NETWORKING

by Mohd Imran

PROTOCOL

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network

SERVERS

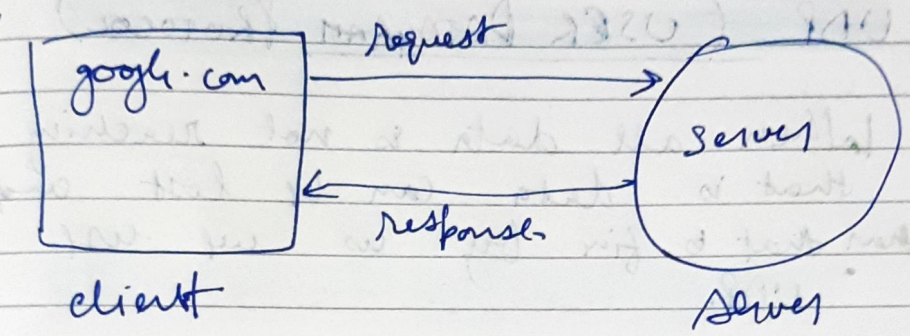
A server is a computer program or device that provides a service to another computer program and its user also known as the client.

In a data center, the physical computer that a server program runs on is also frequently referred to as a server.

Client-Server Model

Date : / /
Page No.

Eg.



~~Types of Protocols~~

TCP (TRANSMISSION CONTROL PROTOCOL)

→ It will ensure that the data will reach its destination and it will not be corrupted on the way.

→ It lies between the application and Network layer which are used in providing reliable delivery services

→ It is a connection-oriented protocol for communications that helps in the exchange of messages between the devices over a network.

→ It is a Transport layer Protocol.

→ It does congestion Control.

→ It maintains the order of data using sequence No.

Date : / /
Page No.

UDP (USER DATAGRAM PROTOCOL)

→ When all data is not reaching that is data can be lost and when that is fine by us we use UDP.

→ Unlike TCP, it is an unreliable and connectionless protocol.

→ It is a Transport layer Protocol.

→ UDP is used for real-time services like computer gaming, voice or video communication, live conferences, etc.

HTTP (HYPERTEXT TRANSFER PROTOCOL)

→ It is used by web browsers.
→ It uses TCP inside it.
→ Basically it decides the format of the data that is being transferred between web clients and servers.
→ default port is port 80.

PACKETS

→ A packet is a small segment of a larger message.

Date : / /
Page No.

→ Data sent over computer networks such as the internet, is divided into packets.

IP ADDRESSES (Internet Protocol)

→ An IP address is a series of numbers that identifies any device on a network

→ An IP address is a 32-bit number.

→ Computers use IP addresses to communicate with each other and to other networks as well.

→ its format

X . X . X . X

↓

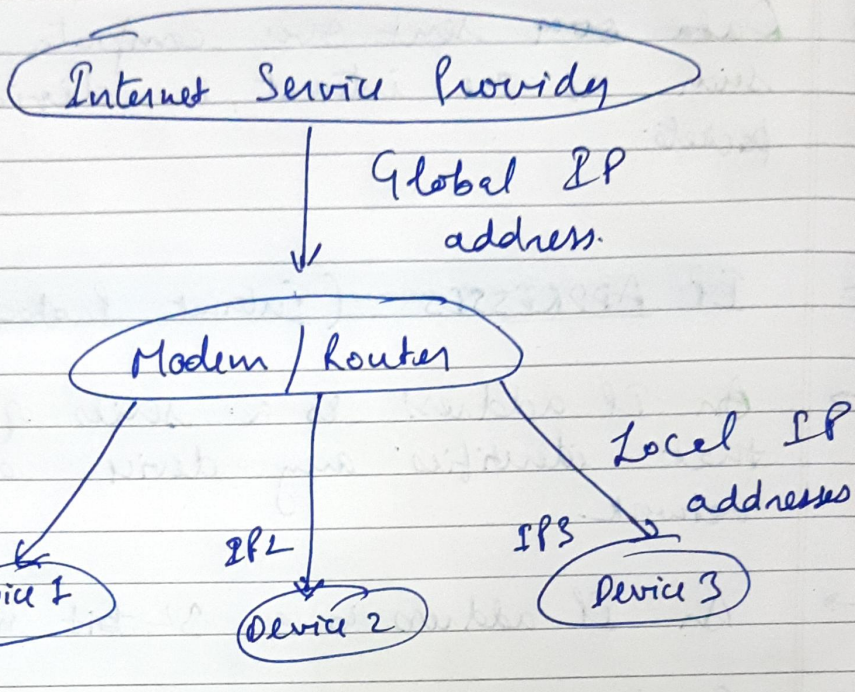
0-255

Every single X can have the value between 0 to 255

Eg. 192.168.2.30

192.168.2. → Network Address

30 → device address



→ Any device connected to the modem will have same IP address i.e. Global IP address.

→ In addition, modem/router will give all the connected devices their separate Local IP addresses with the help of DHCP.

DHCP (Dynamic Host Configuration Protocol)

→ DHCP is an application layer protocol which is used to provide-

(i) Subnet Mask
(ii) Router Address
(iii) DNS Address
(iv) Vendor class Identifier

Date : / /
Page No.

→ DHCP port number is 67 for server and 68 for client.

→ It is a client server protocol which uses UDP services.

NAT (Network Address Translation)

→ When a device connected to the router/modem sends request to modem/router then it goes to ISP and then to the server.

then the data is received on Public/Global IP address by the network/ISP and then it is sent to the respective device local IP with the help of NAT.

→ NAT identifies the local IP addresses of the devices and masks their port numbers as well so that no two devices/hosts will have same port number.

→ The idea of NAT is to allow multiple devices to access the internet through a single public address. To

achieve this, the translation of a private IP address to a public IP address is required.

NAT is a process in which one or more local IP address is translated into one or more Global IP address in order to provide internet access to the local hosts.

★ Applications are differentiated using port numbers.
Every application have different port numbers which is used by the IP address to decide to which application the data needs to be sent.

PORT NUMBERS

→ IP address will identify the computer and Port Number will identify the application.

→ All the HTTP stuff will happen on port 80.

→ Port no. is a 16 bit number

Total = $2^{16} \approx 65,000$

Date : / /
Page No.

→ Port no. 0 – 1023 are reserved ports.

Port no. 1024 – 49152 are registered for specific applications

the remaining ones we can use.

#1. LAN

Local Area Network.

A local Area Network is a collection of devices connected together in one physical location, such as building/ office or home.

It covers small area.

#3. WAN

Wide Area Network.

It is a collections of local Area Networks (LAN) or other networks that communicate with one another

A WAN is essentially a network of networks.

#2. MAN

Metropolitan Area Network.

a MAN is smaller than a wide Area Network (WAN) but larger than a Local Area Network (LAN)

A MAN is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns.

SONET (in WAN)

Synchronous Optical Networking.

It basically carries the data using optical fibres hence it can cover larger distances.

FRAME RELAY (in WAN)

Its basically a way to connect LAN to the WAN.

MODEM

→ A modem converts the digital data signals into analogue data signals.

→ Modem stands for Modulation and Demodulation.

ROUTER

→ A router receives and sends data on computer networks.

→ A router routs the data packets based on their IP addresses.

→ Data packets contains various kind of data such as files, communications, images and simple transmissions like web interactions.

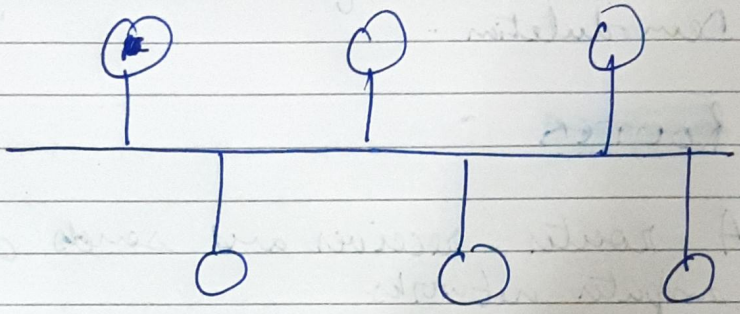
→ The data packets have several layers of sections, one of which carries identifying information such as sender, data type, size and most importantly, the destination IP address.

Date : / /
Page No.

TOPOLOGIES

Ways of connecting computers.

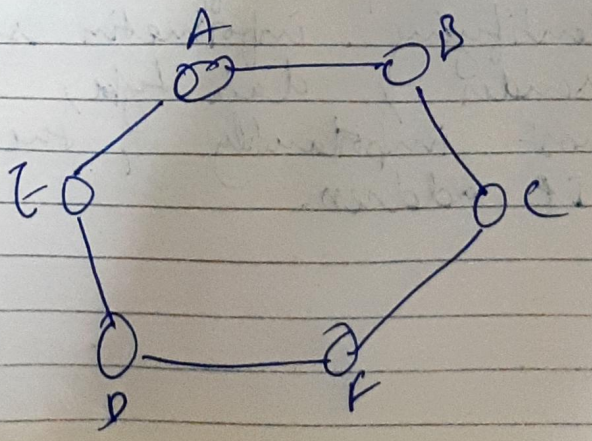
(i) BUS TOPOLOGY



Limitations → if the link is main cable gets broken, it will spoil the entire network

→ In this only one person can send data at a time.

(ii) RING TOPOLOGY.



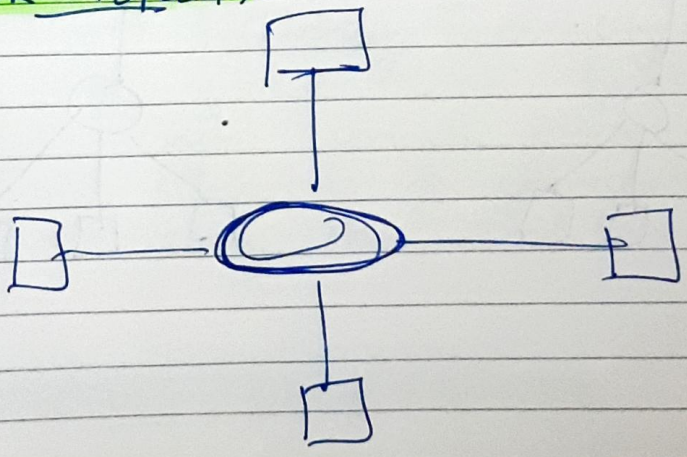
In this every system communicate with another computer.

If we want to target from A to F it would have to go through computer B & C.

Limitations → If one of the cable breaks, we wouldn't be able to transfer data

→ Lot of unnecessary calls are being made

(iii) STAR TOPOLOGY

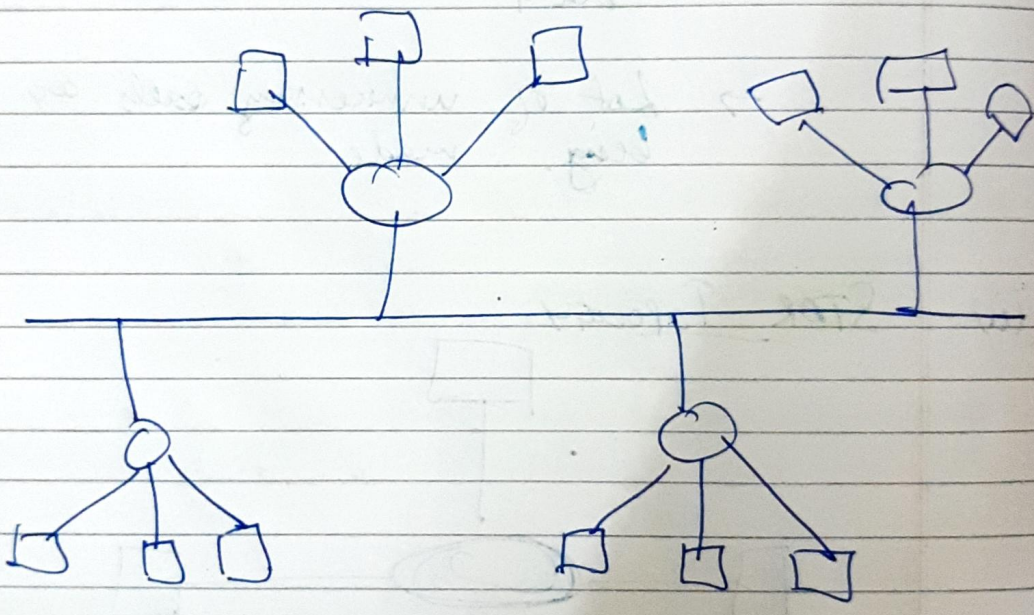


In this there is one controlling device which is connected to all computers.
Every communication is done through that only.

Limitations :→ If the central device fails the whole network will go down.

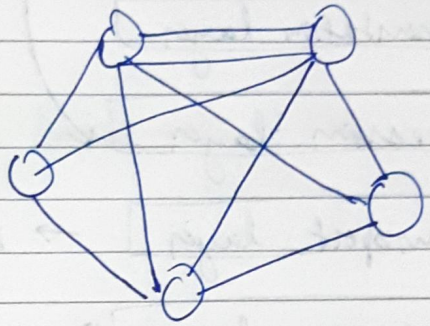
(iv) TREE TOPOLOGY (BUS + STAR)

In this some star networks connected like a bus.



(v) MESH TOPOLOGY

In Mesh every single computer will be connected to every single computer



Limitations: → very expensive as so much wire is used.

→ ~~Scalability~~ Scalability issues as if we want to add one more computer then it would have to be connected with every other computer.

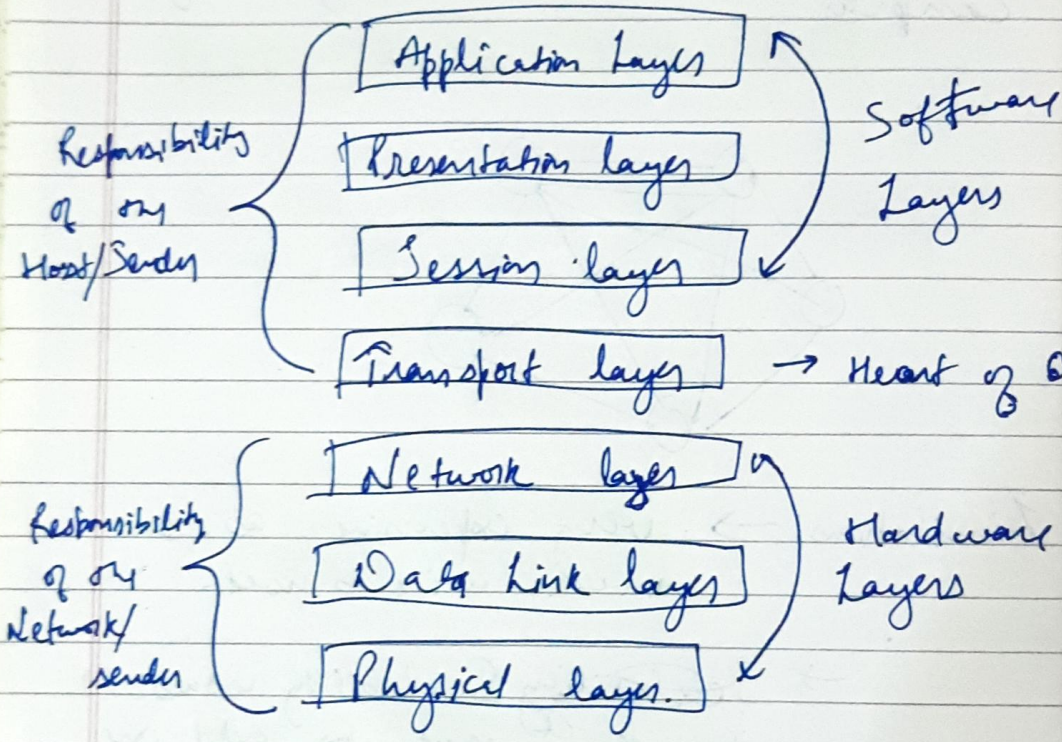
STRUCTURE OF NETWORK

OSI MODEL

It stands for Open Systems Interconnection model.

Date : / /
Page No.

→ OSI consists of seven layers and each layer performs a particular network function.



APPLICATION LAYER → Its implemented in software. This layer provides the services to the user.

PRESENTATION LAYER → It is responsible translation, compression & encryption.

Date : / /
Page No.

SESSION LAYER → It is used to establish, manage and terminate the sessions.

TRANSPORT LAYER → It provides reliable message delivery from process to process.

NETWORK LAYER → It is responsible for moving the packets from source to the destination.

It works for the transmission of received data segments from one computer to another that is located in a different network.

Router lives over here.

It assigns sender's and receiver's IP address to every segment and it form an IP packet. This is known as logical addressing.

DATA LINK LAYER → It is used for error free transfer of data frames.

Date : / /
Page No.

PHYSICAL LAYER → It provides a physical medium through which bits are transmitted.

TCP/IP MODEL

It is basically known as Internet Protocol suite.

It consists of 4 layers.

- Application Layer
- TRANSPORT LAYER
- Internet Layer
- Network Access Layer

APPLICATION LAYER → This is the topmost layer and defines the interface of host programs with the transport layer services.

This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

Date : / /
Page No.

TRANSPORT LAYER → It is responsible for error-free and end-to-end delivery of data.
The protocols defined here are TCP and UDP.

INTERNET LAYER → It defines the protocols for logical transmission of data over the network.

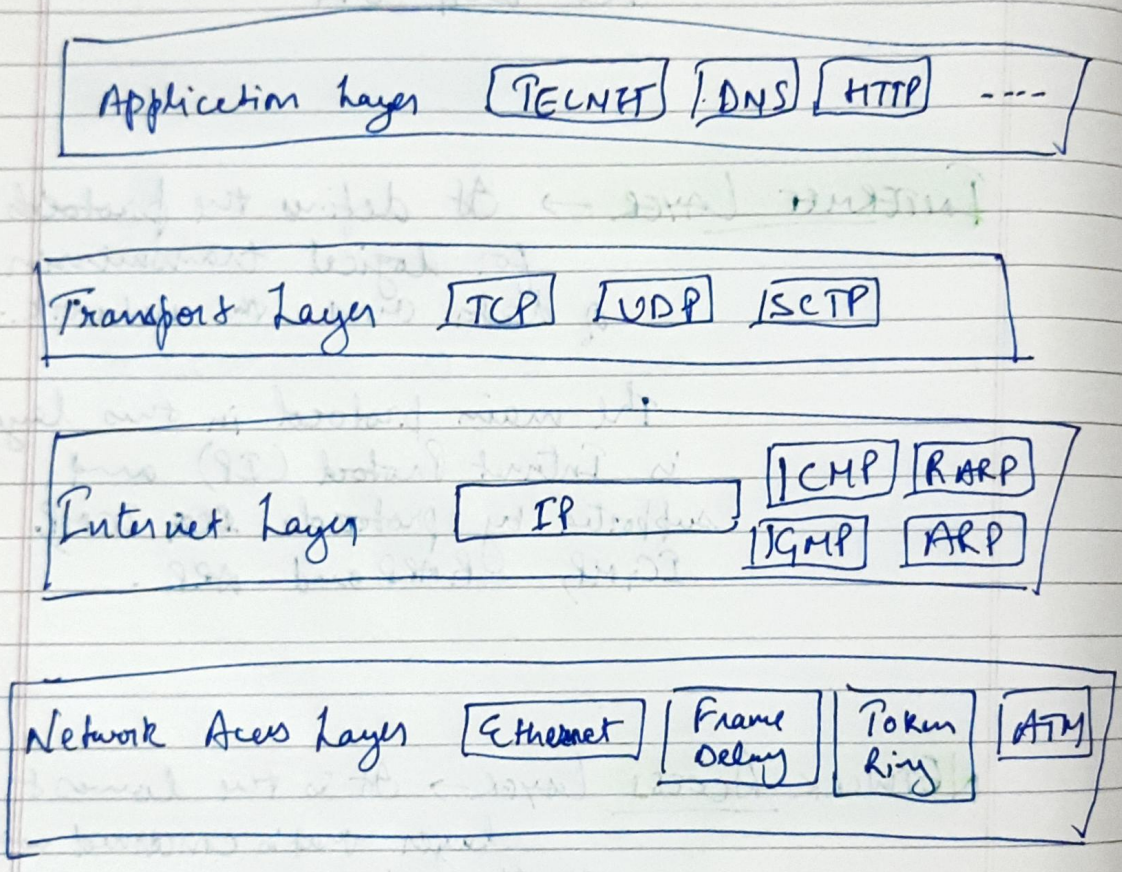
The main protocol in this layer is Internet Protocol (IP) and supported by protocols ICMP, IGMP, RARP and ARP.

NETWORK ACCESS LAYER → It is the lowest layer that is concerned with the physical transmission of data.

TCP/IP does not specifically define any protocol here but supports all the standard protocols.

Date : / /
Page No.

the following diagram shows the layers and the protocols in each of the layer!



NETWORKING DEVICES

(i) REPEATER

→ A repeater operates at the physical layer.

Date : / /
Page No.

→ Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

→ Repeaters do not amplify the signal

→ when the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.

→ It is a 2 port device.

(ii) **HUB**

→ A hub is basically a multiport repeater.

→ A hub connects multiple wires coming from different branches

→ Hubs cannot filter data, so data packets are sent to all connected devices.

types of Hubs

(a) **Active Hubs** → These are the hubs which have their own power

supply and can clean, boost and relay the signal along the network.
It serves both as a repeater as well as wiring center.
These are used to extend max distance between nodes.

(b) PASSIVE HUB → These are hubs which collect wiring from nodes and power supply from active hub.
These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance b/w nodes.

(iii) BRIDGE

→ A bridge operates at data link layer.

→ A bridge is a repeater, with additional functionality of filtering content by reading the MAC addresses of source and destination.

→ It is also used for interconnecting two LAN's working on same protocol.

→ It has a single input and single output port, thus making it a 2 port device.

Types of Bridges:-

(a) TRANSPARENT BRIDGES → These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network.
These bridges make use of two processes i.e. bridge forwarding and bridge learning.

(b) SOURCE ROUTING BRIDGES → In these bridges routing operation is performed by source station and the frame specifies which route to follow.

(iv) SWITCH

→ A switch is a multiport bridge with a buffer and a design that can boosts its efficiency and performance.

Date : / /
Page No.

→ Switch is a data link layer.

→ Switch can perform error checking before forwarding data, that makes it efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.

(V) ROUTERS -

→ A router is a device like switch that routes data packets based on their IP addresses.

→ Router is mainly a Network layer device.

(Vi) GATEWAY

→ It is a passage to connect two networks together that may work upon different networking models.

→ Gateways are also called protocol converters and can operate at any network layer.

(vii) **BROUTER**

→ It also known as bridging router.

→ It is a device which combines features of both bridge and router.

→ It can work either at the data link layer or at network layer.

WEB PROTOCOLS

TCP/IP Protocols.

→ HTTP / HTTPS
→ DHCP
→ FTP
→ SMTP (Simple Mail Transfer Protocol)
→ POP3 & IMAP
→ SSH
→ VNC (virtual Network computing) for graphical control
→ TELNET (port 23)
→ UDP

Date : / /
Page No.

HTTP METHODS

While browsing, the end user (browser action) sends request to the web server and the server sends the correlated response.
HTTP defines a set of request methods to indicate the chosen action to be performed.

There are 9 pre-defined methods used with HTTP and HTTPS.

(i) **GET**

the GET method is used to retrieve or get information from the web server.

(ii) **HEAD**

the head method is identical to get except that the server transfers my status line and header section only, without the response body.

(iii) **POST**

This request is used to transmit important structured data to the server.
for eg. customer data, file uploads, etc

using HTML forms to create or update a resource.

(iv) **PUT**

Similar to post, it replaces all the current representations of the target resource with the uploaded content.

It put data at a specific location

(v) **DELETE**

This method is used to delete the resource at the specified URL or from the server.

(vi) **TRACE**

This method allows the client to see what is being received at the server end of the request chain and to use that data for testing.

(vii) **CONNECT**

This transforms the request connection to a transparent TCP/IP tunnel, typically to create SSL-encrypted data exchange (HTTPS) through an unencrypted HTTP proxy.

This is called HTTP tunneling.

(viii) **PATCH**

This methods applies partial modifications to a resource.

This Patch method is faster and less resource consuming than the Put method when making partial changes to the specified resource.

(ix) **OPTIONS**

This HTTP method ~~is~~ request should return data describing what other methods the server supports at the given URL without indicating a resource action or requesting a resource retrieval.

STATUS CODES

The status-code element is a server response, is a 3-digit integer where the first digit of the status-code defines the class of the response and the last two digit do not have any categorization role.

Date : / /
Page No.

there are 5 values for the first digit.

(i) 1xx : INFORMATIONAL

It means the request has been received and the process is continuing.

(ii) 2xx : SUCCESS

It means the action was successfully received, understood and accepted.

(iii) 3xx : REDIRECTION

It means further action must be taken in order to complete the request

(iv) 4xx : CLIENT ERROR

It means the request contains incorrect syntax or cannot be fulfilled.

(v) 5xx : SERVER ERROR

It means the server failed to fulfill an apparently valid request.

Date : / /
Page No.

COOKIES

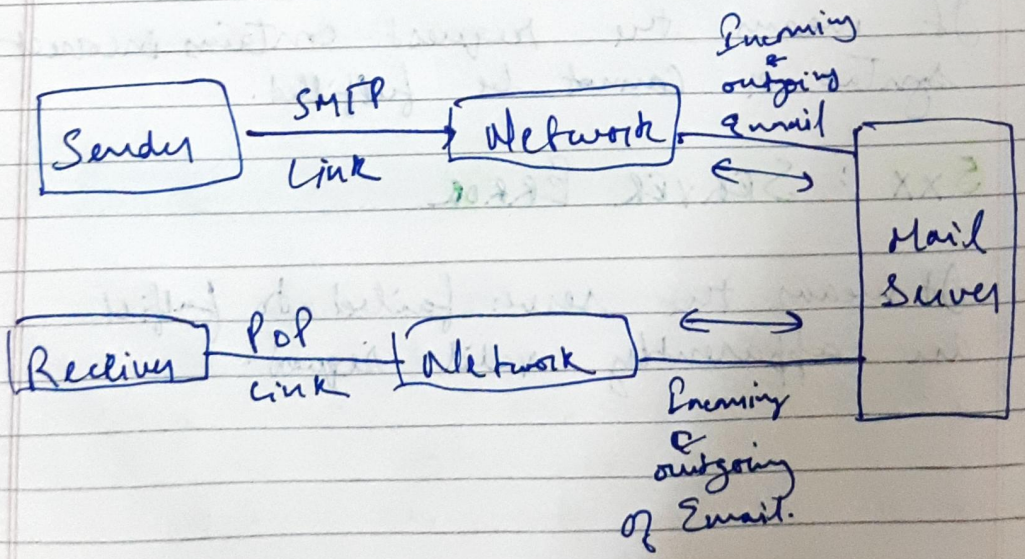
→ A cookie is a piece of data from a website that is stored within a web browser that the website can retrieve at a later time.

→ Cookies are used to tell the server that users have returned to a particular website.

→ It is a unique string

→ It is stored in client's / our browser.

How EMAIL WORKS?



Date : / /
Page No.

SMTP → SMTP stands for **Simple mail transfer Protocol**.
It basically uses the internet network connection to send and receive messages over the internet.

PoP → PoP stands for **Post office Protocol** for email.
It approach is just to drop the email over the servic mail providers and then leave it for services to handle the transfer of messages.

IMAP → IMAP stands for **Internet Messag Access Protocol**.
IMAP has some special advantages over POP like it supports bidirectional communication over email and there is no need to store conversations on servers as they are already well maintained in a database.

Date : / /
Page No.

DNS (DOMAIN NAME SYSTEM)

→ DNS is a hostname for IP Address translation servic.

→ It is a servic that translates and map the domain name into IP addresses.

→ This allows the users of networks to utilize user-friendly names when looking for other host instead of remembering the IP addresses.

→ It uses UDP.

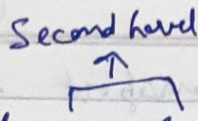
There are various kinds of Domain:

Generic Domain : .com (commercial)
.edu (educational)
.org (nonprofit organization)
.info (Information servic provid)
.gov (government institutions)
and many mor.

Country Domain : .in (India)
.us
.uk
these are country specific

Inverse Domain : It is used for mapping an address to a name.

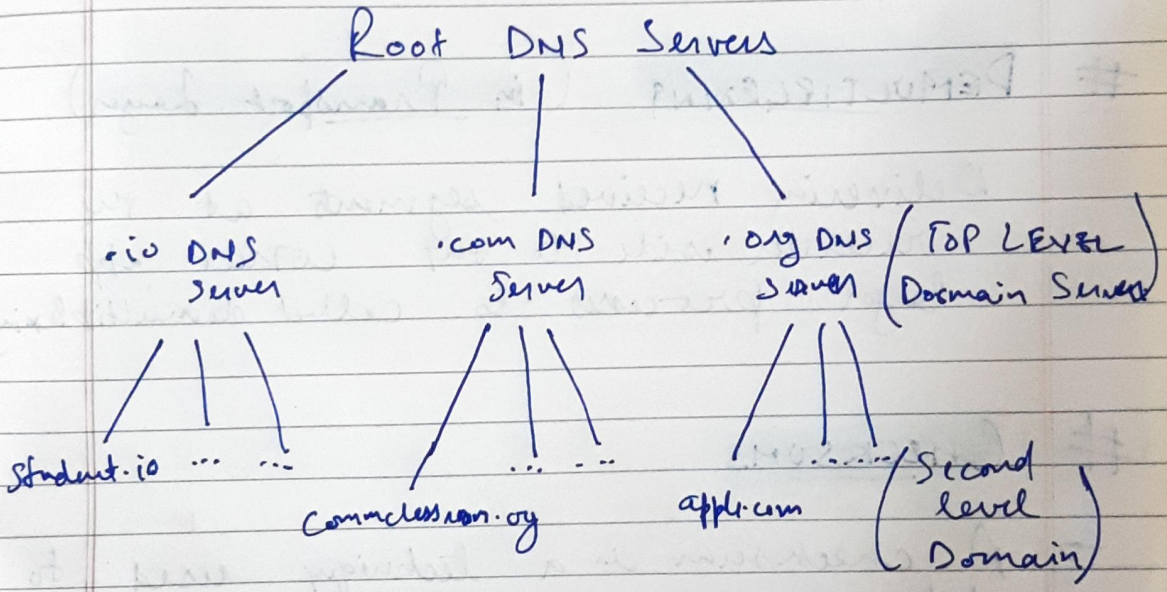
Date : / /
Page No.



mail . google . com

Sub-domain Top level Domain.

ORGANIZATION OF DOMAIN



→ Root DNS servers are the first point of contact.

→ Root DNS servers are maintained by root-servers.org.

→ Top level Domain Name are managed by ICANN (Internet Corporation for Assigned Name & Number). We can check at icann.org.

Date : / /
Page No.

MULTIPLEXING (in Transport Layer)

Gathering data from multiple application processes of the sender, enveloping that data with a header, and sending them as a whole to the intended receiver is called multiplexing.

DEMULTIPLEXING (in Transport Layer)

Delivering received segments at the receiver side to the correct app layer processes is called demultiplexing.

CHECKSUMS

→ A checksum is a technique used to determine the authenticity of received data i.e. to detect whether there was an error in transmission.

→ UDP uses checksums.

TIMERS

Timers used by TCP to avoid excessive delays during communication are called as TCP timers.

There are 4 types of timers :-

(i) RETRANSMISSION TIMER

→ also known as Time Out Timer.

→ TCP uses a time out timer for retransmission of lost segments / packets.

→ 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 receive any acknowledgement and the time goes off then 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.

Date : / /
Page No.

(ii) 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.

(iii) KEEP ALIVE TIMER

→ TCP uses a keep alive timer to prevent long idle 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 segment, it assumes that the client is down.

→ Then, server terminates the connection automatically.

(iv) **TIME WAIT TIMER**

→ TCP uses a time wait timer during connection termination.

→ Sender starts the time wait timer after sending the ACK for the 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.

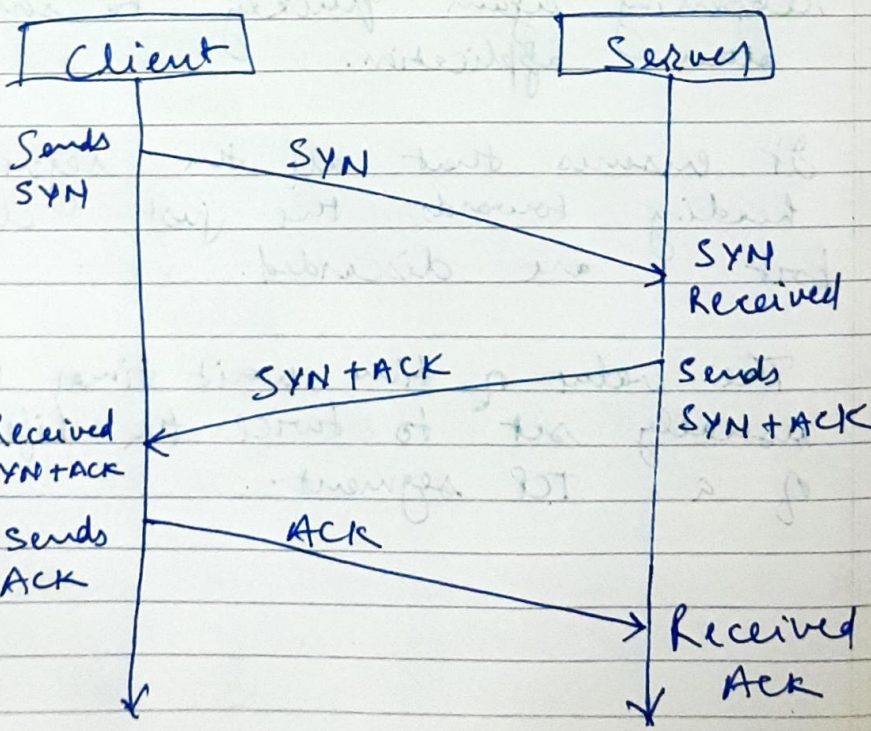
→ The value of time wait timer is usually set to twice the lifetime of a TCP segment.

Date : / /
Page No.

3-WAY HANDSHAKE

A three-way handshake is a method used in a TCP/IP network to create a connection between a local host/client and server.

It is a three step method designed to allow both communicating ends to initiate and negotiate the parameters of the network TCP socket connection at the same time before data such as HTTP and SSH is transmitted.



Date : / /
Page No.

Step 1 (SYN)

In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN (Synchronize Sequence Number) which informs the server the client is likely to start communication and with what sequence it starts segment with.

Step 2 (SYN + ACK)

server responds to the client request with SYN + ACK signal bits set. Acknowledgement (ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with.

Step 3 (ACK)

In the final part client Acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer.

Date : / /
Page No.

ROUTING

Routing is a process that is performed by Network Layer devices in order to deliver the packets by choosing an optimal path from one network to another.

CONTROL PLANE

→ The control Plane is that part of a network that controls how data packets are forwarded.

→ For eg. the process of creating a routing table is considered part of the control plane.

IPv4

→ IP stands for Internet Protocol and v4 stands for version 4.

→ IPv4 addresses are 32-bit numbers and are expressed in decimal notation.

→ eg. 192.0.1.126

Date : / /
Page No.

IPv6

→ It was developed by Internet Engineering Task force (IETF) to deal with the problem of IPv4 exhaustion in future.

→ It is 128-bit address. having an address space of 2^{128}.

→ It is not backward compatible

→ eg.

a:a:a:a:a:a:a:a

↙

Hexadecimal
16 bit

SUBNET MASK

A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other identifies the network it belongs to.

Eg. 192.168.2.30

Subnet ID → Host ID

Date : / /
Page No.

MIDDLEBOX

→ A middlebox is a computer networking device that ~~performs~~ transforms, inspects, filters, and manipulates traffic for purposes other than packet forwarding.

→ Mostly found in Network layer but can also be found in transport layer.

Examples:

(i) FIREWALLS

Firefalls filter traffic based on set of predefined security rules by a network administrator.

(ii) IDS (Intrusion Detection System)

IDS monitor traffic and collect data for offline analysis for security anomalies.

(iii) NAT (Network Address Translators)

* Explained in starting of NOTES

(iv) WAN OPTIMIZERS

They improve bandwidth consumption and perceived latency between endpoints.

(v) LOAD BALANCERS

they provide one point of entry to a service, but forward traffic flows to one or more hosts that actually provide the service.