dynamic web applications.
- **Example:** Apache HTTP Server, Nginx, Microsoft Internet Information Services (IIS)

2. Application Server:

- **Description:** Application servers host and run software applications, providing access to application functionality and data over a network. They handle tasks such as application logic, data processing, and user authentication.
- **Example:** Java EE application servers (e.g., Apache Tomcat, JBoss), Microsoft .NET Framework

3. Mail Server:

- **Description:** Mail servers are responsible for sending, receiving, and storing email messages. They handle tasks such as message routing, storage, and retrieval, allowing users to send and receive emails seamlessly.
- **Example:** Postfix, Microsoft Exchange Server, Sendmail

4. FTP Server:

- **Description:** FTP (File Transfer Protocol) servers facilitate the transfer of files between clients and servers over a network. They provide a secure and efficient way to upload, download, and manage files.

- **Example:** vsftpd (Very Secure FTP Daemon), FileZilla Server, Microsoft FTP Server (IIS)

5. Real-Time Communication Server:

- **Description:** Real-time communication servers enable real-time communication and collaboration between users over a network. They support services such as instant messaging, video conferencing, voice calls, and presence detection.
- **Example:** XMPP (Extensible Messaging and Presence Protocol) servers, Microsoft Skype for Business Server, Zoom

6. Virtual Server:

- **Description:** Virtual servers are software-based servers that run multiple virtualized instances of operating systems and applications on a single physical server. They enable efficient resource utilization, scalability, and flexibility in deploying and managing server workloads.
- **Example:** VMware vSphere, Microsoft Hyper-V, KVM (Kernel-based Virtual Machine)

➢ These types of servers serve specific functions and play essential roles in various aspects of computing and networking.

Note:

- The world's first web server, called CERN httpd, was indeed developed by Tim Berners-Lee in 1989. This server software was created while Berners-Lee was working at CERN (European Organization for Nuclear Research) in Switzerland. Initially called "httpd" (Hypertext Transfer Protocol daemon), it was later renamed "W3C httpd" to reflect its association with the World Wide Web Consortium (W3C), which Berners-Lee founded to standardize and promote the web's development.

- CERN httpd was the first software to implement the HTTP protocol, which is the foundation of data communication on the World Wide Web. It served as both a web server and a web browser, allowing users to access and publish documents over the internet. This groundbreaking invention laid the foundation for the modern web and revolutionized the way information is shared and accessed worldwide.

❖ **Parameters of server**: - Network, Internet, Data Centre, Host, Port, Protocol, Hardware, O.S, &Power.

1. **Network:** The network parameter refers to the connectivity of the server within a network. It includes aspects such as the server's IP address, subnet mask, gateway, and DNS settings. Servers are typically connected to local area networks (LANs), wide area networks (WANs), or the internet.
2. **Internet:** This parameter relates to the server's connectivity to the internet. It includes considerations such as internet service provider (ISP), bandwidth, public IP address, and firewall settings to control inbound and outbound traffic.
3. **Data Centre:** Data centers house servers and other computing equipment in a controlled environment. Parameters related to data centers include physical security, temperature and humidity control, power redundancy, cooling systems, and fire suppression systems.
4. **Host:** The host parameter refers to the server's hostname or domain name. It is used to identify the server within a network or on the internet.
5. **Port:** Ports are numeric identifiers used by servers and applications to communicate over a network. Each service running on a server listens on a specific port number. Common port numbers include 80 for HTTP, 443 for HTTPS, 22 for SSH, and 25 for SMTP.

6. **Protocol:** Protocols define the rules and conventions for communication between devices on a network. Servers use various protocols to provide services and exchange data with clients. Examples include HTTP, HTTPS, FTP, SMTP, IMAP, POP3, and SSH.
7. **Hardware:** Hardware parameters include the physical components of the server, such as the CPU (central processing unit), RAM (random access memory), storage drives (HDD or SSD), network interface cards (NICs), and other peripherals. The server's hardware specifications determine its processing power, memory capacity, and storage capacity.
8. **Operating System (OS):** The operating system is the software that manages the server's resources and provides a platform for running applications and services. Common server operating systems include Linux distributions (e.g., Ubuntu Server, CentOS), Unix variants (e.g., FreeBSD), and Microsoft Windows Server.
9. **Power:** Power parameters relate to the server's power supply and consumption. This includes considerations such as redundant power supplies for fault tolerance, uninterruptible power supplies (UPS) for backup power in case of outages, power consumption metrics, and energy efficiency measures.

➢ These parameters collectively define the infrastructure, configuration, and operational aspects of servers, ensuring their functionality, performance, and reliability in providing services to clients and users.

❖ server operating systems including Linux, Unix, Windows Server (2016), and macOS Server:

1. Linux:

- **Description:** Linux is a Unix-like operating system kernel developed by Linus Torvalds in 1991. It is open-source and freely available, making it popular for server deployments due to its flexibility, stability, and security features.
- **Advantages:** Linux offers a wide range of distributions (distros) tailored for server use, such as Ubuntu Server, CentOS, Debian, and Red Hat Enterprise Linux (RHEL).
- **Use Cases:** Linux servers are widely used for web hosting, cloud computing, containerization (e.g., Docker, Kubernetes), virtualization (e.g., KVM, Xen), database servers (e.g., MySQL, PostgreSQL), and high-performance computing (HPC) clusters.

2. Unix:

- **Description:** Unix is a family of multitasking, multiuser computer operating systems originally developed in the 1970s at Bell Labs. While there are various Unix variants, they share common design principles and features, including a hierarchical file system, shell scripting, and support for networking protocols.
- **Advantages:** Unix operating systems offer stability, reliability, and robust networking capabilities, making them suitable for mission-critical server deployments. They provide built-in support for multiuser environments.

- **Use Cases:** Unix servers are commonly used in enterprise environments for hosting business-critical applications, database servers, file servers, and network infrastructure services.

3. Windows Server (2016):

- **Description:** Windows Server is a server operating system developed by Microsoft as part of the Windows NT family. Windows Server 2016 is one of the releases in the Windows Server line, offering features such as Active Directory, Group Policy, Remote Desktop Services, and Hyper-V virtualization.
- **Advantages:** Windows Server provides a familiar user interface and seamless integration with other Microsoft products and services. It offers robust support for enterprise workloads, including file sharing, print services, web hosting (IIS), database servers (SQL Server), and application virtualization (e.g., with Microsoft App-V).
- **Use Cases:** Windows Server is commonly used in environments that rely heavily on Microsoft technologies, such as businesses using Active Directory for user authentication and group management, SharePoint for collaboration, and Exchange Server for email services.

4. macOS Server:

- **Description:** macOS Server is an operating system developed by Apple Inc. based on the Unix-like macOS operating system. It provides server software and services that integrate seamlessly with Apple's ecosystem of devices and services.
- **Advantages:** macOS Server offers a user-friendly interface, intuitive management tools, and tight integration with other Apple products such as macOS, iOS, and iCloud. It provides services such as file sharing (AFP, SMB), time machine backups, macOS and iOS device management (with Profile Manager), and collaboration tools (Wiki, Calendar, Contacts).
- **Use Cases:** macOS Server is commonly used in small to medium-sized businesses, educational institutions, and creative industries that rely on Mac computers and iOS devices.

➢ These server operating systems offer distinct features, capabilities, and use cases, catering to different requirements and preferences in server deployments. Organizations choose the most suitable operating system based on factors such as performance, reliability, compatibility with existing infrastructure, and specific application or workload requirements.

❖ Features of server:

1. **Availability:** Servers are designed to be available and accessible to users or clients whenever they are needed. High availability ensures that services and applications hosted on the server are accessible with minimal downtime.
2. **Reliability:** Servers are expected to perform consistently and reliably under normal operating conditions. They should be able to handle workload demands without experiencing frequent failures or disruptions.
3. **Durability:** Servers are built to withstand continuous operation over extended periods without experiencing hardware failures or degradation in performance. They are designed with robust components and mechanisms to ensure long-term reliability.
4. **Fault Tolerance:** Servers incorporate fault-tolerant features and redundancy to mitigate the impact of hardware failures or errors. Redundant components such as power supplies, storage drives, and network interfaces ensure that critical functions can continue uninterrupted in the event of a failure.
5. **Low Failure Rates:** Servers are engineered to have low failure rates, meaning they are less likely to experience hardware or software failures compared to consumer-grade computers.

This reliability is achieved through rigorous testing, quality control measures, and the use of high-quality components.

6. **Uptime:** Uptime refers to the amount of time that a server is operational and available for use. Servers strive to achieve high uptime percentages, minimizing downtime and ensuring continuous access to services and applications.
7. **Uninterruptible:** Servers are equipped with features such as uninterruptible power supplies (UPS) and backup power sources to ensure continuous operation even in the event of power outages or disruptions.
8. **Hardware Redundancy:** Servers often incorporate hardware redundancy to increase reliability and fault tolerance. Redundant components such as power supplies, fans, and network interfaces ensure that critical functions can continue even if one component fails.
9. **Clustering or Server Farm:** Clustering or server farms involve deploying multiple servers together to work as a single system. This approach enhances performance, scalability, and fault tolerance by distributing workloads across multiple servers.
10. **Dual Power Supply:** Many servers feature dual power supplies for redundancy and fault tolerance. If one power supply fails, the other can continue to power the server, ensuring uninterrupted operation.
11. **Energy Consumption:** Servers are designed to be energy-efficient, minimizing power consumption while maximizing performance. Energy-efficient hardware components, power management features, and optimization techniques help reduce the environmental impact and operating costs associated with server operation.

❖ How a server works:

- server works by receiving requests from client devices, processing those requests, accessing resources as needed, generating responses, and sending them back to the clients. It operates continuously, handling multiple requests simultaneously and maintaining state information as required. Server administrators oversee the server's operation, ensuring optimal performance, reliability, and security.

1. Receiving Requests:

- server continuously listens for incoming requests from client devices, which could include requests for accessing web pages, files, databases, or other resources. These requests are typically transmitted over a network using communication protocols like HTTP, FTP, or TCP/IP.

2. Processing Requests:

- Upon receiving a request, the server's operating system (e.g., Linux, Windows Server) processes the request and determines the appropriate action to take.
- The server may need to access files, databases, or other resources to fulfill the request. It performs the necessary computations or operations to generate a response.

3. Accessing Resources:

- Depending on the nature of the request, the server may need to access various resources such as files stored on disk drives, databases containing data, or applications running on the server.
- The server retrieves the required resources from storage or memory and manipulates them as needed to generate the response.

4. Generating Responses:

- Once the server has processed the request and accessed the necessary resources, it generates a response to send back to the client. The response could include data, files, web pages, or other information requested by the client.

5. Sending Responses:

- After generating the response, the server sends it back to the client over the network.
- The response is transmitted using the appropriate communication protocol and may be encrypted for security purposes (e.g., HTTPS).

6. Handling Concurrent Requests:

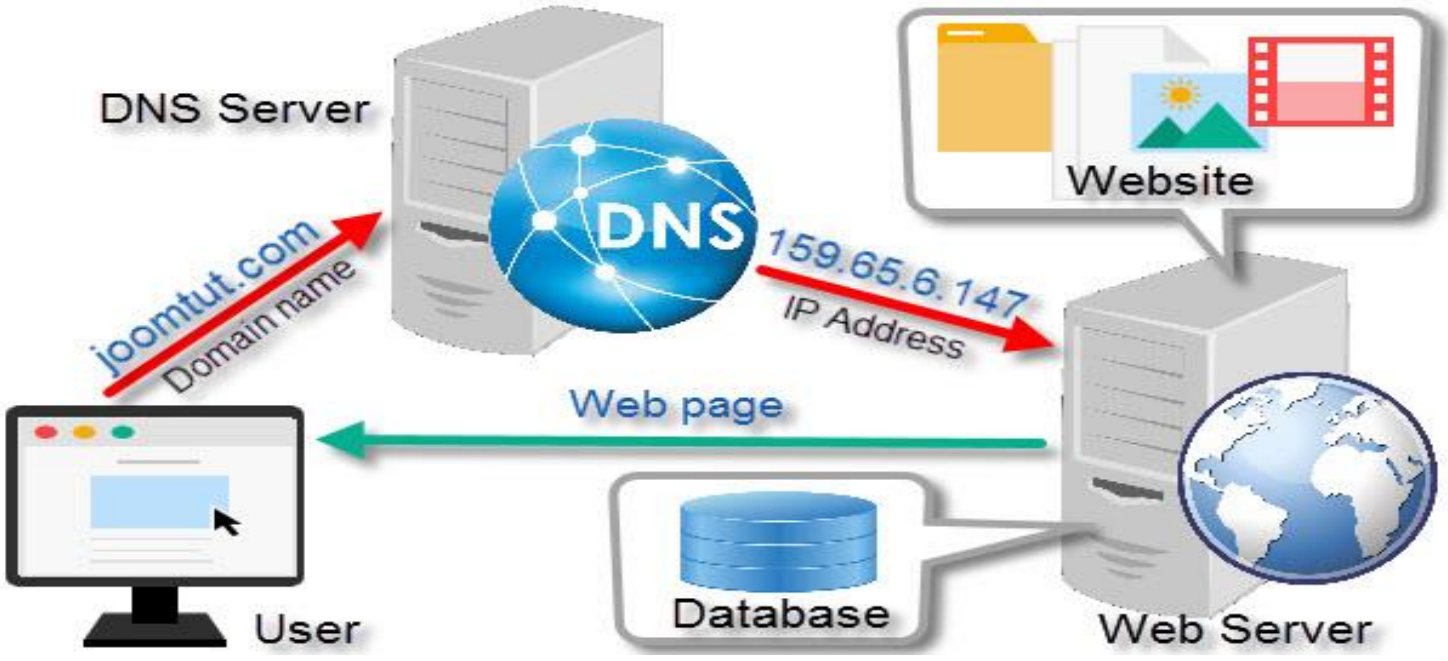
- Servers are designed to handle multiple requests simultaneously, often employing techniques such as multithreading or multiprocessing. This allows the server to serve multiple clients concurrently without sacrificing performance or responsiveness.

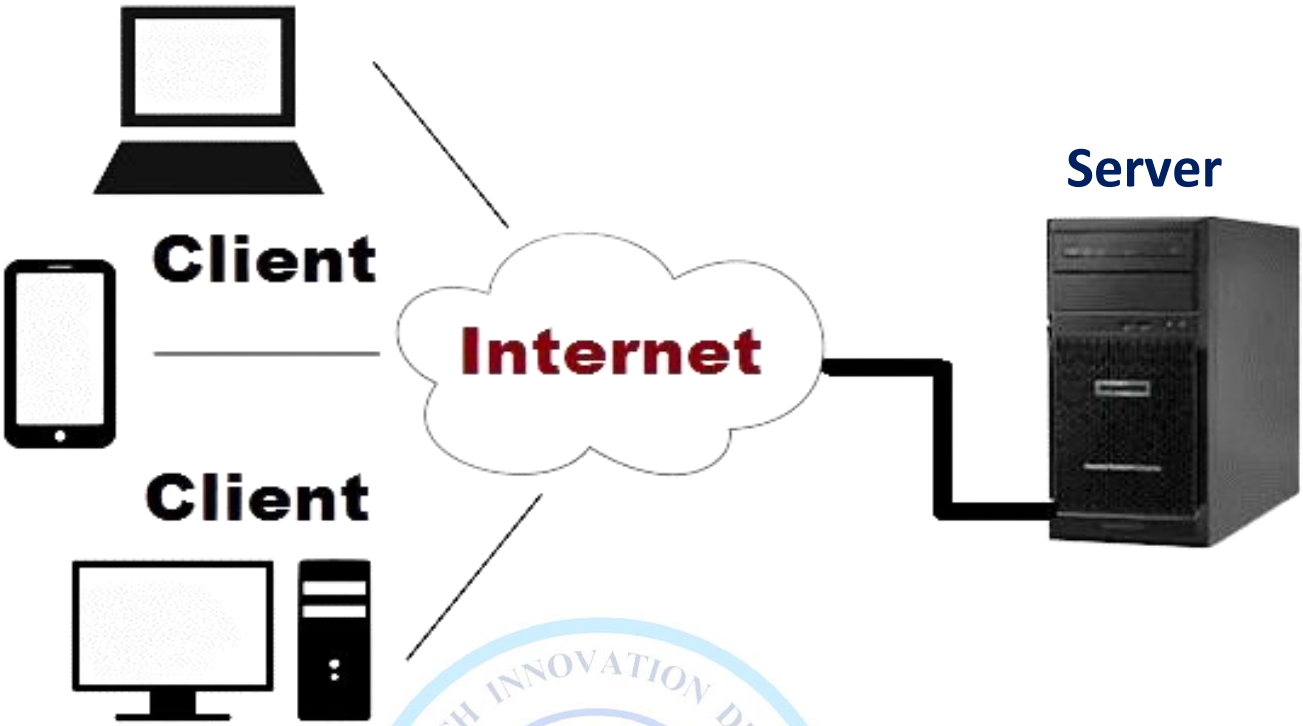
7. Maintaining State:

- In some cases, servers need to maintain state information between requests, especially in web applications or client-server interactions.
- Session management techniques such as cookies, session IDs, or server-side storage mechanisms are used to track user sessions and maintain continuity across multiple requests.

8. Monitoring and Management:

- Server administrators monitor the server's performance, resource usage, and health to ensure optimal operation. Monitoring tools and management software allow administrators to identify and address issues such as performance bottlenecks, security vulnerabilities, and hardware failures.





❖Advantages Disadvantages of server:

Advantages of Servers:

- ✓ **Centralized Data Storage:** Servers provide centralized storage for data, files, applications, and resources, making it easier to manage and access information across multiple users and devices within a network.
- ✓ **Resource Sharing:** Servers enable resource sharing among multiple users and devices, allowing them to access shared files, printers, databases, and other resources, which promotes collaboration and productivity.
- ✓ **Centralized Management:** Servers allow centralized management of network resources, user accounts, security policies, and configurations, simplifying administration and ensuring consistency across the network.
- ✓ **Scalability:** Servers are scalable, allowing organizations to add or upgrade hardware components, storage capacity, and processing power to accommodate growing demands, increased workloads, and expanding user bases.
- ✓ **Security Features:** Servers offer security features such as access controls, authentication mechanisms, encryption, firewalls, and intrusion detection systems (IDS), helping protect data, applications, and network infrastructure from unauthorized access, cyber threats, and data breaches.

Disadvantages of Servers:

- ✓ **Initial Cost:** Setting up and deploying servers can incur significant initial costs, including hardware, software licenses, networking equipment, and infrastructure upgrades, which may be prohibitive for small businesses or organizations with limited budgets.

- ✓ **Complexity:** Servers can be complex to set up, configure, and maintain, requiring expertise in server administration, networking, security, and software management, which may necessitate dedicated IT staff or external support services.
- ✓ **Single Point of Failure:** Servers can become single points of failure if they experience hardware failures, software crashes, or security breaches, potentially leading to downtime, service disruptions, and data loss, especially if redundancy and failover mechanisms are not in place.
- ✓ **Maintenance Overhead:** Servers require regular maintenance, updates, patches, and backups to ensure optimal performance, reliability, and security, which can incur additional costs, administrative overhead, and downtime for scheduled maintenance activities.
- ✓ **Security Risks:** Servers are susceptible to various security risks, including cyber attacks, malware infections, data breaches, and denial-of-service (DoS) attacks, which can compromise the confidentiality, integrity, and availability of data, applications, and network services.

Web Server

- A web server is computer software and hardware that accepts requests via the HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure) protocols and delivers web content to client devices, such as web browsers. It is a dedicated computer or server software responsible for hosting and serving websites on the World Wide Web.

❖ Use of Web Server:

1. Processing and Managing HTTP/HTTPS Requests:

- A web server is primarily used to process and manage HTTP and HTTPS requests from client systems, such as web browsers or other web-enabled applications.
- It receives incoming requests for web content, such as web pages, images, or files, and processes them according to the requested URL and parameters.

2. Storing Website Data:

- Web servers store and host website data, including HTML files, CSS stylesheets, JavaScript scripts, images, multimedia files, and other resources.
- This data is organized into directories and accessible to clients via URLs, allowing users to access and view web pages and content hosted on the server.

3. Protecting Website Data:

- Web servers play a crucial role in protecting website data from unauthorized access, data breaches, and cyber threats.

- They implement security measures such as encryption (HTTPS), access control mechanisms, firewalls, intrusion detection systems (IDS), and web application firewalls (WAFs) to safeguard sensitive information and ensure the integrity and confidentiality of website data.

4. Managing User Sessions and Authentication:

- Web servers often handle user authentication and session management for web applications and websites.
- They manage user login sessions, authenticate users based on credentials, and enforce access control policies to restrict access to protected areas of the website or application.

5. Logging and Monitoring:

- Web servers generate logs and maintain records of HTTP requests and responses for auditing, troubleshooting, and performance monitoring purposes.
- These logs provide valuable insights into website traffic, user behavior, errors, security incidents & server performance, helping administrators identify & address issues proactively.

6. Load Balancing and Scaling:

- Web servers can be configured for load balancing and scaling to distribute incoming traffic across multiple server instances or nodes. Load balancers distribute requests evenly to optimize performance and ensure high availability, while scaling mechanisms automatically add or remove server instances based on demand to handle fluctuations in traffic.

7. Content Delivery and Caching:

- Web servers support content delivery and caching mechanisms to improve website performance and reduce latency.
- They cache frequently accessed resources, such as static files and images, to serve them more quickly to users and reduce the load on backend servers.

❖ Example:

- Apache (Http server project), Microsoft IIS, Nginx, Apache Tomcat etc.

1. Apache HTTP Server (Apache):

- **Description:** Apache HTTP Server, commonly known as Apache, is one of the most widely used open-source web servers. It is known for its reliability, flexibility, and extensive feature set.
- **Use Cases:** Apache is used for hosting static and dynamic websites, serving web pages, handling HTTP requests, and supporting various programming languages and frameworks.

2. Microsoft Internet Information Services (IIS):

- **Description:** Microsoft Internet Information Services (IIS) is a web server software developed by Microsoft for the Windows operating system. It provides robust support for hosting and serving websites, web applications, and services on Windows servers.
- **Use Cases:** IIS is commonly used in Windows-based environments for hosting ASP.NET applications, serving web pages, supporting Windows-specific technologies, and integrating with other Microsoft products and services.

3. Nginx:

- **Description:** Nginx is a high-performance, lightweight web server and reverse proxy server known for its efficiency, scalability, and low resource usage. It is designed to handle high traffic loads and concurrent connections efficiently.
- **Use Cases:** Nginx is used for serving static and dynamic web content, load balancing, reverse proxying, caching, and supporting microservices architectures.

4. Apache Tomcat:

- **Description:** Apache Tomcat is an open-source Java Servlet Container and web server developed by the Apache Software Foundation. It implements the Java Servlet, JavaServer Pages (JSP), and WebSocket specifications, allowing developers to deploy Java web applications.
- **Use Cases:** Apache Tomcat is commonly used for hosting Java-based web applications, serving dynamic content, and supporting enterprise Java development.

5. Node.js (with Express.js):

- **Description:** Node.js is a server-side JavaScript runtime environment built on the V8 JavaScript engine. While not a traditional web server, Node.js can be used to create web servers using frameworks like Express.js.
- **Use Cases:** Node.js is used for building fast, scalable, and real-time web applications, APIs, and microservices using JavaScript on the server-side.

❖ How Web Server works:

1. Receiving Client Request/Response:

- **Read & Verify:** The web server reads the incoming HTTP request sent by the client, typically via a web browser. It verifies the integrity of the request and ensures that it conforms to the HTTP protocol standards.
- **URL Normalization:** If necessary, the server normalizes the requested URL to ensure consistency and compatibility across different platforms and configurations.
- **URL Mapping:** server maps the requested URL to a specific resource or file on the server's filesystem. This mapping determines which file or script will be served in response to request.
- **URL Path Redirections:** In some cases, the server may need to redirect the client to a different URL or location based on predefined rules or configurations.

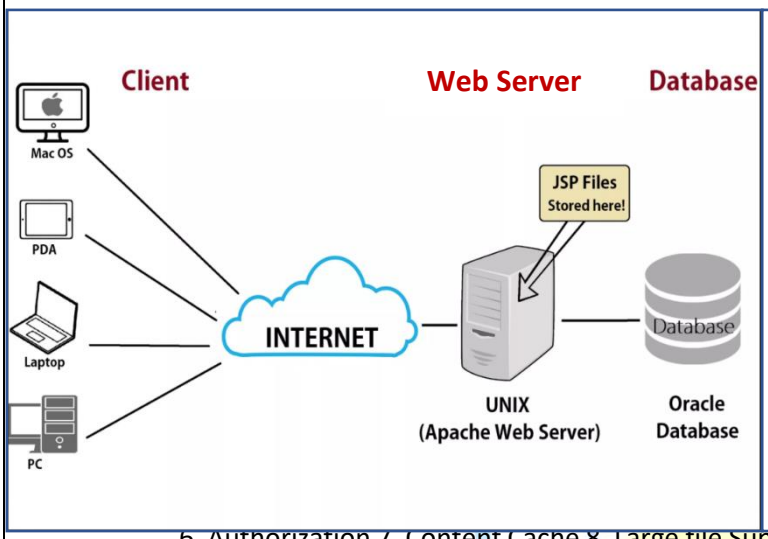
2. Executing or Refusing HTTP Request Method:

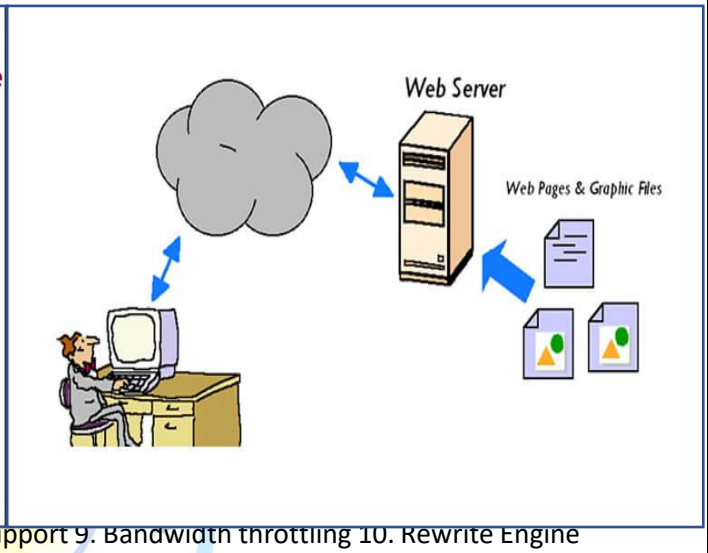
- **URL Authorization:** The server checks whether the client is authorized to access the requested URL or resource. This may involve authentication mechanisms such as basic authentication, digest authentication, or token-based authentication.
- **URL Redirection:** If the request method or URL needs to be redirected, the server sends an appropriate HTTP redirection response (e.g., 301 Moved Permanently, 302 Found, 307 Temporary Redirect).
- **Directory Index File:** If the requested URL corresponds to a directory on the server, the server may look for a default index file (e.g., index.html, index.php) to serve as the entry point for the directory.

- **Regular Files:** For requests targeting regular files (e.g., HTML files, images, CSS files), the server retrieves the requested file from the filesystem and prepares to send it as the response.

3. Response/Replies:

- **HTTP Response:** Based on the requested URL and method, the server generates an appropriate HTTP response to send back to the client. This response includes a status code indicating the outcome of the request (e.g., 200 OK, 404 Not Found, 500 Internal Server Error), response headers, and the requested content.
- **Logs:** The server logs details of the request, including the client's IP address, timestamp, requested URL, response status code, and other relevant information. These logs are useful for troubleshooting, performance monitoring, and security analysis.





6. Authorization 7. Content Cache 8. Large file Support 9. Bandwidth throttling 10. Rewrite Engine 11. Custom Error Page 12. Security

1. Static Content Serving:

- Web servers are capable of serving static content such as HTML files, images, CSS stylesheets, JavaScript files, and other static resources directly to clients without any processing.

2. HTTP/HTTPS:

- Web servers support the HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure) protocols for communication between clients and servers. HTTPS provides encrypted communication over SSL/TLS, ensuring secure data transmission.

3. Logging:

- Web servers generate logs that record details of HTTP requests and responses, including client IP addresses, requested URLs, response status codes, timestamps, and other relevant information. These logs are useful for monitoring, troubleshooting, and security analysis.

4. Dynamic Content Serving:

- Web servers can also serve dynamic content generated by server-side scripts or applications. This includes dynamically generated HTML pages, database-driven content, server-side scripting languages (PHP, Python, Ruby), and web application frameworks (Django, Flask, Ruby on Rails).

5. Virtual Hosting:

- Web servers support virtual hosting, allowing multiple websites to be hosted on the same physical server. Each website has its own domain name, configuration, and content directory, enabling efficient resource utilization and cost savings.

6. Authorization:

- Web servers provide authorization mechanisms to control access to web resources based on user permissions and authentication credentials. This includes user authentication methods such as basic authentication, digest authentication, and token-based authentication.

7. Content Cache:

- Web servers can cache frequently accessed content in memory or on disk to improve performance and reduce latency. Content caching reduces the need to regenerate or fetch content from backend servers, resulting in faster response times for clients.

8. Large File Support:

- Web servers are capable of serving large files, such as multimedia files, software downloads, and archives, efficiently and reliably. They optimize file transmission and delivery to ensure smooth and uninterrupted downloads for clients.

9. Bandwidth Throttling:

- Web servers can throttle or limit the amount of bandwidth allocated to individual clients or IP addresses to prevent network congestion, optimize resource usage, and ensure fair distribution of bandwidth among users.

10.Rewrite Engine:

- Web servers often include a rewrite engine that allows administrators to define and implement URL rewriting rules. This enables URL manipulation, redirection, and rewriting based on predefined patterns or conditions.

11.Custom Error Pages:

- Web servers support custom error pages that can be displayed to clients in case of HTTP errors (e.g., 404 Not Found, 500 Internal Server Error). Administrators can customize error pages to provide helpful information and guidance to users.

12.Security:

- Web servers implement security features and mechanisms to protect against various threats and vulnerabilities, including denial-of-service (DoS) attacks, cross-site scripting (XSS), SQL injection, and unauthorized access. This includes SSL/TLS encryption, access control, firewall integration, and security patches and updates.

❖Advantages Disadvantages of web server:

Advantages of Web Servers:

- ✓ **Content Delivery:** Web servers efficiently deliver web content, including web pages, images, videos, and files, to clients (such as web browsers or other client applications) over the internet.
- ✓ **Platform Independence:** Web servers can run on various operating systems, including Windows, Linux, Unix, and macOS, providing flexibility and compatibility with different environments.
- ✓ **Scalability:** Web servers are scalable, allowing organizations to handle increasing traffic and accommodate growing demands by adding more server resources or implementing load balancing techniques.
- ✓ **Security Features:** Web servers offer security features such as SSL/TLS encryption, access control mechanisms, and security patches to protect against cyber threats, data breaches, and unauthorized access.

- ✓ **Application Support:** Web servers support various programming languages, frameworks, and technologies, enabling the hosting of dynamic web applications, APIs, and services.

Disadvantages of Web Servers:

- ✓ **Complexity:** Setting up and configuring a web server can be complex, requiring expertise in server administration, networking, security, and software configuration.
- ✓ **Resource Consumption:** Web servers consume system resources such as CPU, memory, and disk space, especially when handling large volumes of traffic or resource-intensive applications.
- ✓ **Maintenance Overhead:** Web servers require regular maintenance, updates, and security patches to ensure optimal performance, stability, and security, which can incur additional costs and administrative overhead.
- ✓ **Single Point of Failure:** A web server can become a single point of failure if it experiences hardware failures, software crashes, or security breaches, potentially leading to downtime and service disruptions.
- ✓ **Security Risks:** Web servers are vulnerable to various security risks, including cyber attacks, malware infections, data breaches, and denial-of-service (DoS) attacks, which can compromise the confidentiality, integrity, and availability of web services.

HTTP/HTTPS

Hypertext Transfer Protocol Secure

HTTPS: -. HTTP is a client-server Protocol. it is State less but not session less.

Use: - information of particular website is exchanged between web server & web Browser.

Components: -

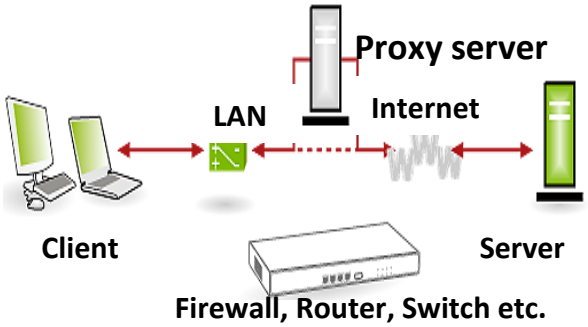
Client: - user agent is any tool that acts a behalf of the user Browser is always entity initiating request.

Proxy: - Between web Browser and the server numbers computers and machines relay the HTTP Message those operating at the application are called Proxies.

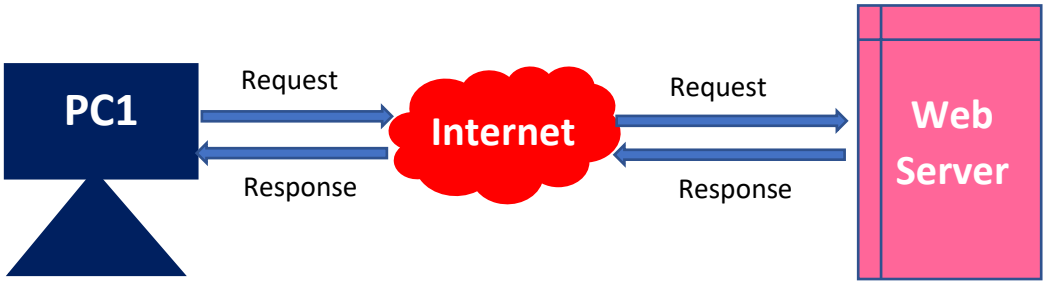
Example: -Firewall, Gateway, Router, Switch etc.

-Proxies perform following functions: -

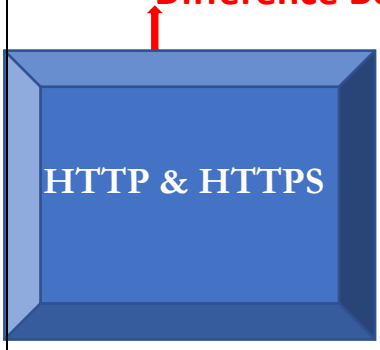
1.caching: - like the history and Browser cache
2.Filtering: - like an antivirus scan
3. Load Balance: - to allow multiple servers to sever Load.
4.Authentication: - to control access to different resource.
5.Logging: - allowing the storage of historical information



Server: - it is a software or h/w device that accepts and responds to requests made over a network.



Difference Between HTTP AND HTTPS :-



Http: -

-http URL begins with htttp://
-http Works at application level
-http is not encrypted (because send in plain text)
-http not required any certification
-Http use port no 80

Https: -

-https URL begins with htttps://
-https Works at Transport level
-https is encrypted
-http required SSL certification
-Http use port no 443

❖ HTTP (Hypertext Transfer Protocol):

- HTTP (Hypertext Transfer Protocol) is indeed a client-server protocol commonly used for communication between web browsers (clients) and web servers. Here's an explanation of the characteristics you mentioned:
- **Stateless:** HTTP is stateless, which means that each request from the client to the server is independent and not dependent on previous requests. The server does not maintain any information about past interactions with the client between requests. This simplicity makes HTTP lightweight and scalable but also poses challenges for maintaining session-related information.
- **Not Sessionless:** While HTTP is stateless, it is not inherently sessionless. Sessions can be established and maintained using various mechanisms, such as cookies, session IDs, or tokens. These mechanisms allow web applications to maintain stateful interactions with clients across multiple HTTP requests.
- HTTPS builds on top of HTTP by adding encryption via SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols to secure the communication between the client and the server. This encryption ensures that data transmitted over the network is protected from eavesdropping and tampering, enhancing the security and privacy of web communications.

❖Use of http and https:

- Both HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure) are protocols used for exchanging information between web servers and web browsers.

1. HTTP (Hypertext Transfer Protocol):

- HTTP is the foundation of data communication on the World Wide Web. It is used for transmitting web pages, images, text, multimedia, and other resources from web servers to web browsers.
- When you type a website's URL into your browser's address bar and hit enter, your browser sends an HTTP request to the corresponding web server.
- The web server processes the request and sends back an HTTP response containing the requested web page or resource.
- HTTP operates over TCP/IP (Transmission Control Protocol/Internet Protocol) and is typically transmitted over port 80.

2. HTTPS (HTTP Secure):

- HTTPS is a secure version of HTTP that encrypts the data transmitted between the web server and the web browser using SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols.
- HTTPS provides encryption and authentication mechanisms that protect the confidentiality, integrity, and authenticity of data transmitted over the internet.
- It is commonly used for transmitting sensitive information such as login credentials, personal data, financial transactions, and confidential communications
- To establish an HTTPS connection, the web server presents a digital certificate issued by a trusted Certificate Authority (CA) to the web browser, verifying the server's identity.
- HTTPS operates over the same underlying protocols as HTTP but uses port 443 for secure communication.

❖ How HTTP and HTTPS Works:

➢ HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) are protocols used for communication between web browsers and web servers. While both protocols facilitate the transfer of data over the internet, HTTPS adds an additional layer of security through encryption. Let's explore how each protocol works in detail:

1. How HTTP Works:

- Client-Server Communication: When you type a URL (Uniform Resource Locator) into your web browser and press enter browser initiates HTTP request to the corresponding web server.

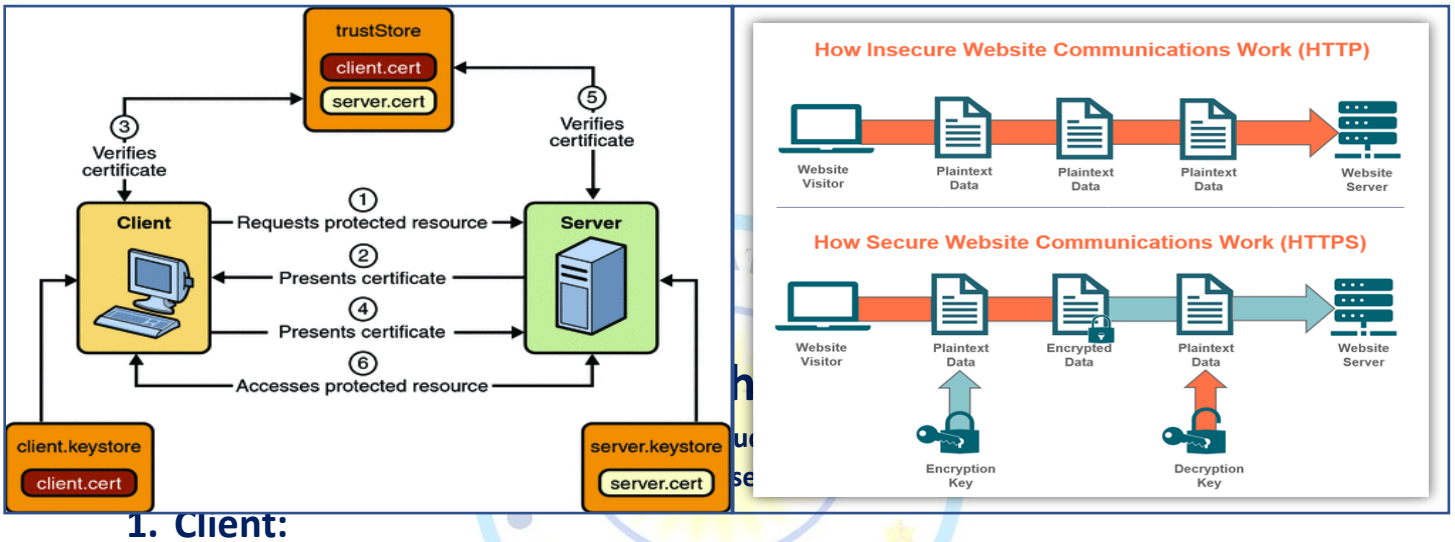
1. **Request-Response Cycle:** The HTTP request typically consists of a method (such as GET, POST, PUT, DELETE), a path (the URL), headers (additional information about the request), and sometimes a body (data to be sent to the server). The server processes the request and generates an HTTP response, which includes a status code indicating the outcome of the request (e.g., 200 OK for success, 404 Not Found for resource not found).
2. **Stateless Protocol:** HTTP is a stateless protocol, meaning that each request-response cycle is independent of previous interactions. This means that the server does not maintain any information about past requests from the same client.

2. How HTTPS Works:

➢ HTTPS builds upon the foundation of HTTP but adds encryption to ensure secure communication between the client and server. Here's how HTTPS works:

1. **Secure Handshake:** When a client initiates an HTTPS connection to a server, it begins with a secure handshake process. During the handshake, the client and server exchange cryptographic keys and negotiate encryption algorithms to establish a secure connection.

2. **Encryption:** Once the secure connection is established, all data transmitted between the client and server is encrypted using symmetric encryption. This means that the data is scrambled using a shared secret key that is known only to the client and server, making it unreadable to anyone intercepting the communication.
3. **Digital Certificates:** HTTPS relies on digital certificates issued by trusted third-party Certificate Authorities (CAs) to verify the identity of the server. These certificates contain information about the website owner and are used to authenticate server's identity to client.
4. **HTTPS URLs:** URLs using HTTPS are similar to those using HTTP but start with "https://" instead of "http://". This indicates that the connection is encrypted and secure.
5. **Data Integrity:** In addition to encryption, HTTPS ensures data integrity by using cryptographic hash functions to verify that the data has not been tampered with during transmission.



1. Client:

- The client refers to the web browser or client application that initiates the HTTPS connection to access a website or web service.
- The client sends HTTPS requests to the server to retrieve web pages, resources, or perform other actions.
- Examples of clients include web browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge, as well as mobile apps and other client-side applications.

2. Proxy:

- A proxy is an intermediary server that sits between the client and the server, forwarding requests and responses between them.
- Proxies can perform various functions to enhance security, performance, and control access to resources. Some of the common functions performed by proxies include:
- **Caching:** Proxies can cache frequently accessed web content locally, reducing latency and bandwidth usage by serving cached content to clients instead of fetching it from the original server. This helps improve performance and reduce network traffic.
- **Filtering:** Proxies can act as content filters, inspecting and analyzing web traffic to block or allow specific content based on predefined rules or policies. For example, proxies can block malicious websites, advertisements, or inappropriate content, enhancing security and compliance.
- **Load Balancing:** Proxies can distribute incoming traffic across multiple backend servers to improve performance, scalability, and fault tolerance. Load balancing proxies monitor server

health and availability, directing requests to the most suitable server based on factors such as server load, response time, and geographic proximity.

- **Authentication:** Proxies can enforce authentication mechanisms to control access to web resources based on user credentials, IP addresses, or other factors. Authentication proxies authenticate users before allowing them to access protected resources, ensuring only authorized users can access sensitive data or services.
- **Logging:** Proxies can log details of incoming and outgoing web traffic, including HTTP requests, responses, client IP addresses, URLs, and other metadata. Logging proxies provide visibility into web usage patterns, security incidents, and performance metrics, facilitating monitoring, auditing, and troubleshooting.

3. Server:

- The server refers to the web server that hosts the website or web service requested by the client.
- The server receives HTTPS requests from clients, processes them, and sends back HTTPS responses containing the requested content.
- Examples of servers include web servers such as Apache HTTP Server, Nginx, Microsoft IIS, and application servers hosting web applications, APIs, or services.

4. SSL/TLS Protocols:

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that provide encryption and authentication for secure communication over the internet.
- TLS is the successor to SSL and is widely used in HTTPS implementations. These protocols establish a secure connection between the client (web browser) and the server, ensuring that data exchanged between them is encrypted and protected from eavesdropping and tampering.

5. Digital Certificates:

- Digital certificates are cryptographic documents that verify the authenticity and identity of a website or web server.
- When a web browser connects to a website using HTTPS, the server presents its digital certificate to the browser as proof of its identity.
- Digital certificates are issued by Certificate Authorities (CAs) and contain information such as the website's domain name, public key, validity period, and the CA's digital signature.

6. Public Key Infrastructure (PKI):

- Public Key Infrastructure is a system of hardware, software, policies, and procedures used to manage digital certificates and cryptographic keys.
- PKI enables the secure exchange of digital certificates, facilitates the verification of digital signatures, and ensures the integrity and authenticity of digital transactions.
- Certificate Authorities (CAs) play a central role in PKI by issuing, revoking, and managing digital certificates for websites and web servers.

7. Encryption Algorithms:

- Encryption algorithms are mathematical algorithms used to encrypt and decrypt data transmitted over the internet.
- In HTTPS, symmetric and asymmetric encryption algorithms are used to secure data transmission between the client and the server.

- Symmetric encryption algorithms, such as AES (Advanced Encryption Standard), are used to encrypt and decrypt data efficiently.
- Asymmetric encryption algorithms, such as RSA (Rivest-Shamir-Adleman), are used for key exchange and digital signatures.

8. Secure Handshake Protocol:

- The Secure Handshake Protocol is a process used to establish a secure connection between the client and the server before any data is transmitted.
- During the handshake process, the client and the server exchange cryptographic parameters, negotiate encryption algorithms, and verify each other's digital certificates.
- The handshake protocol ensures that both parties agree on the encryption keys and security parameters used for communication, establishing a secure and authenticated connection.

❖Difference between http and https:

1. Security:

- **HTTP:** HTTP is not secure by default. Data transmitted over HTTP is sent in plain text, making it vulnerable to interception, eavesdropping, and tampering. This lack of encryption means that sensitive information such as login credentials, personal data, and financial transactions can be intercepted and viewed by malicious actors.
- **HTTPS:** HTTPS adds a layer of security to HTTP by encrypting the data transmitted between the client and the server using SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols. This encryption ensures that data exchanged over HTTPS is encrypted and protected from eavesdropping and tampering, enhancing the security and privacy of web communications.

2. Protocol:

- **HTTP:** HTTP is a standard protocol used for transmitting hypertext documents, images, videos, and other web content between clients (web browsers) and servers.
- **HTTPS:** HTTPS is a secure version of HTTP that uses SSL/TLS encryption to secure communication between clients and servers. It operates over the same underlying protocol as HTTP but adds encryption to protect data transmission.

3. Port:

- **HTTP:** HTTP typically operates over port 80 by default. When you access a website using HTTP, your web browser sends requests to the server's port 80.
- **HTTPS:** HTTPS operates over port 443 by default. When you access a website using HTTPS, your web browser sends requests to the server's port 443, which is dedicated to secure communication.

4. URL Syntax:

- HTTP: URLs for HTTP websites begin with "http://" followed by the domain name or IP address of the website (e.g., http://www.example.com).
- HTTPS: URLs for HTTPS websites begin with "https://" followed by the domain name or IP address of the website (e.g., https://www.example.com). The "s" in "https" indicates that the connection is secure and encrypted.

5. Certificate Requirement:

- **HTTP:** HTTP does not require digital certificates for communication between clients and servers.

- **HTTPS:** HTTPS requires digital certificates to establish secure connections between clients and servers. Digital certificates are issued by trusted Certificate Authorities (CAs) and contain information about the website's identity, encryption keys, and validity period.

❖ Advantage and disadvantage and use of http and https:

• HTTP (Hypertext Transfer Protocol):

Advantages:

- ✓ Simplicity: HTTP is easy to implement and understand, making it suitable for basic web browsing and communication.
- ✓ Fast Performance: HTTP tends to have faster performance compared to HTTPS due to the lack of encryption overhead.
- ✓ Compatibility: HTTP is widely supported by web browsers, servers, and web applications.

Disadvantages:

- ✓ Lack of Security: HTTP transmits data in plain text, making it vulnerable to interception, eavesdropping, and tampering.
- ✓ Privacy Concerns: HTTP does not provide privacy protections for sensitive data transmitted over the internet.
- ✓ Limited for Secure Transactions: HTTP is not suitable for transmitting sensitive information such as login credentials, personal data, and financial transactions.

Uses:

- ✓ Basic Web Browsing: HTTP is commonly used for accessing websites, retrieving web pages, and transmitting non-sensitive information over the internet.
- ✓ Unencrypted Communication: HTTP is used for communication where security and privacy are not critical considerations, such as accessing public information or non-sensitive resources.

❖ HTTPS (HTTP Secure):

Advantages:

- ✓ Enhanced Security: HTTPS encrypts data transmitted between the client and server, providing protection against interception, eavesdropping, and tampering.
- ✓ Privacy Protection: HTTPS ensures the privacy of sensitive information by encrypting it during transmission, reducing the risk of data breaches and unauthorized access.
- ✓ Trust and Authentication: HTTPS uses digital certificates to authenticate websites and verify their identity, establishing trust between clients and servers.

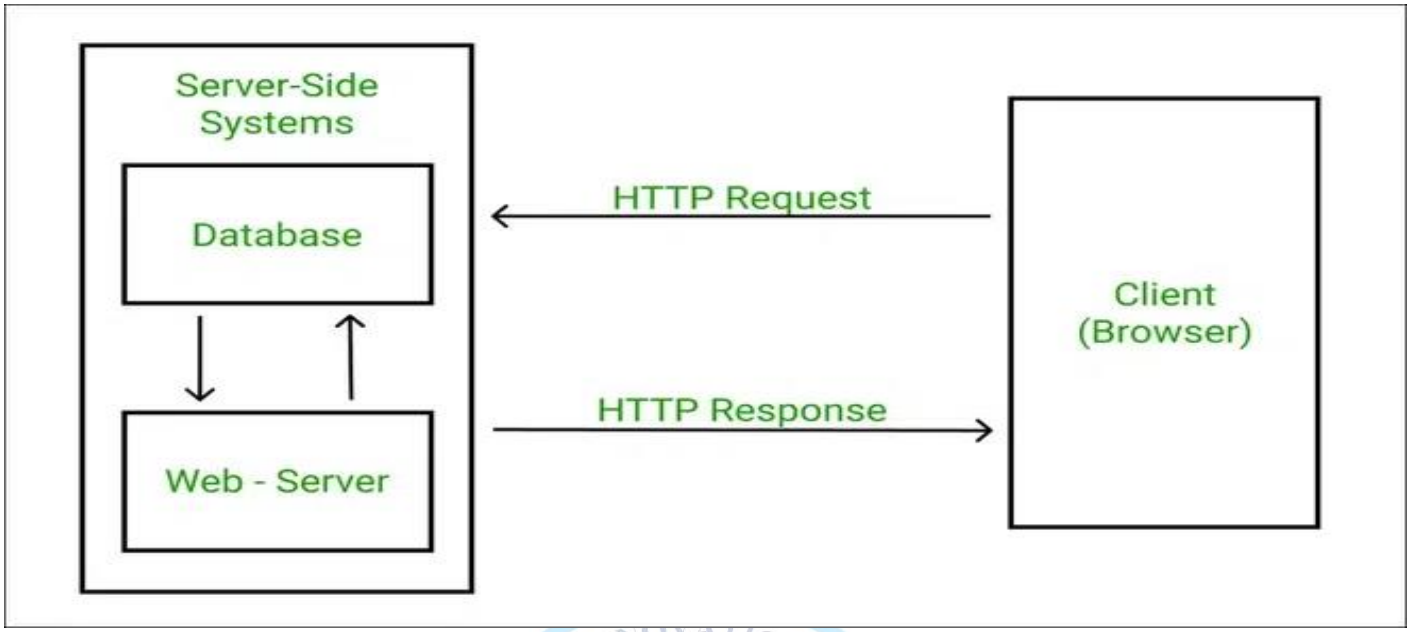
Disadvantages:

- ✓ Overhead: HTTPS encryption introduces additional computational overhead and latency compared to HTTP, potentially impacting performance.
- ✓ Implementation Complexity: Setting up and maintaining HTTPS requires additional configuration, digital certificates, and server resources.
- ✓ Compatibility Issues: Some older web browsers, devices, and systems may not fully support HTTPS, leading to compatibility issues for certain users.

Uses:

- ✓ Secure Transactions: HTTPS is used for transmitting sensitive information such as login credentials, personal data, financial transactions, and confidential communications securely over the internet.
- ✓ E-commerce: HTTPS is essential for online shopping, e-commerce websites, and payment gateways to ensure secure transactions and protect customer data.

- ✓ Secure Communication: HTTPS is used for secure communication between clients and servers in various industries, including banking, healthcare, government, and e-government services.



COMPUTER MALWARE

- Computer malware, often simply referred to as "malware," is a type of malicious software designed to infiltrate and damage computer, server, client, or computer network. It includes a wide range of malicious programs such as viruses, worms, Trojans, ransomware, spyware, adware, and more.

Types of Computer malware :

1) **Viruses:** Viruses are programs that attach themselves to legitimate files or programs and spread when those files are executed. They can corrupt files, steal data, or cause other harmful effects.
2) **Worms:** Worms are standalone malware programs that replicate themselves to spread across networks and computers without the need for human interaction. They can consume network bandwidth, degrade system performance, or carry out other malicious activities.
3) **Trojans:** Trojans disguise themselves as legitimate software or files to trick users into executing them. Once activated, Trojans can perform various malicious actions, such as stealing sensitive information, creating backdoors for remote access, or damaging files.
4) **Ransomware:** Ransomware encrypts files on a victim's system and demands a ransom payment in exchange for decryption keys. It can effectively lock users out of their own data until they pay the ransom.
5) **Spyware:** Spyware secretly gathers information about a user's activities, such as browsing habits, keystrokes, or personal information, and sends it to a third party without the user's consent.

5.5 Computer Virus:

- Computer viruses are unwanted software programs or pieces of code that interfere with the functioning of the computer. They spread through contaminated files, data, and insecure networks.
- computer virus is a malicious software program designed to replicate itself and infect computer systems by inserting its code into other programs or documents.
- One example of a computer virus is the "ILOVEYOU" virus, which emerged in 2000. It spread through email as a love letter and, when opened, infected the user's computer, causing widespread damage by overwriting files and spreading to contacts in the email address book.

Types of Computer Virus:

1) **Overwrite Virus: -**It is overwriting the code of the host computer system's file with its own malicious code
2) **Append Virus:** - this virus appends its malicious code to the end of the host program's file
3) **Macro Virus-**It's altering or infects the macros of a document or data file
4) **Boot Virus: -** its altering boot sector program stored in hard disk or any other storage device
5) **Resident Virus: -** it's stays permanently in the primary memory (RAM) of the computer
6) **Multipartite Virus: -** it's spreads and infects in multiple ways. It infects both the boot sector and the executable files stored on the hard drive simultaneously. Etc.

How computer virus works:

- A computer virus works by attaching itself to a host program or file and spreading to other files or systems
- When the infected program is executed, the virus activates, replicates, and may carry out malicious actions, such as corrupting data, stealing information, or disrupting normal operations.)
- Viruses often rely on human actions, like opening infected email attachments or downloading compromised files, to propagate and infect new systems

Computer antivirus:

What is computer antivirus:

- A computer antivirus is a type of software designed to detect, prevent, and remove malicious software (malware) from a computer system. It serves as a crucial component of cybersecurity by protecting computers from various threats such as viruses, worms, Trojans, ransomware, spyware, adware, and more.

Types of computer antivirus:

1. **Signature-Based Antivirus:** This type of antivirus software identifies malware by comparing files on the computer with a database of known malware signatures. If a file's signature matches any in the database, it is flagged as malicious. **Example:** Norton Antivirus.
2. **Heuristic-Based Antivirus:** Heuristic antivirus uses algorithms to detect previously unknown malware based on its behavior or characteristics. It doesn't rely solely on signature matching but analyzes the code's behavior to identify potential threats.
   - **Example:** Kaspersky Antivirus.
3. **Behavioral-Based Antivirus:** This type of antivirus monitors the behavior of programs in real-time and identifies suspicious activities that may indicate malware. It observes actions such as unauthorized file modifications, attempts to access sensitive areas of the system, or unusual network behavior
   Example: Bitdefender Antivirus.
4. **Cloud-Based Antivirus:** Cloud-based antivirus relies on cloud servers to analyze files and identify threats. This approach allows for faster detection and response to new malware threats since the cloud servers maintain updated databases and analysis tools.
   Example: Panda Security Cloud Antivirus.
5. **Full Security Suites:** Some antivirus software comes as part of comprehensive security suites that include additional features such as firewall protection, secure browsing, email scanning, and password management.
   Examples: McAfee Total Protection, Avast Premium Security.

CYBER ATTACKS

- Cyber-attack is a malicious and deliberate attempt by an individual or organization to exploit vulnerabilities in computer systems, networks, or devices for various purposes, including theft, disruption, or damage. These attacks can target individuals, businesses, governments, or even critical infrastructure, and they can take many forms, ranging from simple phishing emails to sophisticated malware infections and distributed denial-of-service (DDoS) attacks.

Cyber-attacks can have diverse objectives, including:

1. **Information Theft:** Stealing sensitive information such as personal data, financial records, or intellectual property.
2. **Financial Gain:** Obtaining money through fraudulent activities like phishing scams, ransomware attacks, or identity theft.
3. **Disruption:** Disrupting the normal operations of systems or networks, causing inconvenience, financial loss, or damage to reputation.
4. **Espionage:** Gathering intelligence or trade secrets for competitive advantage or political purposes.
5. **Sabotage:** Intentionally causing damage to systems, networks, or data, often for revenge or ideological reasons.
6. **Cyber Warfare:** Engaging in attacks against the infrastructure or networks of other nations for strategic or military objectives.

- Cyber-attacks can be launched using various methods, including malware (such as viruses, worms, trojans, and ransomware), social engineering techniques (like phishing and pretexting), denial-of-service attacks, exploiting software vulnerabilities (through techniques like hacking or SQL injection), and more.

❖Types of Cyber-attacks:

- Money Laundering, Information Theft, Cyber Pornography, Email spoofing, Denial of Service (DoS), Cyber Stalking, ,Logic bombs, Hacking Spamming Etc.

1. **Money Laundering:** Money laundering is the process of concealing the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses. For example, a criminal might set up a shell company to "legitimize" money obtained from illegal activities, such as drug trafficking or fraud.
2. **Information Theft:** Information theft involves stealing sensitive information, such as personal data, financial records, or intellectual property, for malicious purposes. For instance, a hacker might infiltrate a company's database and steal customer credit card information to sell on the dark web.
3. **Cyber Pornography:** Cyber pornography involves the distribution or creation of sexually explicit material using digital means. An example would be the operation of websites that host or distribute illegal pornography, exploiting and profiting from such content.
4. **Email Spoofing:** Email spoofing is the forging of an email header to make it appear as though the email originated from someone or somewhere other than the actual source. For example, a cybercriminal might spoof the email address of a legitimate bank to trick recipients into providing sensitive information like passwords or financial details.
5. **Denial of Service (DoS):** A Denial of Service attack aims to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of illegitimate traffic. For instance, attackers might use a botnet to flood a website's server with traffic, making it unavailable to legitimate users.
6. **Cyber Stalking:** Cyber stalking involves the persistent and unwanted harassment or monitoring of an individual through electronic means, such as email, social media, or messaging apps. An example would be an individual repeatedly sending threatening or invasive messages to someone via social media.
7. **Logic Bombs:** A logic bomb is a piece of code intentionally inserted into a software system that will execute a malicious function when certain conditions are met. For example, a disgruntled employee might plant a logic bomb in a company's network that activates on their termination date, deleting critical files or causing system failures.
8. **Hacking:** Hacking refers to gaining unauthorized access to computer systems or networks for malicious purposes. An example would be a hacker exploiting a software vulnerability to gain access to a company's database and steal sensitive information.
9. **Spamming:** Spamming involves sending unsolicited, often irrelevant or inappropriate messages in bulk, typically via email. For example, a spammer might send out millions of emails advertising fake products or attempting to phish for personal information.

- These are just a few examples of the various types of cyber-attacks that can occur, each with its own methods, motivations, and potential consequences.

❖Computer Ethics & Good Practices:

- Computer ethics refers to the moral principles and guidelines that govern the behavior and use of technology, particularly computers and the internet. Adhering to computer ethics ensures responsible and ethical behavior in the digital realm. Here are some computer ethics principles and good practices:

1. **Respect for Privacy:** Respect the privacy of individuals by safeguarding their personal information and data. Avoid unauthorized access to confidential data and ensure that privacy settings are appropriately configured on devices and applications.
2. **Integrity:** Maintain the integrity of computer systems, software, and data by refraining from malicious activities such as hacking, unauthorized tampering, or spreading malware. Ensure that data is accurate, reliable, and securely stored.
3. **Security:** Take proactive measures to protect computer systems, networks, and data from cyber threats. Use strong passwords, encryption, firewalls, and antivirus software to prevent unauthorized access, data breaches, and cyber attacks.
4. **Honesty and Truthfulness:** Be honest and truthful in all online interactions, communications, and transactions. Avoid spreading false information, misleading content, or engaging in deceptive practices such as phishing or online scams.
5. **Intellectual Property Rights:** Respect intellectual property rights by adhering to copyright, trademark, and patent laws. Avoid unauthorized copying, distribution, or use of copyrighted material, software, or digital content without proper authorization or licensing.
6. **Cyberbullying and Harassment**: Refrain from engaging in cyberbullying, harassment, or discrimination against others online. Treat others with respect, civility, and empathy in digital communications and social interactions.
7. **Environmental Responsibility:** Practice environmental responsibility by minimizing electronic waste, conserving energy, and promoting sustainable practices in the production, use, and disposal of electronic devices and equipment.
8. **Digital Citizenship:** Act as responsible digital citizens by promoting digital literacy, safety, and inclusion in online communities. Encourage ethical behavior, critical thinking, and responsible use of technology among peers, colleagues, and society at large.
9. **Professional Conduct:** Adhere to ethical standards and professional codes of conduct in computing-related professions, such as software development, IT management, cybersecurity, and data science. Uphold professional integrity, transparency, and accountability in all professional activities.
10. **Continuous Learning and Adaptation:** Stay informed about emerging technologies, ethical issues, and best practices in computer science and information technology. Continuously update skills, knowledge, and ethical awareness to adapt to evolving ethical challenges and technological advancements.

- By following these computer ethics principles and good practices, individuals, organizations, and society can foster a culture of ethical behavior, trust, and responsibility in the digital age.

❖Introduction of Cyber Laws about Internet Fraud:

- Cyber laws encompass a wide range of legal regulations and principles designed to address various aspects of cyberspace, including online activities, digital transactions, and internet-based crimes. One crucial area of cyber law pertains to internet fraud, which involves deceptive practices carried out over the internet with the intention of unlawfully obtaining money, sensitive information, or other valuable assets from individuals or organizations.
- Internet fraud encompasses a diverse array of fraudulent schemes and activities conducted through various online platforms, such as websites, email, social media, and online marketplaces.

Common examples include phishing scams, identity theft, online auctions fraud, credit card fraud, and investment scams.

- To combat internet fraud and protect individuals and businesses from financial losses and harm, governments around the world have enacted cyber laws and regulations specifically targeting fraudulent activities conducted online. These laws aim to establish legal frameworks, define criminal offenses, and prescribe penalties for perpetrators of internet fraud.

• Key components of cyber laws related to internet fraud may include:

1. **Criminalization of Fraudulent Activities:** Cyber laws typically criminalize various forms of internet fraud, including unauthorized access to computer systems, theft of personal or financial information, deceptive practices in online transactions, and dissemination of false or misleading information for fraudulent purposes.
2. **Jurisdiction and Extraterritoriality:** Cyber laws often address jurisdictional issues related to internet fraud, determining which laws apply when fraudulent activities cross national borders or involve parties located in different jurisdictions. Some cyber laws may have extraterritorial reach, allowing authorities to prosecute perpetrators operating outside their territorial boundaries.
3. **Regulation of Electronic Transactions:** Cyber laws may regulate electronic transactions, such as online payments, digital contracts, and electronic signatures, to ensure their legality, validity, and security. These laws may establish standards for encryption, authentication, and electronic records management to prevent fraud and promote trust in electronic commerce.
4. **Data Protection and Privacy:** Cyber laws often include provisions for data protection and privacy to safeguard personal and sensitive information from unauthorized access, use, or disclosure. These laws may require organizations to implement security measures, obtain consent for data processing, and notify individuals in the event of data breaches or privacy violations.
5. **Enforcement and Penalties:** Cyber laws establish mechanisms for the enforcement of anti-fraud provisions and prescribe penalties for individuals or entities found guilty of internet fraud. Penalties may include fines, imprisonment, asset forfeiture, and restitution to victims, depending on the severity of the offense and the applicable legal jurisdiction.
6. **International Cooperation and Collaboration:** Given the global nature of internet fraud, cyber laws often emphasize international cooperation and collaboration among law enforcement agencies, governments, and industry stakeholders to combat cross-border fraud schemes, share intelligence, and coordinate investigative efforts effectively.

❖ Good Computer Security Habits:

- Developing good computer security habits is essential for protecting your personal and sensitive information, preventing unauthorized access to your devices and accounts, and maintaining the integrity and confidentiality of your digital data.
- Here are some key computer security habits to follow:

1. **Use Strong and Unique Passwords:** Create strong and unique passwords for each of your accounts, incorporating a combination of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable passwords such as "123456" or "password."

2. **Enable Two-Factor Authentication (2FA):** Enable two-factor authentication whenever possible to add an extra layer of security to your accounts. 2FA requires a second form of verification, such as a code sent to your phone or generated by an authenticator app, in addition to your password.
3. **Keep Software Updated:** Regularly update your operating system, software applications, and antivirus programs to patch security vulnerabilities and protect against known threats. Enable automatic updates whenever possible to ensure that your devices are always running the latest security patches.
4. **Use Secure Wi-Fi Networks:** Avoid connecting to unsecured or public Wi-Fi networks, which are more susceptible to eavesdropping and hacking. Instead, use encrypted Wi-Fi networks with strong passwords to protect your internet traffic from interception.
5. **Be Cautious of Phishing Attempts:** Be skeptical of unsolicited emails, messages, or phone calls requesting sensitive information or urging you to click on suspicious links or download attachments. Verify the authenticity of the sender before responding or taking any action.
6. **Backup Your Data Regularly:** Backup your important files and data regularly to an external hard drive, cloud storage service, or backup software. This ensures that you can recover your data in the event of a hardware failure, ransomware attack, or other data loss incidents.

7. **Practice Safe Browsing Habits:** Be cautious when browsing the internet and visiting websites, especially those with unknown or suspicious content. Avoid clicking on pop-up ads, downloading files from untrusted sources, or visiting potentially malicious websites.
8. **Secure Your Mobile Devices:** Apply security measures to your smartphones, tablets, and other mobile devices, such as setting a passcode or biometric lock, enabling device encryption, and installing security updates regularly.
9. **Use Secure Payment Methods:** When making online purchases or transactions, use secure payment methods such as credit cards or reputable payment platforms that offer buyer protection. Avoid entering sensitive financial information on unsecured or unfamiliar websites.
10. **Educate Yourself:** Stay informed about the latest cybersecurity threats, trends, and best practices by reading security blogs, attending workshops or webinars, and following reputable cybersecurity experts and organizations. Educate yourself and others about common cyber threats and how to mitigate them effectively.

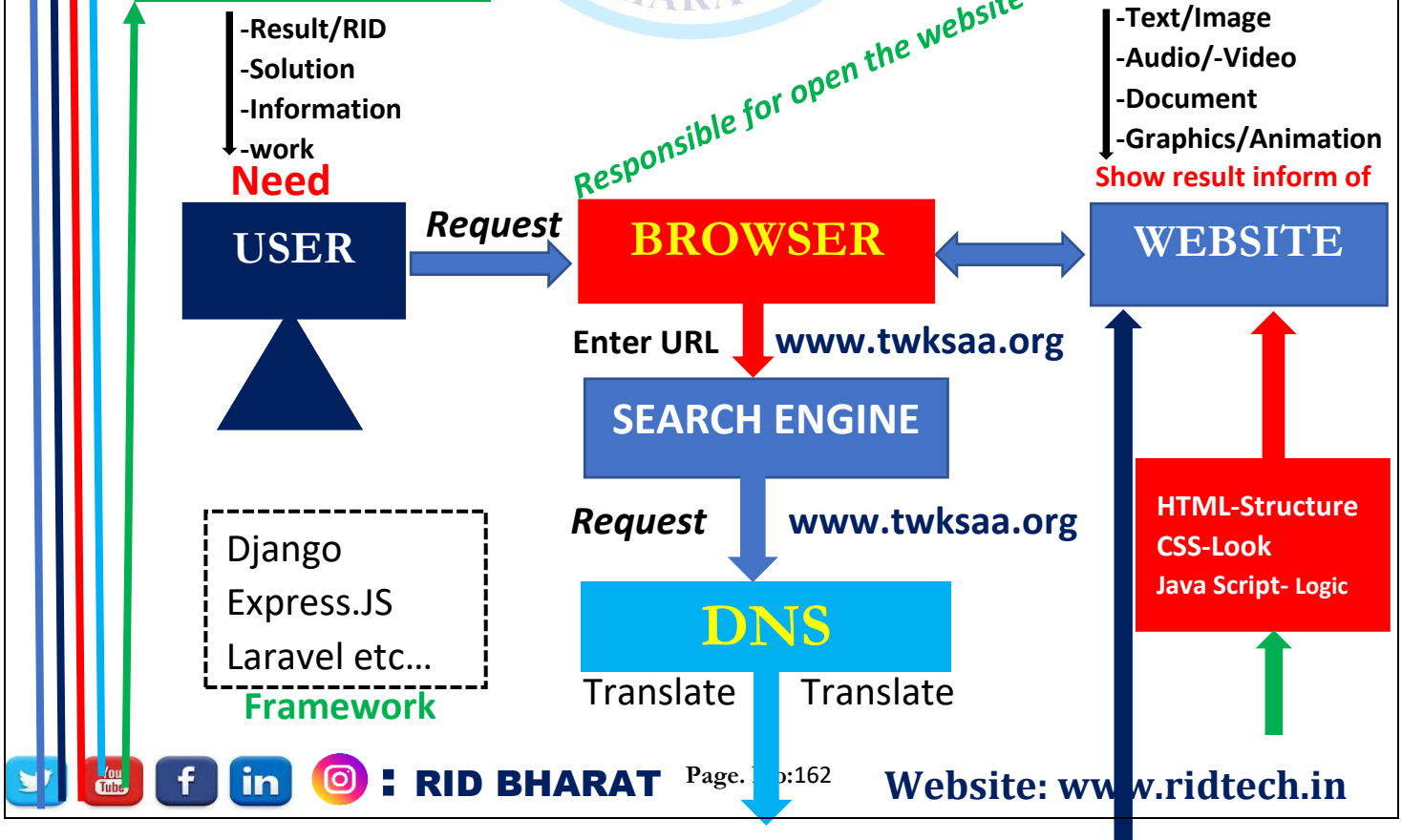
Definition: - website is collection of web page and related content that is identified by a common "Domain name"

Types: - 1). Static Website 2). Dynamic Website

Static Website: - consists of a series of HTML files, each one representing a physical page of a website.

Dynamic Website: -change or customizes itself frequently and automatically.

How Web Works



Web: The web is a global system of interconnected computer networks that use the Internet protocol suite to access and share information. It allows users to access and share information over the Internet. Or Web is virtual directory on web server. Or Web [Portion of Internet]

Site: Site [Location] A site refers to a location or a collection of web pages hosted on a web server and accessible through a specific domain or URL.A site refers to a specific location on the internet identified by a unique domain name and accessible via a web browser.

Page:

- A page refers to a single, individual document or resource on the web.
- It is a single document or resource that is part of a website and can be accessed through a specific URL?

Web Page:

- A web page is a single hypertext document available on World Wide Web (WWW).
- Hyper Text document that contains information beyond what is displaying.
- The term "Hyper" is derived from a Greek term, which means "beyond"
-

DHCP

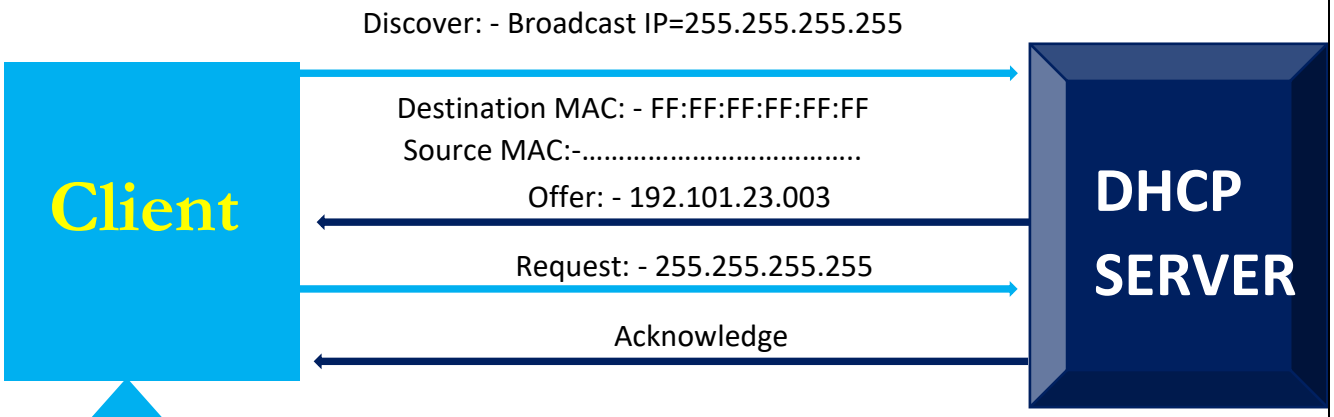
Dynamic Host Configuration Protocol

Definition: - DHCP is an automatically assign IP address to client. It is client server-based model. It's works on application layer, IP address assigned is known as dynamic IP address. DHCP IP address range is called scope.

BOOTP: - It is another method to allocate dynamic Ip address but MAC address must be entered manual. DHCP is advance version of BOOTP.

DHCP Provide: - 1. IP address 2. Subnet mask 3. Domain Name 4. Default Gateway 5. DNS Server address 6.Wins server Address.

DORA Process: - DHCP automatically assign IP address dynamically by DORA Process.



-Discover(port-68): - UDP Broadcast from DHCP client to locate available server Layer2 Broadcast FF: FF: FF: FF: FF: FF Layer3 Broadcast: - 255.255.255.255

-Offer(port-67): - DHCP server to client in Response to DHCP discover with offer of configuration parameter (DHCP server offer IP, MAC add of client, subnet mask, Lease Length)

-Request(port-68): - then client Broadcast to DHCP server request for offered IP Address.

-Acknowledge(port-67): - server to client with configuration parameters including network address.

DHCP
T3 SKILL CENTER

Definition: - SMTP (simple mail transfer Protocol) is an application layer protocol.it is Push based Protocol.

Use: - it used for send mail and it is used by the client send mail to the server it's used TCP port-25 because TCP is connection oriented. SMTP requires each message in 7-bit ASCII Format.

SMTP Commands: - 1.HELO & EHLO:- initiate a new protocol session between client & server.
2.MAIL FROM:- to initiate sending an email message or to identify sender.
3.DATA:- indicating the start of transmission of email message . last message is "."
4.RSET:-Reset connection if it encounter or error.
5.QUIT:- Terminates the protocol session.

"SMTP"
RID.org

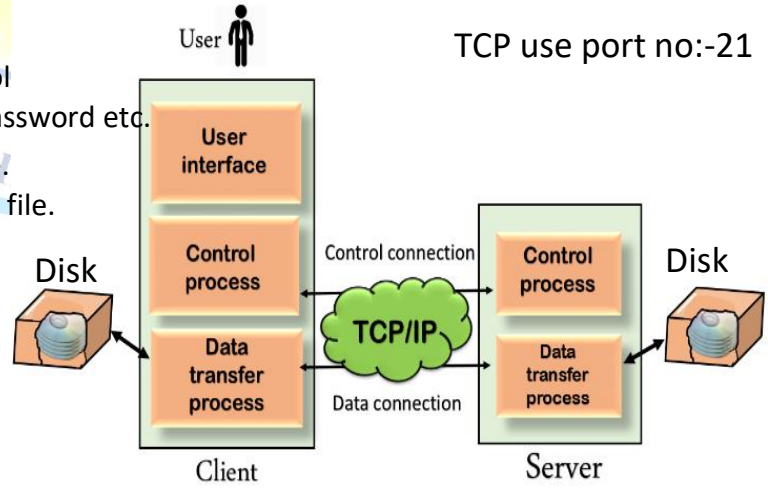
Definition: - FTP (file transfer Protocol) it is an application layer protocol.
To transfer a file 2 TCP connection are used by FTP in parallel control connection & data connection.

TCP Work Flow

TCP use port no:-21

-Contral connection: - for sending control information like user identification password etc.

-Data connection: - for sending actual file.
It is also used for downloading the file.



FTP Data Structure: -

-1. File Structure: - in file structure there is no internal structure and the file is considered to be continuous sequence of data a byte.

-2. Record Structure: - in record structure file is made up of sequential records.

-3. Page Structure: - in page structure the file is made up of independent indexed pages

Transmission mode of FTP: -

-1. Stream Mode: - Data transmission in continuous stream of bytes

-2. Block Mode: - Data transmission in Blocks.

-3. Compressed Mode: -Data is compressed then send generally used for sending large files.

FTP is not secure, it is plan text files transfer, data is not encrypted.

SFTP: - Secure Transfer Protocol

Data is encrypted. SFTP use SSH & SSL/TLS for security. It is use port no-22. SFTP was designed by IETF as an extended version of SSH2.0, Allowing file transfer over SSH and use with transport layer.

FTP, SFTP & TFTP

POP3 AND IMAP PROTOCOLS

- POP3 (Post Office Protocol version 3) and IMAP (Internet Message Access Protocol) are two commonly used protocols for retrieving emails from a mail server to a client device, such as a computer or smartphone. While both protocols serve a similar purpose, they have differences in how they handle email storage, synchronization, and access.

❖ POP3 (Post Office Protocol version 3):

- **Download and Delete Model:** POP3 is primarily designed for offline email access. When a client connects to a POP3 server to retrieve emails, the emails are downloaded from the server to the client device's email client (such as Outlook or Thunderbird). By default, emails are typically deleted from the server after being downloaded to the client device.
- **Limited Synchronization:** POP3 typically offers limited synchronization capabilities. Once emails are downloaded to a client device, they are no longer accessible on the server unless explicitly configured otherwise. This means that actions taken on emails (such as read, delete, or move) are not synchronized between the client device and the server.
- **Port:** POP3 commonly uses port 110 for non-encrypted connections and port 995 for encrypted connections (POP3S).
- **Efficient Use of Server Resources:** Since emails are downloaded and removed from the server, POP3 can be more efficient in terms of server resources and storage space, especially for users who access their emails from a single device.

❖ IMAP (Internet Message Access Protocol):

- Server-Side Email Management: IMAP is designed for managing emails on the server, allowing users to access their emails from multiple devices while keeping them stored centrally on the server. When a client connects to an IMAP server, emails remain on the server and are synchronized between the server and the client device.
  - **Synchronization Across Devices:** IMAP offers robust synchronization capabilities, ensuring that changes made to emails (such as read, delete, or move) on one device are reflected across all devices connected to the same IMAP account. This enables seamless access to emails from multiple devices.
  - **Port:** IMAP commonly uses port 143 for non-encrypted connections and port 993 for encrypted connections (IMAPS).
  - **Greater Storage Flexibility:** Since emails remain on the server, IMAP provides greater flexibility in managing email storage and access. Users can access their entire mailbox from any device without worrying about downloading or deleting emails.

"Difference Between POP3 and IMAP" it is pull based Protocol.

POP3(Post-office protocol version 3) and IMAP (Internet mail access Protocol) are used for Receive mail.

POP3: -

-only allows downloading message
-it is used port 110 and with SSL port 995
-access from a single device at a time
-Read the mail after downloading
-does not allow user to organize mails & folder
-user can not search message before downloading
-no backup messages

IMAP: -

-Allow see in the folder without download
-it is used port 43 & with SSL port 993
-access from multiple devices
-can be read partially before download
-can organize email directly in sever
-user can create, delete & rename email on the mail server
-Backup is possible

What is RID Organization (RID संस्था क्या है)?

- **RID Organization** यानि **Research, Innovation and Discovery Organization एक** संस्था हैं जो TWF (TWKSAA WELFARE FOUNDATION) **NGO** द्वारा RUN किया जाता है | जिसका मुख्य उदेश्य हैं आने वाले समय में सबसे पहले **NEW (RID, PMS & TLR)** की खोज, प्रकाशन एवं उपयोग भारत की इस पावन धरती से भारतीय संस्कृति, सभ्यता एवं भाषा में ही हो |
- देश, समाज, एवं लोगों की समस्याओं का समाधान **NEW (RID, PMS & TLR)** के माध्यम से किया जाये इसके लिए ही **इस RID Organization** की स्थपना 30.09.2023 किया गया है | जो TWF द्वारा संचालित किया जाता है |
- TWF (TWKSAA WELFARE FOUNDATION) NGO की स्थपना 26-10-2020 में बिहार की पावन धरती सासाराम में Er. RAJESH PRASAD एवं Er. SUNIL KUMAR द्वारा किया गया था जो की भारत सरकार द्वारा मान्यता प्राप्त संस्था हैं |
- Research, Innovation & Discovery में रूचि रखने वाले आप सभी विधार्थियों, शिक्षकों एवं बुधीजिवियो से मैं आवाहनं करता हूँ की आप सभी **इस RID संस्था** से जुड़ें एवं अपने बुध्दि, विवेक एवं प्रतिभा से दुनियां को कुछ नई **(RID, PMS & TLR)** की खोजकर, बनाकर एवं अपनाकर लोगों की समस्याओं का समाधान करें |

MISSION, VISSION & MOTIVE OF "RID ORGANIZATION"

मिशन	हर एक ONE भारत के संग
विजन	TALENT WORLD KA SHRESHTM AB AAYEGA भारत में और भारत का TALENT भारत में
मकसद	NEW (RID, PMS, TLR)

MOTIVE OF RID ORGANIZATION NEW (RID, PMS, TLR)

NEW (RID)		
R	I	D
Research	Innovation	Discovery
NEW (TLR)		
T	L	R
Technology, Theory, Technique	Law	Rule
NEW (PMS)		
P	M	S
Product, Project, Production	Machine	Service

RID रीड संस्था की मिशन, विजन एवं मकसद को सार्थक हमें बनाना हैं |
भारत के वर्चस्व को हर कोने में फैलना हैं |
कर के नया कार्य एक बदलाव समाज में लाना हैं |
रीड संस्था की कार्य-सिध्दांतों से ही, हमें अपनी पहचान बनाना हैं |

Er. Rajesh Prasad (B.E, M.E)
Founder:
TWF & RID Organization

Computer Network के इस E-Book में अगर मिलती त्रुटी मिलती है तो कृपया हमें सूचित करें |

Computer Network के इस E-Book में अगर मिलती त्रुटी मिलती है तो कृपया हमें सूचित करें | WhatsApp's No: 9102707903 or Email Id: ridorg.in@gmail.com

धन्यवाद

धन्यवाद