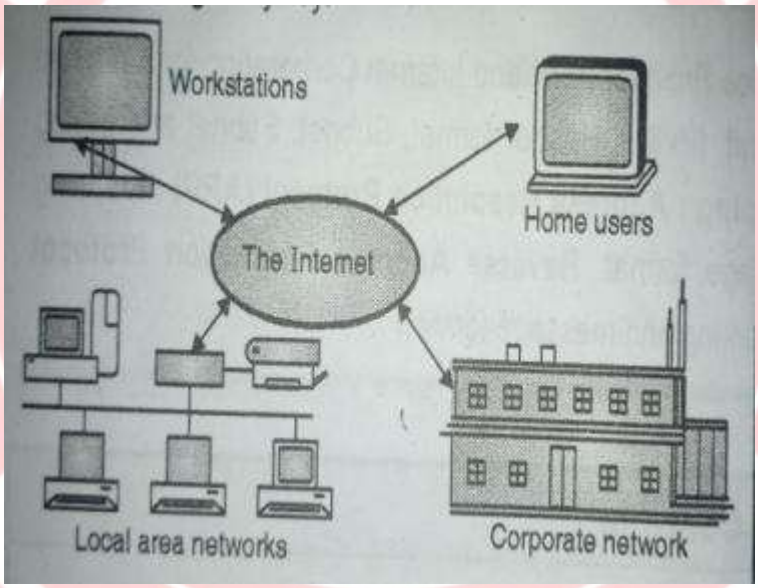
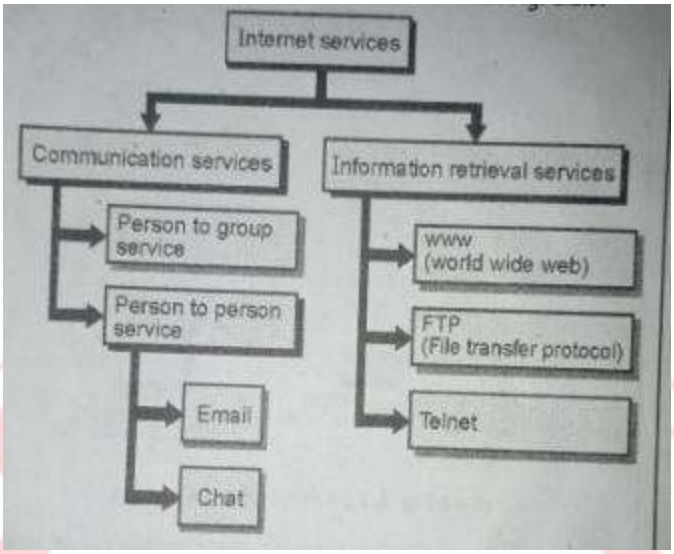
ACN
Unit 1
Internet architecture and network layer

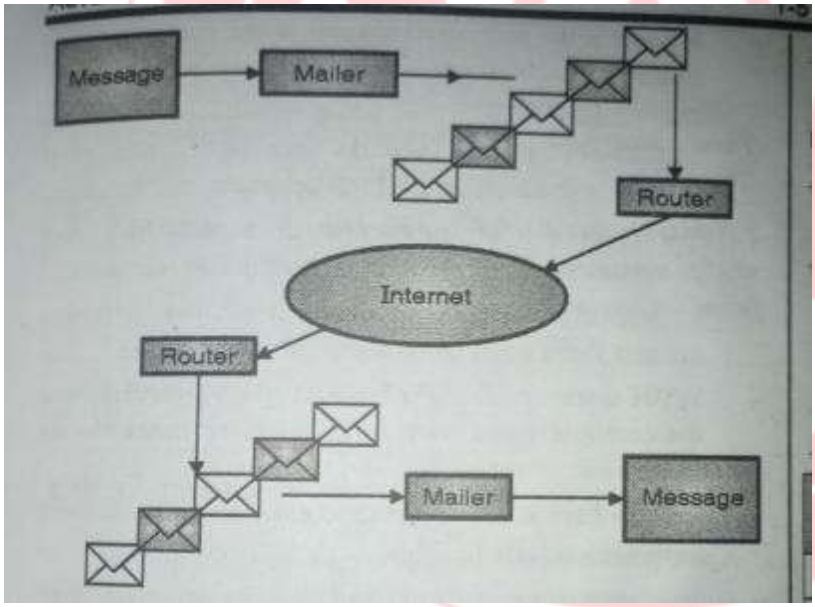
- **ARPANET**:- Advanced Packet Switching Network
- **NSFNET**:- National Science Foundation Network
- **Internet**:-
    - Global information system logically linked together by globally unique address space based on IP and supports communication using TCP/IP providing higher level services
    - Network of networks
    - Interconnection of networks



- **Internet Services:**



- **Route followed by packets:**



- **Internet Address:**
  - Addressing system assigns names and numbers to identify computers in internet
  - Names → Domain names
  - Numbers → IP addresses

– Commonly used domain types are as follows :

Domain name	Description
com	A company or commercial organization
edu	Educational Institutes.
gov	Government organization
mil	Military sites
net	Network resources or Internet service provider.
org	Non profit or non commercial organizations.

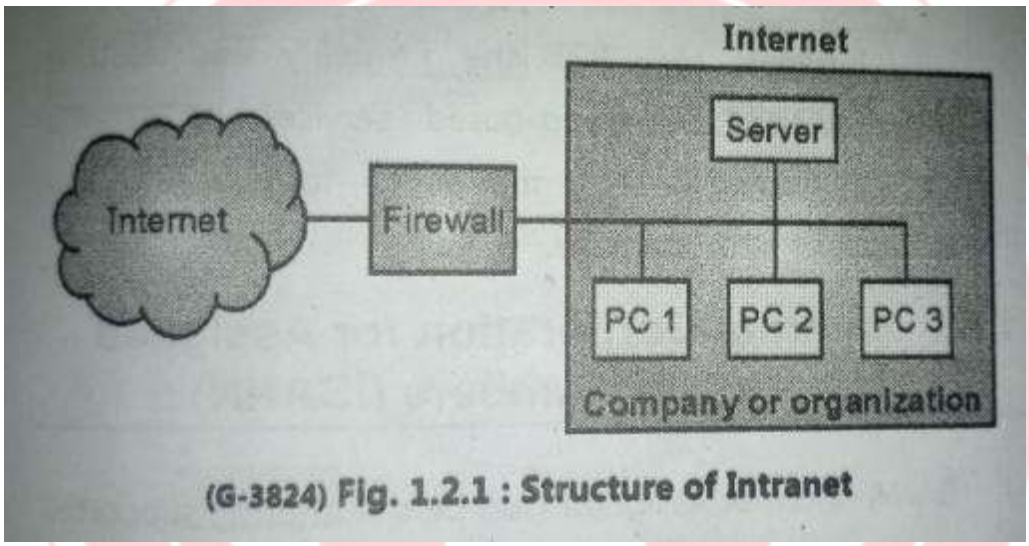
Abbreviation	Country name
au	Australia
fr	France
ca	Canada
uk	United Kingdom
in	India

- **ISP (Internet Service Provider):**
  - They offer various options and packages to public
  - Major payers are
  - VSNL (Videsh Sanchar Nigam Ltd.
  - MTNL (Mahanagr Telephone LTD)
  - Airtel,
  - Jio,
  - Vodafone-Idea,
  - BSNL, and
  - Hathway.

Who Owns Internet

- IETF – Internet Engineer Task Force
- IRTF – Internet Research Task Force
- IAB – Internet Architect Board.

- **Intranet**
  - It is a private network utilized by companies or organizations.
  - It is the implementation of internet technology within a corporate organization
  - As this is a private network, so no one from the outside world can access this network.
  - Used to protect your data and provide data security



(G-3824) Fig. 1.2.1 : Structure of Intranet

- **Why is Intranet Important?**
  - Improves internal communication
  - Connects employees across locations and time zones
  - Boosts recognition and reward
  - Simplifies employee onboarding
  - Provides organizational clarity
  - Encourages knowledge sharing
- **Advantages of intranet:**
  - Ease of administration
  - High development speed

- Flexibility in information presentation
- the cost of conveying data utilizing the intranet is very low.
- It can be utilized as a correspondence center point where employees can store data at whatever point they need and download files in just a few seconds.
- It connects employees with each other.
- The documents stored on the intranet are much more secure.

- **Disadvantages:**
  - Security risks
  - Unauthorized access and misuse by employees
  - Limited scalability
  - Maintenance overload
  - Limited access
  - Lack of flexibility

Sr. No.	Feature	Intranet	Internet
1.	Accessibility	Private (restricted to authorized users).	Public (accessible to anyone).
2.	What is?	A private network, within an Enterprise or Organization.	Worldwide/global system of connected networks.
3.	Purpose	Internal communication.	Global information sharing.
4.	Security	Highly secure (Firewalls, VPNs).	Less secure.
5.	User-base	Limited to organization members.	Open to all.
6.	Network	Localized Network.	Worldwide Network.
7.	Expensive	More expensive.	Less expensive.
8.	Content type	Organization-specific resources.	Diverse global content.
9.	Reliability	More reliability.	Less reliability.

- **ICANN-** Internet Corporation for Assigned Names and Numbers
- Responsible for internet Domain Names and Addresses
- Roles of ICANN:
  - Managing and coordinating DNS
  - Assigning domain names and operations to root server
  - Allocating IP addresses and managing global internet protocol address space
  - Ensuring that domain names and IP addresses are unique and accessible globally
- ICANN has divided port numbers into following ranges:

- Well known ports
    - 0 to 1023
- Registered ports
    - 1024 to 49151 → not assigned and controlled by ICANN
    - Can be registered with ICANN to avoid duplication
- Dynamic ports(private ports)
    - 49152 to 65535
    - Neither controlled nor registered with ICANN
    - Temporary or private ports

- **Advisory bodies of ICANN**
    - *GAC*- Government Advisory Committee
        - Advises matters related to internet
    - *GNSO*- Generic Names Supporting Organization
        - Represent non-country codes
        - for TLD- top level domain registries, business and individual users
        - Develops policies for generic TLDs
    - *CCNSO*- Country Code Names Supporting Organization
        - Develops policies for country code TLDs
    - *ALAC*- At-Large Advisory Committee
        - For individual internet users
    - *SSAC*- Security And Stability Advisory Committee
        - Advises on matters related to security and stability of DNS and Internet Infrastructure
- **IPv4 Header Format**

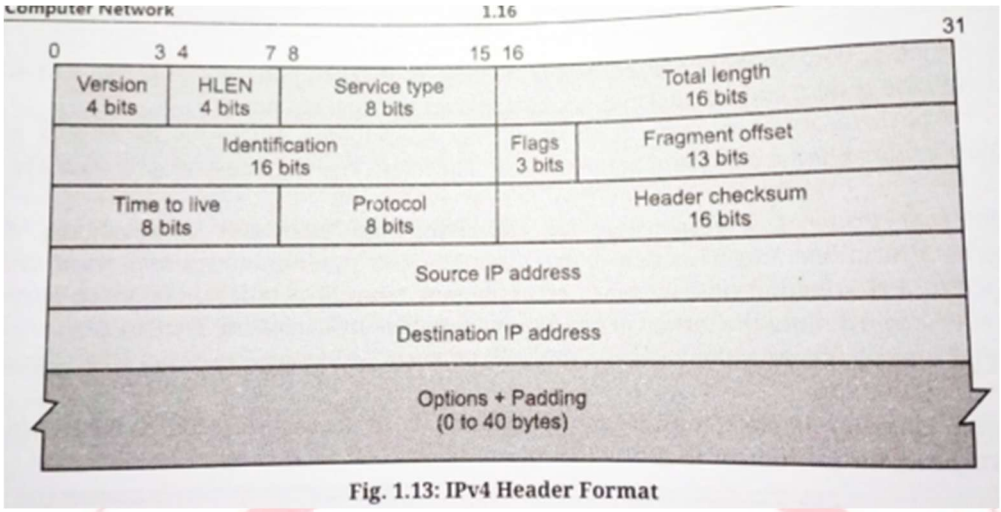
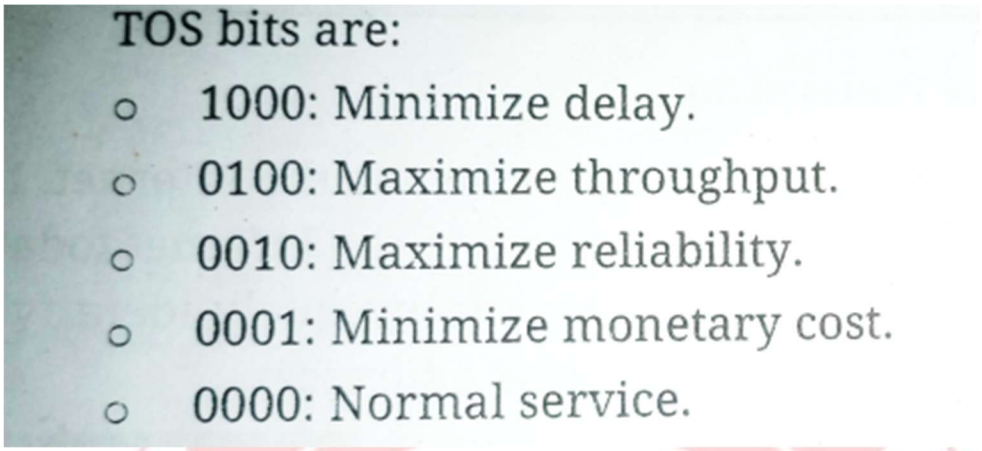


Fig. 1.13: IPv4 Header Format

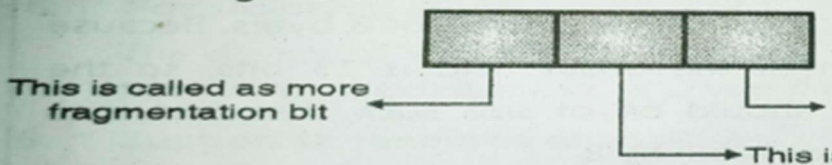
- **Version(VER):**
  - 4-bit field
  - Defines version of IP format
  - Current version is 4 → hence IPv4
  - Field indicates- IP software running on processing machine– that datagram belongs to IPv4
  - If some other IP version → datagram is discarded
- **HLEN(Header Length):**
  - 4- bit field defines datagram object in 4-byte word
  - Length of header is variable
  - Between 20 to 60 bytes
  - Default header length – 20 bytes
    - Value of field is 5→5 x 4=20
  - For max size
    - Value of field is 15→15 x 4=60
- **Type of Service(TOS)**
- Provides network service parameters
- Composed of 3-bits precedence field(generally ignored)
- 4 TOS bits and unused bit- must be 0
- 4 TOS bits are:



- **Total length**
  - 16-bit field
  - Defines total length of datagram
  - Max length= 2raised to 16- 1
  - Contains combined data and header length
  - HLEN X 4 -> header length
  - Length of Data= Total Length – Header Length
- **Identification**
- Identifies datagrams source host
- when datagram is fragmented- identification field is copied to all fragments
- **This number is used by destination to reassemble fragments**
- **Flags**
- 3-bit field
- First bit- reserved- should be 0
- Second bit- known as “Do Not Fragment” bit
  - If 1 – datagram is not fragmented
  - If 0 – machine should fragment datagram(if necessary)
- Third bit-(M)- “More Fragment Bit”
  - M=1 ,datagram is not last fragment
  - M=0, datagram is last or the only fragment

6. Flags :

– Flag is a three bit field. The 3 bits are as shown in Fig. 1.9.5.

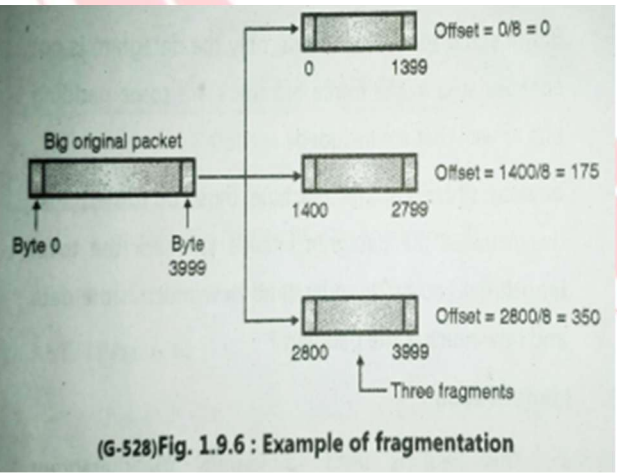


(G-527)**Fig. 1.9.5 : Flag bits**

6. Flags: This router fragment activity is controlled by following three flags:

Sr. No.	Flag	Description
1.	0	Reserved, must be zero.
2.	DF (Do not Fragment)	0 means allow fragmentation; 1 means do not allow fragmentation.
3.	MF (More Fragments)	0 means that this is the last fragment of the datagram; 1 means that additional fragments will follow.

- **Fragmentation offset**
  - 13 bits field
  - Used to indicate the relative position of this fragment with respect to complete datagram
  - It is the offset of data in original datagram
  - In units of 8 bytes
  - Fragments should be divisible by 8



(G-528)**Fig. 1.9.6 : Example of fragmentation**

- **Time to live (TTL)**

- If routing table gets corrupted → datagram travels between routers → but never reaches destination
- *TTL*- limits the lifetime of datagram
- It limits the journey of packet intentionally
- TTL field ia 1 – for local network packet
- When packet reaches to first router TTL is changed to 0

- **Protocol**
  - 8-bit field
  - Defined higher level protocols which uses services of IP layer
  - Data from different protocols is encapsulated into IP datagram
  - Contains- name of protocol and destination IP address
  - At destination this value helps in demultiplexing

Protocol	Description
0	Reserved.
1	Internet Control Message Protocol (ICMP).
2	Internet Group Management Protocol (IGMP).
3	Gateway-to-Gateway Protocol (GGP).
4	IP (IP encapsulation).
5	Stream.
6	Transmission Control Protocol (TCP).
8	Exterior Gateway Protocol (EGP).
9	Private Interior Routing Protocol.
17	User Datagram Protocol (UDP).
41	IP Version 6 (IPv6).
50	Encap Security Payload for IPv6 (ESP).
51	Authentication Header for IPv6 (AH).
89	Open Shortest Path First.

- **Header checksum**
  - Covers on header only
  - When header field changes checksum is recomputed and verified
  - It checks and monitors communication errors

- It does not cover data followed by header

- **Source address**
  - 32-bit field
  - Stores source address
  - This field must remain unchanged during the time datagram travels from source host to destination host
- **Destination address**
  - Defines/stores IP address of destination
  - 32-bit field
  - This field must remain unchanged during the time datagram travels from source host to destination host
- **Options**
  - Last field of header
  - Used for additional information
  - Not required for every datagram
  - Used for network testing and debugging
  - When used- header length is greater than 32bits
- **IPv6 Header Format:**
  - Design for future Internet → Internet version 2
  - Latest version of IT
  - Enables network nodes to incorporate seamlessly
  - IPv6 fixed headed is 40 bytes long

-

1. Version (4 bits)

- Represents version of IP

2. Traffic class (8 bits)

- Divided in to 2 parts
- Most significant bits – used for type of service to be provided to this packet
- Least significant 2 bits – used for Explicit Congestion Notification (ECN)

3. Flow label (20 bits)

- Used to maintain sequential flow of packets
- Source labels the sequence to help router identify packet belongs to specific flow of information.
- This field avoids reordering of data packets.
- It is designed for streaming / real time data.

4. Payload length (16 bit)

- Tells router how much information of packet contains in its payload
- Payload is composed of extension header and upper layer data
- Using 16 bits upto 65535 bytes can be indicated.
- If extension header contains Hop By Hop extension header - payload exceeds 65535 bytes – this field is set to zero.

5. Next Header (8 bits):

- the type of extension header
- It defines header which follows the base header.

6. Hop Limit (8 bits):

- It stops packet to loop in network
- infinitely same as TTL in IPv4
- Hop limit is decremental by one – as it passes a link (Router/ Hop)
- When field reaches zero packet is discarded

7. Source Address (128 bits):

- The IPv6 address of the packet's originator.

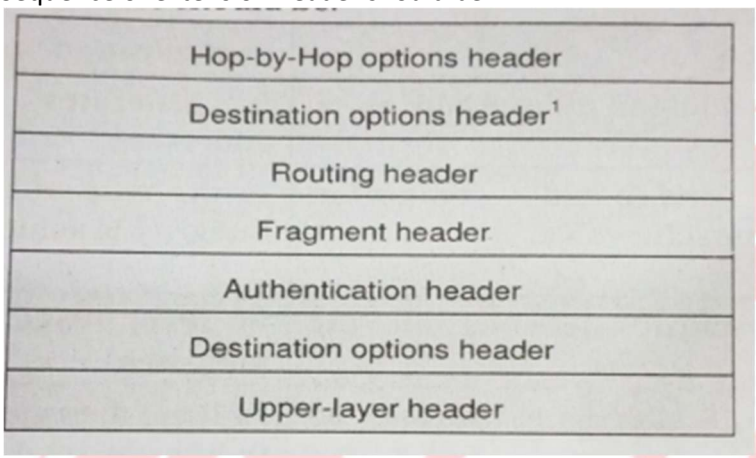
8. Destination Address (128 bits):

- The IPv6 address of the packet's final destination.
- Intermediate nodes use this information for correct routing.

IPv6 Extension Header:

- Used to encode optional internet layer information

- Placed between IPv6 header and upper layer header
- Extension header are chained together using next header field
- If no more extension header – it indicates upper layer header (TCP UDP ICNT)
- Sequence of extension header should be



- Extension Headers are arranged one after another in a linked list manner, as depicted in Fig. 1.15.

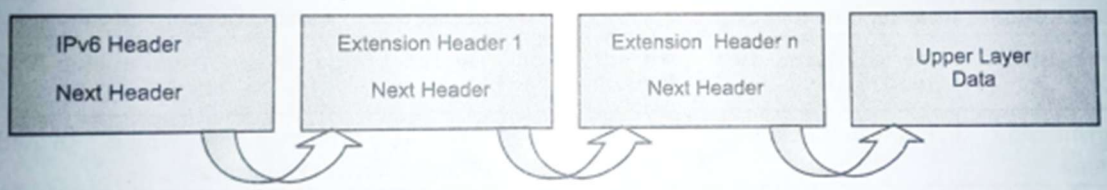


Fig. 1.15: Extension Headers Connected Format

- Following table illustrates the difference between IPv4 and IPv6:

Parameters	IPv4	IPv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon (:).
Classes	IPv4 has five different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask (means that IPv4 converts IP addresses into a subnet of different sizes)).	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets.
Use in Industry	Many companies have historically used and continue to use IPv4, including major tech companies like Apple, Microsoft, and Google, as well as other organizations like Ford Motor Company and AT&T.	These addresses are used by Comcast, Reliance Jio, T-Mobile USA, Sky broadband, Claro, Softbank, Orange, SK telecom, Cox communication, Kabel Deutschland and many more.

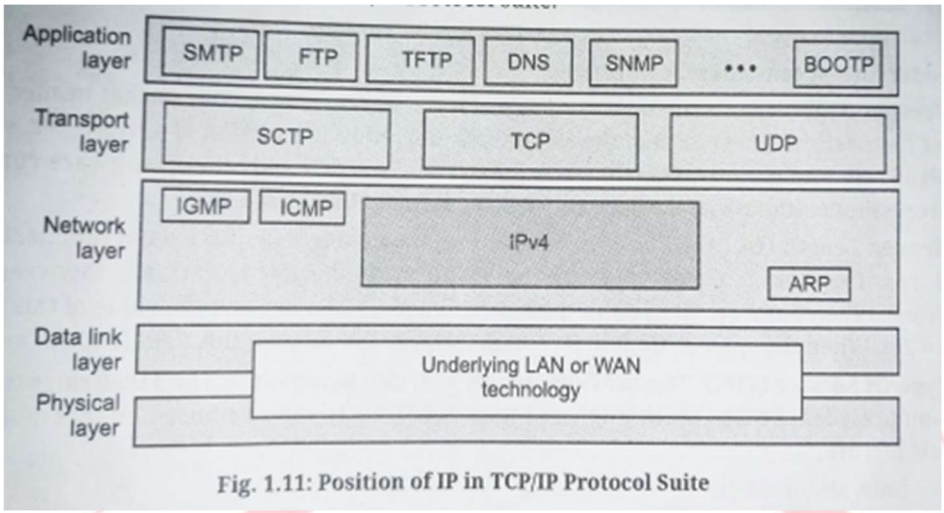


Fig. 1.11: Position of IP in TCP/IP Protocol Suite

ROUTERS IN THE INTERNET AND ITS FUNCTIONS

- **Routers-** specialized network devices that direct data packets between different networks by selecting optimal paths, based on routing tables and algorithms.
- They **analyze** the destination IP address in each packet header and decide which interface or link the packet should be forwarded through.
- Routers **help** segment broadcast domains, reducing network congestion and improving security between network segments.
- They **implement security** policies, like filtering traffic using ACLs, and support redundancy using protocols like HSRP or VRRP for high availability.
- **IP Address and IP Addressing(with IPv4 address)**
- IP Addressing:
  - Method used to identify hosts and network devices
- **IP Address:**
  - Address used to uniquely identify a device on IP network
  - Numerical 32 bits representation
  - 2 parts:
    - Network ID- identifies network
    - Host ID- identifies device

Fig. 1.16 (a): Parts of an IP Address

Fig. 1.16 (b): Example of an IP Address

- **Address Space**
- Total number of addresses used by protocol
- If protocol uses N bits to define address→ address space is 2N
- Each bit has 2 values- 0 or 1
- IPv4 - 32 bit addresses – so address space 64 bits
    - More than 4 billion devices
- Classful Addressing – divides address space in 5 classes

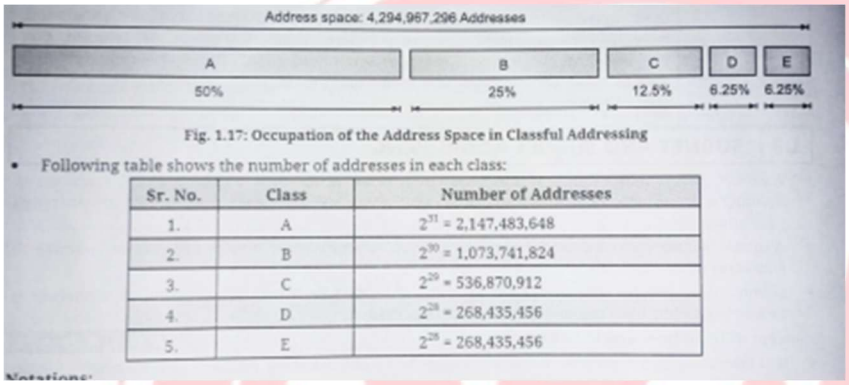


Fig. 1.17: Occupation of the Address Space in Classful Addressing

- Following table shows the number of addresses in each class:

Sr. No.	Class	Number of Addresses
1.	A	2^{31} = 2,147,483,648
2.	B	2^{30} = 1,073,741,824
3.	C	2^{29} = 536,870,912
4.	D	2^{28} = 268,435,456
5.	E	2^{28} = 268,435,456

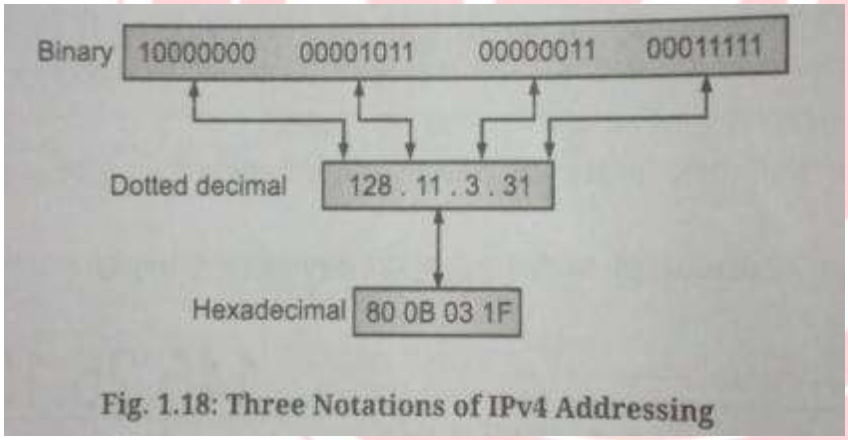


Fig. 1.18: Three Notations of IPv4 Addressing

- Hexadecimal notation is used for network programming
- Dotted decimal notation – human readable format
- **Classful addresses**

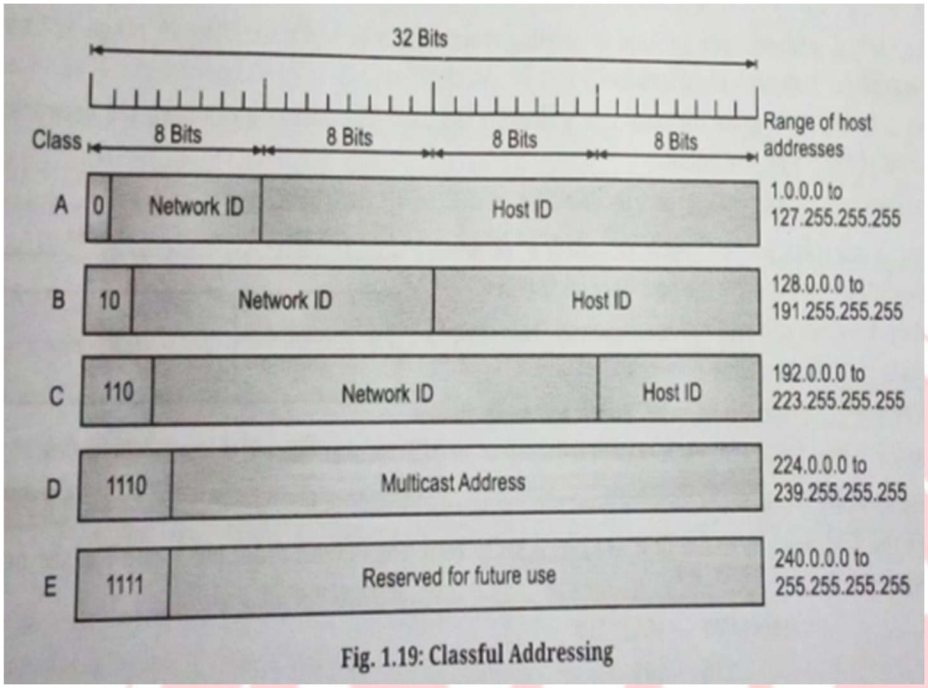


Fig. 1.19: Classful Addressing

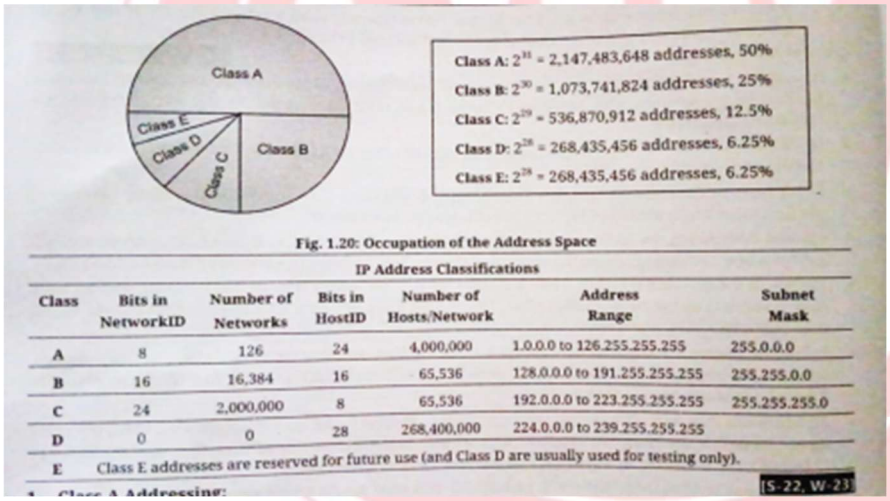


Fig. 1.20: Occupation of the Address Space

IP Address Classifications

Class	Bits in NetworkID	Number of Networks	Bits in HostID	Number of Hosts/Network	Address Range	Subnet Mask
A	8	126	24	4,000,000	1.0.0.0 to 126.255.255.255	255.0.0.0
B	16	16,384	16	65,536	128.0.0.0 to 191.255.255.255	255.255.0.0
C	24	2,000,000	8	65,536	192.0.0.0 to 223.255.255.255	255.255.255.0
D	0	0	28	268,400,000	224.0.0.0 to 239.255.255.255	
E	Class E addresses are reserved for future use (and Class D are usually used for testing only).					

- **Class A Addressing:**
- First bit of first octet is 0
- Highest order bit of network byte is always 0
- Range of first octet 1 to 127
  - 00000001 - 01111111
- IP address – 1.x.x.x to 127.x.x.x.
- Default subnet mask - 255.0.0.0

- 126 networks and 16777214 hosts

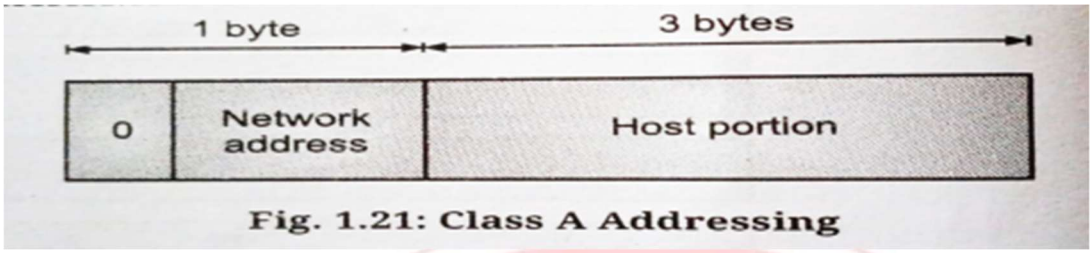
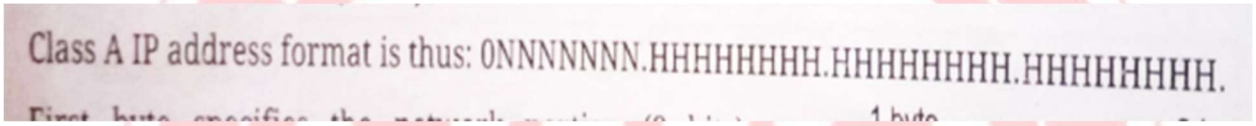


Fig. 1.21: Class A Addressing

- First byte – network portion(8 bits)
- Remaining bytes host portion(24 bits)
- Network values 0 &126 → reserved
- Class A- used for large network addressing
- More than 16 million host values for each class A network


Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH.

- **Class B Addressing**
  - first octet starts with 10
  - Address range:
    - 10000000 - 10111111
    - 128 - 191
  - IP address range:
    - 128.0.X.X to 191.255.X.X
    - Default class B – 255.255.x.x
  - Class B has → 16384 network addresses
    → 65534 host addresses
  - This class is used for – medium sized networks
  - More than 16 thousand networks
  - 65000 nodes in each network

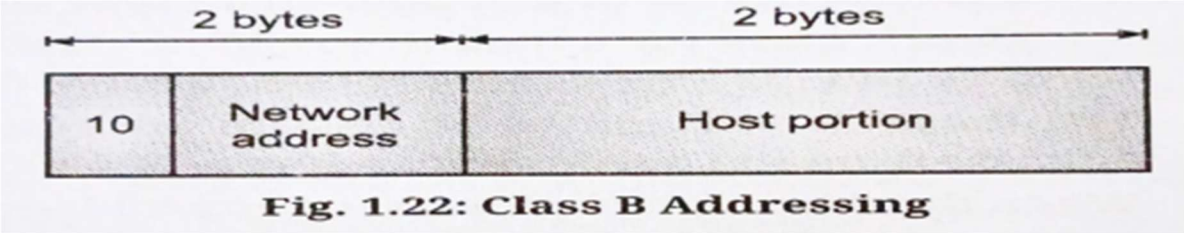


Fig. 1.22: Class B Addressing

- Class B IP address format is: 10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH.

- **Class C Addressing**
  - First 3 bits- 110
  - Higher order bits of network portion – 110
  - Address range- 11000000- 11011111
    - 192- 223
  - IP address range : 192.0.0.X to 223.255.255.X
  - Default class C address 255.255.255.X
  - 2097152- network addresses
  - 254 host addresses
  - There are more than 2 million class C networks
  - 254 nodes in each network

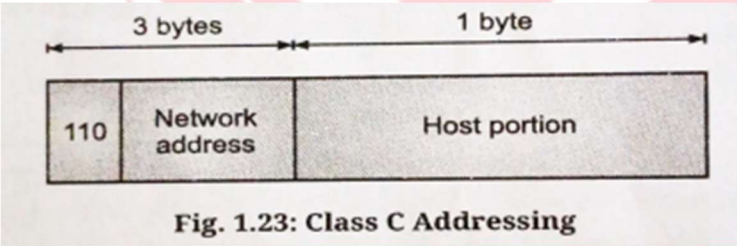


Fig. 1.23: Class C Addressing

- Class C gives 2097152 (221) Network addresses and 254 (2[illegible])
- Class C IP address format is: 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH.

2 bytes 1 byte

- **Class D Addressing**
  - First 4 bits : 1110
  - 11100000 – 11101111
  - 224 – 239

- IP address range : 224.0.0.0 to 239.255.255.255
- Class D – reserved for multitasking
- Data is for multiple hosts
- No need to extract host address from class D
- Doesn't have subnet mask
- Defines group ID

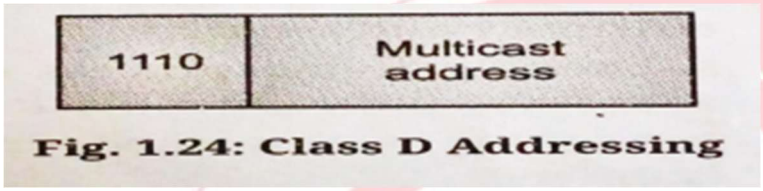


Fig. 1.24: Class D Addressing

- **Class E Addressing**
  - IP address- reserved for experimental purpose
  - Only for R&D and study
  - IP address range: 240.0.0.0 – 255.255.255.254
  - Class is not equipped with any subnet mask

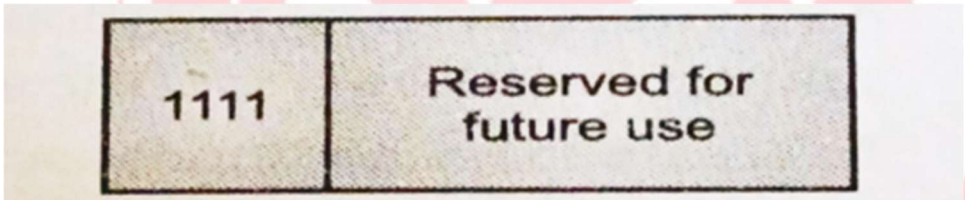
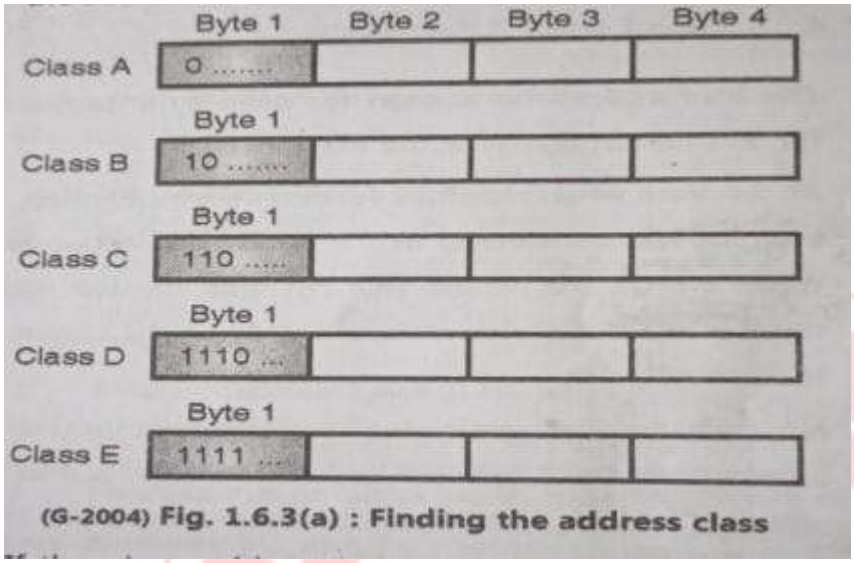


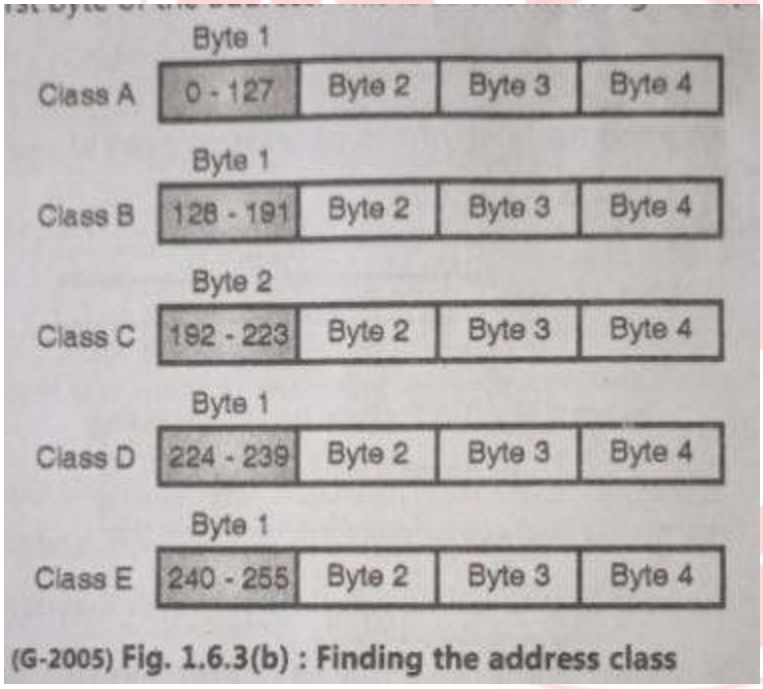
Fig. 1.25: Class E Addressing

- **How to recognize classes?**
- Binary Notation →



(G-2004) Fig. 1.6.3(a) : Finding the address class

- Dotted decimal notation→



(G-2005) Fig. 1.6.3(b) : Finding the address class

- Network Address:
  - Used in routing a packet to its destination network
  - Router extracts network address from destination address of packet
  - We need a network mask

- Network mask- 32-bit number with leftmost bits all set to 1's
- (32-n) rightmost bits all set to 0's
- Destination address is ADNed with default mask→result is network address

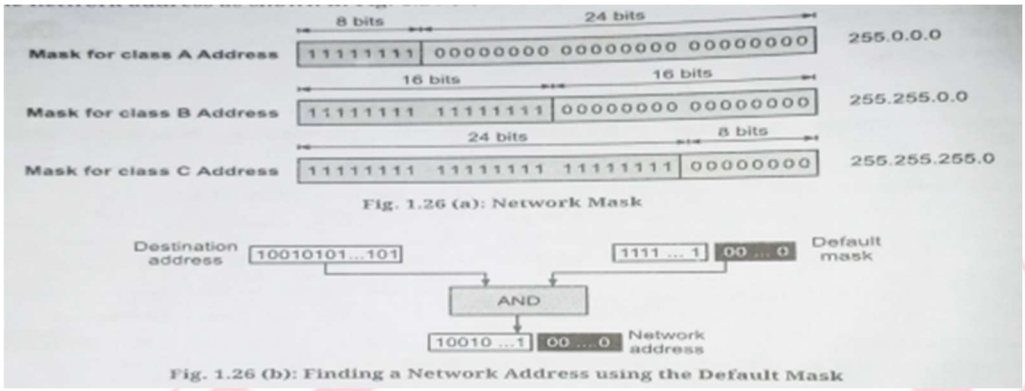


Fig. 1.26 (a): Network Mask

Fig. 1.26 (b): Finding a Network Address using the Default Mask

- **SUBNET AND SUBNET ADDRESSING**
- **SUBNET:**
  - logical subdivision of IP network
  - Smaller network within larger network
  - Improves network security and efficiency.
- **SUBNETTING (SUBNET ADDRESSING):**
  - Process of dividing larger network into smaller networks called as **subnetworks/subnet**, manageable segments
  - Sub division by borrowing bits from host position of IP address
  - Each segment with own **unique** range of IP addresses
- Benefits of subnetting

  1. Efficient IP address usage
  2. Improved network performance
     - BY reducing network traffic and improving routing efficiency
  3. Enhanced security
  4. Easier network management
- **Address masking**
  - Known as subnet masking.
  - Uses – Subnet mask to divide IP address into network portion and host portion.

- Allows a larger network to be divided into subnetworks
- A **mask** is used to determine what subnet an IP address belong to.
- The process that extract address of physical network from an IP address is called **masking.**
- Subnet mask is a 32-bit value
- Subnets are created using subnet mask.

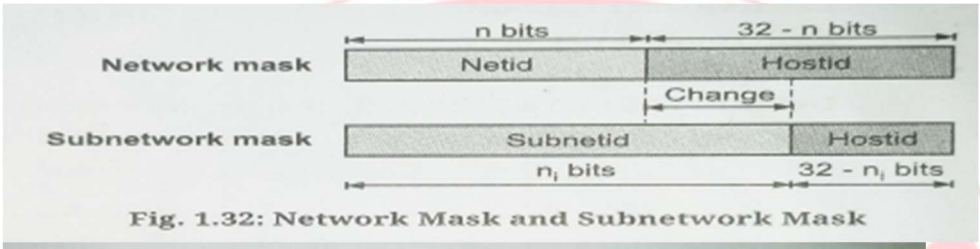


Fig. 1.32: Network Mask and Subnetwork Mask

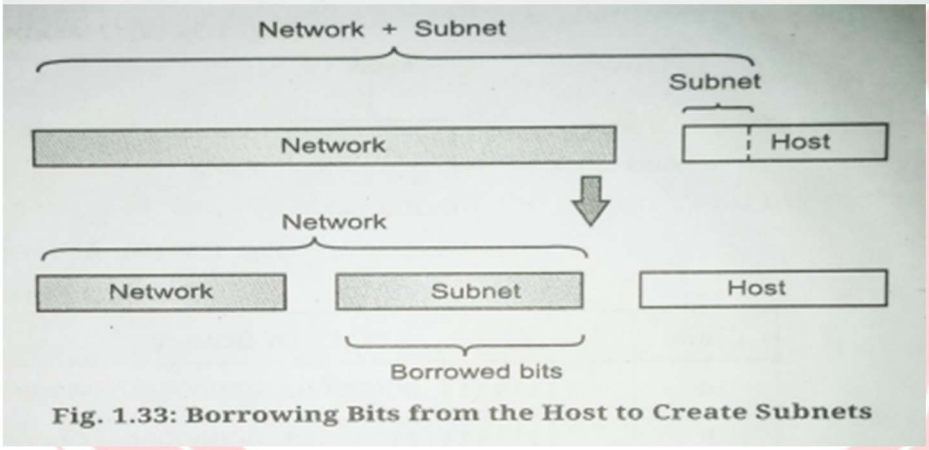


Fig. 1.33: Borrowing Bits from the Host to Create Subnets

- Network mask is used when network is not subnetted.
- Subnetwork has subnet ID and host ID
- Subnets are created by borrowing bits from the host portion of IP address.
- Network portion of IP address and new subnet bits are used to define new subnet
- Router use this information to forward data packets to proper subnets
- Number of bits in subnet mask determines number of available subnets
- $2^{(\text{number of bits})}$ -2 = number of available subnets
- **Advantages of subnetting**

  1. Network traffic isolation – less traffic on each subnet
  2. Simplified administration
  3. Improved security

- Subnets can isolate internal networks from external networks

- **Supernetting**
  - Process of combining multiple networks into a single larger network
  - Also called as CIDR (Classless Inter-Domain Routing)
  - A lot of unused address spaces in classful addressing
  - Ex.
    - Class A has more than 16million host addresses
    - Class B has more than 65000 host addresses
    - But limited number of address space has been allocated for internet use
    - Class C has max 256 addresses
  - Midsize organization may need more addresses
  - Solution is supernetting – organization can combine several class C blocks.

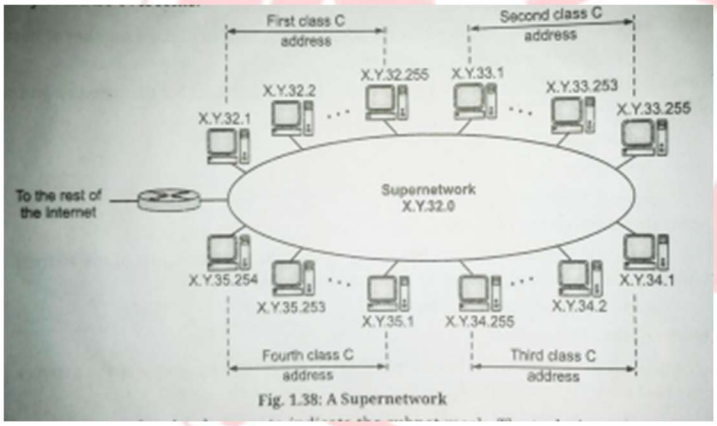


Fig. 1.38: A Supernetwork

  - **Supernet mask**
    - Reverse of subnet mask
    - For supernetting we need to know first address in the block and supernet mask

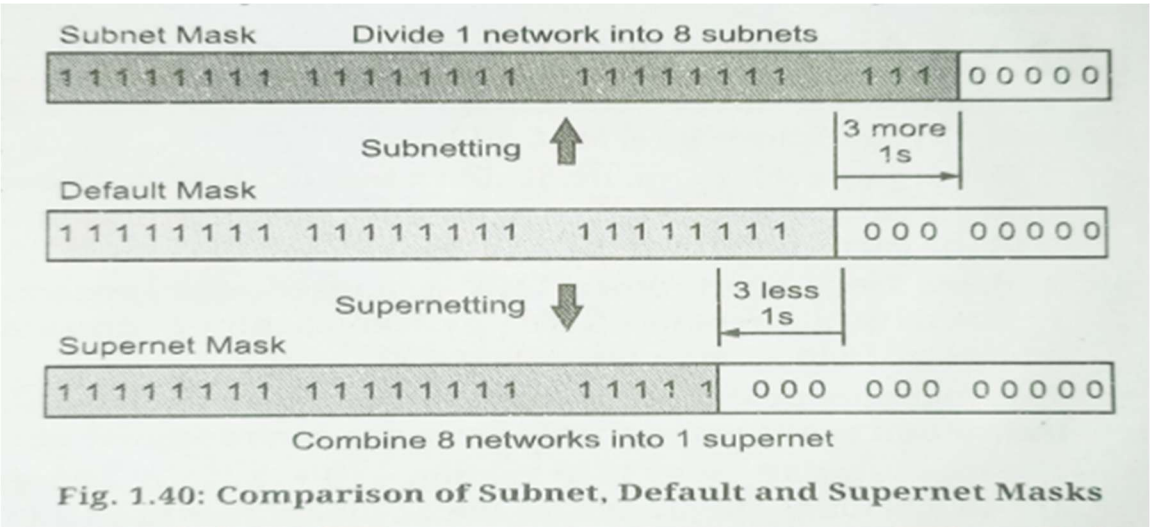


Fig. 1.40: Comparison of Subnet, Default and Supernet Masks

- **Address mapping**
  - It's a process of translating one type of address to another so that the devices can communicate efficiently across networks.
  - A packet starting from source host may pass through several different physical network before finally reaching the destination hosts
  - Host and routers are recognized at network level by their logical addresses (inter network address)
  - At physical level host and router are recognized by their physical address (local address)
- **ARP (Address Resolution Protocol)**
  - Used to convert logical address (IP address) to physical address (MAC- media access-controlled address)
  - It's a network layer protocol
  - This conversion is need because IP address and MAC address differ in length.
  - In IPv4 : IP address- 32 bits & MAC address- 48 bits
  - MAC address- data link layer (local address to router)
    - Establishes and terminates connection between 2 devices

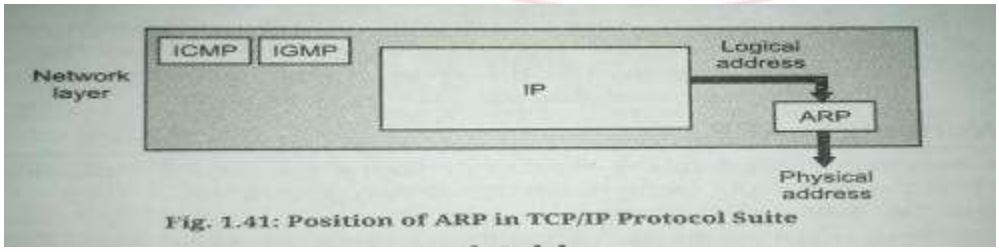


Fig. 1.41: Position of ARP in TCP/IP Protocol Suite

- **Mapping of IP address(Logical) to MAC address (physical)**
- 2 types:
    - Static mapping
        - Mapping table created and stored at each machine
        - Table helps associating both addresses
        - Mapping becomes difficult if MAC address changes
        - Changed MAC address must be updated periodically
    - Dynamic mapping
        - A protocol is used for finding other addresses
        - When one type of address is known
        - 2 protocols
            - ARP→ maps IP to MAC
            - RARP(Reserved Address Resolution Protocol)→ maps MAC to IP
- **Working of ARP→**

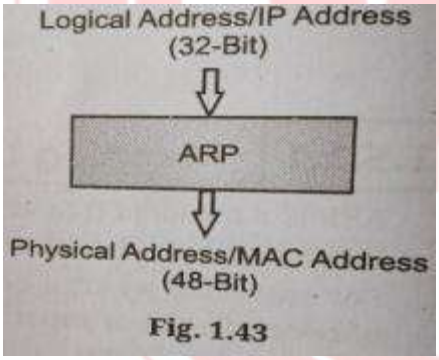


Fig. 1.43

- **Working of RARP→**

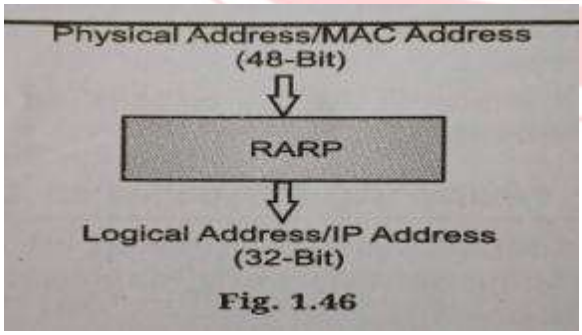
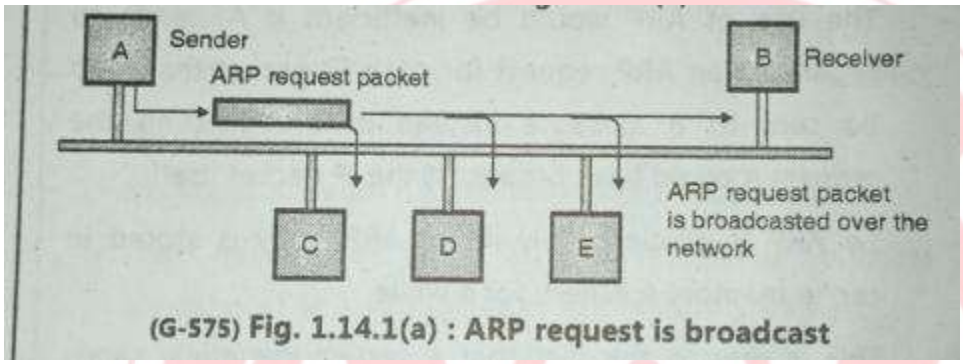
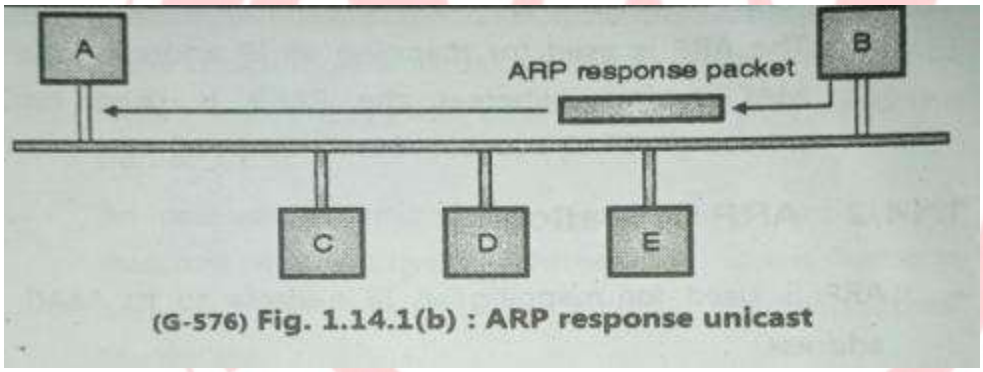


Fig. 1.46

- **ARP Operation:**
  - Finds MAC address
  - ARP request packet- contains IP and MAC address of A & IP address of B
  - Every host receives packet but only B responds
  - Response packet- contains IP and MAC address of B
  - Response is unicast



(G-575) Fig. 1.14.1(a) : ARP request is broadcast



(G-576) Fig. 1.14.1(b) : ARP response unicast

- **ARP Packet Format:**

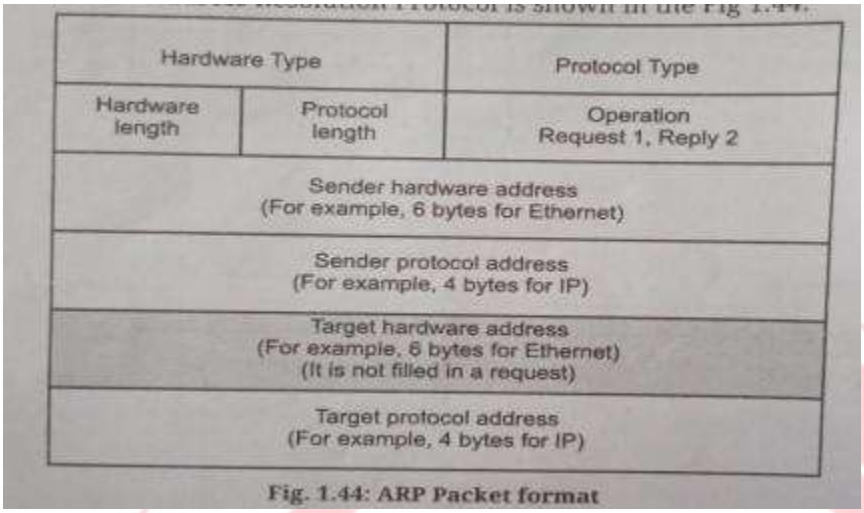
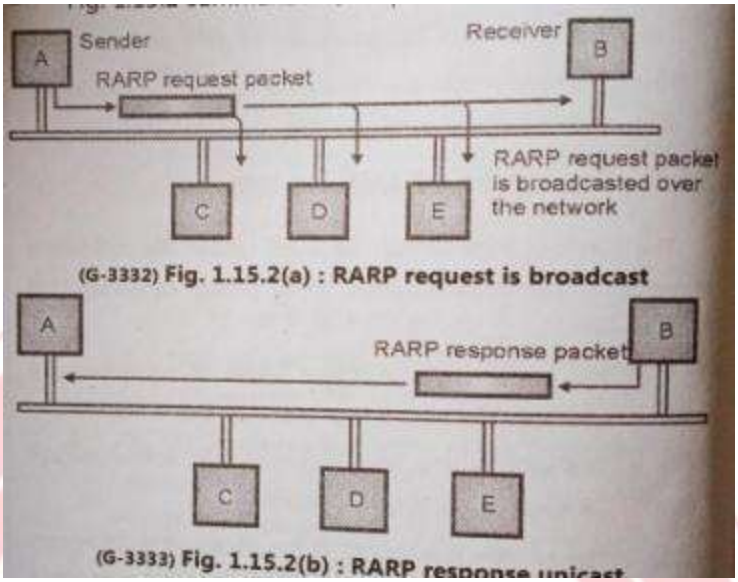


Fig. 1.44: ARP Packet format

- **Hardware Type(HTYPE):**
  - 16-bits field
  - Defines type of network on which ARP is running
  - ARP can be used on any physical network
- **Protocol Type(PTYPE):**
  - 16- bits field
  - Defines protocol using ARP
  - ARP can be used with any higher-level protocol like IPv4
- **Hardware Length(HLEN):**
  - 8-bit field
  - Defines length of physical address in bytes
  - E.g. value 6 is for Ethernet
- **Protocol Length(PLEN):**
  - 8-bits field
  - Defines length of logical address in bytes
  - Value is 4 for IPv4
- **Operation (OPER):**
  - 16-bits field
  - Defines type of packet
  - Request packet or reply packet

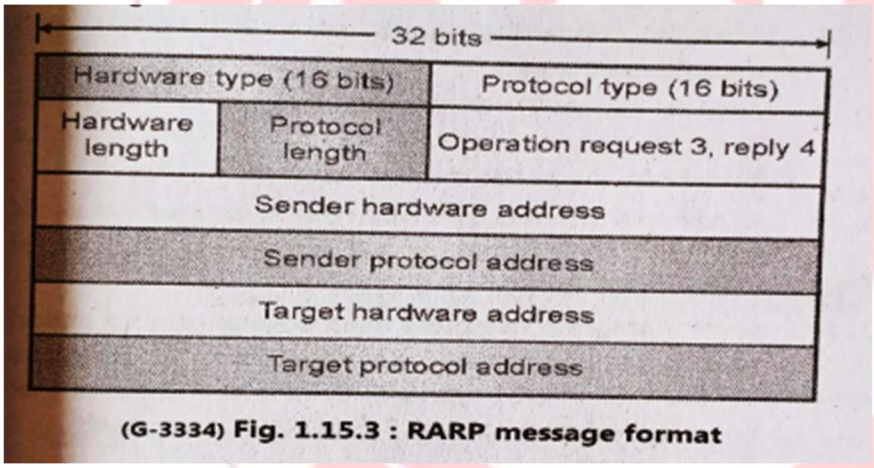
- **Sender Hardware Address(SHA):**
  - Variable length field
  - Defines physical address of sender
- **Sender Protocol Address(SPA):**
  - Variable length field
  - Defines logical address of sender
- **Target Hardware Address(THA):**
  - Variable length field
  - Defines physical address of target
  - Contains all 0's for ARP
  - As receivers physical address is not known
- **Target Protocol Address(TPA):**
  - Variable length field
  - Defines logical address of target
- **RARP(Reverse Address Resolution Protocol)**
  - Determines IP address using MAC address
  - Useful for diskless machines
  - Not having capability to store IP address
  - Newly booted workstation uses RARP



(G-3332) Fig. 1.15.2(a) : RARP request is broadcast

(G-3333) Fig. 1.15.2(b) : RARP response unicast

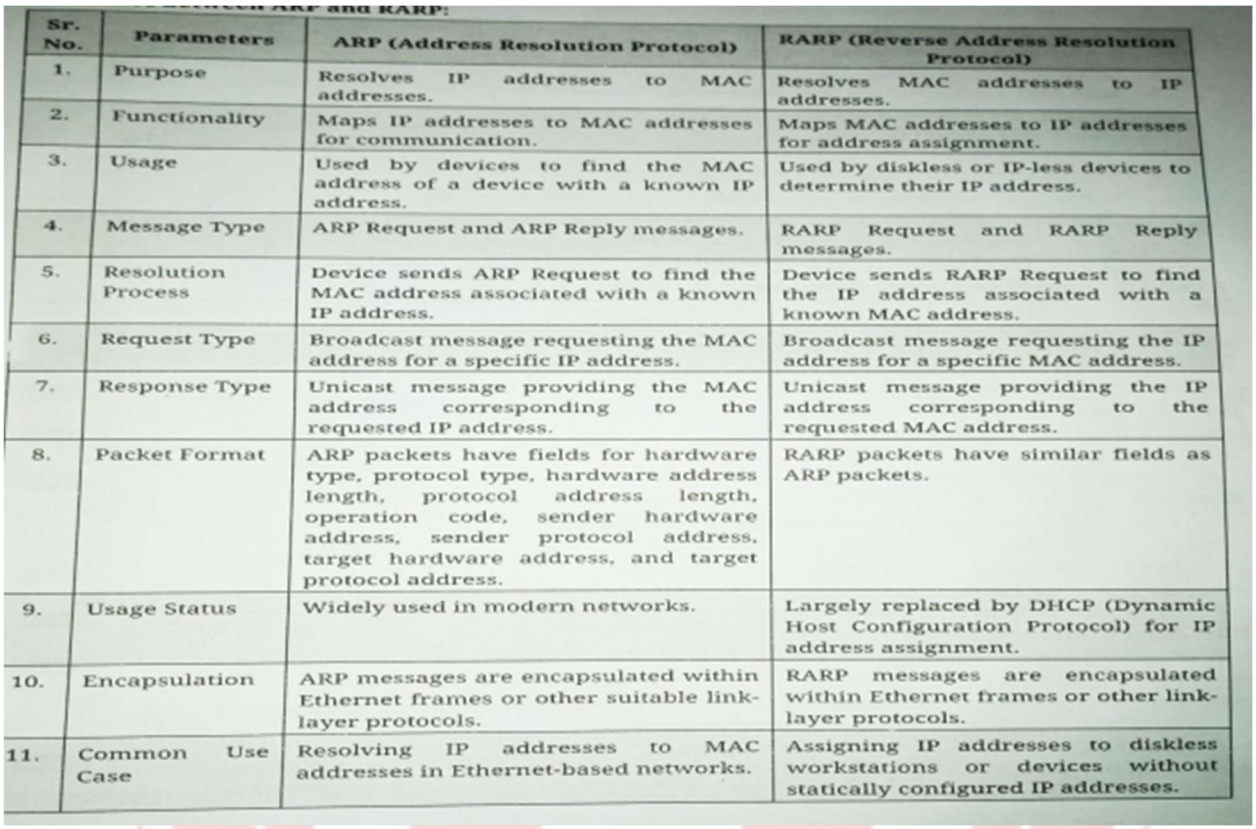
- **Operation of RARP→**
- **RARP packet format:**



(G-3334) Fig. 1.15.3 : RARP message format

- **Advantages of RARP**
  - Simplified device configuration
  - Reduced overhead
  - Prevention of IP conflict
  - Supports older devices that do not support modern protocol
- **Disadvantages of RARP**
  - RARP server must be within same physical network
  - Router can not forward the packet sent by RARP so communication beyond local network is not possible

- Can not handle networks with multiple subnets
- Not suitable for modern network



Sr. No.	Parameters	ARP (Address Resolution Protocol)	RARP (Reverse Address Resolution Protocol)
1.	Purpose	Resolves IP addresses to MAC addresses.	Resolves MAC addresses to IP addresses.
2.	Functionality	Maps IP addresses to MAC addresses for communication.	Maps MAC addresses to IP addresses for address assignment.
3.	Usage	Used by devices to find the MAC address of a device with a known IP address.	Used by diskless or IP-less devices to determine their IP address.
4.	Message Type	ARP Request and ARP Reply messages.	RARP Request and RARP Reply messages.
5.	Resolution Process	Device sends ARP Request to find the MAC address associated with a known IP address.	Device sends RARP Request to find the IP address associated with a known MAC address.
6.	Request Type	Broadcast message requesting the MAC address for a specific IP address.	Broadcast message requesting the IP address for a specific MAC address.
7.	Response Type	Unicast message providing the MAC address corresponding to the requested IP address.	Unicast message providing the IP address corresponding to the requested MAC address.
8.	Packet Format	ARP packets have fields for hardware type, protocol type, hardware address length, protocol address length, operation code, sender hardware address, sender protocol address, target hardware address, and target protocol address.	RARP packets have similar fields as ARP packets.
9.	Usage Status	Widely used in modern networks.	Largely replaced by DHCP (Dynamic Host Configuration Protocol) for IP address assignment.
10.	Encapsulation	ARP messages are encapsulated within Ethernet frames or other suitable link-layer protocols.	RARP messages are encapsulated within Ethernet frames or other link-layer protocols.
11.	Common Use Case	Resolving IP addresses to MAC addresses in Ethernet-based networks.	Assigning IP addresses to diskless workstations or devices without statically configured IP addresses.