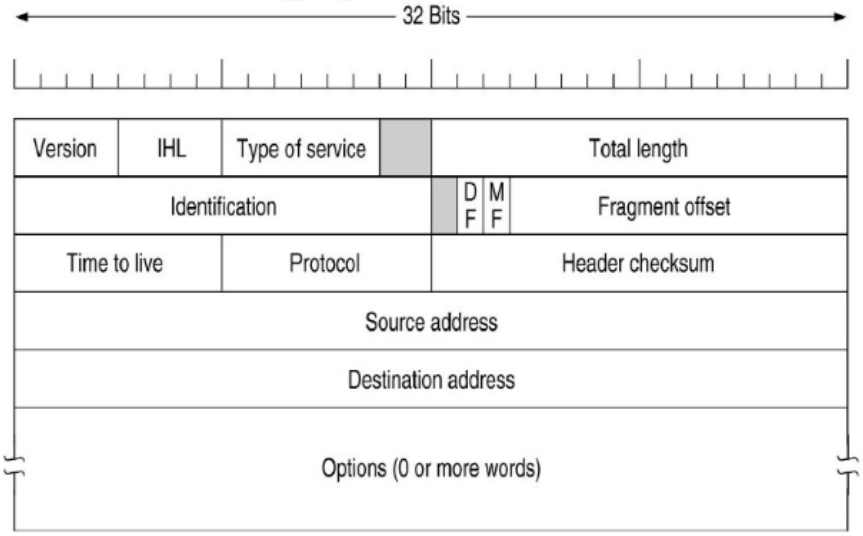
1. What is IP? Also give the frame format of IP?

- IP is a
  - Network layer protocol
  - Datagram oriented protocol
- Packets in IP layer are called datagrams. A datagram has 2 parts header & data

IP Header Structure :-

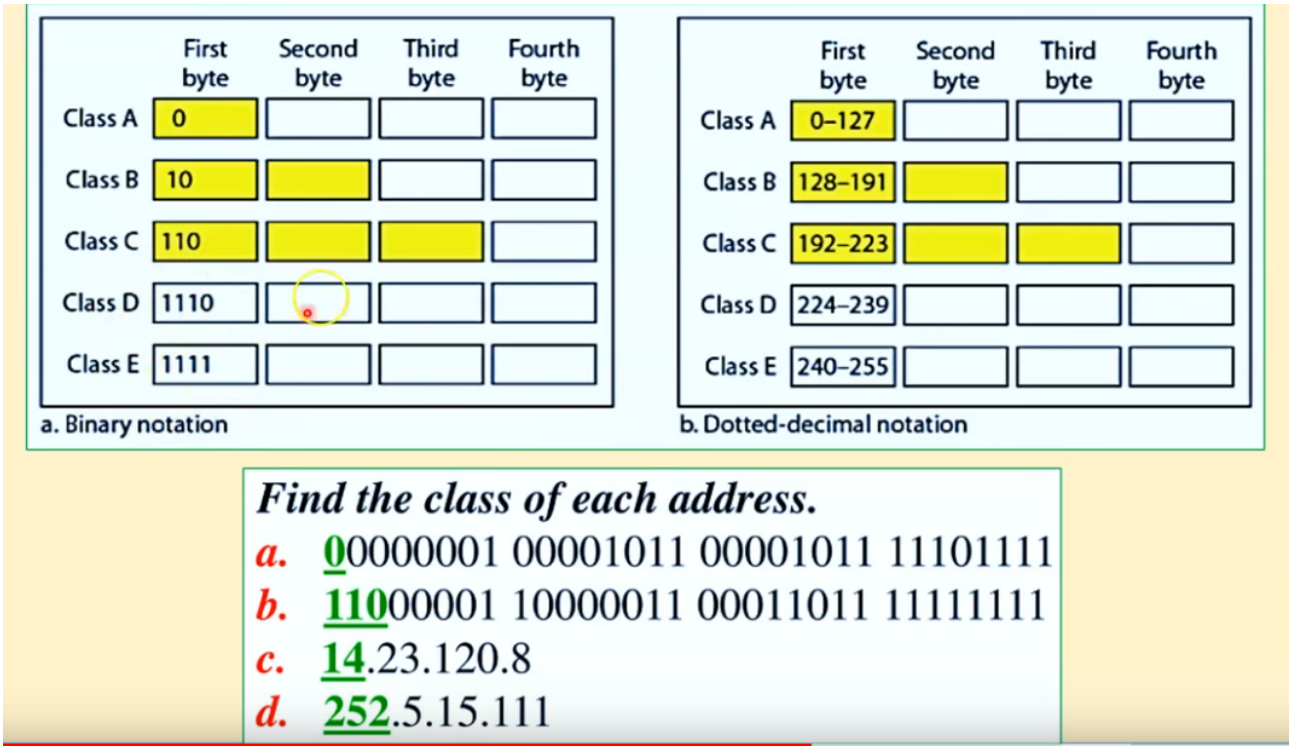


- The structure of IP consists of the following
- Version:
  - Defines the version of IP
  - 4 bit long field
  - IPV4,IPV6
- IHL (IP Header length):
  - Defines length of datagram header'
- Type of service field:
  - to distinguish between different classes of service
- Total length
  - Defines the total length of IP datagram
  - Length of header as well as data field
- Identification field
  - Identifies each datagram from others
- DF Stands for Do not Fragment
- MF Stands for More Fragments
- Fragment offset

    - Position of fragment w.r.t the whole datagram
    - Identifies the location of the fragment in a packet
- Time to Live
    - Age, lifetime
- Protocol
    - Defines the high level protocol
- checksum
    - to detect error
- Source address
- Destination address
- options

---

2. What is classful and classless addressing..?

- IPv4 addressing used the concept of classes.
- In classful addressing, the address space is divided into five classes:
    - A, B, C, D, and E.
- If the address is given in binary notation, the first few bits can immediately tell us the class of the address.
- If the address is given in decimal-dotted notation, the first byte defines the class
- 

- For example

- For the first question a)
  - First bit is 0
  - 0 means its of Class A
- 2nd Question b
  - First 3 bits are 110
  - Indicates Class C
- 3rd Question c
  - First number is 14
    - 14 Comes between 0-127
      - So its from Class A
- 4th Question d
  - First number is 252
    - 252 comes between 240 and 255
      - Its from class E

Netid and hostid

- Classes A,B and C are divided into Netid and Host id
- In the figure, the colored ones are Netid
- Uncolored ones are hostid
- This doesnt apply to classes D and E

Mask

❖ Mask

- The mask can help us to find the netid and the hostid.
- For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.
- A 32-bit number made of contiguous 1s followed by contiguous 0
- The concept does not apply to classes D and E

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

- This is similar to the colored and uncolored figure we saw earlier
- Colored ones are in 1's, uncolored ones are in 0's, Each slot is 8 bits

Classless Addressing

In classless addressing, the concept of fixed classes is abandoned. Instead, entities, whether small or large, are granted blocks or ranges of addresses based on their needs and size.

---

3. What is sub netting..?

- In networking, the concept of subnetting involves breaking down a large block of addresses that an organization has been granted into smaller, contiguous groups called subnets.
- Subnetting allows for better organization and management of IP addresses within a large network.
- Although the external world still sees the organization as a single entity, internally, it operates with several subnets.
- To manage this structure, the organization creates smaller subblocks of addresses, with each assigned to a specific subnet.
- Additionally, each subnet must have its own subnet mask to maintain internal communication and organization.

---

4. A network on the internet has a subnet mask of 255.255. 240.0. What is the maximum number of hosts it can handle..?

---

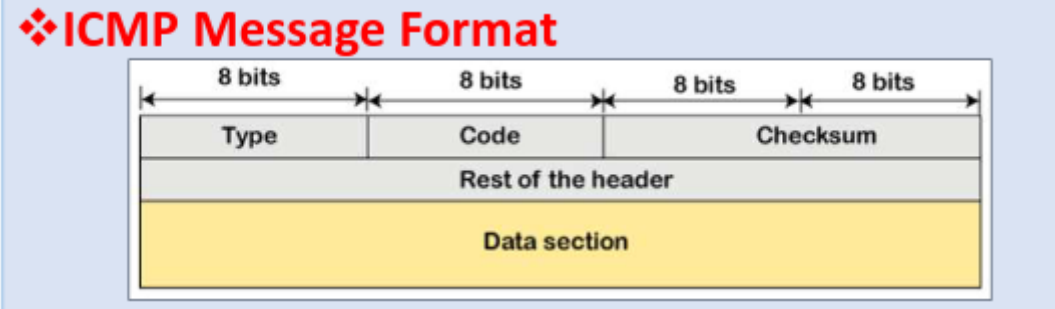
5. Discuss about internet control message protocol..?

- IP Does not have inbuilt mechanism for sending error and control messages
  - It depends on internet control message protocol (ICMP) for error control
- ICMP is used for reporting Errors and management queries
- used by networks devices like routers for sending error messages
- The ICMP resides in the IP layer

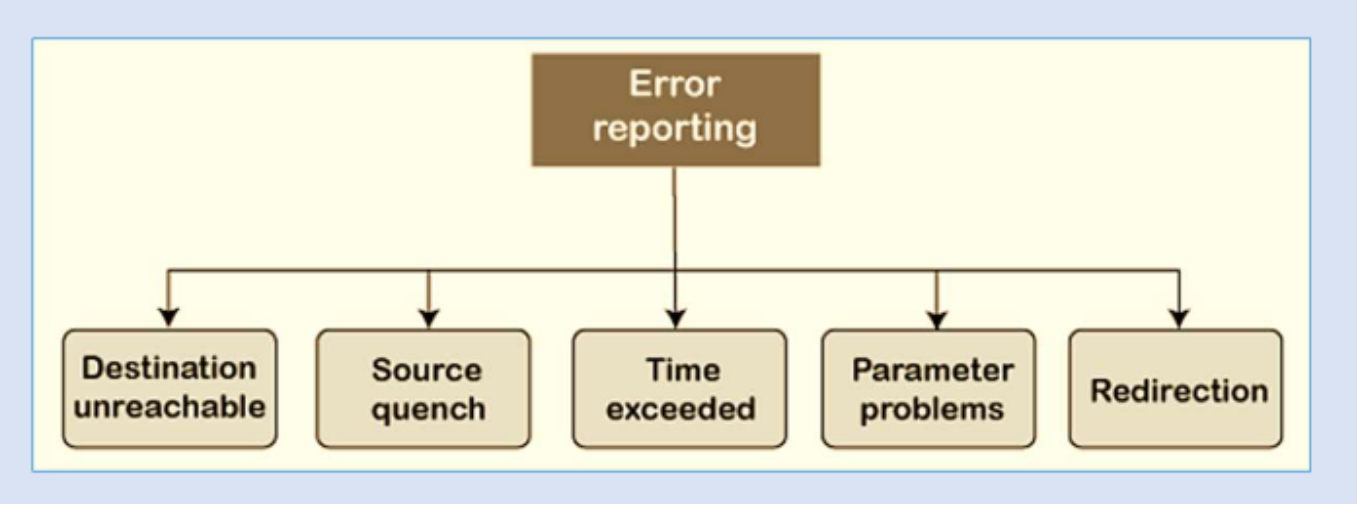
ICMP Message format

- Type
  - It is an 8-bit field. It defines the ICMP message type.
  - 0 to 127 are defined for ICMPv6
  - 128 to 255 are the informational messages
- Code
  - It is an 8-bit field that defines the subtype of the ICMP message
- Checksum
  -It is a 16-bit field to detect whether the error exists in the message or not

The ICMP protocol always reports the error messages to the original source.



Types of Error reporting messages



1. Destination unreachable
   1. Occurs when packet does not reach the destination
2. Source quench
   1. Request to decrease the traffic rate
   2. If the receiving host feels the rate of sending packets is too fast, it can do a source quench to the host to slow down so no packets are lost

3. Parameter problem
    1. When packet comes to router, the calculated header checksum should be equal to received header checksum, only then its accepted
4. Time exceeded
    1. Sometimes the situation arises when there are many routers that exist between the sender and the receiver.
    2. When the sender sends the packet, then it moves in a routing loop.
    3. The time exceeded is based on the time-to-live (TTL) value
    4. When the packet traverses through the router, then each router decreases the value of TTL by one.
    5. Whenever a router decreases a datagram with a time-to-live value to zero, then the router discards a datagram and sends the time exceeded message to the original source
5. Redirection
    1. When the packet is sent, then the routing table is gradually augmented and updated. The tool used to achieve this is the redirection message

ICMP Query Messages

Echo-request and echo-reply message

- A router or a host can send an echo-request message. It is used to ping a message to another host that "Are you alive"

Timestamp-request and timestamp-reply message

- Suppose the computer A wants to know the time on computer B, so it sends the timestamp-request message to computer B.
- The computer B responds with a timestamp-reply message

---

6. What is ARP.? Explain its working.

- Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address
- ARP provides a dynamic mapping from an IP address to the corresponding hardware address.
- When one host wants to communicate with another host on the network, it needs to resolve the IP address of each host to the host's hardware address

- This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet

Working of ARP

- When a host tries to interact with another host, an ARP request is initiated
- If the IP address is for the local network, the source host checks its ARP cache to find out the hardware address of the destination computer.
- If the correspondence hardware address is not found, ARP broadcasts the request to all the local hosts
- All hosts receive the broadcast and check their own IP address. If no match is discovered, the request is ignored
- The destination host that finds the matching IP address sends an ARP reply to the source host along with its hardware address, thus establishing the communication
- The ARP cache is then updated with the hardware address of the destination host

---

7. Define reverse Address Resolution Protocol. (RARP).?

- Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted.
- To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter.

Method

1. Source Device “Generates RARP Request Message”
2. Source Device “Broadcasts RARP Request Message”
3. Local Devices “Process RARP Request Message”
4. RARP Server Generates RARP Reply Message
5. RARP Server Sends RARP Reply Message
6. Source Device Processes RARP Reply Message

---

8. Write short note on BOOTP

- BOOTP is used to give IP addresses to each member of that network for participating with other networking devices by the main server
- BOOTP is used during the bootstrap process when the computer is initially starting up, hence the name.

Working of BOOTP

- broadcasts a message containing its MAC address onto the network
  - This message is called a “BOOTP request,”
- This request is picked up by the BOOTP server, which replies to the client with the following information that the client needs
  - client’s IP address, subnet mask, and default gateway address
  - IP address and host name of the BOOTP serve
  - The IP address of the server that has the boot image, which the client needs to load its operating system
- When the client receives this info
  - it configures and intializes TCP IP protocol
  - Connects to server where the boot image is stored
  - Loads the image and starts OS

Uses of BOOTP

- Used in diskless environment
- Transfer of data between client and server
- No external storage outside of cloudnetwork required

---

9. What is DHCP..? Discuss the DHCP header with diagram

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so they can communicate using IP (Internet Protocol)

Working

- Maintains unique address of IP address using a DHCP Server
- Sends a request to DHCP when a client configured to work with DHCP connects to a network

- Server acknowledges by providing an IP Address to client

Advantage

- Centralized management of IP addresses
- Reuse of IP address
- Ease of adding clients to network

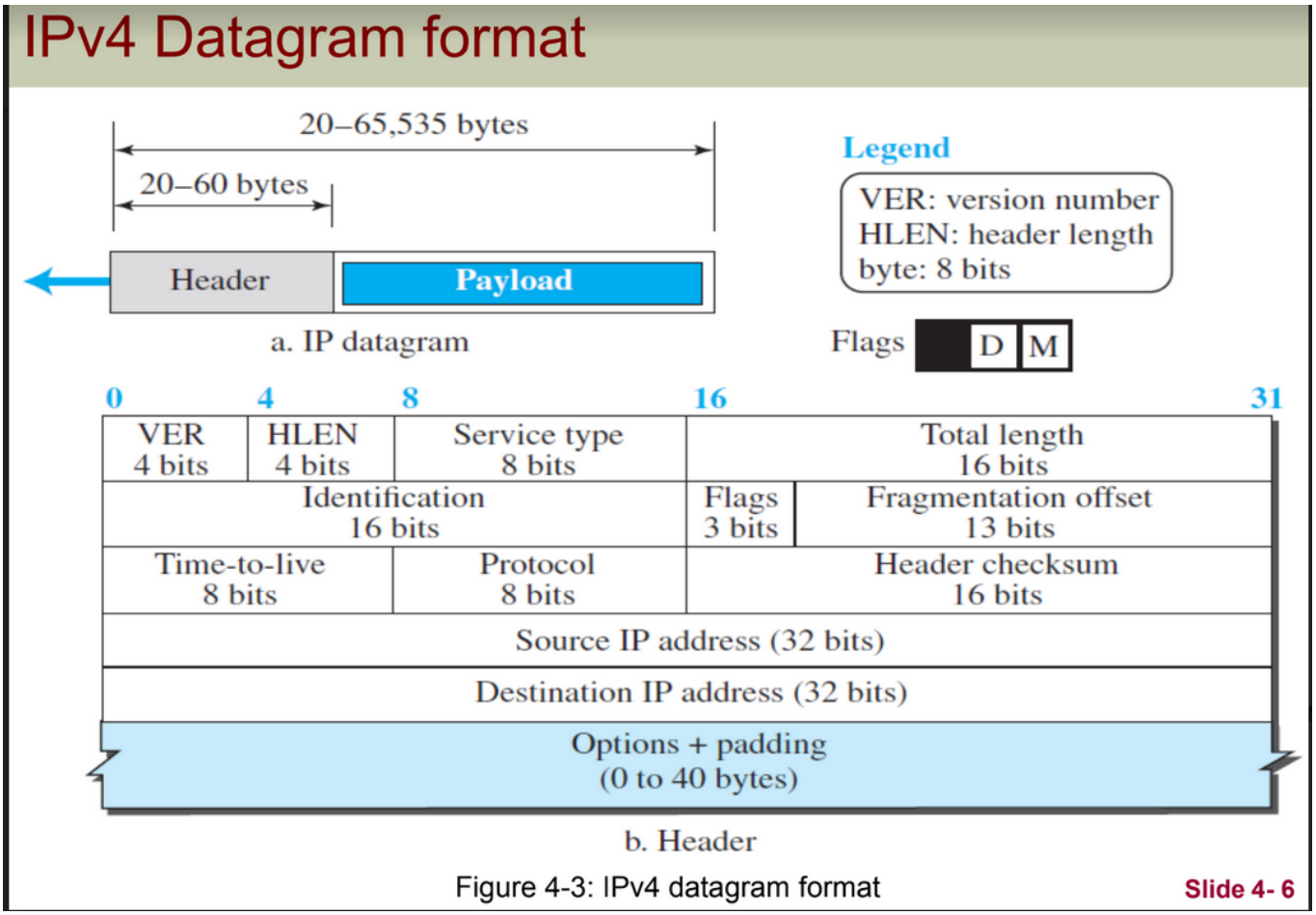
Disadvantage

- Ip Conflicts

---

10. Explain the IPV4 with its datagram format..?

- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device
- Two devices on the Internet can never have the same address at the same time
- IPv4 uses 32-bit addresses, which means that the address space is **2^32** or 4,294,967,296 (more than 4 billion). This means that, theoretically, more than 4 billion devices could be connected to the Internet.



- The IP Datagram has a header and payload
- VER -> Version Number
- HLEN -> HeaderLength
- Service Type
- Total length

---

11. Differentiate IPV4 and IPV6.

Comparison :- IPv4 & IPv6

IPv4	IPv6
32 bit address space	128 bit address space
Address Representation in decimal	In hexadecimal
2^{32}possible ways to represent address	2^{128}ways
Packet flow identification : not available	Available and uses flow label field in the header
Checksum Field :Available	Not available
Has 5 different classes of IP address	Does Not contain classes of IP address
End-to-end connection integrity: Unachievable	achievable
Security features: Security is dependent on application	IPsec is inbuilt in the IPv6 protocol
DHCP or manual configuration	Does not require DHCP or manual configuration
Header includes options	All optional data moved to IPv6 extension headers
Not Provide Encryption and Authentication	Provide Encryption and Authentication