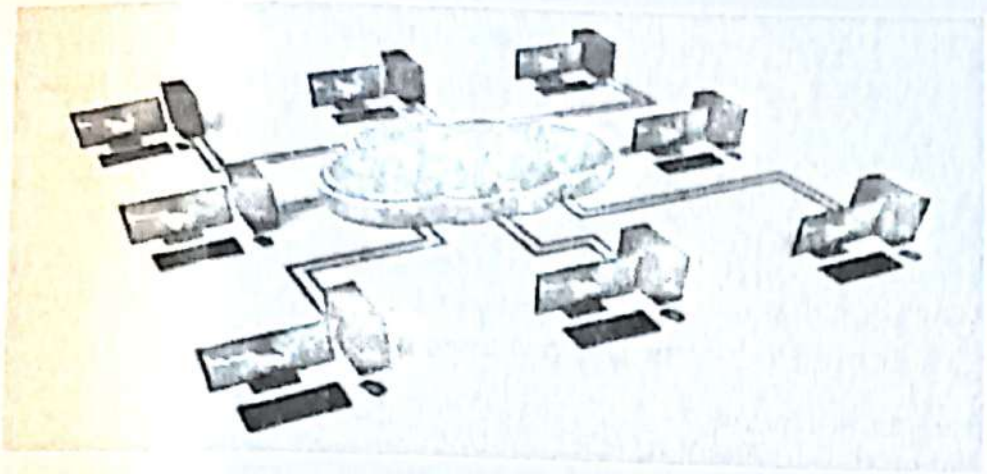


4

INTERNET PROTOCOL (IP)

Introduction

It is the Internet Protocol (IP) that is the heart of the Internet. Networks running different protocols are connected together to form the global network because of the IP. In this chapter, we will study IP version 4 which is presently running on most of the routers and end systems. We will also discuss IP version 6 which is the next version of the IP that is being deployed and that will become predominant in coming years. We will also discuss various routing protocols. Details of Internet Control Message Protocol (ICMP) are also presented in this chapter.

4.1 OVERVIEW OF INTERNET PROTOCOL

Internet Protocol (IP) is the protocol that makes various networks linked to each other.

- IP defines the data formats for transferring data between various networks.
- It also specifies the addressing and routing mechanisms.
- The service delivered by IP is unreliable connectionsless packet service.
- The service is unreliable because there is no guarantee that the packets will be delivered—packets may be lost if there is congestion, though "best-effort" is made for the delivery.

- The packets may not be received in sequence, packets may be duplicated and packets may arrive at the destination with variable delay.
- The service is connectionless because each packet is handled independently.
- IP defines the rules for discarding packets, generating error messages, hosts and routers should process the packets.
- IP is implemented as software.
- This software must run on each and every end system and on each and every router in any internet that uses the TCP/IP protocol suite.
- This is the host to host network layer protocol designed for network.
- IP is a connectionless datagram protocol with no guarantee of reliability.
- It can detect the error and discards the packets if it is corrupted.
- If IP is to be made reliable, then it must be **paired with a reliable protocol such as TCP at the transport layer.**
- Each IP datagram is handled independently and each one can follow a different route to the destination.
- So there is possibility of receiving out of order packets at the destination. Some packets may even be lost or corrupted.
- IP relies on a higher level protocol to take care of all these problems.

4.1.1 Datagram

Packets in IP layer are called datagram.

- It has a variable length packets with two parts namely header and the data.
- The header is 20 to 60 byte in length. It contains the information required for routing and delivery.
- The other part of datagram is data field which is of variable length.

4.1.2 Services Provided by IP

IP provides the following services :

- **Addressing :**
  - IP header contains 32-bit addresses which identify the sending and receiving hosts.

- These addresses are used by intermediate routers to select a path through the network for the packet.

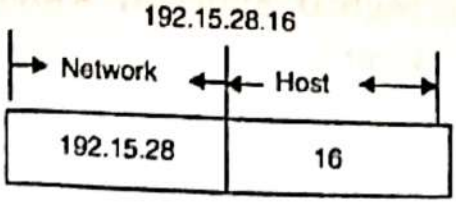
- **Fragmentation :**
  - IP packet may be split, or fragmented, into a smaller packet.
  - This permits a large packet to travel across a network which can handle smaller packets– IP fragments and reassembled packets transparently.
- **Packet time out :**
  - Each packet contains a Time To Live (TTL) field, which is decremented every time a routers handles the packet.
  - If TTL reaches to zero, the packet is discarded, preventing packets from running in circle forever and flooding in network
- **Type of Service :** IP supports traffic prioritization by allowing packets to be labeled with an abstract type of service.

Special IP Addresses :

(a)	0.000 ..... .000		All zeros means HOST
(b)	00 00	HOST	A Host on this network
(c)	111 1111		All 1's means broadcast on local network
(d)	Network	1111 11	Broadcast on distant network
(e)	127	Anything	Loop back (Reserved Address for debugging network software)

4.1.3 Address Mask

- An address mask determines which portion of an IP address identifies the network and which will identify the host.
- Like an IP address, in mask is also represented by four octect.
- If a given bit of mask is 1, the corresponding bit of the IP address is in the network portion of the address, and if a given bit of mask is zero, the corresponding bit of IP address is in the host portion.
- For example consider a class C address



- To differentiate the network and host parts we have to use a mask 255.255.255.0
- Table shows the mask address 255.255.255.0

(IP Address (in decimals binary form)

Element	Network			Host
Mask	255	.255	.255	.0
	111 111 11	111 111 11	111 111 11	00000000
Address	192	.15	.28	.16
	11000000	00001111	00011100	00010000

- If a field network address is entirely used for network number the corresponding field of the mark has decimal value 255 (binary 1111 1111) and if an address field is entirely used for the host ID, the corresponding field of the mark has the decimal value 0.

Table

Decimal value in the field of mark	Binary value in the field of mask	Function
255	111 111 11	Identify network number
0	000 000 00	Identify host ID

- Accordingly the address mask for three network classes described above are

Address Class	Address Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

- These masks are also called as a default mask.

4.2 INTERNET ADDRESSING SCHEME

4.2.1 IP address

- **IP address is the logical address, which is used to identify a computer in the network.**
- Networks using the TCP/IP protocol route messages based on the IP address of the destination.

- The format of an IP address is a 32-bit numeric address which is divided into four 8 bit fields separated by periods called **octet.**
- Since each of the eight positions can have two different states (1 or 0) the total number of possible combinations per octet is 2^8 or 256.
- So each octet can contain any value between 0 and 255.
- Combine the four octets and you get 2^{32} or a possible 4,294,967,296 unique values.
- IP Address format : The 32 bit is grouped into group of 8 bits, seprated by dots.

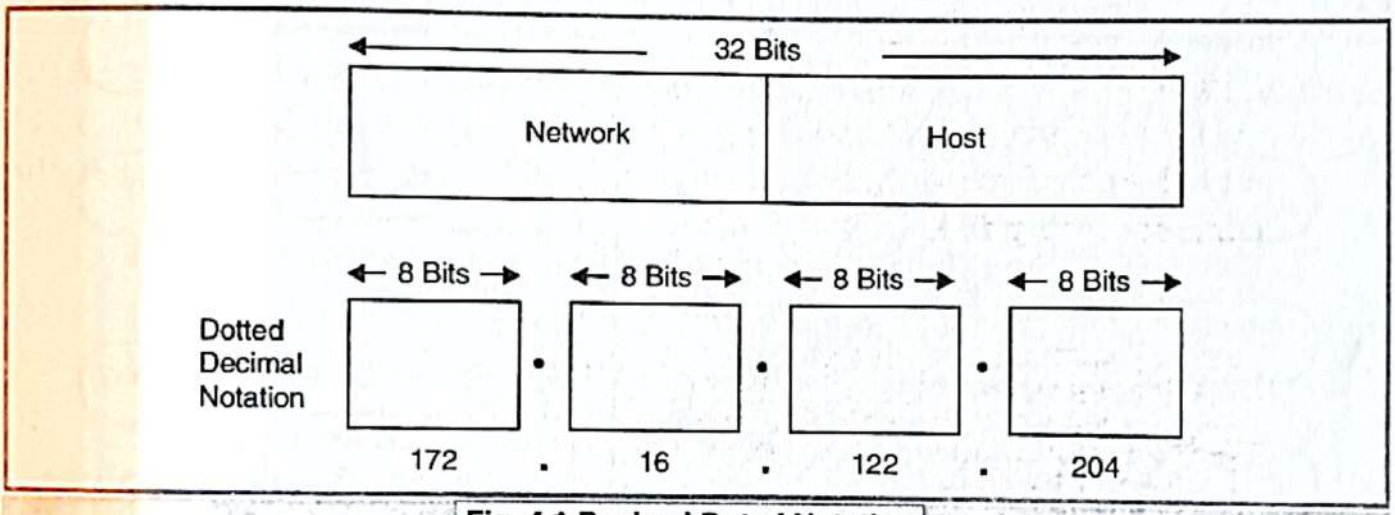


Fig. 4.1 Decimal Doted Notation

A typical IP address looks like

216.27.61.137

- As we know thatcomputers can communicate in **binary form only.** It will Look at the same IP address in binary as :

11011000.00011011.00111101.10001001

- Out of the almost 4.3 billion possible combinations, certain values are restricted from use as typical IP addresses.
- For example, the IP address **0.0.0.0** is reserved for the default network and the address **255.255.255.255** is used for broadcasts.
- The octets are split into two sections : **Net** and **host.**
- The Net section always contains the first octet.
- It is used to identify the network that a computer belongs to.
- Host (sometimes referred to as **Node**) identifies the actual computer on the network. The Host section always contains the last octet.

(a) Classful network

- **Classful network** is a term that is used to describe the network architecture of the Internet until around 1993.
- It divided the address space for Internet protocol into five address classes.
- Each class, coded by the first three bits of the address, defined a different size or type (unicast or multicast) of the network.

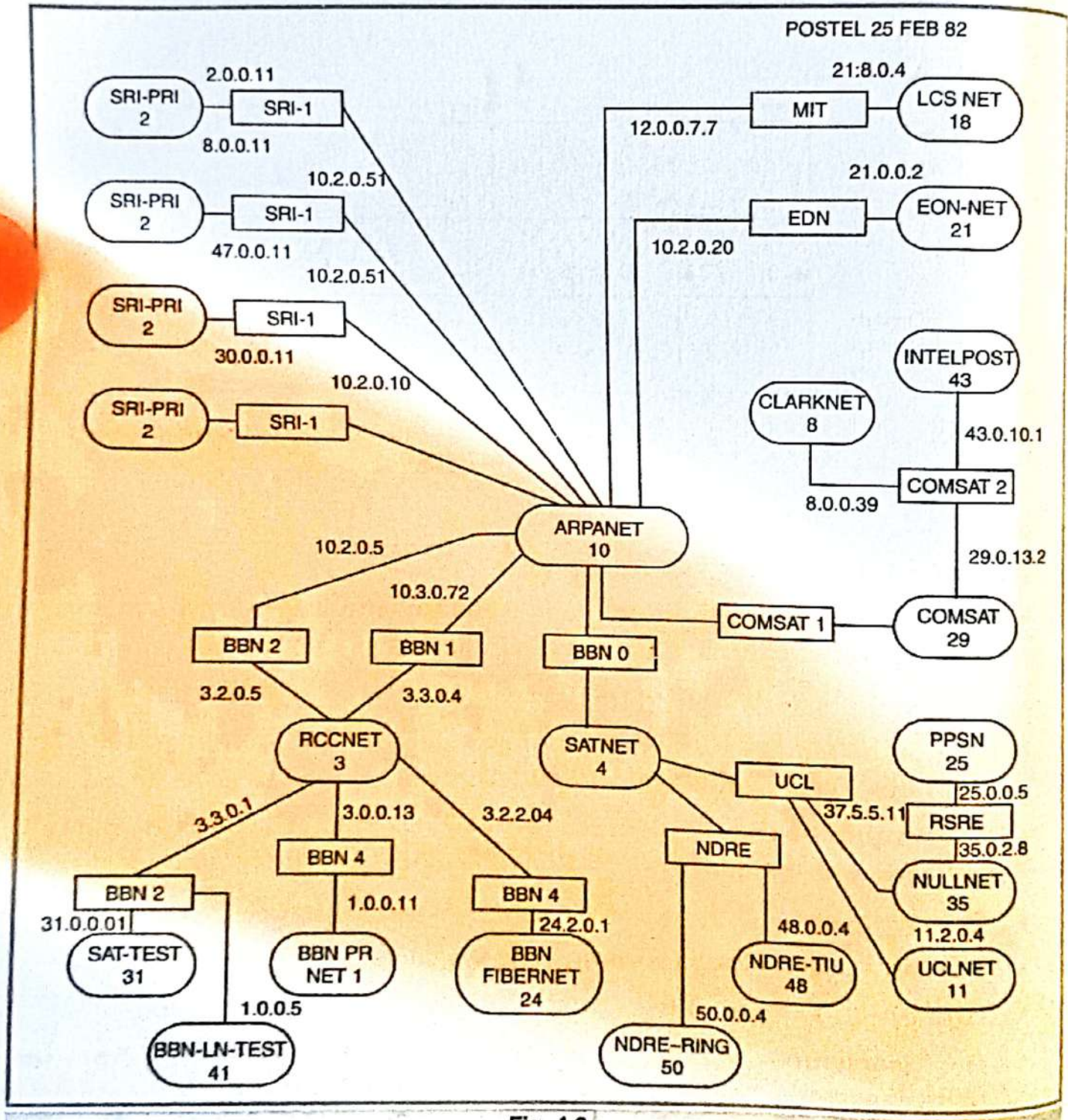


Fig. 4.2

4.2.1.1 IP Address Classes

- To remain compatible with the existing IP address space and the IP packet structure, the definition of IP addresses was changed in 1981.
- The number of usable host addresses available is always 2^N–2 (where N is the number of bits used, and the subtraction of 2 adjusts for the use of the all-bits-zero host portion for network address and the all-bits-one host portion as a broadcast address.
- The IP addrsses are classified into 5 types as :

  1. Class A, 2. Class B, 3. Class C, 4. Class D, 5. Class E

(a) Class A

- This class is for very large networks, such as a major international company.
- IP addresses with a first octet from 1 to 126 are part of this class.
- The other three octets are used to identify each host.
- This means that there are 126 Class A networks each with 16,777,214 (2^{24} – 2) possible hosts for a total of 2,147,483,648 (2^{31}) unique IP addresses.
- Class A networks account for half of the total available IP addresses.
- In Class A networks, the high order bit value (the very first binary number) in the first octet is always 0.

• Bitwise representation of class A

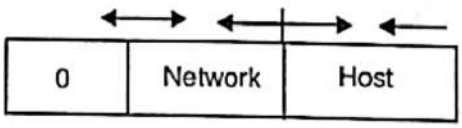
1. 0. 0. 0 = 00000001.00000000.00000000.00000000

126.255.255.255 = 01111111.11111111.11111111.11111111

0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH

Here n indicates a binary slot used for network ID.

And H indicates a binary slot used for host ID.



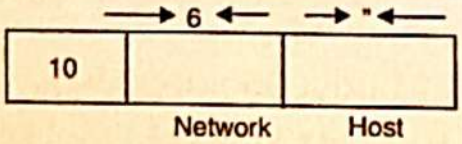
- The "0" in first field identifies that it is calss A network address.
- **Loopback** –The IP address **127.0.0.1** is used as the loopback address.
- This means that it is used by the host computer to send a message back to itself.
- It is commonly used for troubleshooting and network testing.

(b) Class B

- Class B is used for medium-sized networks. **A good example is a large college campus.**
- IP addresses with a first octet from 128 to 191 are part of this class.
- Class B addresses also includes the second octet as part of the Net identifier.
- The other two octets are used to identify each host.
- This means that there are 16,384 (2^{14}) Class B networks each with 65,534 (2^{16}– 2) possible hosts for a total of 1,073,741,824 (2^{30}) unique IP addresses.
- Class B networks make up a quarter of the total available IP addresses.
- Class B networks have a first bit value of 1 and a second bit value of 0 in the first octet.

- **Bitwise representation of class B**

128. 0.0.0 = 10000000.00000000.00000000.00000000
191.255.255.255 = 10111111.11111111.11111111.11111111
10nnnnnn.nnnnnnnn HHHHHHHH.HHHHHHHH
Here n indicates a binary slot used for network ID.
And H indicates a binary slot used for host ID.



- The first "10" field identifies that it is class B network.

(c) Class C

- Class C addresses are commonly used for small to medium-size businesses.
- IP addresses with a first octet from 192 to 223 are part of this class. Class C addresses also include the second and third octets as part of the Net identifier.
- The last octet is used to identify each host.
- This means that there are 2,097,152 (2^{21}) Class C networks each with 254 (2^8–2) possible hosts for a total of 536,870,912 (2^{29}) unique IP addresses.

- Class C networks make up an eighth of the total available IP addresses. Class C networks have a first bit value of 1, second bit value of 1 and a third bit value of 0 in the first octet.

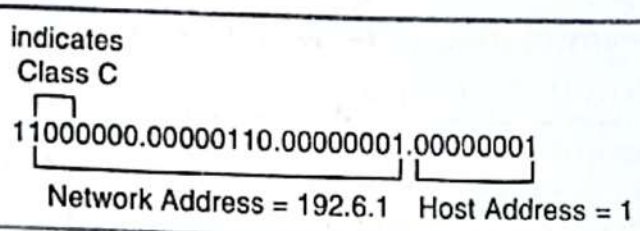


Fig. 4.3

• Bitwise representation of class C

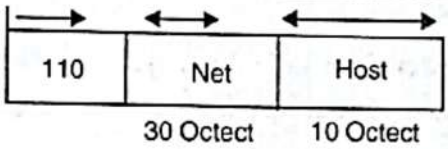
192. 0. 0. 0 = 11000000.00000000.00000000.00000000

223.255.255.255 = 11011111.11111111.11111111.11111111

110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH

Here n indicates a binary slot used for network ID.

And H indicates a binary slot used for host ID.



(d) Class D

- Used for multicasts,
- Class D is slightly different from the first three classes.
- It has a first bit value of 1, second bit value of 1, third bit value of 1 and fourth bit value of 0.
- The other 28 bits are used to identify the group of computers the multicast message is intended for.
- Class D accounts for 1/16th (268,435,456 or 2^{28}) of the available IP addresses.

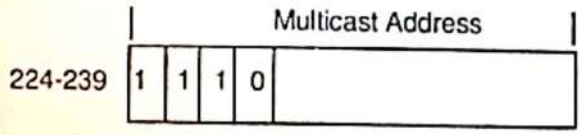
• Bitwise representation of class D

224. 0. 0. 0 = 11100000.00000000.00000000.00000000

239.255.255.255 = 11101111.11111111.11111111.11111111

1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Here X indicates a binary slot (without specified purpose)

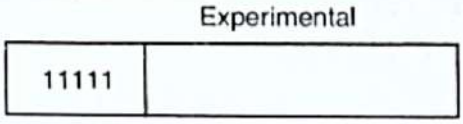


(e) Class E

- Class E is used for experimental purposes only. Like Class D, it is different from the first three classes.

- It has a first bit value of 1, second bit value of 1, third bit value of 1 and fourth bit value of 1.
- The other 28 bits are used to identify the group of computers the multicast message is intended for. Class E accounts for 1/16th (268,435,456 or 2^{28}) of the available IP addresses.

• Bitwise representation of class E
240. 0. 0. 0 = 1111000.00000000.00000000.00000000
255.255.255.255 = 11111111.11111111.11111111.11111111
1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX
Here X indicates a binary slot (without specified purpose)



Broadcast – Messages that are intended for all computers on a network are sent as broadcasts. These messages always use the address. 255.255.255.255.

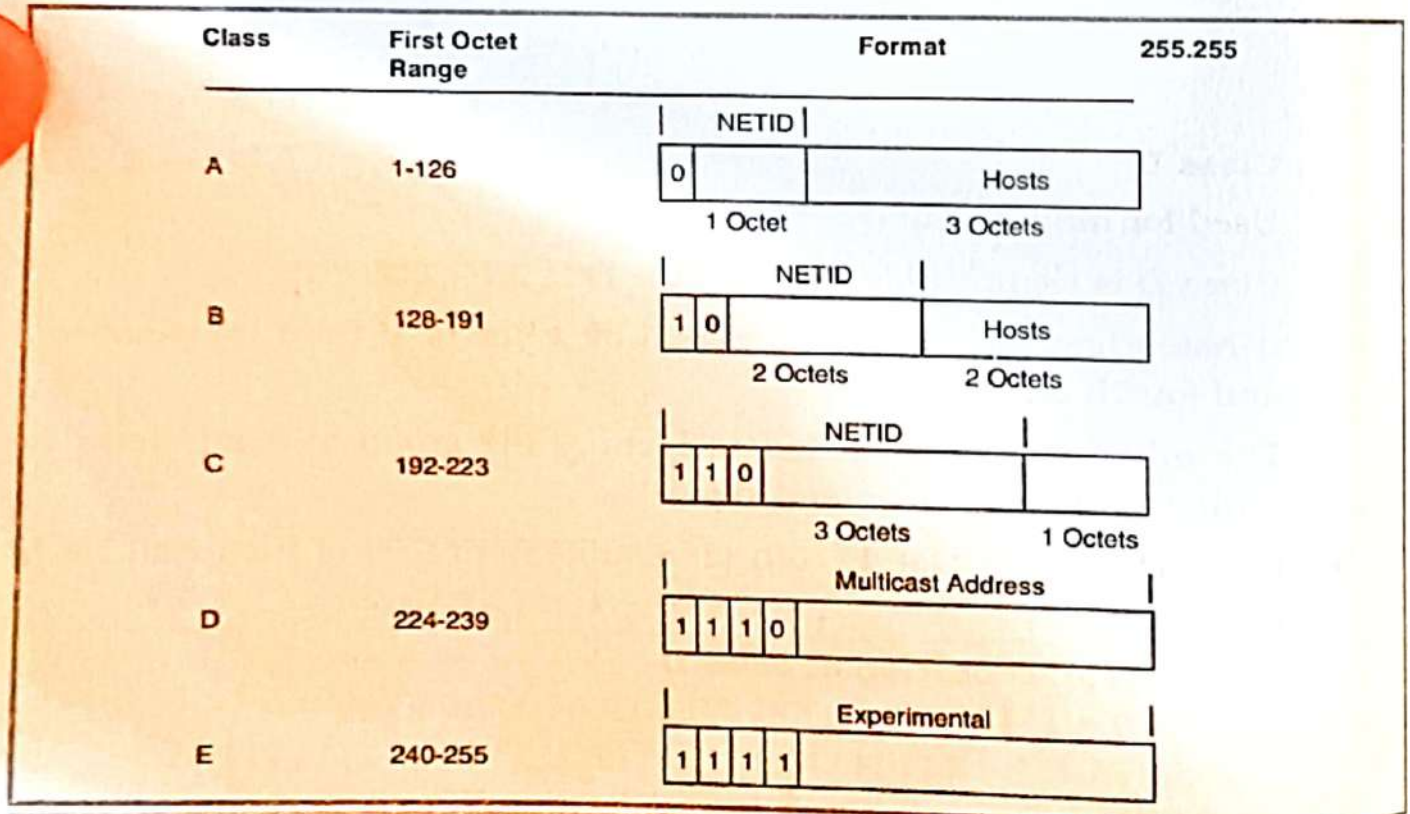


Fig. 4.4

Class	First	First Byte	No. of networks/ Bits	No. of hosts/ No. of Bits for Value	purpose bits for hosts n/w
A	1-126	0	126/8	16,777,214/24	N/W with large no. of hosts

B	128-191	10	16,384/16	65,534/16	Medium sized large sized N/W
C	192-223	110	2,097,152/24	254/8	Used for LAN
D	224-239	1110	—	—	Used for Multicasting
E	240-255	1111	—	—	Future use

4.2.1.2 IP BIT ALGORITHM

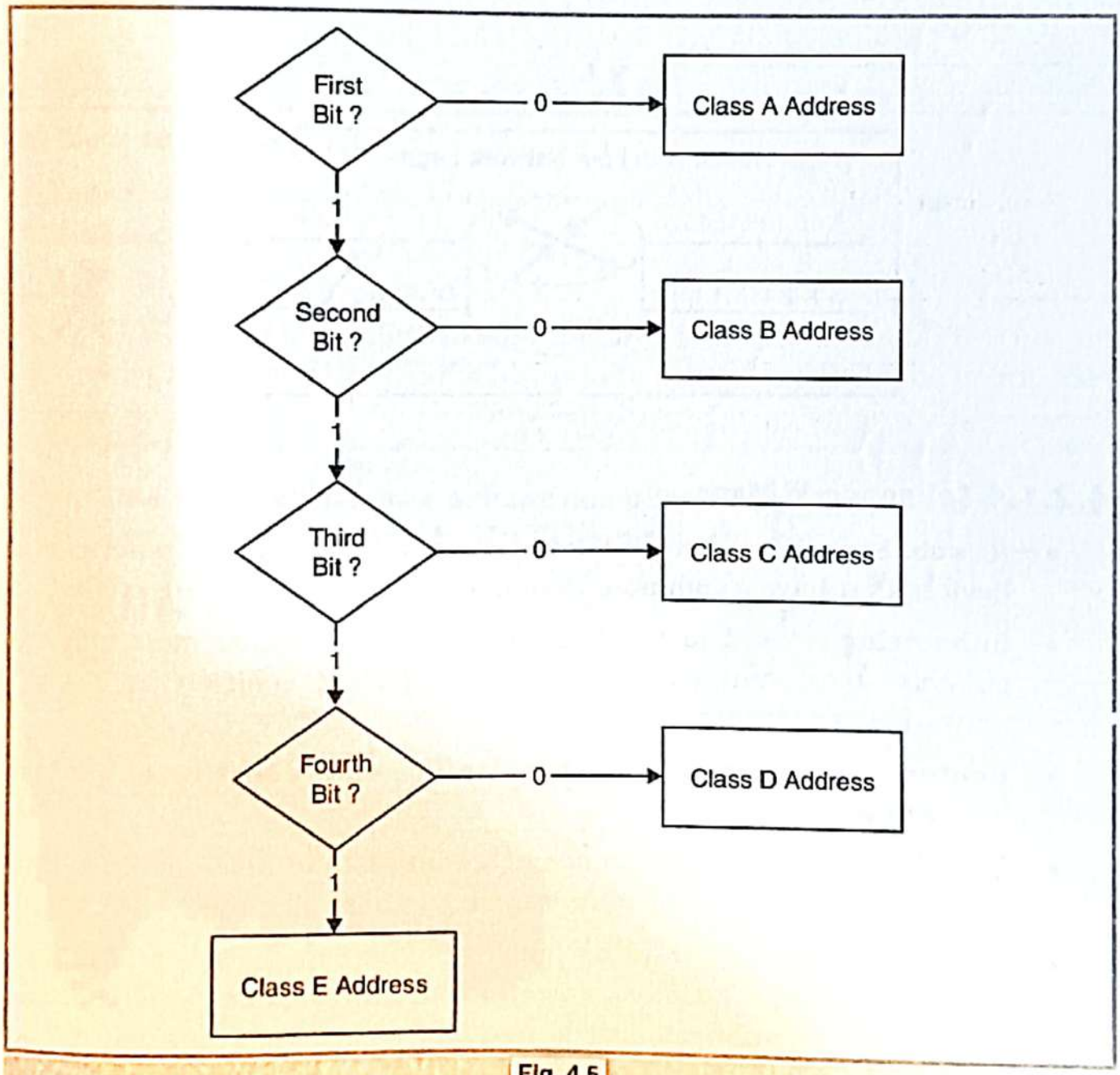


Fig. 4.5

4.2.1.3 Private IP address

- Private IP addresses are those addresses which are used on private network but not on internet.

- This is used to sale the IP addresses because if every host on every network has a public IP then these will be finished just in few years.
- But by using private address, the home user can run internet on private address.
- This is configured with the help of NAT (Network Address Translation)

Range of private addresses

Class	Range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

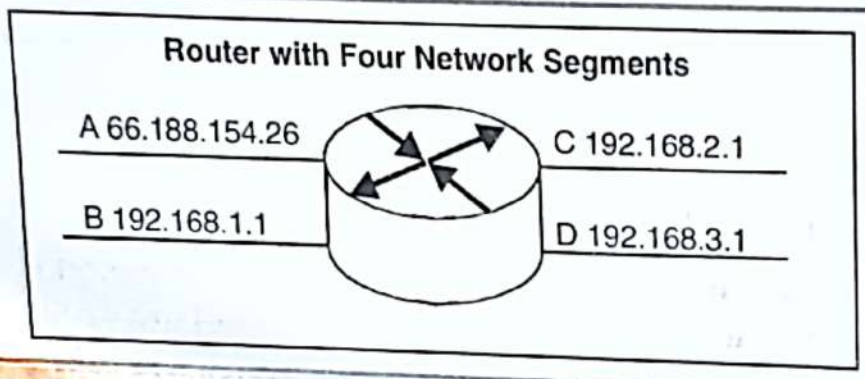


Fig. 4.6

4.2.1.4 Subnetwork Mask

- A **subnetwork**, or subnet, describes networked computers and devices that have a common, designated IP address routing prefix.
- **Subnetting** is used to break the network into smaller more efficient subnets to prevent excessive rates of packet collision in a large network.
- **Routers are used to manage traffic and constitute borders between subnets.**
- A routing prefix is the sequence of leading bits of an IP address that precede the portion of the address used as host identifier.
- In IPv4 networks, the routing prefix is often expressed as a "**subnet mask**", which is a bit mask covering the number of bits used in the prefix. An IPv4 subnet mask is frequently expressed in quad-dotted decimal representation, *e.g.*,255.255.255.0 is the subnet mask for the 192.168.1.0 network with a 24-bit routing prefix (192.168.1.0/24).
- The host ID and the Network ID in an IP address can be distinguished using subnet mask.

- For example the default subnet mask of class C IP address is 255.255.255.0. This can be represented in binary as given below :

1111 1111	1111 1111	1111 1111	0000 0000

- In this all 1's represent the network ID and all 0's represent the host ID.
- The table given below gives the default subnet mask used for class A, B, and C IP address.

Class	Representation	Default Subnet mask	First Byte Value
A	N:H:H:H	255.0.0.0	1-126
B	N:N:H:H	255.255.0.0	128-191
C	N:N:N:H	255.255.255.0	192-223

(a) How to do subnetting :

To perform subnetting we must know about the following things:

1. Classes
2. No. of subnets or PC per subnet

- CIDR (Class-less Inter Domain Routing) is the method that ISP use to allocate an amount of IP addresses to a company or home users. ISP gives the IP addresses to us in the form something look like : 192.168.10.10/28.
- **This tells us what the subnet mask is, The slash notation means how many bits turn to 1's.** The maximum could be \32 but the largest subnet mask available is \30 because we have to keep two bits for the host bits.

Subnet mask	CIDR
255.0.0.0	\8
255.128.0.0	\9
255.192.0.0	\10
255.224.0.0	\11
255.240.0.0	\12
255.248.0.0	\13
255.252.0.0	\14
...	...
...	...
...	...
255.255.255.252	\30

(b) Incorrect Subnet Mask

- If a network uses a subnet mask other than the default mask for its

address class, and a client is still configured with the default subnet mask for the address class, communication will fail to some nearby network but not to distant ones.

- As an example, if you create four subnets (such as in the subnetting example) but use the incorrect subnet mask of 255.225.255.0 in your TCP/IP configuration, hosts will not be able to determine that some computers are on different subnets than their own.
- When this happens, packets destined for hosts on different physical networks that are part of the same Class C address will not be sent to a default gateway for delivery.
- A common symptom of this is when a computer can communicate with hosts that are on its local network and can talk to all remote networks except those that are nearby and have the same class A, B, or C address.
- To fix this problem, just enter the correct subnet mask in the TCP/IP configuration for that host.

4.3 STATIC AND DYNAMIC IP ADDRESSES

4.3.1 Static IP addressing

- When a computer is configured to use the same IP address each time it powers up, this is known as a Static IP address.
- Static IP addresses are manually assigned to a computer by an administrator. In some cases, a network administrator may implement dynamically assigned static IP addresses.
- In this case, a DHCP server is used, but it is specifically configured to always assign the same IP address to a particular computer.
- **This allows static IP addresses to be configured centrally, without having to specifically configure each computer on the network in a manual procedure.**

4.3.1.1 Uses of static addressing

- Some infrastructure situations have to use static addressing, such as when finding the Domain Name System host that will translate domain names to IP addresses.
- Static addresses are also convenient, but not absolutely necessary, to locate servers inside an enterprise. An address obtained from a DNS

server comes with a time to live, or caching time, after which it should be looked up to confirm that it has not changed.

- Even static IP addresses do change as a result of network administration.

4.3.1.2 Configuring Static IP Address

- A static IP address is manually configured on a client computer. To configure static IP address, follow the following steps :
  1. Click **start -> Setting -> Control Panel -> Network and Internet Connections ->** Click on **Network Connections.**
  2. In the **Network Connections** window right-click on **Local Area Connections** and click **Properties.**
  3. In the **Local Area Connection Properties** window, choose **Internet Protocol (TCP/IP)** and click **Properties.**
  4. In the **TCP/IP Properties window,** select **Use the following IP address** option and enter the values for IP address, subnet mask and default gateway.
  5. Click **OK** to close the **TCP/.IP Properties** window.
  6. Click **Close** to close the **Local Area Connection Properties** window.

4.3.2 Dynamic IP addressing

- When the computer's IP address is assigned automatically, it is known as a Dynamic IP address. Dynamic IP addresses are assigned either by the computer interface or host software itself, as in Zeroconf), or assigned by a server using Dynamic Host Configuration Protocol (DHCP).
- Even though IP addresses assigned using DHCP may stay the same for long periods of time, they can generally change.
- In the absence of both an administrator (to assign a static IP address) and a DHCP server, the operating system may assign itself an IP address using state-less auto configuration methods, such as Zeroconf.

4.3.2.1 Uses of dynamic addressing

- Dynamic IP addresses are most frequently assigned on LANs and broadband networks by Dynamic Host Configuration Protocol (DHCP) servers.

- They are used because it avoids the administrative burden of assigning specific static addresses to each device on a network.
- It also allows many devices to share limited address space on a network if only some of them will be online at a particular time.
- In most current desktop operating systems, dynamic IP configuration is enabled by default so that a user does not need to manually enter any settings to connect to a network with a DHCP server.
- Dialup and some broadband networks use dynamic address features of the Point-to-Point Protocol.

4.3.2.2 Sticky dynamic IP address

- A **sticky dynamic IP address** or **sticky IP** is a term created by cable and DSL users to describe a dynamically assigned IP address that does not change often.
- This is however an informal term, as a sticky IP does not differ in any way from other dynamic IP addresses.
- Even though IP addresses may not change often for cable or DSL users, the addresses are still controlled by the standard DHCP process.
- Since the modems are often online for extended periods of time, the leases on the IP addresses are commonly renewed, and therefore may not change.
- When the modem is turned off, a new IP address may be assigned when the modem is turned back on, as a different host on the network may have been assigned the old IP address.
- IP address changes may also be triggered by resetting the DHCP server configuration; therefore causing the modem to receive a new IP address.

4.3.2.3 Configuring Dynamic IP Address

To configure dynamic IP address, follow the following steps :

1. Click **start -> Setting -> Control Panel -> Network and Internet Connections ->** Click on **Network Connections.**
2. In the **Network Connections** window right-click on **Local Area Connections** and click **Properties.**
3. In the **Local Area Connection Properties** window, choose **Internet Protocol (TCP/IP)** and click **Properties.**

4. In the **TCP/IP Properties** window, select **obtain an IP address automatically.**
5. Click **OK** to close the **TCP/.IP Properties** window.
6. Click **Close** to close the **Local Area Connection Properties** window.

4.3.2.4 Configuring Alternate IP Address

- This feature is available only when the computer is configured as a DHCP client.
- Sometimes when DHCP server is not available, the client computer can communicate with the network using alternate IP address.
- The alternate IP address is suited for the portable computers that are configured to access IP address from DHCP server in a network and need to use static IP address when not connected to the network.

To configure alternate IP address, follow the following steps :

1. Click **start -> Setting -> Control Panel -> Network and Internet Connections ->** Click on **Network Connections.**
2. In the **Network Connections** window right-click on **Local Area Connections** and click **Properties.**
3. In the **Local Area Connection Properties** window, choose **Internet Protocol (TCP/IP)** and click **Properties.**
4. In the **TCP/IP Properties window,** select **Obtain an IP address automatically.**
5. Click the Alternate Configuration tab. This tab displays two options.
6. The **Automatic private IP address** option is selected by default.
7. Click on User Configured option in the Alternate Configuration tab. This option is used to assign a static TCP/IP configuration. Enter IP address, subnet mask, default gateway information.
8. Click **OK** to close the **TCP/IP Properties** window.
9. Click **Close** to close the **Local Area Connection Properties** window.

4.3.2.5 Incorrect IP Address

- If you put computers with IP addresses that should be on separate subnets on a local network with each other, they will not be able to communicate.
- They will try to send packets to each other through a router that will not be able to forward them correctly. A symptom of this problem is a computer that can talk to hosts on remote networks, but cannot communicate with some or all computers on their local network.

- To correct this problem, make sure all computers on the sam physical network have IP addresses on the same IP subnet.

4.4 SUBNETING

- As we previously discussed, an **IP address** is 32 bits long.
- One portion of the address indicates a network (netid), and the othe portion indicates the host (or router) on the network (hostid).
- This means that there is a sense of hierarchy in IP addressing.
- To reach a host on the Internet, we must first reach the networ using the first portion of the address (netid).
- Then we must reach the host itself using the second portion (hostid).
- In other words, Classes A,B and C in IP addressing are designed wit two levels of hierarchy.
- In many cases, these two levels of hierarchy are not enough.
- For example, imagine an organization with a Class B address. The organisation has two-level hierarchical addressing, but it cannot have more than one one physical network.

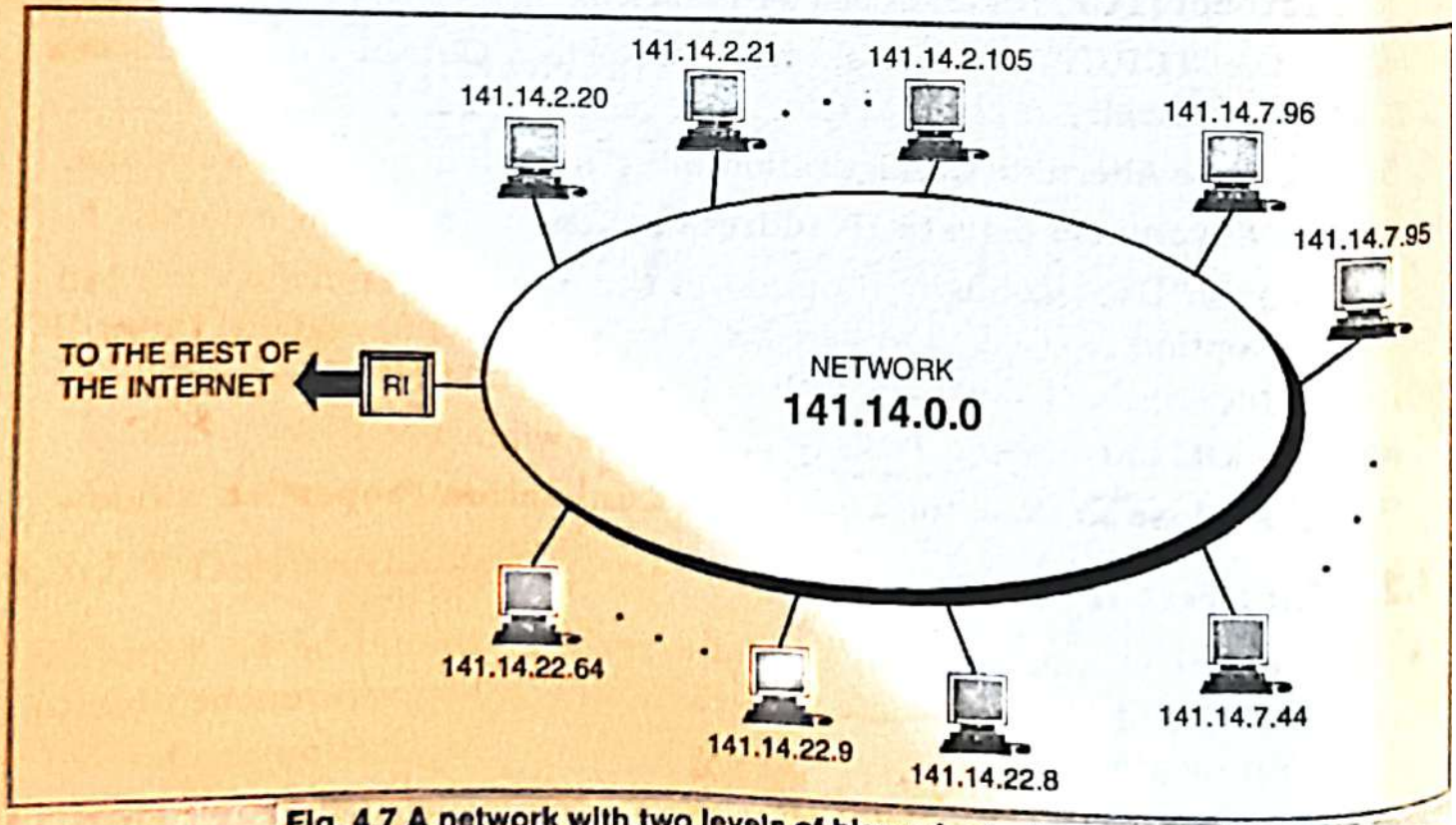


Fig. 4.7 A network with two levels of hierarchy (not subnetted)

- With this scheme, the organisation is limited to two levels of hirearchy.

- The hosts cannot be organized into groups, and all of the hosts are at the same level.
- The organization has one network with many hosts.
- One solution to this problem is **subnetting,** the further division of a network into smaller networks called **subnetwork.**
- For example, Figure 4.8 shows the network divided into three subnetworks.
- In this example, the rest of the Internet is not aware that the network is divided into three physical subnetworks : the three subnetworks still appear as a single network to the rest of the Internet.
- A packet destined for host 141.14.2.21 still reaches router R1.
- The destination address of the IP datagram is still a class B address where 141.14 defines the netid and 2.21 defines the hostid.
- However, when the packet arrives at router RI, the interpretation of the IP address change.
- Router RI knows that the network 141.14 is physically divided into three subnetwork. It knows that the last two octets define two things; subnetid and hostid.
- Therefore, 2.21 must be interpreted as subnetid 2 and hostid 21.
- The router R1 uses the first two octets (141.14) as the netid, the third octer (2) as the subnetid, and the fourth octet (21) as the hostid.

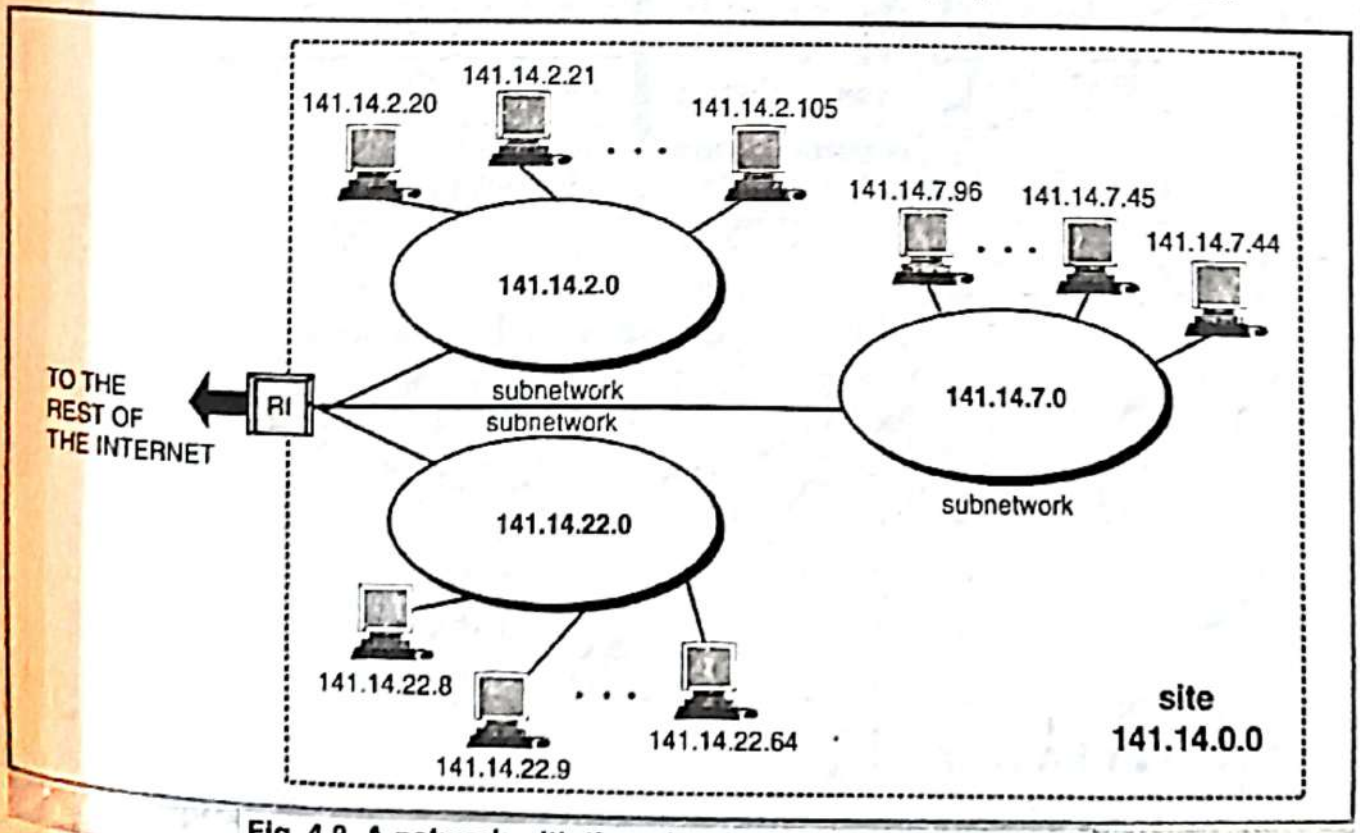


Fig. 4.8 A network with three level of hierarchy (subnetted)

4.5 MASKING

- Masking is a process that extracts the address of the physical network from an IP address.
- Masking can be done whether we have subnetting or not.
- If we have not subnetted the network, masking extracts the network address from an IP address.
- If we have subnetted, masking extracts the **subnetwork address** from an IP address.

4.5.1 Masks without subnetting

- To be compatible, routers use a mask even if there is no subnetting.
- The masks for networks that are not subnetted can be defined in Table 1.

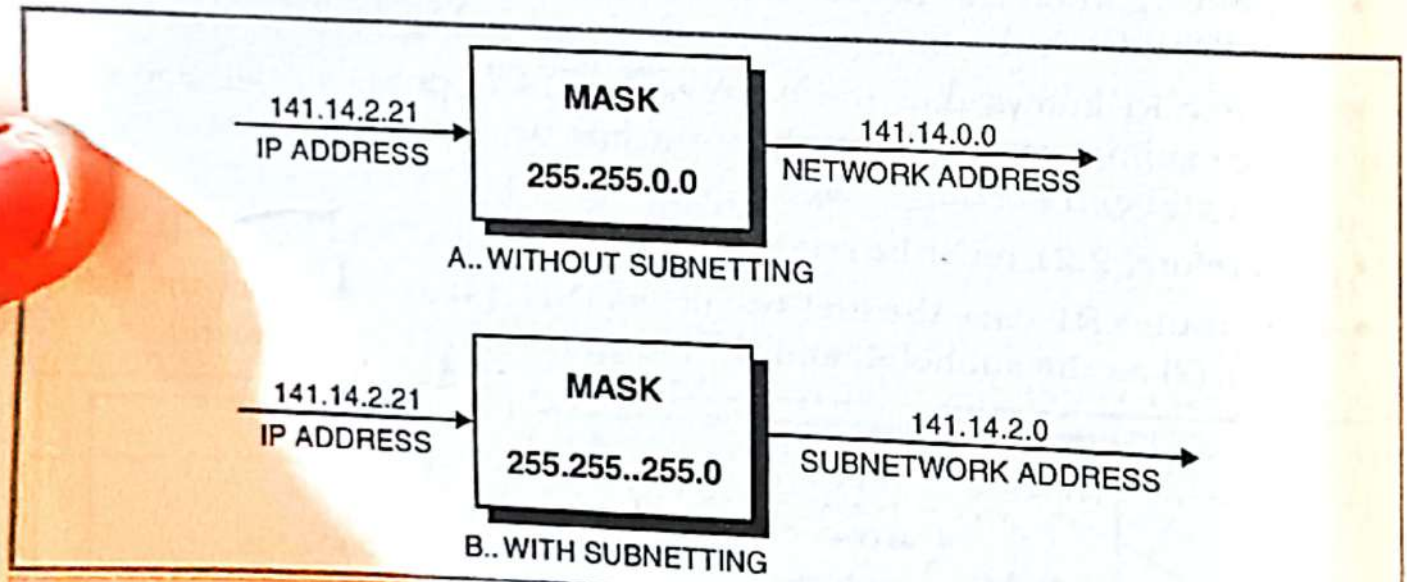


Fig. 4.9 Masking

Table 1 Mask for unsubnetted networks

Class	Mask Address	(Example)	Network Address (Example)
A	255.0.0.0	15.32.56.7	15.0.0.0
B	255.255.0.0	135.67.13.9	135.67.0.0
C	255.255.255.0	201.34.12.72	201.34.12.0
D	N/A	N/A	N/A
E	N/A	N/A	N/A

4.5.2 Masks with subnetting

- When there is subnetting, the mask can very.
- Table 2 shows some examples of masks used for subnetting.

Table 2 Masks for subnetted networks

Class	*Mask Address*	*(Example)*	*Network Address (Example)*
A	255.255.0.0	15.32.56.7	15.0.0.0
B	255.255.2.55.0	135.67.13.9	135.67.0.0
C	255.255.255.192	201.34.12.72	201.34.12.0
D	N/A	N/A	N/A
E	N/A	N/A	N/A

4.6 ADDRESSING

- In addition to the physical addressed contained on network interface cards (NICs) that identify individual devices, the Internet requires an additional addressing convention.
- This address identifies the connection of a host to its network.

Each *Internet address* consists of four bytes (32 bits), defining three fields :

(*a*) Class type

(*b*) netid

(*c*) hostid

These parts are of varying lengths, depending on the class of the address (See figure 4.10).

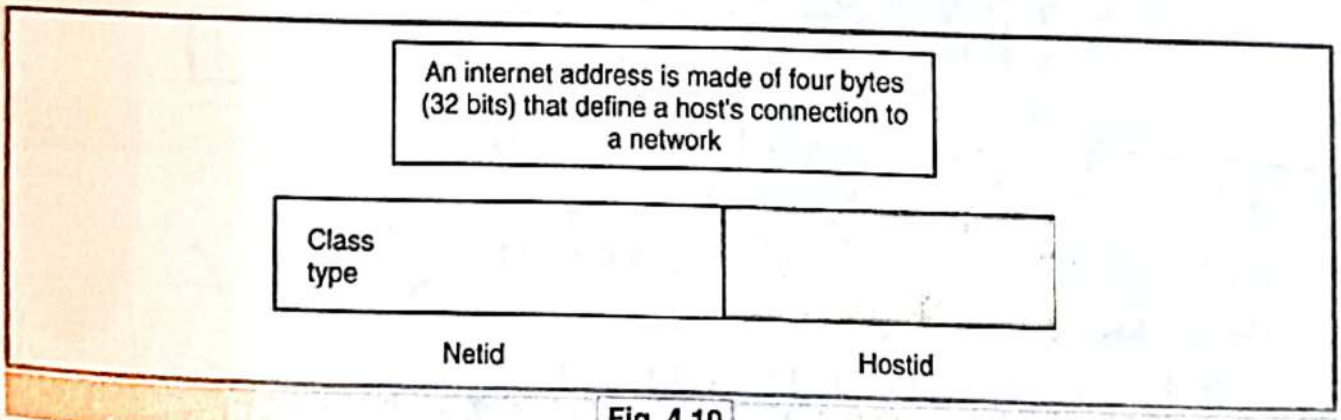


Fig. 4.10

Classes.

- These are five different field-length patterns is use, each defining a *class of address.*
- All such classes are designed to cover the needs of different types of organizations.
- For examples, class A addresses are numerically the lowest.

- They use only one byte to identify class type and netid, and leave three bytes available for hostid numbers. This division means that class A networks can accomodate far more hosts than can class B or class C networks, which provides two and one-byte hostid fields, repectively.
- Currently both class A and B free full. Addresses are available in class C only.
- Class D is reserved for *multicast addresses.*
- *Multicasting* allows copies of a datagram to be passed to a select group of hosts rather than to an individual host.
- Multicasting allows transmission to a selected subset.
- Class E addresses are reserved for future use. Figure 4.11 shows the structure of each *IP address class.* Example 4.1

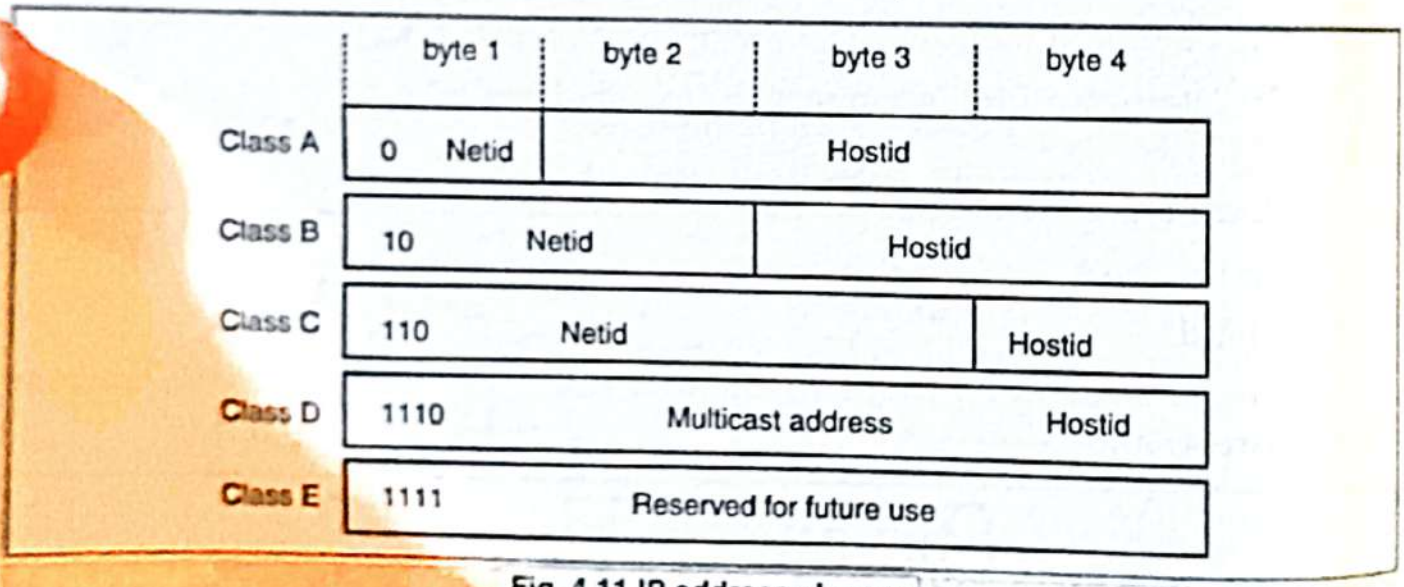


Fig. 4.11 IP address classes

What is the class of each of the following addresses ?

(a) 11011101 10001111 11111100 11001111

(b) 10011101 10001111 11111100 11001111

(c) 01111011 10001111 11111100 11001111

(d) 11110101 10001111 11111100 11001111

(e) 11101011 10001111 11111100 11001111

Solution :

The first bits define the class :

(a) Class C

(b) Class B

(c) Class A

(*d*) Class E

(*e*) Class D

Examples of Addressing

- Internet addresses are usually written in decimal form with decimal points separating the buytes-*dotted-decimal notation.*
- This is done to make the 32-bit form shorter and easier to read. Figure 4.12 shows the bit pattern and decimal format of a possible address.

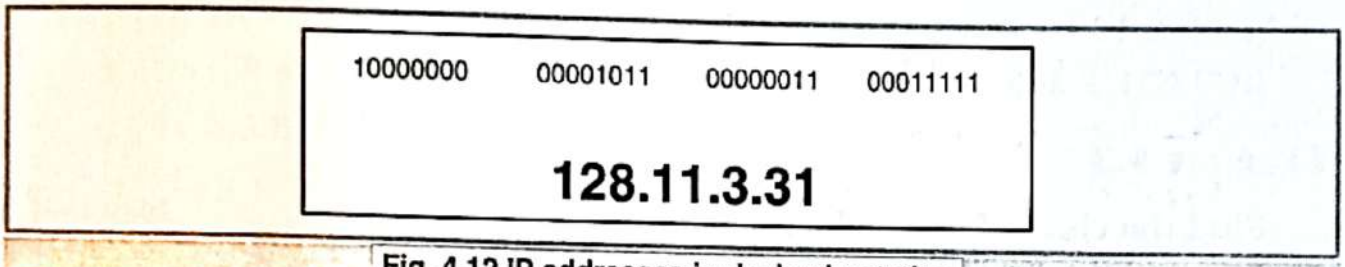


Fig. 4.12 IP addresses in decimal notation

- Looking at the first byte of an address in decimal form, we can determine at a glance to which class a particular address belongs (See Figure 4.13)

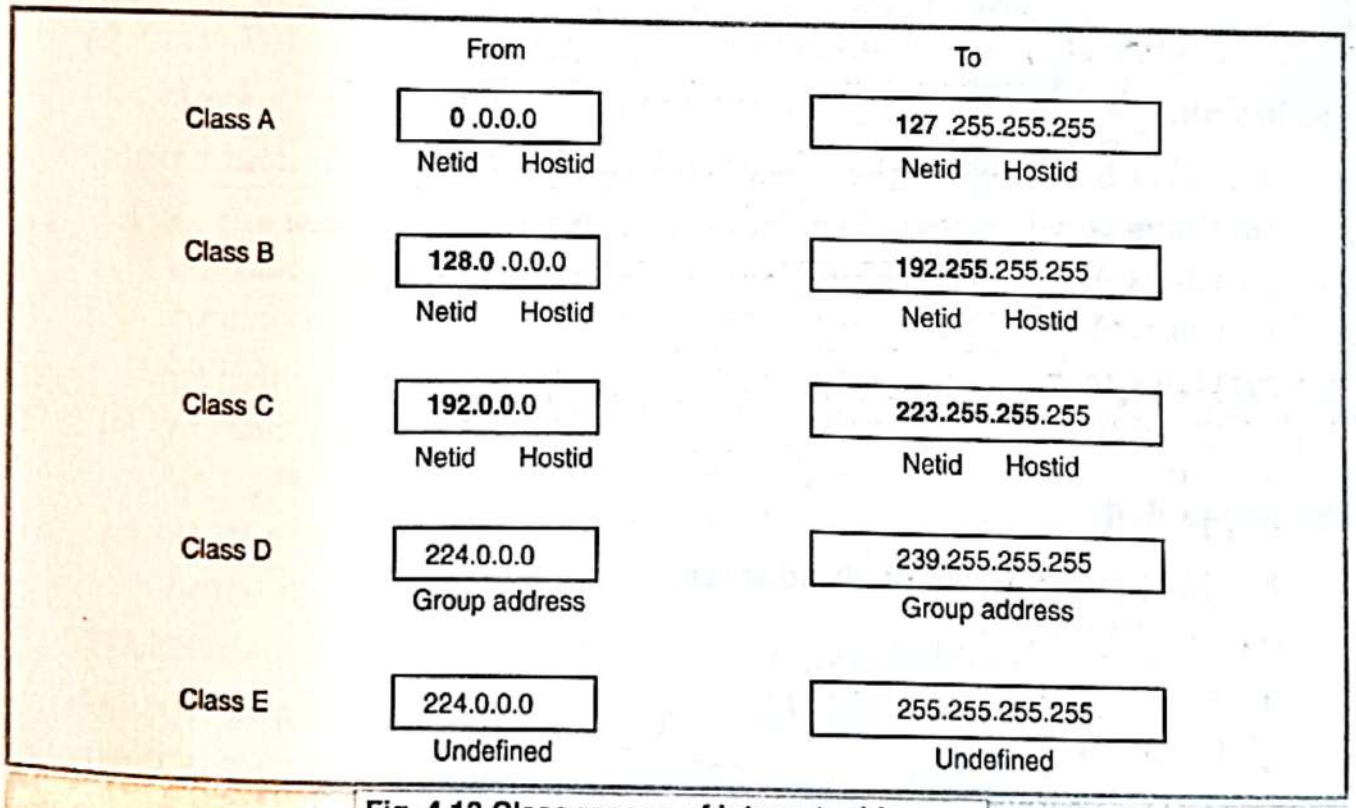


Fig. 4.13 Class ranges of internet addresses

Example 4.2

Write each following in dotted-decimal notation :

(*a*) 11011101 10001111 11111101 00001111

(*b*) 10011101 10001111 11111100 11001111

(c) 11111110 10000001 01111110 00000001
(d) 11111101 10001010 00001111 00111111
(e) 01011101 00011111 00000001 11110101

Solution :

Each byte is converted to a decimal number between 0 and 255.
(a) 221.143.253.15
(b) 157.143.252.207
(c) 254.129.126.1
(d) 253.138.15.63
(e) 93.31.1.245

Example 4.3

Find the class of each address :
(a) 226.34.78.7
(b) 4.22.145.90
(c) 245.7.3.8
(d) 197.76.9.23
(e) 28.6.8.4

Solution.

The first byte defines the class
(a) Class D
(b) Class A
(c) Class E
(d) Class C
(e) Class B

Example 4.4

Find the network for each address :
(a) 227.34.78.7
(b) 4.23.145.90
(c) 198.76.9.23
(d) 129.6.8.4
(e) 246.7.3.8

Solution :

First find the class and them find the network address
(a) Class D, no network address

(*b*) Class A, network address : 4.0.0.0
(*c*) Class C, network address : 198.76.9.0
(*d*) Class B, network address : 129.6.0.0
(*e*) Class E, no network address

Example 4.5

Find the netid and hostid for each address :

(*a*) 227.34.78.7
(*b*) 4.23.145.90
(*c*) 198.76.9.23
(*d*) 129.6.8.4
(*e*) 246.7.3.8

Solution

First find the class and then find the netid and hostid

(*a*) Class D, no hostid or netid
(*b*) Class A, netid : 4 hostid : 23.145.90
(*c*) Class C, netid 198.76.9 hostid : 23
(*d*) Class B, netid : 129.6 hostid : 8.4
(*e*) Class E, no hostid or netid

Telnet functions at the top three layers of the OSI model, as follows :

(*a*) At the session layer, it provides dialog control, using the half-duplex method. It also provides session administration, handling connection establishment, file transfer, and releasing the connection.

(*b*) At the presentation layer, Telnet is concerned with translation, using the byte order and character codes.

(*c*) At the application layer, this protocal supplies the service use functions for remote operation.

TELENT is a general-purpose client-server application program.

TELNET is a terminal emulation protocol which provides remote terminal connection services. It also provides remote log on capability. Originally it was designed to work with simple scroll mode terminals. Two modules of TELNET as

* User TELNET
* Server TELNET

The user telnet is a module which interacts with the terminal I/O module

to communicate with a local terminal. The conversion of real terminal characteristics into the network standard and vice versa is done by it. On the other hand the server telnet is a module which interacts with an application in such a manner that remote terminal appears to the application local terminal. There is a TCP connection on which the terminal traffic between user telnet and server telnet is carried.

The most commonly used terminal emulations are for digital equipment corporation (DEC) VT-52, VT-100 and VT-220 terminals. A special version of TELNET program is TN 3270 which is specially designed for use with large IBM computers 3270 and 327 X serial terminals.

4.6.1 Dotted Decimal Notation

- As it is difficult for us to read the IP address if it is written in 32-bit format, dotted decimal notation is uses. If the IP addressed is

11111110 01111111 10000001 10101010

it can be represented as 254.127.129.170 for easy readability. Internet Network Information Center (INTERNIC) is the central authority to assign IP addresses.

- INTERNIC gives the network id and the organisation is free to assign host addresses.
- Many organisations assign local IP address without obtaining the network id from INTERNIC. This is ok if the network remains isolated but if it is connected to the Internet later on, there amy be an address clash.

4.7 ADDRESS RESOLUTION PROTOCOL (ARP)

- Consider a case when a router connected to a LAN receives a packet for one of the nodes on the LAN.
- The packet is routed up to the router based on the network id.
- How does the router send the packet to that specific node ?
- Remember, the packet has to be sent to the node using the physical address and the received packet contains only the IP address.
- The ARP solves this problem. The router connected to the LAN sends a broadcast message with the IP address of the node as the destination address.
- All the nodes receive this packet and the node with that IP address.

- All the nodes receive this packet and the node with that IP address responds with its physical address.
- Subsequently, the packets will be transmitted to that node with that physical address.
- Since broadcasting is a costly propositions, the router can keep a cache in which the physical addresses corresponding to the IP addresses are stored for subsequent usage.
- Since the physical address may change, the router keeps the physical address in the cache only, as it is likely to be valid only for a certain period of time.
- In the Ethernet frame, the ARP message is embedded in the data field.
- The type field of the Ethernet frame contains the code 0806 (hex) to indicate that it is an ARP message.

4.8 REVERSE ADDRESS RESOLUTION PROTOCOL (RARP)

- Machines which do not have a secondary storage (diskless machines) do not know their IP addresses.
- At the time of bootup, the machine has to get its own IP address.
- The physical address of the machine is known, as it is a part of the hardware i.e., the network card. As you can see, this problem is inverse of the earlier problem, and hence Reverse Address Resolution Protocol (RARP) is developed.
- In RARP, the machine which wants to find out its IP address, broadcasts a packet with its own network address.
- A RARP server,. which stores the IP addresses corresponding to all the network addresses (in secondary storage) receives the packet, and then sends a reply to the machine with the information on its IP address. So, a requirement for RARP to succeed is that a designated RARP server should be present which contains the lookup table.
- Sometimes, for providing a reliable service, primary and secondary RARP servers will be installed in the LANs.
- If the primary RARP server fails, the secondary RARP server will take over and provide the IP addresses to the nodes on the LAN.

4.9 IP DATAGRAM FORMAT

4.9.1. IPv4

- The IP that runs on most of the hosts and routers on the Internet is IP version 4 (IPv/4).
- Gradually, the IP software will be upgraded to IP version 6 (IPv6). We will first study the IPv4 and then study IPv6.
- The basic unit for data transfer is called 'packet' in IP version 6. We will use the words 'datagram' and 'packet' interchangeably in the following discussion, the datagram of IPv4 has a header and the data fields. The detailed format of the datagram is shown in Fig. 4.14. Each of the fields is explained below :

4	4	8	16	16	3	3	12	8	16	32	32	Variable	8	Variable
Version	Header Length	Service Type	Length of Datagram	Datagram ID	Flags	Fragment Offset	Time to Live	Protocol	Header Checksum	Source IP Address	Destination IP Address	Options	Padding	Data

Fig. 4.14 IPv4 Datagram Format

Version number (4 bits) : Version number of the IP. The version presently running in most of the systems is version 4. Version 6 is now slowly being deployed. This field ensures that the correct version of the software is used to process the datagram.

Header length (4 bits) :

- Length of the IP header in 32 bit words. Note that some fields in the header are variable and hence the IP datagram header length may vary.
- The minimum length of the header is 20 bytes and hence minimum value of this field is 5.

Service type (8 bits) :

- These bits specify how the datagram has to be handled by systems.
- The first three bits specify the precedence—0 indicating normal precedence and 7 network control.
- Most routers ignore these bits but if all the routers implement it, these bits can be used for providing precedence to send control information such as congestion control.

- The 4th, 5th and 6th bits are called D, T and R bits. Setting D bit is to request low-delay, setting T bit is to request high throughput and setting R bit is to request high reliability. However, it is only a request, there is no guarantee that the request will be honored.
- Note that these bits are to set the Quality of Service (QoS) parameters.
- But, there is no surety that the required QoS will be provided.
- That is the reason we keep hearing the sentence "IP does not guaranteed a desired QoS".

Length (16 bits) :

- Total length of the datagram in bytes including header and data.
- The length of the data field is calculated by subtracting the header length from the value of this field. Since 16 bits are allotted to this field, the maximum size of an IP datagram is limited to 65,535 bytes.
- Note that the IP datagram size is much larger than that can be accommodated by say a LAN which can handle only 1526 bytes in one frame.
- In such a case, the datagram has to be fragmented and sent over the network.
- The minimum datagram size that every host and router must handle is 576 bytes, Each fragment contains most of the original datagram header.

Identification (16 bits) :

- Unique id to identify the datagram. This field is to let the destination know which fragment belongs to which datagram.
- The Source address, destination address and the Identification together uniquely identify the datagram on the Internet.

Flags (3 bits) :

- If the first bit, called do-not-fragment bit, is set to I, this is to indicate that the datagram should not be fragmented. If a router cannot handle the datagram without fragmenting it the datagram is discarded and an error message is sent to the source.
- The second bit is called more-fragments bit, and is set to 0 to indicate that this is the last fragment. The third bit remains unused.

Fragment offset (3 bits) :

- Specifies the offset of the fragment in the datagram, measured in 8 octets (one octet is 8 bits), starting at offset 0. The destination

receives all the fragments and reassembles the fragments using the offset value starting with 0 to the highest value.

Time-to-Live (12 bits) :

- It may happen that a packet on the internet may go round and round without reaching the destination, particularly when using the dynamic routing algorithms.
- To avoid such unnecessary traffic, this field is very useful. This field contains the number of hops a packet can travel.
- At every router, this field is decremented by 1 and either the packet reaches the destination before the filed becomes 0, or if it reaches 0 earlier, it is discarded, The default hop count is 64—i.e, the packet can traverse at most through 64 routers.

Protocol (8 bits) : Protocol field specifies which high layer protocol is encapsulated in the data area of the IP packet. The higher layer protocol can be TCP or UDP.

Header checksum (16 bits) :

The bit pattern is considered as a 16-bit integer and these bit pattern are added using one's complement arithmetic and the one's complement of the result is taken as the header checksum.

Note that checksum is calculated only for the header and this value has to be calculated at each router as some of the fields in the header change at each router.

For calculation of the checksum, this field is considered to be having all 0's.

Source IP address (32 bits) : This field contains the IP address of the source which is sending the datagram.

Destination IP address (32 bits) : This field contains the IP address of the final destination.

Options : This is a variable length field. This field contains data for network testing and debugging. The format for option field is option code of one octet followed by data for the option. These options are for operations such as recording the route of a datagram, time-stamping of a datagram along the route and source routing which specifies the route to be taken by the datagram.

- When record route option is set, each router adds its IP address in the options field and then forwards it, When source route option is set and the IP addresses of all the hops are mentioned in the options field, the datagram takes only that route.

- This is not of any significance from an end user point of view, the network administrators used it for finding the throughput of the specific paths.
- However, one needs to know the topology of the network to specify the source routing.
- When timestamp option is set, each router inserts its IP address (32 bits) (which again is optional) and timestamp (32 bits) in the options field which can be analysed at the destination.

Padding (8 bits) :

- To make the IP header to be an exact multiple of 32 bits, the padding bits are added if required.

Data (variable) :

- This is a variable field whose length is specified in the datagram header. It should be an integer multiple of 8 bits.

4.9.2 IPV6

IPv6 is the next generation Internet Protocol designed as a successor to the IP version 4. IPv6 was designed to enable high-performance, scalable Internet. This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.

Features

1. Larger address space : IPv6 has 128-bit address space, which is 4 times wider in bits in compared to IPv4's 32-bit address space. So there is a huge increase in the address space.

2. Better header format :

- IPv6 uses a better heard format. In its header format the options are separated from the base header.
- The options are inserted when needed, between the base header and upper layer data.
- Theis helps in speeding up the routing process.

3. New options : New options have been added in IPv6 to increase the functionality.

4. Possibility of extension : IPv6 has been designed in such a way that there is a possibility of extension of protocol if required.

5. More security : IPv6 includes security in the basic specification. It includes encryption of packets (ESP : Encapsulated Security Payload) and authentication of the sender of packets (AH : Authentication Header).

6. Support to resource allocation : To implement better support for real time traffic (such as video conference), IPv6 includes flow lable in the specification. With flow label mechanism , routers can recognize to which end-to-end flow the packets belongs.

7. Plug and play : IPv6 includes plug and play in the standard specification. It therefore must be easier for novice users to connect their machines to the network, it will be done automatically.

8. Clearer specification and optimization : IPv6 follows good practices of IPv4, and rejects minor flaws/obsolete items of IPv4.

4.9.2.1 IPv6 Addresses

An IPv6 address consists of 16 bytes (octets) i.e. it is 128 bits long as shown in Fig. 4.15.

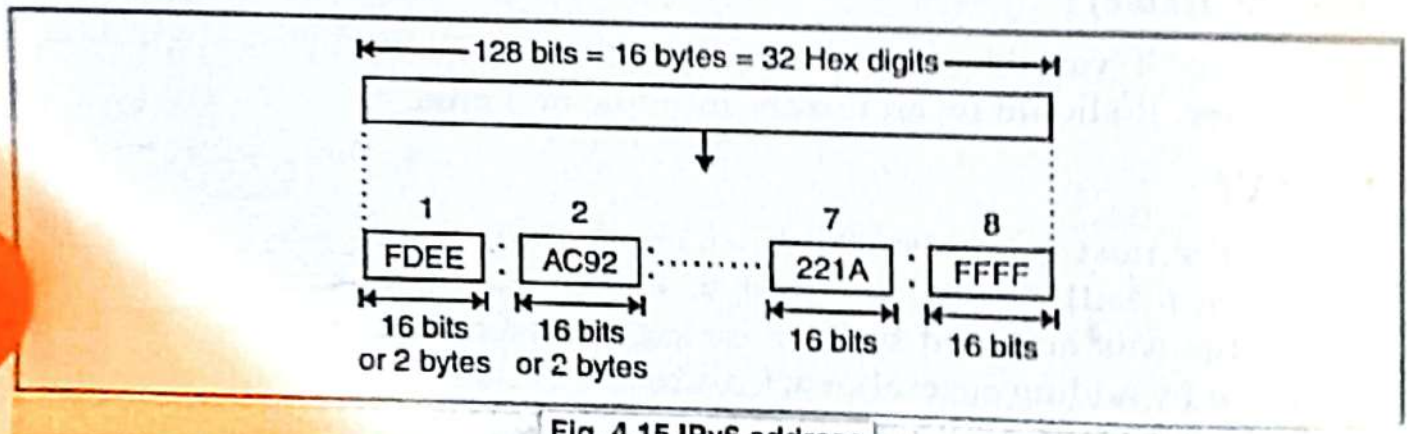


Fig. 4.15 IPv6 address

Hexadecimal Colon Notation

- IPv6 uses a special notation called hexadecimal colon notation. In this, the 128 bits are divided into 8 sections, each one is 2 bytes long.
- 2 bytes correspond to 16 bits. So in hexadecimal notation will require four hexadecimal digits.
- Hence the IPv6 address consists of 32 hex digits and every group of 4 digits is separated by a colon as shown in Fig. 4.15.
- IPv6 uses 128-bit addresses. Only about 15% of the address space is initially allocated, the remaining 85% being reserved for future use.
- This remainder may be used in the future for expanding the address spaces of existing address types or for totally new uses.

4.9.2.2 Abbrevation

- The IPv6 address, even in hexadecimal format is very long. But in this address there are many of the zero digits in it.

- In such a case, we can **abbreviate** the address. The leading zeros of a section (four digits between two colons) can be omitted.
- Note that only the leading zeros can be dropped but the trailing zeros cannot be dropped. This is illustrated in Fig. 4.16.

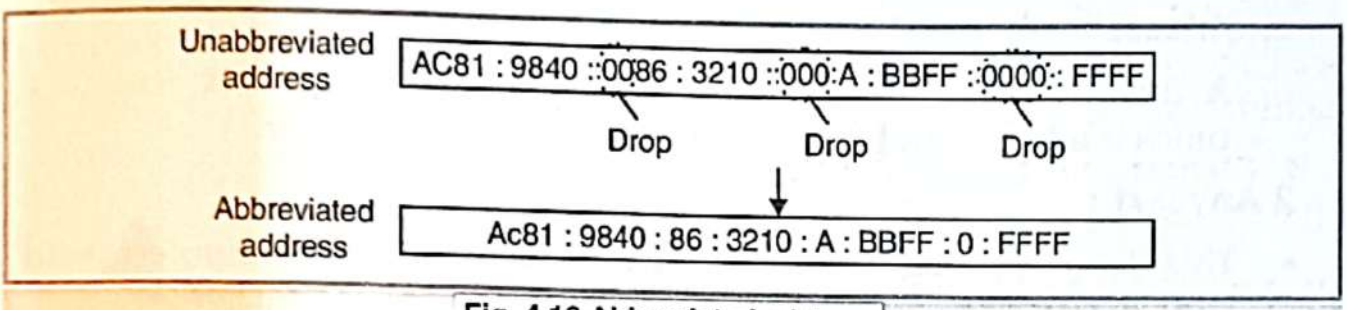


Fig. 4.16 Abbreviated address

Further abbreviation

- Further abbreviation are possible if there are consecutive sections consisting of only zeros.
- We can remove the zeros completely and replace them with double semicolon as shown in Fig. 4.17

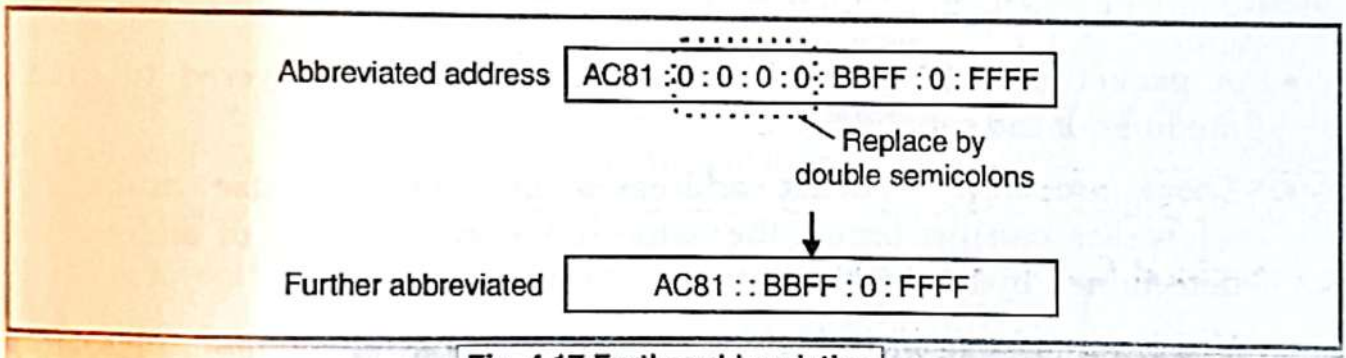


Fig. 4.17 Further abbreviation

- It is important to note that abbreviation is allowed only once per address. Also note that if there are two runs of zero sections, then only one of them can be abbreviated.

4.9.2.3 CIDR Notation

IPv6 Protocol allows classless addressing and CIDR notation. Fig. 4.18 shows how to define a prefix of 60 bits using CIDR.

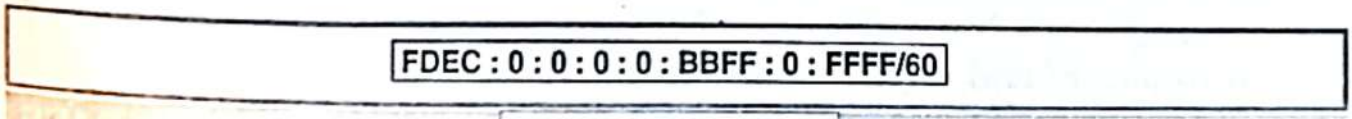
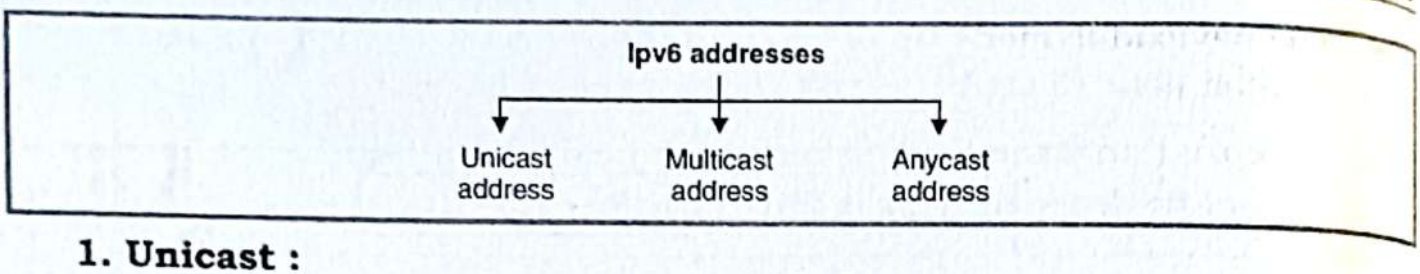


Fig. 4.18 CIDR address

4.9.2.4 Categories of Address

IPv6 defines three different types of addresses.



1. Unicast :

A unicast address defines a single computer. A packet sent to a unicast address and delivered to that specific computer.

2 Anycast :

- This is a type is of address defines a group of computers with addresses which have the same prefix.
- A packet sent to an anycast address must be delivered to exactly one of the members of the group which is the closest or the most easily accessible.

3. Multicast addresses

- A multicast address defines a group of computers which may or may not share the same prefix and may or may not be connected to the same physical network.
- A packet sent to a multicast address must be delivered to each member of the set.
- There are no broadcast addresses in IPv6, because multicast addresses can perform a the same function. The type of address is determined by the leading bits.
- Multicast addresses all start with FF (1111 1111) and all other addresses are unicast addresses.
- Anycast addresses are assigned from the unicast address space and they do not differ syntactically from unicast addresses.
- Anycast addressing is a rather new concept and there is little experience with the widespread use of anycast addresses.
- Therefore some restrictions apply to anycast addressing in IPv6 until more experience is gained.
- An anycast address may not be used as the Source Address of an IPv6 packet and anycast addresses may not be assigned to hosts but to routers only.

4.9.2.5 IPv6 Packet Format

- The IPv6 packet is shown in Fig. 4.19. Each packet consists of a base header which is mandatory followed by the payload.

- The payload is made up of two parts.

1. Optional extension headers and 2. Data from an upper layer

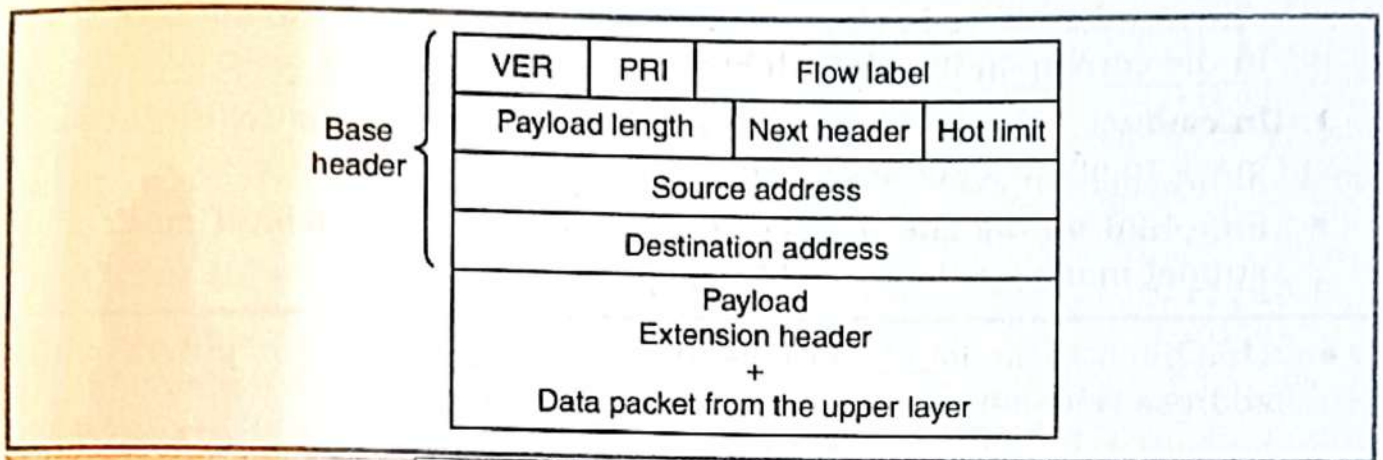


Fig. 4.19 Format of an IPv6 datagram

- The base header is 40 byte length whereas the extension header and the data from upper layer contain upto 65,535 bytes of information.

Base header

Fig. 4.19 shows the base header. It has eight fields. These fields are as follows :

1. Version (VER) : It is a 4 bit field which defines the version of IP such as IPv4 or IPv6. For IPv6 the value of this field is 6.

2. Priority : It is a 4 bit field which defines the priority of the packet which is important in connection with the traffic congestion.

3. Flow label : It is a 24 bit (3 byte) field which is designed for providing special handling for a particular flow of data.

4. Payload length : This is a 2 byte length field which is used to define the total length of the IP datagram excluding the base header.

5. Next header : It is an 8 bit field which defines the header which follows the base header in the datagram.

6. Hop limit : This is an 8 bit field which has the same purpose as TTL (time to live) in IPv4.

7. Source address : It is a 16 byte (128 bit) internet address which identifies the original sources of datagram.

8. Destination address : This is a 16 byte (128 bit) internet address which identifies the final destination of datagram. But this field will contain the address of the next router if source routing is being used.

4.10 SUBNET MASK

- The number of 1s in the subnet mask is more than the number of 1s in the corresponding default mask.
- In subnet mask we change some of the leftmost 0s in the default mask to make a subnet mask.
- Fig. 4.20 shows the difference between a class B default mask and subnet mask for the same block.

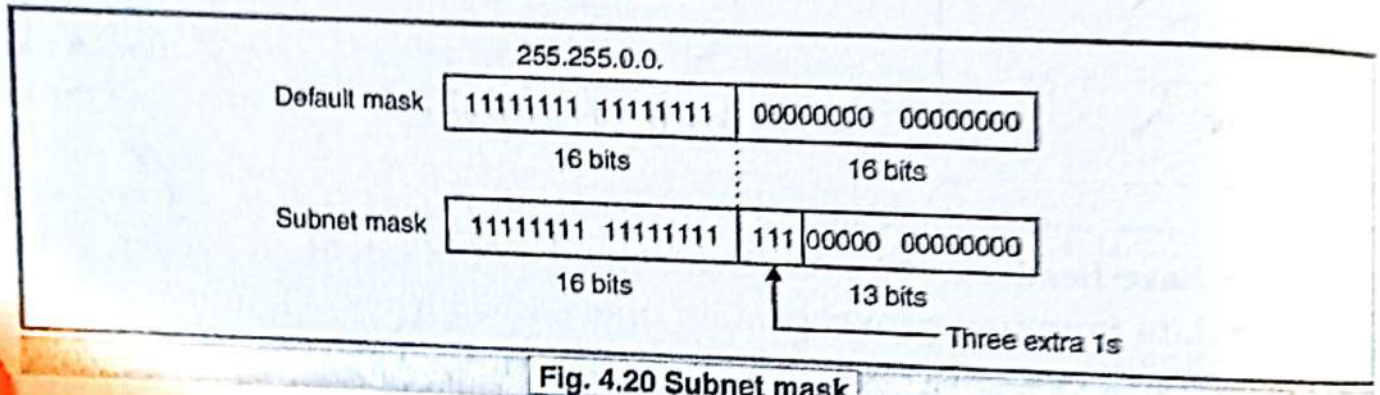


Fig. 4.20 Subnet mask

Number of subnets

The number of subnets is determined by the number of extra 1s. For 3 extra 1s the number of subnets will be $2^2 = 8$. For n 1s the number of subnets is 2^n.

Example : A router inside an organization receives the same packet with a destination address 190.240.34.95. If the subnet mask is 19 (first 19 bits are 1s an following bits are 0s). Find the subnet address.

Solution

- To find the subnet address, AND the destination address with the subnet mask as shown in Fig. 4.21

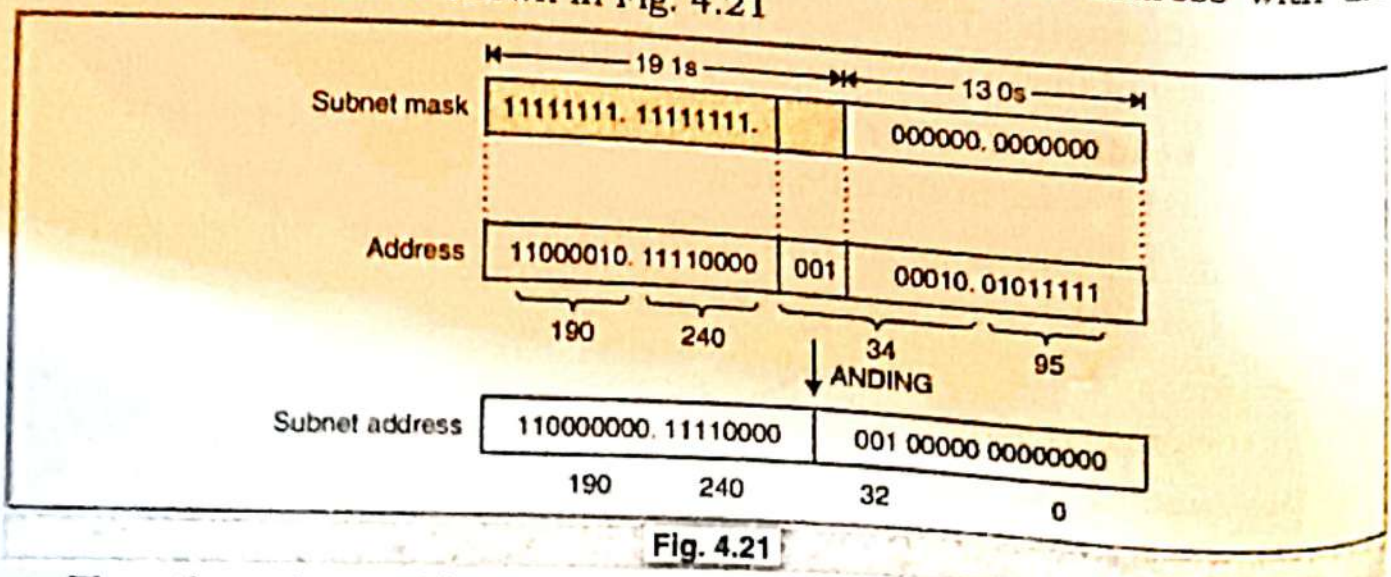


Fig. 4.21

Thus the subnet address is 190.240.32.0

4.11 SUPRENETTING

- The class A and B addresses are almost depleted. But class C addresses are still available.
- But the size of class C address with a maximum number of 256 addresses does not satisfy the needs of an organization. More addresses will be required.
- The solution to this problem **is supernetting**.
- In supernetting an organization combineds several class C blocks to create a large range of addresses i.e. several networks are combined to create a super network.
- By doing this the organization can apply for a set of class C blocks instead of just one.

Example of supernetting

- If an organization needs 1000 addresses, they can be obtained by using four C blocks (one C block corresponds to 256 addresses)..
- The organization can then use these addresses in one supernetwork.

4.12 LIMITATIONS OF IP

The IP as we know it, is running since late 1970's. During those early days of the Internet, there were no PCs and computers were either 'super computer' or mainframes or minis. With the advent of PCs, there has been a tremendous growth in the usage of computers, and the need for networking them, and above all to be on the Internet to access worldwide resources. In 1990's, the need was felt to revise the IP protocol to cater to the exponential growth of the Internet, to provide new series that require better security and to provide new services that require better security and to provide real-time services for audio and video conferencing. IP version 4 has the following limitations.

- The main drawback of IP version 4 is its limited address space due to the address length of 32 bits. Nearly 4 billion addresses are possible with this address length, which appears very high (with a population of 6 billion and a large percentag of the population in the developing world has never seen a computer). But then, now we want every TV to be connected to the Internet, We want Internet-enabled appliances such as refrigerators, cameras and so on. This requirement makes

the present address length of 32 bits insufficient, and it needs to be expanded.

- The present IP format does not provide the necessary mechanisms to transmit audio and video packets which require priority processing at the routers so that they can be received at the destination with constant delayd, not variable delay. As the Internet is being used extensively for voice and video communications, the neeed for change in the format of the IP datagram is urgent.
- Applications such as e-commerce reqire high security—both in terms of maintaining secrecy while transmitting and authentication of the sender. IP version 4 has very limited security features.
- The IP datagram has fixed header with variable options, because of which each router has to do lot of processing which calls for high processing power of the routers and also lot of delay in processing.

Due to these limitations of IP version 4, IP version 6 has been developed. IP version 5 has been used on an experimental basis for some time, but it was not widely deployed.

4.13 INTENET CONTROL MESSAGE PROTOCOL (ICMP)

- The Internet is a dyanmic network.
- Networks get connected and removed without the knowledge of the senders, who can be anywhere on the earth.
- Each router functions autonomously, routing the datagrams based on the destination IP address and the routing table. It is likely that a datagram cannot be forwarded or delivered to the dstination, or due to congestion the datagram may have to be dropped, and so on.
- There must be a procedure to report errors to the source whenever there is a problem.
- The Internet Control Message Protocol (ICMP) is used for this purpose.
- Every IP implementation must support ICMP also. ICMP message are a part of the data field of the IP datatram.
- ICMP message, which is encapsulated in the data field of the IP datagram, consits if three fields :
- Message type of identify the type of message (8 bits)
- Code field to provide further information on the message type (8 bits)

- Checksum field (16 bits), which uses the same algorithm as the IP checksum
- In addition, ICMP messages contains first 64 datas bits of the datagram which caused the problem. The ICMP type fields and corresponding message types are given in the following table :

Type field	ICMP message type
0	Echo reply
3	Destination unreachable
4	Source quench
5	Change the route (redirect)
8	Echo request
11	Time to live expired for datagram
12	Parameter problem on datagram
13	Time stamp request
14	Time stamp reply
17	Address mask request
18	Address mask reply

- Echo reauest and echo replay messages are use to test the reachability of a system.
- Source sends and echo request to the receiver and the receiver sends an echo reply to the sender.
- The request can contain an optional data field which is returned along with the echo reply.
- When an echo reply is received by the sender, this is an indication that the entire route to the destination is ok and the destination is reachable.
- The system command 'ping' is used to send the ICMP echo requests and display the reply messages.
- Reports of unreachable destination are sent by a router to the source.
- The possible reason is also sent in the ICMP message. The reason can be the following :
  - Network unreachable
  - Host unreachable
  - Protocol unreachable
  - Port unreachable

- Fragmentation has to be done but do-not-fragment bit is set
- Source host failed
- Destination network unknown
- Source routing failed
- Destination network unknown
- Source host isolated
- Communication with the destination network prohibitedd for administrative reasons.
- Network unreachable for type of service and host unreachable for the type of service

- The source quench message is sent by the router to the source when congestion is experienced.
- This message is to inform the source to reduce its rate of datagrams as the router cannot handle such a high speed.
- When a router cannot handle the incoming datagrams, it discards the datagram and sends the source quench message to the source.
- Change the route (redirect) message is sent by a router to the host.
- Generally, it is the router's function and responsibility to update its routes and hosts keep minimal routing information.
- However, when a router detects that a host is using a non-optimal route, it sends an ICMP message to the host to change the route.
- This message contains the IP address of the router the host has to use for the routing.
- Time-to-live-expired message is sent by a router when the hop count becomes zero.
- As mentioned earlier, to ensure that datagrams do not keep on circulating between routers endlessly, this hop count is introduced.
- When hop count becomes zero, the datagram is discarded and message is sent to the source.
- This message is also sent when fragment reassembly time exceeds the threshold value.
- For any other problem because of which the datagram has to be discarded, the router sends a parameter problem message to the source.
- Timestamp request and replay mesages are used between systesm to obtain the time information.

- As each system acts independently, there is no mechanism for synchronising the closcks. A system can send a timestamp request to another system and obtain the timestamp replay.
- This infomation can be used to compute the delays on the network and also to synchronise the clocks of the two systems.
- Subnet address mask request and reply messages are exchanged between machines.
- In some IP address, a portion of the host address correspods to the subnet address.
- The information required to interpret this address is represented in by 32 bits called subnet address mask .
- For example, if a host wants to know the subnet mask used by a LAN, the host sends a subnet address mask request to the router on the LAN or braodcasts the message on the LAN. The subnet address mask replay would contain the subnet address mask.

SUMMARY

The Internet Protocol, the heart of the global Internet, is presented in this chapter. The present version of IP, running on the end systems and routers, is IP version 4. The two main functions of IP are addressing and routing. IP version 4 has an address length of 32 bits. Each system is given a 32-bit IP address which uniquely identifies the system globally. This addressing scheme can cater to at most 4 billion addresses. This turns out to be a small number in future, particularly when we would like to connect even consumer items such as TV, mobile phopnes etc, to the Internet. The latest version of IP, IP version 6, has an address length of 128 bits.

In addition to the address length, IP version 4 has limitations for handling secure applications and real-time applications. The detailed formats of IP version 4 and version6 have are presented which bring out the salient features of both the versions.

Another important function of IP is routing. We studied the routing protocols within an autonomous system and between antonomous systems. An autonomous system is a network within the administrative control of an organisation. Routers within an autonomous system can share the routing information using protocols such as Open Shortest Path First (OSPF) and flooding . Routers connected to differnet autonomous systems can share the routing information using Exterior Gateway Protocol or Border Gateway Protocol.

The Internet Control Message Protocol (ICMP) is used to repoprt errors and to send management information between routers. ICMP messages are sent as a part of the IP datagram. The details of ICMP are also presented in this chapter.

EXERCISE

SHORT ANSWER QUESTIONS

1. Describe the format of IP version 4 datagram.
2. What are the limitations of IP version 4 and explain how IP version 6 addresses these limitations.
3. Describe the format of IP version 6 packet.
4. Describe the protocols used for routing within autonomous systems.
5. Describe the protocols use for routing between autonomous systems.
6. Explain the ICMP protocol and its functionality.

DESCRIPTIVE QUESTIONS

1. Fins out the IP address of your computer.
2. Calulate the total number of addresses supported by Class B IP address format. Note that 14 bits are usesd for network id and 16 bits for host id.
3. Calculate the total number of addresses supported by Class C IP address format. Note that 24 bis are used for network id and 8 bits for host id.
4. Calculate the maximum number of addresses supported by IP version 6.
5. Write a technical paper on IP version 6.

□□□□□