Computer networks.

Network is a connection of several computers

→ purpose of this network is to share the resources such as files, documents, printers, servers etc.

Types of networks.

LAN Local area network
WAN wide area network.
MAN metropolitant area network.

~~Local Area Network~~ (WAN) ~~(MAN)~~

(LAN)	(WAN)	(MAN)
→ Connection of computers in a limited range such as college, home, building.	→ connection will be among different cities or states.	→ connection of different LAN's.
→ purpose of LAN is to share resources such as printer.	→ Transmission media is satellite or telephone cable	→ connected with in the city.
→ High security	→ sharing of data	→ sharing of data
→ Lack of privacy.	→ connection of MAN's.	→ less security.
	→ Data sharing using routers	→ transmission media is fibre optics.
	→ less security.	→ more cables are required for transmi

Network topologies

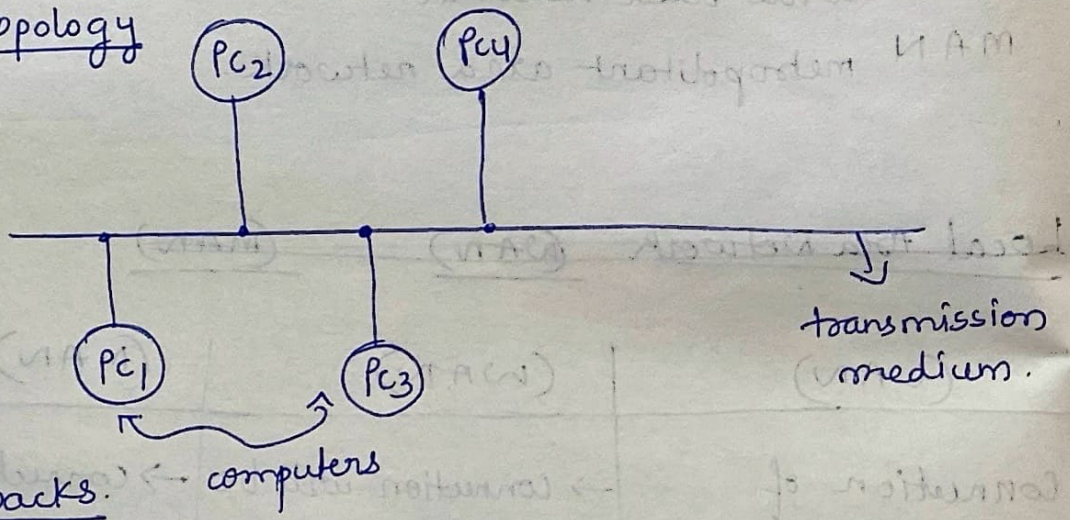
Topology means arranging the computers in a network.

Types of topology

1) Bus
2) Star
3) Ring.
4) Mesh.
5) hybrid.

} Arrangement of computers.

Bus topology



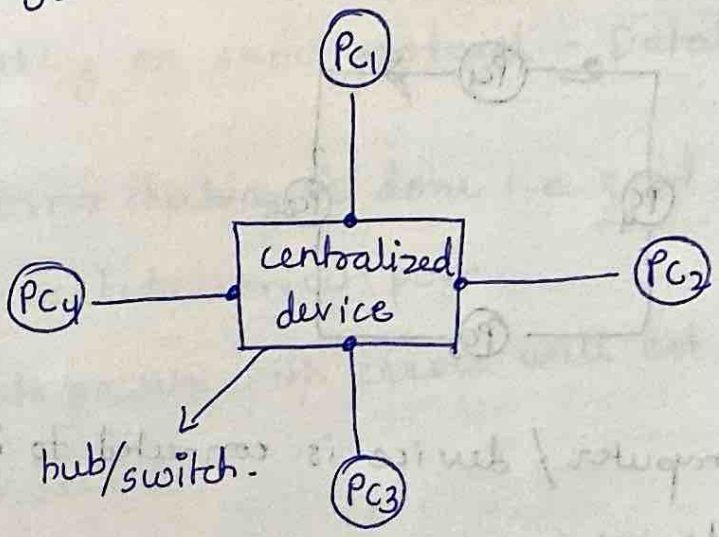
drawbacks.

* Data collisions.
* more no of computers signal strength decreases.
* no security

Advantages

* less expensive
* easy installation
* ease of reconfiguration.

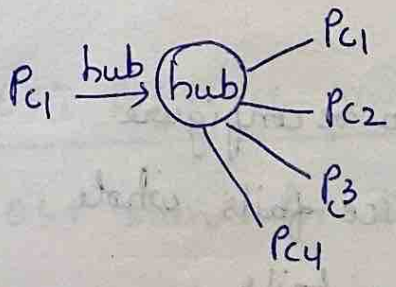
② star topology



hub : transmission is broadcast

switch : transmission is only to destination, other devices will not receive the data. (unicast transmission)

$PC_1 \xrightarrow{hub} PC_3$



$PC_1 \xrightarrow{switch} PC_3$

$PC_1 \rightarrow$ switch.

switch $\rightarrow PC_3$.

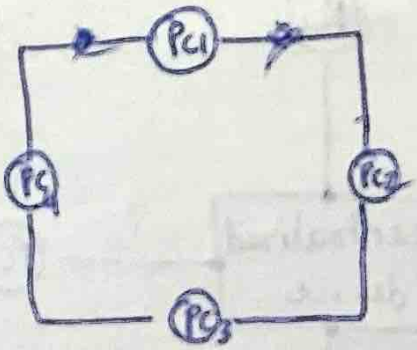
Advantages

* secured if we use switch
* less expensive

drawbacks.

* If hub/switch fails, whole network fails.

③ Ring topology



→ every computer / device is connected to its adjacent nodes or devices

→ data is transmited in unidirectional and circular fashion.

Advantages

* no collision
* easy to identify faults.

disadvantages

* expensive
* difficult to reconfigure
* If any device fails, whole transmission fails
* less security.

Network devices.

* Repeater : Regenerating a signal to maintain the signal strength - physical layer
* hub : hub is used to transfer the data packets to all connected devices.

* **Bridge**: Interconnecting two LAN's which are working on same protocol. - Datalink layer.

* **Switch**: Error checking is done i.e good data packets are sent to correct port.
  → Data packets with errors will not be forwarded.

* **Router**: Packets will be routed to destinations in best route path
  → Dynamically. routing will be done.
  - network layer.

OSI Reference model.

→ OSI stands for Open System Interconnection
→ Developed by International Standard Org (ISO)
→ It is a 7 layered Architecture which is used to transmit data from one system to another system

layers:

* physical layer
* Datalink layer
* Network layer
* transport layer
* session layer
* presentation layer
* Application layer.

1) physical layer provides physical medium to transfer raw bits.

2) data link layer bits will be converted to frames and be transmitted.

3) Network layer frames are converted to packets which move from source to dest.

4) Transport layer using protocols reliable message such as packets will be transmitted

5) Session layer : establishing and terminating of session will be created.

6) presentation layer : Here Data compression, encrypt is done.

7) Application layer : various services are provided directly to the user.

physical layer.

→ It is the lower layer or hardware layer.

→ establishes, maintains, terminates physical connection between two devices.

→ Information is in the form of bits (0's & 1's)

functions of physical layer.

→ Bit synchronization i.e only one bit should be transmitted at a time & no overlapping should exist

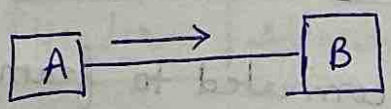
→ Bit rate control : It defines how many bits can be transmitted per second.

→ physical topology : Responsible to arrange the devices in a network.

→ transmission mode : Responsible to define the mode of transmitting the data.

Ex: simplex, half duplex, full duplex.

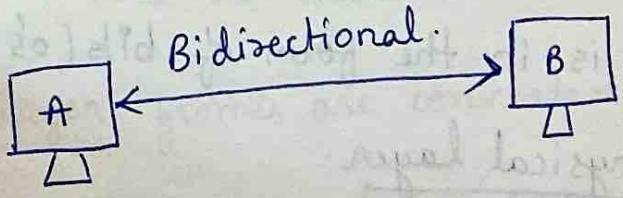
① Simplex mode : transmission is only in unidirectional way.



Ex: monitor, Keyboard.

② half duplex : transmission is done in bidirectional way.

→ only one device can send or receive data at a time.



Ex: walkie Talkie.

③ full duplex : Transmission is done in bidirectional way.

→ Data can be transmitted at the same time from both sender and receiver.

Ex : telephone.

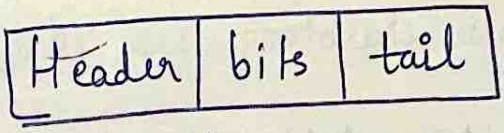
Data link Layer.

→ Raw bits will be converted to frames.

→ Responsible to transmit error free data.

functions of Datalink layer.

① framing : Raw bits are converted to frames by adding header bits and tail bits to the raw bits.



frame.

② physical addressing : destination address will be included as a header in the frame.

③ error control : error control mechanism will be implemented & calculated bits (CRC) will be added in tail.

→ If any error occured, receiver sends acknowledgement to retransmit the corrupted data.

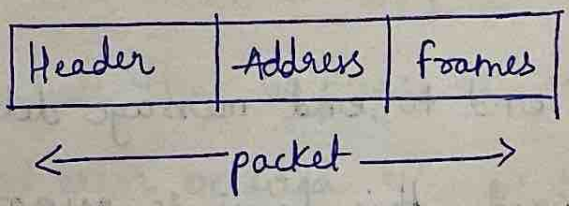
④ flow control : maintaing constant bitrate, so that less chance of data corruption.

Network layer.

→ Data is represented as packets.

→ conversion of physical address to logical address.

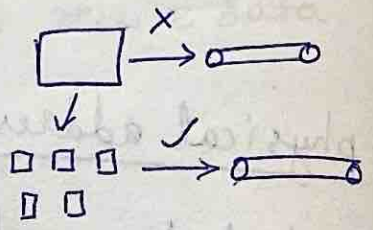
→ Routing the packets from source to dest.



* Internetworking.

logical connection b/w different networks.

* fragmentation.



If bandwidth > packet size

data loss happens.

So packets are fragmented. to avoid data loss

Services.

→ Guaranteed delivery.

→ In order packets.

→ Guaranted max jitter: The time difference b/w packets should be same at sender and receiver side.

Transport layer.

→ Data is represented in form of segments.

→ provides logical communication b/w the applications on diff paths.

→ Responsible for end to end message delivery.

→ if any error occured, this layer is responsible to retransmit the data.

* TCP & UDP are protocols used in transport layer.

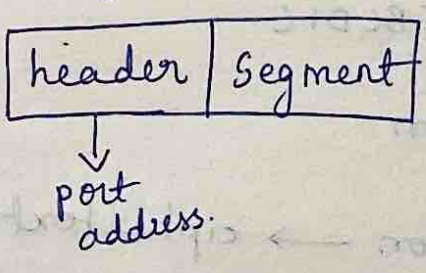
Services

→ end to end delivery

→ Reliable delivery.

→ Flow control.

→ Addressing



→ connection oriented / connection less.

Session layer.

Services

① Session establishment, maintainence & termination.

② Synchronization.

* creating checkpoints.

Ex: 100 pages of data.

checkpoint = 20 pages.

if error occurs at 65 page, then we can conclude that 60 pages are transmitted properly and error occured b/w 61 to 65

③ It allows two systems to communicate in half duplex or full duplex.

Presentation layer.

Services.

① Translation : data translation.

ASCII -> EBCDIC

② Encryption / decryption.

Sender Data → encryption → ciphertext

Receiver ciphertext → decryption → data.

③ Compression :

size of data will be reduced

Application layer.

Ex : web browser, messenger etc.

→ produces data, that would be transmitted over a network.

① File transfer, Access and management

② email services

③ file / Directory services.

TCP/IP model.

→ It was developed prior to OSI model.
→ It consists of only 5 layers. i.e physical, datalink, network, transport and application layer.

Network layer.

→ It is the lowest layer of osi model.
→ It is combination of physical and datalink layer.
→ It defines how data is sent from one device to another device.
→ protocols used in this layer are ethernet, X.25, frame relay, ~~ARP~~.

Internet layer.

→ second layer of TCP/IP model.
→ Also known as network layer.
→ main responsibility is to transfer data packets from one device to another device irrespective of the route they take.

There are several protocols used in Internet layer:

i) IP Protocol: IP protocol is used in this layer and it is the most significant part of this model.

* IP addressing: This protocol assigns IP address to each device which is connected to network. This address is used by Internet in order to send data from one device to another device.

* IP protocol ensures that data is sent or received securely. It encapsulates the data into a message called IP datagram.

* The limit imposed on the size of datagram by data link layer is called as maximum transmission unit (MTU). If the size of a datagram is more than MTU, then the datagram is broken down again into small fragments. These fragments are again reassembled at the receiver side.

* Breaking down the datagram or splitting it is called fragmentation. It can be done at sender side or by routers.

9i) ARP protocol:

→ stands for Address Resolution protocol.

→ It is a communication protocol used to map known IP address to physical or MAC address.

Process:

① IP and MAC Address:

* IP address: Every device in TCP/IP network is assigned a unique identifier. this address is used to route the data from sender to receiver.

* MAC Address: Device on a local network has a physical hardware address called as media access control address. It is a unique address assigned to each device on network interface card.

② ARP Request: when a device (lets take it as device A) wants to communicate and send data from device A to device B. But, device A has only target device IP address, it needs to find

corresponding MAC address. Device A sends ARP Request message to all the devices which are connected on a same network. The ARP request contains Device A's own IP and MAC address.

③ ARP Reply: The device with matching IP address replies directly to Device A with its MAC address.
→ other devices would just ignore the message

④ ARP cache: After receiving the reply, Device A stores the new IP-to-MAC address mapping in ARP cache.
* This helps in faster future communications with Device B, as Device A wont need to send ARP Requests again.

⑤ ARP table: Each device maintains an individual ARP table which consists of IP-to-Mac address mapping.

(iii) ICMP protocol:

→ It stands for Internet control message protocol.

→ It is a mechanism used by hosts or routers to send notifications about the problems which have arised when a datagram is being sent from sender to receiver.

→ A datagram travels from router-to-router until it reaches its destination, when this process is happening and some unusual conditions arise. such as disabled links, then ICMP used to inform the sender about the issue.

There are two mainly used terms:

* ICMP test: used to test whether the destination is reachable or not.

* ICMP Reply: used to test whether the destination device is responding or not.

→ So, the main aim of ICMP is to report the problems but does not correct them.

→ ICMP can only send the notification to the

sender because the datagram consists of source and dest IP address only but not of routers.

Transport layer :

→ responsible for reliability, flow control, correction of data which is being sent over the network.

→ There are 2 protocols used i.e TCP and UDP:

* User datagram Protocol :

→ It provides connectionless service.

→ It is an unreliable protocol i.e it does not gaurantee the delivery of data.

→ UDP discovers the errors, ICMP reports the errors to the sender.

UDP consists :

i) Source address : address of the source device which sends the data.

ii) Destination address : address of the destination device which receives the messege.

iii) Length : total number of bytes of user datagram in bytes.

iv) checksum : It is a 16-bit field used in error detection.

* Transmission control protocol :

→ provides full transport layer services.

→ creates a virtual circuit between sender and receiver and it is active during the transmission

→ TCP is a reliable protocol as it detects the errors and retransmits the damaged frames.

→ At senderside, TCP divides the message into several segments and these segments are assigned some number of sequence.

→ At receiverside, TCP again reassembles all the segments according to the sequence to form the original message.

Application layer:

→ top most layer of TCP/IP.

→ allows users to interact with the applications.

→ There is an ambiguity occurs in application layer. Every app cannot be placed in application layer except those which interact with the communication systems.

Ex: texteditor cannot be considered in application layer. while web browser using HTTP protocol to interact with the network is considered.

protocols used in application layer are:

* HTTP/HTTPS
* SNMP (Simple network management protocol)
* SMTP (Simple mail transfer protocol)
* DNS (Domain name System)
* TELNET
* FTP (file transfer protocol)

Domain Name System.

→ DNS stands for Domain name system.

→ It is a service which provides mapping between name of a host on network and the numerical address.

→ This service translates domain name to IP address. which allows users to utilize user friendly names instead of remembering IP address.

DNS components:

* DNS resolver: The clients computer that intiates DNS queries.

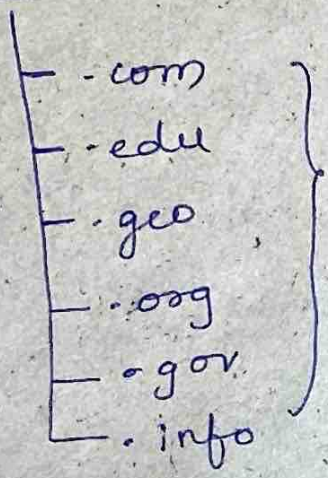
* Recursive DNS server: These are intermediary servers that perform the actual work of finding the IP addresses associated with the domain name.

* Root DNS servers: The top level servers in DNS hierarchy. They provide authoritative serves for each top level domain.

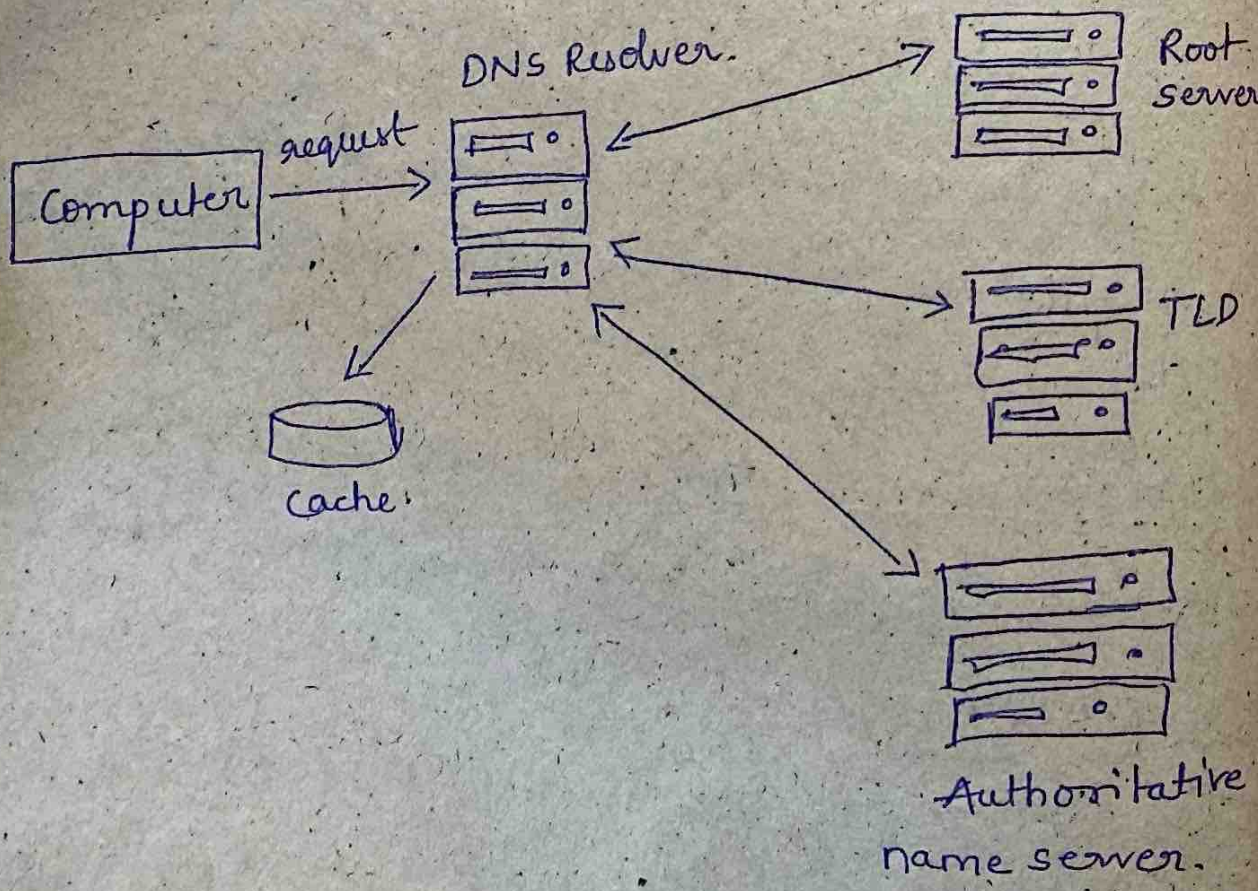
* TLD DNS servers: Servers responsible for top level domains. They maintain information about domain names directly under their TLD.

Authoritative DNS Servers: These servers store the actual DNS records for a domain.

Root server.



Internet corporation for assigned names & numbers (ICANN) is responsible for giving domain names



Process:

→ when a user enters a domain name in a web browser, the DNS Resolution begins.

→ DNS resolver chicks its cache to see if it has the IP address for the requested domain. If not it contact recursive DNS server.

→ The recursive DNS server may have the answer in its cache or will start the resolution process by querying the root DNS server.

→ The root DNS server directs the resolver to the appropriate TLD DNS server.

→ The TLD server, in turn directs the resolver to the authoritative DNS server for specific domain.

→ The authoritative DNS server provides the IP address, which is then returned to the user's device through the recursive server.

DNS Caching: To reduce the load on DNS servers and improve response times, DNS resolvers cache DNS query results for a certain period.

→ (Time to live) TTL is a parameter that specifies how long the information can be cached by the resolvers.

FTP :

→ FTP stands for file transfer protocol.

→ It is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

→ client - server architecture : FTP follows a client server architecture, where one computer (client) request and download files, and another computer (server) provides access to and manage the files.

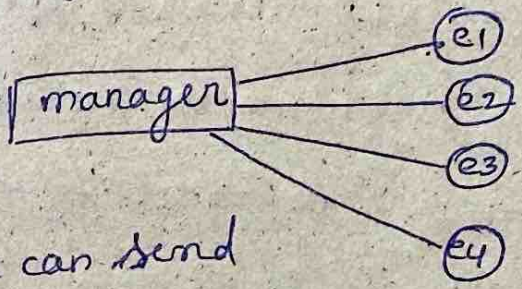
→ Two modes of operation :

* Active mode : In active mode, client opens a random port for data transfer and server connects to this port. This mode can sometimes encounter issues with firewalls.

* passive mode : In passive mode, the server opens a random port for data transfer, and client connects to this port. This mode can overcome the issues related to firewalls and NAT.

Advantages:

→ speed
→ efficient
→ security
→ Back & forth movement:



→ manager can send files to all employees.
→ All employees can send files to manager.

→ FTP uses 21 port for command and control. a range of dynamic ports.

Telnet

→ Telnet is a network protocol, which allows users to log into a remote computer, access its resources and execute the commands as if they were physically present at that computer.

Key aspects:

→ used for text based communication. It enables users to interact with a remote system using command line interface.

→ It operates on a client server model. The user's computer runs a telnet client, and the remote system runs telnet server.

→ The default port number is 23. when a user tries to connect to a remote system via telnet, users typically specify host name or IP address of remote server and the port number.

→ Telnet establishes a clear text communication, meaning that the communication b/w client & server is not encrypted. This makes telnet insecure for transmitting sensitive information.

→ Telnet provides virtual terminal evaluation, allowing the user to access the remote system comma line interface as if they were using a local terminal. This enables the execution of commands and interac with applications on the remote system.

SMTP

→ SMTP stands for simple mail transfer protocol.

→ It is a protocol used for sending and receiving email messages on the internet.

→ SMTP follows client-server model. An SMTP client (sender) communicates with an SMTP server (receiver) to send an email.

→ SMTP uses port 25 by default for unencrypted communication. SMTPS uses port 465 for secure communication.

components:

→ user agent: The user agent is the email client used by the sender to compose, read and send emails.

→ Mail submission agent: The MSA is responsible for accepting outgoing emails from the user agent and submitting them to mail transfer agent. This typically happens in the same server.

→ Mail transfer agent : The MTA is responsible for routing and transferring emails b/w mail servers. The MTA determines the destination server for the recepient email address and forwards the mail accordingly.

→ Mail delivery agent (MDA) : responsible for delivering the received emails to the recepient's mail ~~address~~ box. It places the emails in the appropriate mailbox for the recepient to retreive using their user agent.

→ MX Records : The MX Record is a DNS record that specifies the mail servers responsible for receiving emails on behalf of a domain.

Example :

→ Alice uses her email to compose an email. She addresses it to Bob and writes a message. Alice clicks send, and her email client communicates with her email server to submit the outgoing email.

The MSA checks whether Alice is a valid user

→ Alice's MTA looks up MX Records for Bob's domain to find the address of bob email server.

→ ~~Bob~~ MTA initiates SMTP session with Bob's email server using SMTP client.

→ Bob's email server responds to the connection request.

→ Bob's SMTP server receives the email and places it in Bob's mail box using MDA.

→ Bob's server sends delivery confirmation to Alice's email server.

→ Bob checks his email using email client. He sees ~~Alice~~ email from Alice in his Inbox and reads the message.

HTTP

→ unsecured protocol
→ no encryption provided
→ port no 80
→ Begins with http://
→ No certificate is required

HTTPS

→ secured protocol.
→ uses SSL/TLS encryption
→ port no 443.
→ Begins with https://
→ requires SSL/TLS certificates.

SNMP protocol.

→ stands for Simple network management protocol.
→ Used to manage and monitor network devices.
→ Allows admins to collect information, configure devices and manage network performance.
→ This protocol works on the concepts of manager-agent model.

* Manager: It is a type of software which monitors and manages the network. It requests the information from devices and also asks the devices to perform certain actions.

* Agent: It is a type of software which runs on the devices which are in the network. like routers, servers etc. The agent collects the information about the devices.

Example: Let's say you have a network of devices with multiple routers. and you want to monitor the bandwidth of the each router.

1) Manager: you have a monitoring tool that supports SNMP. you configure it to monitor the bandwidth of routers.

2) Agent: Each router in your network has an SNMP agent running in it. This agent keeps track of various parameters such as bandwidth usage.

3) SNMP Requests: The manager periodically sends SNMP Requests to the agent asking for specific information such as bandwidth usage.

4) SNMP traps: Agents can send SNMP traps to the manager when certain events occur. for instance, if bandwith usage goes above threshold value.

5) Response: The agent will respond to the SNMP requests made by the manager and send the requis

information to the manager. The data is processed by manager. If a trap is received, then the manager can take appropriate actions, such as sending an alert or configuring the device.

SSL and TLS.

SSL (Secure Socket Layer) and TLS (Transport layer Security) are protocols that provide secured communication over a computer network. They are commonly used to secure the data transmitted b/w a user's browser and website, ensuring that the information remains protected from unauthorized access.

where TLS / SSL is used :

→ Secure web browsing
→ Email security
→ VPNs
→ File transfer protocols.

post number

Think of a post number as an apartment ~~building~~ number in a large building. just like a building can have many apartments, a computer can run many programs or services. Each service on a computer is assigned a unique post number which helps the computer know which program to send incoming data to.

Ex:

→ Imagine a computer as a big building with many rooms in it (services or programs)

→ Inside the building (computer), there are different programs or services running, like a web browser, email service, or a game. Each program is like an apartment.

→ Now, think of post number as the apartment numbe It is a unique number assigned to each program or service. For ex, browsers often use post number 80, while secure browsing uses post number 443.

→ when data comes to the computer, like receiving a mail. The computer looks at the post number to figure out which program or service the data is meant for and sends the data accordingly.