UNIT V Network Devices & Protocol

5.1 Networking Devices:

HUB:

A hub is a center of activities. In network terminology, a hub is a device where all connecting mediums come together. A hub is a medium used to collect signals from the input line(s) and redistribute them in various available wirings around a topology (topologies such as: 10baseT, 10baseF etc).

Hub basically acts as signal splitter, it accepts signal through its input port and passes it to the output ports. Some hubs help in regenerating the weak signals prior to sending them to the intended output lines, whereas some hubs help in synchronizing the data communication (in simple words, the hub not only provides the means of interface within the network, it also provides some additional and useful features). Sometimes, multiple hubs are interconnected in the network.

Generally hubs are used more commonly where star topology is used. The bridge creates two separate collision domains, the network after it has been segmented using a bridge.

If one LAN segment is busy, and the bridge needs to forward a frame onto the busy segment, the bridge simply buffers the frame (holds the frame in memory) until the segment is no longer busy. Reducing collisions, and assuming no significant change in the number of devices or the load on the network, greatly improves network performance.

A bridge between two hubs really creates two separate 10BASE-T networks , the total network bandwidth is doubled to 20 Mbps, as compared with the 10BASE-T network .

The Need of a Hub

Generally when we build a network using two or more computers, we need a hub. However, it is possible to connect two computers to each other directly without the need of a hub but when we add a third computer in the network, we need a hub to allow proper data communication within the network.

Types of Hubs

There are many types of hubs with various features/specifications, which provide the type of functionality you need in building a network. There are three main types of hubs: Passive hub, Active hub and Intelligent hub.

Passive Hubs

As the name suggests, passive hubs are the ones, which do not provide any additional feature except for working just as an interface between the topology. These types of hubs do not help in rectifying/enhancing the signals they pass on in the network, in other terms, they do not help in enhancing the performance of the network /LAN. It is very hard to get any help from the passive hubs while troubleshooting in case there is any fault in the hardware or the network.

A passive hub simply receives signal(s) on input port(s) and broadcasts it (them) on the output port(s) without even rectifying it (them).This type of HUB is just a wiring arrangement of joining ports. Passive hub does not require power supply.

Active Hubs

As you must have guessed from the name, active hub is a type of hub that takes active participation in data communication within the network/LAN.

Active hubs come with various features, such as receiving the signal (data) from the input port and storing it for sometime before forwarding it, this feature allows the hub to monitor the data it is

forwarding, some hubs come with a feature that helps in transmitting data that has high priority before the data that has lower priority (this feature is very important for some applications and some types of network), some hubs help in synchronizing data communication (by retransmitting the packets, which are not properly received at the receiving computer or by adjusting retransmission of the data packets to compensate timing), and some active hubs come with a feature that rectifies the data/signal before forwarding it in the network/LAN.
Active hubs also help in troubleshooting at a certain level. If there is a bottleneck within the network/LAN, active hubs can be used to find out the problem to a certain extent. Active hubs have some benefits over the use of passive hubs; however, active hubs are more expensive than passive hubs as they provide additional features.
A Passive Hub is just a connector. It connects the wires coming from different hubs. An active hub acts as a multiport repeater. Passive hub will not regenerate the signal but active hub will regenerate the signal ..... so active hub is better.

Intelligent Hubs

Intelligent hubs add some more features to that provided by the active hubs. An intelligent hub provides all the features of a passive and an active hub; it also provides some features, which help in managing the network resources effectively and efficiently.
Intelligent hubs help in improving the performance of the network/LAN that you are using. As an active hub helps in finding out where the problem persists, an intelligent hub itself finds out the problem in the network, diagnoses it and tries to rectify it without letting the problem hamper the performance of the network.
Intelligent hubs provide a feature that helps in determining the exact cause and exact place of the fault, this saves a lot of time and energy which otherwise would have been required for finding out the exact place of fault and identifying the solution for it.
Another feature of the intelligent hub is that they can decide which packet goes in which output line, this helps in controlling and minimizing data traffic in the network, which results in improved performance of the network/LAN.
Intelligent hubs also help in managing the data communication within the network, it recognizes the slower devices automatically and helps them to transmit the data with their own speed, and during this time, the hub manages the traffic within the network effectively. This feature also improves the performance of the network.
An intelligent hub also adopts the changes in the network very easily and it also supports different technologies without the need of changing anything in configuration. Nowadays, as the technology is progressing exponentially at every second, bigger and complex networks are built and need for hubs with additional features is increasing. The hubs are also being developed to incorporate the new features and help in building high performance, flexible and more manageable networks.

Switches

Like hubs, switches are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data that they receive. Where as a hub forwards the data it receives to all of the ports on the device, a switch forwards it only to the port that connects to the destination device.
It does this by learning the MAC address of the devices attached to it, and then by matching the destination MAC address in the data it receives. By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways.
First, by creating a direct path between two devices and controlling their communication, it can greatly reduce the number of collisions on the network. As you might recall, collisions occur on Ethernet networks when two devices attempt to transmit at exactly the same time.
Ethernet segment can use full- duplex logic , A switch’s effect of segmenting an Ethernet LAN into one collision domain per interface is sometimes called micro segmentation , all switch interfaces are running at 100 Mbps, with four collision domains.

In addition, the lack of collisions enables switches to communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send and receive data from the switch at the same time. Contrast this with half-duplex communication, in which communication can occur in only one direction at a time. Full-duplex transmission speeds are double that of a standard, half-duplex, connection. So, a 10Mbps connection becomes 20Mbps, and a 100Mbps connection becomes 200Mbps.
The net result of these measures is that switches can offer significant performance improvements over hub-based networks, particularly when network use is high.
Irrespective of whether a connection is at full or half duplex, the method of switching dictates how the switch deals with the data it receives.
The following is a brief explanation of each method:
Cut-through—In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is very fast, but creates the possibility of errors being propagated through the network, as there is no error checking.
Store-and-forward—Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.
Fragment Free—To take advantage of the error checking of store-and forward switching, but still offer performance levels nearing that of cut through switching, Fragment Free switching can be used. In a Fragment Free-switching environment, enough of the packet is read so that the switch can determine whether the packet has been involved in a collision. As soon as the collision status has been determined, the packet is forwarded.

Operating CISCO LAN Switches
The switch uses default settings so that all interfaces will work, assuming that the right cables and devices connect to the switch, and the switch forwards frames in and out of each interface.
Most Enterprises will want to be able to check on the switch's status, look at information about what the switch is doing, and possibly configure specific features of the switch.
Cisco has two major brands of LAN switching products. The Cisco Catalyst switch brand includes a large collection of switches, all of which have been designed with Enterprises (companies, governments, and so on) in mind. The Catalyst switches have a wide range of sizes, functions, and forwarding rates. Cisco Catalyst switch to monitor, configure, and troubleshoot problems.
The **Cisco Linksys s**witch brand includes a variety of switches designed for use in the home. Cisco uses the same concept of a command-line interface (CLI) with its router products and most of its Catalyst LAN switch products. The CLI is a text-based interface in which the user, typically a network engineer, enters a text command and presses Enter. Pressing Enter sends the command to the switch, which tells the device to do something.
The process of sending frames out all other interfaces, except the interface on which the frame arrived, is called flooding. Switches flood unknown unicast frames as well as broadcast frames.
Switches also flood LAN multicast frames out all ports .
STP blocks some ports from forwarding frames so that only one active path exists between any pair of LAN segments.

Repeaters :

Repeaters are physical Hardware device that have a primary function to Regenerate the electrical signal.
· A **repeater** is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of location LAN, so that the signal can cover longer distances.
· *All transmission media have a particular data carrying capacity but after some distance data will be weaken automatically during traveling and that weak or corrupted data called*

*as **attenuation***. Attenuation therefore limits the distance any medium can carry data.
· Repeaters are also used extensively in broadcasting, where they are known as translators, boosters or TV relay transmitters.
· Repeaters are often used in cable television and submarine communications cables, because the attenuation (signal loss) over such distances would be unacceptable without them. Repeaters are used in both copper-wire cables carrying electrical signals, and in fiber optics carrying light.
· An electronic device to receive a signal on a port and retransmits it at a higher level or higher power. it used when you need to go further distances than the cabling will allow.
· Adding a device that amplifies the signal can allow it to travel farther, increasing the size of the network.

The benefit of repeater is in three ways:

· 1. repeater boosts, increase signal power.
· 2. it help to enlarge network.
· 3. to connect longer distance networks.

The limitation of repeater :

· it cannot connect two distinct and dissimilar networks such as wireless LAN connect to Ring LAN.
· It will connect only similar networks such as Ethernet (BUS topology LAN) to STAR network because both uses a same packet format.

Repeaters fall into two categories :

· **Signal-Amplifiers** – Simply amplify the entire incoming signal. Unfortunately, they amplify both the signal and the noise.
This repeater is less expensive.
Signal-Regenerator – create an exact duplicate of incoming data. The original signal is duplicated, boosted to its original strength, and sent.
· It accept incoming signals and read whole data then all reading information will stored after that previous incoming data is deleting and it regenerate data using that stored information of data then regenerated data will send towards destination LAN.
· This repeater is more expensive than amplifier.

Bridge

A *bridge* is a device that connects two or more local area networks, or two or more segments of the same network.
· You can use a bridge to connect these two networks so that they can share information with each other.Bridges connect network segments. The use of a bridge increases the maximum possible size of your network.
· When bridges were introduced in the 1980's, they typically joined two homogeneous networks (for example, two kinds of Ethernet networks). More recently it has become possible for bridges to connect networks with different physical and data link layer protocols. For example, you can use a bridge to connect a Wireless network to wired network, or an Ethernet to Appletalk network and Ethernet to a TokenRing network and TokenRing to ATM.
· The organization may be geographically spread over several buildings separated by considerable distances. It may be cheaper to have separate LANs in each building and connect them with bridges than to run a single cable over the entire site.
· Unlike a repeater, which simply passes on all the signals it receives, a bridge selectively determines the appropriate segment to which it should pass a signal.
· Like switches, bridges learn the MAC addresses of all connected clients, servers, and peripherals, and associate each address with a bridge port (network connection). When a bridge (or switch) receives an incoming frame, it opens and reads its destination MAC address. If the

port that will receive the frame is different from the port connected to the sender, then the bridge forwards the frame to the destination port. If the port that will receive the frame is the same as the port connected to the sender, the bridge drops the frame.
· Traditional bridges connect a single workgroup to another workgroup. More recently, however, manufacturers have produced multiport bridges. Multiport bridges allow network managers to connect more than two network segments to each other.
· Bridges filter network traffic. They examine each set of data, transmitting only appropriate data to each connected segment. (Hubs, by contrast, broadcast all information to each connected computer, whether or not that computer is the intended recipient.) In this manner, bridges help reduce overall network traffic.

Router:

Like bridges, *routers* are devices whose primary purpose is to connect two or more networks and to filter network signals so that only desired information travels between them. For example, routers are often used to regulate the flow of information between school networks and the Internet. However, routers can inspect a good deal more information than bridges, and they therefore can regulate network traffic more precisely. They also have another important capability: they are aware of many possible paths across the network and can choose the best one for each data packet to travel.

 Features of Router :-

1) Multiple Active Paths
2) Identify address
3) Traffic Management
4) Sharing information
5) Filtering bad data
6) Performance

1) Multiple Active Paths:

Routers are able to keep track of multiple active paths between any given source and destination network.
This makes it more flexible and active towards faults than bridge.
This is because in a bridge multiple online active paths are not allowed.

2) Identify address:

Routers work on Network layer and can access more information from packet than bridge.
Router can identify source and destination network addresses within packet.

3) Traffic Management:

Router provides excellent traffic management using intelligent path selection.
Router select the best route, which is based on traffic loads, line speeds, number of one attached to another router.

4) Sharing information:

Router can share status and routing information with other routers. Routers can communicate with each other by doing this they can listen to network and identify which connections are busy and which are not.

5)Filtering bad data:

Routers do not forward any information that does not have a correct network address. This is the reason they don't forward bad data.

6)Performance:

Routers perform complex task and it is continuously busy to execute network data.
This means they are slower than bridge because they keep processing data intensively.

 Types of Routing :-

There are two types of routers 1.Static Router 2.Dynamic Router

1) Static Router :-

Each router has its own software called 'Routing Table'. Administrator is a person who

configures and maintains whole network as well as networking devices.
Administrators have to manually configure routes between each network when the routers do not communicate amongst themselves that type of routers are called static routers.
Its advantage is that complete control remains with the network administrator.

2) Dynamic Router :-

Dynamic routers are those routers, which automatically find their own routes by communicating with each other.
These routers are self configured. This is because their routing tables are built and modified through these communications and these changes are quickly reflected. e.g. router failure pr broken links.

Gateways -

Routers can successfully connect networks with protocols that function in similar ways. When the networks that must be connected are using completely different protocols from each other, however, a more powerful and intelligent device is required.
A *gateway* is a device that can interpret and translate the different protocols that are used on two distinct networks.

What is the difference between?

Router: - Device to interconnect SIMILAR networks, e.g. similar protocols & workstations & servers. Used to connect LAN, MAN to WAN, because all use same type of packet.

Gateway: - Device to interconnect DISSIMILAR network e.g dissimilar protocols technology and servers such as Ethernet to ATM. Here Ethernet use packet and ATM use cell.

Protocol: FTP, HTTP,SMTP, DNS

1. FTP (File Transfer Protocol)

FTP protocol (File Transfer Protocol) is, as its name indicates a protocol for transferring files. The original specification for the File Transfer Protocol was written by Abhay Bhushan and published as RFC 114 on 16 April 1971. The implementation of FTP dates from 1971 when a file transfer system (described in RFC141) between MIT machines (Massachusetts Institute of Technology) was developed. Many RFC have since made improvements to the basic protocol, but the greatest innovations date from July 1973.

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.
File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet.
As a user, you can use FTP with a simple command line interface (for example, from the Windows MS-DOS Prompt window) or with a commercial program that offers a graphical user interface. Your Web browser can also make FTP requests to download programs you select from a Web page. Using FTP, you can also update (delete, rename, move, and copy) files at a server. You need to logon to an FTP server. However, publicly available files are easily accessed using anonymous FTP. Basic FTP support is usually provided as part of a suite of programs that come with TCP/IP. However, any FTP client program with a graphical user interface usually must be downloaded from the company that makes it.

2. Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. HTTP functions as a request-response protocol in the client-server computing model. A web browser, for example, may be the client and an application running on a computer hosting a web site may be the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body.
HTTP resources are identified and located on the network by Uniform Resource Identifiers (URIs)—or, more specifically, Uniform Resource Locators (URLs)—using the http or https URI schemes. URIs and hyperlinks in Hypertext Mark up Language (HTML) documents form webs of inter-linked hypertext documents. On the Internet the World Wide Web was established in 1990 by English computer scientist and innovator Tim Berners-Lee.

3. Simple Mail Transfer Protocol (SMTP)

SImple Mail Transfer Protocol is an Internet protocol designed to send and receive e-mail messages between e-mail servers over the Internet.
SMTP was developed to send e-mail messages across the Internet. In the OSI model, SMPT is an application layer protocol that utilizes TCP as the transport protocol to transmit mail to a destination mail exchanger, in other words, SMTP is used to transmit mail to a mail server. Mail can be transmitted by a client to the mail exchanger server, or from mail exchanger to mail exchanger. Mail sent via SMTP is usually sent from one mail exchanger to another, directly. E-mail was never designed to be instantaneous, but that is often how it appears to us.

Mail Exchangers (MX)

Mail Exchangers are the name given to the applications that support the SMTP protocol. Mail Exchangers such as sendmail or Microsoft Exchange should listen for IP datagrams that arrive on the network interface with a TCP port number of 25 and on . This port is one of the 'well known ports' defined in RFC 1700. When a message is received, the mail exchanger should check to see if it is for one of it's users, then move the mail to the user's mailbox.
To identify the mail exchangers for a domain name, DNS zone files for the domain contain an MX resource record identifying the host name and IP address of the mail exchangers.
Simple mail transfer protocol differs from Post Office Protocol version 3 (POP3). POP3 is used by e-mail client applications such as Microsoft Outlook, Mozilla Thunderbird, Eudora and other e-mail applications to retreive mail stored in personal mailboxes at the mail server.

E-Mail Clients

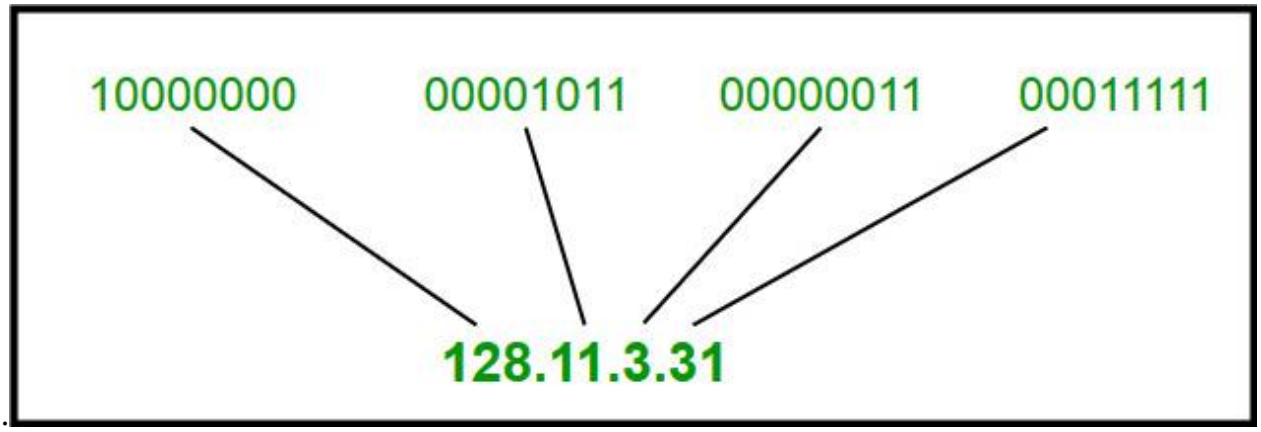
E-mail is a client-server protocol that allows the exchange of messages and attachments in various formats. An e-mail client is a software application which seamlessly handles all the technical communications tasks to connect to and find the e-mail at the server, download the e-mail messages, organizes them and presents them to the user in a usable format. An e-mail client also provides the means to compose new messages, reply to and forward received messages, and to organize the messages for later review.
E-mail clients use POP3 or IMAP instead of SMTP. SMTP is used strictly between mail servers.
Outlook Express
Outlook
Mozilla Thunderbird
Web Mail Systems

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

A name server (also spelled nameserver) consists of a program or computer server that implements a name-service protocol. It maps a *human-recognizable* identifier to a system-internal, often numeric, identification or addressing component.
The most prominent types of name servers in operation today are the name servers of the Domain Name System (DNS), one of the two principal name spaces of the Internet. The most important function of these DNS servers is the translation (resolution) of humanly memorable domain names and hostnames into the corresponding numeric Internet Protocol (IP) addresses, the second principal Internet name space, used to identify and locate computer systems and resources on the Internet.
The Internet maintains two principal namespaces, the domain name hierarchy and the Internet Protocol (IP) address system. The Domain Name System maintains the domain namespace and provides translation services between these two namespaces. Internet name servers implement the Domain Name System. A DNS name server is a server that stores the DNS records, such as address (A) records, name server (NS) (see also List of DNS record types) and responds with answers to queries against its DB.
The top hierarchy of the Internet Domain Name Server is served by the root name servers maintained by delegation by the **Internet Corporation for Assigned Names and Numbers (ICANN).**

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 2^{32}.
Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation



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

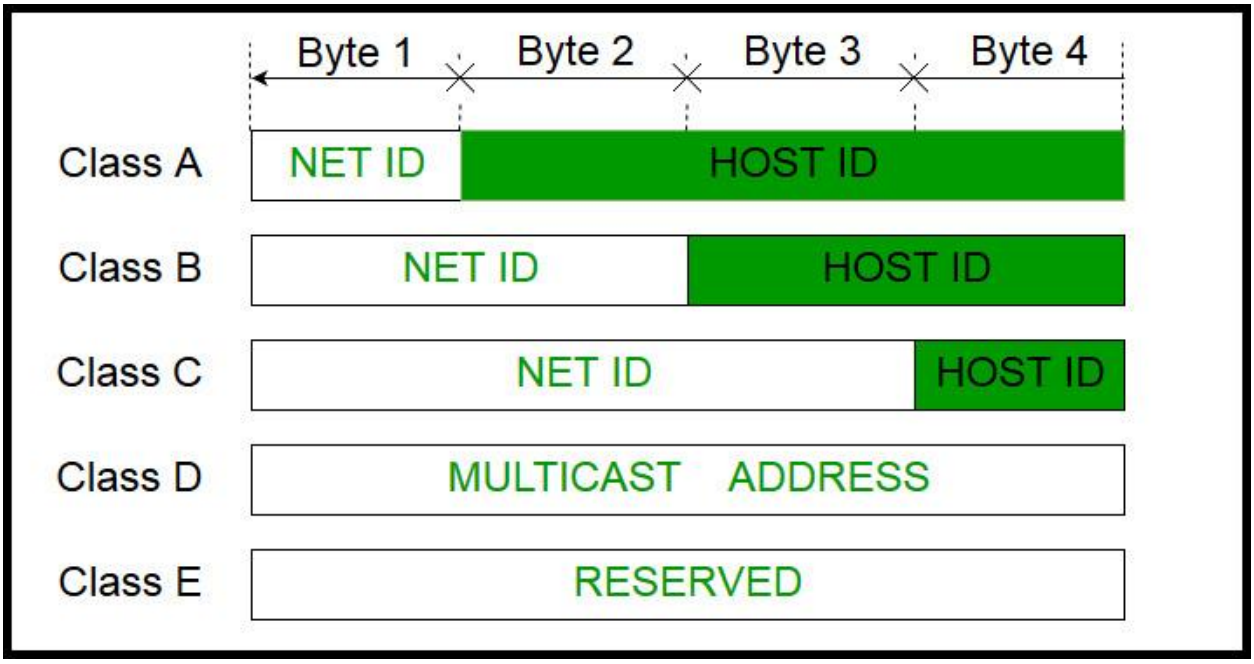
- Class A
- Class B
- Class C
- Class D
- Class E

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.



Class A Address

The first bit of the first octet is always set to zero. So that the first octet ranges from 1 – 127. The class A address only include IP starting from 1.x.x.x to 126.x.x.x. The IP range 127.x.x.x is reserved for loop back IP addresses. The default subnet mask for class A IP address is 255.0.0.0. This means it can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2). Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH.

Class B Address

Here the first two bits in the first two bits is set to zero. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses. Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of this class has its first 3 bits set to 110. Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives 2097152 (2^{21}) Network addresses and 254 (2^8-2) Host addresses. Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Class D Address

The first four bits of the first octet in class D IP address are set to 1110. Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not intended for a particular host, but multiple ones. That is why there is no need to extract host address from the class D IP addresses. The Class D does not have any subnet mask.

Class E Address

The class E IP addresses are reserved for experimental purpose only for R&D or study. IP addresses in the class E ranges from 240.0.0.0 to 255.255.255.254. This class too is not equipped with any subnet mask

Class	Starting Address	Ending Address	Subnet mask
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	255.255.255.255
E	240.0.0.0	255.255.255.255	255.255.255.255

For the IP addresses from Class A, the first 8 bits (the first decimal number) represent the network part, while the remaining 24 bits represent the host part. For Class B, the first 16 bits (the first two numbers) represent the network part, while the remaining 16 bits represent the host part. For Class C, the first 24 bits represent the network part, while the remaining 8 bits represent the host part.

Web mail systems provide a website that handles all the tasks normally reserved for a local e-mail application. Users can open a web browser and connect to Google, Yahoo, AOL and several other providers and perform most if not all of the tasks that can be performed with a standard e-mail client.

Gmail
Yahoo Mail
AOL Mails