"Set-1"

Computer Network (CN) - 2021 Fall.

1a) Define Intranet. Which network model is used for connecting devices with in office and why? Explain with need and diagram along with advantages and disadvantages.

Ans:-

Intranet is a private network contained within an enterprise that is used to securely share company information and computing resources among employees.
Only authorized people and system can access it.

I prefer using Local Area network (LAN) ~~with~~ network model with in office for connecting devices.

As,
A local area network is a collection of computers that are linked together in a small area, such as a building or office. A local area network connects two or more computers via a communication medium such as twisted pair, coaxial cable and so on. As well as, in local area network, data is

transfered at an extremely fast rate.

Advantages of LAN

→ Inexpensive transmission media.
→ A large rate of interconnection between devices.
→ It is used to high data transmission rates.
→ It allows file-locking
→ It is flexible and growth-oriented.
→ It provides full proof of the security system against illegal access to data.
→ Ease of management.
→ The connected devices can be accessed, managed and controlled from one location.

Disadvantages of LAN

→ Sometimes the peripheral devices may be fewer and users requests will be higher so it may cause time consumption.

- It's a local area network so beyond 1km you should create another local area network or any other network.
- If the server crashes then it may affect all the computers within that network.
- Malware Spreading
- Some current application program will not run in a network environment.

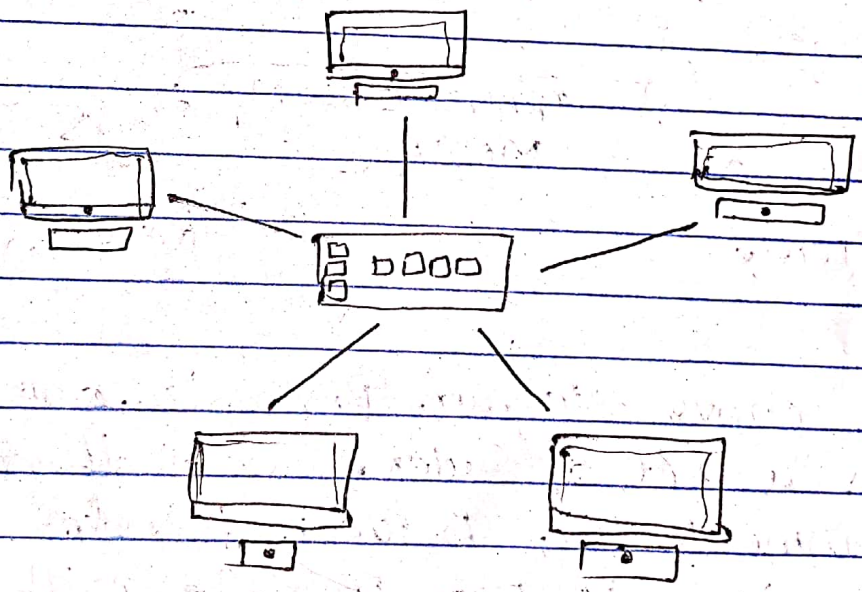
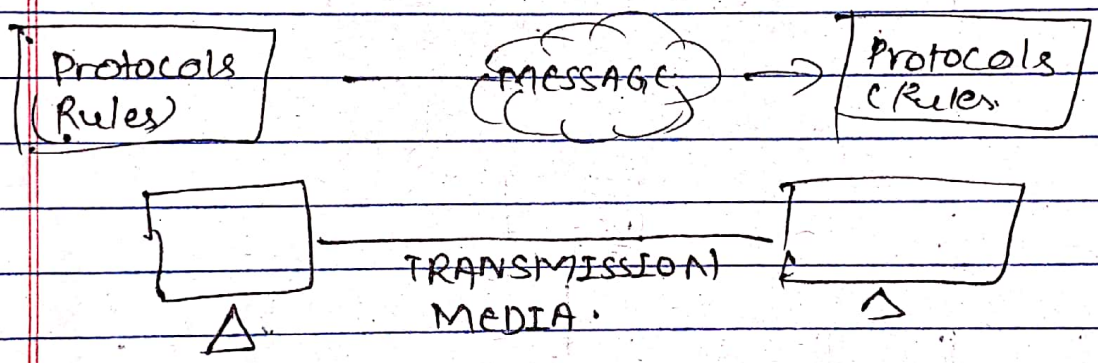


Figure:- Local Area Network.

1 b) Define protocols and standards: Compare TCP/IP and OSI reference.

Ans. Protocols:-

In order to make communication successful between devices, some rules and procedures should be agreed upon at the sending and receiving ends of the systems. Such rules and procedures are called protocols.



In above diagram Protocols are shown as a set of rules. Such that communication between sender and receiver is not possible without protocols.

Standards:

Standards are the set of rules for data communication that are needed for exchange of information among devices. It is important to follow standards which are created by various standard organizations like IEEE, ISO, ANSI etc.

Types of standards.

1) De Facto Standards (By Fact)
2) De Jure Standard. (By Law)

TCP/IP :- Transmission control protocol / Internet Protocol.

OSI :- Open System Interconnection.

OSI	TCP/IP
It is a generic, protocol independent standard. It is acting as an interaction gateway between the network and the final-user.	TCP/IP model depends on standard protocols about which the computer network has created. It is a connection protocol that assign the network of host over the internet.
It provides quality services	It does not provide quality service.

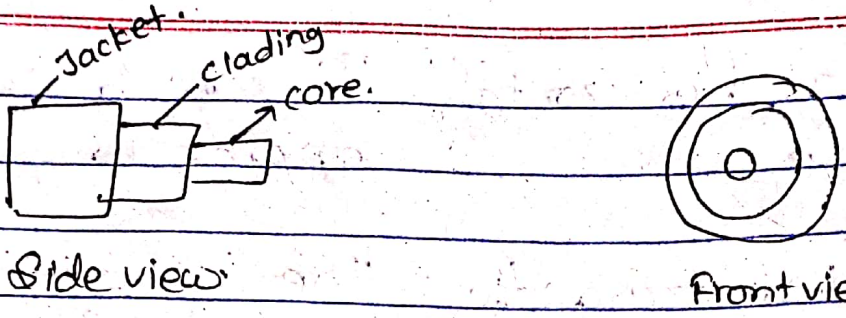
The OSI model was developed first, then protocols were created to fit the network architecture's needs.	The protocols were created first and then built the TCP/IP model.
It is difficult as distinguished to TCP/IP.	It is simpler than OSI.
The OSI model represents defines administration, Interfaces and convention It describes clearly which layer provides services	It does not mention the services, interfaces and protocols.
It provides both connection and connectionless oriented transmission in the network layer. However, only connection-oriented transmission in transport layer.	It provides connection less transmission in network layer. and support connection and connectionless-oriented transmission in transport layer.

It uses a horizontal approach	It uses a vertical approach.
The smallest size of the OSI header is 5 bytes	The smallest size of the TCP/IP header is 20 bytes.
Protocols are unknown in the OSI model and are returned while technology modifies	In TCP/IP, returning protocol is not difficult.

2a) Why do we use fiber optics for long distance communication? Explain fiber optics single mode of propagation? Describe about network performance bandwith and latency. Write a command to check latency to server with IP 4.4.8.8 from your computer with Windows/Linux Os.

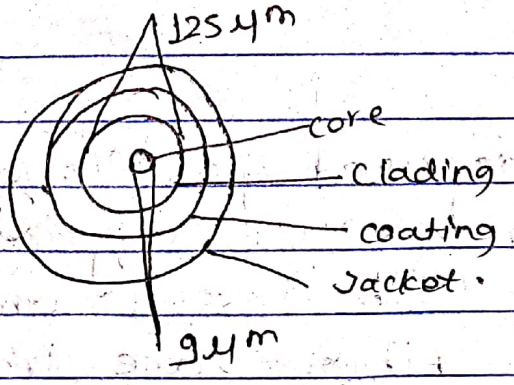
Ans.

Fiber optics is used for long distance communication because signals travel along them with lesser amound of loss. Also, fibers are immune to electromagnetic interference.



Single Mode fibers have a small glass core, typically around 9μ. Single mode fibers are used for high speed data transmission over long distances. They are less susceptibe to attenation that multimode fibers.

It has small diametral core that allows only one mode of ligh to propagate. Because of this, the number of light reflections created as the light passes through the core decreases.



Bandwidth:- This is about the volume of data that can be transferred over a network. The standard measurement for data transfer speed is megabits per second (mbps).
It is a measure of how much data can move measured in x bits per second. It measure size.

Latency:- Latency is a measure of the delay in moving the data (measure in milliseconds), between two nodes.
It measures speeds.
It is usually measured in milliseconds

Latency = propagation time + transmission time + queuing time + processing time.

Command for checking latency to server of IP address 4.4.8.8 is

trace route 4.4.8.8.

2b Differentiate between Distance Vector Routing algorithm and Link State Routing algorithm with example. What are features of IPV6 protocol and provide one example of IPV6.

Ans

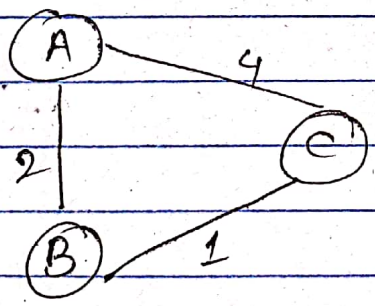
Distance Vector Routing	Link State Routing.
- It is a dynamic routing algorithm in which each routes computes a distance between itself and each possible destination i.e. its immediate neighbour.	- It is also a dynamic routing algorithm in which each router shares knowledge of its neighbours with every other router in the network.
Sharing of information with the neighbors takes place at regular intervals.	Information sharing takes place only whenever there is a change.
It make use of Bellman-Ford Algorithm for making routing tables.	It make use of Dijkstra's Algorithm for making routing tables.

- Traffic is less
- Converges slowly i.e. good news spreads fast where as bad news spreads slowly.
- Persistent looping proble i.e loop will there forever.

Traffic is more.
Converges fastly.
-> No persistent loops, only transient loop.

Eg:-

In the network, there are 3 routers A, B & C with some weights



Feature of IPV6.

- Larger address space (128 bit address space)
- Supports resources allocation via flow control field.
- Support more security
- Better header format.

3a) Define codeword. Explain with example how transmission error is detected and corrected using hamming code.

Ans.

A code word is an element of an error-correcting code C. If C has length n, then a codeword in C has the form $(c_1, c_2 \cdots c_n)$ where each c_i is a letter in the alphabet of C.

Let us take an example :- 7-bit hamming code received is 1011011.

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	1	1	0	1	1

Received code word.

For, P_1,

$P_1\ D_3\ D_5\ D_7$ - 1011. odd parity hence error occurs

For, P_2,

$P_2\ D_3\ D_6\ D_7$ - 1001. even parity hence no error

For P_4,

$P_4\ D_5\ D_6\ D_7$ - 1101 odd parity hence error occur

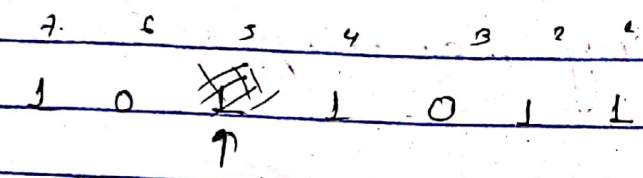
Error word $E = P_4\ P_2\ P_1$

$= 1\ 0\ 1.$

5^{th} bit.

Hence 5^{th} bit of the transmitted code is

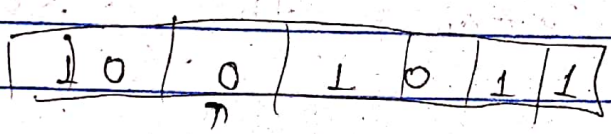
error.



incorrect bit.

We inverted the incorrect bit to obtain the correct code word.

i.e.



after inverted.

Correct codeword = [1001011].

3b) A company have 3 different department with 65, 32 and 12 network devices. Explain how you will design network for this company from provided network of 10.10.100.0/24. Provide network address, broadcast address, subnet mask, wild card mask and useable IP pool for each subnet.

Sol^n:.

Given IP = 10.10.100.0/24

00001010.00001000.01100100.00000000

Subnet mask =

11111111.11111111.11111111.00000000

255.255.255.0

Network address = IP AND subnet Mask

= 00001010.00001000.01100100.00000000

= 10.10.100.0.

We have,

Maximum number of host = $2^n - 2$.

For, 65 computers. [$\because n$ = no. of host bits]

$65+2 = 2^n$

$67 = 2^n$.

$67 = 2^7$

$= 128$

$\therefore$ no. of host bit = 7.

new subnet mask become. = [32 - 7. = 25.]

i.e. 255.255.255.128.

Subnet id = 256 - 128 = 128.

Broadcast address = 10.10.100.127.

Wild card mask. = 0.0.0.127

255.255.255.255 - 10.10.100.128

subnet mask.

Useable ip pool =>

255.255.255.127.

Wild card mask =

Useable IP pool = 10.10.100.1 to
10.10.100.126

For 32 computers.

IP address = 10.10.100.128

new subnet mask = 255.255.255.192

network id: 10.10.100.128.

subnet id = 256 - 192 = 64.

no of host = 64.

Broadcast address = 10.10.100.191

Wild card mask. = 0.0.0.192

Useable IP pool = 10.10.100.129 to
10.10.100.190

for 12 network devices.

maximum no. of host = $2^{\text{no. of host}} - 2$.

$12 + 2 = 2^4$

$= 16$.

no. of host = 4.

new subnet mask = 11111111.11111111.11111111.11110000

wildcard mask = 00000000.00000000.00000000.00001111.

network address = 10.10.100.192.

broadcast address = 10.10.100.207.

useable IP pool = 10.10.100.193 to 10.10.100.206.

4a. Draw IEEE 802.3 Frame Formod. Explain random access protol : ALOHA.

Ans.

Preamble	SFD	Destination address	source address	length	Data	CRC
7B	1B	6B	6B	2B	46-1500	4B

802.3 - Frame Format.

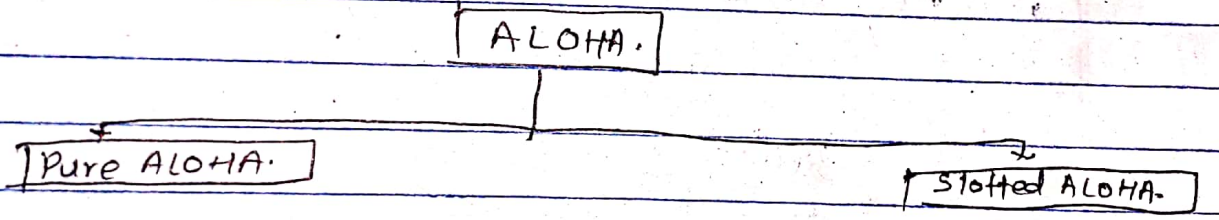
802.3 - Ethernet.

Random access protocol : ALOHA.

- It is a system for coordinating and arbitrating access to a shared communication Networks channel. This approach was introduced by Norman Abramson in 1970s at the university of Hawaii, It is a new method to solve the channel allocation problem.

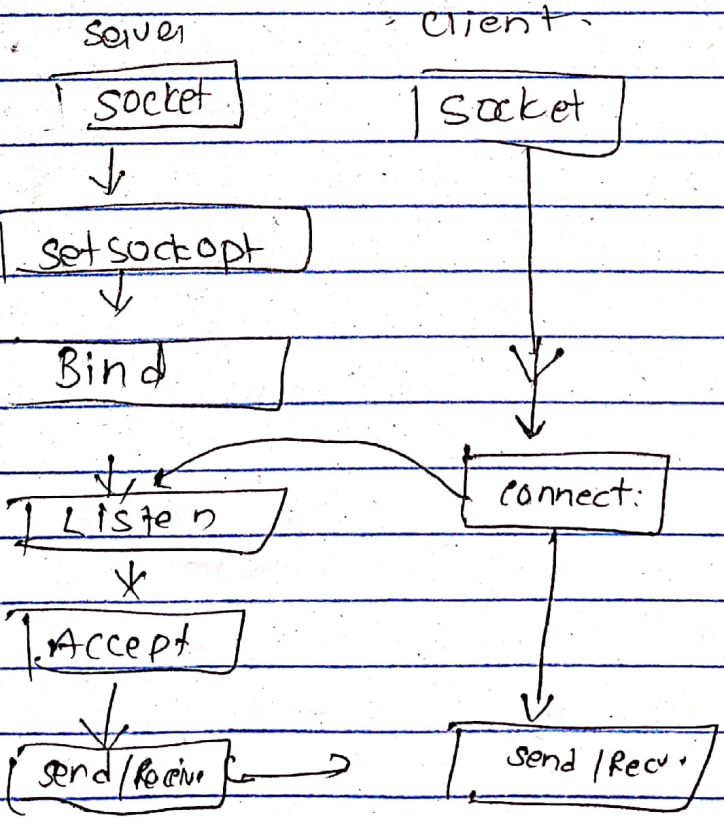
A shared communication system. like ALOHA requires a method of handing collisions that occurs when two or more systems attempt. to transmit on the chanel at the same time.

In the ALOHA system, a node transmits whenever data is available to send. If another node transmit at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted. Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision.



4b) What do you mean by Socket Programming? Explain TCP Client/server Socket flow with suitable diagram.

Ans Socket programming is a way of connecting two nodes on a network to communicate with each other.
One socket(node) listen on a particular port at an IP, while the other socket reaches out to the other to form a connection. The server forms the listener socket while the client reaches out to the server.



If we are creating a connection between client and server using TCP then it has few functionality like, TCP is suited for applications that requires high reliability, and transmission time is relatively less critical. TCP rearranges data packets in the order specified. There is absolute gurantee that the data transferred remains intact and arrives in the same order in which it was sent. TCP does flow control and requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control. It also does error checking and error recovery.

5a) In your opinion what are the main causes of congestion in network. Explain about closed loop congestion control.

Ans Network Congestion in a network may occours if the load on the network (the number of packets sent to the network) is greater than the capacity of the network (the number of packets a network can handle).

- When too many packets are pumped into the system, congestion occurs leading into degradation of performance.
- Congestion shows lack of balance between various networking equipment.

Where,
Congestion control refers to the mechanism and technique to control the congestion and keep the load below the capacity.

Congestion control

Open loop

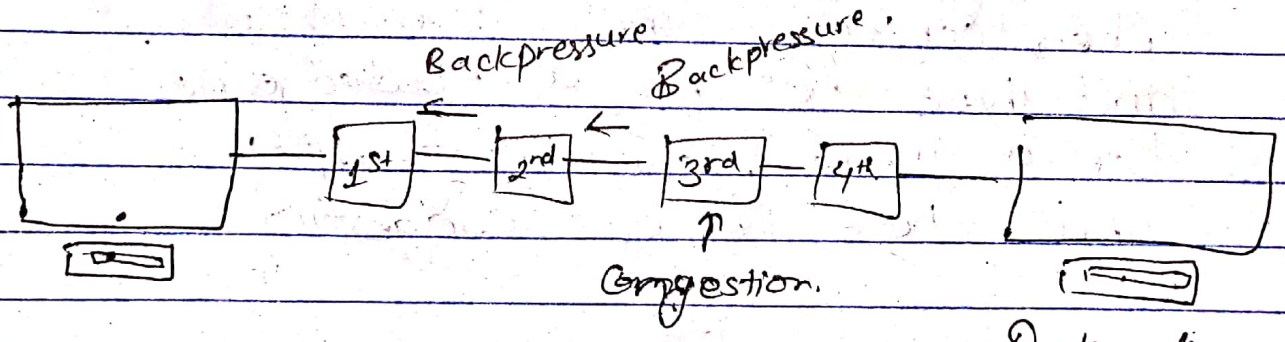
Closed loop.

Closed loop congestion control.

Closed-loop congestion control mechanism try to alleviate congestion after it happens. Several mechanisms have been used by different protocols.

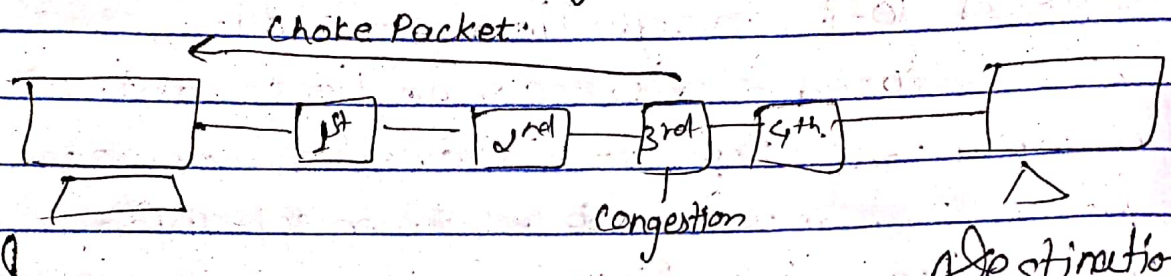
1) Back-pressure.

It is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and rejeat receiving data from above nodes. It is a none to nodes congestion control technique that propagate in opposite direction of data flow.



2) Choke Packet Technique

→ Choke packet technique is applicable to both virtual networks as well as diagram subnets. A Choke packet is a packet sent by a node to the source to inform it of congestion.



3) Implicit Signaling

In Implicit Signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network for example when sender sends several packets and there is no acknowledgement for a while, one assumption is that there is a congestion.

4) Explicit Signaling:-
In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating a different packet as in case of choke packet techique.
Explicit signaling can occur in either forward or backward direction.

5b) Explain about DNS, its importance, name resolution, iterated and recursive query with neat diagram.

Ans DNS stands for Domain Name System. DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address. DNS is required for the functioning of the internet. Each node in a tree has a domain name is a sequence of symbols specified by dots.

DNS is a TCP/IP protocol used on different platforms.

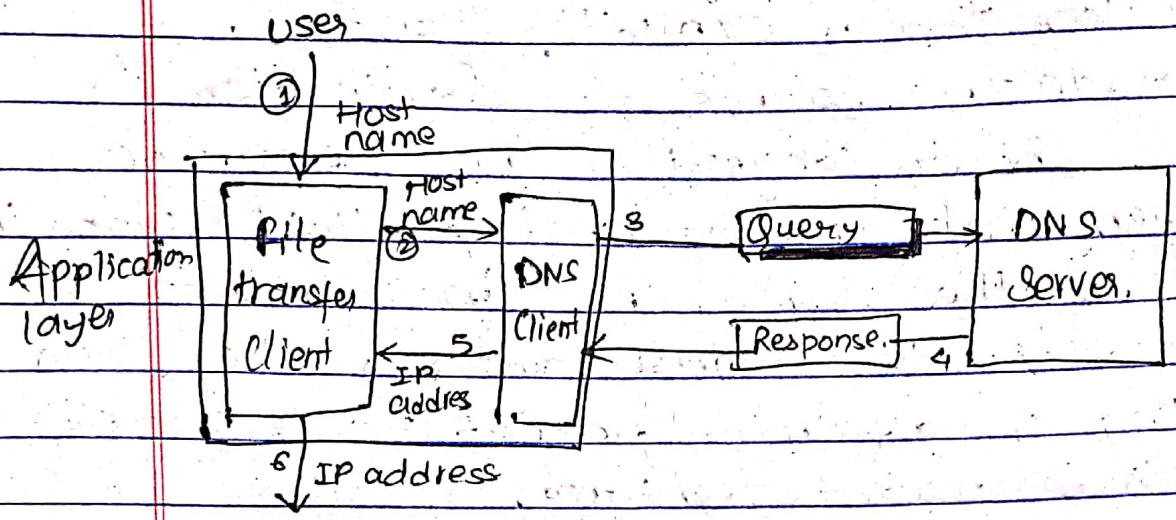


Figure :- Purpose of DNS

A DNS is what converts your URL to an IP address and routes messages to your website and its pages and subdomains.

DNS Importance :-

- DNS ensures that the internet is not only user friendly but also works smoothly, loading whatever content we ask for quickly and efficiently.

Name Resolution: (Address Resolution)

Name Resolution ~~server~~ transforms a DNS name into IP ~~address~~ address. The process have two phases. In 1st phase, we locate a DNS name server that has information we need: the address that goes with a particular name.

In 2nd phase, we send that server a request containing the name we want to resolve and it sends back the address required.

Here there are two DNS name resolution technique:

1) Iterative and another is recursive resolution.

Recursive DNS Query: In Recursive DNS Query, the DNS client Sends a Query to DNS server for name resolution. The reply to the DNS Query can be an answer to the query or an error message.

If DNS server doesn't know the answer

to provide accurate answer to the DNS Client. DNS Server may query other DNS servers on behalf of the DNS Client.

Iterative DNS Query:
In Iterative DNS Query, when a DNS client asks the DNS server for the name resolution, the DNS server provides the best answer it has. If the DNS server doesnot know the answer to the DNS Query from the client, the answer can be a reference to another lower level DNS server also.

6a) What do you mean by symmetric and asymmetric key algorithm? Explain RSA with suitable algorithm to perform key generation for public key, private key, encryption and decryption.

Ans

A symmetric key algorithm uses the same key for both encryption and decryption and the key can be used for bidirectional communication which is why it is called symmetric.

It works by taking the plaintext message and combining it with a shared key that is input to the algorithm.

A asymmetric key works in the similar manner to symmetric key algorithm, where plaintext is combined with a key, input to an algorithm, and output ciphertext. The major difference is the keys used for the encryption and decryption portions are differents, thus the asymmetric of the algorithm. The key pair is comprised of private and public key.

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public key and Private key. As the name describes that the Public key is given to everyone and private key is kept private.

For eg.:-
A client sends it public key to the server and requests for some data.
The server encrypts the data using client's public key and sends the encrypted data.
Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

RSA Encryption.

- Suppose the sender wish to send some text message to someone whose public key is (n, e)
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the plaintext P_i which is a number modulo n. The encryption process is simple. mathematic step as

$$C = P^e \bmod n.$$

In other word, the ciphertext 'C' is equal to the plaintext P multiplied by itself e times and then reduced modulo n. Then this means C is also a number less than n.

RSA Decryption.

- The decryption process for RSA is also very straight forward. Suppose that the receiver of public key pair (n, e) has received a ciphertext 'C'.
- Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$$\text{Plaintext} = C^d \bmod n.$$

Q6. Difference between Switch and Hub. Explain exterior routing protocol.

Ans

Switch	Hub.
A switch is a control unit that turns the flow of electricity on or off in a circuit.	A hub is a networking device that allows one to connect multiple PC's to a single network.
Switch is operated on Physical layer of OSI model	Hub is operated on Physical layer of OSI model.
Switch is a Unicast, multicast and broadcast type transmission.	Hub is a broad cast type transmission.
Switch can have 24 to 48 ports	Hub have 4/12 ports
Different ports have own collision domain	There is only one collision domain.
Switch is a full duplex transmission mode.	Hub is half duplex transmission mode.

Packet filtering is provided.	Packet filtering is not provided.
Switch can be used as repeater.	It cannot be used as repeater
It is an intelligent device that sends message to selected destination so it is expensive.	It is not an intelligent device that sends message to all ports hence it is comparatively inexpensive.
It is ~~generally not~~ widely used.	It is ~~widely used.~~ generally not used.
Hacking of systems attached to ~~hub~~ switch is little easy.	Hacking of systems attached to hub is complex.

Exterior Routing Protocol. ~~(EGP)~~ also known as Exterior Gateway Protocol.

It is used to exchange net-reachability information between Internet gateway belonging to the same or different autonomous system.

EGP has 3 major function.

- Establish a set of neighbours.
- Check status of neighbours (If they are alive/reachable)
- Inform neighbours of the networks that reachable within their AS's

Advantage and disadvantages.

EGP was the first exterior gateway protocol that gained widespread acceptance in the Internate.

EGP is a simple reachability protocols.

Since this routing protocol is designed to be centrally controlled, it reduces the scalability which is a major draw back in today's fast growing Internet.

Q no 7: Write short notes on:-

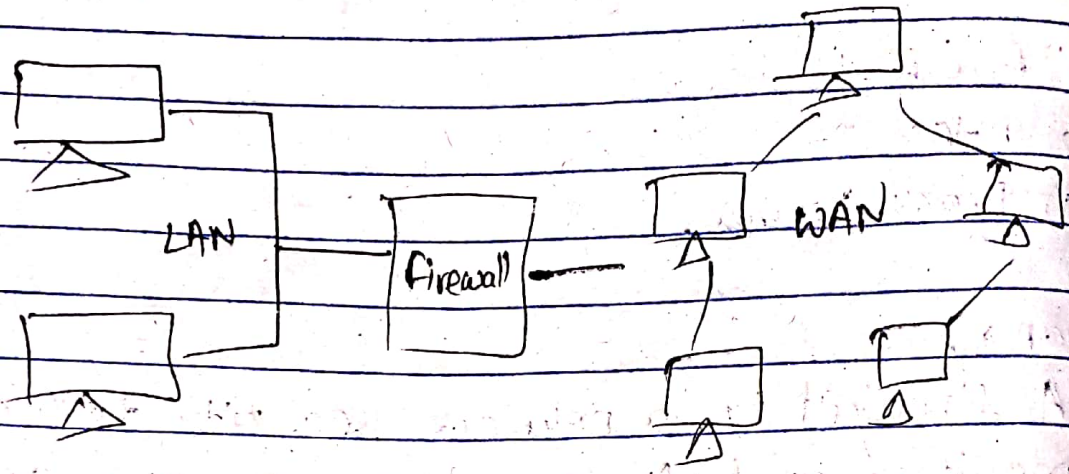
a) Fire Wall
b) DHCP
c) Proxy Server.

Ans.

A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Accept: allow the traffic
Reject: block the traffic but reply with an "unreachable error"
Drop: block the traffic with no reply.

It establish a barrier between secured internal networks and outside untrusted network, such as the Internet.



There are 4 generation of of firewall. Firewalls are generally of two types

1) Host-Based Firewalls
2) Network-Based Firewalls.

bans DHCP

Dynamic host configuration protocol

It is a network management protocol used to dynamically assign an IP address to ~~any~~ any devices, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement

for any user configuration to connect to a DHCP based network.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is default protocol used by the most routers and networking devices.

DHCP manages the provision of all the nodes or devices added or dropped from the network.

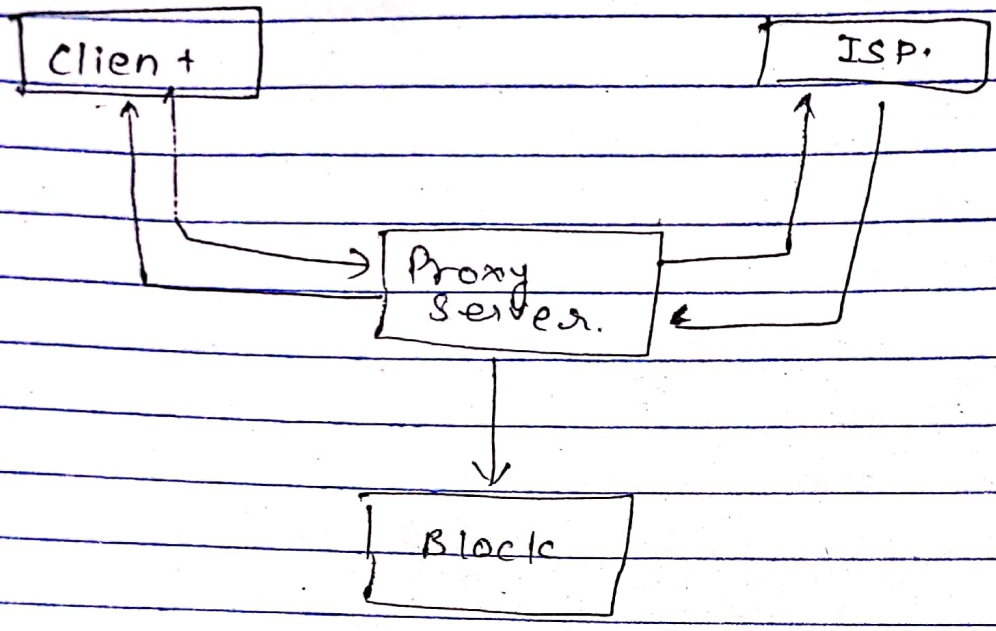
DHCP maintains the unique IP address of the host using a DHCP server.

It sends requests to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

c) Proxy Server

Proxy Server is a computer on the network that has its own IP address. But sometimes, we want to access those websites or servers that are. It is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server. It works as a gateway between the end-user and the internet. It has its own IP address. It separates the client system and web servers. It collects and provide information related to user requests.
The most important point about a proxy server is that it does not encrypt traffic.

There are two main purposes of proxy sever:
- To keep the system behind its anonymous
- To speed up access to a resource through caching.



Mechanism of Proxy Server.