Chapter Four

Network Layer Addressing and Routing

Layer-3 in the OSI model is called Network layer. Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of
the packet between two systems on the same network (links), the network layer ensures
that each packet gets from its point of origin to its final destination.

The network layer is responsible for the delivery of individual packets from the source to the destination host.

The network layer adds a header that includes the logical addresses of the sender
and receiver to the packet corning from the upper layer. If a packet travels through the Internet, we need this addressing system to help distinguish the source and destination.

Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

Functionalities

Devices which work on Network Layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal. These can be:

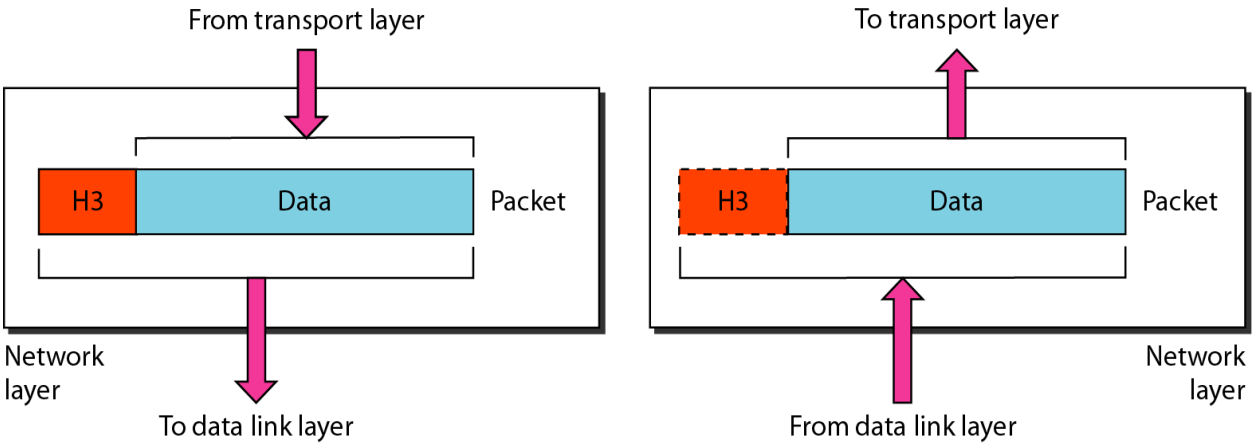
- Addressing devices and networks.

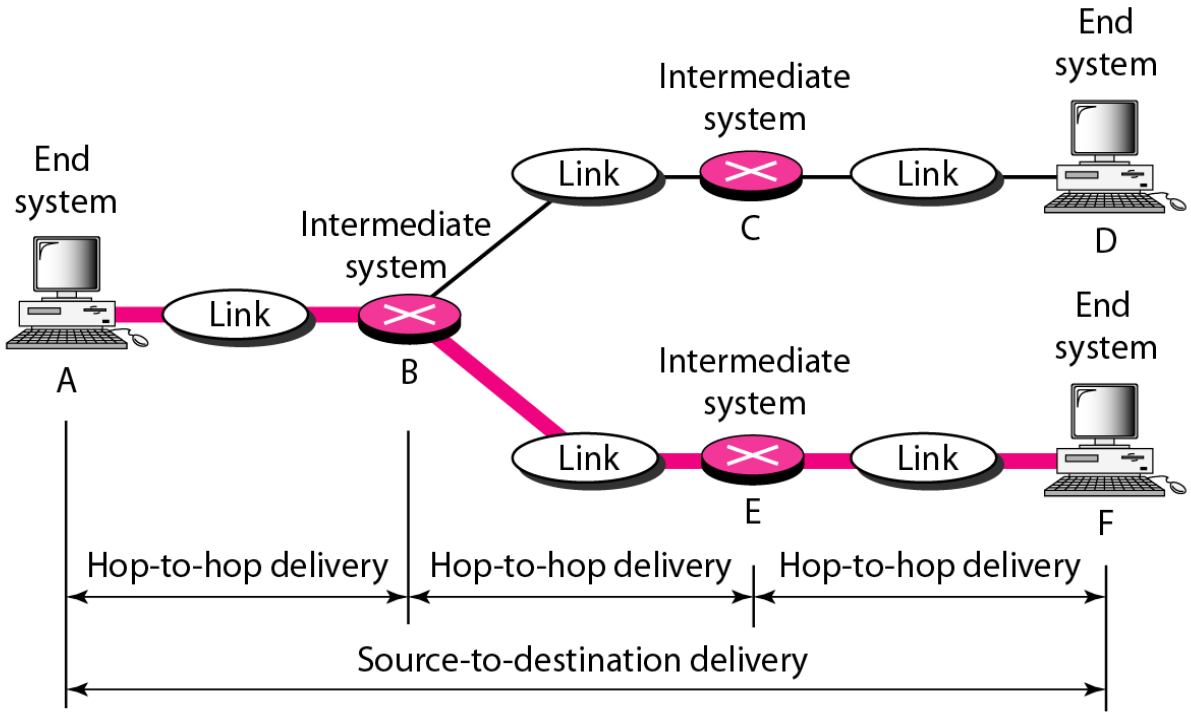
- Routing and Forwarding.
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism.

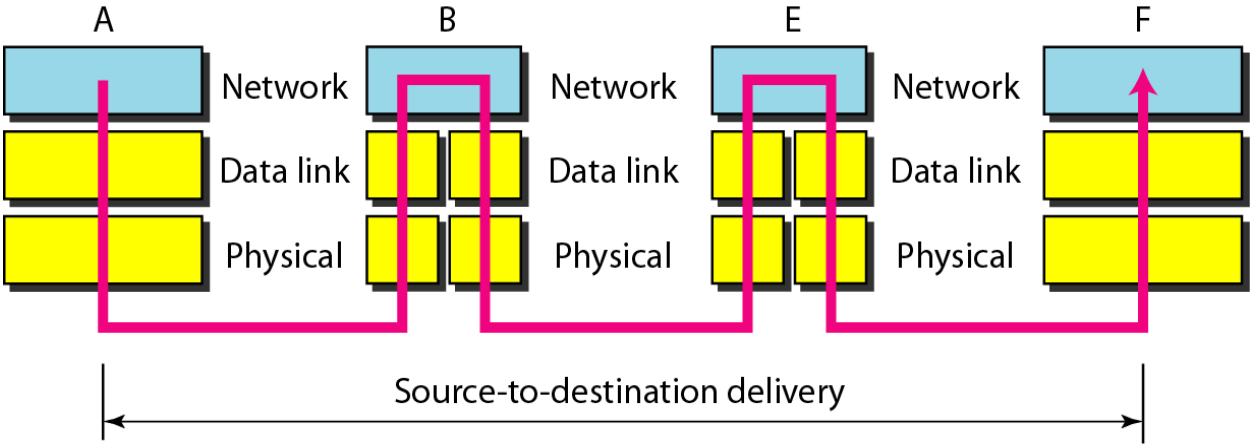
Network Layer

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links)
- Is responsible for the delivery of individual packets from the source host to the destination host.
- Logical connection setup, data forwarding, routing and delivery error reporting are the network layer's primary responsibilities.
- Its the backbone of the OSI Model. It selects and manages the best logical path (virtual circuit) for data transfer between nodes by assigning destination and source IP addresses to each data segment.

- Internet Protocol (IP) is the most important protocol in this layer. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.
- The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols.
- IP does not provide reliability, flow control or error recovery. These functions must be provided at a higher level.
- Part of communicating messages between computers is a routing function that ensures that messages will be correctly delivered to their destination. IP provides this routing function


From transport layer
H3
Data
Packet
Network layer
To data link layer
To transport layer
H3
Data
Packet
Network layer
From data link layer


End system
Intermediate system
End system
Link
Link
C
D
Intermediate system
End system
Link
A
B
Intermediate system
Link
Link
E
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
Source-to-destination delivery


A
B
E
F
Network
Network
Network
Data link
Data link
Data link
Physical
Physical
Physical
Source-to-destination delivery

- IP transports data in packets called *datagrams,* each of which is transported separately.
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated.

Address Resolution (ARP) is used to associate a logical address with a physical address. It used to find the physical address of the node when its Internet address is known .

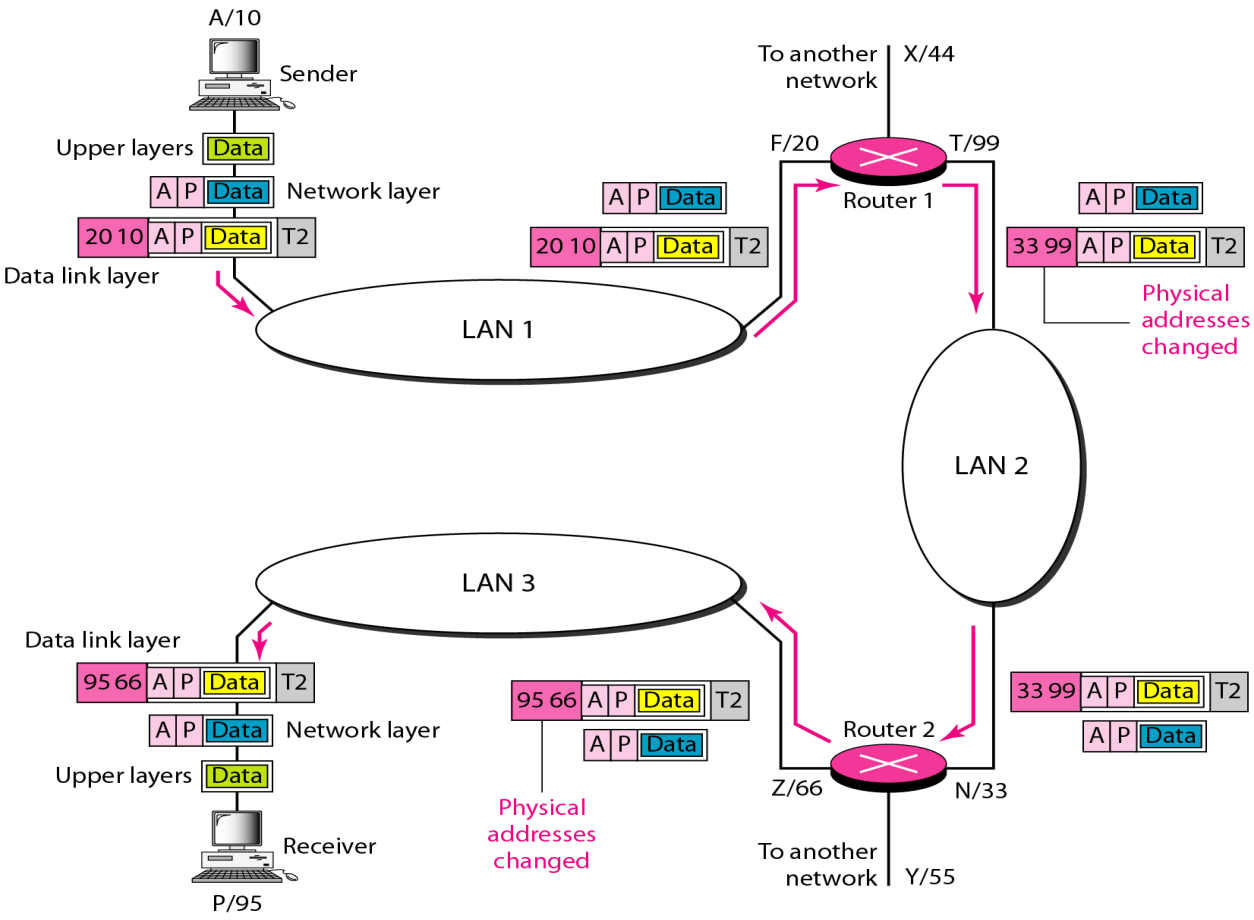
Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time.

Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

Gateways- is a device that provide connectivity between two or more network segments. It may be a router, firewall or other that enables traffic to flow in and out of the network.

Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

Example:- Figure below shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.



Functions of Network Layer:

- ✓ Internetworking
- ✓ Logical Addressing
- ✓ Routing: it determines the best optimal path out of the multiple paths from source to the destination.
- ✓ Packetizing: A Network Layer receives the data from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Packetizing

The process of encapsulating the data received from upper layers of the network(also called as payload) in a network layer packet at the source and decapsulating the

payload from the network layer packet at the destination is known as packetizing.

The source host adds a header that contains the source and destination address and some other relevant information required by the network layer protocol to the payload received from the upper layer protocol, and delivers the packet to the data link layer.

IP addressing

An IP address (*internet protocol address*) is a numerical representation that uniquely identifies a specific interface on the network. IP stands for Internet Protocol and describes a set of standards and requirements for creating and transmitting data packets, or datagrams, across networks.

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.

There are two versions of IP in use today, IPv4 and IPv6. The original IPv4 protocol is still used today on both the internet, and many corporate networks. However, the IPv4 protocol only allowed for 2^{32} addresses. This, coupled with how addresses were allocated, led to a situation where there would not be enough unique addresses for all devices connected to the internet.

IPv6 was developed by the Internet Engineering Task Force (IETF), and was formalized in 1998. This upgrade substantially increased the available address space and allowed for 2^{128} addresses. In addition, there were changes to improve the efficiency of IP packet headers, as well as improvements to routing and security.

IPv4 ADDRESSES

An IPv4 address is a 32-bit address that *uniquely* and *universally* defines the connection of a device (for example, a computer or a router) to the Internet. IPv4 addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time. The IPv4 addresses are universal in the sense that the

addressing system must be accepted by any host that wants to be connected to the Internet.

Address Space

A protocol such as IPv4 that defines addresses has an address space. IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet

Notations

There are two prevalent notations to show an IPv4 address: **binary notation** and **dotted decimal** notation.

Binary Notation

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a

4-byte address. The following is *an* example of an IPv4 address in binary notation:

01110101 10010101 00011101 00000010

Dotted-Decimal Notation

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the *dotted~decimal* notation of the above address:

117.149.29.2

Example 19.3

Find the error, if any, in the following IPv4 addresses.

a. 111.56.045.78

b. 221.34.7.8.20

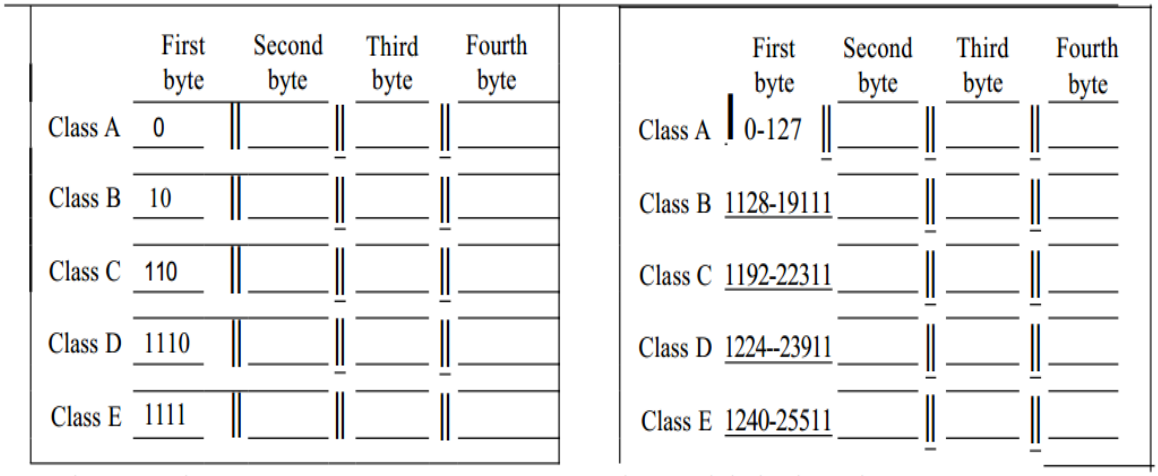
c. 75.45.301.14

d. 11100010.23.14.67

Classful Addressing

IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.

We can find the class of an address when given the address in binary notation or dotted-decimal notation. If the address is given in binary notation, the first few bits can immediately tell us the class of the address. If the address is given in decimal-dotted notation, the first byte defines the class. Both methods are shown in Figure 19.2.



Example 19.4

Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Classes and Blocks

One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size as shown in Table 19.1.

Table 19.1 *Number ofblocks and block size in classfullPv4 addressing*

Class	*Number ofBlocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,	

Class A addresses were designed for large organizations with a large number of attached hosts or routers. Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers. Class C addresses were designed for small organizations with a small number of attached hosts or routers.

A block in class A address is too large for almost any organization. This means most of the addresses in class A were wasted and were not used. A block in class B is also very large, probably too large for many of the organizations that received a class B block. A block in class C is probably too small for many organizations. Class D addresses were designed for multicasting as we will see in a later chapter. Each address in this class is used to define one group of hosts on the Internet. The Internet authorities wrongly predicted a need for 268,435,456 groups.

This never happened and many addresses were wasted here too. And lastly, the class E addresses were reserved for future use; only a few were used, resulting in another waste

of addresses. In c1assfnl addressing, a large part of the available addresses were wasted.

Netid and Hostid

In classful addressing, an IP address in class A, B, or C is divided into netid and hostid. These parts are of varying lengths, depending on the class of the address.

In class A, one byte defines the netid and three bytes define the hostid. In class B, two bytes define the netid and two bytes define the hostid. In class C, three bytes define the netid and one byte defines the hostid.

Mask

Although the length of the netid and hostid (in bits) is predetermined in classful addressing, we can also use a mask (also called the default mask), a 32-bit number made of contiguous Is followed by contiguous as. The masks for classes A, B, and C are shown in Table . The concept does not apply to classes D and E.

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	18
B	11111111 11111111 00000000 00000000	255.255.0.0	116
C	11111111 11111111 11111111 00000000	255.255.255.0	124

- The mask can help us to find the netid and the hostid. For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid. The last column of Table shows the mask in the form */n* where *n* can be 8, 16, or 24 in classful addressing. This notation is also called slash notation or Classless Interdomain Routing (CIDR) notation.

Subnetting

During the era of classful addressing, subnetting was introduced. If an organization was granted a large block in class A or B, it could divide the addresses into several

contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors. Subnetting increases the number of Is in the mask, as we will see later when we discuss classless addressing.

what is an IP subnet?

An IP subnet, often called a subnetwork, is a subdivision of an IP network. They can be best understood as the logical organization of connected network devices. Subnetting allows a company to break its large network into smaller, more organized divisions. The advantages of subnetting include:

- **Improved efficiency:** By breaking large networks into smaller ones, your customers can simplify basic tasks like troubleshooting.
- **Better security:** Subnetting can help customers more easily deploy security measures such as firewalls.
- **Reduce network traffic:** Smaller networks equate to smaller broadcast domains. This can free up network congestion.

Class A Address

- The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127
- Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only.
- The IP range 127.x.x.x is reserved for **loopback** IP addresses.
- The default subnet mask for Class A IP address is **255.0.0.0** which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Class B Address

- An IP address which belongs to class B has the first two bits in the first octet set to 10.
- 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 Class C IP address 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.HH

Class D Address

- Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of
  - Class D has IP address range from 224.0.0.0 to 239.255.255.255.
  - Class D is reserved for Multicasting.
  - In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

- This IP Class is reserved for experimental purposes only for R&D or Study.
- IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254.
- Like Class D, this class too is not equipped with any subnet mask.

IPv4 - Reserved Addresses

- There are a few reserved IPv4 address spaces which cannot be used on the internet.
- These addresses serve special purpose and cannot be routed outside the Local Area Network.

Private IP Addresses

- Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses.
- These IPs can be used within a network, campus, company and are private to it.
- These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.
- In order to communicate with the outside world, these IP addresses must have to be translated to some public IP addresses using NAT process, or Web Proxy server can be used.
- IP class, while using private address range, can be chosen as per the size and requirement of the organization.
- Larger organizations may choose class A private IP address range where smaller organizations may opt for class C.
- These IP addresses can be further sub-netted and assigned to departments within an organization.

Loopback IP Addresses

- The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host’s self-address, also known as localhost address.
- This loopback IP address is managed entirely by and within the operating system. Loopback addresses, enable the Server and Client processes on a single system to communicate with each other.

- When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.

IPv4 - Example

- In this part how actual communication happens on the Network using Internet Protocol version 4.

Packet Flow in Network

- All the hosts in IPv4 environment are assigned unique logical IP addresses. When a host wants to send some data to another host on the network, it needs the physical (MAC) address of the destination host. To get the MAC address, the host broadcasts ARP message and asks to give the MAC address whoever is the owner of destination IP address. All the hosts on that segment receive the ARP packet, but only the host having its IP matching with the one in the ARP message, replies with its MAC address. Once the sender receives the MAC address of the receiving station, data is sent on the physical media.
- To understand the packet flow, we must first understand the following components –

MAC Address: Media Access Control Address is 48-bit factory hard coded physical address of network device which can uniquely be identified. This address is assigned by device manufacturers.

Address Resolution Protocol: Address Resolution Protocol is used to acquire the MAC address of a host whose IP address is known. ARP is a Broadcast packet which is received by all the host in the network segment. But only the host whose IP is mentioned in ARP responds to it providing its MAC address.

Proxy Server: To access the Internet, networks use a Proxy Server which has a public IP assigned. All the PCs request the Proxy Server for a Server on the Internet. The Proxy Server on behalf of the PCS sends the request to the server and when it receives a response from the Server, the Proxy Server forwards it to the client PC.

Dynamic Host Control Protocol: DHCP is a service by which a host is assigned IP address from a pre-defined address pool. By using DHCP services, a network administrator can manage assignment of IP addresses at ease.

Domain Name System: It is very likely that a user does not know the IP address of a remote Server he wants to connect to. But he knows the name assigned to it, for example, tutorialpoints.com. When the user types the name of a remote server he wants to connect to, the localhost behind the screens sends a DNS query. Domain Name System is a method to acquire the IP address of the host whose Domain Name is known.

Network Address Translation: Almost all PCs in a computer network are assigned private IP addresses which are not routable on the Internet. As soon as a router receives an IP packet with a private IP address, it drops it.

- In order to access servers on public private address, computer networks use an address translation service, which translates between public and private addresses, called Network Address Translation. When a PC sends an IP packet out of a private network, NAT changes the private IP address with public IP address and vice versa.

- *We can now describe the packet flow. Assume that a user wants to access **www.tutorialspoint.com** from her personal computer. She has internet connection from her ISP. The following steps will be taken by the system to help her reach the destination website*

Step 1 – Acquiring an IP Address (DHCP)

- When the user's PC boots up, it searches for a DHCP server to acquire an IP address. For the same, the PC sends a DHCPDISCOVER broadcast which is received by one or more DHCP servers on the subnet and they all respond with DHCPOFFER which includes all the necessary details such as IP, subnet, Gateway, DNS, etc. The PC sends DHCPREQUEST packet in order to request the offered IP address. Finally, the DHCP sends DHCPACK packet to tell the PC that it can keep

the IP for some given amount of time that is known as IP lease.

- Alternatively, a PC can be assigned an IP address manually without taking any help from DHCP server. When a PC is well configured with IP address details, it can communicate other computers all over the IP enabled network.

Step 2 – DNS Query

- When a user opens a web browser and types www.tutorialpoints.com which is a domain name and a PC does not understand how to communicate with the server using domain names, then the PC sends a DNS query out on the network in order to obtain the IP address pertaining to the domain name. The pre-configured DNS server responds to the query with IP address of the domain name specified.

Step 3 – ARP Request

- The PC finds that the destination IP address does not belong to his own IP address range and it has to forward the request to the Gateway. The Gateway in this scenario can be a router or a Proxy Server.
- Though the Gateway's IP address is known to the client machine but computers do not exchange data on IP addresses, rather they need the machine's hardware address which is Layer-2 factory coded MAC address. To obtain the MAC address of the Gateway, the client PC broadcasts an ARP request saying "Who owns this IP address?" The Gateway in response to the ARP query sends its MAC address. Upon receiving the MAC address, the PC sends the packets to the Gateway.
- An IP packet has both source and destination addresses and it connects the host with a remote host logically, whereas MAC addresses help systems on a single network segment to transfer actual data. It is important that source and destination MAC addresses change as they travel across the Internet (segment by segment) but source and destination IP addresses never change.

IPv6

The network layer protocol in the TCPIIP protocol suite is currently IPv4 (Internetworking Protocol, version 4). IPv4 provides the host-to-host communication between systems in the Internet. Although IPv4 is well designed, data communication has evolved since the inception of IPv4 in the 1970s. IPv4 has some deficiencies (listed below) that make it unsuitable for the fast-growing Internet.

- ✓ Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.
- ✓ The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation ofresources not provided in the IPv4 design.
- ✓ The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

To overcome these deficiencies, IPv6 (Internetworking Protocol, version 6), also known as IPng (Internetworking Protocol, next generation), was proposed and is now a standard. In IPv6, the Internet protocol was extensively modified to accommodate the unforeseen growth of the Internet. The format and the length of the IP address were changed along with the packet format. Related protocols, such as ICMP, were also modified. Other protocols in the network layer, such as ARP, RARP, and IGMP, were either deleted or included in the ICMPv6 protocol (see Chapter 21). Communications experts predict that IPv6 and its related protocols will soon replace the current IP version.

The adoption of IPv6 has been slow. The reason is that the original motivation for its development, depletion ofIPv4 addresses, has been remedied by short-term strategies such as classless addressing and NAT. However, the fast-spreading use of the Internet, and new services such as mobile IP, IP telephony, and IP-capable mobile telephony, may eventually require the total replacement of IPv4 with IPv6.