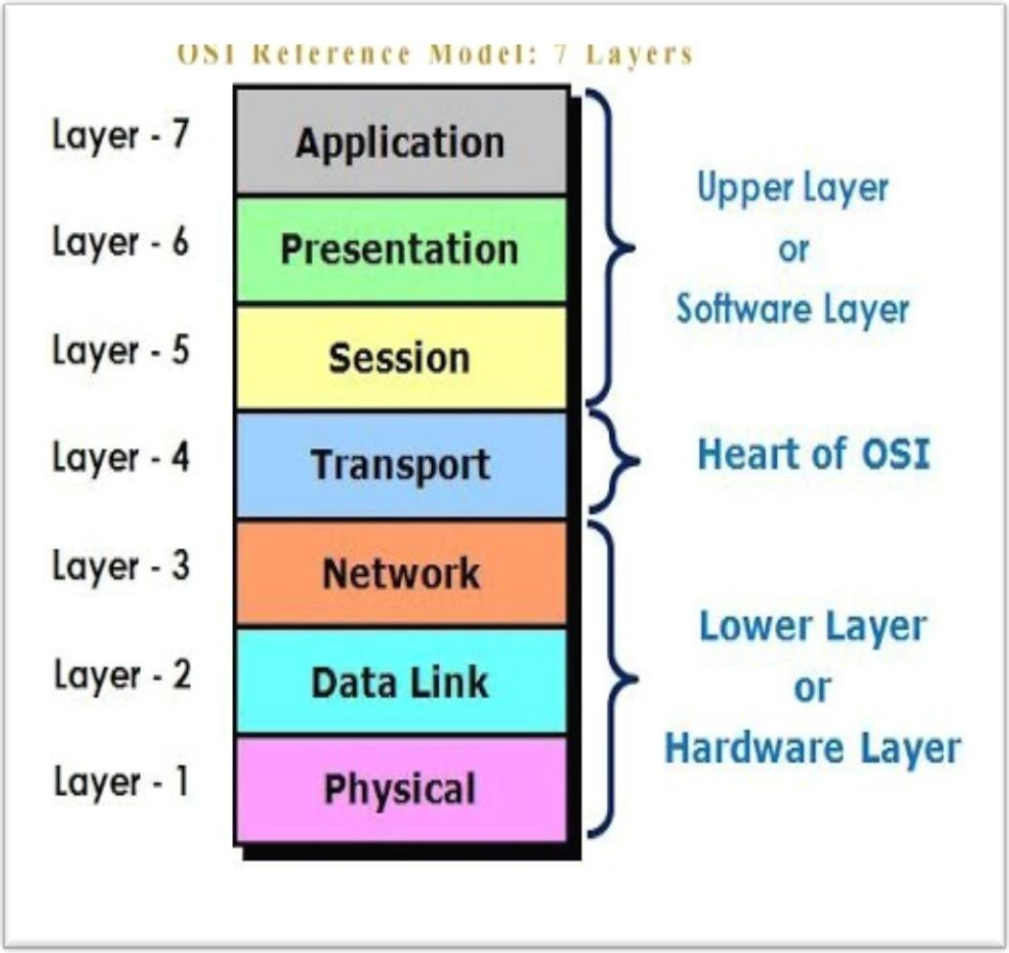
Unit 5: Reference models Weightage: 20 Marks

Course: Data Communication and Computer Network

Program Code: CO4I

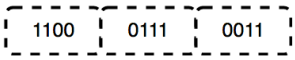
OSI Reference Model:

- OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization of Standardization**', in the year 1984.
- It is a 7 layer architecture with each layer having specific functionality to perform.
- All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are :

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

* Hub, Repeater, Modem, Cables are Physical Layer devices.
** Network Layer, Data Link Layer and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The functions of the data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **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.
5. **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.

** Packet in Data Link layer is referred as **Frame**.*
*** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
**** Switch & Bridge are Data Link Layer devices.*

3. Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by the network layer.
The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* *Segment* in Network layer is referred as **Packet**.

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

• **At sender's side:**

Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

Note: The sender need to know the port number associated with the receiver's application. Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

• **At receiver's side:**

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. **Connection less service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

** Data in the Transport Layer is called as **Segments**.*

*** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*

*Transport Layer is called as **Heart of OSI** model.*

5. Session Layer (Layer 5) :

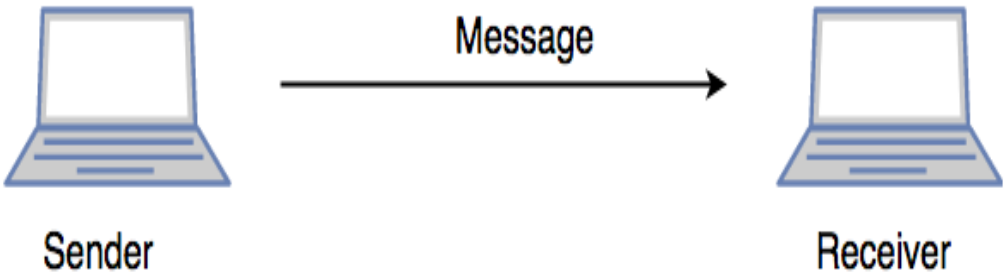
This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
The functions of the session layer are :

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

***All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as "Application Layer".*
***Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*

SCENARIO:

Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data) and converted into bits (0's and 1's) so that it can be transmitted.



6. Presentation Layer (Layer 6) :

Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

1. **Translation :** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption :** 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.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
Ex: Application – Browsers, Skype Messenger etc.
**Application Layer is also called as Desktop Layer.*

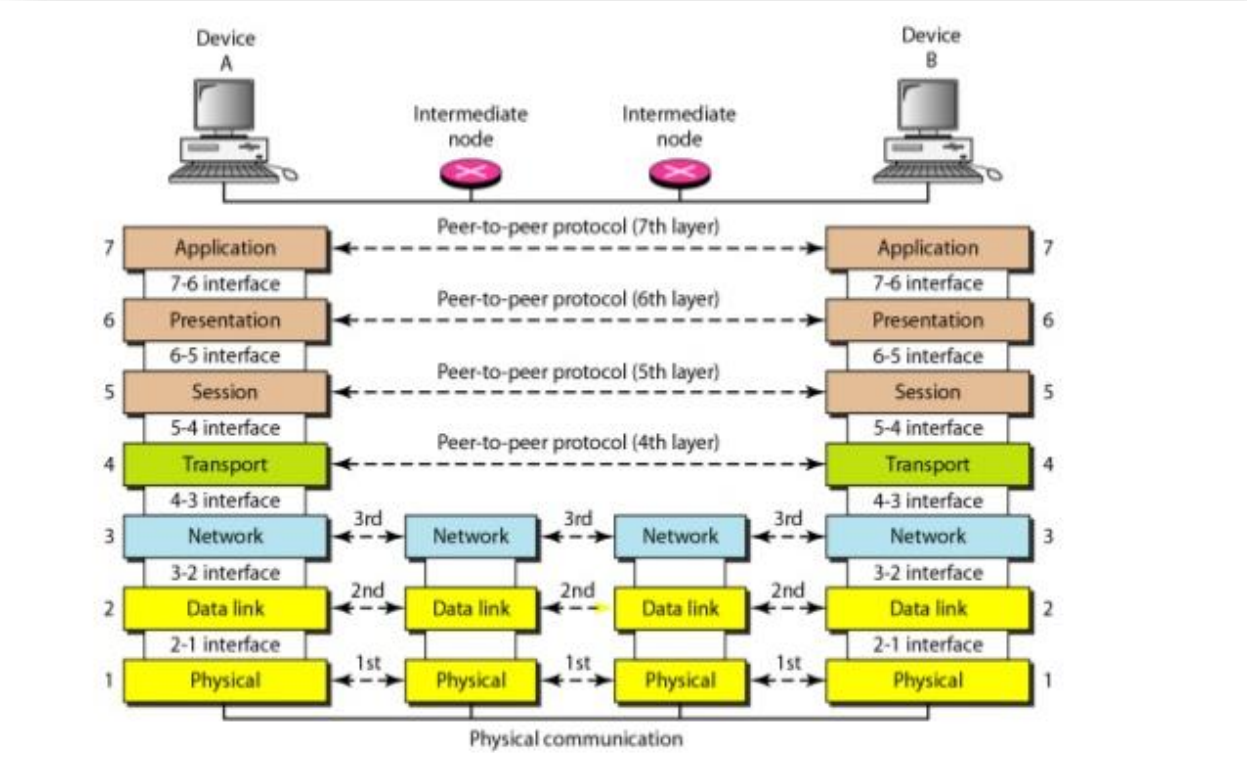
The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

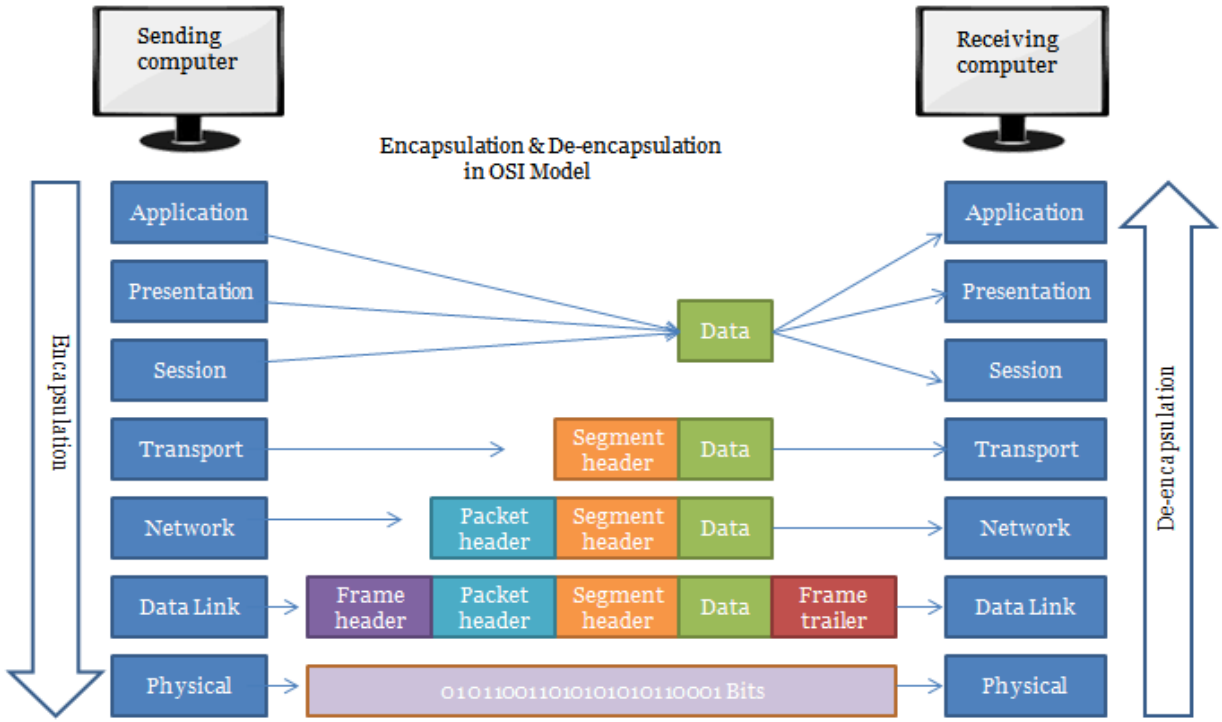
OSI model acts as a reference model and is not implemented in the Internet because of its late invention. Current model being used is the TCP/IP model.

PEER-TO-PEER PROCESS

- **Peer-to-peer processes**
  - Are the processes on each machine that communicate at a given layer
  - Between machines layer x communicates with layer x on another machine by protocols
  - Communication between machines is peer-to-peer processing using the protocols appropriate to a given layer
- The passing of the data and network information down through the layers of the sending device and backup through the layers of the receiving device is made possible by **interface** between each pair of adjacent layers
- **Interface** defines what info. and services a layer must provide for the layer above it



DATA ENCAPSULATION & DECAPSULATION IN THE OSI MODEL



Encapsulation process takes place in the sending computer while the de-encapsulation process takes place in the receiving computer.

After encapsulation, each layer uses a specific name or term to represent the encapsulated data

Let's understand each term in detail with step by step data encapsulation process.

Data

Upper layer (application layer in TCP/IP) or layers (application, presentation and session layers in OSI) create data stream and handed it down to the transport layer.

Upper layers don't use header and trailer with data. But if require, the application that initiates the connection can add header and trailer with data. For example, browsers use HTTP protocol to fetch websites from webservers. HTTP protocol uses a header with data.

Since the use of header and trailer in upper layers is application specific, in encapsulation diagram and terms encapsulated data in upper layers is commonly referred as the data.

Segment

Transport layer breaks the received data stream from upper layers into smaller pieces. Next, it creates a header for each data piece. This header contains all necessary information about the piece that the transport layer in remote host needs to reassemble the data stream back from the pieces. Once header is attached, data piece is referred as segment. Once segments are created, they are handed down to the network layer for further processing.

Packet

Network layer creates a header for each received segment from transport layer. This header contains information that is required for addressing and routing such as source software address and destination software address. Once this header is attached, segment is referred as packet. Packets are handed down to the data link layer.

In original TCP/IP model the term packet is mentioned as the term datagram. Both terms packet and datagram refer to the same data package. This data package contains a network layer header and an encapsulated segment.

Frame

Data link layer receives packets from network layer. Unlike transport layer and network layer which only create header, it also creates a trailer with header for each received packet. The header contains information that is required for switching such as source hardware address and destination hardware address. The trailer contains information that is required to detect and drop corrupt data packages in the earliest stage of de-encapsulation. Once header and trailer are attached with packet, it is referred as frame. Frames are passed down to the physical layer.

Bits

Physical layer receives frames from data link layer and converts them a format that the attached media can carry. For example, if the host is connected with a copper wire, the physical layer will convert frames in voltages. And if the host is connected with a wireless network, the physical layer will convert them in radio signals.

De-encapsulation

De-encapsulation takes place in receiving computer. In de-encapsulation process, header and trailer attached in encapsulation process are removed.

Physical layer picks encoded signals from media and converts them in frames and hands them over to the data link layer.

Data link layer, first, reads the trailer of frame to confirm that the received frame is in correct shape. It reads rest of the frame only if the frame is in correct shape.

If frame is fine, it reads the destination hardware address of the frame to determine the fame is intended for it or not.

If frame is not intended for it, it will discard that frame immediately. If frame is intended for it, it will remove the header and the trailer from the frame. Once data link layer's header and trailer are removed from the frame, it becomes packet. Packets are handed over to the network layer.

Network layer checks destination software address in the header of each packet. If packet is not intended for it, network layer will discard that packet immediately. If packet is intended for it, it will remove the header. Once network layer's header is removed, packet will become segment. Segments are handed over to the transport layer.

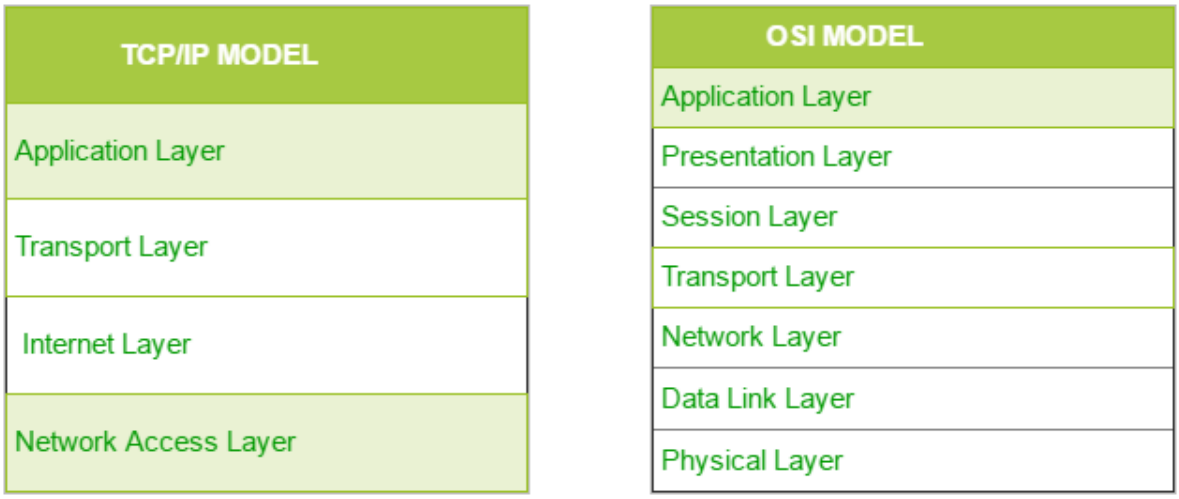
Transport layer receives segments from network layer. From segment headers it collects all necessary information and based on that information it arranges all segments back in correct order. Next, it removes segment header from all segments and reassembles them in original data stream. Data stream is handed over to the upper layers.

Upper layers format data stream in such format that the target application can understand.

TCP/IP Model

- It stands for Transmission Control Protocol/Internet Protocol.
- The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:
    1. Process/Application Layer
    2. Host-to-Host/Transport Layer
    3. Internet Layer
    4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :



The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

1. Network Access Layer –This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer –This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer –This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.
3. In a communications network, a network **node** is a connection point that can receive, create, store or send data along distributed network routes.
4. Each network node -- whether it's an endpoint for data transmissions or a redistribution point -- has either a programmed or engineered capability to recognize, process and forward transmissions to other network nodes.
5. In a telecommunications network, a **link** is a communication channel that connects two or more devices for the purpose of data transmission.
6. The link may be a dedicated **physical link** or a **virtual circuit** that uses one or more physical links or shares a physical link with other telecommunications links.

Transmission Control Protocol (TCP) Services:

Common TCP/IP Protocols and Ports

Protocol	TCP/UDP	Port Number	Description
File Transfer Protocol (FTP)	TCP	20/21	FTP is one of the most commonly used file transfer protocols on the Internet and within private networks. An FTP server can easily be set up with little networking knowledge and provides the ability to easily relocate files from one system to another. FTP control is handled on TCP port 21 and its data transfer can use TCP port 20 as well as dynamic ports depending on the specific configuration.
Secure Shell (SSH)	TCP	22	SSH is the primary method used to manage network devices securely at the command level. It is typically used as a secure alternative to Telnet which does not support secure connections.
Telnet	TCP	23	Telnet is the primary method used to manage network devices at the command level. Unlike SSH which provides a secure connection, Telnet does not, it simply provides a basic unsecured connection. Many lower level network devices support Telnet and not SSH as it required some additional processing. Caution should be used when connecting to a device using Telnet over a public network as the login credentials will be transmitted in the clear.
Simple Mail Transfer Protocol (SMTP)	TCP	25	SMTP is used for two primary functions, it is used to transfer mail (email) from source to destination between mail servers and it is used by end users to send email to a mail system.
Domain Name System (DNS)	TCP/UDP	53	The DNS is used widely on the public internet and on private networks to translate domain names into IP addresses, typically for network routing. DNS is hieratical with main root servers that contain databases that list the managers of high level Top Level Domains (TLD) (such as .com). These different TLD managers then contain

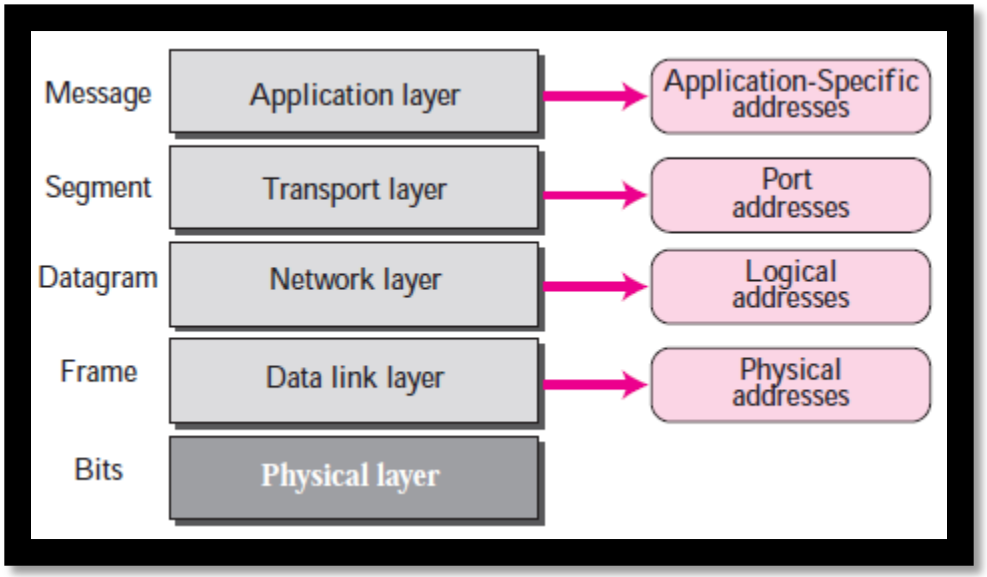
			information for the second level domains that are typically used by individual users (for example, cisco.com). A DNS server can also be set up within a private network to private naming services between the hosts of the internal network without being part of the global system.
Dynamic Host Configuration Protocol (DHCP)	UDP	67/68	DHCP is used on networks that do not use static IP address assignment (almost all of them). A DHCP server can be set up by an administrator or engineer with a poll of addresses that are available for assignment. When a client device is turned on it can request an IP address from the local DHCP server, if there is an available address in the pool it can be assigned to the device. This assignment is not permanent and expires at a configurable interval; if an address renewal is not requested and the lease expires the address will be put back into the poll for assignment.
Trivial File Transfer Protocol (TFTP)	UDP	69	TFTP offers a method of file transfer without the session establishment requirements that FTP uses. Because TFTP uses UDP instead of TCP it has no way of ensuring the file has been properly transferred, the end device must be able to check the file to ensure proper transfer. TFTP is typically used by devices to upgrade software and firmware; this includes Cisco and other network vendors' equipment.
Hypertext Transfer Protocol (HTTP)	TCP	80	HTTP is one of the most commonly used protocols on most networks. HTTP is the main protocol that is used by web browsers and is thus used by any client that uses files located on these servers.
Post Office Protocol (POP) version 3	TCP	110	POP version 3 is one of the two main protocols used to retrieve mail from a server. POP was designed to be very simple by allowing a client to retrieve the complete contents of a server mailbox and then deleting the contents from the server.
Network Time	UDP	123	One of the most overlooked protocols is NTP. NTP is used to synchronize the devices on the

Protocol (NTP)			Internet. Even most modern operating systems support NTP as a basis for keeping an accurate clock. The use of NTP is vital on networking systems as it provides an ability to easily interrelate troubles from one device to another as the clocks are precisely accurate.
NetBIOS	TCP/UDP	137/138/139	NetBIOS itself is not a protocol but is typically used in combination with IP with the NetBIOS over TCP/IP (NBT) protocol. NBT has long been the central protocol used to interconnect Microsoft Windows machines.
Internet Message Access Protocol (IMAP)	TCP	143	IMAP version3 is the second of the main protocols used to retrieve mail from a server. While POP has wider support, IMAP supports a wider array of remote mailbox operations which can be helpful to users.
Simple Network Management Protocol (SNMP)	TCP/UDP	161/162	SNMP is used by network administrators as a method of network management. SNMP has a number of different abilities including the ability to monitor, configure and control network devices. SNMP traps can also be configured on network devices to notify a central server when specific actions are occurring. Typically, these are configured to be used when an alerting condition is happening. In this situation, the device will send a trap to network management stating that an event has occurred and that the device should be looked at further for a source to the event.
Border Gateway Protocol (BGP)	TCP	179	BGP version 4 is widely used on the public internet and by Internet Service Providers (ISP) to maintain very large routing tables and traffic processing. BGP is one of the few protocols that have been designed to deal with the astronomically large routing tables that must exist on the public Internet.
Lightweight Directory Access Protocol (LDAP)	TCP/UDP	389	LDAP provides a mechanism of accessing and maintaining distributed directory information. LDAP is based on the ITU-T X.500 standard but has been simplified and altered to work over TCP/IP networks.

Hypertext Transfer Protocol over SSL/TLS (HTTPS)	TCP	443	HTTPS is used in conjunction with HTTP to provide the same services but doing it using a secure connection which is provided by either SSL or TLS.
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	TCP/UDP	636	Just like HTTPS, LDAPS provides the same function as LDAP but over a secure connection which is provided by either SSL or TLS.
FTP over TLS/SSL	TCP	989/990	Again, just like the previous two entries, FTP over TLS/SSL uses the FTP protocol which is then secured using either SSL or TLS.

Addressing:

Four levels of addresses are used in the TCP/IP protocol: **physical address, logical address, port address, and application-specific address** as shown in Figure.



Physical Addresses

- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
- The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address.
- Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network.
- Example: Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below: A 6-byte (12 hexadecimal digits) physical address **07:01:02:01:2C:4B**

Logical Addresses

- Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media.
- A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. An internet address in IPv4 in decimal numbers **132.24.75.9**
- No two publicly addressed and visible hosts on the Internet can have the same IP address.
- The physical addresses will change from hop to hop, but the logical addresses remain the same.
- The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network). There are limitations on broadcast addresses.

Port Addresses

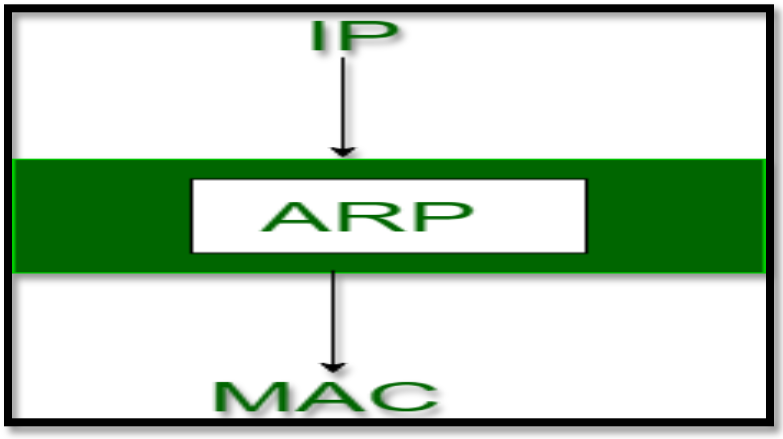
- There are many application running on the computer. Each application run with a port no.(logically) on the computer.
- A port number is part of the addressing information used to identify the senders and receivers of messages.
- Port numbers are most commonly used with TCP/IP connections.
- These port numbers allow different applications on the same computer to share network resources simultaneously.
- The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.
- Example: a port address is a 16-bit address represented by one decimal number **753**

Application-Specific Addresses

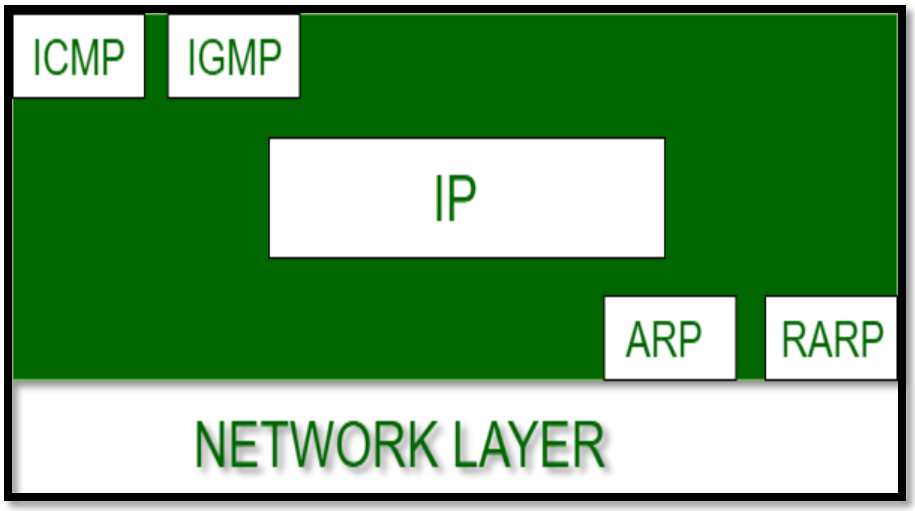
- Some applications have user-friendly addresses that are designed for that specific application.
- Examples include the e-mail address (for example, forouzan@fhda.edu) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.

Address Resolution Protocol (ARP):

- Most of the computer programs/applications use **logical address (IP address)** to send/receive messages, however the actual communication happens over the **physical address (MAC address)** i.e from layer 2 of OSI model.
- So our mission is to get the destination MAC address which helps in communicating with other devices.
- This is where ARP comes into the picture, its functionality is to translate IP address to physical address.



- The acronym ARP stands **for Address Resolution Protocol** which is one of the most important protocols of the Network layer in the OSI model.
- Note: ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.



Dynamic Host Configuration Protocol

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol).
- DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.

DHCP does the following:

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

How DHCP works

DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP

clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

The DHCP lease process works as follows:

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, client broadcasts a query for this information.
- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
- When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

Benefits of DHCP

Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

Network address translation (NAT)

- To access Internet, one public IP address is needed but as you use private IP address in our private network, translation of private IP address to a public IP address is required.
- Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.
- Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to destination.
- It then makes the corresponding entries of ip address and port number in the NAT table. NAT generally operates on router or firewall.

Network Address Translation (NAT) working –
Generally, the border router is configured for NAT i.e the router which have one interface in local (inside) network and one interface in global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to local (private) IP address.
If NAT run out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is send.

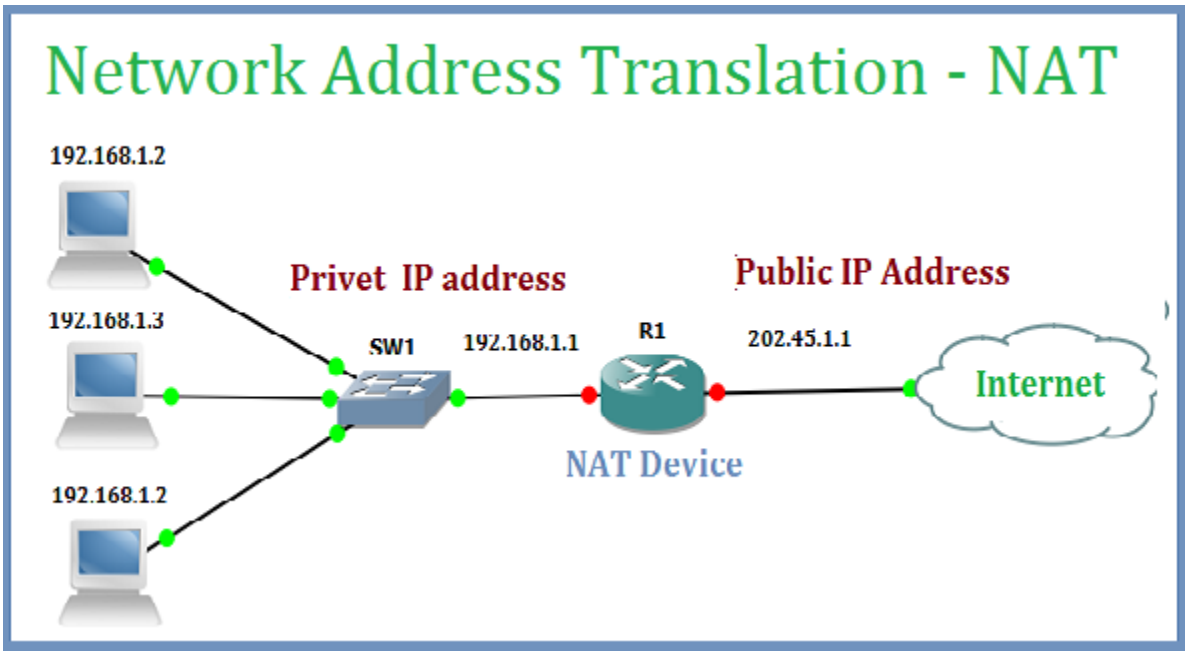
Why mask port numbers?

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on host side, at the same time. If NAT does only translation of ip addresses, then when their packets will arrive at the NAT, both of their

IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies on the public ip address of the router. Thus, on receiving reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses –

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organisation. These are the network Addresses in which the translation of the addresses will be done.



Inside local address – An IP address that is assigned to a host on the Inside (local) network. The address is probably not a IP address assigned by the service provider i.e., these are private IP address. This is the inside host seen from the inside network.

Inside global address – IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.

Outside local address – This is the actual IP address of the destination host in the local network after translation.

Outside global address – This is the outside host as seen form the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:

Static NAT – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global address. This is generally used for Web hosting. These are not used in organizations as there are many devices who will need Internet access and to provide Internet access, public IP address is needed.

Suppose, if there are 3000 devices who needs access to Internet, the organization have to buy 3000 public addresses that will be very costly.

Dynamic NAT – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool are not free, then the packet will be dropped as only fixed number of private IP address can be translated to public addresses.

Suppose, if there is pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who wants to access the Internet are fixed. This is also very costly as the organization have to buy many global IP addresses to make a pool.

Port Address Translation (PAT) – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to single registered IP address .Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

- NAT conserves legally registered IP addresses .
- It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.

- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

Transport Layer: Connection-Oriented and Connectionless Services

Two distinct techniques are used in data communications to transfer data. Each has its own advantages and disadvantages. They are the connection-oriented method and the connectionless method:

Connection Oriented Services

There is a sequence of operation to be followed by the users of connection oriented service. These are:

1. Connection is established.
2. Information is sent.
3. Connection is released.

In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection.

Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

Connection Less Services

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

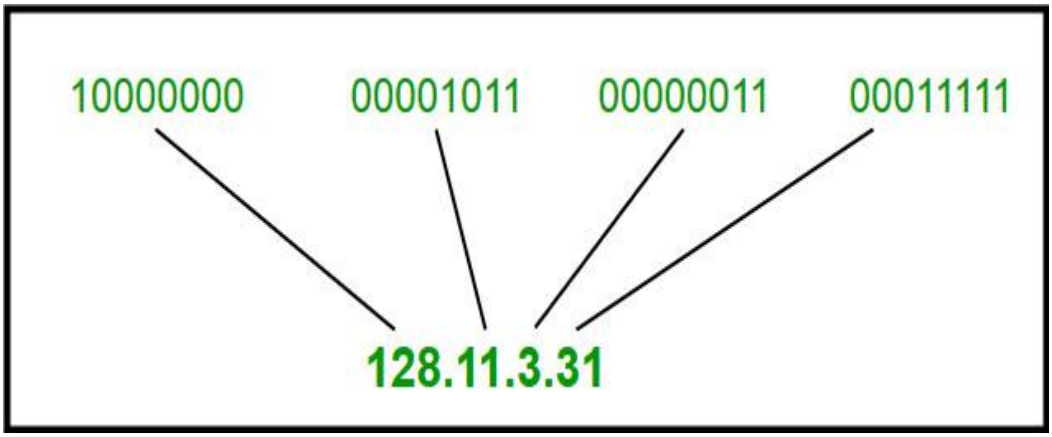
Connection-Oriented and Connectionless Protocols

Connection-Oriented (CO) Protocols	**Connectionless (CL) Protocols**
Require a handshake	Do not require a handshake
Have larger headers and more overhead	Have smaller headers and less overhead
Provide packet acknowledgments, data segmentation, flow control, and error detection and correction	Do not provide additional services
Acknowledge transmitted packets, so they are considered reliable	Do not acknowledge transmitted packets, so they are considered unreliable
Example: TCP	Example: UDP

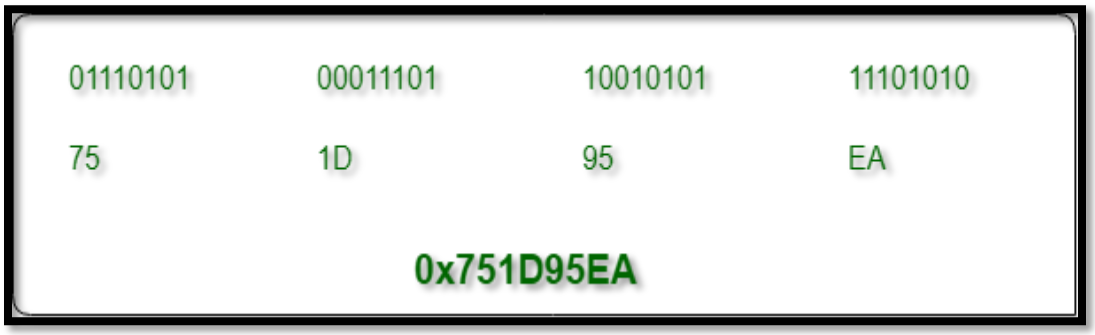
Introduction of IP Addressing

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 232. Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation:



Hexadecimal Notation:



Some points to be noted about dotted decimal notation:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).

1. **Classful Addressing**
   The 32 bit IP address is divided into five sub-classes. These are:

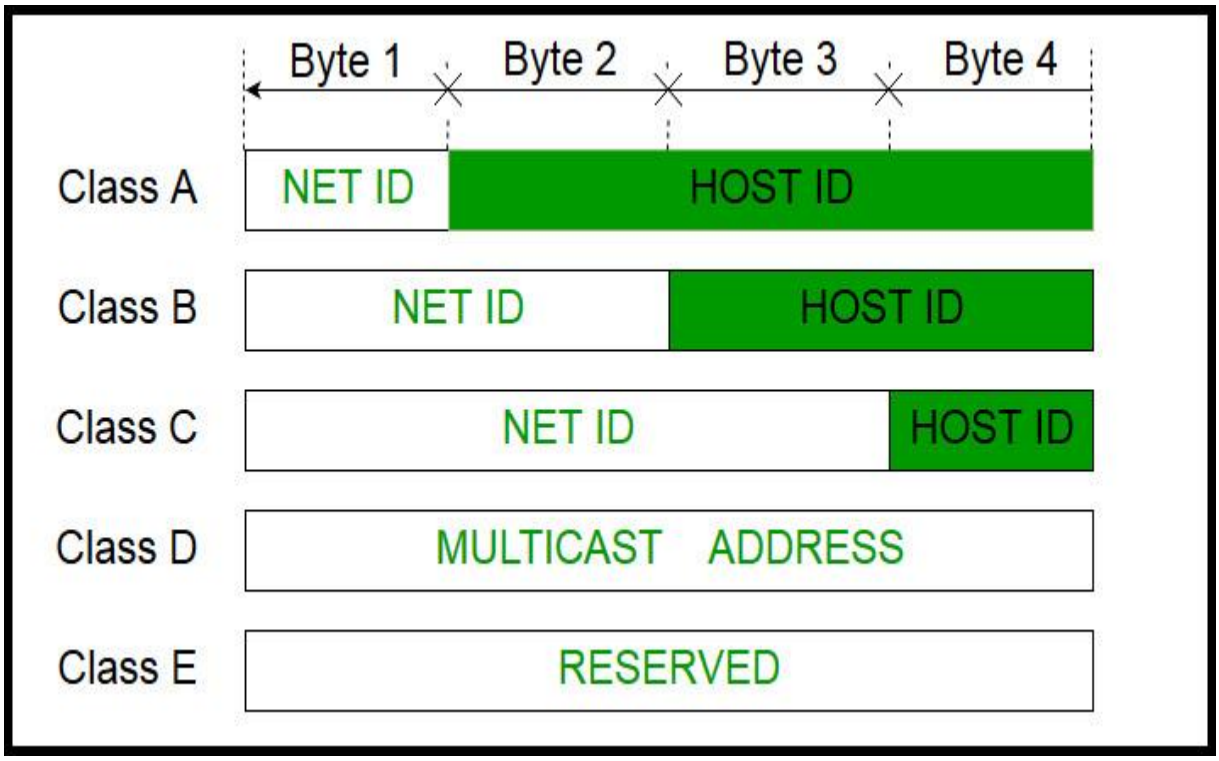
- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.
IPv4 address is divided into two parts:

Network ID

Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A:

IP address belonging to class A are assigned to the networks that contain a large number of hosts.

The network ID is 8 bits long.

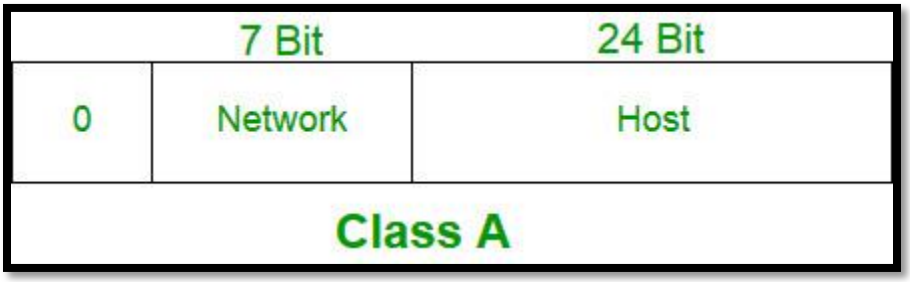
The host ID is 24 bits long.

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 of:

2^7-2= 126 network ID(Here 2 address is subracted 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



Class B:

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

The network ID is 16 bits long.

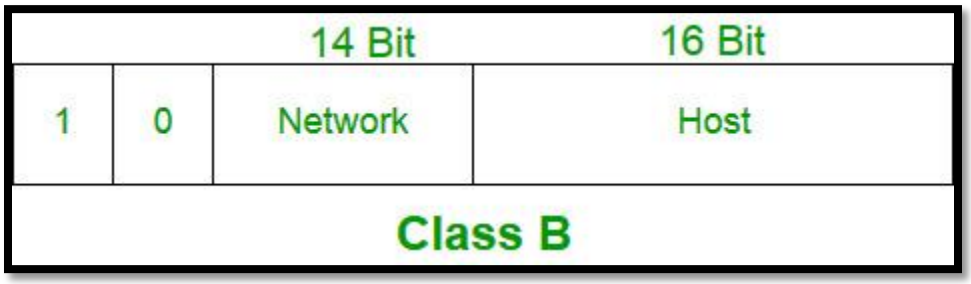
The host ID is 16 bits long.

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 of:

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.



Class C:

IP address belonging to class C are assigned to small-sized networks.

The network ID is 24 bits long.

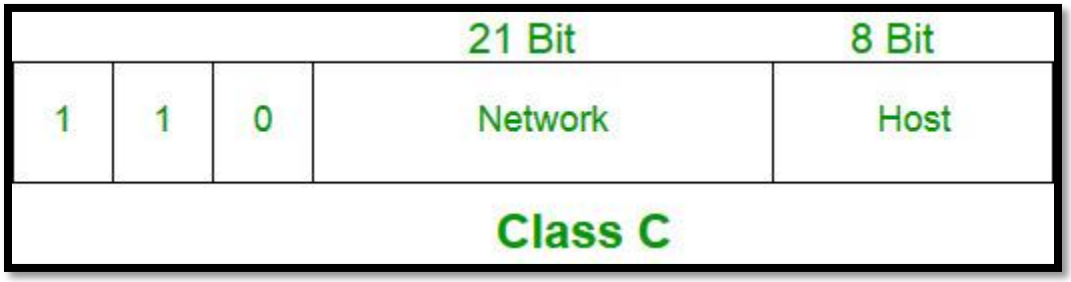
The host ID is 8 bits long.

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

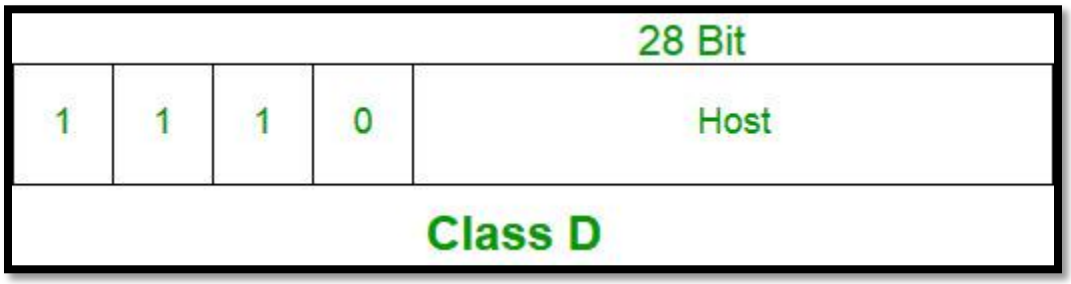
IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.



Class D:

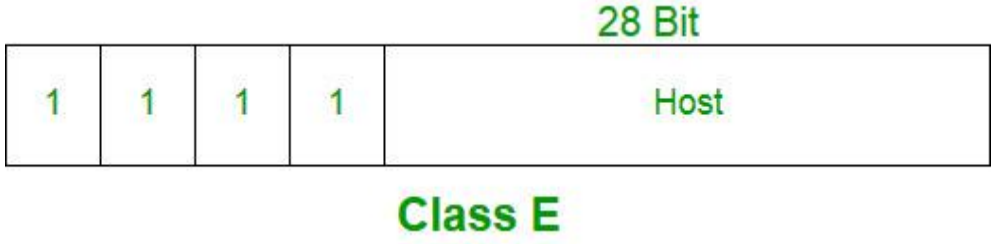
IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

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



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 – 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.



Range of special IP addresses:

169.254.0.0 – 169.254.0.16 : Link local addresses
127.0.0.0 – 127.0.0.8 : Loop-back addresses
0.0.0.0 – 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.

Summary of Classful addressing :

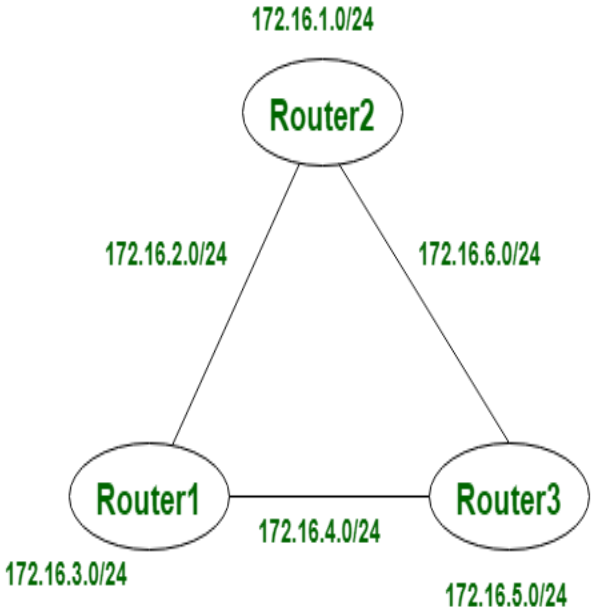
CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Problems with Classful Addressing:

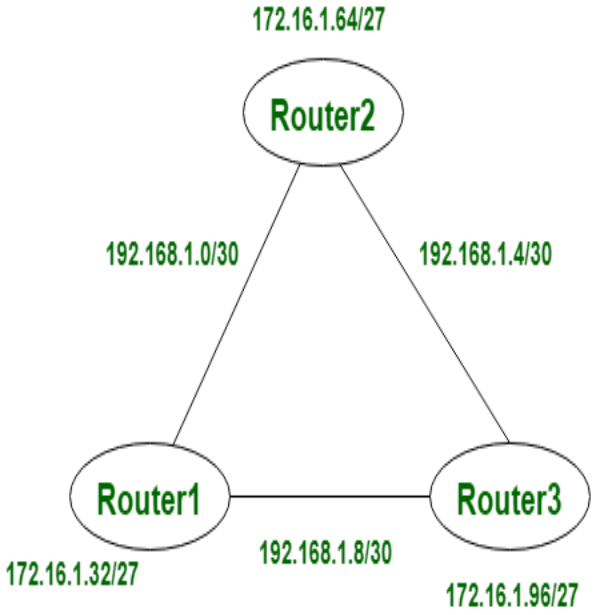
The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993.

2. **Classless Routing/Addressing :**
   Classless Routing imports subnet mask and in this, triggered updates are used. In classless routing, VLMS (Variable Length Subnet Mask) is supported and also CIDR (Classless Inter-Domain Routing). In classless routing, hello messages are used for checking status. In classless routing, subnet mask is not same throughout, it may vary for all devices, we can see it in the given picture.



Classful: Subnet mask is same throughout the topology



Classless: Subnet mask can change in the topology

Let's see that the difference between classful routing and classless routing:

S.NO	CLASSFUL ROUTING	CLASSLESS ROUTING
1.	In classful routing, VLMS(Variable Length Subnet Mask) is not supported.	While in classless routing, VLMS(Variable Length Subnet Mask) is supported.
2.	Classful routing requires more bandwidth.	While it requires less bandwidth.
3.	In classful routing, hello messages are not used.	While in classless routing, hello messages are used.
4.	Classful routing does not import subnet mask.	Whereas it imports subnet mask.
5.	In classful routing, address is divided into three parts which are: Network, Subnet and Host.	While in classless routing, address is divided into two parts which are: Subnet and Host.
6.	In classful routing, regular or periodic updates are used.	Whereas in this, triggered updates are used.
7.	In classful routing, CIDR(Classless Inter-Domain Routing) is not supported.	While in classless routing, CIDR(Classless Inter-Domain Routing) is supported.
8.	In classful routing, subnets are not displayed in other major subnet.	While in classless routing, subnets are displayed in other major subnet..

What is IP Subnetting?

- IP Subnetting is a process of dividing a large IP network in smaller IP networks. In Subnetting we create multiple small manageable networks from a single large IP network.

Let's take an example.

- To best utilize available addresses if we put more than 16000000 hosts in a single network, due to broadcast and collision, that network will never work. If we put less hosts then remaining addresses will be wasted.
- Subnetting provides a better way to deal with this situation. Subnetting allows us to create smaller networks from a single large network which not only fulfill our hosts' requirement but also offer several other networking benefits.

What is Supernetting?

The time came when most of the class A and class B addresses were depleted;

however,there was still a huge demand for midsize blocks.

The size of a class C block with amaximum number of 256 addresses did not satisfy the needs of most organizations.

Even a midsize organization needed more addresses. One solution was supernetting.

In supernetting, an organization can combine several class C blocks to create a largerrange of addresses. In other words, several networks are combined to create a super-network or asupernet.

An organization can apply for a set of class C blocks instead of just one. For example, an organization that needs 1000 addresses can be granted fourcontiguous class C blocks. The organization can then use these addresses to create onesupernetwork. Supernetting decreases the number of 1s in the mask. For example, if anorganization is given four class C addresses, the mask changes from /24 to /22. We willsee that classless addressing eliminated the need for supernetting.

Subnet Mask/ Masking:

- A subnet mask is a number that defines a range of IP addresses that can be used in a network.
- ubnet masks are used to designate subnetworks, or subnets, which are typically local networks LANs that are connected to the Internet.
- Systems within the same subnet can communicate directly with each other, while systems on different subnets must communicate through a router.
- Therefore, subnetworks can be used to partition multiple networks and limit the traffic between them.
- A subnet mask hides, or "masks," the network part of a system's IP address and leaves only the host part as the machine identifier.
- A common subnet mask for a Class C IP address is 255.255.255.0. Each section of the subnet mask can contain a number from 0 to 255, just like an IP address.

What is IPv4?

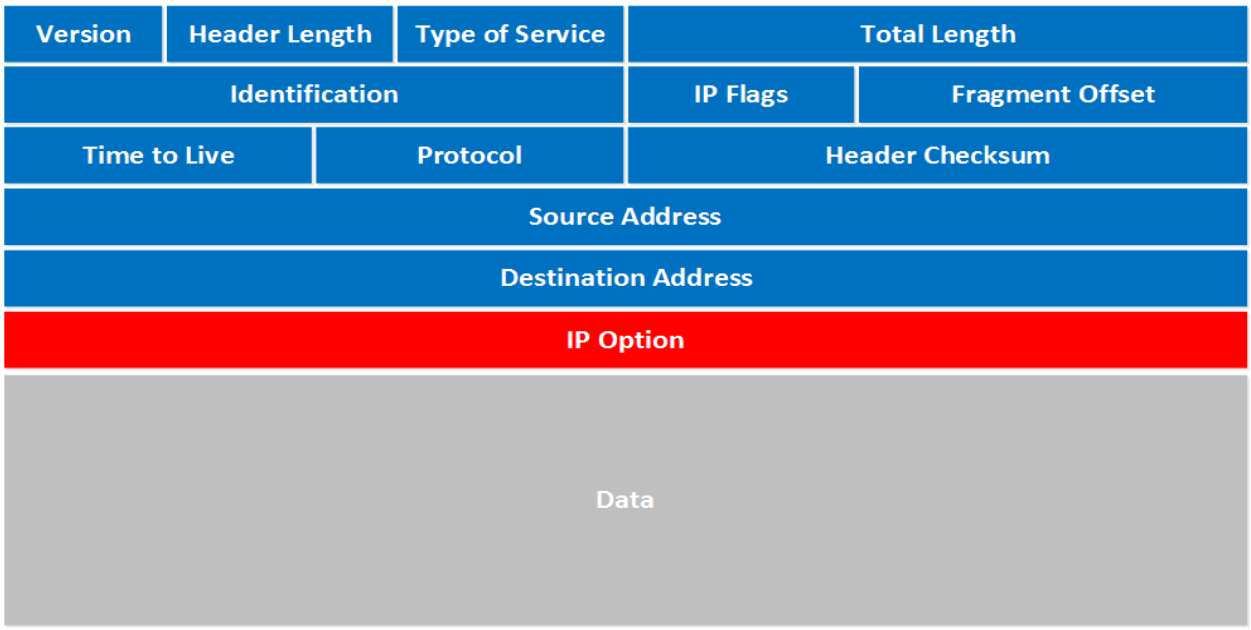
IPv4 was the first version of IP. It was deployed for production in the ARPANET in 1983. Today it is most widely used IP version. It is used to identify devices on a network using an addressing system.

The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. Till date, it is considered the primary Internet Protocol and carries 94% of Internet traffic.

Features of IPv4

- Connectionless Protocol
- Allow creating a simple virtual communication layer over diversified devices
- It requires less memory, and ease of remembering addresses
- Already supported protocol by millions of devices
- Offers video libraries and conferences

IPv4 Datagram Header
Size of the header is 20 to 60 bytes.



VERSION: *Version of the IP protocol (4 bits), which is 4 for IPv4*
HLEN: *IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.*
Type of service: *Low Delay, High Throughput, Reliability (8 bits)*
Total Length: *Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.*
Identification: *Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)*
Flags: *3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)*
Fragment Offset: *Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.*
Time to live: *Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.*
Protocol: *Name of the protocol to which the data is to be passed (8 bits)*
Header Checksum: *16 bits header checksum for checking errors in the datagram header*
Source IP address: *32 bits IP address of the sender*
Destination IP address: *32 bits IP address of the receiver*
Option: *Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*
Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

What is IPv6?

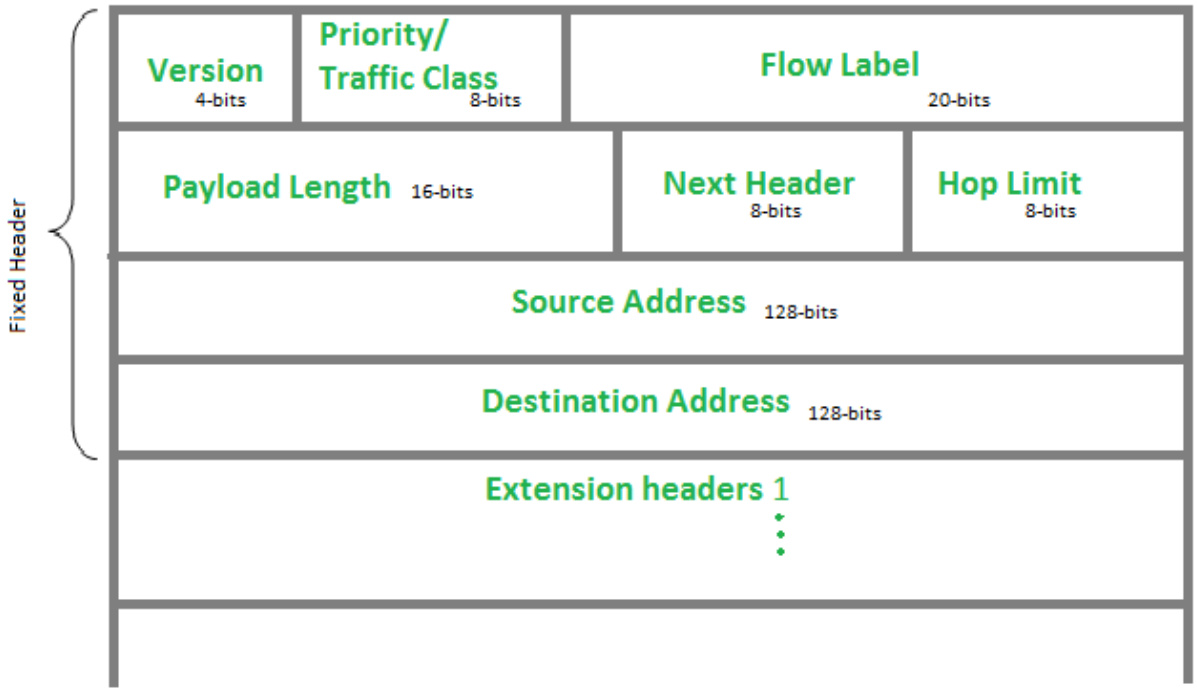
It is the most recent version of the Internet Protocol. Internet Engineer Taskforce initiated it in early 1994. The design and development of that suite is now called IPv6.

This new IP address version is being deployed to fulfill the need for more Internet addresses. It was aimed to resolve issues which are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 also called IPng (Internet Protocol next generation).

Features of IPv6

- Hierarchical addressing and routing infrastructure
- Stateful and Stateless configuration
- Support for quality of service (QoS)
- An ideal protocol for neighboring node interaction

IPv6 Header Format:



Version (4-bits) : Indicates version of Internet Protocol which contains bit sequence 0110.

Traffic Class (8-bits) : The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on priority of the packet. If congestion occurs on router then packets with least priority will be discarded.
As of now only 4-bits are being used (and remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.
Priority assignment of Congestion controlled traffic :

Priority	Meaning
0	No Specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to Uncontrolled data traffic.
Source node is allowed to set the priorities but on the way routers can change it. Therefore, destination should not expect same priority which was set by source node.

Flow Label (20-bits) : Flow Label field is used by source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real time service. In order to distinguish the flow, intermediate router can use source address, destination address and flow label of the packets. Between a source and destination multiple flows may exist because many processes might be running at the same time. Routers or Host that do not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, source is also supposed to specify the lifetime of flow.

Payload Length (16-bits) : It is a 16-bit (unsigned integer) field, indicates total size of the payload which tells routers about amount of information a particular packet contains in its payload. Payload Length field includes extension headers(if any) and upper layer packet. In case length of payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and jumbo payload option is used in the Hop-by-Hop options extension header.

Next Header (8-bits) : Next Header indicates type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packet, such as TCP, UDP.

Hop Limit (8-bits) : Hop Limit field is same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and packet is discarded if value decrements to 0. This is used to discard the packets that are stuck in infinite loop because of some routing error.

Source Address (128-bits) : Source Address is 128-bit IPv6 address of the original source of the packet.

Destination Address (128-bits) : Destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

Differences Between IPv4 and IPv6

Feature	IPv4	IPv6
Address length	32 bits	128 bits
Header size	20-60 bytes	40 bytes
IPSec support	Optional	Required
QoS support	Some	Better
Fragmentation	Hosts and routers	Hosts only
Checksum in header	Yes	No
Options in header	Yes	No
Link-layer address resolution	ARP (broadcast)	Multicast Neighbor Discovery Messages
Multicast membership	IGMP	Multicast Listener Discovery (MLD)
Router Discovery	Optional	Required
Uses broadcasts?	Yes	No
Configuration	Manual, DHCP	Automatic, DHCP
DNS name queries	Uses A records	Uses AAAA records
DNS reverse queries	Uses IN-ADDR.ARPA	Uses IP6.ARPA

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

Difference between Synchronous and Asynchronous Communication modes.

S.No.	Asynchronous Transmission	Synchronous Transmission
(i)	In asynchronous transmission, information is transmitted character by character.	In synchronous transmission, blocks of about 100 characters are transmitted at high-speed on the transmission line.
(ii)	At the beginning of a character, a start bit is sent. The nature of the start signal is standardized and is "understood" by the receiving end equipment which prepares to receive the coded character. The start signal is followed by the bits of coded character. If ASCII code is used, the seven coded bits and a parity bit are sent. Following the character code is stop signal.	A distinctive synchronization pattern is sent at the beginning of the block. The synchronization pattern is followed by codes to identify sender and receiver and the message characters. The message is terminated by an end of message character followed by a check character to aid detection of any transmission error.
(iii)	It is cheap.	It is expensive.
(iv)	It takes more time in data transmission.	It takes less time.
(v)	It does not require any local storage at the terminal end.	It needs for local buffer storages at the two ends of the line to assemble blocks.
(vi)	It does not require any synchronized clocks.	It requires accurately synchronized clocks at both ends.
(vii)	The transmission line is idle during the time intervals between transmitting characters.	Synchronous transmission is efficient utilization of the transmission line.
(viii)	It is used in low-speed communication like the connection of a terminal to a computer.	It is used in high-speed applications like the transmission of data from one computer to another.

OR

Asynchronous Communication	Synchronous Communication
Transmitter and receiver works at different clock	Transmitter and receiver works at same clock
Start and Stop bits are used for synchronization.	No Start and stop bits
Overhead is more due to start and stop bits	Less overhead compared to asynchronous communication
Distance limitation is more compared to synchronous communication	Communication is possible if device is closer to each other distance.
No Separate Clock Pin	Common CLK for synchronization
Cheap, Less Hardware	Expensive , Complex, Hardware
Example: RS232, RS485	Example: I2C, SPI