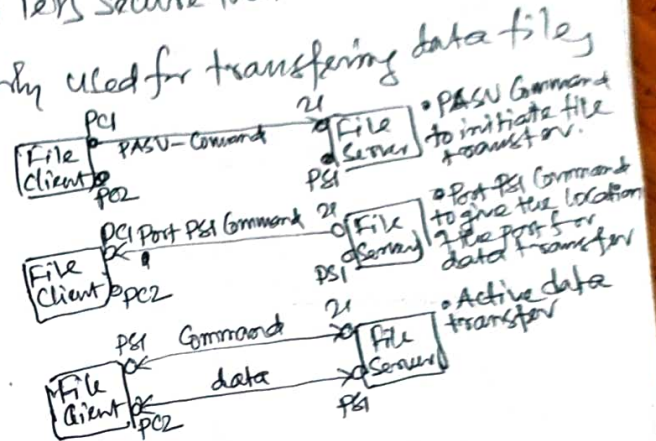


FTP, SFTP & TFTP in Comp Net.

- FTP, SFTP, TFTP are used to transfer files over the Computer Net.
- FTP - File Transfer Protocol (Port NO - 21):
 - It has two channels, one is for data & the second is for Command (out-band Protocol)
 - It does not use any encryption mechanism \Rightarrow data tampering is possible.
 - It uses TCP for data Communication.
- SFTP - (Secure Shell) File Transfer Protocol (Port NO - 22)
 - It has single channel for data & Command (in-band Protocol).
 - Both data & Command are encrypted in SFTP.
 - It uses TCP for data Communication.
- TFTP - Trivial File Transfer Protocol (Port no. - 69)
 - It does not require authentication, making it less secure than others -
 - It uses UDP for data Communication.
 - It is not used over the internet, it is mainly used for transferring data files within LAN.

Working of FTP:



Practical of Wireshark for FTP & HTTP:

1. open the Wireshark (click on it).
2. open the Command Prompt in Windows.
3. Go to Capture \rightarrow interface \rightarrow make setting for wired / others \rightarrow hit Start.
4. In the Command prompt \rightarrow ftp ftp.mcafee.com
: anonymous
Password: 123456.

5. Go to the directory list ftp> dir. Show several files like outputfile.txt ----.
- ftp> ascii \rightarrow type set to A
- ftp> binary \rightarrow type set to 1
- ftp> ascii
- ftp> hash \rightarrow hash mark printing on ftp.
- ftp> get outputfile.txt
- ftp> quit \rightarrow quitting the session (close the window).

Application Layer Protocols:

- DNS - Domain Name System → DNS is used to get IP from the domain name
- SMTP - Simple Mail Transfer Protocol →
 - Used by email clients like Gmail, Outlook, Yahoo etc.
 - Sends email from the sender's device to the receiver's mailbox.
- POP - Post Office Protocol
 - This service is also based on email.
 - retrieves & organises emails from the receiver's mail server to the receiver's computer.
- FTP - File Transfer Protocol
 - it is used for file transfer.
- HTTP - Hyper Text Transfer Protocol
 - is used for browsing webpage.

How much time domain name & IP are valid?

Domain Name	IP	TTL
Google.com	xx ✓	xx
Amazon.in	xx ✓	xx
xxx	xx	xx

DNS - Domain Name System

Basics

- helps us to get IP addr. from domain names & vice versa.
- Google.com ↔ IP addr. of google.com.
- DNS uses UDP Protocol.
- You can have your own domain names for your new webpage like www. .co.in.
- IP addr. are dynamic, so they can change with time. Recently accessed domains are stored as entries for faster access to the domain.
- nslookup google.com.

Domain Names:

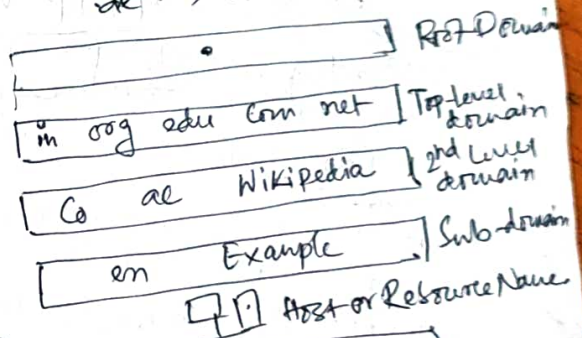
Generic Domain

- .com → Commercial domain.
- .org → organization "
- .edu → Educational/Insti "
- .net → Itp/some company also use it.
- .mil → military organization.

High Hierarchical Access to Domain names:

Country Domains:

- .in → India
- .jp → Japan
- .uk → United Kingdom.
- .de → Germany.



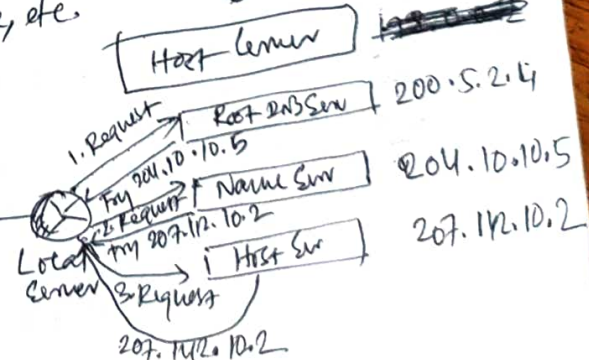
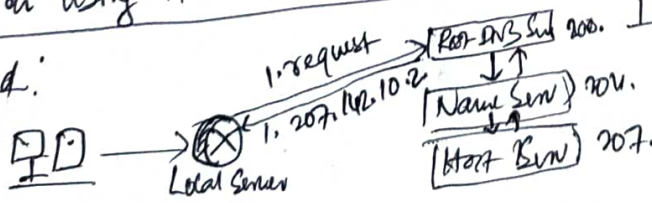
DNS database organization (Distributed Database):

- 13 root servers are there in the world to avoid single-point failure.
- Name server means .com, .in, .org.
- Host server hosts the database like youtube, Google, etc.

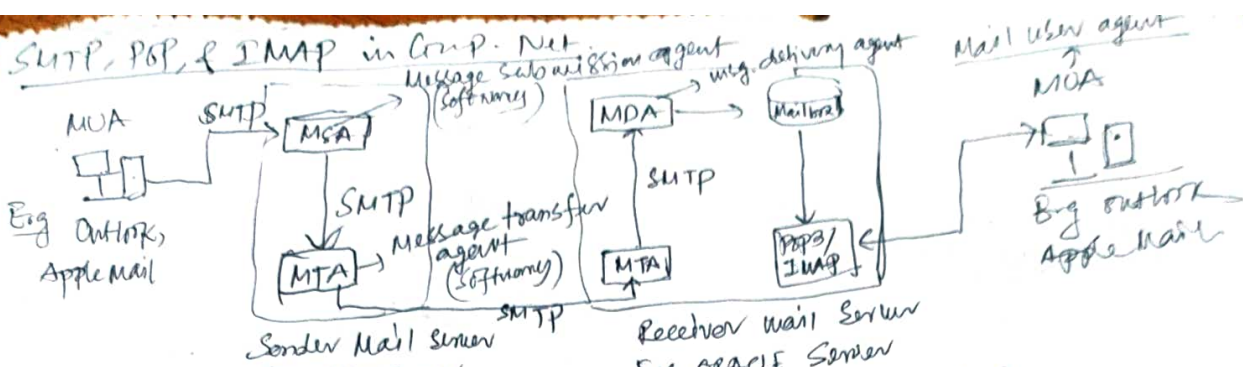
DNS entry:

Address Resolution using iterative method:

Recursive Method:



SMTP, POP, & IMAP in Comp. Net



Parameters

Full Form

Transfer Proper

Port No.

Transport Layer

Eg. IBM Server
SMTP

Simple Mail
Transfer Proto

Send Mail (Push
Mail)

25

TCP

POP

Post Office
Proto

Retrieve Mail (POP
Mail)

110 (Default) &
995 (SSL)

TCP

IMAP

Internet Message
Access Protocol

Retrieve Mail (POP Mail)

143 (Default) & 993 (SSL)

TCP

HTTP in Comp Net

Basics

• Hypertext
• HTTP usually use

transfer Protocol
• Port no. is 80

TCP for reliable Services.

- Server stays stateless. Many clients are connected to the server, so the server cannot maintain the state of each client.
- Client state is maintained using cookies.
- HTTP is an-band Protocol. (Command & data are on the same connection).

Types of HTTP

• HTTP 1.0 (Non Persistent Connection)

- TCP connection is established for each HTTP req-response transaction.
- After that the server sends the response back to the client, the connection is closed.
- If the connection needs to make another req., it has to establish a new TCP connection.
- Simple Implementation
- Predictable resource usage
- Increase in overhead & higher latency (due to 3-way handshaking)

HTTP 1.1 (Persistent Connection)

- The client & server maintain the connection open after initial req-response exchange.
- So for a new req. by the client, no need to establish a new TCP connection.
- Reduce overhead
- Faster response time.

HTTP Methods

- GET: The GET method is used to retrieve data from the server.
- HEAD: It is similar to GET, but it only req. the headers of the resource and not the actual content.
- POST: Post is used in filling forms on the server and the client fill forms back to the server.
- PUT: Used for uploading the object on the server. (upload file on the server)
- DELETE: The delete method is used to req. the removal of an object on the server.
- CONNECT: The connect method is used by HTTPS to enable secure connection.
- OPTIONS: Used to req. information about the communication option available for a particular URL.
- TRACE: Used to see what are the intermediate servers have received and how they interpret the request.
- PATCH: Used to apply partial modifications to a resource.

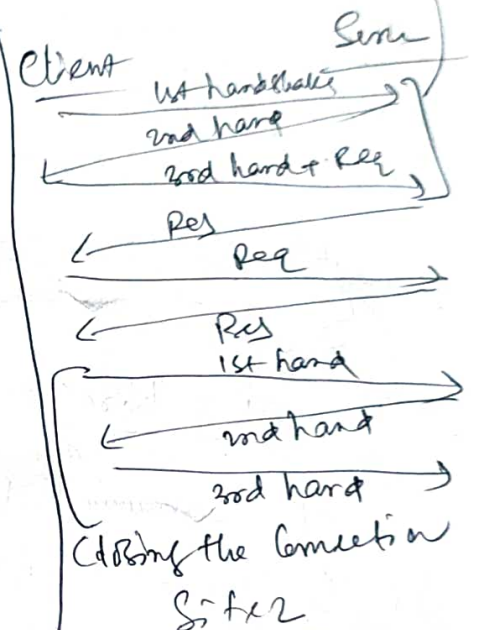
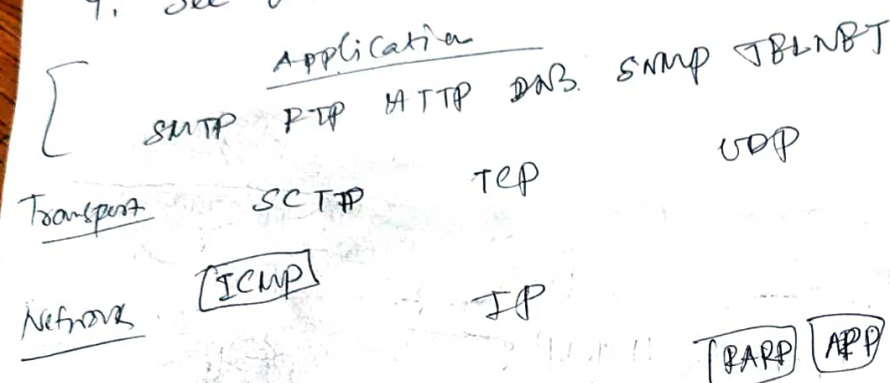
* Go to Wireshark interface.

1. open terminal/Command Prompt:
 - > ipconfig /all
 - > arp -a
 - > Ping www.google.com → get the ipg server

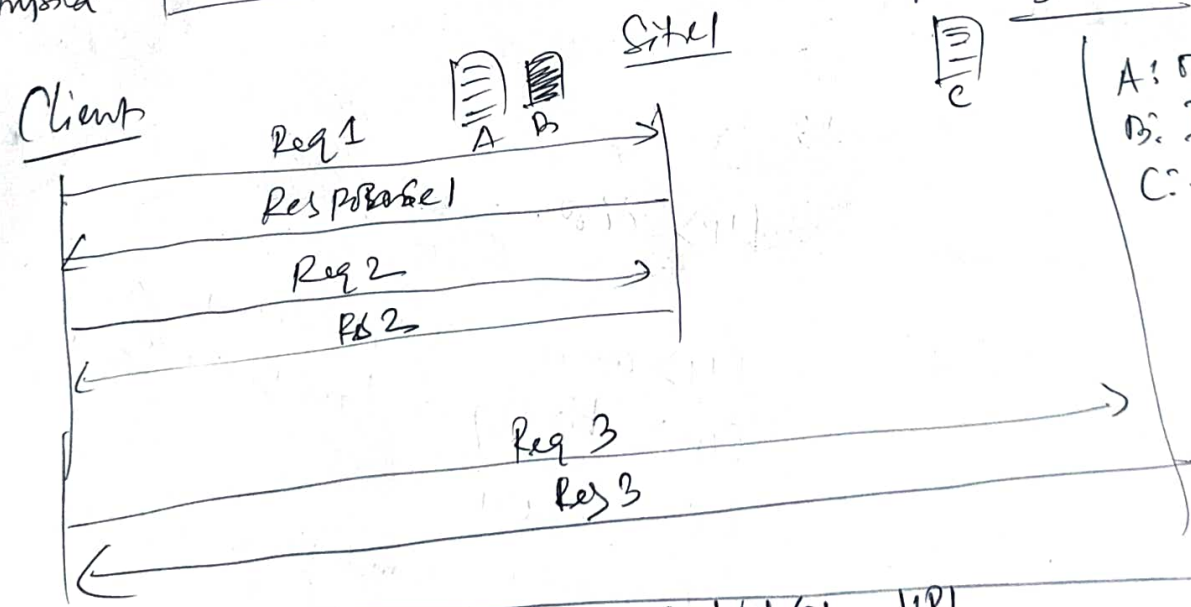
(IPg machine
not address
Default Gateway MAC)

2. Go to Wireshark - Search http only.
3. Open the browser www.google.com → download a picture.
4. See Wireshark and analyze it.

opening the connection



Data Physical
Protocols defined by the underlying networks (host to network).



A: original document
B: Image
C: Referenced file

1. your IP address
2. your Machine MAC.
3. Default Gateway MAC.
4. Website URL
5. Website IP Address.
6. → dest. MAC → default gateway's MAC.