1)

Layer	Name	PDU
7	Application	Data
6	Presentation	
5	Session	
4	Transport	Segment
3	Network	Packet
2	Datalink Layer	Frame
1	Physical Layer	Bits

=> Application Layer:-

(i) closest to the user, it provides services like email, web browsing & file transfer.

(ii) It interacts directly with software application to implement communication components.

=> Presentation Layer:-

(i) Translates data between application and network formats (like encryption, encoding).

(ii) Ensures data from the sender is readable by the receiver.

=> Session Layer:-

(i) Establishes, maintains & terminates communication sessions between devices.

(ii) It keeps track of dialogs and ensures proper data synchronization.

=> Transport Layer:

(i) Ensures reliable data transfer with error recovery & flow control (e.g; TCP, UDP)

(ii) It breaks data into segments and reassembles them at the receiver's end.

=> Network Layer:

(i) Handles logical addressing (i.e; IP address) & determines the best path for data to travel.

(ii) It manages packet forwarding and routing between devices on different networks.

=> Data Link Layer:

(i) Responsible for reliable node-to-node data transfer and error detection/correction.

(ii) It also handles framing & controls how data is placed on the physical medium.

=> Physical Layer:

(i) Deals with the actual transmission of raw bits over the physical medium (eg- cables, radio signals).

(ii) It defines hardware elements like cables, connectors, voltage levels & data rates.

2)

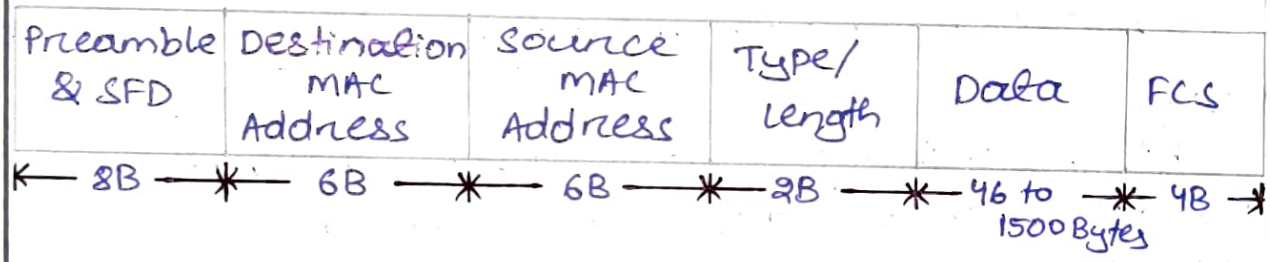
OSI Model	TCP/IP Model
(i) It has 7 layers, each with a clear & separate function.	(i) It has 4 layers and is more practical and implementation-oriented.
(ii) It is more theoretical and mainly used for understanding how networks work.	(ii) used widely in real-world networks like the internet & office LANs.

For setting up a computer network in an office, the TCP/IP model is more appropriate since it's practically used, faster to implement & compatible with modern networking devices.

3)

Physical Address	Logical Address
(i) It is the hardware address (MAC address) permanently assigned to a device's NIC.	(i) It is the IP address assigned to identify a device logically on a network.
(ii) used for communication within the same local network (LAN).	(ii) used for communication across different networks.
(iii) Associated with the Data Link layer of the OSI model.	(iii) Associated with the network layer of the OSI model.

4)



=> Preamble & SFD:

(i) The preamble is made up of 7 Bytes & SFD is 1 Byte in size.

(ii) This field is used to indicate start of the frame to the receiver.

=> Destination MAC Address:

This field is 48 bits (6 Bytes) in length and it contains layer 2 physical address of the receiver.

⇒ Source MAC Address:
This field is 48 bits (6 Bytes) in length and it contains layer 2 physical address of the sender.

⇒ Type/Length:
This field is 2 Bytes in length. It is used to identify the upper layer protocol (IPV4, IPv6) that is encapsulated within the frame.

⇒ Data:
(i) The data field range 46 to 1500 Bytes and contain the raw data from the application layer of the networking model.

(ii) The minimum length is 64 Bytes & if the frame less than 64 Bytes additional bits known as the pad are inserted to increase the size of the frame to the minimum length.

⇒ FCS:
This field is made up of 4 bytes in length and used to verify the intigrity of a frame and direct errors.

5) There are 65536 service ports (0-65535) available in the transport layer.
These ports are divided into three main category:

(i) well-known ports (0-1023):
used for standard devices or services like HTTP(80), FTP(21), & DNS(53).

(ii) Registered ports (1024-49151):
Assigned to specific user applications or software by IANA.

(iii) Dynamic or private ports (49152-65535):
used for temporary or client-side communication, choosen dynamically by the OS.

6) => Senden side:

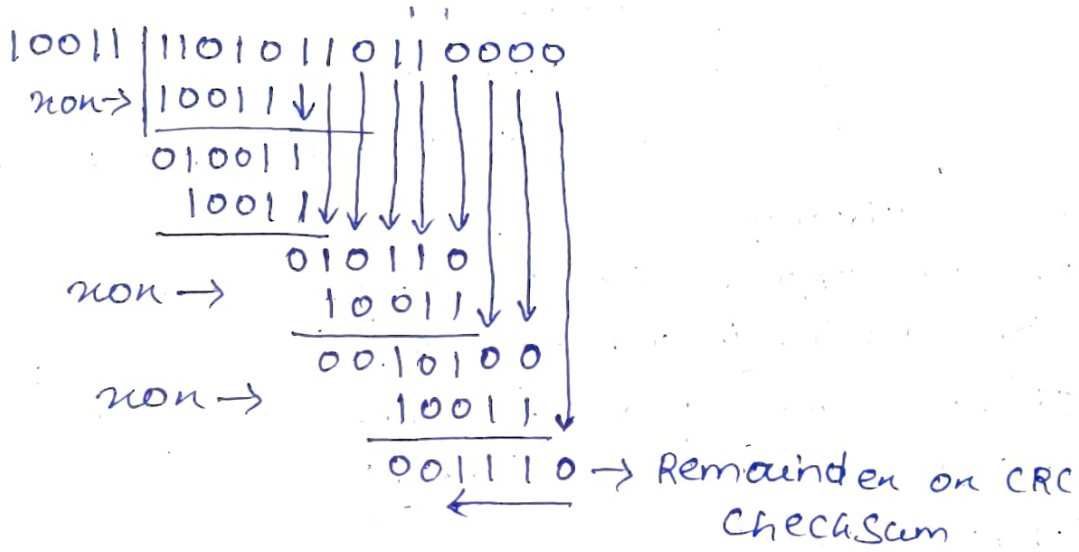
Let message (m):

$m(x) = 11010110 11$

$G(x) = x^4 + x + 1 = 10011$

Highest degree of $G(x) = 4$

So, $m(x) = 11010110110000$



11010110111110

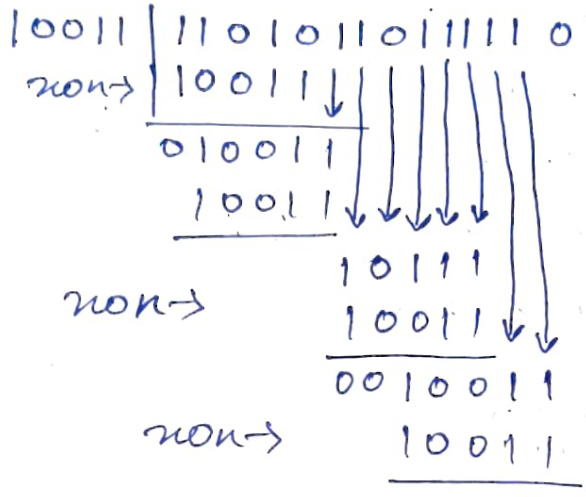
Senden → Receiver

(m(x) + CRC)

=> Receiver Side:

M(x) = 11010110111110

G(x) = 10011



(Errror-free Headen)

7) Network Topology:

(i) The arrangement or layout of computers, cables and devices in a network.

(ii) It shows how devices are connected and how data flows between them.

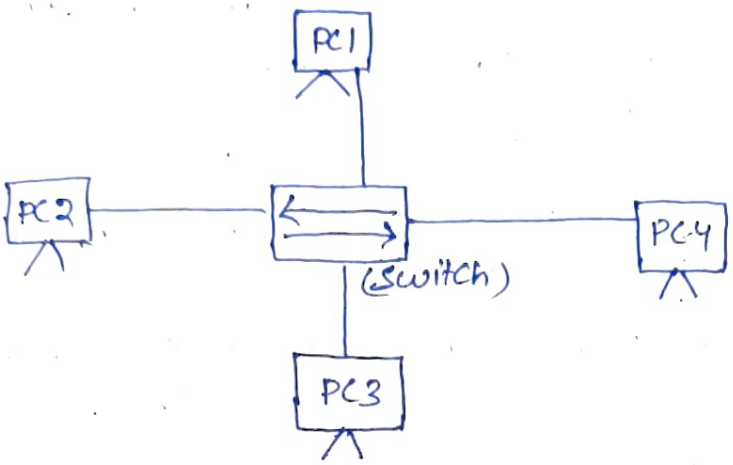
=> Physical Topology:

(i) It shows the actual physical layout of devices and cables (e.g: star, bus or ring).

(ii) Focuses on hardware connections and network structure.

(iii) In a star topology, all computers are connected through a central switch.

=> Diagram of star topology:



=> Logical Topology:

(i) It defines how data moves within the network, regardless of physical layout.

(ii) Focuses on data flow and communication paths between nodes.

(iii) Even in a star setup, data may flow like a bus topology logically.

=> Diagram of bus topology:

8) => Mesh Topology:

(i) Every device is connected to every other device.

(ii) Number of links = $\frac{n(n-1)}{2}$

$= \frac{6(6-1)}{2}$

$= 15$ links

=> Bus topology:

(i) All devices share a single common backbone cable.

(ii) Number of links = 1 main cable

=> Ring Topology:

(i) Each device connects to two neighboring devices forming a closed loop.

(ii) Number of links = 6 links (equal to number of devices).

=> Star Topology:

(i) All devices connect to a central hub or switch.

(ii) Number of links = n = 6 links.

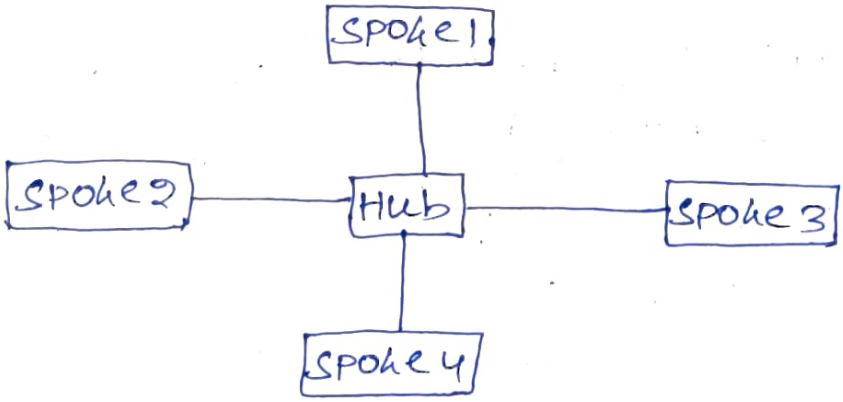
9) Hub & spoke Topology:-

(i) In this topology, there is a central hub (main node) connected to multiple spoke nodes (branch nodes).

(ii) All communication between spokes happens through the central hub only.

(iii) It is commonly used in WANs where branch offices connect to a central head office.

=> Diagram:



=> Similarities with star topology:

(i) Both have a central device that controls communication.

(ii) Easy to add or remove nodes without disturbing the whole network.

=> Differences from star topology:

(i) Star is mostly used in LANs, while Hub and Spoke is used in WANs.

(ii) In Hub & Spoke, the hub connects different network locations, not just local devices.

10) Advantages of fibre optic cable over copper cable:

(i) Higher Bandwidth:

Fiber optics can carry much more data than copper cables.

(ii) Faster Speed:

Data travels as light signals, giving very high transmission speed.

(iii) Longer Distance:

Signals can travel several kilometers without loss or amplification.

(iv) Less Interference:

Immune to electromagnetic interference (EMI) unlike copper wires.

(v) Better Security:

Difficult to tap or hack, making it more secure for data transmission.

11)

Shielded Twisted Pair (STP)	Unshielded Twisted pair (UTP)
(i) Has an extra metallic shield (foil or braided mesh) around the twisted wires.	(i) NO extra shielding, only pairs insulated copper wires twisted together.
(ii) Provides better protection against electromagnetic interference (EMI).	(ii) Less protection from EMI but suitable for office and home networks.
(iii) Slightly costlier and thicker, used in noisy industrial environments.	(iii) Cheaper, light and easier to install compared to STP.
(iv) Grounding is required for proper functioning to avoid signal distortion.	(iv) Does not need grounding; which makes installation simpler.

12) Refractive Index of the core optical fibre $n1 = 1.48$
cladding $n2 = 1.40$.

(a) Yes, the optical fibre satisfies the necessary condition for light transmission because
$n_1 > n_2$ $(1.48 > 1.40)$

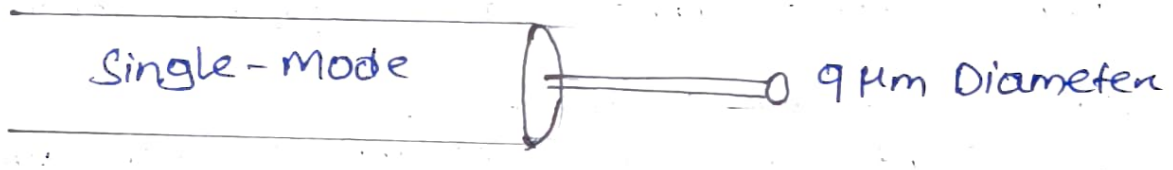
(b) Total Internal Reflection (TIR)

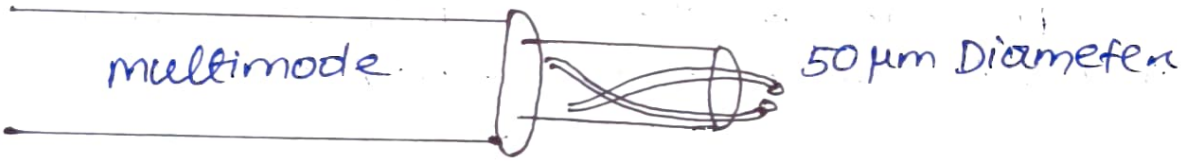
condition:

Light will be guided through the fibre core only if the refractive index of the core (n_1) is greater than that of the cladding (n_2) i.e. $n_1 > n_2$

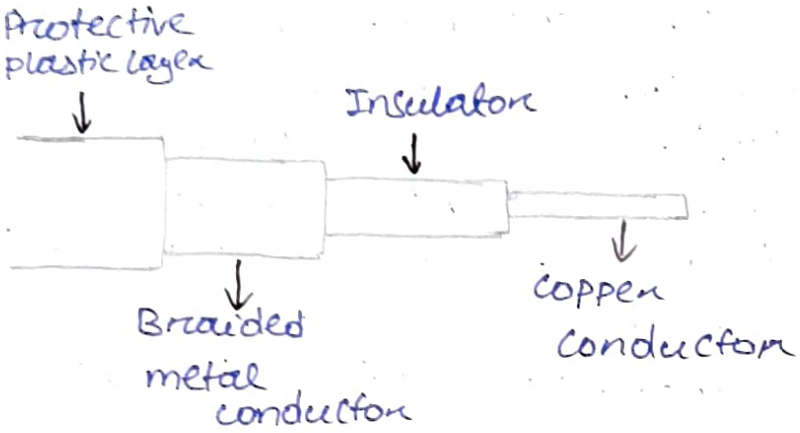
13)

Feature	Single Mode Fiber (SMF)	Multi Mode Fiber (MMF)
Core diameter	Very small (about 8 - 10 μm).	Larger (about 50 - 62.5 μm).
Light path	Allows only one light mode to propagate.	Allows multiple light modes to propagate.
Distance	Suitable for long-distance transmission.	used for short-distance communication.
Data Rate	Higher bandwith and speed.	Lower bandwidth due to modal dispersion.
Light source	uses laser diode	uses LED
cost	more expensive	Cheaper & easier to install.





14)



=> Copper conductor:
Made of copper; carries the actual electrical signal.

=> Insulator:
Separates the inner conductor from the outer shield and maintains signal integrity.

=> Braided metal conductor:
prevents electromagnetic interference (EMI) and signal leakage.

=> protective plastic layer:-
provides mechanical protection and insulation from external damage.

15)

Feature	Private IP Address	Public IP Address
usage	used within local networks (e.g. homes, schools, offices)	used on the internet for global communication.
Access	Not routable on the Internet; only works inside LAN.	Routable on the Internet; unique globally.
cost	Free to use; no registration needed.	Purchased/assigned by ISPs or organisations.
Example	192.168.10.1, 10.10.10.1, 172.16.25.2, 172.31.22.3	8.8.8.8, 142.250.183.110

=> How Private Address space solves classful Addressing Limitation:-

(i) In classful addressing, many IPs were wasted because organizations had to use large fixed blocks (Class A, B or C).

(ii) private IP ranges allow reusing the same addresses in different local networks without conflict.

(iii) It reduces wastage and, with NAT (Network Address Translation), multiple private devices can share one public IP for Internet Access.

16) Fields modified in the IP Header by NAT:-

=> Source IP Address:-

(i) Changed from the private IP of the internal device to the public IP of the NAT device.

(ii) It is needed so that the packet can be routed correctly on the Internet, since private IPs are not globally valid.

=> Checksum (Header checksum):
Modified because the IP address change alters the header's binary data, so a new checksum must be calculated to maintain integrity.

=> These modifications are necessary because:
(i) NAT translation allows multiple internal devices to share a single public IP, conserving IP addresses.

(ii) It ensures proper communication between private networks and external public networks by making packets routable on the internet.

17) Dynamic NAT allocation:

PC2 (10.7.7.62) → 55.4.4.1 (first free public IP assigned)

PC4 (10.7.7.64) → 55.4.4.2 (next free public IP assigned)

PC1 (10.7.7.61) → 55.4.4.3 (last free public IP assigned)

PC3 (10.7.7.63) → No public IP available (Pool exhausted)

So, PC3's translation is denied/queued until one of the existing mappings (PC2/PC4/PC1) times out or is released.

18) => Port Address Translation:

(i) PAT is an extension of NAT that allows multiple private devices to share a single public IP address.

(ii) It does this by using different port numbers to identify the each internal connection uniquely.

(iii) PAT is also called NAT overload because many internal IPs can map to one external IP.

=> How PAT works:

When several devices from a private network access the internet, PAT assigns the same public IP, but gives each device a unique port number.

eg:

10.0.0.2 : 1025 ⟶ 55.4.4.1 : 4001

10.0.0.3 : 1026 ⟶ 55.4.4.1 : 4002

10.0.0.4 : 1027 ⟶ 55.4.4.1 : 4003

Here, all devices use the same public IP (55.4.4.1) but have different port mappings.

=> Port mapping concept:

(i) Port mapping keeps a translation table that links each internal IP and port to a unique external port.

(ii) When responses come back from the internet, the router uses this table to route data to the correct internal device.

19) 100.50.25.10 → valid IP address belongs to class A

200.250.300.10 → Invalid IP address (because 300>255, not allowed in IPv4).

20) 2001:0db8:0000:0000:0001:0000:0000:0001

Routing prefix (48 bits):

2001:0db8:0000::/48

Subnet ID (16 bits):

0000

Interface ID (64 bits):

0001:0000:0000:0001

21) IPv6 uses ICMPv6 messages for address configuration & network discovery.

There are 2 important message types:

(i) RS (Router Solication message):

Sent by a newly connected host (end device) to request network configuration information from routers.

ICMPv6 type = 133

(ii) RA (Router Advertisement message):

Sent by routers to advertise their presence and provide IPv6 network parameters.

ICMPv6 type = 134

=> How a newly connected device obtains an IPv6 Address using RA.

(i) Device joins network → sends RS

The new device (host) broadcasts an RS message to discover nereby routers.

(ii) Router replies → sends RA

The router responds with an RA message containing:-

(a) The network prefix (i.e. 2001:db8:acad:1::/64)

(b) other configuration parameters.

(iii) HOST forms its IPv6 address:-

Using SLAAC (Stateless Address configuration)

IPv6 Address = Prefix (from RA) + Interface ID (derived from MAC Address or random value)

eg:

Prefix: 2001:db8:acad:1::/64

Interface ID: ::abcd:ef12:3456

Final IPv6:

2001:db8:acad:1::abcd:ef12:3456

(iv) HOST Performs Duplicate Address Detection (DAD):-

To ensure the address is unique on the network.

(v) HOST starts communication:-

once DAD succeeds, the device uses this IPv6 address to communicate.

22) Purpose of EUI-64 in IPv6:

(i) It auto-generates the 64-bit interface identifier from a device's 48-bit MAC, so hosts can form a globally by linking unique IPv6 Address without manual config.

(ii) It flips the universal/Local (U/L) bit so the resulting interface identifier correctly indicates a locally derived address & avoids MAC/IPv6 ambiguity.

Given:

Network prefix (64-bit): 2001:DB8:0:1111

48-bit MAC: FC:99:47:75:CE:E0

= FC99:4775:CEE0

Inserting FFFE into MAC from 48 bit to 64 bit

FC99:47FF:FE75:CEE0

FC = 1111 1100

= 1111 1110 (FE)

Final 64-bit interface identifier:

FE99:47FF:FE75:CEE0

Self-generated IPv6 address:

2001:DB8:0:1111:FE99:47FF:FE75:CEE0

23) => Use of Subnet mask:

(i) A subnet mask is used to separate the network portion & host portion of an IP address.

(ii) It helps routers identify which part represents the network & which part identifies individual devices.

(iii) Subnet masks are essential for routing, subnetting, & efficient IP address management.

Eg: Class C address = 192.168.10.0

Subnet mask = 255.255.255.0

Having only 1 network with 254 hosts.

By using a customized subnet mask, 255.255.255.192,

It can divide the network into 4 subnets, each with 62 hosts.

=> How it overcomes classful addressing limitation:

(i) In classful addressing, subnet sizes are fixed (wastage occurs if fewer hosts exist).

(ii) Customized subnet mask (classless subnetting) allow flexible division of networks based on actual needs, reducing IP wastage and improving utilization of available address space.

24) Given:

192.168.10.10/26

(a) Subnet mask:

11111111.11111111.11111111.11000000

→ 255.255.255.192

(b) Network ID:

/26 is block size = 256 - 192 = 64 in last octet.

192.168.10.10 fall in the first block

Network ID: 192.168.10.0

(c) Number of usable address:

Host bits = 32-26 = 6 → total addresses

$2^6 = 64$

usable = total - 2(network + broadcast)

= 64 - 2

= 62 usuable addresses

(d) First and last usable IP:

Network = 192.168.10.0

Broadcast = network + 63 = 192.168.10.63

1st usable = 192.168.10.1

Last usable = 192.168.10.62

25) PC1 = 192.168.1.126 is in first subnet (0-127).
Router = 192.168.1.129 is in the second subnet (128-255).

As configured, the PC cannot directly forward packets through that router because they are on different /25 subnets.

26) Given Destination IP: 144.16.68.117
The router forwards the packet via interface eth2 (144.16.68.0/24) because, it provides the longest prefix match for the destination 144.16.68.117.

27) Given:
ISP block 16.12.64.0/20
Each org needs 256 addresses (i.e./24).

(a) Number & range of addresses in ISP block:
/20 → host bits = 32-20 = 12 → total addresses = 2^{12} = 4096

Subnet mask = 255.255.240.0

Address range: 16.12.64.0 upto 16.12.79.255
(Since /20 covers third octect values 64 through 79).

4096 addresses from 16.12.64.0 → 16.12.79.255

=> The range address for each organization:

	n/w	range
org1 →	16.12.64.0/24	16.12.64.0 → 16.12.64.255
org2 →	16.12.65.0/24	16.12.65.0 → 16.12.65.255
org3 →	16.12.66.0/24	16.12.66.0 → 16.12.66.255
org4 →	16.12.67.0/24	16.12.67.0 → 16.12.67.255
org5 →	16.12.68.0/24	16.12.68.0 → 16.12.68.255
org6 →	16.12.69.0/24	16.12.69.0 → 16.12.69.255
org7 →	16.12.70.0/24	16.12.70.0 → 16.12.70.255
org8 →	16.12.71.0/24	16.12.71.0 → 16.12.71.255

Each org will get 256 addresses (usable hosts per org = 254)

=> unallocated range:

16.12.72.0 → 16.12.79.255

= 8 X 256

= 2048 addresses

28)

Features	FTP (File Transfer protocol)	TFTP (Trivial File Transfer Protocol).
Reliability	Reliable, uses TCP for connection-oriented data transfer ensuring error control & acknowledgement.	Less reliable, uses UDP, so no error connection or retransmission mechanism.
Features	supports authentication directory listing, & file management commands.	Very simple - used mainly for boot files or configuration transfers, no authentication or complex communication.

29) => POP3 (Post office protocol v3):

(i) It downloads emails from the mail server to the local device and usually delets them from the server after download.

(ii) Best for users who access email from one device, as messages are stored offline.

=> IMAP (Internet message ACCess protocol):

(i) It keeps emails on the server and allow users to view and manage them from multiple devices.

(ii) Ideal for modern users who check mail from phones, laptops or web clients since it syncs in real-time.

30) DHCP (Dynamic Host configuration protocol) automatically assigns IP addresses to devices in a network.

The 4-step handshake between the client and DHCP server ensures proper IP allocation.

(i) DHCP Discover:

The client broadcasts a discover message to find available DHCP servers.

(ii) DHCP offer:

DHCP servers responds with an offer message containing an available IP address and configuration info.

(iii) DHCP request:

The client replies with a Request message, confirming it wants to use the IP offered by a specific server.

(iv) DHCP ACknowledge (ACK):

The DHCP server sends an ACK message confirming the lease of the IP address to the client.