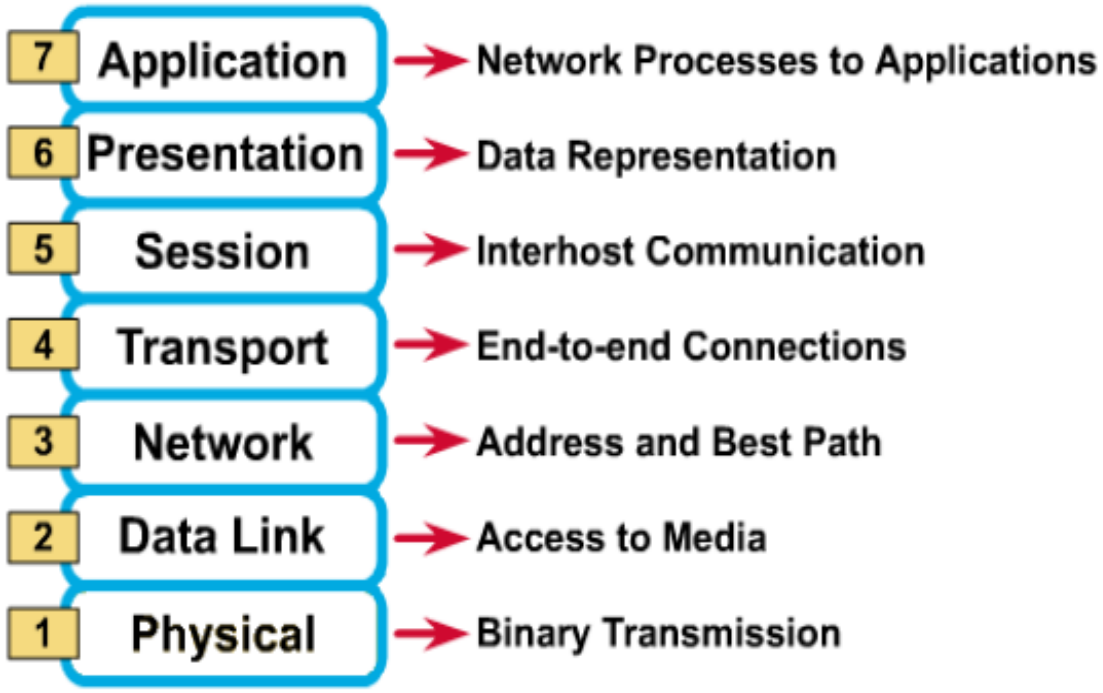
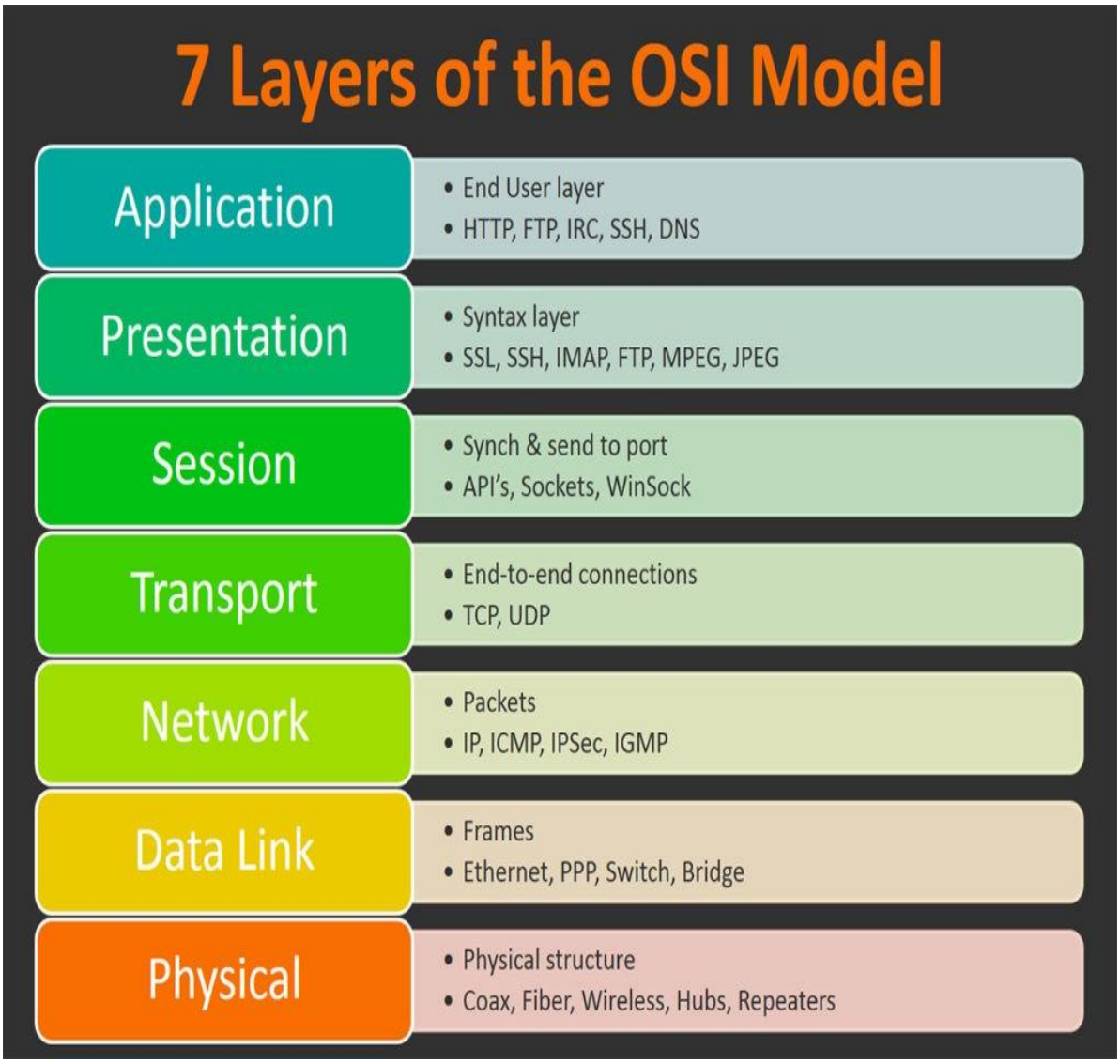
Unit: 5	**Computer Network Basics:** Introduction – OSI layer model – Function of each layer network types – LAN- WAN– MAN – internet – intranet – extranet – Blue tooth Technology. **TCP/IP**: Introduction, History of TCP/IP, Function of each layer of TCP/IP, User Datagram Protocol, Comparison of OSI and TCP/IP. IP Addressing, IP address classes, Subnet Addressing, Domain Name System, Email – SMTP, POP,IMAP; FTP, HTTP, Overview of IP version 6.

What is OSI ?

- In 1984 in order to facilitate network interconnection without necessarily requiring complete redesign, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- The OSI model defines a basic framework for how modern networks operate. It separates the methods and protocols required for a network connection into seven different layers. Each higher layer relies on services provided by a lower layer.



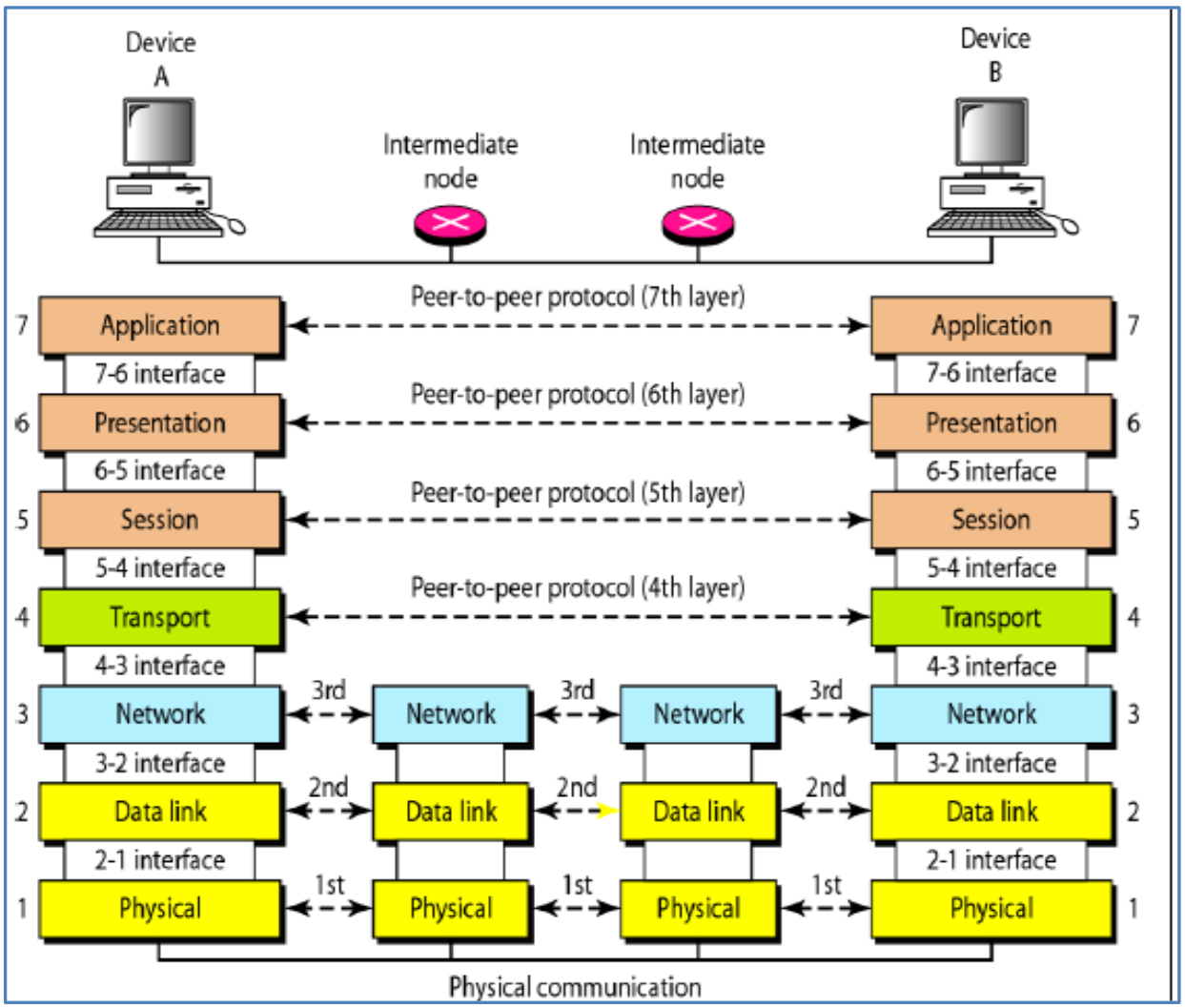
Seven layers OSI reference model



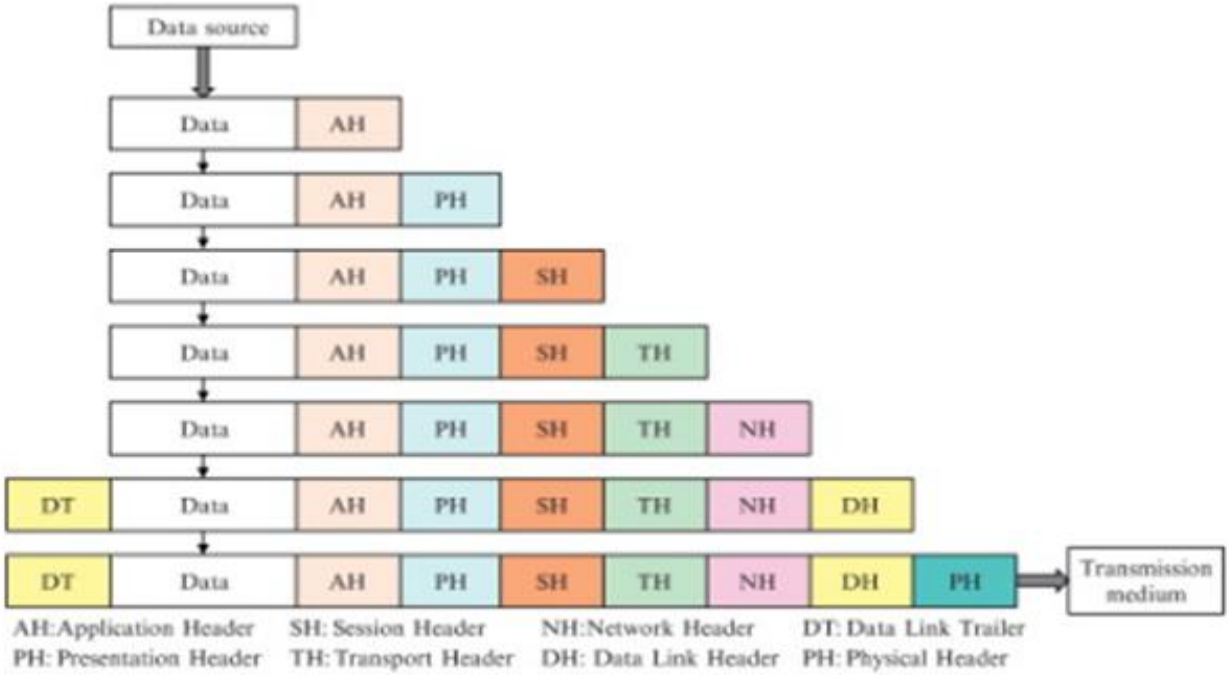
Seven OSI reference model layers along with the devices and protocols associated with each layer.

Keep in mind:

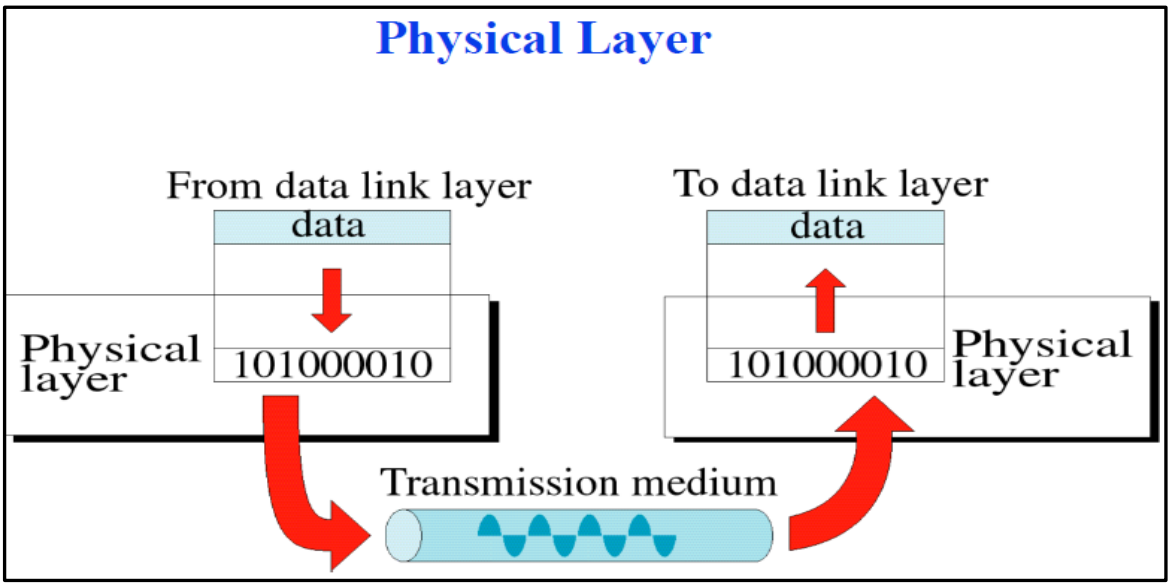
- ✓ ISO is an organization, OSI is a model
- ✓ It was developed to allow systems with different platforms to communicate with each other. Here platform could be hardware (processor) and software (operating systems).
- ✓ OSI is a network model that defines the protocols for network communications.



Communication & Interfaces in the OSI model



Physical Layer (lowest layer of the OSI reference model)



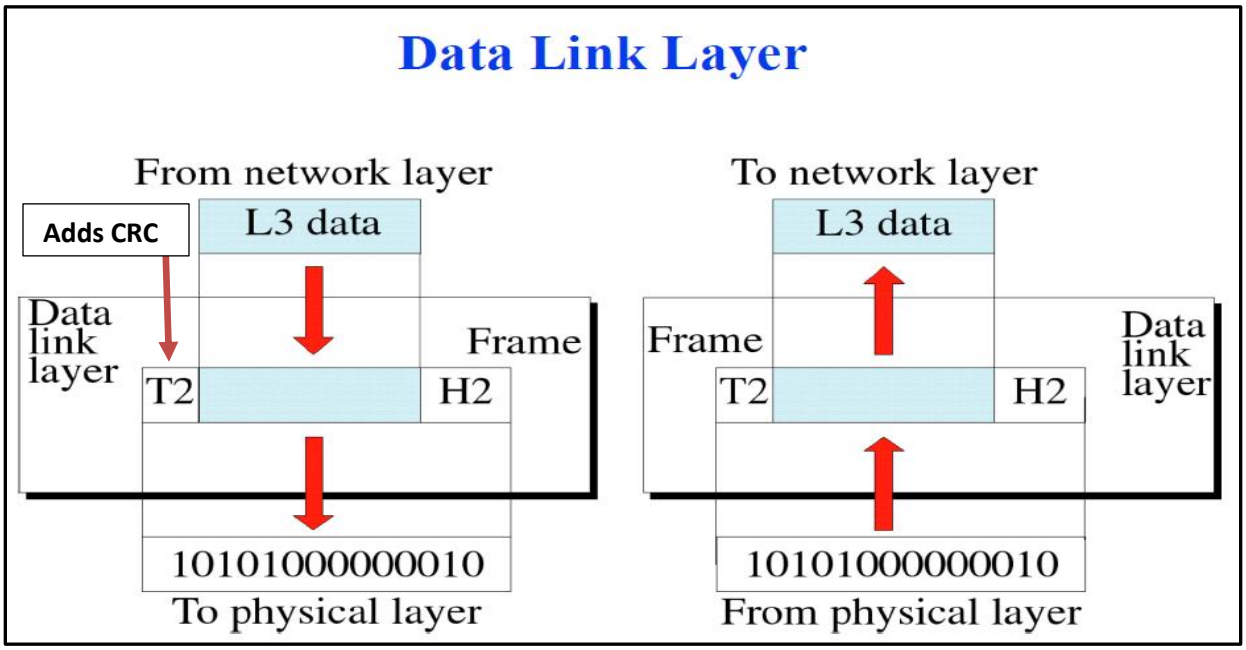
Functionality of the Physical Layer:

- The Physical Layer provides the physical characteristics of the transmission medium
  - Mechanical specification of electrical connectors and cables, for example maximum cable length
  - Electrical specification of transmission line
  - Bit-by-bit or symbol-by-symbol delivery
- It controls the electrical, mechanical functional specifications for activating, maintaining, and deactivating the physical link between end systems.
- It transfers bits from the senders to the receiver by converting them into voltage (electrical) signals or pulses of light or wireless radio link.
- This layer performs machine port-level addressing, synchronization, multiplexing and different switching operations.
- Physical layer receives data from Data Link Layer and encodes it into signals to be transmitted onto the medium. On the receiver side, the physical layer receives the signals from the transmission medium decodes it back into data and sends it to the Data Link Layer.

Keep in mind:

- ✓ Hub, Repeater, Modem, Cables are Physical Layer devices.

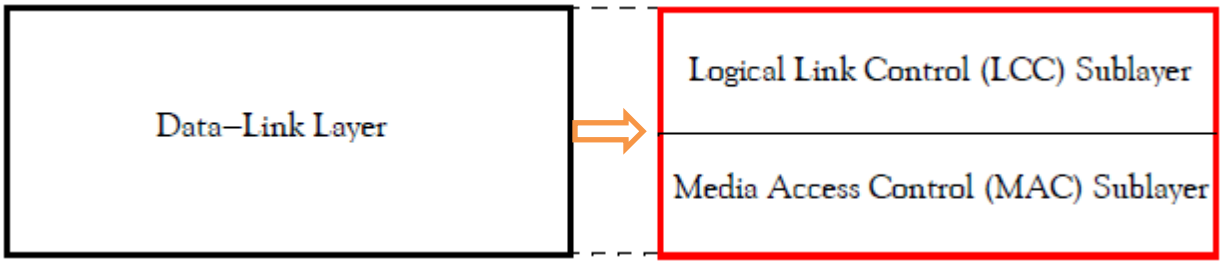
Data link layer:



Functionality of the Data link Layer:

- **Framing:** On the sender side, the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as frames and sends it to the physical layer. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer. This process is called framing.
- **Physical addressing**: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
- **Error control**: The data link layer provides error control mechanism to identify lost or damaged frames, duplicate frames and then retransmit them. Error control information is present in the trailer of a frame.
- **Flow Control**: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates that amount of data that can be sent before receiving acknowledgement.
- **Access control**: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

The IEEE 802 team enhanced the OSI model by dividing the Data Link Layer into two sublayers. These sublayers are the ***Media Access Control (MAC***) Sublayer and the ***Logical Link Control (LLC)*** Sublayer**.**



Keep in mind:

- ✓ **CRC** (Cyclic Redundancy Check) code is used to provide error detection and verification information and it is added to the trailer part of a frame.

- ✓ **Media Access Control (MAC)**

The MAC sublayer function is to ensure that only one device can transmit on any type of media at any time. If two or more devices attempt to transmit at the same time on the same media, a collision of signals will occur. MAC sublayer defines three ways to control access to media as flow control mechanism. These are:

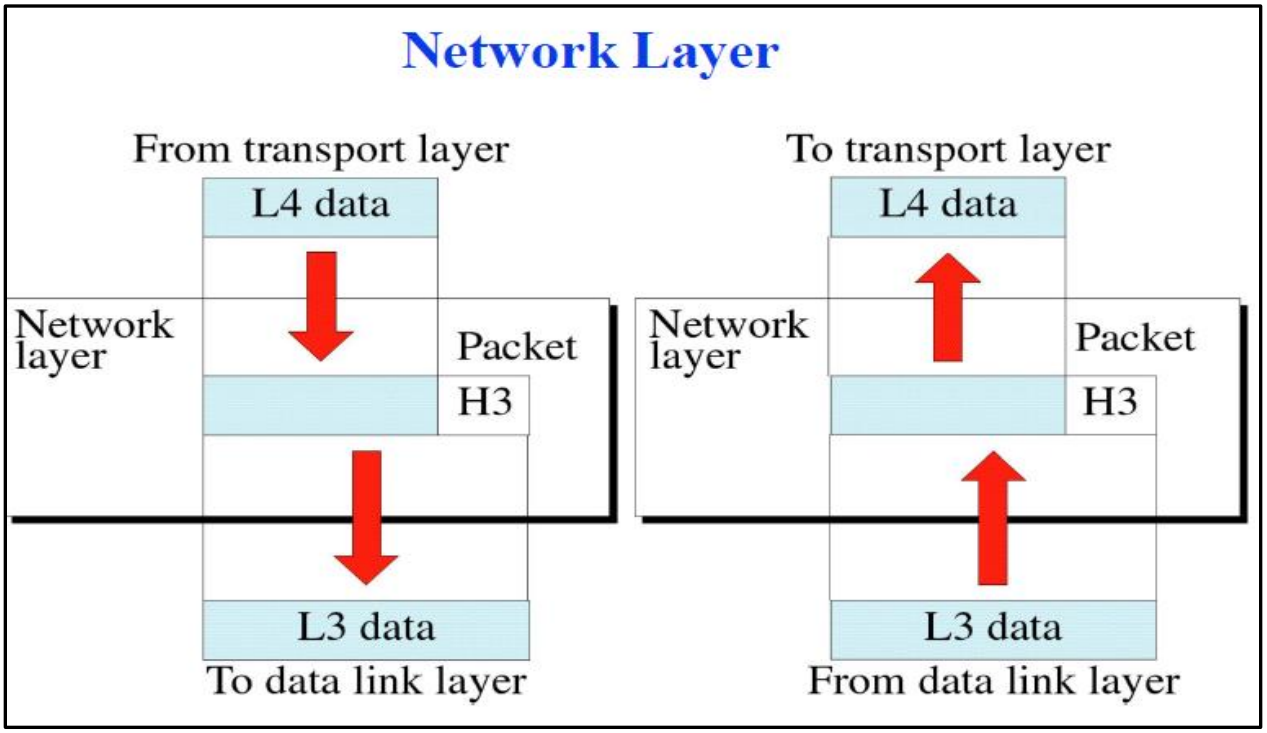
- ♦ **Addressing**: The MAC sublayer handles the physical addresses of devices on the network. It is a 48-bit address, example of this address for an Ethernet card could be 00−E0−18−90−1E−CB. Although every client in a network can be assigned a name (a logical name) by the software, the Physical layer does not recognized it. Therefore, for messages to be sent to the proper destination a unique address that it can recognize is the MAC address.

- ♦ **Contention**: On a network, contention refers to the competition among network devices for the opportunity to use a media or network resource. In one sense, contention applies to a situation in which two or more devices attempt to transmit at the same time, thus causing a collision on the line. With recent design improvements, contention−based networks devices listen for other signals on the media before transmitting. Although collisions are not totally eliminated, but can be minimize by using a protocol that is known as Carrier Sense Multiple Access, or CSMA. It is of two types: CSMA/CD and CSMA/CA. CSMA/CD stands for Carrier Sense Multiple Access/Collision Detection and CSMA/CA is Carrier Sense Multiple Access/Collision Avoidance

- ♦ **Deterministic**: A deterministic network dictates that the network must follow certain rules and procedures before transmitting. The two types of deterministic networks are:
  - Token passing
  - Polling

- ✓ Data Link layer is handled by the **NIC (Network Interface Card)** and device driver of the host machine.
- ✓ NIC or LAN card, Switch, Bridge are Data Link Layer devices.

Network Layer:



Functionality of the Network Layer:

- **Internetworking**: It provides Internetworking for end-to-end delivery of packets.
- **Logical Addressing**: When packet is sent outside the network, network layer adds Logical (network) address of the sender and receiver to each packet and commonly known as IP address to recognize devices on the network. Network addresses are assigned to local devices by network administrator and assigned dynamically by a special server called DHCP (Dynamic Host Configuration Protocol) server.
- **Routing**: In the routing process, information in each packet informs the network where to send the packet to reach its destination and tells the receiving computer from where the packet originated. The network layer is most important when the network connection passes through one or more routers, which are hardware devices that examine each packet and, from their source and destination addresses, send the packets to their proper destination. Over a complex network, such as the Internet, a packet might go through ten or more routers before it reaches its destination.
- **Segmentation**: The network layer also defines how to fragment a packet into smaller packets to accommodate different media and communicating devices.

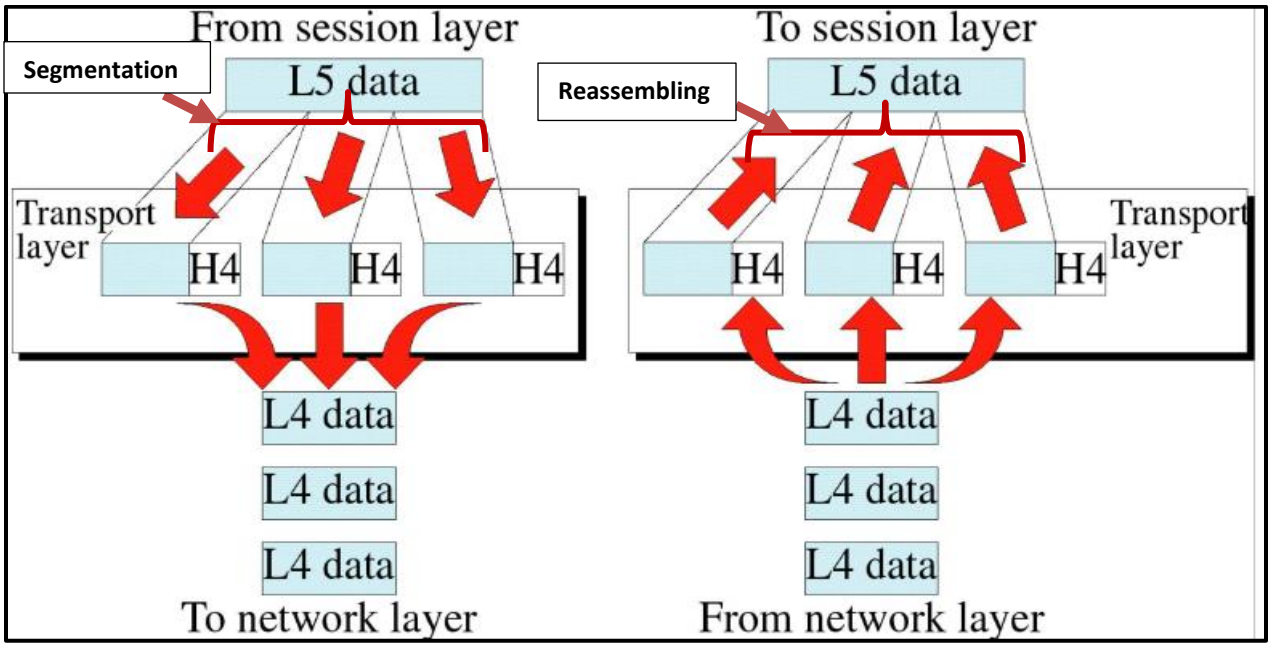
Keep in mind:

- ✓ Layer-3 switch and router are network layer devices

Functionality of the Transport Layer:

- It is responsible **for process-to-process delivery** of the entire message. A logical address at network layer facilitates the transmission of data from source to destination device. But the source and the destination both may be having multiple processes communicating with each other. Hence it is important to deliver the data not only from the sender to the receiver but also from the correct process on the sender to the correct process on the receiver. The transport layer takes care of process to process delivery of data and makes sure that it is intact and in order.

- **Segmentation** of message into packet and **reassembling** the packets into message. At the sending side, the transport layer receives data from the session layer, divides it into units called segments and sends it to the network layer. At the receiving side, the transport layer receives packets from the network layer, converts and arranges into proper sequence of segments and sends it to the session layer.



Segmentation of message into packet and reassembling the packets into message

- **Port addressing**: Computers run several processes. Transport layer (TL) header include a port address for each process.

- **Flow Control**: Flow control facility prevents the source form sending data packets faster than the destination can handle.

- **Error control**: TL ensures that the entire message arrives at the receiving TL without error. Transport layer provides error and flow control but unlike data link layer these are end to end rather than node to node delivery.

- **Connection Control**: It is of two types: Connection Oriented and Connectionless Transmission

  - Connection Oriented Transmission: In this type of transmission the receiving devices sends an acknowledgement back to the source after a packet or group of packet is received. So, this type of transmission is reliable and secure. It is a slower transmission process because it is a three-step process:

    - Connection Establishment (Setup)
    - Data Transfer
    - Termination / Disconnection

  - Connectionless Transmission: In this type of transmission the receiving devices does not sends an acknowledgement back to the source. So it is a faster transmission method as there is no connection setup and termination phase in this process.

Keep in mind:

- ✓ Segmentation of message into packet and reassembling the packets into message are all related to memory organization of a particular host computer. So Transport layer is controlled and operated by the Operating System of the host machine. Hence, it is a part of the Operating System and it communicates with the Application Layer by making system calls.
- ✓ Transport Layer is called as Heart of OSI model.

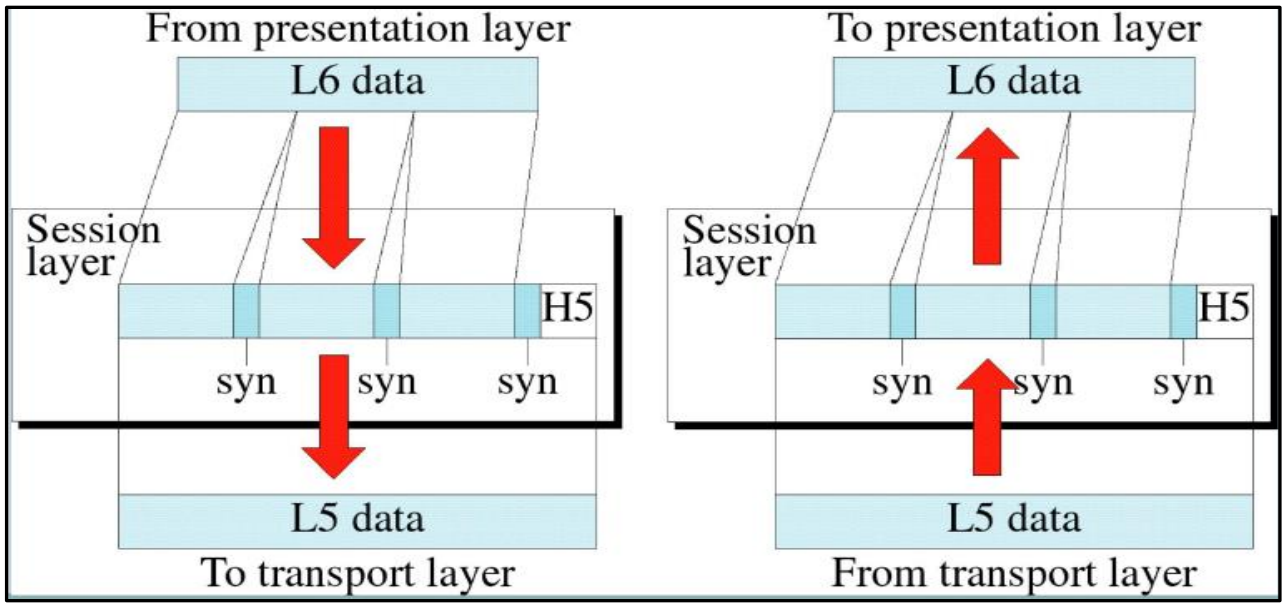
Functionality of the Session Layer:

- **Establishing, Maintaining and terminating a session**: When sending device first contact with the receiving device, it sends a **syn** (synchronization) packet to establish a connection and determines the order in which information will be sent. On the other side the receiver sends an **ack** (acknowledgement) to the sender to establish the connection. In this process a session can be set and finally terminate.

- **Dialog Control**: Session layer establishes a session between the communicating devices called dialog and synchronizes their interaction. So it is often called the network dialog controller. This layer allows two systems to start their mode of communication whether it is in half-duplex or full-duplex mode.

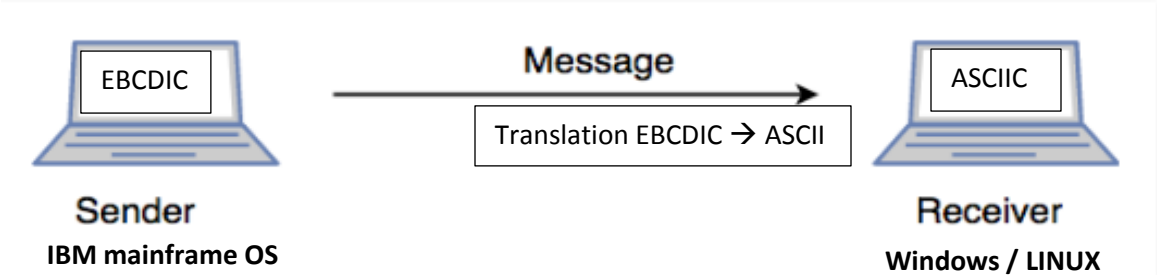
- **Dialog separation**: Process of adding **checkpoints** or **synchronization points** and **markers** to the stream of data is called dialog separation. For example, during the transfer of data between two machines somehow if the session breaks down, it is the session layer which re-establishes the connection. It also ensures that the data transfer starts from where it breaks keeping it transparent to the end user by introducing **synchronization points or checkpoints** in data streams for long communications. This ensures that data streams up to the checkpoints are successfully received and acknowledged. In case of any failures, only the streams after the checkpoints have to be re-transmitted.

- **Authentication:** when a user logins to a remote server user should be **authenticated** before getting access to the files and application programs.



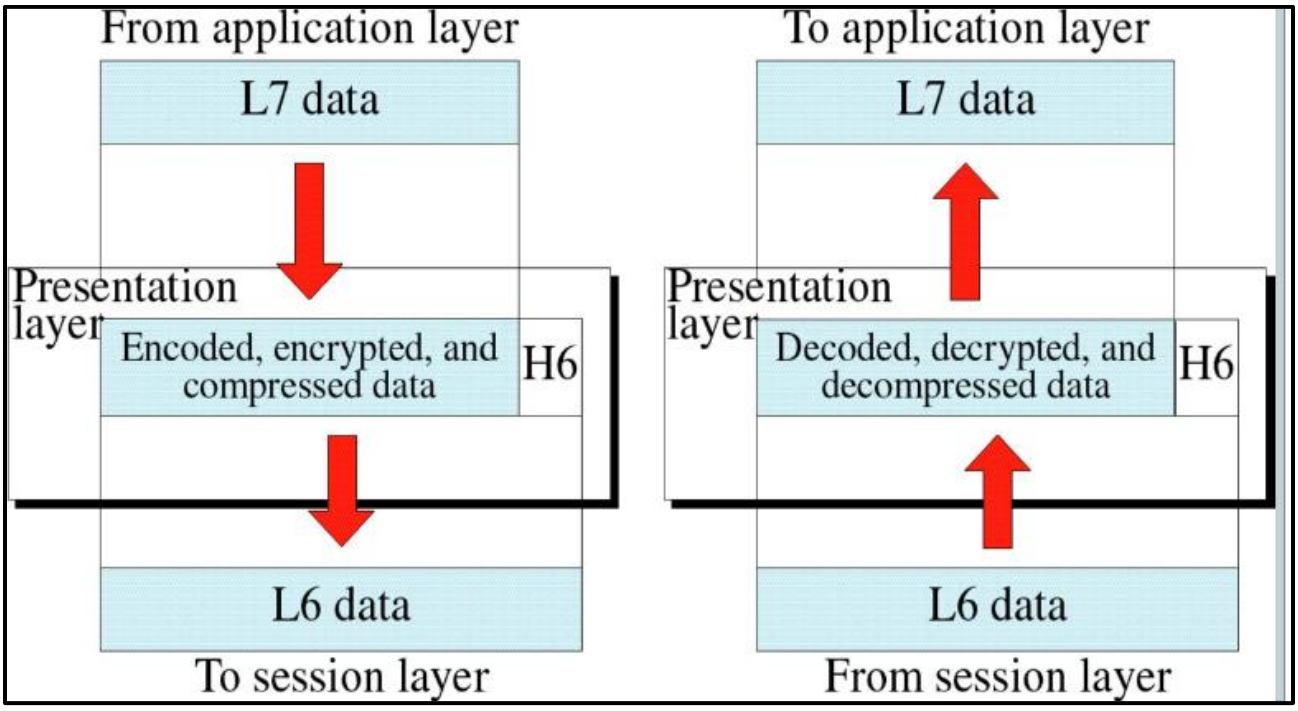
Functionality of the Presentation Layer:

- **Data Presentation or Translation**: The sending and receiving devices may run on different platforms (hardware, software and operating systems). As different computers use different encoding systems/schemes, it is to be ensured that the data being sent is in the format that the recipient can process it. Hence the presentation layer is responsible for interoperability between these different encoding methods. For example, Windows or Linux uses ASCII code but IBM mainframe uses EBCDIC code. Another example, Apple Mac OS or Linux OS (S64) use 'Big Endian' and Windows follow 'Little Endian' for data representation.



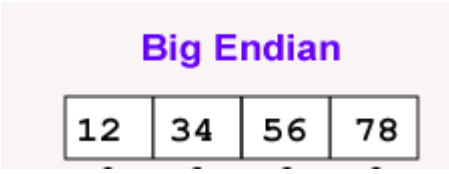
- **Compression**: Compression ensures faster data transfer. The data compressed at sender end has to be decompressed at the receiving end, both activities are performed by the Presentation layer. Data compression reduces the number of bits contained in the information hence enhance the utilization of the network bandwidth.

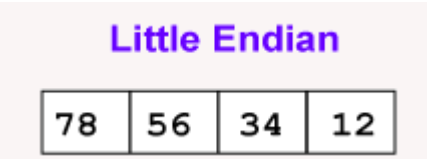
- **Encryption**: Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.



Keep in mind:

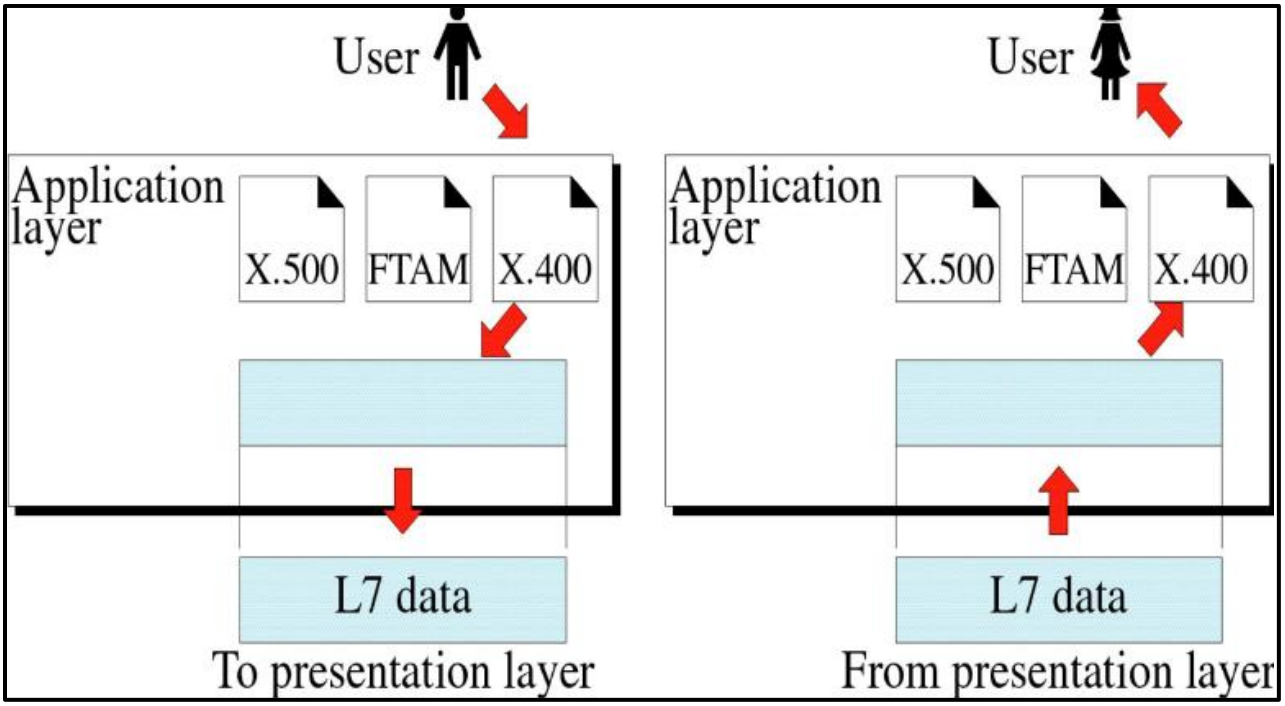
- ✓ EBCDIC (Extended Binary Coded Decimal Interchange Code) is an 8-bit character encoding (code page) used on IBM mainframe operating systems, like z/OS, OS/390, VM and VSE, as well as IBM minicomputer operating systems like OS/400 and i5/OS. It is also employed on various non-IBM platforms such as Fujitsu-Siemens' BS2000/OSD, HP MPE/iX, and Unisys MCP.
- ✓ Big Endian Byte Order: The most significant byte (the "big end") of the data is placed at the byte with the lowest address. The rest of the data is placed in order in the next three bytes in memory.
- ✓ Little Endian Byte Order: The least significant byte (the "little end") of the data is placed at the byte with the lowest address. The rest of the data is placed in order in the next three bytes in memory.





Functionality of the Application Layer:

- **Network Resource**: Prime responsibility of the application layer is to provide access to network resources. It contains the application protocols with which the user gains access to the network.
- **Mail Services**: This application provides various e-mail services.
- **File transfer & Access**: It allows users to access files in a remote host, to retrieve files from remote computer for use etc.
- **Remote log-in**: A user can log into a remote computer and access the resources of that computer.
- **Accessing the World Wide Web**: Most common application nowadays is the access of the World Wide Web.

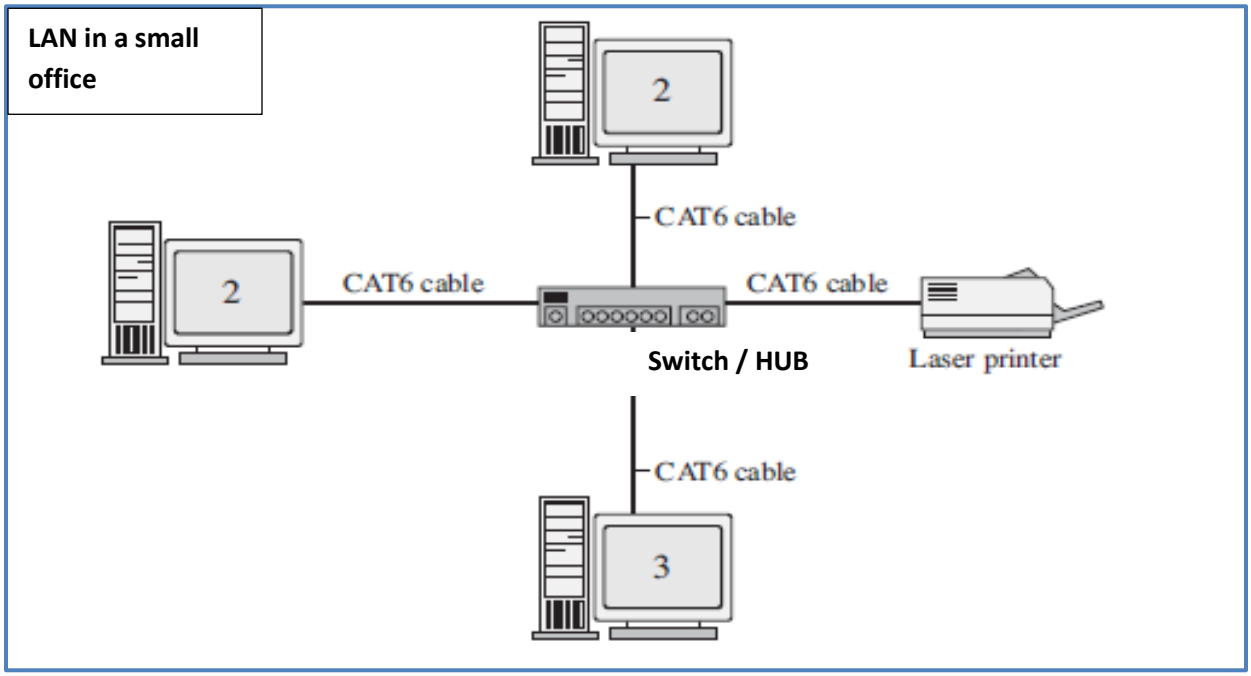


Categories of Network:

Three basic categories of computer networks on the basis of their size are: LAN, MAN and WAN. An area of a network is simply a network that spans a specific geographic area and serves a specific purpose. In a nutshell, a LAN, a WAN, and a MAN are basically all the same. The differences are the geographical area that each covers, as well as some of the communication protocols that are in use.

Local Area Network

A Local Area Network (LAN) is a group of computer and peripheral devices which are connected in a limited area, usually limited to a few kilometers of area such as school, Hospital, laboratory, Apartment, and office building. It is a widely useful network system for sharing resources like files, printers, games, and other applications. The simplest type of LAN network is to connect computers and a printer in someone's home or office. It is a network which consists of less than 5000 interconnected devices across several buildings.



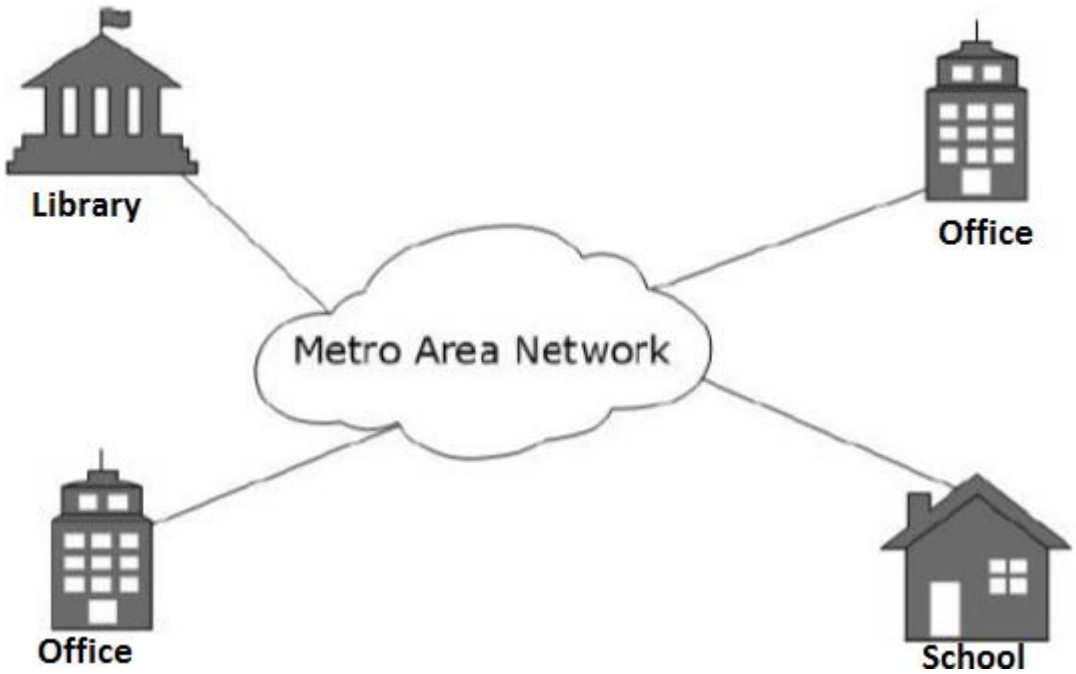
- LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.
- LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps.
- LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to function on a wireless connection.

Advantages of LAN

- Computer resources like hard-disks, DVD-ROM, and printers can be shared. This significantly reduces the cost of hardware component.
- We can use the same software over the network (i.e. network version) instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.
- The three major LAN technologies are Token Ring, Ethernet, and Fiber Distributed Data Interface (FDDI).

Metropolitan Area Network

Metropolitan Area Network (MAN) is of size between LAN and WAN. It is larger than LAN but smaller than WAN. It may comprise the entire network in a city like Kolkata. In Metropolitan area network various Local area networks are connected with each other through telephone or fiber-optic lines. MANs allow communication over a large geographical area, utilizing protocols such as ATM, FDDI, Fast Ethernet, or Gigabit Ethernet. This is a better solution than communication between LANs over a WAN, which relies on routing to decipher and allow communication of different protocol types between various area networks. Communication over a WAN is also slower and more expensive than what is offered by a MAN. MANs also provide control of the transmission of data from endpoint to endpoint, whereas the WAN solution requires that users have to rely on the service provider for a portion of the data flow control.



Characteristics of MAN

Important characteristics of MAN network:

- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers cables
- Data rates supported by MAN are adequate for distributed computing applications.

Advantages of MAN

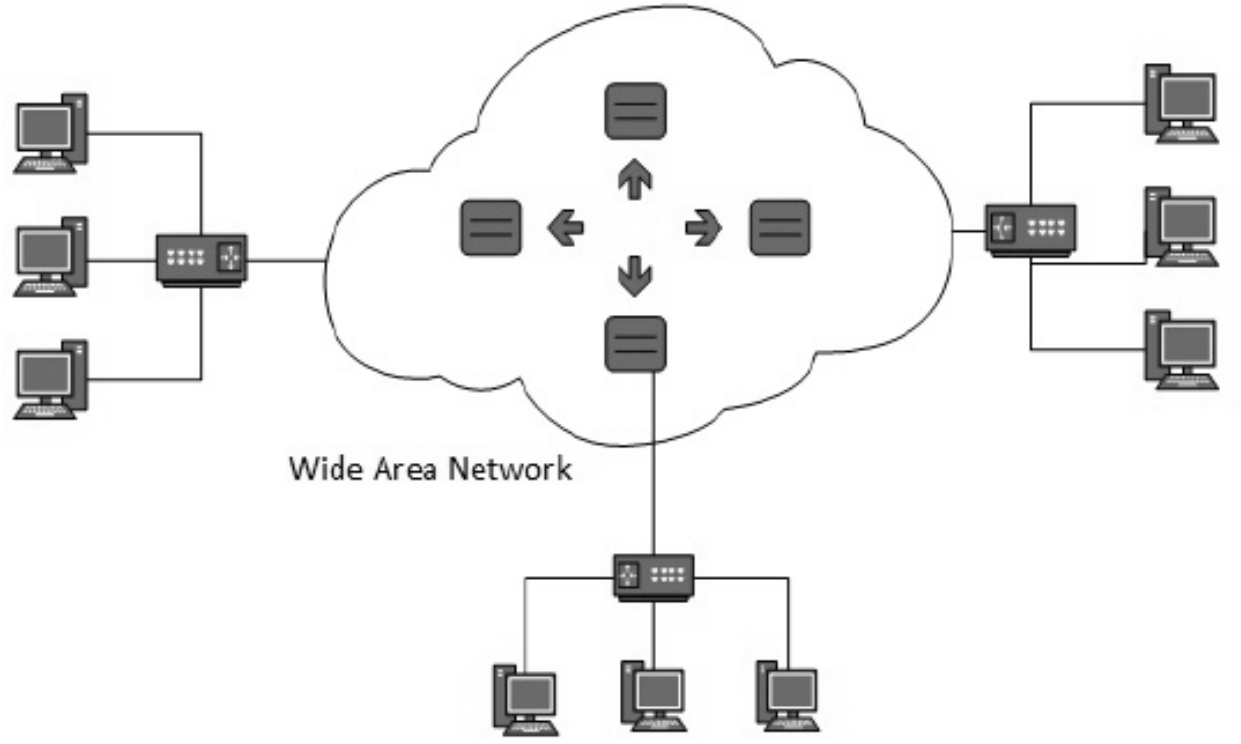
- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater access to WANs.
- The dual bus in MAN network provides support to transmit data in both directions concurrently.

Disadvantages of MAN

- Need more cable to setup MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers
- It is very difficult to manage if the size and number of LANs network increases. This is due to security and extra configuration problems.

Wide Area Network

Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone, WANs use very expensive network equipment.



Advantages of WAN

- **Centralized infrastructure**: One of the main advantage of WAN is the that we do not need to maintain the backup and store data on local system as everything is stored online on a data centre, from where we can centrally access the data through WAN.

- **Privacy**: We can setup the WAN in such a way that it encrypts the data that uses can share online such a way the data is secure and minimizes the risk of unauthorized access.

- **Increased Bandwidth**: With the WAN we get to choose the bandwidth based on the need, a large organization can have larger bandwidth that can carry large amount of data faster and efficiently.

- **Area:** A WAN can cover a large area or even a whole world though internet connection thus we can connect with the person in another country through WAN. Some communication protocols that are used on WANs to handle the transmission of data are: Asynchronous Transfer Mode (ATM), Frame relay, Packet over SONET (POS) and X.25.

Disadvantages of WAN:

- **Antivirus**: Since WAN user systems are connected with a large communication systems with heterogeneous devices and software, there is possibility that the user may unknowingly download the virus that can affect user's system and become a threat to the user's privacy and may lead to data loss. So Anti-virus software needs to be installed for the WAN users.
- **Expensive**: Cost of installation is very high.
- **Issue resolution**: Issue resolution takes time as the WAN covers large area, it is really difficult to pin point the exact location where the issues raised and causing the problem.

Some points to be remembered:

- ✓ Fault tolerance refers to the ability of a system (computer, network, cloud cluster, etc.) to continue operating without interruption when one or more of its components fail.
- ✓ Congestion refers to a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss and the blocking of new connections. In a congested network, response time slows with reduced network throughput. Congestion occurs when bandwidth is insufficient and network data traffic exceeds capacity.

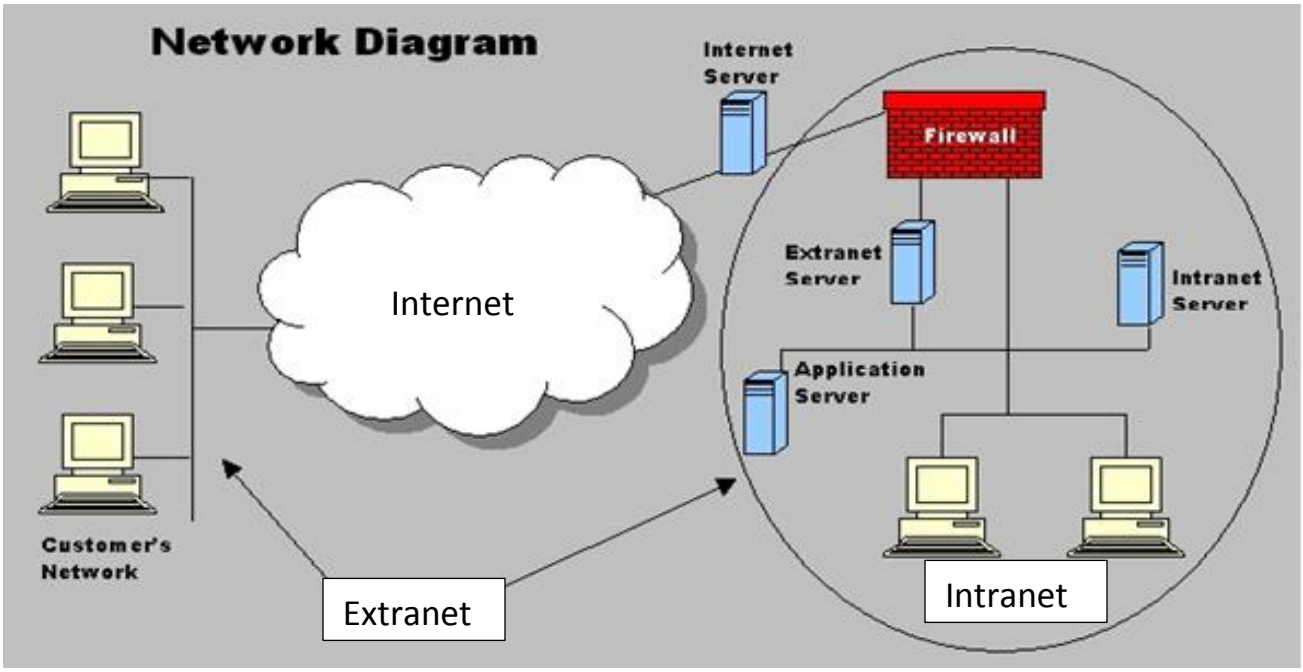
Following are the important differences between LAN, MAN and WAN.

Key-Terms	LAN	MAN	WAN
Definition	LAN stands for Local Area Network. It is a group of computers and peripheral devices which are connected in a limited area, usually limited to a few kilometers of area such as school, laboratory, home, and office building.	MAN stands for Metropolitan Area Network. It may comprise the entire network in a city like .Kolkata.	WAN stands for Wide Area Network. It is made of all the networks in a (geographically) large area. The network in the entire state of West Bengal could be a WAN.
Speed	LAN speed is quiet high.	MAN speed is average.	WAN speed is lower than that of LAN.
Delay	Network Propagation Delay is small in LAN.	Network Propagation Delay is moderate in MAN.	Network Propagation Delay is longer in WAN.
Congestion	LAN has low congestion as compared to WAN.	MAN has higher congestion than LAN.	WAN has higher congestion than both MAN and LAN.
Fault Tolerance	Fault Tolerance of LAN is higher than WAN.	Fault Tolerance of MAN is lower than LAN.	Fault Tolerance of WAN is lower than both LAN and MAN.
Maintenance	Designing and maintaining LAN is easy and less costly than WAN.	Designing and maintaining WAN is complex and more costly than LAN.	Designing and maintaining WAN is complex and more costly than both LAN and MAN.
Ownership	LAN is often owned by private organizations.	MAN ownership can be private or public.	WAN ownership can be private or public.

Intranet

An intranet is a private (LAN) computer network that uses Internet Protocol technologies to securely share information or operational systems within that organization. When an organization doesn't want to share some of its confidential or sensitive information in public domain, the information is normally shared through an intranet to its members (staff). So the members of the organization (staff) may access the intranet from their workplace. Security of the intranet is enforced through a firewall.

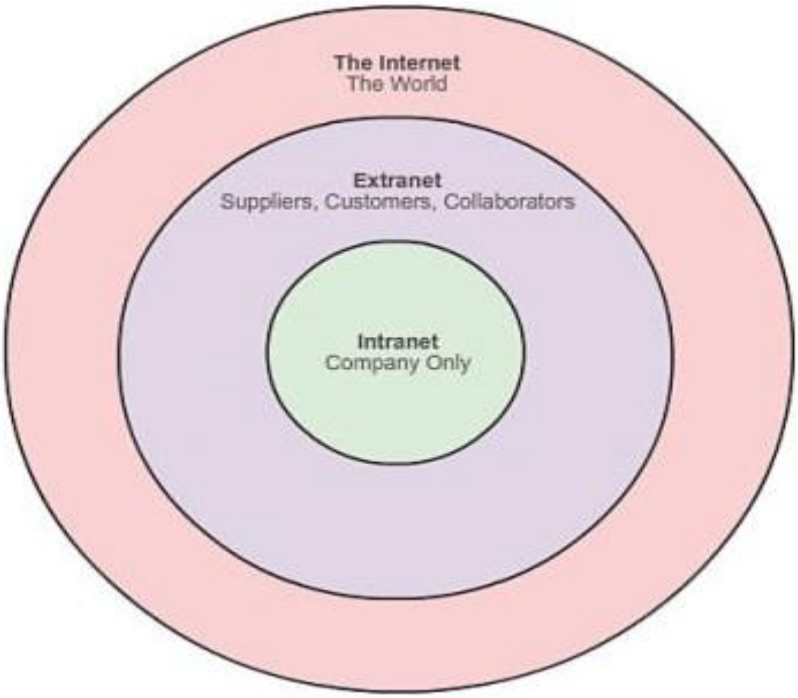
Depending on the structure of the intranet, staff (users) may also access the internal network with username and password from an internet-connected device by connecting remotely to the company's intranet. Usually a remote-access VPN (Virtual Private Network) is used for such a purpose to provide an encrypted and secure remote connection. An intranet can be used to facilitate working in groups for tele and video conferencing. Like internet, the intranet uses TCP/IP internet protocol for communication and it also allows the sharing of information via web browser. However, only approved computers can connect to the intranet and view the internal web pages.



Extranet

An extranet is a controlled private network which is an intranet that is opened up to allow outside users to access information, typically about a specific company or educational institution and the access normally is provided by a server to clients' through Internet. An extranet is often a private part of a website. It is restricted to selected users through user IDs, passwords and other authentication mechanisms on a login page. So an extranet network system requires security and privacy. These are included through firewall server management system using digital certificates or similar kinds of user authentication method or by encryption of messages or by tunneling through the public network using virtual private networks (VPNs).

Hence, an extranet is a kind an intranet with some additional control over it. Here some resources may be accessed by specific groups of users outside the organization under the control of the network administrator. For example, an organization may allow authorized customers to access about the product specifications, its availability, and its online ordering. A university or a college can allow distance learning students access to the computer Labs after authentication (userid and password) have been checked.



Internet

An Internet is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents, file sharing, electronic mail, telephony, FTP, audio and video streaming and applications of the World Wide Web (WWW). Internet uses very high speed backbone of fiber optics to inter-connect various continents and sometimes fibers are laid under the sea known as submarine communication cable.

Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page.

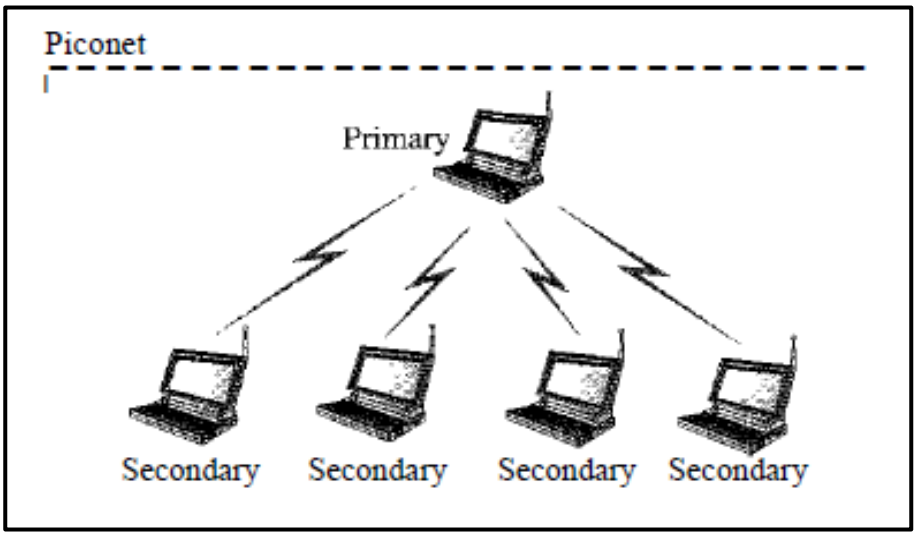
An **internet (lowercase i)** is a group of distinct networks connected to one another via a gateway. So Internet is a superset of internets or internet is a subset of Internet.

Bluetooth Networking

Bluetooth is a wireless LAN technology designed to connect devices of different functionality such as telephones, notebooks, computers (desktop and laptop), mobile phone, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there make a chaos. Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at a conference. Bluetooth was originally started as a project by the Ericsson Company. Architecture. Bluetooth defines two types of networks: piconet and scatternet.

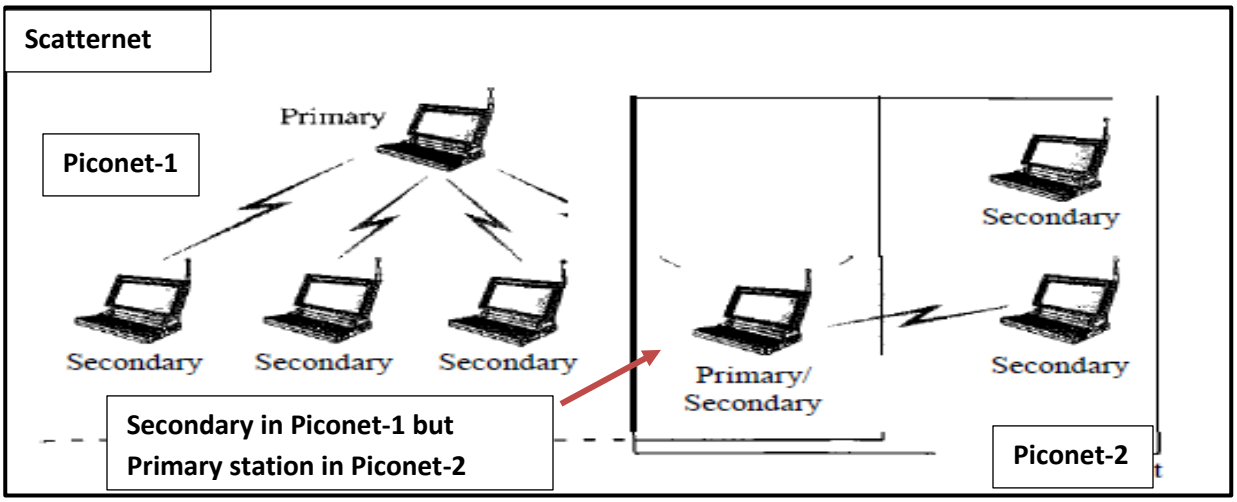
- ***Piconets***

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary and the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary but a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many.



❖ ***Scatternet***

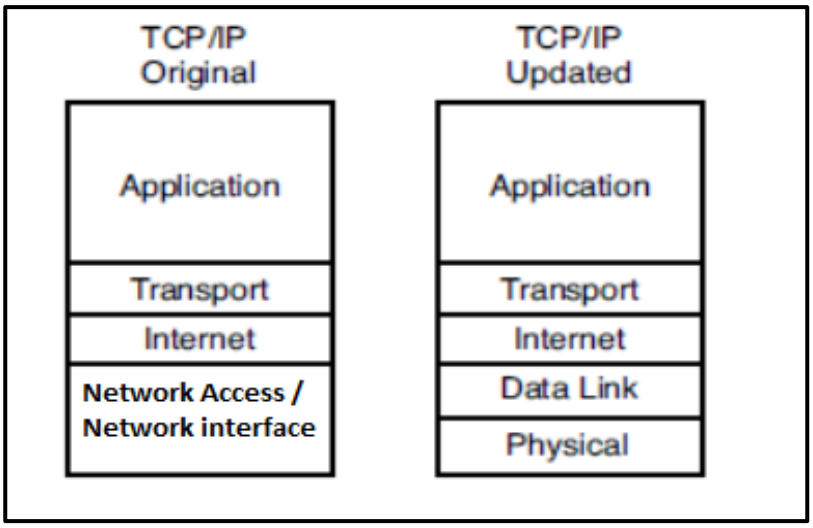
Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver the messages to secondaries in the second piconet. A station can be a member of two piconets.

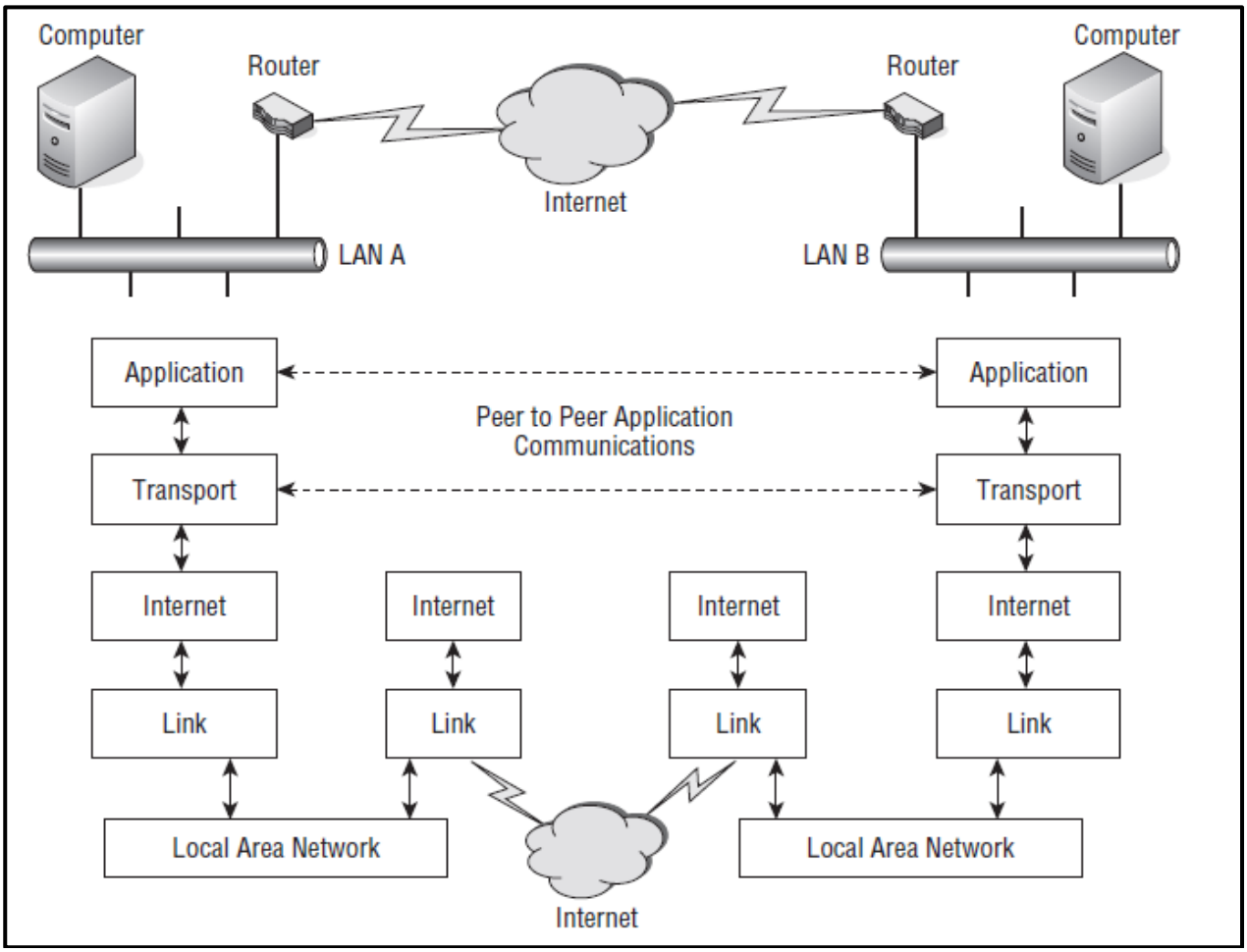


Introduction TCP/IP

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.

Modern TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.





The relationship between network elements and the TCP/IP network stack

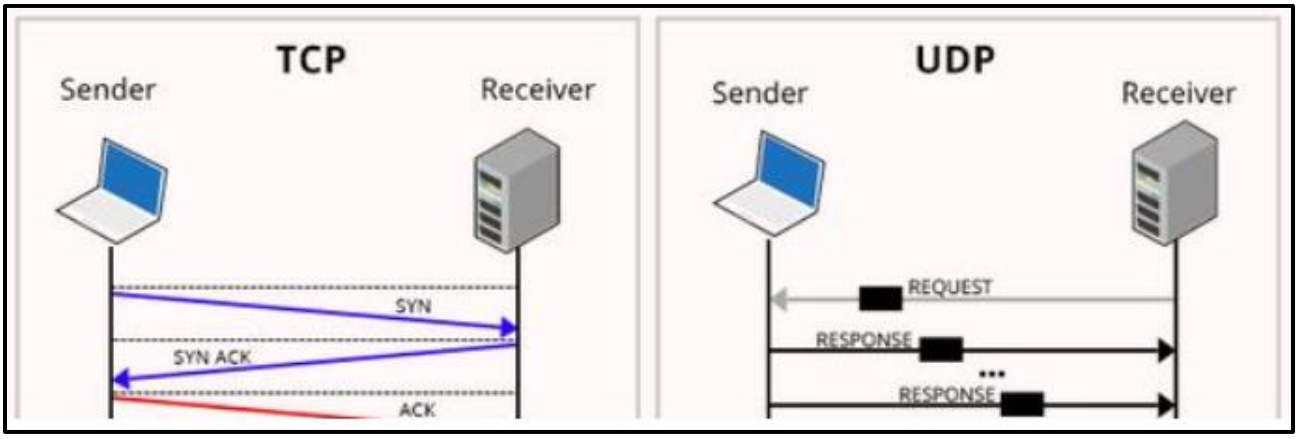
OSI Model	TCP/IP Model	TCP/IP Protocol Suite
Application Presentation Session	Application	Telnet, FTP, SMTP, DNS, SNMP
Transport	Transport	TCP, UDP
Network	Internet	IP, ICMP, ARP
Data Link Physical	Network Interface	Ethernet, ATM, Token Ring, Frame Relay

Name the layers of the TCP/IP reference model and responsibility is of each layer

- ***Network interface layer***: The network interface layer corresponds to the Physical and Data Link layers of the OSI reference model. This layer is also often referred to as the link layer. The network interface layer is responsible for the device drivers and hardware interfaces that connect a node to the transmission medium.
- ***Internet layer:*** The Internet layer corresponds to the Network layer of the OSI reference model. The Internet layer is responsible for the delivery of packets through a network. All routing protocols (RIP, OSPF, IP, etc.) are members of this layer. Nodes that perform functions at this layer are responsible for receiving a datagram, determining where to send it, and then forwarding it toward the destination. When a node receives a datagram that is destined for the node, this layer is responsible for determining the forwarding method for information that is in the packet. Finally, this layer contains protocols that send and receive error messages and control messages as required.
- **Transport layer:** The transport layer corresponds to the Transport layer of the OSI reference model. There are two primary protocols that operate at this layer. These are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). TCP provides full transport-layer services to applications. It is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data. At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.
- **Application layer**: The top level of the TCP/IP stack is the application layer. This layer is used to process requests from hosts and make sure a connection is made to an appropriate port. A port is basically an address used to direct data to the proper destination application. Application layer in the TCP/IP reference model assumes most of the functions performed by the Session and Presentation layers of the OSI reference model. All upper-layer protocols are handled at this layer.

User Datagram Protocol (UDP)

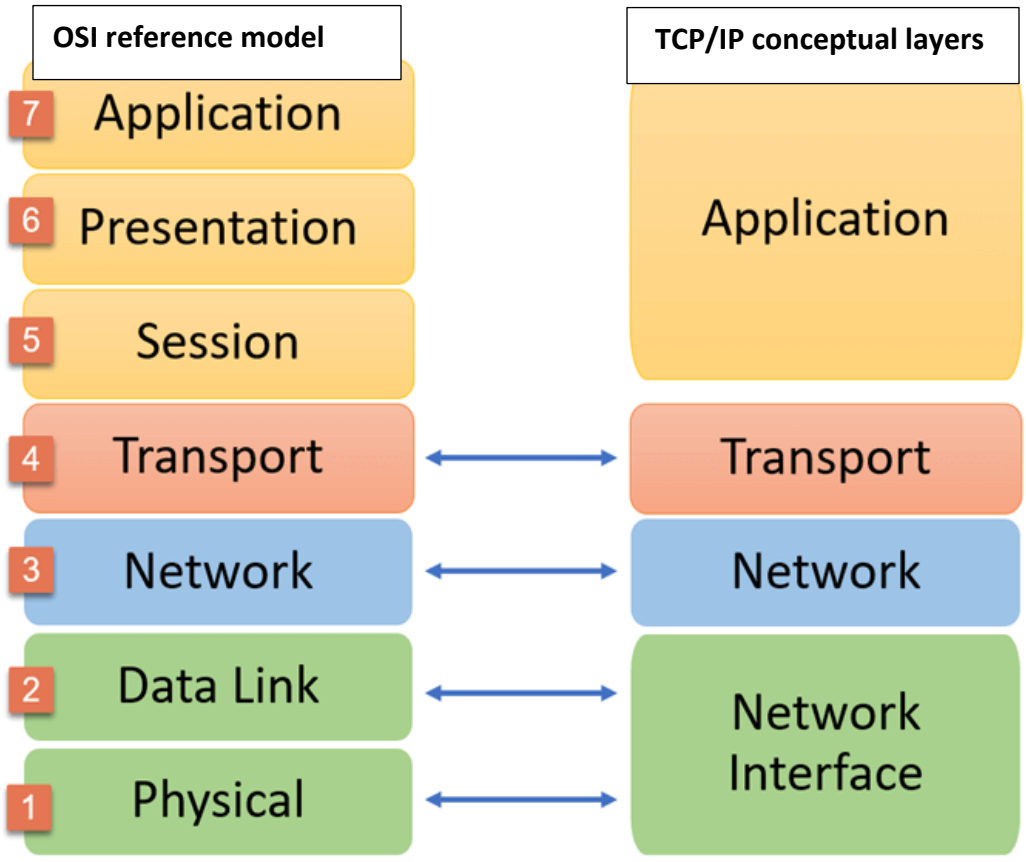
User Datagram Protocol is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer. It is a connectionless protocol. This means UDP packets are transported over the network without a connection being established and without any acknowledgement that the data packets arrived at the destination. UDP is useful in applications such as videoconferencing and audio feeds, where such acknowledgements are not necessary. UDP does not have a procedure for terminating the data transfer; the source either stops delivery of the data packets or the client terminates the connection.



Comparison TCP and UDP protocol

Features	TCP	UDP
Basic Function	Transmission Control Protocol needs to establish a connection between the computers before transmission the data	User Datagram Protocol sends the data directly to the destination computer without checking whether the system is ready to receive or not
Connection Type	Connection Oriented	Connection Less
Speed	Slow	Fast
Reliability	Highly Reliable as it sends acknowledgement of data and has retransmission ability.	Unreliable as neither takes acknowledgement nor it retransmits the lost data.
Header Size	20 Bytes	8 Bytes
Protocol connection setup	Connection-oriented, the connection must be established prior to transmission	Connectionless, data is sent without setup
Data interface to the application	Stream-based	Message-based
Features provided to manage the flow of data	Flow control using sliding window protocol	No flow control mechanism
Implemented over	Applications where reliable transmission of data matters.	Application where data delivery speed matters.
Applications and protocols	FTP, Telnet, SMTP, IMAP etc.	DNS, BOOTP, DHCP, TFTP etc.

Comparison between OSI and TCP/IP model

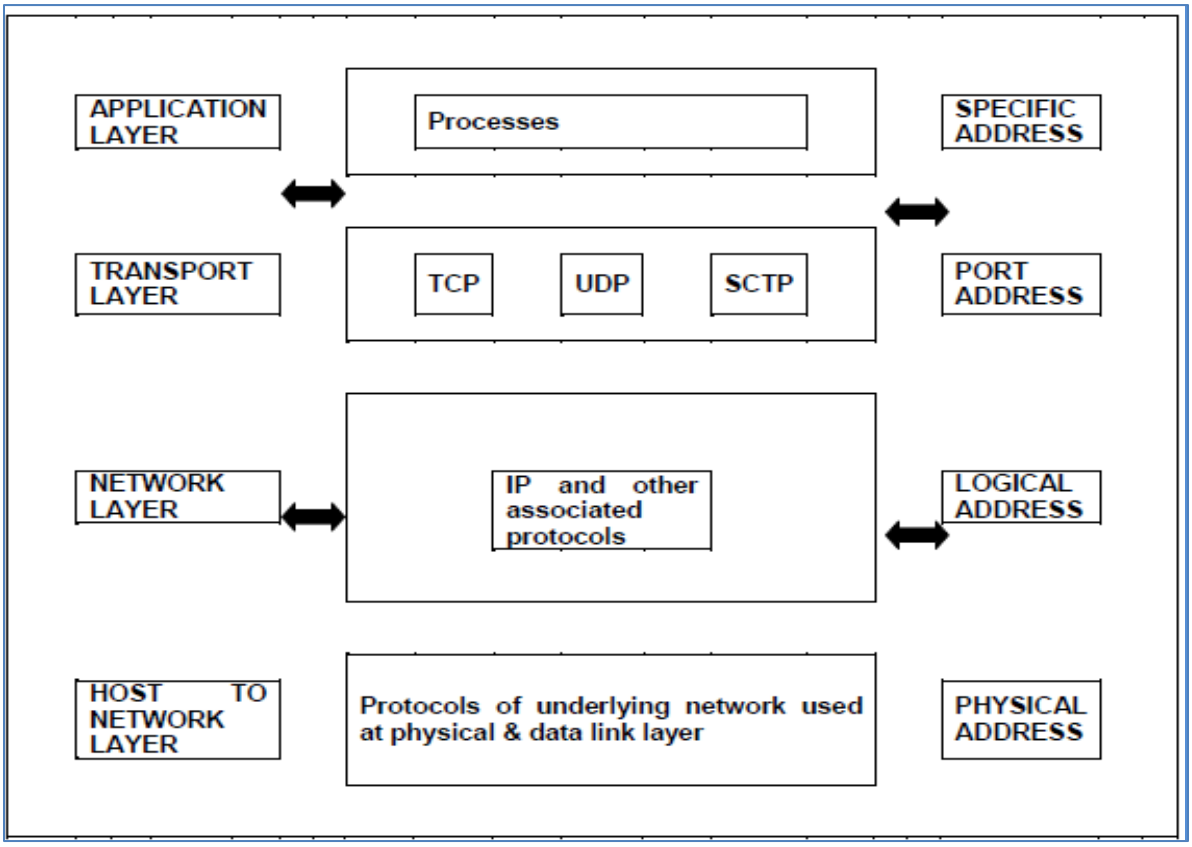


Here are some important comparisons between the OSI and TCP/IP model:

OSI Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.
In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	The minimum header size is 20 bytes.

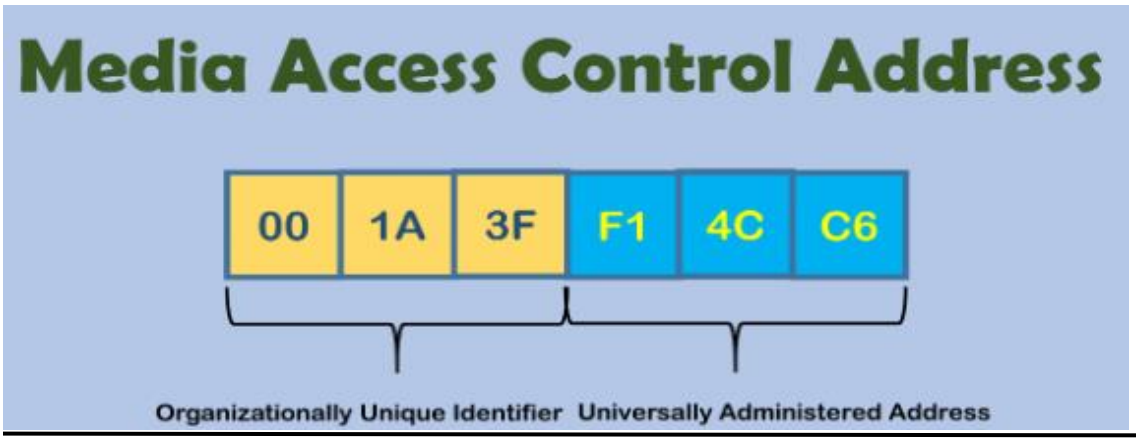
The TCP/IP protocol suited involves 4 different types of addressing:

1. Physical Address
2. Logical Address
3. Port Address
4. Specific Address



Physical Address or MAC address or Ethernet address

- Physical Address is the lowest level of addressing, also known as link address.
- It is local to the network to which the device is connected and unique inside it.
- The physical address is usually included in the frame and is used at the data link layer.
- MAC is a type of physical address that is 6 byte (48 bit) in size and is imprinted on the Network Interface Card (NIC) of the device.
- The size of physical address may change depending on the type of network. For example, an Ethernet network uses a 6 byte MAC address.



Logical Address or IP address

- Logical Addresses are used for universal communication.
- Most of the times the data has to pass through different networks; since physical addresses are local to the network there is a possibility that they may be duplicated across multiples networks also the type of physical address being used may change with the type of network encountered. For ex: Ethernet to wireless to fiber optic. Hence physical addresses are inadequate for source to destination delivery of data in an internetwork environment.
- Logical Address is also called as IP Address (Internet Protocol address).
- At the network layer, device i.e. computers and routers are identified universally by their IP Address.
- IP addresses are universally unique.
- Currently there are two versions of IP addresses being used:
  - IPv4: 32 bit address, capable of connecting 2^{32} nodes
  - IPv6: 128 bit address, capable of connecting 2^{128} nodes

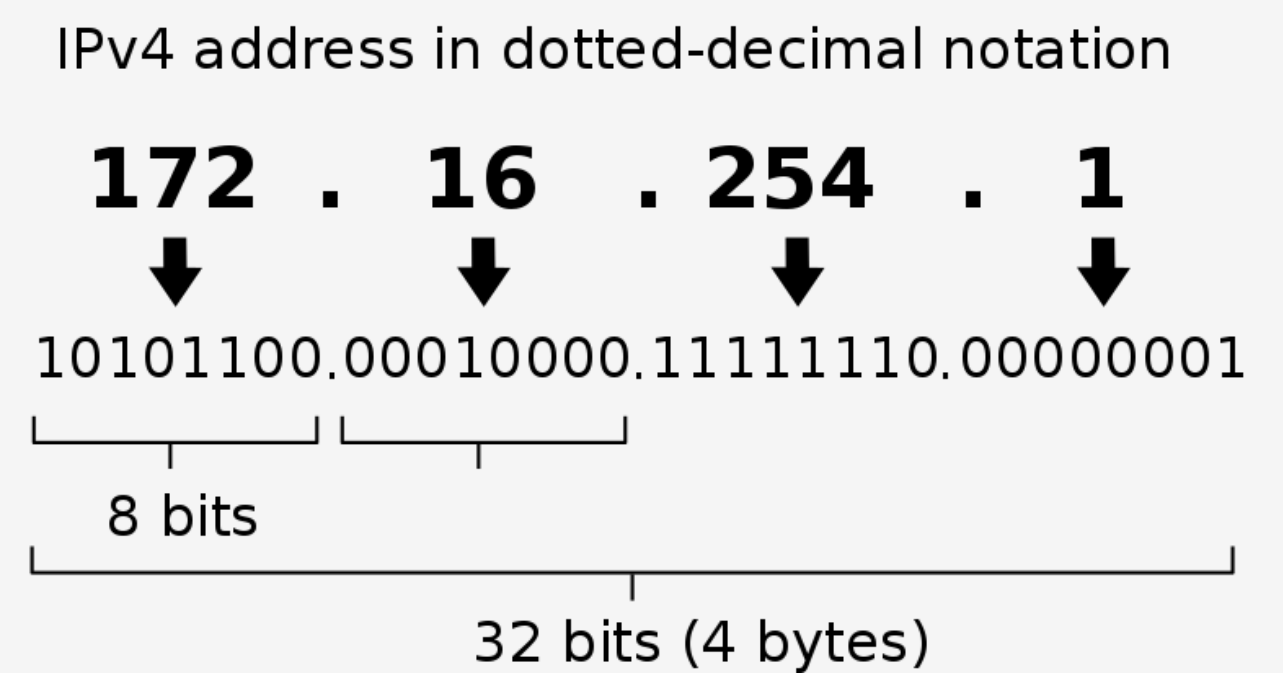
Notations: There are two type of notations used in IPv4 address:

1. Binary notation

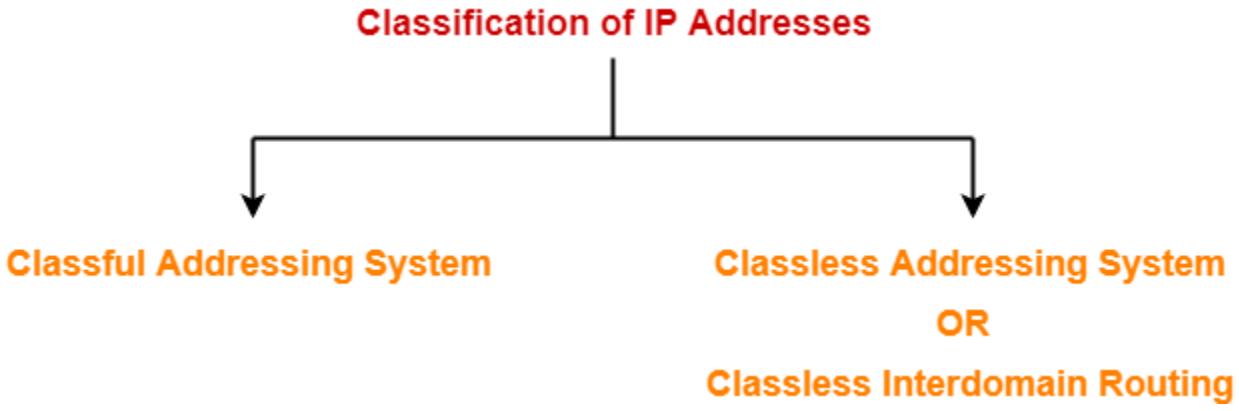
The IPv4 address is displayed as 32 bits. ex. 11000001 10000011 00011011 11111111

2. Dotted decimal notation

To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value ranging from 0 to 255. Ex. 129.11.11.239



There are two systems in which IP Addresses:



Classful addressing: In classful addressing, the address space is divided into five classes: **A, B, C, D, and E.**

Address Class	Bit Pattern of First Byte	First Byte Decimal Range	Host Assignment Range in Dotted Decimal
A	0xxxxxxx	1 to 127	1.0.0.1 to 126.255.255.254
B	10xxxxxx	128 to 191	128.0.0.1 to 191.255.255.254
C	110xxxxx	192 to 223	192.0.0.1 to 223.255.255.254
D	1110xxxx	224 to 239	224.0.0.1 to 239.255.255.254
E	11110xxx	240 to 255	240.0.0.1 to 255.255.255.255

Specific bit pattern in the first byte of an IP address corresponds to a range of addresses and maps to a specific address class.

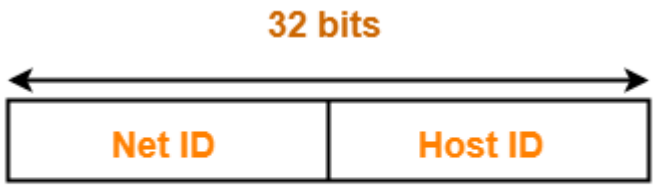
First three classes A, B, and C — were designated for unicast single source–to–single destination communication. Addresses in Class D were reserved for IP Multicast applications, which allows one-to-many communication. Class E addresses were reserved for experimental purposes.

To make the addresses in each of the unicast address classes (A, B, and C) support a specific maximum number of hosts, the 32-bit address field was delineated into network identifier (network ID) bits and host identifier bits (host ID) as follows:

- Class A— 8-bit network ID, 24-bit host ID
- Class B— 16-bit network ID, 16-bit host ID
- Class C— 24-bit network ID, 8-bit host ID

The order of bits in the first octet determine the classes of IP address. Accordingly, IPv4 address is divided into two parts:

- Network ID
- Host ID



Format of an IP Address

Public IP Address Classes range

Class	1st Octet DEC range	1st Octet BIN	Start address	Finish address	1st Octet High order Bits	Network/ Host	Default Subnet Mask
A	1-126	00000001-01111110	0.0.0.0	126.255.255.255	0	N.H.H.H	255.0.0.0
B	128-191	10000000-10111111	128.0.0.0	191.255.255.255	10	N.N.H.H	255.255.0.0
C	192-223	11000000-11011111	192.0.0.0	223.255.255.255	110	N.N.N.H	255.255.255.0
D	224-239	11100000-11101111	224.0.0.0	239.255.255.255	1110		
E	240-255	11110000-11111111	240.0.0.0	254.255.255.255	11110		

Note: Class A address **127.0.0.0 - 127.255.255.255** cannot be used and is for **LOOPBACK** and diagnostic

Private IP Address Classes range

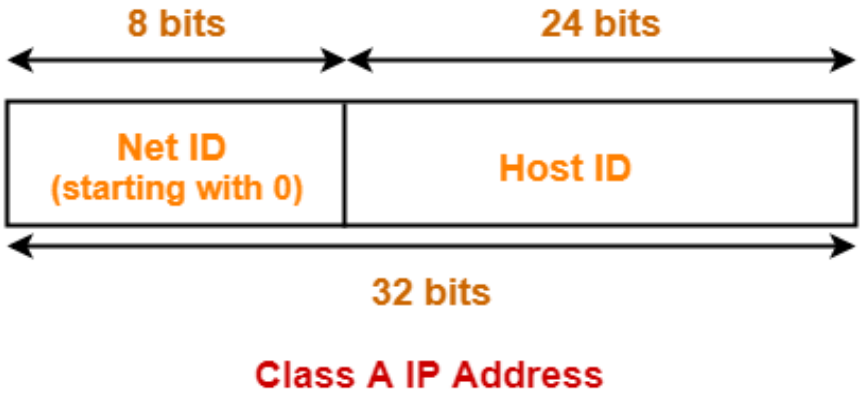
Class	1st Octet DEC range	1st Octet BIN	Start address	Finish address	1st Octet High order Bits	Network/ Host	Default Subnet Mask
A	10	00001010	10.0.0.0	10.255.255.255	0	N.H.H.H	255.0.0.0
B	172	10101100	172.16.0.0	172.31.255.255	10	N.N.H.H	255.255.0.0
C	192	11000000	192.168.0.0	192.168.255.255	110	N.N.N.H	255.255.255.0

Class	Range	Network / Hosts
A	1 to 126	N . H . H. H
B	128 to 191	N . N . H . H
C	191 to 223	N . N . N . H
D	224 to 239	Reserved for Multitasking
E	240 to 254	Experimental, reserved for research

Class A

IP addresses belonging to class A are assigned to the networks that contain a large number of hosts. If the 32 bit binary address starts with a bit 0, then IP Address belongs to class A.

- The network ID is 8 bits long.
- The host ID is 24 bits long.



Class A IP Address

So the higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total

2^7-2= 126 network ID (Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address.)

2^{24}– 2 = 16,777,214 host ID

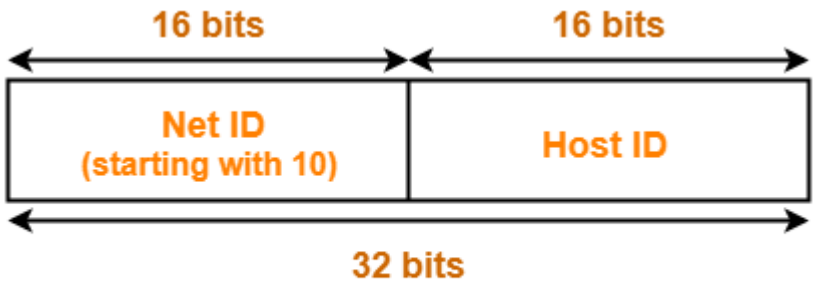
IP addresses belonging to class A ranges from **1.x.x.x – 126.x.x.x**

Use: Class A is used by organizations requiring very large size networks like NASA, Pentagon etc.

Class B:

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks. If the 32 bit binary address starts with bits 10, then IP Address belongs to class B.

- The network ID is 16 bits long.
- The host ID is 16 bits long.



Class B IP Address

So the higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total

2^{14} = 16384 network address

2^{16} – 2 = 65534 host address

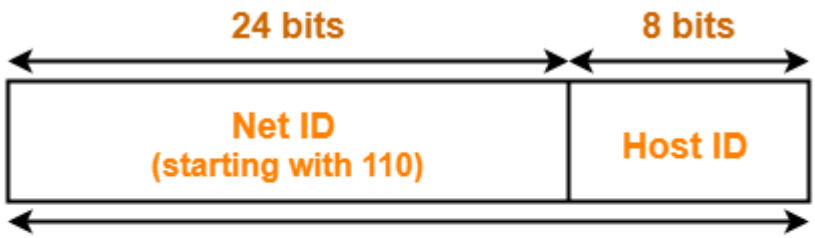
IP addresses belonging to class B ranges from **128.0.x.x – 191.255.x.x**.

Use: Class B is used by organizations requiring medium size networks like IRCTC, banks etc.

Class C

IP address belonging to class C are assigned to small-sized networks. If the 32 bit binary address starts with bits 110, then IP Address belongs to class C.

- The network ID is 24 bits long.
- The host ID is 8 bits long.



Class C IP Address

So the higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

2^{21}= 2097152 network address

2^{8}– 2 = 254 host address

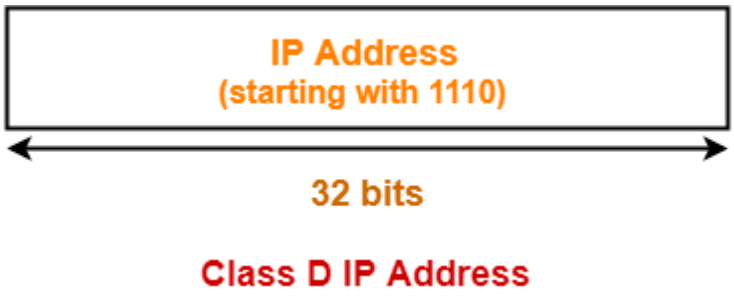
IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

Use:

- ✓ Class C is used by organizations requiring small to medium size networks.
- ✓ For example- engineering colleges, small universities, small offices etc.

Class D

IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.



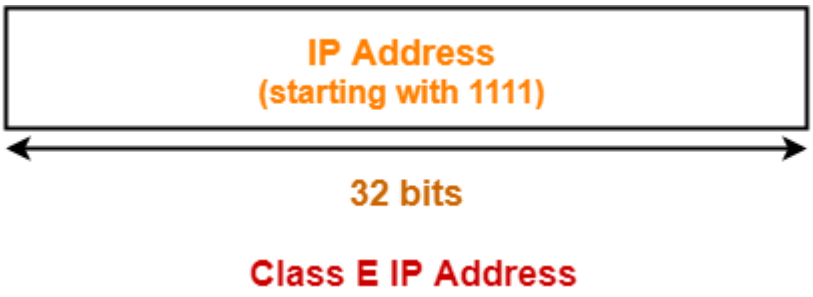
Class D does not possess any sub-net mask. IP addresses belonging to class D ranges from **224.0.0.0 to 239.255.255.255.**

Use:

- ✓ Class D is reserved for multicasting.
- ✓ In multicasting, there is no need to extract host address from the IP Address.
- ✓ Class D data is not destined for a particular host.

Class E

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from **240.0.0.0 to 255.255.255.254**. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Use: Class E is reserved for future or experimental purposes.

Range of special IP addresses:

- ✓ 169.254.0.0 to 169.254.0.16 : Link local addresses
- ✓ 27.0.0.0 to 127.0.0.8 : Loop-back addresses
- ✓ 0.0.0.0 to 0.0.0.8 : used to communicate within the current network.

Rules for assigning Host ID:

- ❖ Host ID's are used to identify a host within a network. The host ID are assigned based on the following rules:
  - ♦ Within any network, the host ID must be unique to that network.
  - ♦ Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
  - ♦ Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for assigning Network ID:

- ❖ Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:
  - ♦ The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
  - ♦ All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
  - ♦ All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Classes of IP Address

All the classes of IP Address are summarized in the following table

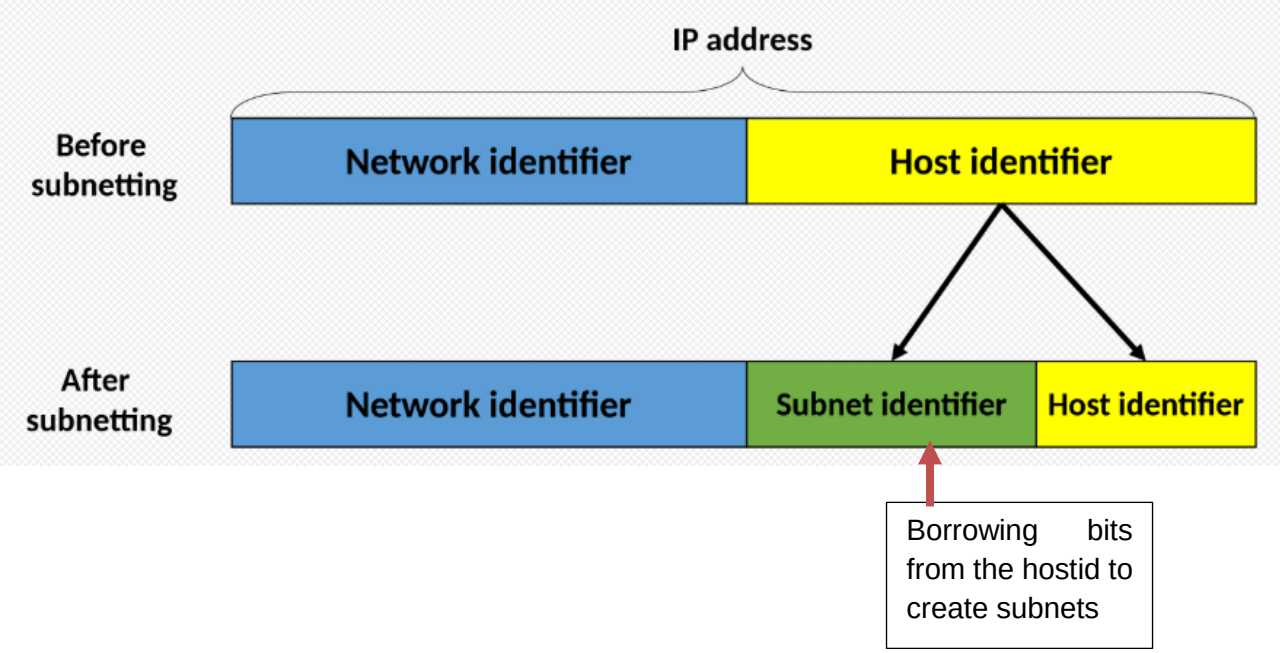
Class of IP Address	Total Number of IP Addresses	1st Octet Decimal Range	Number of Networks available	Hosts per network	Default Subnet Mask
Class A	2^{31}	1 – 126	$2^{7} – 2$	$2^{24} – 2$	255.0.0.0
Class B	2^{30}	128 – 191	2^{14}	$2^{16} – 2$	255.255.0.0
Class C	2^{29}	192 – 223	2^{21}	$2^{8} – 2$	255.255.255.0
Class D	2^{28}	224 – 239	Not defined	Not defined	Not defined
Class E	2^{28}	240 – 254	Not defined	Not defined	Not defined

Subnetting and Supernetting

Computer networks can be broken into many networks or small networks and it could be combined to form large networks depending upon our need. This is done by IP subnetting and supernetting.

Subnetting

Dividing the network into smaller contiguous networks or subnets is called subnetting. Thus Subnetting is a technique used to break (or partition) networks into subnets. ***The subnets are created through the use of subnet masks.*** The subnet mask identifies what bits in the IP address are to be used to represent the network / subnet portion of an IP address. ***Subnets are created by borrowing bits from the host portion of the IP address.*** This is shown in below Figure:



Advantages of subnetting

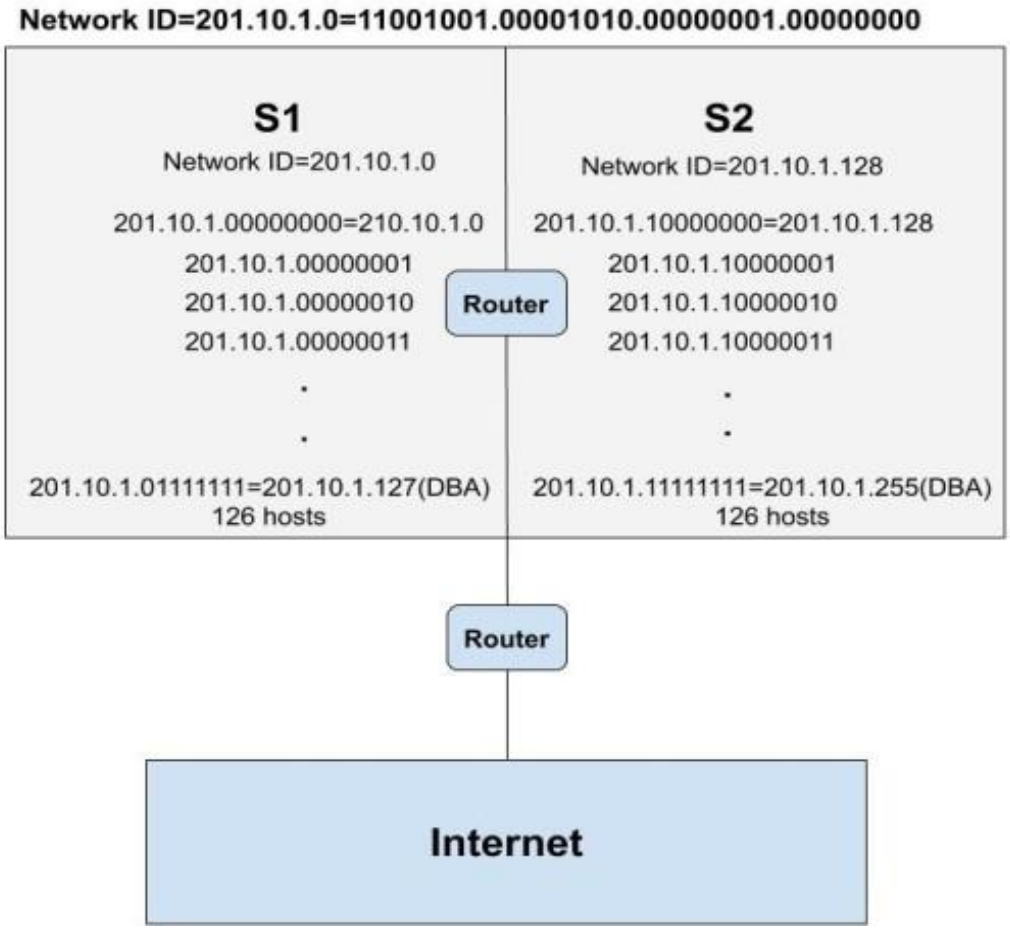
Suppose we take a network of class A. where 2^{24} hosts are present. Now to manage such a large number of hosts is very tedious and complex job. So if we divide this large network into the smaller networks then maintaining each network would be very easy.

How we can do subnetting ?

Suppose we have a class C network having network ID as 201.10.1.0. So the total number of hosts is 256(for class C host is defined by last octet i.e. 2^8). But, the total usable host is 254. This is because the first IP address is for the network ID and the last IP address is Direct Broadcast Address (for sending any packet from one network to all other hosts of another network).

So, in subnetting we will divide these 254 hosts logically into two networks. In the above class C network, we have 24 bits for Network ID and the last 8 bits for the Host ID. We are going to borrow the left-most bit of the host address and declare for identifying the subnet. If the leftmost bit of the host address is 0 then it is the 1st subnet network and if the leftmost bit is 1 then it would be 2nd subnet network. Using 1 bit we can divide it into 2 networks i.e. 2^1. If we want to divide it into four networks then we need 2 bits (2^2 = 4 networks).

So, the range of IP address which is in 1st subnet network is from 201.10.1.0 to 201.10.1.127. The range of IP address that lies in the 2nd subnet network is from 201.10.1.128 to 201.10.1.255.



In the 1st subnet network (S1), we have a total of 126 hosts only because the first and last IP address is reserved for the network ID and the Direct Broadcast Address respectively. Similarly, in the 2nd subnet network, we have 126 hosts.

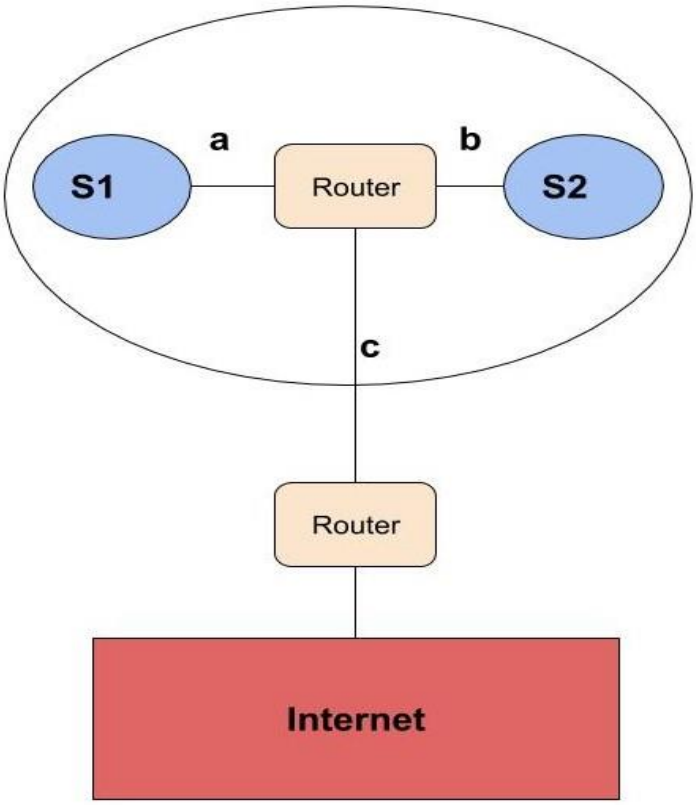
Overall, there are 252 usable hosts after subnetting. So, because of subnetting, there is a loss in the number of IP addresses. The subnet mask is represented as 11111111.11111111.11111111.10000000 i.e. 255.255.255.128 for the above network.

The router inside the network will have the routing table which will be as follows:

Network ID	Subnet Mask	Interface
201.10.1.0	255.255.255.128	a
201.10.1.128	255.255.255.128	b

Routing Table

This network will have two subnets as in the diagram below:



Supernetting or Aggregation

It is the opposite of Subnetting. Here multiple smaller networks are combined together to form a large network.

Sub netting	Super netting
A process of dividing a network into the sub networks.	A process of combining small networks into a larger network.
The number of bits of network addresses is increased.	The number of bits of host addresses is increased.
Mask bits are moved towards right of the default mask.	Mask bits are moves towards left of the default mask.
Sub netting is implemented using VLSM (variable length subnet mask)	Super netting is implemented using CIDR classless inter domain routing.
The objective is to reduce the address depletion.	The objective is to simplify and fasten the routing process.

Domain name service / system (DNS): DNS server translates a human readable name to an IP address or an IP address to a domain name. The translation of a name to an IP address is called forward domain name service, and translation of an IP address to a domain name is called reverse domain name service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers. So DNS resolution involves converting a hostname (such as www.webscte.org) into a computer IP address (say 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the particular Internet device.

Domain: There are various kinds of Domain:

1. **Generic domain**: **.**com (commercial), .edu (educational), .mil (military), .org (non-profitable organization), .net (similar to commercial) all these are generic domain.
2. **Country domain** .in (india) .us .uk.
3. **Inverse domain**: if we want to know what is the domain name of the website then IP to domain name mapping is performed. So DNS can provide both the mapping. For example to find the IP address of www.google.co.in, we have to type **nslookup** command.

C:\> nslookup

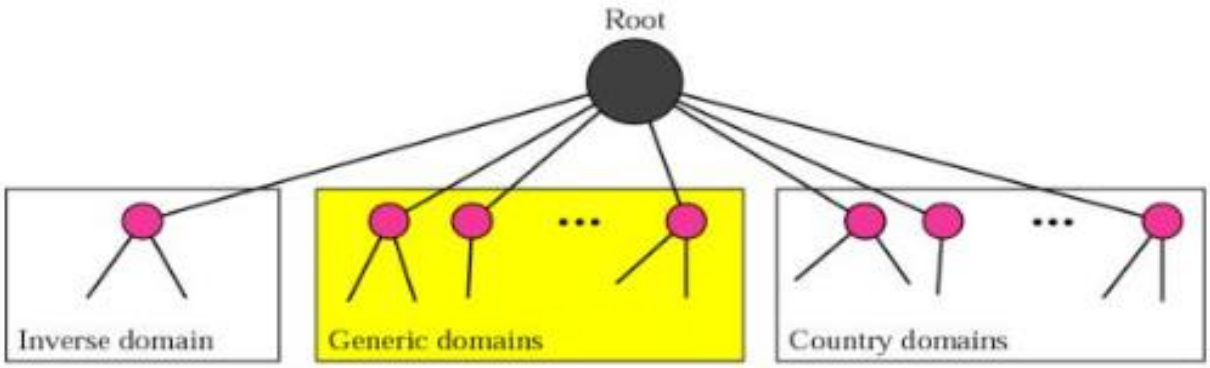
Output

Name: www.google.co.in ← Domain name

Addresses: **2404:6800:4009:80b::2003** ← **IPv6**

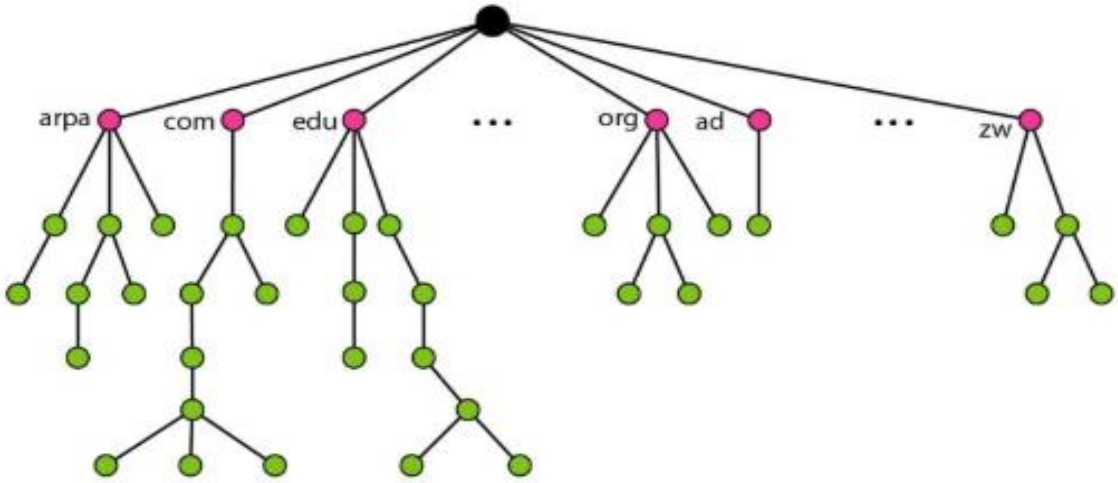
172.217.160.195 ← IPv4

DNS in the Internet

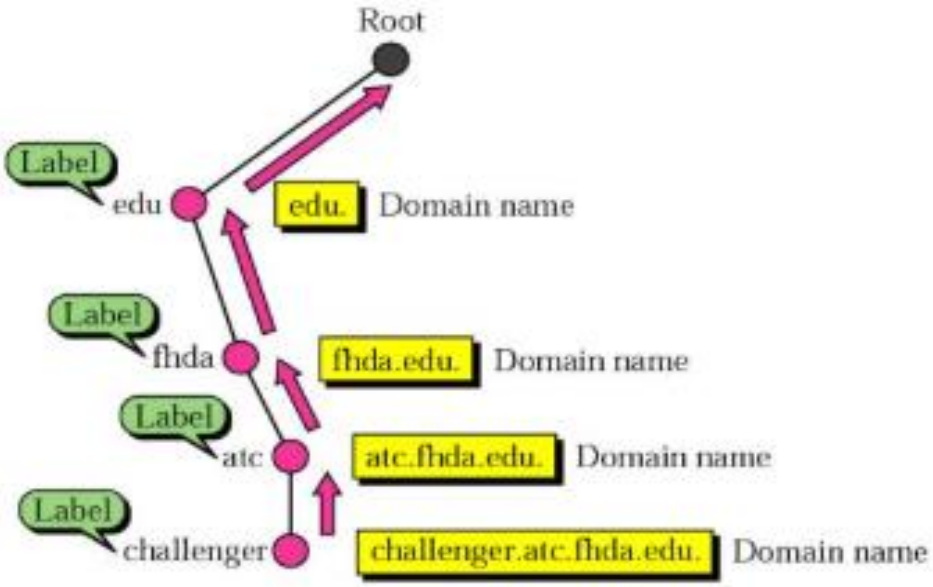


Domain name space

- Flat name space, Hierarchical name space



Domain names and labels



Domain name is of two types:

FQDN and PQDN

- FQDN (Fully Qualified Domain Name)
- PQDN (Partially Qualified Domain Name)

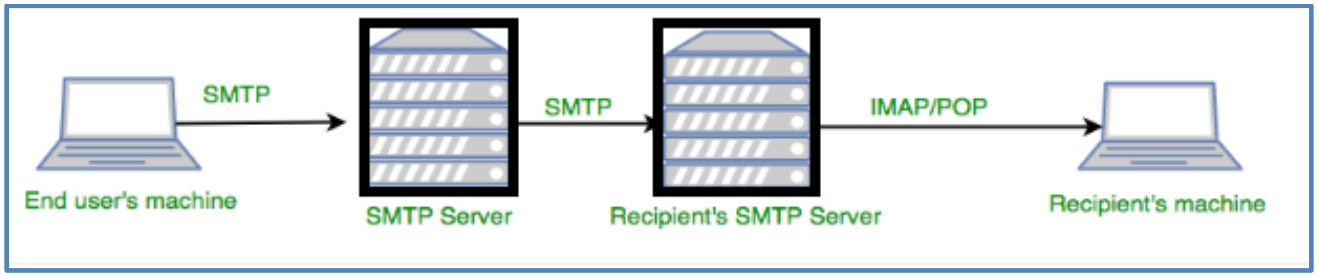
FQDN	PQDN
challenger.atc.fhda.edu. cs.hmme.com. www.funny.int.	challenger.atc.fhda.edu cs.hmme www

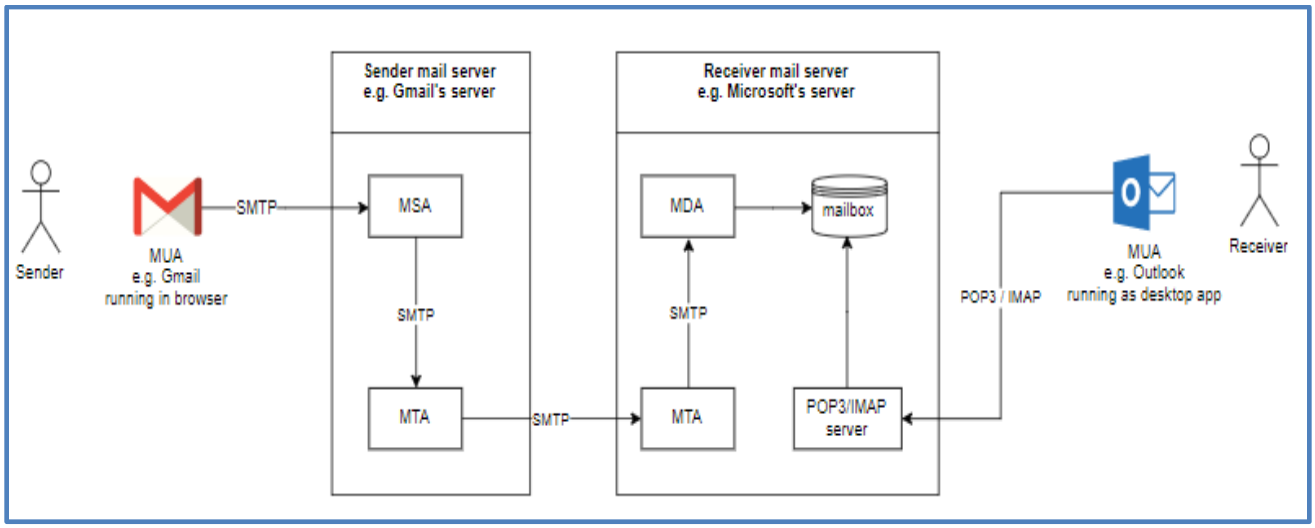
Resolution

- Name-address resolution: a name to address/an address to a name
- Resolver: DNS client called by a host
- Recursive resolution and iterative resolution

Email

Electronic mail (email, e-mail, eMail or e-Mail) is a method of exchanging messages ("mail") between people using electronic devices. Electronic mail is probably the most widely used TCP/IP application in the Internet community today. There are different components involved in an email transmission from sender to recipient.





❖ MUA (Mail User Agent)

A mail user agent (MUA) is a program that allows us to receive and send e-mail messages. It can be software applications, such as Outlook Express and Lotus notes, or they can be webmail services such as those provided by Yahoo!, Microsoft Outlook.com, and Gmail. MUAs are the component within the Simple Mail Transfer Protocol (SMTP) system responsible for creating email messages for transfer to a Mail Transfer Agent (MTA).

❖ MSA (Mail Submission Agent)

A server program that receives mail from an MUA, checks for any errors, and transfers it (with SMTP) to the MTA hosted on the same server.

❖ **MTA (Mail Transfer Agent)**

A server application that receives mail from the MSA, or from another MTA. It will find (through name servers and the DNS) the MX (Mail Exchange) record from the recipient domain's DNS zone in order to know how to transfer the mail. It then transfers the mail (with SMTP) to another MTA (which is known as SMTP relaying) or, if the recipient's server has been reached, to the MDA. Examples of MTAs are Postfix, Exim, Sendmail, qmail.

❖ **MDA (Mail Delivery Agent)**

A server program that receives mail from the server's MTA, and stores it into the mailbox. MDA is also known as LDA (Local Delivery Agent).An example is Dovecot, which is mainly a POP3 and IMAP server allowing an MUA to retrieve mail, but also includes an MDA which takes mail from an MTA and delivers it to the server's mailbox.

❖ **SMTP**

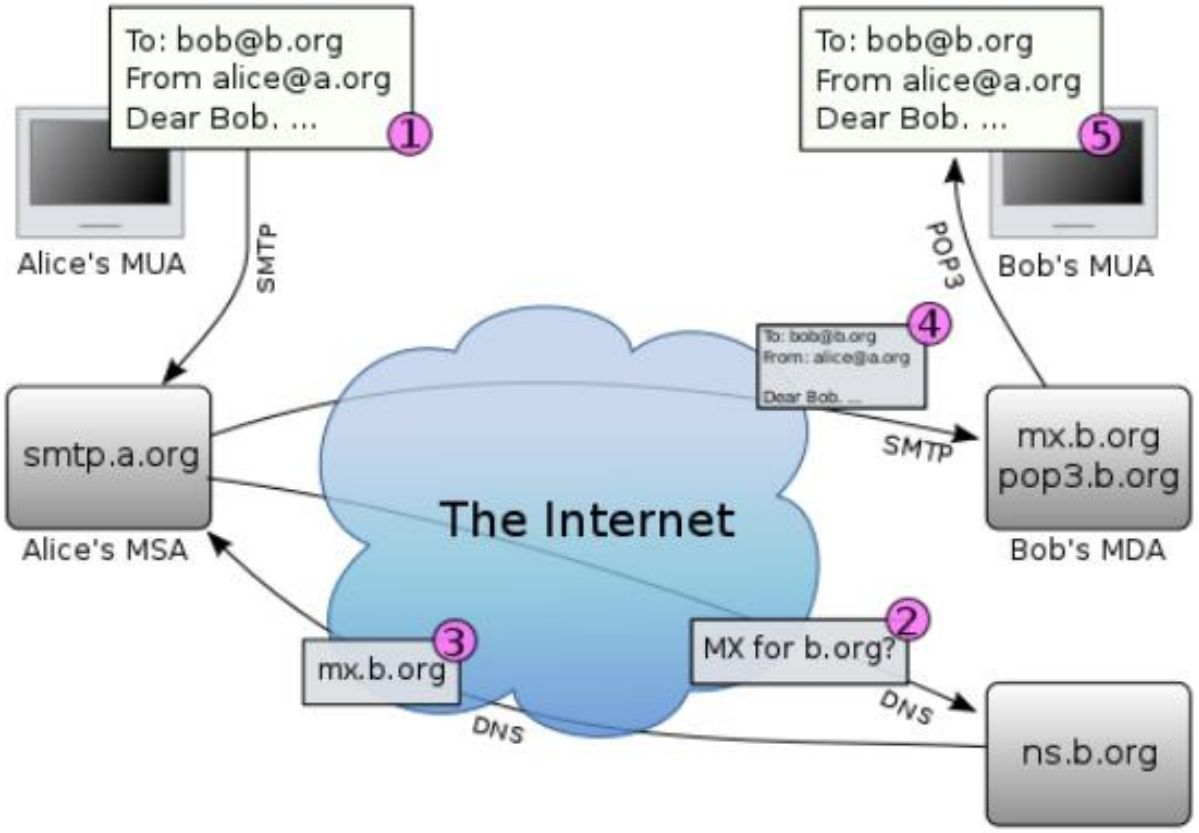
SMTP Protocol is used by MUAs to send emails to an MSA. The recommended SMTP port for sending mail (from an MUA to an MSA) is the port 587, which uses TLS (Transport Layer Security) encryption.

❖ **IMAP/POP3**

IMOP and POP3 Protocols are used by MUAs to retrieve emails from a server mailbox. POP3 deletes the email messages from the server after they have been downloaded. IMAP is usually preferable as it maintains all email messages on the server, permitting management of a mailbox by multiple email clients.

Other Features:

- We can send files along with our emails by using the Attachment feature. This is a common way of sending longer documents, spreadsheets, photographs etc. to other people.
- The CC (Carbon Copy) function lets us send a copy of the email to other people.
- The BCC (Blind Carbon Copy) function also lets you send a copy of the email to other people. This function hides the names of the recipients from each other.

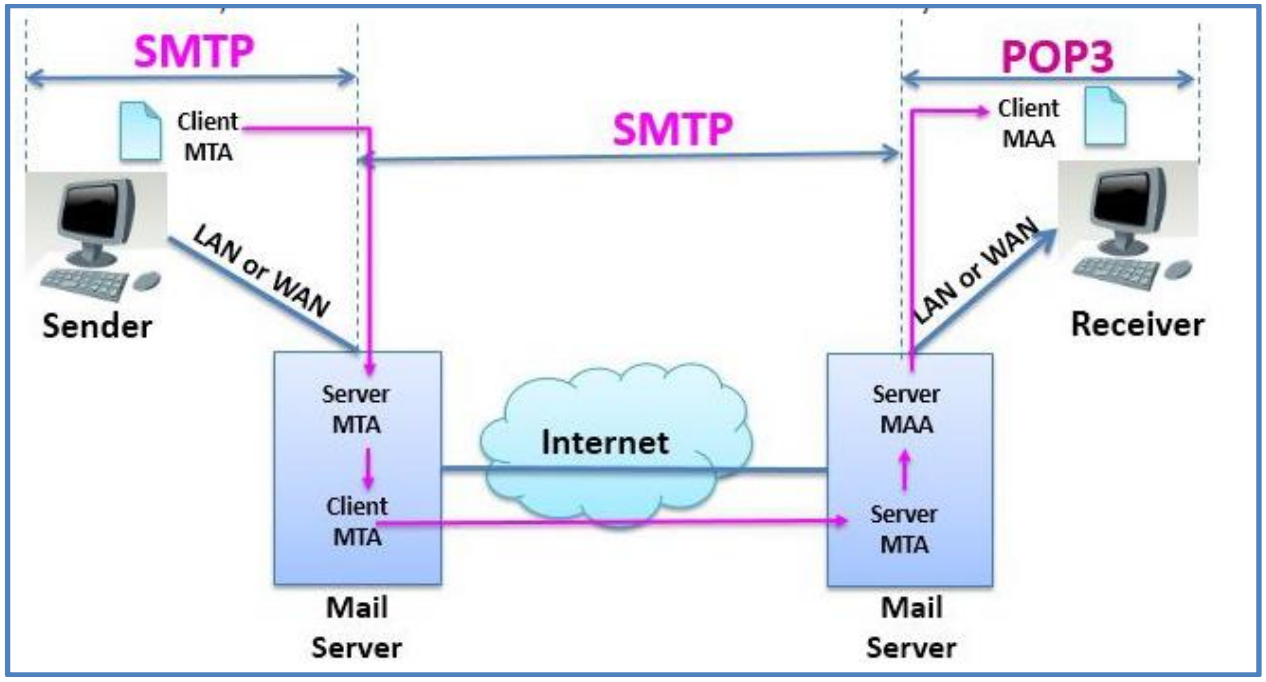


The above diagram gives an example of what happens when email is sent from one person to another using the traditional method. In this example, Alice is sending email to Bob.

1. First, Alice writes a message to Bob in her e-mail program. Her e-mail program puts the message together along with some other information, such as her email address, the address of the person she is writing to, the time at which she is sending her message, and so on. When it is ready, Alice's mail program sends the message to a central computer called a mail server (or a Mail Transfer Agent) using some rules called the Simple Mail Transfer Protocol. A Mail User Agent (MUA), also referred to as an email client, is a computer application that allows you to send and retrieve email.
2. The mail server that Alice is using to send her message (smtp.a.org) takes Alice's message and looks at the address to see where the message is being sent. The mail server then goes out on the internet and tries to find the mail server that Bob is using. It does this by talking to a Domain Name System (DNS) server, which keeps records about how to find different computers on the internet, including mail servers.
3. The DNS server gives Alice's mail server the proper address for the server that Bob is using to receive his email (mx.b.org).
4. Alice's mail server sends the message to Bob's email server, which puts it into Bob's mailbox.
5. Bob opens his e-mail program and downloads his messages using one of two sets of rules—either the Post Office Protocol (POP) or the Internet Message Access Protocol (IMAP). His messages include the new message from Alice.

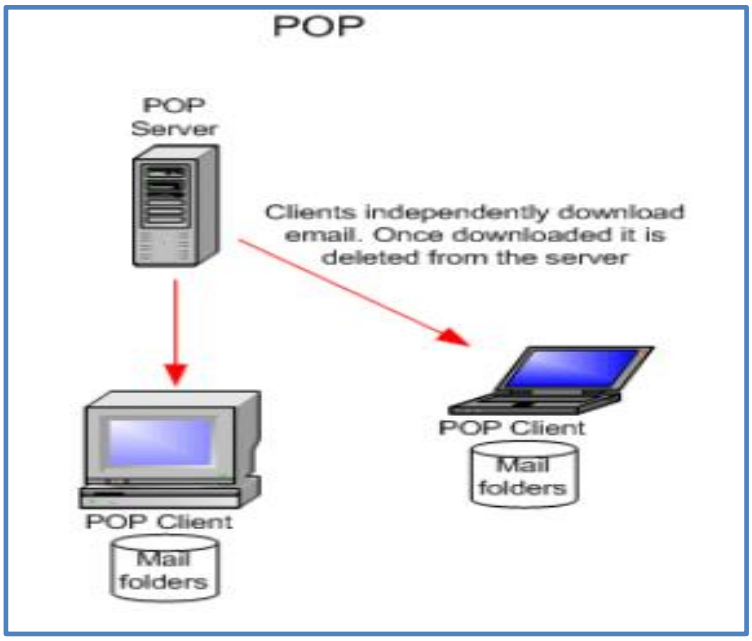
Message Access Agent: POP and IMAP

The first and the second stages of mail delivery use SMTP. However, SMTP is not involved in the third stage because ***SMTP is a push protocol***; it pushes the message from the client to the server. In other words, the direction of the bulk data (messages) is from the client to the server. On the other hand, the third stage needs a pull protocol; the client must pull messages from the server. The third stage uses a message access agent. Currently two message access protocols are available: Post Office Protocol, version 3 (POP3) and Internet Mail Access Protocol, version 4 (IMAP4). Figure below shows the position of these two protocols:



POP3

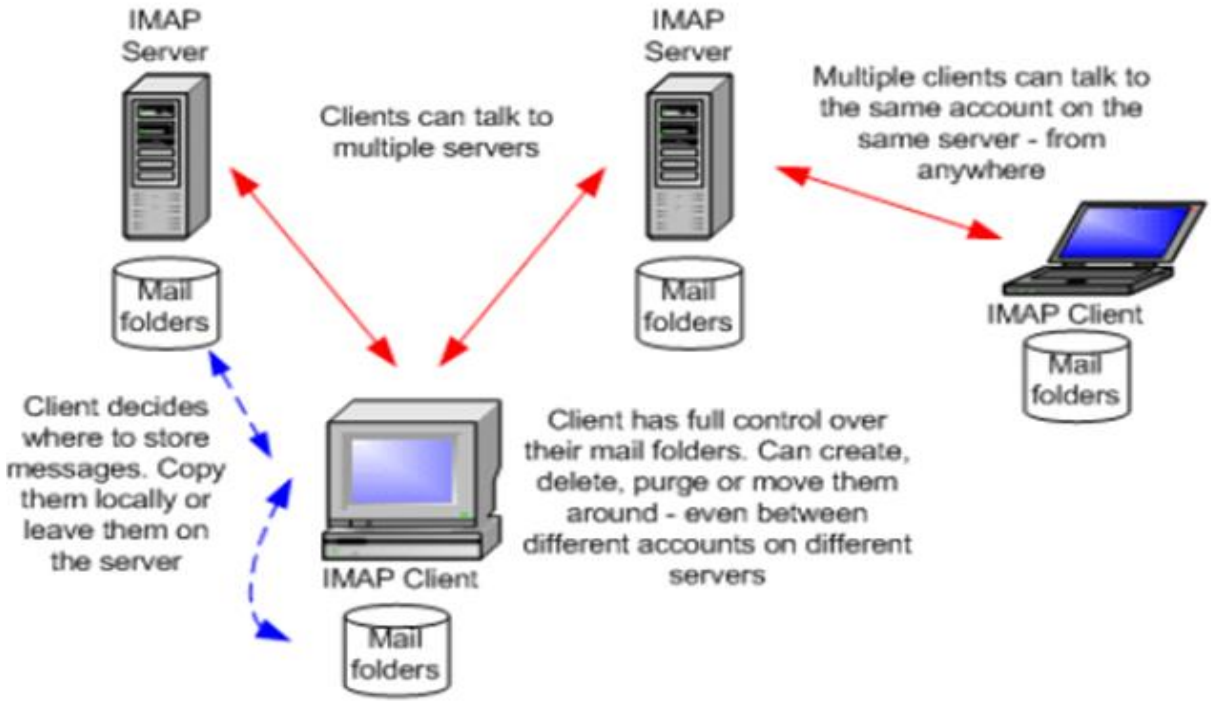
Post Office Protocol, version 3 (POP3) is simple and limited in functionality. The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server. POP3 has two modes: the delete mode and the keep mode. In the delete mode, the mail is deleted from the mailbox after each retrieval. In the keep mode, the mail remains in the mailbox after retrieval. The delete mode is normally used when the user is working at her permanent computer and can save and organize the received mail after reading or replying.
Mail access starts with the client when the user needs to download e-mail from the mailbox on the mail server. The client opens a connection to the server on TCP port 110. It then sends its user name and password to access the mailbox. The user can then list and retrieve the mail messages, one by one. Below figure shows an example of downloading using POP3.



Internet Mail Access Protocol (IMAP)

IMAP4 is similar to POP3, but it has some addition features. So IMAP4 is more powerful and more complex. POP3 is deficient in several ways. It does not allow the user to organize her mail on the server; the user cannot have different folders on the server. (Of course, the user can create folders on her own computer.) In addition, POP3 does not allow the user to partially check the contents of the mail before downloading. IMAP4 provides the following extra functions:

- A user can check the e-mail header prior to downloading.
- A user can search the contents of the e-mail for a specific string of characters prior to downloading.
- A user can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
- A user can create, delete, or rename mailboxes on the mail server.
- A user can create a hierarchy of mailboxes in a folder for e-mail storage.

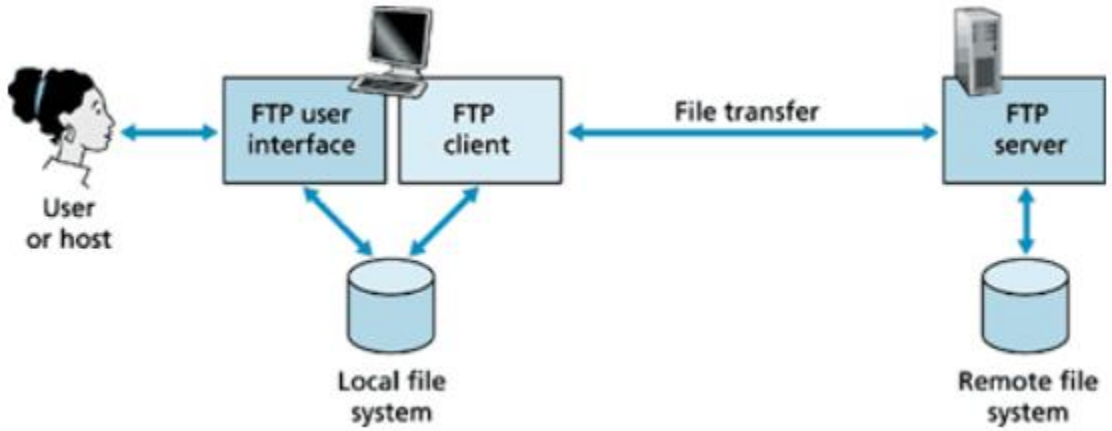


-

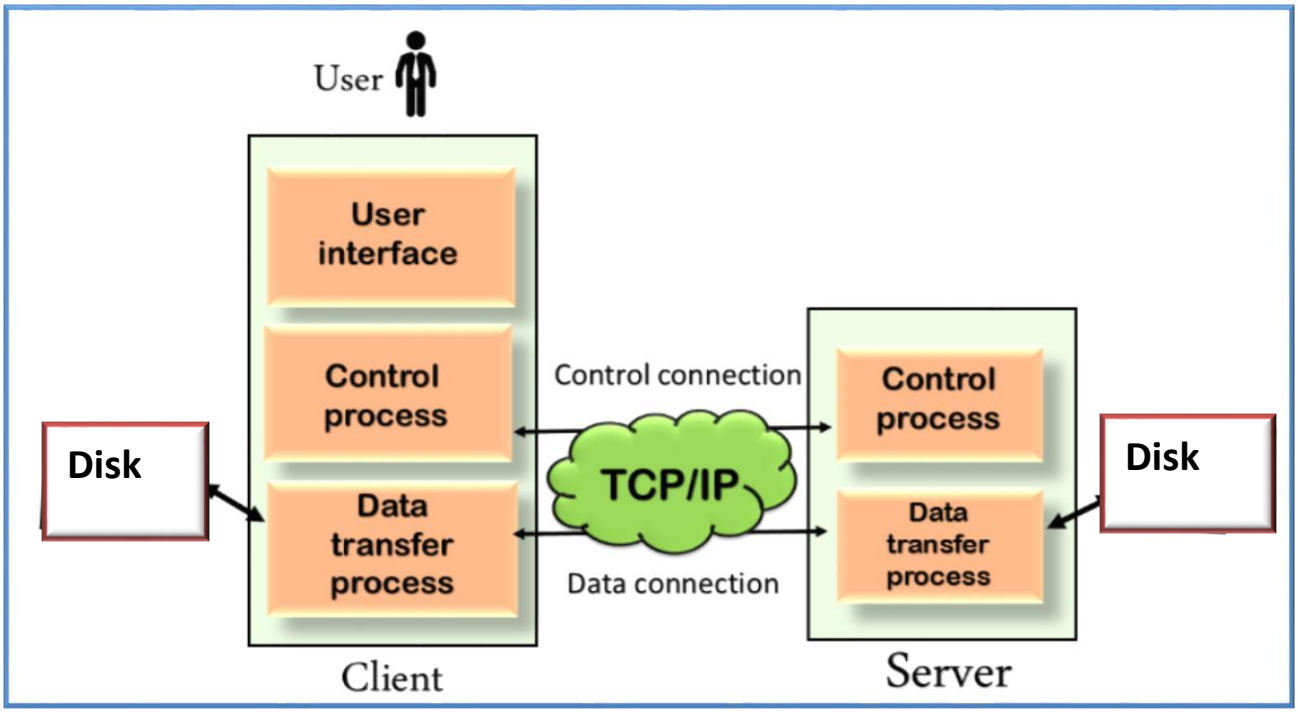
Comparison between POP3 and IMAP

Features	POP3	IMAP
Basic	To read the mail it has to be downloaded first.	The mail content can be checked partially before downloading.
Organize	The user cannot organize mails in the mailbox of the mail server.	The user can organize the mails on the server.
Folder	The user cannot create, delete or rename mailboxes on a mail server.	The user can create, delete or rename mailboxes on the mail server.
Content	A user cannot search the content of mail for prior downloading.	A user can search the content of mail for specific string of character before downloading.
Read new message	Fast	Relatively slow
Functions	POP3 is simple and has limited functions.	IMAP is more powerful, more complex and has more features over POP3.
Delete email	Deleted email go straight into —Deleted Folder	Deleted email will be marked streak on its header. To remove it permanently done —Purge Deleted Messages

File Transfer Protocol (FTP)



File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. It is built on client-server architecture and uses separate control and data connections between the client and the server. For secure transmission it hides (encrypts) the username and password, and encrypts the content, FTP is often secured with SSL/TLS ("FTPS"). SSH File Transfer Protocol ("SFTP") is sometimes used. FTP is an application-layer protocol used to send and receive files between an FTP client and an FTP server. Usually, this is done with the FTP program or another program that can also use the protocol (many are available). FTP transfers can be either text-based or binary-based, and they can handle files of any size.

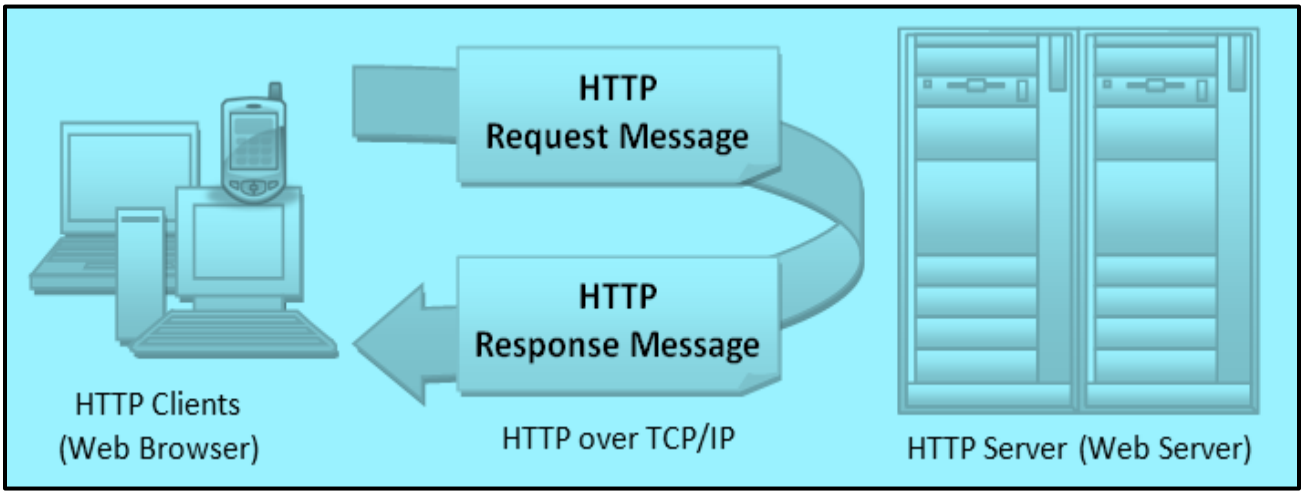


Role of FTP protocol: FTP protocol defines the way in which data must be transferred over a TCP/IP network. The aim of FTP protocol is to:

- allow file sharing between remote machines
- allow independence between client and server machine system files
- enable efficient data transfer

Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. HTTP uses a set of rules for transferring files, such as text, graphic images, sound, video, and other multimedia files, on the World Wide Web. HTTP functions as a combination of FTP and SMTP. It is similar to FTP because it transfers files and uses the services of TCP. However, it is much simpler than FTP because it uses only one TCP connection. There is no separate control connection; only data are transferred between the client and the server.



HTTP uses the services of TCP on well-known port 80. HTTP is fundamentally an insecure protocol. Text-based information is sent between the client and the server. To address the need for secure web networking, alternatives are available, such as HTTP Secure (HTTPS) and Secure Sockets Layer (SSL). Requests from a web client to a web server are connection-oriented, but they are not persistent. Once the client receives the contents of an HTML page, the connection is no longer active.

IPv6

Address space for IPv4 is quickly running out due to the rapid growth of the Internet and the development of new Internet-compatible mobile technologies. Examples of this include the IP addressable telephone, wireless personal digital assistants (PDAs), cell phones, game consoles, and home-networking systems. There have been many predictions of when the IPv4 address pool will be exhausted. Techniques such as Network Address Translation/Port Address Translation (NAT/PAT), Dynamic Host Control Protocol (DHCP), and Classless Inter-Domain Routing (CIDR) have been implemented to prolong the life of IPv4. These techniques reuse the existing IPv4 address space and handle the address space allocation more efficiently. Another solution to the limited number of available IPv4 addresses is to migrate to IPv6. IP version 6 (IPv6) is the solution proposed by the Internet Engineering Task Force (IETF) for expanding the possible number of IP addresses to accommodate the growing users on the Internet. IPv6, introduced in 1999, is also called IPng (Internet Protocol next generation).
IPv4 and IPv6 are not compatible technologies, and they cannot communicate directly with each other. So, before migrating to an IPv6 environment, the network devices and network equipment need to be IPv6 compatible or enabled.
IPv6 numbers are written in hexadecimal rather than dotted decimal, as with IPv4. For example, the following is an IPv6 address represented by 32 hexadecimal digits. (Keep in mind: 32 hex digits with 4 bits/hex digit = 128 bits): **6789: ABCD: 1234:EF98:7654:321F: EDCB: AF21**
IPv4 numbers can be written in the new IPv6 form by writing the IPv4 number in hexadecimal and placing the number to the right of a double colon.
For Example: Convert the IPv4 address of 192.168.5.20 to an IPv6 hexadecimal address
Solution:
First convert each dotted-decimal number to hexadecimal.

Decimal	Hex
192	C0
168	A8
5	05
20	14

Use a calculator or a lookup table to convert the decimal numbers to hexadecimal. The IPv6 address will have many leading 0s; therefore, the IPv6 hex address can be written in double-colon notation as

:: C0A8:0514

IPv4 addresses can also be written in IPv6 form by writing the IPv4 number in dotted-decimal format, as shown. Note that the number is preceded by 24 hexadecimal 0s:
0000: 0000: 0000: 0000: 0000: 0000:192.168.5.20

This number can be reduced as follows: **:: 192.168.5.20**