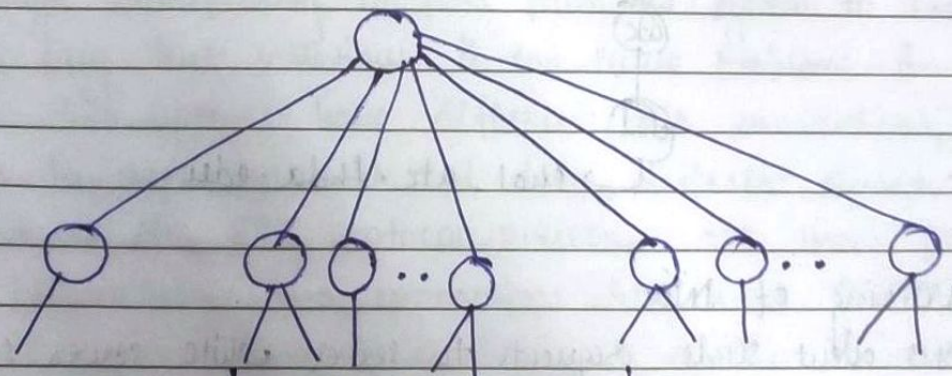
UNIT 3

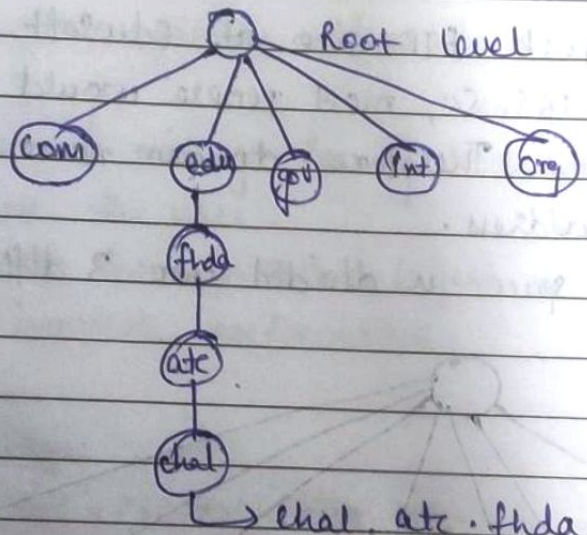
① DNS ① Stands for Domain Name System.
② An application layer protocol that defines how the application processes running on different systems, pass the messages to each other.
③ Directory service that provides a mapping btw the name of a host on the network and its numerical address.
④ It is required for functioning of internet.
⑤ DNS is a service that translates domain name into IP address. This allows the users to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
⑥ For example, suppose FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by ftp.EduSoft.com. Therefore, domain name is more reliable than IP address.
⑦ The domain name space is divided into 3 different sections:



Inverse Domain	Generic domains	Country Domains
→ Used for mapping address to a name.	→ Defines the registered hosts according to their generic Behaviour.	→ format is same as generic domain
→ To determine whether the client is on the authorized list or not.	→ Each node in a tree defines the domain name → uses 3-character labels	→ It uses 2 character labels. eg: us for United States.

Generic Domains: 3 character labels.

label	Description
biz	Business or firms
com	Commercial Organizations
edu	Educational Institutions
gov	Government Institutions
int	international Organizations.
mil	Military Groups.



Working of DNS.

1. DNS client sends requests to server while server sends respon (to obt
2. Client requests contain a name which is converted into IP addr (forward DNS lookups)
requests containing IP address that is converted into a name → Reverse DNS lookups.
3. If a client sends a request containing hostname, then th DNS resolver sends a request to DNS server to obtain the IP address of a hostname.
4. If the DNS server does not contain the IP address associate

with a hostname, then it forwards the request to another server.

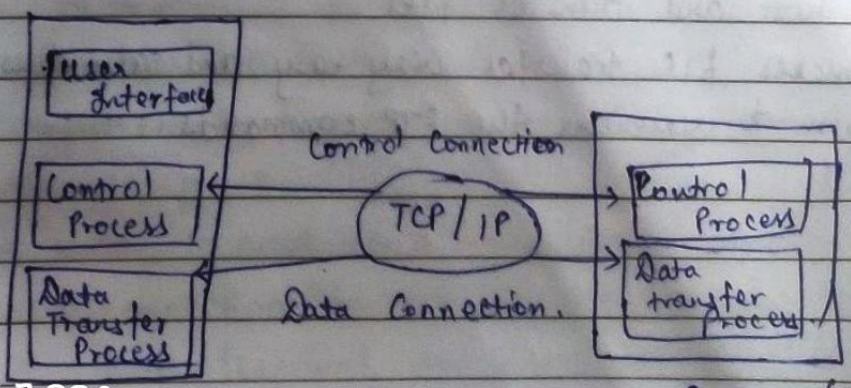
FTP:

1. Stands for file Transfer Protocol.
2. Standard internet protocol provided by TCP/IP used for transmitting files from one host to another.
3. Mainly used for transferring the web page files from their creator to the computer.
4. Also used for downloading the files to the computer from other servers.

Objectives: → It provides sharing & downloading of files.
→ Used to encourage the use of remote computers.
→ transfers data more reliably and efficiently.

Why FTP?

→ Although transferring of files from one system to another is very easy but sometimes it can cause problems. for eg. when two systems have different file conventions, different ways to represent text and data, different directory structures, etc. FTP protocol overcomes all these problems by establishing two connections b/w hosts. One connection is used for data transfer and another connection is used for control connection.



FTP Connections

Control Connection:
→ Uses very simple rules
→ We can transfer a line of command or a line of response at a time.
→ Made b/w the control processes.
→ Remains connected during the entire interactive FTP session.

Data Connection:
→ Uses very complex rules as data types may vary.
→ Connection is made b/w data transfer processes.
→ Opens when a command comes for transferring file and closes when the file is transferred.

FTP Clients:
→ A program that implements file transfer protocol which allows you to transfer files b/w 2 hosts on the internet.
→ It allows the user to connect to a host & download / upload the files.
→ It has a set of commands that we can use to connect to the host and transfer files.
→ It makes file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

1. Speed: One of the fastest way to transfer files.
2. Efficient: We do not need to complete all the operations to get the entire file.
3. Security: we need to login with username & password. ∴ It is secure
4. Back & forth movement: Allows to transfer the files back & forth.

Disadvantages of FTP:

1. Standard requirement is that it should be encrypted. Not all the providers offer encryption.
2. The size limit of the file is 2GB that can be sent.
3. It doesn't allow you to run simultaneous transfers to multiple ~~users~~ receivers.
4. It is not compatible with every system.

TELNET (Terminal Network)

→ The main task of internet is to provide services to users. For example, users want to run different application programs at remote site and transfer the results to a local site. This requires a client server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.

→ The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. A program that allows a user to log on to a remote computer.
TELNET is used to meet such demands.

→ It provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

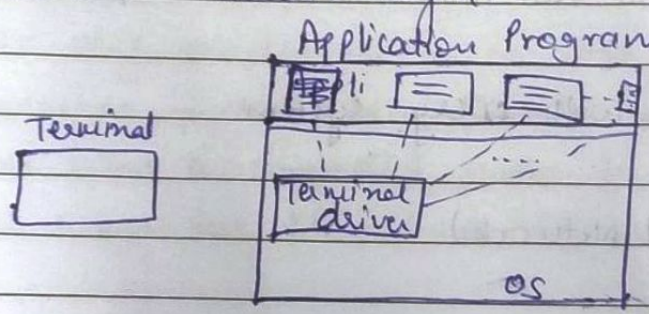
Two types of login: ① Local login
② Remote login.

Local login:

→ When a user logs in to a local computer.

→ When the keystrokes entered by the user are accepted by the terminal driver, the terminal driver passes these instructions to OS which in turn invokes the desired application program.

→ The OS has special meaning to special characters. For example, in unix, 'z' means suspend. Such situations do not create any problem b/c the terminal driver knows the meaning of such characters. But it can cause problems in Remote login.



Remote login:

→ When the user wants to access an application program on Remote Computer.

Working: (at local site)

① The user sends the keystrokes to terminal driver.

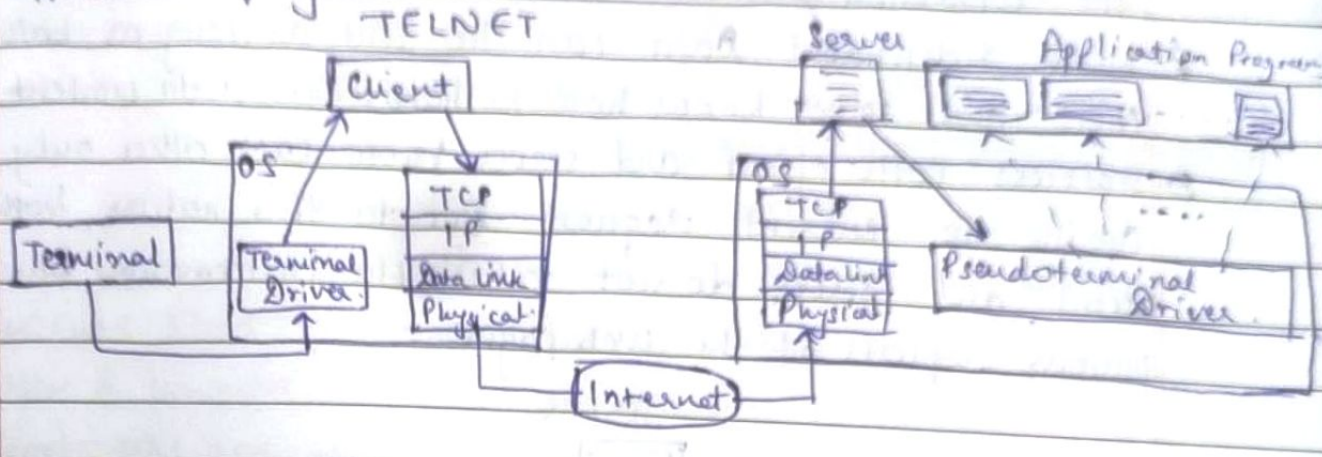
② The characters are then sent to TELNET client.

③ The TELNET client transforms the characters into a universal character set and delivers them to the local TCP/IP stack.

Working (at the remote site).

① The commands are transmitted to TCP/IP at the remote machine.

⑦ Characters are delivered to OS then passed to TELNET server.
⑧ TELNET Server transforms the characters which can be understood by remote computer.
⑨ The OS then passes these characters to the appropriate application program.



HTTP

① Stands for HyperText Transfer Protocol.
② Protocol used to access data on world wide web (www).
③ Can be used to transfer the data in the form of plain text, hyper text, audio, video, etc.
④ It is very efficient. Allows us to use in a hypertext environment where there are rapid jumps from one document to another.
⑤ Similar to FTP. But HTTP uses only one connection, there is no control connection.
⑥ Similar to SMTP as the data is transferred b/w the server & client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

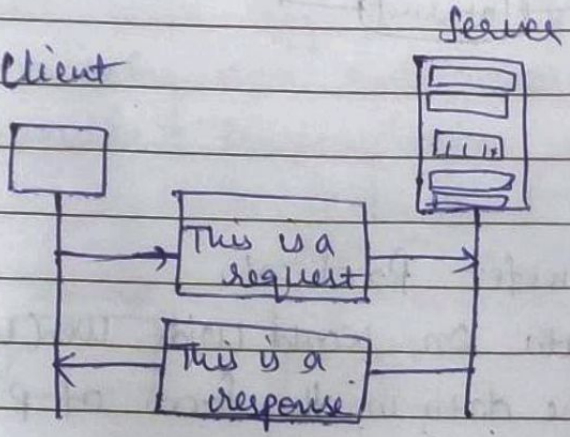
Features (HTTP)

① Connectionless protocol: The connection b/w the client and server exists only during the current request and response time. HTTP client initiates a request and waits for response from

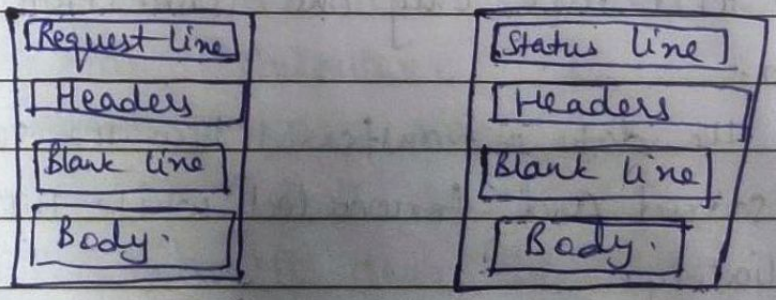
the Server. When the server receives the request, the Server processes the request and sends the response to the HTTP client after this which the client disconnects the connection.

② Media Independent: Data can be sent as long as both client and server know how to handle the data content.

③ Stateless: Both client and server know each other only during the current request. Due to this nature, both client and server do not retain the information b/w various requests of the web pages.



HTTP messages → Request (sent by client)
→ Response (sent by server)

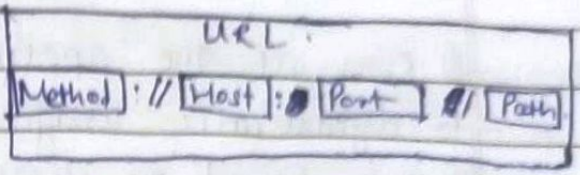


Request Message format

Response Message format

Uniform Resource Locator (URL)

→ A client that wants to access the document on the internet needs an address. For this, HTTP uses the concept of URL.
→ Standard way of specifying any information on the internet.
→ four parts → ① · Method
② · Host computer
③ · Port
④ · Path.



→ Method: Used to retrieve document from a server.
→ Host: A computer where the information is stored.
→ Port: URL can also contain port number of server. But it is an optional field. Port is seperated from the Host by a colon (:)
→ Path: Path is the pathname of the file where the information is stored.

DHCP (Dynamic Host Configuration Protocol)

→ Network management protocol used to dynamically assign an IP address to any device, or node, or network so they can communicate using IP (Internet Protocol).
→ There is no need to manually assign IP Addresses to new devices.
→ Can be implemented on local N/ws as well as large enterprise N/ws
→ Default Protocol used by most Routers & Networking equipments.
→ Also called RFC (Request for comments).

→ Manages the provision of all the nodes/devices added or dropped from the N/W.
→ Maintains the unique IP address of Host during DHCP server.
→ It sends a request to the DHCP Server whenever a client/node/device connects to a N/W.

→ It is also used to configure Proper Subnet Mask, default Gateway and DNS server information on the node or dev

Working of DHCP:

① Runs at the application layer of TCP/IP protocol stack to dynamically assign IP addresses.
② It is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as inform about client. It assigns the addresses out of those address pools.

① A client (N/w device) must be connected to the intern
② DHCP client requests an IP address. Client broadcasts a query for this information.
③ DHCP server responds to the client request by providing IP server address and other information.
This configuration information ~~[illegible]~~ a includes a time period called a lease for which the allocation is valid.
④ When refreshing an assignment, a DHCP client requests the same parameters but the DHCP server may assign a new IP address. (Based on the policies set by administrator).

Components of DHCP:

① DHCP server: Holds the IP address and other related info.
② DHCP client: End point that receives configuration info. from DHCP server. This could be any device like computer, laptop, et.
③ IP address pool: Range of IP addresses that are available to DHCP [illegible] Typically handled out sequentially from lowest to highest

④ Subnets: Partitioned segments of IP networks. Used to keep the networks manageable.

⑤ Lease: Length of time for which the DHCP client holds the IP address into. When a lease expires, the client has to renew it.

⑥ DHCP Relay: A host/router that listens for client messages being broadcast on that N/w and forwards them to a configured server.

Benefits of DHCP:

① Centralized administration of IP configuration: DHCP IP configuration info. can be stored in a single location and enables that administrator to centrally manage all IP address configuration.

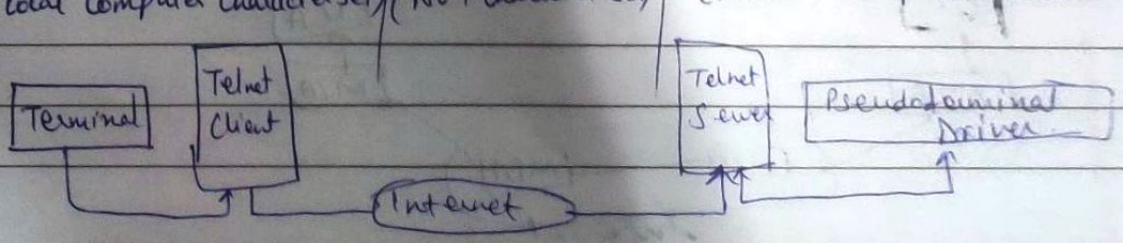
② Dynamic Host Configuration: DHCP automates the host conf process and eliminates the need to manually configure individual hosts.

③ Seamless IP host configuration: Ensures that the DHCP client gets accurate and timely IP configuration parameter such as IP address, subnet mask, default gateway, etc.

④ Flexibility and scalability: Increased flexibility.
Allows the administrator to easily change IP configuration when infrastructure changes.

Network Virtual Terminal: (NVT)

→ Interface that defines how data and commands are sent across the N/w.



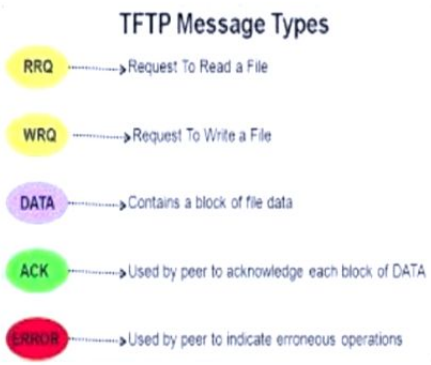
TFTP: Trivial File Transfer Protocol (TFTP) is designed for these types of file transfer. It is so simple that the software package can fit into the read-only memory of a diskless workstation. It can be used at bootstrap time. The reason that it fits on ROM is that it requires only basic IP and UDP. However, there is no security for TFTP. TFTP can read or write a file for the client. *Reading* means copying a file from the server site to the client site. *Writing* means copying a file from the client site to the server site.

The benefit of using TFTP is that it enables bootstrapping code to use the similar underlying TCP/IP protocols that the operating framework uses once it starts execution. Thus it is the possibility for a device to bootstrap from a server on another physical network.

Features of TFTP: The main features of TFTP are as follows:

- TFTP is based on the client-server principle and uses well-known UDP port number 69 for the TFTP server.
- TFTP is an unsecured protocol and does not support authentication.
- TFTP incorporates idle – RQ (stop and wait) error recovery mechanism.
- Every TFTP data unit bears a sequence number.
- Each data unit is separately acknowledged. After taking the acknowledgement, the next data unit is transmitted.
- Error recovery is by retransmission after timeout. TFTP uses adaptive timeout with an exponential back-off algorithm.

TFTP Messages: There are five types of TFTP messages, RRQ, WRQ, DATA, ACK, and ERROR, as shown in Fig:



1. **Read Request** –The client uses this command to get 0 copy of a file from the server

Read Request (1)	File Name	0	mode	0
2 octets	variable	1 octet	variable	1 octet

2. **Write Request** – The client uses this command to write a file into the server

Read Request (1)	File Name	0	mode	0
2 octets	variable	1 octet	variable	1 octet

3. **Data** – This TFTP message contains blocks of data.

Data (3)	Sequence Number	Data
2 octets	2 octets	up to 512 octets

4. **Acknowledgement**– The client and the server used this to acknowledge the received data units.

Ack (4)	Sequence Number
2 octets	2 octets

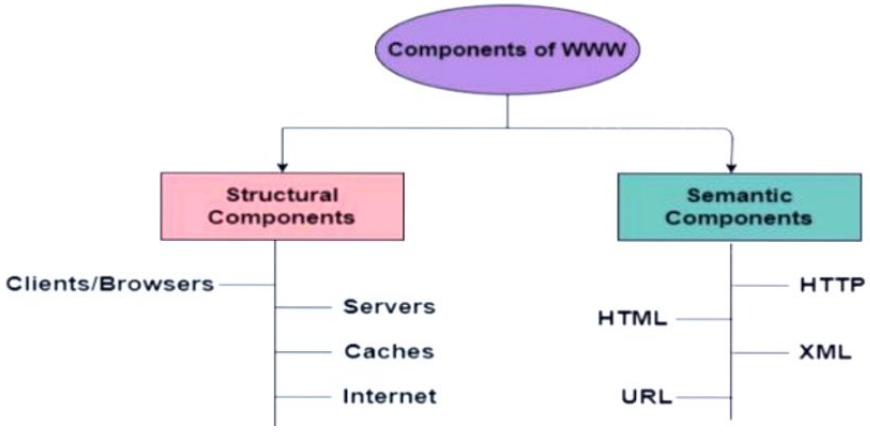
ERROR: The ERROR message is used by the client or the server when a connection cannot be established or when there is a problem during data transmission. It can be sent as a negative response to RRQ or WRQ. It can also be used if the next block cannot be transferred during the actual data transfer phase. The error message is not used to declare a damaged or duplicated message.

FTP	TFTP
FTP stands for File Transfer Protocol.	TFTP stands for Trivial File Transfer Protocol.
The software of FTP is larger than TFTP.	While software of TFTP is smaller than FTP.
FTP works on two ports: 20 and 21.	While TFTP works on 69 Port number.
FTP services are provided by TCP.	While TFTP services are provided by UDP.
The complexity of FTP is higher than TFTP.	While the complexity of TFTP is less than FTP complexity.
There are many commands or messages in FTP.	There are only 5 messages in TFTP.
FTP need authentication for communication.	While TFTP does not need authentication for communication.
FTP is generally suited for uploading and downloading of files by remote users.	While TFTP is mainly used for transmission of configurations to and from network devices.
FTP is a reliable transfer protocol.	While; TFTP is an unreliable transfer protocol.
FTP is based on TCP.	While; TFTP is based on UDP.
FTP is slower.	TFTP is faster as compared to FTP.

WWW (World Wide Web): The **World Wide Web** or Web is basically a collection of information that is linked together from points all over the world. It is also abbreviated as **WWW.** It provides flexibility, portability, and user-friendly features. It mainly consists of a worldwide collection of electronic documents (i.e. Web Pages). It is basically a way of exchanging information between computers on the Internet. The WWW is mainly the network of pages consists of images, text, and sounds on the Internet which can be simply viewed on the browser by using the browser software. It was invented by Tim Berners-Lee.

Components of WWW: The Components of WWW mainly falls into two categories:

1. Structural Components
2. Semantic Components



DATE / /
PAGE

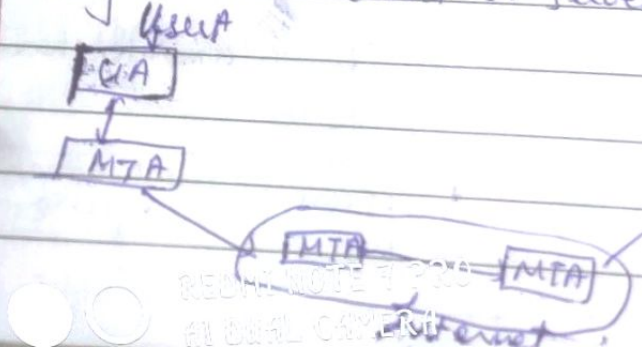
SMTP (Simple Mail Transfer Protocol)

→ Set of communication guidelines that allows the software to transmit an electronic mail over internet.
→ Program used for sending messages to other computers user based on e-mail address.
→ It can be done on same as well as different computers
→ It can send single message to one or more recipients.
→ Messages can include text, voice, video, etc.
→ It can also send messages on N/ws outside internet
→ Main purpose is to set up communication rules b/w servers.
→ If the recipient address is wrong, then receiving server replies with an error message of some kind.

→ We break the SMTP client and SMTP server into 2 components → User agent (UA)
→ Mail transfer Agent (MTA)

UA prepares the message and puts in the envelope created.
MTA transfers mail accross internet.

→ SMTP allows a more complex system by adding relaying system. Instead of Having just one MTA at sender's side and one at receiver's side, more MTAs can be added acting as either client or server to relay the mail.



Working of SMTP:

① Composition of mail: User sends e-mail by composing an electronic mail message using a Mail User Agent (MUA)
→ The message contains 2 parts → Body & Header.
Body is the main part and Header contains information such as the senders and recipients address.

② Submission of mail: After composing the email, the mail client then submits the composed e-mail to SMTP server.

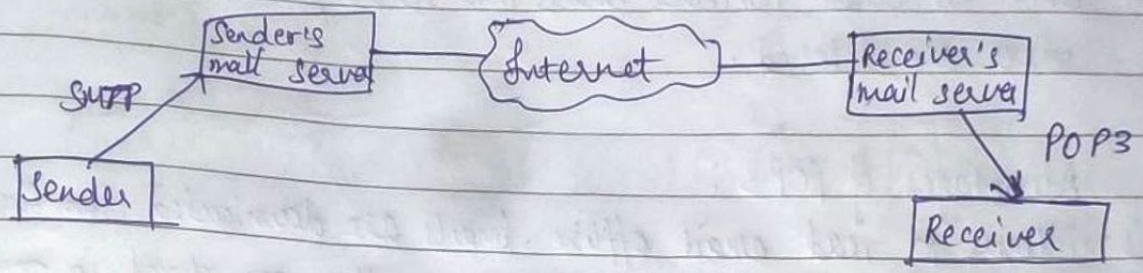
③ Delivery of Mail: E-mail address contains 2 parts: username of recipient and domain name. Eg: vivek@gmail.com. vivek is recipient's name and gmail.com is domain name. If domain name of recipient is different from senders domain name, then MSA will send the mail to Mail Transfer Agent (MTA) to relay the email. The MTA will find the target domain.

④ Receipt and Processing of Mail: Once the incoming message is received, the exchange server delivers it to the incoming server which stores the email where it waits for the user to retrieve it. (Mail Delivery Agent)

⑤ Access and Retrieval of Mail: The stored email is MDA can be retrieved by using MUA (Mail user agent). MUA can be accessed by using login & password.

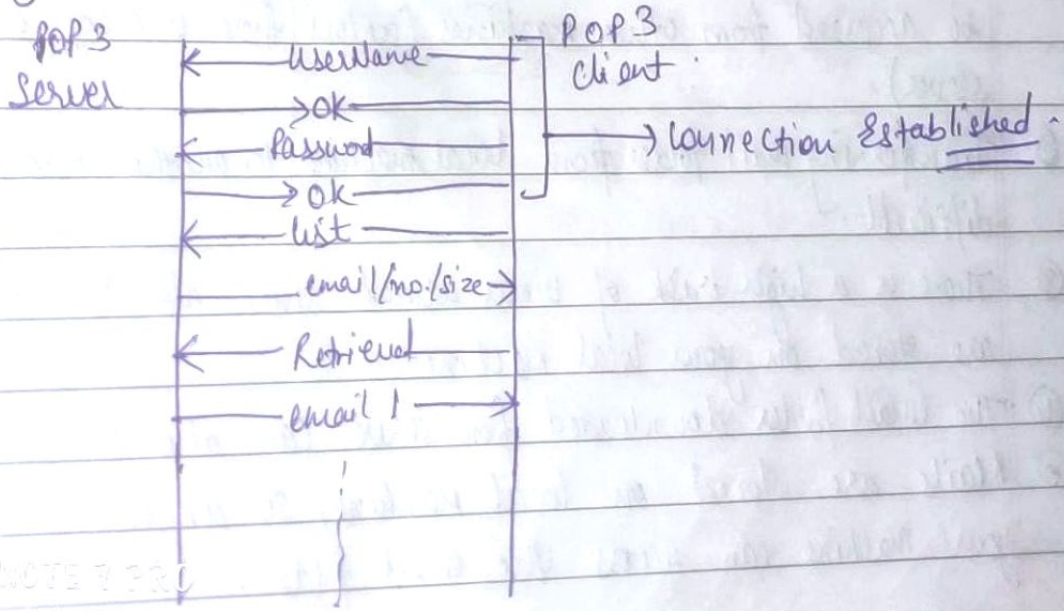
POP (Post office Protocol)

→ When a message is sent, SMTP is used to deliver the message from client to server and then to the recipient server.
→ The message is sent from recipient server to actual server with the help of Message Access Agent (MAA)
→ MAA contains 2 types of Protocols → POP3 & IMAP.



→ The transmission of mail from sender to sender's mail server and then to receiver's mail server is done with the help of SMTP.
→ Then to transmit the mail from receiver's mail server to actual Receiver, POP3 or IMAP is used.
→ SMTP → Push Protocol POP → Pull protocol.

Working of POP3 protocol:



2022/12/10 23

① Server asks for username
② If the username is found in POP3 server, it sends OK message.
③ Server asks for password.
④ Sends OK if passwords match.

CONNECTION ESTABLISHED

→ The client can then see a list of mails and then it can select the mail to retrieve from the list of mails.
→ Once the client retrieves emails from server, all the emails from server are deleted.

Advantages of POP3:

① Allows to read email offline. (mails are downloaded from the server)
② Provides easy & fast access to emails as they are stored in our PC.
③ No limit on the size of email.
④ Requires less server storage.
⑤ Simple protocol, easy to configure and use.

Disadvantages of POP3:

① Mails are deleted from server once downloaded, therefore they cannot be accessed from other machines (unless there is a copy of the mail on server).
② Transferring mail folder from local machine to another machine can be difficult.
③ There is a high risk of virus attack since all the attachments are stored on your local machine.
④ The email folder downloaded from server can also become corrupted.
⑤ Mails are stored on local machine, so anyone who sits on your machine can access the email folder.