Port No.: 16 bit
MAC add: 48 bit
IP add: 32 bit

4. Transport Layer

Transport Layer :

- Transport Layer is the ~~second~~ fourth layer of TCP/IP model.
- It is an end-to-end layer used to deliver messages to a host. It termed as an end-to-end layer because it ~~provides a point-to-point~~ provides a point-to-point connection rather than a hop-to-hop between the source host to destination.
- Unit of ~~data~~ PDU in the Transport Layer is a segment.
- Standard protocols used in Transport layer is TCP, UDP, DCCP, etc.

■ Responsibilities of Transport Layer :

- **Process to Process delivery**: Data link layer requires MAC address of source-destination hosts to deliver a frame, Network layer requires IP address for appropriate routing of packets, Transport Layer requires a Port number to correctly deliver the segments of data to a correct process amongst the multiple processes running on a particular hosts.

  Port Number : It is a 16 bit address used to identify client-Server programs uniquely

- **End-To-End Connection**: The Transport Layer is also responsible for end-to-end communication between hosts, mainly uses TCP and UDP.

  TCP: It is a secure, connection-oriented protocol that uses a handshake protocol to establish a robust connection between two end hosts. It ensures reliable delivery of messages

  UDP: It is a stateless and unreliable protocol that ensures best delivery It is suitable for the application that have no much concern with flow or error control and requires sending the bulk of data like video conferencing. It is often used in multicasting protocol.

- **Multiplexing and Demultiplexing**:

  Multiplexing : multiplexing allows simultaneous use of different applications over a network that is running on a host. The transport layer provide us this mechanism to send packet streams from various application simultaneously over network. Transport layer accept these packets from different processes differentiated by their port number and passes them to network layer after adding proper header.

  Demultiplexing : It is required at receives side to obtain the data coming from various processes. Transport receives the segments of data from the network layer and delivers it to the appropriate process running on the receiver's machine.

- **Congestion Control**

Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occure. As a result retransmission of packets from sources increases the congestion further
In this situation, the transport layer provides congestion control in different ways: It uses Open Loop Congestion control to prevent congestion and closed loop congestion to remove the congestion.
TCP provides leaky bucket technique for congestion control.

- **Data integrity and Errors correction:**

Transport layer checks for the Errors in the messages coming from the application layer by using Error detection codes, computing checksums. It checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not checks for the integrity of data.

- **Flow Control:**

Transport layers provides the flow control mechanism between different layers of TCP/IP model.

Congestion Control in Computer Networks:

Congestion:

→ A state occurs in the network layer when the ~~too~~ message traffic is so heavy that it slows down network response time.

Congestion causes choking of the communication medium. when too many packets are displayed in a method of subnet, subnet's performance degrades Hence., a network's communication channel is called congested if packets are traversing the path and experience delays mainly over the path's propagation delay.

One of the main cause of congestion is that traffic is often bursty.

Traffic Shaping: It is a mechanism to control the amount and the rate of the traffic sent to the network. Approach of congestion control management is called Traffic Shapping.

Two types of Congestion Control or Traffic Shaping:

1. Leaky Bucket
2. Tooken Bucket.

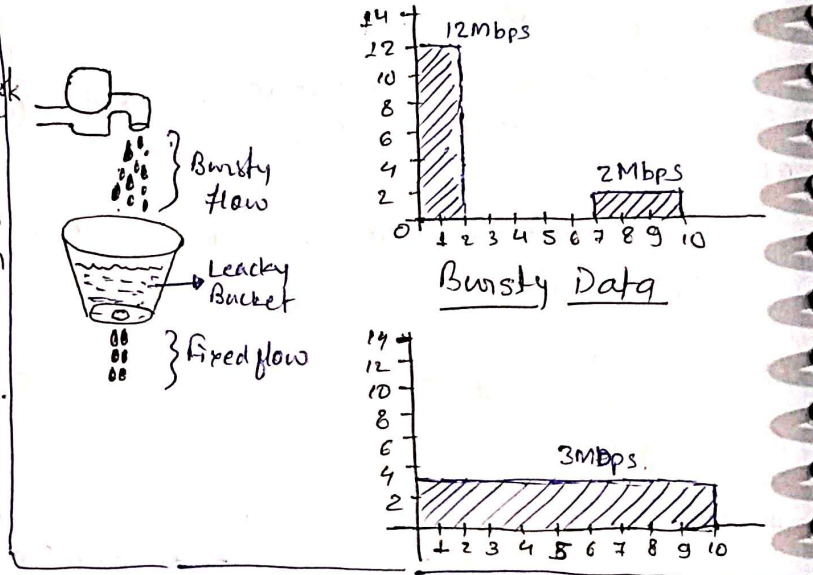
1 Leaky Bucket:

→ This algorithm allows controlling the rate at which a record is injected into a network and manages boustiness in the data rate.

Explanation:-

Suppose we have a bucket in which we are pouring water in a random order but we have to get water in fixed rate, for this we will make a hole at the bottom of the bucket, It will ensure that the water coming out is in fixed rate also if bucket will fill we will stop pouring in it.

The input rate can vary but the output rate remains constant, similarly in networking, Leacky Bucket technique smooth the ~~bs~~ bursty traffic. Bursty traffic chunks are stored in Bucket and ~~set~~ sent out with an average rate.



In the fig. we assume that the network has committed a bandwith of 3 Mbps for a host.

The use of the Leaky Bucket shapes the input traffic to make it conform to this commitment.

In fig. the host sends a burst of data at a rate of 12Mbps for 2sec. (total of 24Mbits). Then the host is silent for 5 sec. and then sends data at the rate of 2Mbps for 3 sec. (6 Mbits of data). In all, the hosts sends total of 30 Mbits of data for 10sec. The leacky Bucket smooths the traffic by sending out data at a rate of 3Mbits for 10sec.

- Without the Leacky Bucket, the beginning burst may hurt the network by consuming more bandwidth than is set aside for this host. So in this way congestion is prevented.

2 Token Bucket Algorithm:

→ It is a control algorithm that indicates when traffic should be sent, This order comes based on the display of tokens in the bucket. The Bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the Bucket are deleted for the ability to share a packet.

When tokens are shown, a flow to transmit traffic appears in the display of tokens. No tokens means no flow sends its packets. Hence a flow transfers traffic upto its peak burst rate in good tokens in the bucket.

- Thus ; the token bucket algorithm adds a token to the bucket each 1/r seconds, The volumn of bucket is b-tokens. when a token is appeans, and the bucket is complete, token is discarded. If a packet of n bytes appears and n tokens are deleted from the bucket. the packet is forwarded to the network.

when a packet of n bytes appears but fewer than n tokens are available, No tokens are removed from the bucket in such a case, and the packet is considered non-conformant. The non-conformant packets can be either dropped or queued for next transmission when sufficient tokens have accumulated in the bucket.

■ Need of Token Bucket Algorithm:

- The leaky bucket Algorithm enforces output patterns at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic, we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Some Advantages of Token Bucket over Leaky Bucket:

- If bucket is full in Token Bucket, the tokens are discarded not packets, while in leaky Bucket, packets are discarded.
- Token Bucket can send large bursts at a faster rate while leaky Bucket always send a packet at constant rate.

Transmission Control Protocol (TCP)

→ The Transmission Control Protocol is the most common transport layer protocol. It works together with IP and provides a reliable transport service between processes using the network layer service.

1 Services and Segment Structure in TCP

(1) Process-to-Process Communication:

- The TCP provides Process-To-Process communication i.e. transfer of data that takes place between individual processes executing on end systems. This is done using port numbers.

(2) Stream Oriented:

- This means that the data is sent and received as a stream of bytes. (unlike UDP or IP that divides the bits into datagram or packets)

(3) Full duplex Service:

- This means that the communication can take place in both direction at a same time.

(4) Connection-Oriented Service:

- Unlike UDP, TCP provides a connection oriented service, which has 3 phases:
  - Connection Establishment
  - Data transfer
  - Connection terminated.

(5) Reliability:

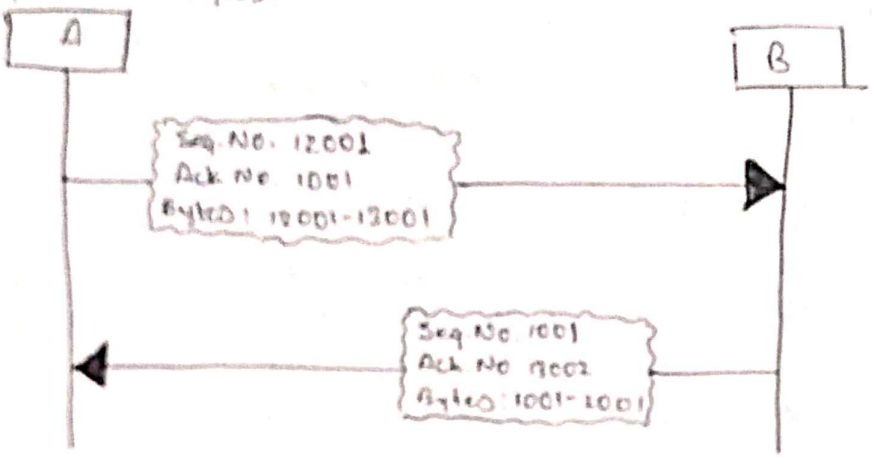
- TCP is reliable as it uses checksum for error detection, attempts to recover lost or corrupted packets by re-transmission, acknowledgement policy and timers. Uses features like byte number, sequence number and acknowledgment number to ensure reliability. Also it uses Congestion Control mechanism.

(6) Multiplexing

- TCP does multiplexing and demultiplexing at the sender and receiver ends respectively as a number of logical connections can be established between port numbers over a physical connection.

Byte Number, Sequence Number and Acknowledgement Number :

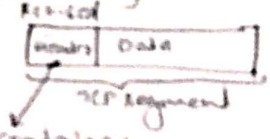
- Sequence numbers are given to segments so at receiver end they can be reassembled if they arrive in different orders. The sequence number of a segment is the byte number of first byte that is being sent.
- The Acknowledgement number is required since TCP provides full-duplex service. The acknowledgment number is the next byte number that the receiver expects to receive which also provides acknowledgement for receiving the previous bytes.



TCP segment Structure

- A TCP segment consist of a data and a header that is added by TCP to data segments.

The header of TCP segment can range from 20-60 bytes



containing:
- Source & Destination port No
- Seq & Ack number
- Reserve bits
- window size, HLEN
- etc

Header fields :

- Source Port Address : 16-bit field that holds the port add of application that is sending the data segment.
- Destination Port Address: 16-bit field that holds the port add of destination that is receiving segments.
- Sequence number : 32 bit field that holds Seq number
- Acknowledgement number : 32 bit field that hold Ack No.
- Header Length (HLEN) : 4-bit field, that indicates the length of Header.
- Control flag : These are 6 1-bit control bits that controls connection establish connection termination, flow control, mode of transfer etc.
- Window size : This field tells the window size of sending TCP in bytes.
- Checksum : This field holds checksums for error control
- Urgent Pointer : This field is used to point to data that is urgently required that needs to reach the receiving process at the earliest.

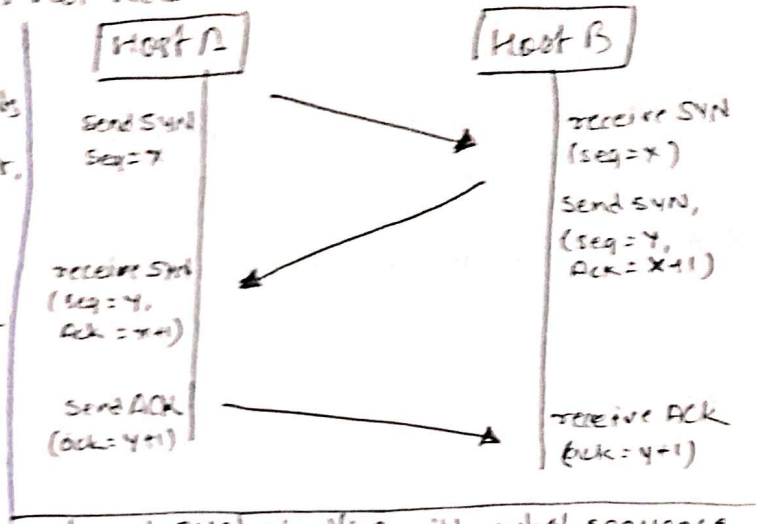
TCP connection :

- TCP is a connection oriented. A TCP connection is established by 3 way-hand shake.

2. TCP - 3 Way Handshake Process:

- From application layer, info is transferred to the Transport layer where TCP comes into picture. Two imp protocol of Transport layer are TCP & UDP out of which TCP is prevalent (as it provides reliability for connection establishment)
- TCP provides reliable communication with PAR (Positive Acknowledgement Retransmission)
- PDU of Transport layer is segment.
- Now a device using PAR, resend the data unit until it receives an acknowledgement. If the data unit is received at the receiver's end is damaged (it checks the data with checksum functionality of transport layer that is used for error detection), then the receiver discards the segment & the sender has to resend the data unit for which positive acknowledgement is not received.

■ How it works:

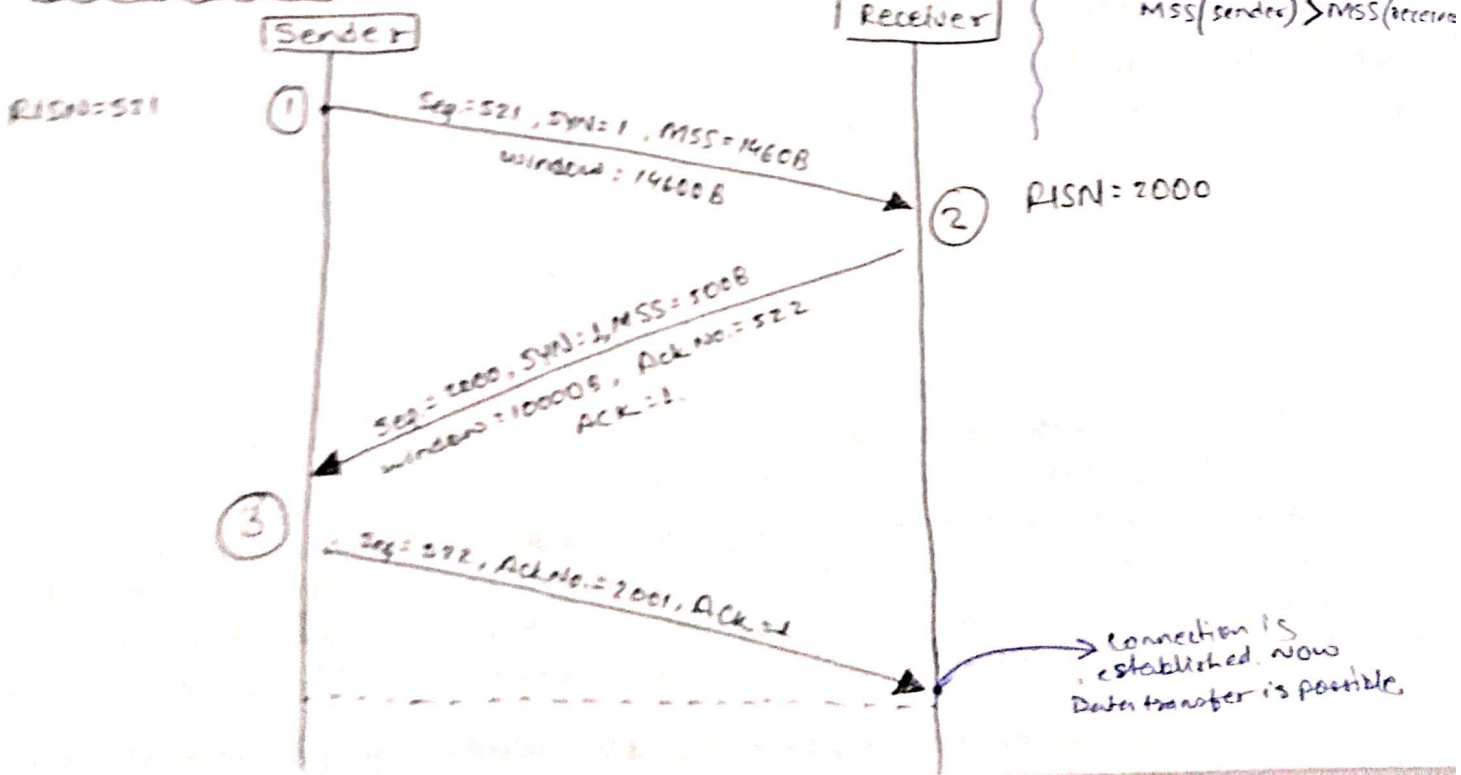


Step 1: SYN: In first step, client wants to establish a connection with a server, so it sends a segment with SYN (Synchronize Sequence No) which informs the server that the client is likely to start communication and with what sequence number it starts segments with.

Step 2: (SYN+ACK): Server responds to the client request with SYN+ACK. Acknowledgement number (Ack) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segment 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.

■ Connection Establishment:



TCP Connection Termination :

→ TCP supports two types of connection release :

① Graceful Connection Release : In this, the connection is open until both parties have closed their sides of connection.

② Abrupt connection Release : In this, either one entity is forced to close the connection or one user closes both directions of data transfer.

3 Error Control in TCP :

- TCP protocol has methods for finding out ~~our~~ corrupted segments, missing segments, out-of-order segments and duplicate segments.

Error Control in TCP is mainly done by the use of three simple techniques :-

① Checksum : Every segment contains a checksum field which is used to find corrupted segments. If the segment is corrupted, then that segment is discarded by the destination TCP and is considered as lost.

② Acknowledgement : It is used to affirm that the data segments have been delivered. Control segments that contain no data but have seq. number will be acknowledged as well but Ack segments are not acknowledged.

③ Retransmission : when a segment is missing, delayed to deliver to a receiver, or is corrupted when it is checked by receiver then that segment is retransmitted again.

segments are retransmitted only during two events :

- when the sender receives three duplicate acknowledgements (ACK)
- when a retransmission timer expires.

4 TCP - Timer :

- TCP uses several timers to ensure that excessive delays are not encountered during communications.

TCP implementation uses four timers :

① Retransmission Timer : To retransmit lost segments, TCP uses Retransmission Timeout (RTO). When TCP sends a segment, the timer starts and stops when the acknowledgement is received. If the timer expires timeout occurs and the segment is retransmitted.

Retransmission Time Out is for 1 Round Trip Time (RTT).

② Persistent Timer : To deal with a zero-window-size deadlock situation, TCP uses a persistence timer. when the sending TCP receives an acknowledgment with a window size of zero, it starts a persistance timer. When persistence timer goes off, the sending TCP sends a special segment called probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged. It is even ignored in calculating the sequence number for the rest of the data.

The probe causes the receiving TCP to resent the acknowledgment which was lost.

③ Keep Alive Timer : A keep Alive Timer is used to prevent a long idle connection between two TCP's. If a client opens a TCP connection to a server, transfers some data and become silent, the client will crash. In this case the connection remains open forever. So a keep Alive Timer is used. Each time the server heard from a client, it resets this Timer. The Timeout is usually 2 hours. If the server does not does not hear from the client after 2 hours, it sends a probe segment. If there is no response after 10 probes, each of which is 75 sec apart, it assumes that the client is down and terminates the connection.

④ Time Wait Timer : This timer is used during TCP connection Termination. The timer starts after sending the last Ack for 2nd FIN and closing the connection.

5 TCP Flags :

- Flags are used to indicates a particular state of connection or to provide some addition information like troubleshooting or to handle control etc
most commonly used flags are SYN, ACK, FIN.
Each flag corresponds to 1 bit information.

Types of flag :

① Synchronization (SYN) : It is used in first step of connection establishment or 3-way handshake process between two hosts.
Only first packet from sender as well as receiver should have this flag
This is used for synchronizing sequence numbers i.e. to tell the other end which sequence number they should accept.

② Acknowledgement (ACK) : It is used to acknowledge packets which are ~~so~~ successful received by the host. The flag is set if the acknowledgement ~~num~~ number filed contains a valid acknowledgement number.

③ Finish (FIN) : It is used to request for connection termination i.e. when there is no more data from the sender, it requests for connection termination. This is the last packet sent by sender. It frees the reserved resources and gracefully terminate the connection.

④ Reset (RST) : It is used to terminate the connection if the sender feels something is wrong with the TCP connection or that the conversation should not exist. It can get send from receiver side when packet is send to particular host that was not expecting it.

⑤ Urgent (URG) : Data inside a segment with URG=1 flag is forwarded to applicat^{n} layer immediately even if there are more data to be given to app. layer. It is used to notify the receiver to process the urgent packets before processing all other packets.

⑥ Push (PSH) : In general, it tells the receiver for process these packets as they are received instead of buffering them.

UDP (User Datagram Protocol):

→ User Datagram Protocol (UDP) is a Transport layer protocol
→ Unlike TCP, it is an unreliable and connection less protocol. So there is no need to establish a connection prior to data transfer.

Though TCP is a dominant transport layer protocol used with most of Internet services, provides assured delivery, reliability etc but all these services cost us additional overhead and latency. Therefore it is slower in some cases. Here UDP comes into pit picture. For real time services like gaming, voice or video communication, live conferences, we need UDP.

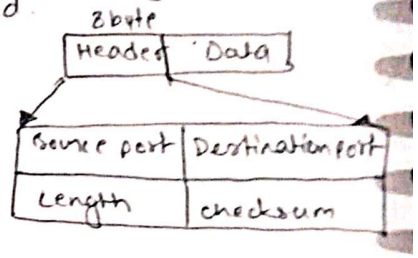
Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets.

There is no error checking in UDP, so it also saves bandwidth.

UDP is more efficient in terms of both latency and bandwidth.

UDP header:

→ UDP header is an 8-bytes fixed & simple header, Unlike TCP, which vary from 20 to 60
→ The first 8 bytes contains all the necessary information (in header) and remaining part contains data.
→ UDP port number fields are each 16 bits long, therefore the range for port number is defined from 0 to 65535, port number 0 is reserved.



Important fields in UDP Header:-

① Source Port: It is a 2 Byte long field, used to identify the port number of source.

② Destination Port: It is a 2 byte long field, used to identify the port number of Destination.

③ Length: Length is a length of UDP including header and the data. It is a 16 bits field.

④ Checksum: It is a 2 Bytes long field, used for error detection.

NOTE: Unlike TCP, the checksum calculation is not mandatory in UDP. No error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

Applications of UDP:-

→ Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control
→ It is a suitable for multicasting as UDP supports packet switching.
→ UDP takes a datagram from network layer, attaches its header and sends it to the user, so it works fast.
→ Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.
→ UDP is used in transport layer, Application layer can do some task through UDP, UDP is also used for some routing update protocols like RIP (Routing Information protocol).

5. Application Layer

→ The application layer is present at the top of OSI model. It is the layer through which users interact. It provides services to the user. Uses web applications or internet application or network application.

Protocols in Application Layer

[1] HTTP

→ The HyperText Transfer Protocol (HTTP) is an application layer protocol that uses TCP as an underlying transport and typically runs on port 80.
HTTP is a stateless protocol i.e. server maintains no information about past client requests.

[2] TELNET :

→ TELNET stands for the TELetype NETwork. It help in terminal emulation
It allows Telnet clients to access the resources of the Telnet Server.
It is used for managing files on the internet. It is used for the initial setup of devices like switches.
The telnet command is a command that uses the Telnet protocol to communicate with a remote device.
Port number of Telnet is 23.
command :
telnet [\\RemoteServer],
\\RemoteServer : Specifies the name of the server to which you want to connect

[3] FTP

→ It stands for File Transfer Protocol. It is the protocol that actually lets us transfer files,
FTP is not just a protocol but is also a program.
Port number of FTP is 20 for data and 21 for control.
command :
ftp machinename,

[4] TFTP

→ Stands for Trivial File Transfer Protocol. It is the stripped-down, stock version of FTP, but its the protocol of choice if you know exactly what you want and where to find it.
Its a technology for transferring files between network devices and is a simplified version of FTP
Port number of TFTP is 69.
command
tftp [options...] [host [port]] [-c command]

5 NFS :

→ Stands for Network File System. It allows remote hosts to mount files over a network and interact with those file systems as though they are mounted locally.
This enables system administrators to consolidate resources onto centralized servers on the network
Port number for the NFS is 2049.

Command

service nfs start

6 SMTP

→ Stands for Simple Mail Transfer Protocol. It is the part of the TCP/IP protocal. Using a process called "Store and forward", SMTP moves your email on and across networks.
It works closely with MTA (Mail Transfer Agent) to send your communication to the right computer and email inbox.
The port Number of SMTP is 25.

Command

MAIL FROM: <mail@abc.com?

7 LPD

→ Stands for Line Printer Daemon. It is designed for printer sharing. It is the part that receives and processes the request. A 'daemon' is a server or agent
Port number of LPD is 515.

8 X window :

→ It defines a protocol for the writing of graphical uses Interface-based client/server applications.
The idea is to allow a program called a client, to run on one computer.
It is primarly used in interconnected mainframes.
Port No. for x window starts from 6000 and inc. by 1 for each server.

command

Run xdm in runlevel 5

9 SNMP :

→ Stands for Simple Network Management Protocol. It gathers the data by polling the devices on the network from a management stations at fixed or random intervals, requiring them to disclose certain information.
It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defines values.
Port no. of SNMP is 161 (for TCP) and 162 (for UDP)

command

snmpget -mALL -v1 -cpublic snmp_agent_ip.Address sysName.0

10 DNS

→ stands for Domain Name System. DNS service translate the domain name into corresponding IP address.
For example domain name www.abc.com might translate to 198.105.232.4
Port No. of DNS is 53.

command

ipconfig /flushdns

11 DHCP :

→ It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server.
Port number of DHCP is 67, 68.

command

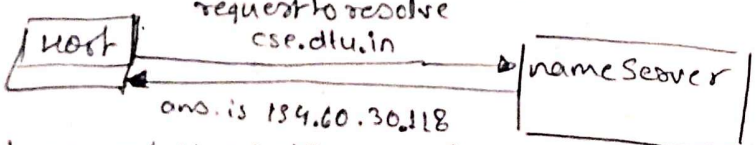
clear ip dhcp binding { address | * }

Domain Name System (DNS)

→ DNS is a host name to IP address translation service. It is an application layer protocol for message exchange between clients & servers.
There is not only one DNS server, There are series of DNS servers used to resolve the domain name. DNS uses cache to work efficently so that it can quickly refer to DNS lookups its already performed rather than performing a DNS lookup over and over again.
Although DNS caching increase the speed of domain name resolution process But the major change in the domain then takes a day to reflect world wide.

Imp Terms

- DNS record: Domain name, ip address, what is the validity? what is time to live ? and all the info related to domain name, These records are used to store them.
- Namespace: set of possible names, flat or hierarchical. Naming System maintains a collection of bindings of names to values. - given a name, a resolution mechanism returns the corresponding value.
- Name Server: It is an implementation of the resolution mechanism.



The Host request the DNS name server to resolve the domain name. And the name server returns the ip address corresponding to that domain name to the host so that the host can further connect to ip address.

Hierarchy of Name Servers:

- **Root Name Server:** It is contacted by name servers that cannot resolve the name. It contacts authoritive name server if name mapping is not known. It then gets the mapping and return the IP address to the host.
- **Top Level Servers:** It is responsible for .com, .org, .edu etc and all top level country domains like .uk, .fr, .ca, .in etc.
  They have info about authoritative domain servers and known names and IP addresses of each authoritative name servers for the second level domai
- **Authoritative name Server:** This is organizations DNS server, providing authoritative hostName to IP mapping for organization servers. It can maintained by organizations or service provider.

For example, In order to reach cse.dtu.in we have to ask the root DNS server. then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritati domain server will return the associative ip address.

Address Resolution in DNS

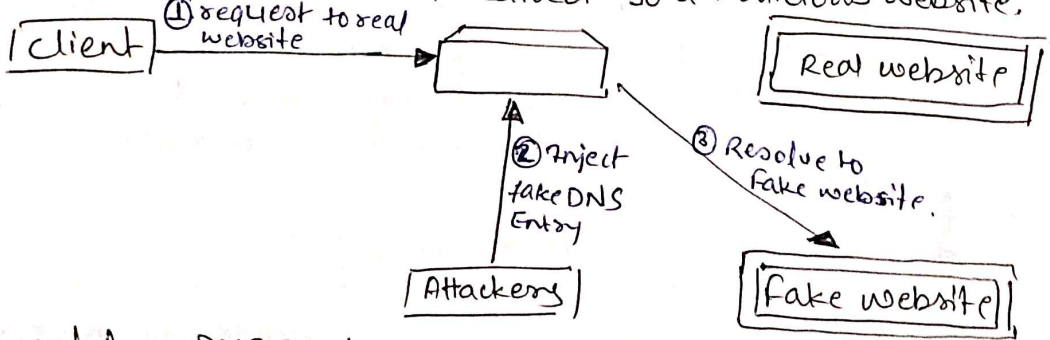
- Mapping a domain name to an IP address is known as Name-Address Resolution The DNS resolver performs this operation by consulting name servers.

A resolution can be of two types:-

1. Recursive Resolution
2. Iterative Resolution.

DNS Spoofing or DNS cache poisoning:

DNS Spoofing: It means getting a wrong entry or IP address of the request site from the DNS server. Attackers find out the flaws in the DNS system and take control and will redirect to a malicious website.



To Prevent from DNS Spoofing:-

→ DNS Security Extensions (DNSSEC) is used to add an additional layer of ~~secu~~ security in the DNS resolution process to prevent security ~~threats~~ threats such as DNS spoofing or DNS cache poisoning.

DNSSEC protects against such attackers by digitally 'signing' data so you can be assured it is valid.

Why does DNS use UDP and not TCP :

→ DNS is an application layer protocol. All application layer protocol use one of the two transport layer protocol, UDP and TCP. TCP is reliable and UDP is not reliable. DNS is supposed to be reliable, but it uses UDP why?

There are the following interesting facts about TCP & UDP on transport layer

① UDP is much faster, TCP is slower as it requires 3-way handshake. The load on DNS server is also important factor. DNS servers (since they use UDP) don't have to keep connections.

② DNS requests are generally very small and fit well within UDP segments.

③ UDP is not reliable, but reliability can be added to the application layer. An application can use UDP and can be reliable by using a timeout and resend at the application layer.

DNS primarily uses UDP on port no. 53 to serve request. DNS queries consist of a single UDP request from the client followed by a single UDP reply from server. When length of answer exceeds 512 bytes and both clients & server supports EDNS, larger UDP packets are used otherwise TCP the queries is sent again using TCP.

Dynamic Host Configuration Protocol (DHCP)

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

- Subnet mask
- Router Address.
- DNS Address
- Vendor Class Identifier.

DHCP servers dynamically distributes network configuration parameters such as IP address, subnet mask, and gateway addresses.

DHCP is based on client-Server model and based on discovery, offer, request and ACK.

DHCP port number for server is 67 and for client is 68. It is a client-Server protocol, uses UDP services.

In DHCP, the client and the server exchange mainly 4 DHCP messages. In order to make connection also called as DORA process. but there are 8 DHCP messages in the process.

These messages are :-

① DHCP Discover message : This message is generated by client host in order to discover if there is any DHCP server/servers are present in the network or not.
This message is 342 or 576 byte long.

② DHCP offer message : The server will respond to host in this message specifying the unleased IP address and other TCP configuration information
This message is broadcast by the server.
Size of message is 342 bytes

(3) DHCP Request message: when client receives a offer letter/message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP add. A client ID is also added in this message.

NOTE: This msg. is broadcast after the ARP request broadcast by the PC to find out whether any other host is not using that offered IP. If there is no reply, then the client host broadcast the DHCP request msg to server showing the acceptance of IP add.

(4) DHCP Acknowledgement message: In response to the request msg received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.

(5) DHCP negative Acknowledgement message: whenever a DHCP server receives a request message that is invalid according to the scopes that is configured with, it send DHCP Nak message to client.

(6) DHCP Decline: If DHCP client determines the offered configuration parameters are different or invalid it sends a DHCP decline message to the server

(7) DHCP release: A DHCP client sends DHCP release packet to servers to release IP address and cancel any remaining lease time.

(8) DHCP inform: If a client has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as Domain name.
In reply to DHCP inform msg, server generates a DHCP Ack msg. with configurations suitable for client without allocating new IP address.

- Advantages of using DHCP
  - centralized management of IP add.
  - ease of adding new clients to network.
  - reuse of IP addresses reducing total number of IP add. that are required
  - Simple reconfiguration of IP add space on DHCP server without needing to reconfigure each client
- Disadvantages of using DHCP:
  - IP conflict can occur.

Simple Network Management Protocol (SNMP)

SNMP

→ It is an application layer protocol that uses UDP port number 161/162. SNMP is used to monitor the network, detect network faults, sometimes it is used to configure remote devices.

SNMP Components:

1. **SNMP manager**: It is a centralized system used to monitor network. It is also known as Network management Station (NMS)
2. **SNMP agent**: It is a software management module installed on a manged devices. like PC, routers, servers, switches etc.
3. **Management Information Base**: It consist of information on resources that are to be managed. This information is organized hierarchically It consists of objects instances which are essentially variables.

SNMP messages:

1. **GetRequest**: SNMP manger sends this msg to request data from SNNIP agent. In response to this SNMP agent responds with requested value through response msg.
2. **GetNextRequest**: This msg can be sent to discover available data on an SNMP agent The SNMP manager can request data continuously until no more data is left In this way the SNMP manager know all the available data on SNMP agent.
3. **GetBulkRequest**: This msg is used to retrive large data at once by SNMP manger from the SNMP agent.
4. **SetRequest**: It is used by the SNMP ~~manger~~ manager to set value of an object instance on the SNMP agent.
5. **Response**: It is a msg. sent from the agent upon a request from the manger.
6. **Trap**: These are the message sent by agent without being requested by the manger. It is sent when a fault has occured.
7. **InformRequest**: Used to identify if the Trap msg has been received by the manger or not.

SNMP security Level:

→ It defines the type of a security algorithm performed on SNMP packets. These are used only in SNNIPv3. There are 3 security levels:

1. **noAuthNoPriv**: This (No Authentication, NO Privacy) security level uses a community string for authentication and no encryption for privacy.
2. **authNoPriv**: This security level (Authentication, No Privacy) uses HMAC with MdE for authentication and no encryption is used for privacy.
3. **authPriv**: This security level (Authentication, Privacy) uses HMAC with Nids or SHA for authentication and encryption uses the DES-56 algorithm!

- SNMP versions

① SNMPv1 : uses comunity strings for authentication. and uses UDP only.

② SNMPv2 : uses community strings for authentication. It uses UDP but can be configured to use TCP.

③ SNMPv3 : It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 encryption for privacy. This version uses TCP

Simple Mail Transfer Protocol (SMTP)

→ Internet systems uses SMTP to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (Post office Protocol) and IMAP (Internet Message Access Protocol) are used to retrive those emails at the receiver's side.

- SMTP ~~SMTP~~ Fundamental

→ SMTP ~~SMTP~~ is an application layer protocol. The client who wants to send mail opens a TCP connection to SMTP server and sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After successfully establishing a TCP connection the client process sends the mail instantly.

- SMTP model (two types)

① End-to-End method
② Store-and-forward method.

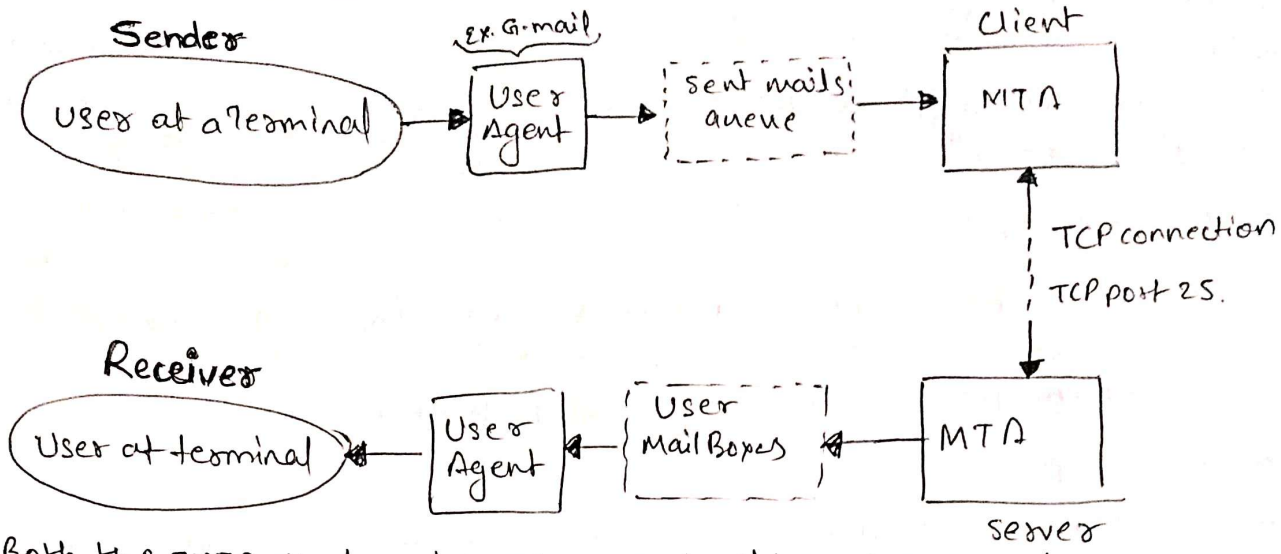
The End-to-End model is used to communicates between different organizations. And Store-and-Forward method is used to communicate within an organization. An SMTP client who wants to send mail, will directly contact to destinations host SMTP, in order to send mail to the destination. The SMTP server keep the mail to itself until it is successfully copied to the receiver's SMTP.

- Model of SMTP system :

→ In SMTP model, user deals with User Agent (UA) Ex. Microsoft Outlook, Yahoo, Gmail.

→ In order to exchange the mail using TCP, MTA (Message Transfer Agent) is used. The user sending the mail doesn't have to deal with MTA as it is the responsibility of system admin to set up local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mails in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agent.

This can be easily understand by the diagram below (in ext page).



★ Both the SMTP client and SMTP server should have 2 components i.e. ① User-Agent (UA)
② Message Transfer Agent (MTA).

File Transfer Protocol (FTP)

→ FTP is an application layer protocol that moves files between local and remote file systems. It runs on the top of TCP like HTTP. To transfer a file, two TCP connections are used by FTP in parallel: ① control connection and ② Data Connection.

① Control Connection:
→ For sending control information like user identification, password, commands to change the remote directory, commands to retrive and store files. etc., FTP use of control connection.
The control connection is initiated on port No. 21.

② Data Connection:
→ For sending the actual file, FTP makes use of a Data connection.
A data connection is initiated on port number 20.

FTP sends the control info. out-of-Band as it uses a separate control connection. Some protocols send their request and response header lines and the data in same TCP connection. Therefore they are ~~known~~ as said to send their control information in-band. HTTP and SMTP are such examples.

■ FTP session:
→ When a FTP session is started between a client and a server, the client initiates a control TCP connection with the server. The client sends control info. over this. When server receives this, it initiates a data connection to the client. Only one file can be sent over one data connection. But the control connection remains active throughout the session. As HTTP is a stateless i.e. it doesn't keep track of any user state, But FTP ~~is~~ needs to maintain a state about its user throughout the session.

Advantages of FTP

- Speed
- File sharing, bet^n two machines file can be shared on the network.
- Efficiency is more in FTP.

Disadvantages of FTP

- File size limit is the drawback of FTP, only 2GB size files can be transferred.
- multiple receivers are not supported by the FTP.
- FTP does not encrypt the data, (biggest drawback of FTP)

Anonymous FTP:

- Anonymous FTP is enabled on some sites whose files are available for public access. A user can access these files without having any username or password. Instead, the username is set to anonymous and the password the guest by default. Here user access is very limited. For example, the user can be allowed to copy the files but not to navigate through directories.

HTTP Non-Persistent & Persistent Connection.

→ Hyper Text Transfer Protocol (HTTP) is an application layer protocol that ~~was~~ uses TCP as an underlying transport and runs on port 80. HTTP is a stateless protocol i.e. server maintains no ~~if~~ information about past client requests.

→ HTTP is a protocol using which hypertext is transferred over the web.

HTTP connections:

① Persistent
② Non-Persistent.

What is RTT (Round-Trip-Time)

→ Measure (in ms) of the latency of a network — that is, the time between initiating a network request and receiving a response.

→ It refers to the time taken by a network request to reach a destination and to revert back to the original source.

Difference between Persistent & non-Persistent connection

Nonpersistent HTTP	persistent HTTP
• requires 2 RTT's per object	• server leaves connection open after sending response
• OS overhead for each TCP connection.	• Subsequent HTTP messages between some client/server sent over open connection
• Browsers often open parallel TCP connections to fetch referenced objects.	• Client sends requests as soon as it encounters a referenced object
	• as little as one RTT for all the referenced objects

Difference Between http:// and https://

→ HTTP is a protocol using which hypertext is transferred over the web. Due to its simplicity, http has been the most widely used protocol for data transfer (hypertext) over the web but the data (i.e. hypertext) exchanged using http isn't as secure as we would like it to be. Infact, hypertext exchanged using http goes as a plain text. i.e. anyone between the browser and server can read it easily

? But why do we need this security over the web?
⇒ for financial Transaction, passwords, imp informations etc.

→ Https was introduced so that a secure session is setup first between server and Browser. Then hypertext was exchanged.
Cryptographic protocols such as SSL and/or TLS is present in Https.
i.e. https = http + cryptographic. → Secure Socket Layer → Transport Layer Security

→ Also another difference between http & https is that http uses default port 80 while https uses default port 443
Security in https is achieved ~~by~~ at the cost of processing time because web server and web Browser needs to exchange encryption keys using certificates before actual data can be transferred.
Basically, setting up of a secure session is done before the actual hypertext exchange between server and browser.

■ Difference bet" http & https

- URL of http starts with "http://" and URL of https "https://"
- HTTP uses port 80 while https uses port 443.
- HTTP is unsecure and https is secure
- HTTP Works at Aplication layer while HTTPS works at transport layer.
- HTTP, encryption is absent while In HTTPS encryption is present.
- HTTP, does not require any certificates, HTTPS requires certificates like SSL.

Multipurpos Internet Mail Protocol (MIME)
Extension

→ It allows to the users to exchange different kinds of data files on the Internet like audio, video, application program etc.

■ Features of MIME

- Able to send multiple attachments with a single message.
- Unlimited message length
- Binary attachments (exe; audio, video, img. etc)

Difference Between Internet and Web

→ The Internet is a global Network while the web (World Wide Web) is a collection of information that can be accessed via internet.

→ Web applications use HTTP protocol which is a layer over TCP protocol, whereas Internet applications can use either TCP or UDP protocol.

Wifi (Wireless Fidelity)

- Wifi stands for wireless fidelity. It is a technology for wireless local area networking with devices based on IEEE 802.11 standards
  Wifi compatible devices can connect to the internet via WLAN network and a wireless Access Point (AP). Every WLAN has an access point which is responsible for receiving and transmitting data from/to user.

Wifi Protected Setup (WPS)

- The Wifi Protected Setup (WPS) is a wireless network security standard that tries to make connections between a router and wireless devices.
- WPS works only for wireless networks that uses a password that is protected with Wifi Protected Access (WPA) or wifi Protected Access II (WPA2) Personal security protocol.
- WPS does not work on wireless network that uses the Wired Equivalent Privacy (WEP) security, which can be easily cracked by hackers.
- In a standard setup, we cant connect a wireless device to a wireless network until we know the network name (ie. Service Set Identifier (SSID)) and its password (also called WPA-PSK key).

Wifi Protected Access (WPA)

- The two security protocols and security certification programs are WPA and WPA2
  WPA also referred as the draft IEEE:802.11i standard, available in 2003.
  WPA2 referred as draft IEEE:802.11i-2004 standard, available in 2004.

WPA

- The WPA protocol implements almost all of the IEEE 802.11i standard. The Temporal key Integrity Protocol (TKIP) was adopted for WPA. WEP uses a 64 bit or 128 bit encryption key that must be manually entered on wireless access points and devices which once entered can never be changed.
  TKIP employs a per-packet key, which means that it dynamically generates a new 128 bit key for each packet and thus prevents the types of attacks that compromised WEP.
- WPA included a message Integrity check, which is designed to prevent attacker to alter or resent data packets. This replaced the Cyclic Redundancy Check (CRC) that was used by WEP. CRC's had a main flaw that it did not provide a sufficiently strong data integrity guarantee for the packets it handled.
  WPA uses a msg integrity check algorithm called (TKIP) to varify the integrity of the packets.
  TKIP is stronger than CRC but algo used in WPA2 is more stronger.
  Researchers discovered a flaw in WPA similar to older weaknesses in WEP and the limitations of the msg integrity code hash function, named Michael, that is used to retrieve the keystream from short packets to uses for re-injection and spoofing.

[2] WPA 2

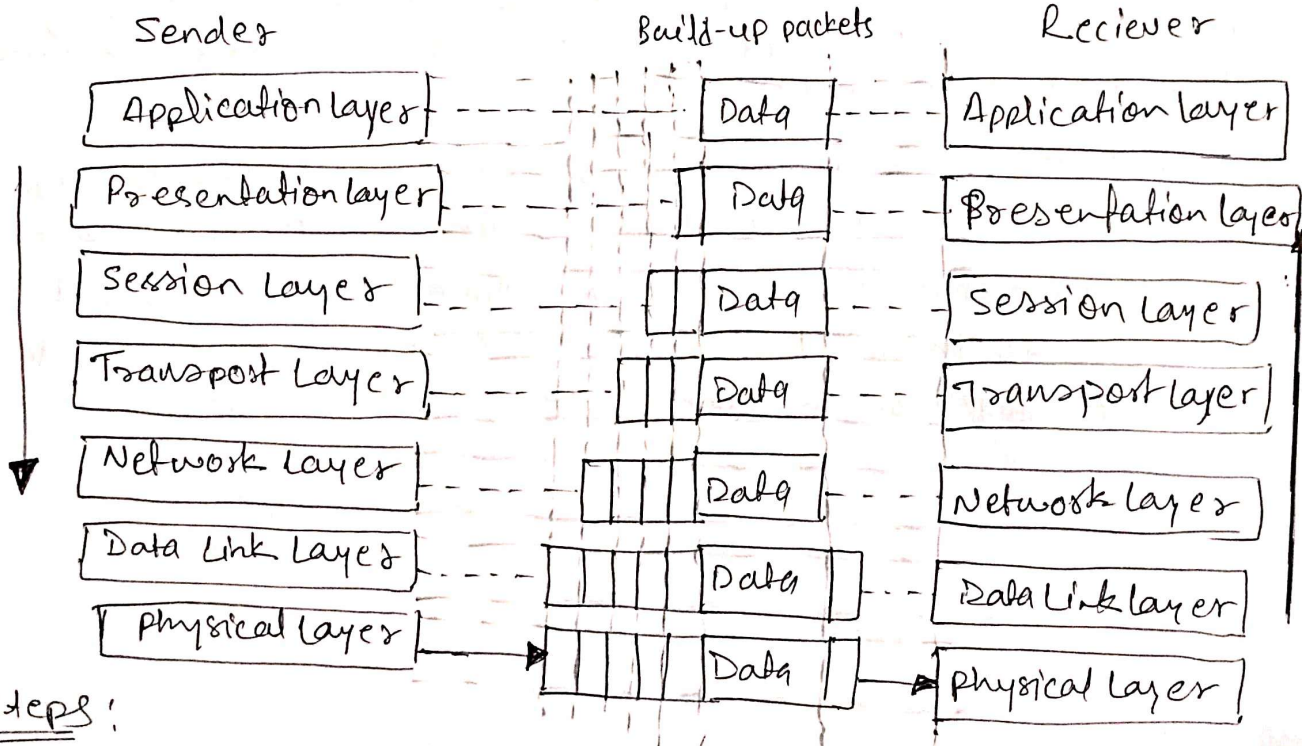
→ WPA2 replaced WPA. WPA2 which requires testing and certification by the wifi Alliance, implemented the mandatory elements of IEEE 802.11i. Particularly, it included mandatory support for CCMP (Counter mode CBC-MAC protocol), an AES (Advanced Encryption standard) based encryption mode. Certification began in September 2004, WPA2 certification is mandatory for all new devices to bear the wifi trademark from March 13, 2006.

How Communication happens using OSI model

→ The OSI model defines a seven layer set of functional elements, from physical interrelations at physical layer (Layer 1) to application layer (Layer 7)

TCP and IP are two network standards that defines the internet.

■ The communication process in the OSI model :



→ Steps :

① Each layer of the sender adds info to the msg received from above layer and moves the entire package just below the layer

② Each layer added its info in the form of headers. Headers are added at the level of the messages (6, 5, 4, 3 and 2). A Header is added at the Data Link layer (Layer 2).

(3) At the physical layer, communication is direct. i.e. the sender sends a stream of bits to the receiver. At the physical layer the entire package is converted into a form that can be transferred to the receiver. On the receiver side, each process is accompained layer-by-layer to receive and delete msg data.

(4) Always the upper OSI layers are implemented in the software (Transport layer, Session layer, Presentation layer, App. layer) and the lower layers are combination of hardware & software. (i.e. layer 2 & 3) except for physical layer which is mostly hardware.

Layer 1, 2, 3 (Physical layer, Data Link layer, Network layer) are network support layers. They deal with physical aspect of moving data such as electrical specification, physical connections, physical address, and transport time and reliability from one device to another

Layer 4 (Transport layer) end to end ensures reliable data transmission

(5) Not all applications need to use 7-layers. The lower three layers are sufficient for most applications. Each layer is made up of electronic circuits and/or software and has a seperate existance from rest of the layers.

(6) Each layers is assumed to handle msgs or data from the layers that are above or below it. (This is done by following protocol rules)

(7) Thus, each layer takes data from adjacent layer, Handles it according to these rules, and then sends the processed data to next layer on the other side.

#Packet Traveling

#OSI Model :

OSI Layer1 - Physical :

- The physical layer of OSI model is responsible for the transfer of bits i.e. the 0's and 1's which make up all computer code.
- This layer represents the physical medium which is carrying the traffic between two nodes. An example would be Ethernet cable or Serial Cable But what about wireless, such as WiFi, As such WiFi, despite it not having a physical, tangible presence, is also considered a layer1 protocol
- In simple words, Layer 1 is anything that carries 1's and 0's bet two nod
- The actual formate of data on the wire can vary with each medium, like, in Ethernet, bits are transferred in form of electric pulse, and In case of WiFi; bits are transferred in the form of radio waves.
- Repeaters & Hub are also operate at this layer.
  Repeaters simply repeats a signal from one medium to other. and A Hub is simply a multi-port Repeater.

OSI Layer 2 - Data Link

- The Data Link Layer of the OSI model is responsible for interfacing with the physical layer. Effectively, Layer 2 is responsible for putting 1's and 0's on the wire. and pulling 1's and 0's from the wire
- The NIC that we plug our Ethernet wire into handles the Layer 2 functionality. It receives signals from the wire, and transmits signals on to the wire.
  WiFi NIC works the same way, receiving and transmitting radio waves which are then interpreted as a series of 1's and 0's.
- Layer 2 will then group together those 1's and 0's into chunks known as Frames.
- There is an addressing system exists at Layer 2 known as MAC address. The MAC add. uniquely identifies each individual NIC.
- Aside from NIC, switch also operates at this layer. A switch's primary responsibility is to facilitate communication within networks.

→ Function of Data Link Layer is to deliver packets from one NIC to another. OR, (Another way):
The role of Layer 2 is to deliver packets from hop to hop.

OSI Layer 3 - Network:

→ The Network layer of OSI model is responsible for packet delivery from end-to-end.
→ It does this by using another addressing scheme that can logically identify every node connected to the Internet. This addressing scheme is known as Internet Protocol (IP address)
→ It is considered logical because an IP address is not a permanent identification of a computer. Unlike the MAC add. which is considered a physical add, the IP add. is not burned into any computer hardware by the manufacture.
→ Routers are Network Devices that Operate at Layer 3 of the OSI model. A Router's primary responsibility is to facilitate communication between networks.

OSI → Layer 2 vs Layer 3

→ Layer 2 uses MAC add. and is responsible for packet to deliver from hop-by-hop
→ Layer 3 uses IP add. and is responsible for packet delivery from end-to-end.
→ When computer has data to send, it encapsulates it in a IP header which will include info. like the Source & Destination IP add. of the two "ends" of the communication.

The IP header and Data are further encapsulated in a MAC add. Header, which will include info. like the Source & Destination MAC add. of the current "hop" in the path towards the final destination.

OSI Layer 4 - Transport

→ The Transport Layer of OSI model is responsible for distinguishing network streams.
→ At any given time on a user's computer there might be an Internet browser open, while music is being streamed, while a messenger is running. Each of these applications are sending and receiving data from the internet and all the data is arriving in form of 1's and 0's on to that computer's NIC.

Something has to exist in order to distinguish which 1's and 0's belong to the messenger or browser or streaming music. That "something" is Layer 4.

→ Layer 4 accomplishes this by using an addressing scheme known as port Numbers.

→ Specifically, two methods of distinguishing network streams exist. They are known as the TCP and the UDP.

→ If Layer 2 is responsible for hop-by-hop delivery, and Layer 3 is responsible for end-to-end delivery, it can be said that Layer 4 is responsible for service-to-service delivery.

■ OSI Layer 5, 6, 7

→ The Session, Presentation, and Application Layers of OSI model handles the final steps before the data transferred through the network (facilitated by Layer 1-4) is displayed to the end user.