

| Network mask | | IP Addressing | | |
|---------------|----------------------|---------------------|-----------------|----------------------------|
| unicasting | N | H | | Range |
| Class A :- | $0 \dots (2^7 - 2)$ | $(2^{24} - 2)$ | | 0 - 0111 client 1 - 126 |
| 255.0.0.0 | 8 bit | 24 bit | | 127 - LBA |
| unicasting | | | | |
| Class B :- | $10 \dots (2^{14})$ | $(2^{16} - 2) + 64$ | 12.8 - 191 | |
| 255.255.0.0 | 16 bit | 16 bit | | |
| unicasting | | | | |
| Class C :- | $110 \dots (2^{21})$ | $(2^8 - 2) + 32$ | 192 - 223 | |
| 255.255.255.0 | 24 bit | 8 bit | | |
| Multicasting | | | | |
| Class D :- | $1110 \dots$ | | +16 [224 - 239] | |
| Research | | | | |
| Class E :- | $1111 \dots$ | | +16 [240 - 255] | |

→ for Network ID all host bit will be 0.

→ for DBA, host bit with all 1.

| | |
|---------------------------|---------------------------------|
| 0 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 |
| 64 96 112 120 124 126 127 | 128 192 224 240 248 252 254 255 |

Private IP range :- { 10.0.0.0 - 10.255.255.255 , 172.16.0.0 - 172.31.255.255 }
 192.168.0.0 - 192.168.255.255 }

NAT Router :- NAT router convert private IP into public IP when packet is going out of network, same router convert public IP into private, when packet is coming inside the network.

→ A computer can have Multiple IP address at different Instances of time. **NOTE :-** This concept is Known as same mac multiple IP address at different Instances of the time.

→ A computer can have multiple MAC addresses to support fault tolerance. **NOTE :-** This concept is Known as Multiple MAC and same IP at different instances of time.

Subnet

Q1.) $IP_1 = 199.48.98.99$

Subnet Mask = $255.255.255.224$

i.) Subnet ID :- $224 = 111\ 00000$
 $99 = \begin{array}{r} 011\ 00011 \\ \hline 011\ 00000 \end{array}$

$= 199.48.98.96$

ii.) No. of Subnets = $(255.255.255.224)$ $\frac{S}{N} \frac{H}{H}$

[Subtracting 2 from No. of subnets. for Net ID and DBA of the Network]

bitwise AND

Subnet mask

$\frac{S}{N} \frac{H}{H}$

$\underline{\underline{2^3 - 2 = 6}}$

iii.) No. of Hosts in each subnet = $2^5 - 2 = \underline{\underline{30}}$

[Subtracting 2 from No. of Hosts. for subnet ID and DBA of that net]

$S\ H$

iv.) 1st subnet $9d = \underline{\underline{001\ 00000}} = 199.48.98.\underline{\underline{32}}$

v.) 2nd subnet $9d = \underline{\underline{010\ 00000}} = 199.48.98.\underline{\underline{64}}$

vi.) 3rd subnet $9d = \underline{\underline{011\ 00000}} = 199.48.98.\underline{\underline{96}}$

vii.) Last subnet $9d = \underline{\underline{110\ 00000}} = 199.48.98.\underline{\underline{192}}$.

NOTE - whenever there is a continuous mask, (there will be a pattern)

no need to calculate further subnet id, $(x+32)$ formula use to

calculate further subnet id. (continuous mask means $224 \underline{\underline{111\ 00000}}$)

viii.) 1st host of 1st Subnet = $\underline{\underline{001\ 00001}} = 199.48.98.\underline{\underline{33}}$

ix.) Subnet 9d of 1st Subnet = $\underline{\underline{001\ 00000}} = 199.48.98.\underline{\underline{32}}$

x.) DBA of 1st Subnet = $\underline{\underline{001\ 11111}} = 199.48.98.\underline{\underline{63}}$

x1.) Last host of 1st Subnet = $\underline{\underline{001\ 11110}} = 199.48.98.\underline{\underline{62}}$

x.) Net ID = $\underline{\underline{000\ 00000}} = 199.48.98.\underline{\underline{0}}$

x1.) DBA of network = $\underline{\underline{0111\ 11111}} = 199.48.98.\underline{\underline{255}}$

x2.) Last Subnet 9d = $\underline{\underline{110\ 00000}} \stackrel{\text{No. of subnets = 6.}}{=} 199.48.98.192.$

x3.) 4th host of 5th Subnet = $\underline{\underline{101\ 00100}} = 199.48.98.164.$

ex2) $IP_1 = 199 \cdot 88 \cdot 99 \cdot \underline{123}$ $IP_2 = 199 \cdot 88 \cdot 99 \cdot \underline{65}$ $IP_3 = 199 \cdot 88 \cdot 99 \cdot \underline{87}$

Subnet mask = $255 \cdot 255 \cdot 255 \cdot \underline{240}$.

Identify which host of which subnet they belongs to?

Ans.) $IP_1 \Rightarrow 0111 \quad 1011 \Rightarrow 11^{\text{th}} \text{ host } 7^{\text{th}} \text{ Subnet}$

$IP_2 \Rightarrow 0100 \quad 0001 \Rightarrow 1^{\text{st}} \text{ host of } 4^{\text{th}} \text{ Subnet}$

$IP_3 \Rightarrow 0101 \quad 0111 \Rightarrow 7^{\text{th}} \text{ host of } 5^{\text{th}} \text{ Subnet.}$

ex3) $IP_1 = 192 \cdot 98 \cdot 88 \cdot 141$ $IP_2 = 192 \cdot 98 \cdot 88 \cdot \underline{161}$ $IP_3 = 192 \cdot 98 \cdot 88 \cdot 151$

Subnet Mask = $255 \cdot 255 \cdot 255 \cdot \underline{240}$. Identify IP's belong to same subnet?

Ans.) $240 - \underline{1111 \ 0000} \quad 161 = \underline{1010 \ 0000}$

$141 - \underline{1000 \ 1101} \quad 151 = \underline{1001 \ --}$

NOTE:- If question asked for identify same subnet, check for subnet only, no need to find host.

ex4) $IP_1 = 200 \cdot 89 \cdot 99 \cdot 119$. Subnet Mask = $255 \cdot 255 \cdot 255 \cdot \underline{41}$. $\rightarrow \begin{array}{c} 00101001 \\ \downarrow \\ \text{Discontinuous mask.} \end{array}$

Ans.) Discontinuous mask is used in security because we cannot determine the values from standard equation.

NOTE:- $(x+32)$ formula cannot use for discontinuous mask.

ex5) D.B.A of subnet is given as $201 \cdot 55 \cdot 77 \cdot 31$, which of the following will be suitable subnet mask? $\rightarrow \begin{array}{c} 00011111 \\ \downarrow \\ \text{first subnet} \end{array}$

a.) $255 \cdot 255 \cdot 255 \cdot 192 - \underline{110000000}$

b.) $255 \cdot 255 \cdot 255 \cdot 128 - \underline{100000000}$

c.) $255 \cdot 255 \cdot 255 \cdot 240 - \underline{\begin{array}{r} 1111 \\ \downarrow \\ 0000 \end{array}}$

d.) None

minimum 4 digit subnet required

ex6) Company Go Hosts, subnet mask?

Ans.) No. of hosts = $2^6 - 2 = 62$

$N + S + H$

$24 + 2 + 6$

$255 \cdot 255 \cdot 255 \cdot 192$

$S = 2$

ARP = MAC

RARP = IP

LAN, MAC address

Networking Devices

1. Bridge - Not a Broadcast Domain separator.

- Collision Domain Separator.
- fault tolerant.
- Learning, Forwarding & Blocking.
- connect similar Network.

2. Router - WAN Device, operations based on IP Address.

- Connecting Dissimilar Networks.
- Broadcast Domain Separator.
- Collision Domain Separator.
- Not a Multiprotocol converter.
- Sophisticated device. (Host to Host addressing)

3. GATEWAY - Broadcast Domain Separator.

Collision Domain Separator.

Multiprotocol converter.

Highly sophisticated router.

4. Repeaters & Hubs - Not a Broadcast Domain Separator.

Not a Collision Domain Separator.

5.) Switches - It maintains a lookup table for forwarding the frames.

↓
(Datalink layer) Collision Domain Separator.

✓ ~~Not a Broadcast Domain Separator.~~

- IPv4 & IPv6:- By default IPv4 is a stateful protocol & IPv6 is a stateless protocol. IPv4 is slow compare to IPv6.
- IPv6 doesn't require ARP protocol because MAC address itself is a part of IPv6 address.
- By default IPv6 doesn't require DHCP server configuration.
- In IPv6, A computer can have multiple IP Addresses at the sametime.
- In IPv6, we don't need a NAT router because there is no need of translation from public IP to private IP or vice versa.
- By default, IPv6 doesn't require NAT configuration because from the origin point, it has the public IP address.
- IPv6 doesn't support broadcasting, it supports only Multicasting.
- IPv6 supports Anycasting i.e. All nodes will have the same address, but the service is provided by nearest node.
- for mobile Networks or wireless Networks - IPv6 is best suitable because of its stateless auto configuration.
- IPv6 doesn't require any mapping table for IP address to MAC address mapping.

"PING":-(Packet Internet gropher):- Ping command is used to troubleshoot in the network. It is used to test the reachability of the system in the network". ICMP protocol is used to implement "ping".

- Loop BACK ADDRESS:- It is used for troubleshooting the self computer whether the computer is properly connected to the port or not.
- LBA will never enter into the network.
- LBA will always be a Destination address only.
- Even a computer is not assigned any IP still we can troubleshoot the self computer by using- DHCP client and Loop Back Address.
- NOTE:- LPA is used as a address in the interprocess communication.

DHCP client:-

CIRCUIT SWITCHING

- Three phases:-
 - 1) Connection establishment
 - data transfer
 - connection release.

- Each data unit will have entire path address.

- Circuit Switching is not a store and forward technique. The packet simply bypass the queue of the router.

- The transmission of packet is done by the source.

- The delay between the data units is 'uniform' or same.

- Resource Reservation is a feature.

- wastage of resources are more.

- 'Congestion' can occur during connection establishment phase.

- It is not a fault tolerant technique because the packets can not be diverted via other paths if link are broken.

- Reliable, used for long messages.

- Circuit switching is slow.

PACKET SWITCHING

- Data can be transmitted directly • data transfer.

- Each data unit will have the destination address, the intermediate path is decided by Router.

- Packet switching is a 'store & forward' technique where the packets are stored, Algorithm is applied on the best path.

- The transmission of data is done not only by the source but also by intermediate routers.

- The delay between the data units is 'variable'.

- Resources are sharable.

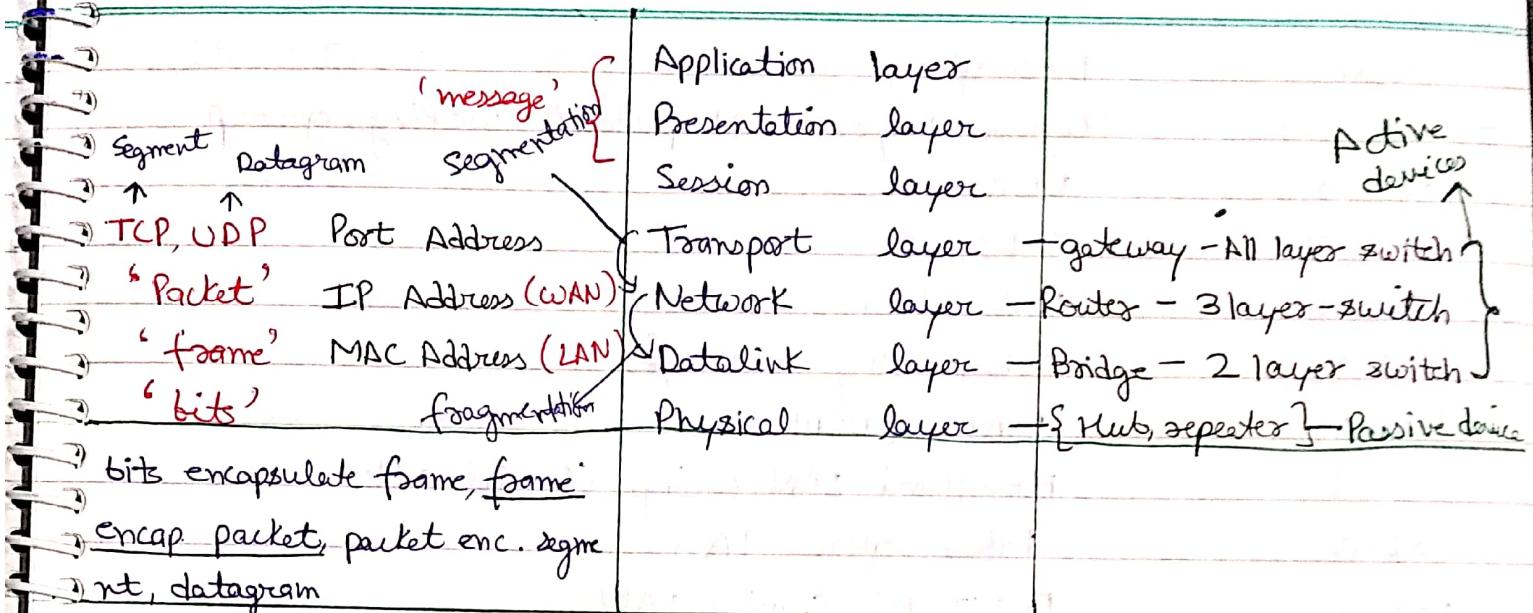
- wastage of resources is less.

- 'Congestion' can occur during data transfer phase.

- It is a fault tolerant technique because the data can be diverted via other paths if link are broken.

- Unreliable, used for short messages.

- Packet switching is fast.

OSI Model :-7 layers :-

- **Data link layer** :- is responsible for 'Node - to - Node' delivery within LAN.
- **Network layer** :- is responsible for 'Source to destination' delivery b/w net._{work}.
- **Transport layer** :- responsible for 'process to process' or 'End to End delivery', that can be identified by Port Address.
- **Combination of Port and IP address is Known as SOCKET ADDRESS.**
- **Network Architecture** is Known as protocol 'stack' Architecture.

SERVICES OF LAYERS:-

- **APPLICATION LAYER** :- Application services like HTTP, FTP, SMTP, DNS, Telnet.
- **Presentation layer** :- Syntax and Semantics of data.
- **Session layer** :- Dialog control, session Management.
- **Transport layer** :- flow control, error control, Segmentation, congestion policies.
- **Network layer** :- Routing algorithms, traffic shaping, fragmentation, IP addressing.
- **Data link layer** :- flow control, error control, Access control, framing.
- **Physical layer** :- Physical & electrical characteristics of cable.

| Name | Description |
|-------------------|--|
| <u>IEEE 802.1</u> | Higher layer LAN protocols working group |
| 802.2 | LLC |
| <u>802.3</u> | Ethernet |
| <u>802.4</u> | Token bus |
| <u>802.5</u> | Token ring MAC layer MANs (DQDB) |
| 802.6 | Broadband LAN using Coaxial cable |
| 802.7 | Fiber optic TAG |
| 802.9 | Integrated Services LAN |
| 802.10 | Interoperable LAN |
| <u>802.11</u> | Wireless LAN |
| 802.12 | 100BaseVG |
| 802.14 | Cable modems |
| <u>802.15</u> | Wireless PAN (Bluetooth) |
| <u>802.16</u> | Wireless MAN |

- TIME TO LIVE (8-bits): - The purpose of TTL is to identify, if any loop is exist for the packet, or not.
- whenever a packet is forwarded by a router, TTL value will be decremented.
- whenever the packet is in a loop, then at one point of time, TTL value will become 'zero' then the next router will drop the packet.
- ICMP will take the source IP from the Dropped packet and informs to source by sending Time exceeded message.
- whenever the link is broken, there is a chance, that packet might be forwarded in the wrong path.
- In practice, it is now a hopcount.
- It also guarantees that packet don't stay in the network for longer than 255 seconds.

ICMP (Internet Control Message Protocol):-

(i.) Source Quench Messages:- when more no. of packets coming in less time then the router buffer will be full in no time. that router is congested, then some packets are dropped.

→ ICMP protocol will take the source IP from the dropped packet and inform to source by sending 'Source Quench Message' then source will reduce the speed of transmission. then the congested router will be free from congestion.

→ If the congested router is far away from the source then ICMP will send, Hop-by-hop source quench messages then every router via the path will reduce the speed of transmission.

ii.) Parameter Problem:-

→ Once the data is transmitted, header bits are modified by the noise then the calculated header checksum will not be equal to received header checksum then the packets will be dropped.

→ ICMP will take the source-IP from the dropped packets & inform to the source by sending 'Parameter Problem' message.

iii.) Time Exceeded Message:- when some fragments are lost in the Networks. then the holding fragments will be dropped by the router.

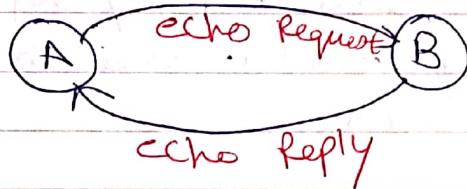
→ ICMP will take the source IP from the dropped fragment and informs to source by sending Time exceeded message.

iv.) Destination Unreachable:- ICMP Error messages are transmitting not only by the router but also by the destination host.

v.) Redirection Message :- whenever a packet is forwarded in a wrong direction, and later it is redirected in correct direction, then ICMP will send Redirection message to update with correct entries.

ICMP Query Messages:-

i.) Echo Request and Reply :- Designed for the diagnostic purpose. These messages are used to determine whether two systems can communicate with each other.



ii.) Time stamp Request & Reply :- Two machines uses these messages to determine the RTT needed for an IP datagram to travel b/w them.

TCP TIMERS :- Time out Timer, Time wait Timer, Keep Alive Timer, Persistent Timer.

1.) Time out Timer :-

TCP uses a time out Timer for retransmission of lost segments.

- Sender starts a time out timer after transmitting a TCP segment to the receiver.
- If sender receives an acknowledgement before the timer goes off, it stops the timer.
- If sender does not receives any acknowledgement and the timer goes off, then TCP Retransmission occurs.
- Sender retransmits the same segment and resets the timer.
- The value of time out timer is dynamic and changes with the amount of traffic in the network.
- Time out timer is also called as Retransmission Timer.

Time Wait Timer:-

TCP uses a time wait timer during connection termination.

- Sender starts the time wait timer after sending the ACK for the second FIN segment.
- It allows to resend the final acknowledgement if it gets lost.
- It prevents the just closed port from reopening again quickly to some other application.
- It ensures that all the segments heading towards the just closed port are discarded.
- The value of time wait timer is usually set to twice the lifetime of a TCP segment.

Keep Alive Timer -

TCP uses a keep alive timer to prevent long idle TCP connections.

- Each time server hears from the client, it resets the keep alive timer to 2 hours.
- If server does not hear from the client for 2 hours, it sends 10 probe segments to the client.
- These probe segments are sent at a gap of 75 seconds.
- If server receives no response after sending 10 probe segments, it assumes that the client is down.
- Then, server terminates the connection automatically.

Persistent Timer -

- TCP uses a persistent timer to deal with a zero-window-size deadlock situation.
- It keeps the window size information flowing even if the other end closes its receiver window.

5) acknowledgment timer

DNS - Port - 53
POP3 - Port - 110

TCP

1. Dynamic header (20-60) Bytes.
2. It is the connection oriented with the help of sequence no.
3. Flow Control.
4. Slow.
(Seq. no are waiting for all seq. to come and send in sequence.)
5. Checksum is mandatory.
6. Error Control.
7. It does not support Multicasting or broad casting.
8. HTTP, FTP, SMTP, Telnet.
9. Doesn't depend on ICMP protocol for error control.

UDP

1. Fixed Header 8 Bytes.
2. It is connectionless (no seq. no's)
3. Has No flow control
(each datagram is independent).
4. Fast (each datagram is independent & not waiting for another datagram to come).
5. checksum is optional.
6. UDP has no error control.
7. It supports Multicasting or Broadcasting.
(Link state)
8. TFTP, DNS, SNMP.
9. Depends on ICMP protocol.

FTP

- i) Downloading a large file.
- ii) Control Connection, Data Connection.
- iii) Ports 20, 21 are used

FTP

- 1.) TCP as Transport Layer.
- 2.) FTP has no flow control at A.L.
- 3.) FTP are Antivirus experts.
- 4.) FTP allows authorized user.
 - i) Internet.
 - ii) Downloading file.

TELNET

- i) chat operations (exchange of words)
- ii) common connection.
- iii) Port 23

TFTP

- 1.) UDP as Transport Layer.
- 2.) TFTP has flow control at A.L.
- 3.)
- 4.) TFTP allows Anonymous user.
 - i) Net access.
 - ii) Antivirus software.

APPLICATION LAYER

159

APPLICATION LAYER:-

"HTTP PROTOCOL":- (hypertext transfer protocol)

- (1) Client - server Protocol.
- (2) Synchronous Protocol.
- (3) Port 80.

→ It is a synchronous protocol because the clock of the client is synchronized with the clock of the server.

4) HTTP Connections :-

Persistent Http Connection.

Non-persistent Http connection.
stateless protocol.

Persistent HTTP:-

→ In case of persistent http, connection will be there only so we can access 'n' no. of objects.

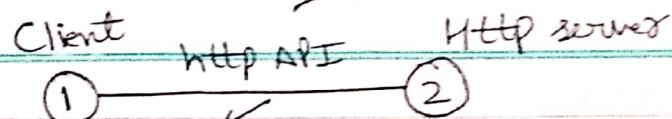
→ This is for user friendly requirement.

Non-Persistent HTTP:-

→ In Non-persistent http, for every individual object a separate connection should be established.

→ This is provided for security concern.

application Programming interface.



HTTP API:-

http methods :-

{ get() head() option()
post() connect() put()
Trace(). }

- 1.) Get Method :- It is used to retrieve the document.
- 2.) Put Method :- It is used to modify the existing document.
- 3.) Post Method :- It is used to place the modified document back to the directory in the server.
- 4.) Head Method :- Head Method is used to get the information about the document.
- 5.) Connect Method :- It is used data will go via a secure channel that to in encrypted form.
http https.
 Connect()
- 6.) Trace Method :- Trace & option() both work like a record root in IP.

NOTE :- By default IPv6 is stateless but we can make it stateful with the help of DHCPv6 server.

HTTP is a **stateless protocol** because client will not store any information about the server once the transaction has been done.

Cookies :- Cookies is a piece of code that is transmitted by a server or a mediating agency to the client Browser.

→ The Advantage of Cookies is :-

- (i.) Authorization
- (ii.) faster response.

File Transfer Protocol :- (FTP)

- 1) Downloading a file.
- 2) Client - Server Protocol.

- FTP will send control commands on port 21 via a control connection.
- Once the file is about to download, a separate data connection is established on port 20.
- Once the file is completely downloaded, data connection is closed, but control connection will remain to download.

SMTP (Simple Mail Transfer Protocol) :-

Multimedia internet mail
→ Extension.

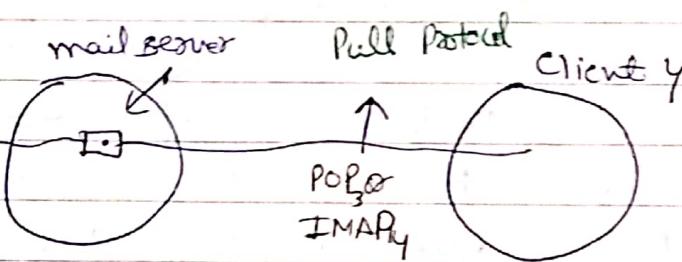
- 1) Text-based Protocol :- Internet → MIME Extension

SMTP is a text based protocol, but we can send graphical data, with the help of MIME Extension, which is provided by Internet Browsers.

- 2) Port - 25

- 3) TCP as T.L.

- 4) Client X
- SMTP
- Push Protocol



Pop: Post office Protocol

- SMTP is a Push Protocol, because it is used for sending mail to mail server.
- POP3 or IMAP4 are Pull Protocol because they are used for retrieving the mail from mail server.

- SMTP combined with POP3 or IMAP4 is a client to client protocol with a mediation done by mail servers.

- SMTP with POP3 is applying store & forward technique.

NOTE: The transfer of mail from one mail server to other mail server will be done by SMTP protocol.

→ Mails can be kept in hierarchy in case of IMAP4, whereas all mails are equal or serial in case of POP3.

→ Security to the mails or attachments are provided by the IMAP4, but not by POP3.

IPV4 Header

| Header | | Data | |
|-------------------------------|--------------------|--------------------------|-------------------------|
| ← 20-60 bytes → | | | |
| VER 4 bit | HLEN 4 bits | Service 8 bits | Total length 16 bits |
| Identification 16 bits | D F | M F | Fragment offset 13 |
| Time to live 8 bits | Protocol 8 bits | Header check sum 16 bits | |
| SOURCE IP Address 32 bit | | | |
| DESTINATION IP Address 32 bit | | | |
| OPTION & 32 bit | | | |
| PADDING | | | |

IPV6

65535 bytes

| Base Header | | Data | |
|-----------------------------------|---|------------------------|--|
| ← 40 bytes → | | [0 → 2 ³²] | |
| VER 4 bits | Priority (traffic class) 8 bit value | Flow Label 20 bits | |
| Pay Load Length 16 bits | Next Header 8 bits | Hop limit 8 bits | |
| Source IP 128 bits (32×4) | | | |
| Destination IP 128 bits (32×4) | | | |

TCP Datagram format

| TCP Header | | Data | |
|-----------------------------|----------------------|------|----------------|
| ← 20-60 bytes → | | | |
| Source Port(16) | Destination Port(16) | | |
| Sequence Number 32 | | | |
| Acknowledgement Number 32 | | | |
| hlen 4 | S C I S P R F T | X Y | Window Size 16 |
| N K N H G I | I S P S T | Y Y | |
| Checksum 16bit | Urgent Pointer 16bit | | |
| Padding + option (40 bytes) | | | |

UDP PROTOCOL

| UDP Header | | Data |
|------------------------------|-----------------------------------|------|
| ← 8 bytes → | | |
| Source Port Number (16 bits) | Destination Port Number (16 bits) | |
| Length (UDP+Data) 16 bits | UDP checksum 16 bit | |
| Application Data (Message) | | |

- DNS : TCP/UDP Port 53
- HTTP : TCP Port 80.
- SMTP : TCP Port 25
- POP : UDP Port 110
- Telnet : TCP Port 23
- Dynamic Host Configuration Protocol : UDP Port 67
- FTP : TCP Ports 20 and 21.

ARP - MAC
RARP - IP

163

- Listen(): Used on server side, cause a bound TCP socket to enter listening state.
- Bind(): Associates a socket with socket address structure.
- Connect(): It assigns a free local port number to a socket. In case of TCP socket, it causes an attempt to establish a new TCP connection.
- Accept(): Accepts a received incoming attempt to create a new TCP connection from the remote client.