IP Addressing & TCP/IP

Protocol

Network protocols are sets of established rules that dictate how to format, transmit and receive data so computer network devices -- from servers and routers to endpoints -- can communicate regardless of the differences in their underlying infrastructures, designs or standards.

How network protocols work

Network protocols break larger processes into discrete, narrowly defined functions and tasks across every level of the network. In the standard model, known as the Open Systems Interconnection (OSI) model, one or more network protocols govern activities at each layer in the telecommunication exchange.

TCP/IP

- A set of cooperating network protocols is called a protocol suite. The **TCP/IP** suite includes numerous protocols across layers -- such as the data, network, transport and application layers -- working together to enable internet connectivity.

These include:

- Transmission Control Protocol (TCP), which uses a set of rules to exchange messages with other internet points at the information packet level;
- User Datagram Protocol (UDP), which acts as an alternative communication protocol to TCP and is used to establish low-latency and loss-tolerating connections between applications and the Internet.
- Internet Protocol (IP), which uses a set of rules to send and receive messages at the Internet address level.
- Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP), each of which has defined sets of rules to exchange and display information.

FTP (File Transfer Protocol)

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Telnet (TELecommunication NETwork)

- Telnet, developed in 1969, is a protocol that provides a command line interface for communication with a remote device or server, sometimes employed for remote management but also for initial device setup like network hardware. Telnet stands for Teletype Network, establish a connection using the Telnet protocol.
- Because it was developed before the mainstream adaptation of the internet, Telnet on its own does not employ any form of encryption, making it outdated in terms of modern security. It has largely been overlapped by Secure Shell (SSH) protocol, at least on the public internet, but for instances where Telnet is still in use

Class Concept of Networking

- IPv4 addresses are 32 bits long (four bytes).
- An example of an IPv4 address is 216.58.216.164, which is the front page of Google.com.
- Maximum number of IPv4 addresses, which is called its address space, is about 4.3 billion. In the 1980s, this was sufficient to address every networked device, but scientists knew that this space would quickly become exhausted. Technologies such as NAT have delayed the problem by allowing many devices to use a single IP address, but a larger address space is needed to serve the modern Internet.

IPv6

- A major advantage of IPv6 is that it uses 128 bits of data to store an address, permitting 2^{128} unique addresses, or 340,282,366,920,938,463,463,374,607,431,768,211,456.
- The size of IPv6's address space — 340 duo decillion — is much, much larger than IPv4.

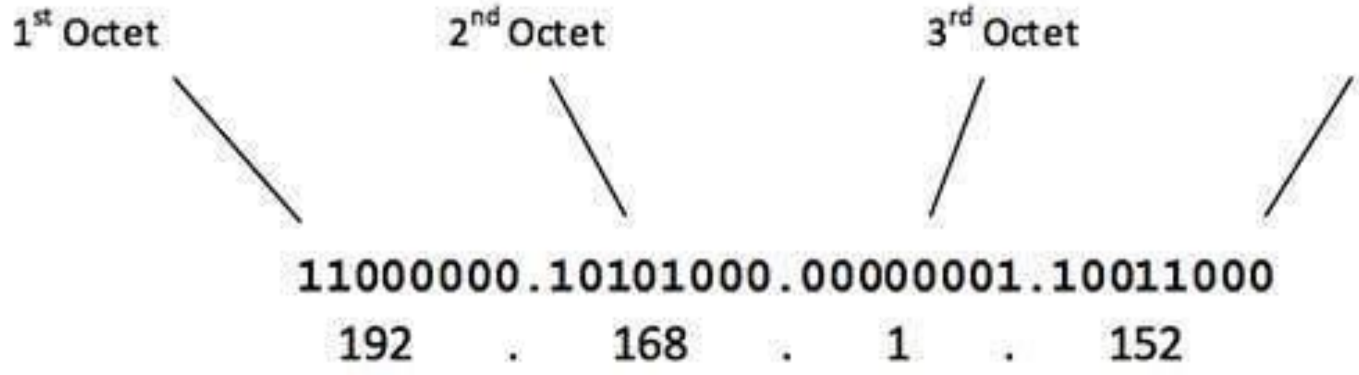
Classes of IP Addressing. (IPv4)

- TCP/IP defines five classes of IP addresses:

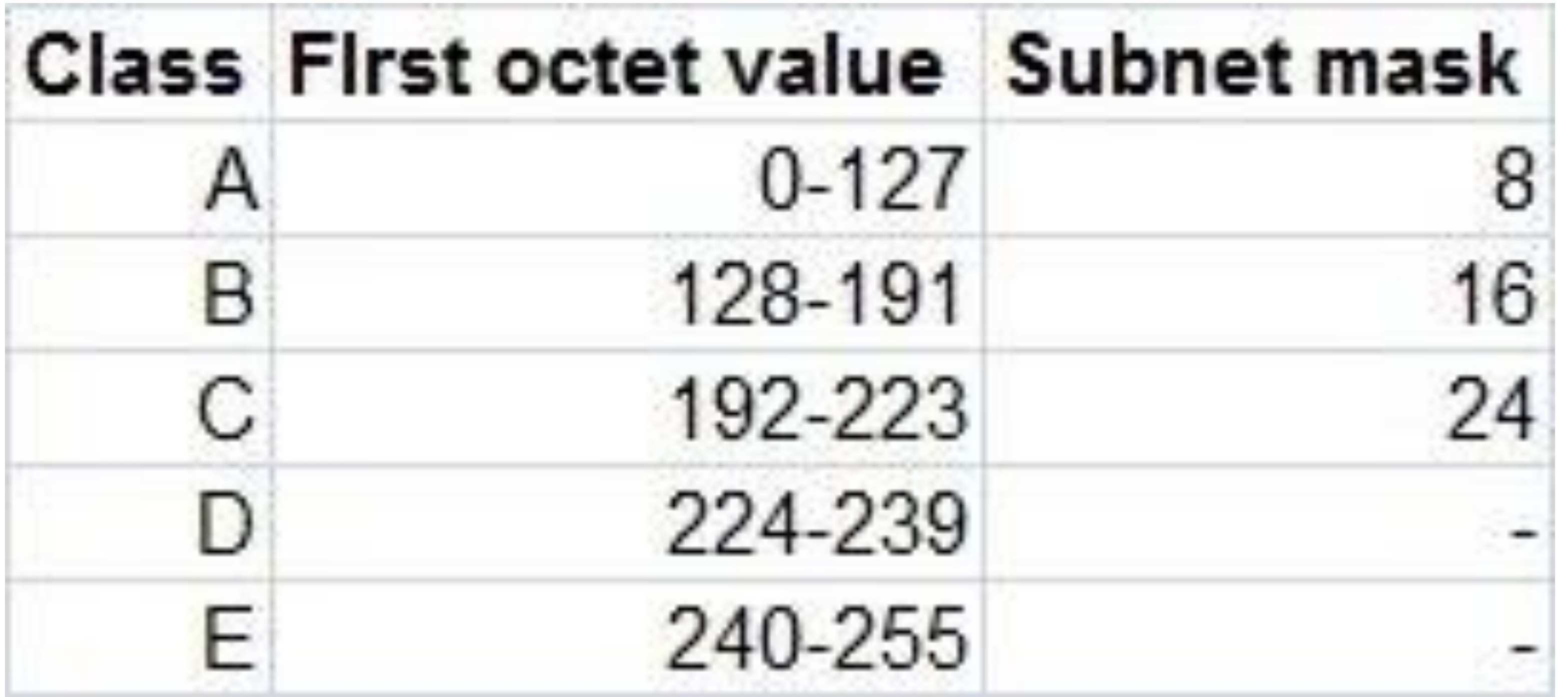
Each class has a range of **class A, B, C, D, and E.** valid IP addresses.

- The value of the first octet determines the class.
- IP addresses from the first three classes (A, B and C) can be used for host addresses.
- The other two classes are used for other purposes – class D for multicast and class E for experimental purposes.

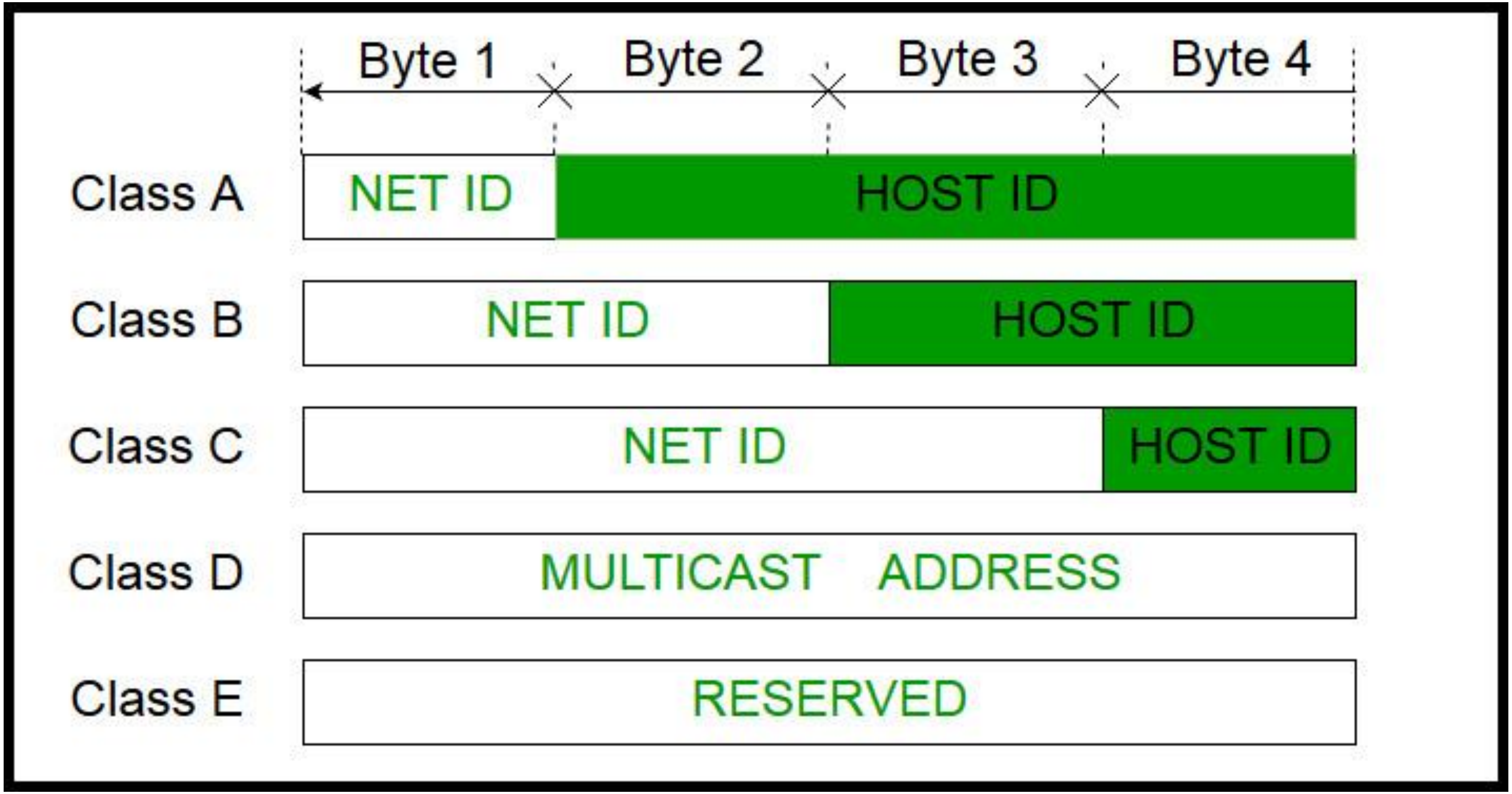
- The system of IP address classes was developed for the purpose of Internet IP addresses assignment.
- The classes created were based on the network size.
- For example, for the small number of networks with a very large number of hosts, the Class A was created.
- **The Class C was created for numerous networks with small number of hosts.**



Classes of IP addresses are:



Class	First octet value	Subnet mask
A	0-127	8
B	128-191	16
C	192-223	24
D	224-239	-
E	240-255	-


Byte 1
Byte 2
Byte 3
Byte 4
Class A
NET ID
HOST ID
Class B
NET ID
HOST ID
Class C
NET ID
HOST ID
Class D
MULTICAST ADDRESS
Class E
RESERVED

Class	Address range	Supports
Class A	**1.0.0.1 - 126.255.255.254**	Supports 16 million hosts on each of 127 networks.
Class B	**128.1.0.1 - 191.255.255.254**	Supports 65,000 hosts on each of 16,000 networks.
Class C	**192.0.1.1 - 223.255.254.254**	Supports 254 hosts on each of 2 million networks.
Class D	**224.0.0.0 - 239.255.255.255**	Reserved for multicast groups.
Class E	**240.0.0.0 - 254.255.255.254**	Reserved for future use, or research and development purposes.

- **For 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.

Consider the following IP addresses:

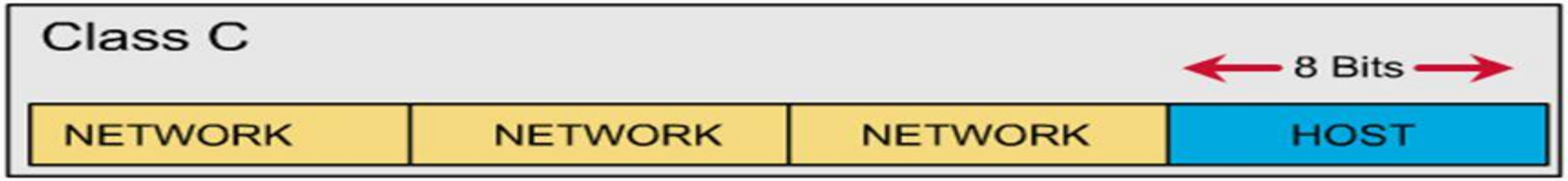
- **10.50.120.7** – because this is a Class A address, the first number (10) represents the network part, while the remainder of the address represents the host part (50.120.7). This means that, in order for devices to be on the same network, the first number of their IP addresses has to be the same for both devices. In this case, a device with the IP address of 10.47.8.4 is on the same network as the device with the IP address listed above. The device with the IP address 11.5.4.3 is not on the same network, because the first number of its IP address is different.
- **172.16.55.13** – because this is a Class B address, the first two numbers (172.16) represent the network part, while the remainder of the address represents the host part (55.13). A device with the IP address of 172.16.254.3 is on the same network, while a device with the IP address of 172.55.54.74 isn't.

- Class C

In a Class C network, the first two bits are set to 1, and the third bit is set to 0. That makes the first 24 bits of the address the network address and the remainder as the host address. Class C network addresses range from 192.0.0.0 to 223.255.255.0. There are over 2 million possible Class C networks.

- Example for a Class C IP address: 192.168.178.1

IP address classes: Class C



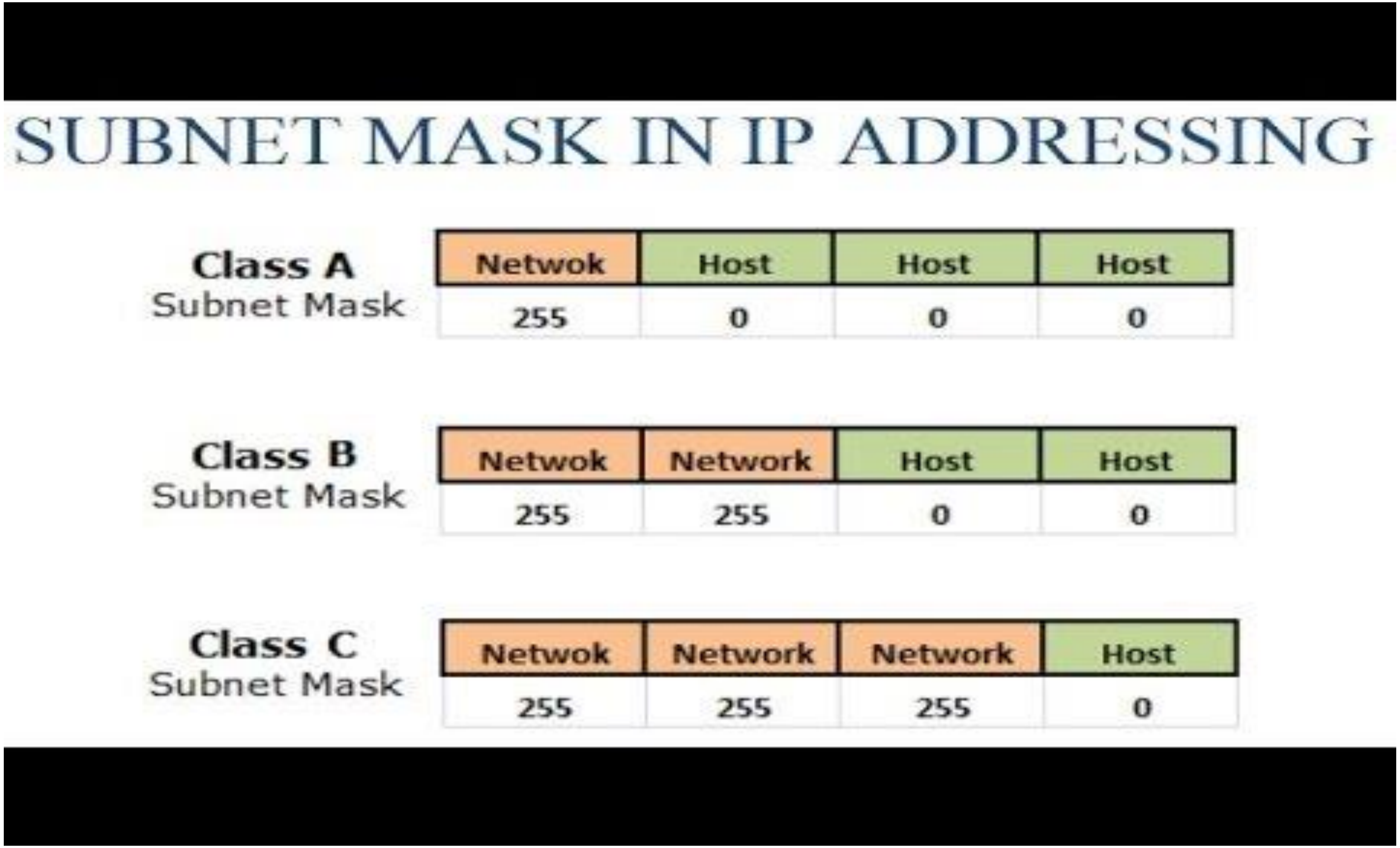
Special IP address ranges that are used for special purposes are:

- **0.0.0.0/8 – addresses used to communicate with the local network**
- **127.0.0.0/8 – loopback addresses**
- **169.254.0.0/16 – link-local addresses (APIPA)**

Subnet Mask

- A subnet mask is a number that defines a range of IP addresses available within a network. A single subnet mask limits the number of valid IPs for a specific network. Multiple subnet masks can organize a single network into smaller networks (called subnetworks or subnets). Systems within the same subnet can communicate directly with each other, while systems on different subnets must communicate through a router.

- 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.
- It uses the same format as an IPv4 address — four sections of one to three numbers, separated by dots.
- Each section of the subnet mask can contain a number from 0 to 255, just like an IP address.
- For example, a typical subnet mask for a Class C IP address is: **255.255.255.0**



SUBNET MASK IN IP ADDRESSING

Class A	Netwok	Host	Host	Host
Subnet Mask	255	0	0	0

Class B	Netwok	Network	Host	Host
Subnet Mask	255	255	0	0

Class C	Netwok	Network	Network	Host
Subnet Mask	255	255	255	0

SMTP

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
- It can send a single message to one or more recipients.
- Sending message can include text, voice, video or graphics.
- It can also send the messages on networks outside the internet.

Working of SMTP

- **Composition of Mail:** A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.
- **Submission of Mail:** After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.
- **Delivery of Mail:** E-mail addresses contain two parts: username of the recipient and domain name. For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name. If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.

- **Receipt and Processing of Mail:** Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.
- **Access and Retrieval of Mail:** The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

Telnet

- Telnet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text-based communication channel between two machines. It follows a user command Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocol for creating remote sessions.
- On the web, Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) simply enable users to request specific files from remote computers, while, through Telnet, users can log on as a regular user with the privileges they are granted to the specific applications and data on that computer.

How Telnet works

- Telnet is a type of client-server protocol that can be used to open a command line on a remote computer, typically a server. Users can utilize this tool to ping a port and find out whether it is open. Telnet works with what is called a virtual terminal connection emulator, or an abstract instance of a connection to a computer, using standard protocols to act like a physical terminal connected to a machine. FTP may also be used along with Telnet for users working to send data files
- Users connect remotely to a machine using Telnet, sometimes referred to as Telnetting into the system. They are prompted to enter their username and password combination to access the remote computer, which enables the running of command lines as if logged in to the computer in person. Despite the physical location of users, their IP address will match the computer logged in to rather than the one physically used to connect.

File Transfer Protocol (FTP),

- File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.
- FTP is a client-server protocol where a client will ask for a file, and a local or remote server will provide it.
- The end-users machine is typically called the local host machine, which is connected via the internet to the remote host—which is the second machine running the FTP software.

How FTP works

- FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content.
- Clients initiate conversations with servers by requesting to download a file.
- Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, known as anonymous FTP.

- FTP sessions work in passive or active modes.
- In active mode, after a client initiates a session via a command channel request, the server initiates a data connection back to the client and begins transferring data.
- In passive mode, the server instead uses the command channel to send the client the information it needs to open a data channel.
- Because passive mode has the client initiating all connections, it works well across firewalls and Network Address Translation (NAT) gateways.

Hyper Text Transfer Protocol (HTTP)

- HTTP stands for HyperText Transfer Protocol.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.

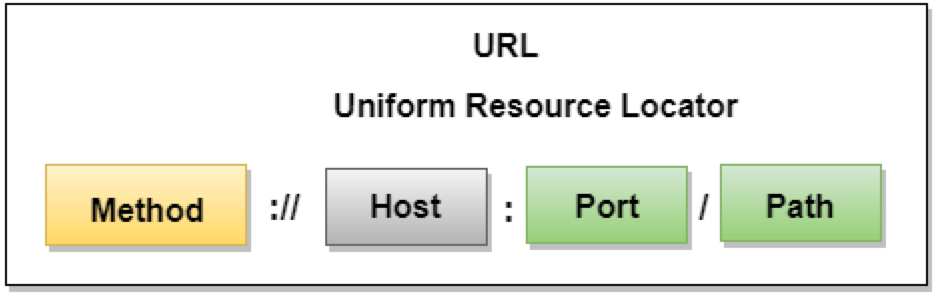
Features of HTTP:

- Connectionless protocol:

HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.

Uniform Resource Locator (URL)

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.



- Method: The method is the protocol used to retrieve the document from a server. For example, HTTP.
- Host: The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- Port: The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- Path: Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

Simple Network Management Protocol (SNMP).

- If an organization has 1000 of devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

- Simple Network Management Protocol (SNMP) –
- SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices.

SNMP components –
There are 3 components of SNMP:

- SNMP Manager –It is a centralised system used to monitor network. It is also known as Network Management Station (NMS)
- SNMP agent –It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.
- Management Information Base –MIB consists of information of resources that are to be managed. These information is organised hierarchically. It consists of objects instances which are essentially variables.

LDAP (Lightweight Directory Access Protocol).

- Lightweight Directory Access Protocol (LDAP) is an internet protocol works on TCP/IP, used to access information from directories. LDAP protocol is basically used to access an active directory.

Features of LDAP:

- Functional model of LDAP is simpler due to this it omits duplicate, rarely used and esoteric feature.
- It is easier to understand and implement.
- It uses strings to represent data

- Directories:
- Directories are set of object with similar attributes, organised in a logical and hierarchical manner. For example, Telephonic Directories. It is a distributed database application used to manage attributes in a directory.
- LDAP defines operations for accessing and modifying directory entries such as:
- Searching for user specified criteria
- Adding an entry
- Deleting an entry
- Modifying an entry
- Modifying the distinguished name or relative distinguished name of an entry
- Comparing an entry

Concept of Dynamic Host Control Protocol.

- In networks with a large number of hosts, statically assigning IP addresses and other IP information quickly becomes impractical.
- Dynamic Host Control Protocol (DHCP) provides administrators with a mechanism to dynamically allocate IP addresses, rather than manually setting the address on each device.
- DHCP servers lease out IP addresses to DHCP clients, for a specific period of time. There are four steps to this DHCP process:

- When a DHCP client first boots up, it broadcasts a DHCP Discover message, searching for a DHCP server.
- If a DHCP server exists on the local segment, it will respond with a DHCPOffer, containing the “offered” IP address, subnet mask, etc.
- Once the client receives the offer, it will respond with a DHCP Request, indicating that it will accept the offered protocol information.
- Finally, the server responds with a DHCPACK, acknowledging the clients acceptance of offered protocol information.

- By default, DHCP leases an address for 8 days. Once 50% of the lease expires, the client will try to renew the lease with the same DHCP server. If successful, the client receives a new 8 day lease.

Network Security

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired'', an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them.

Types of Network Security Devices

- Active Devices : These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.
- Passive Devices : These devices identify and report on unwanted traffic, for example, intrusion detection appliances.
- Preventative Devices : These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.
- Unified Threat Management (UTM) : These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls

- A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.
- Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Hardware and Software Firewalls

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

- Antivirus

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Content Filtering

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

Content filtering can be divided into the following categories −

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

- Intrusion Detection Systems
- Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.
- Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage.