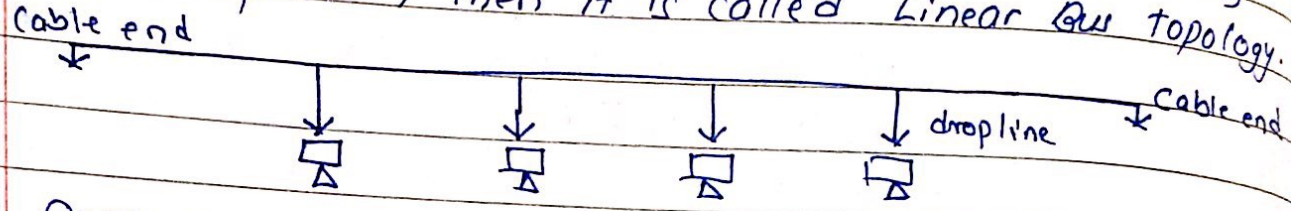
1.a) Explain different topological models in CN ?

→ Network topology: The schematic description of a nlw arrangement, connecting various nodes (sender and receiver) through lines of connection.

A. Bus Topology: every computer and network device is connected to single cable. when it has exactly two endpoints, then it is called Linear Bus topology.

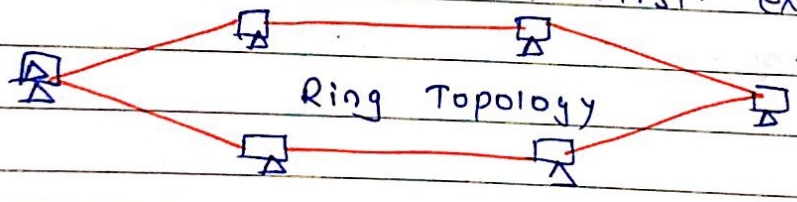


Features: - it transmits data in only one direction
- every device is connected to a single cable

Advantage: ÷ easy to expand, least cable required
- Cost effective, used in small nlw, easy to understand

DisAdvantage: - cable fails leads to whole nlw fails
- Cable has limited length, slower than ring topology
- If nlw traffic has yor nodes are more, nlw performance decr

B. Ring Topology: is called so because it forms a ring as each computer is connected to another computer, with last connected to the first. Exactly 2 neighbours for eac



Features:
- A number of repeaters are used, to prevent data loss. (Or, topology with 100 nodes, one has to pass through 99 nodes to reach 100th node.
- Unidirectional transmission, can be made bidirectional by having 2 connection (dual ring topology), here if one connection fails, 2nd works as backup.

- data is transmitted in sequential manner ie bit by bit

Advantage: - Cheap to install and expand
- transmiting n/w is not affected by adding nodes, as only nodes having tokens can transmit data.

disAdvantage: - troubleshoot difficulty, failure of one → whole.

c. Star Topology: all the computers are connected to single hub through cable, this hub is central node and all other nodes are connected to central node.

features: every node has its own dedicated connection to hub
- Hub acts as repeater for data flow, can be wed: cable

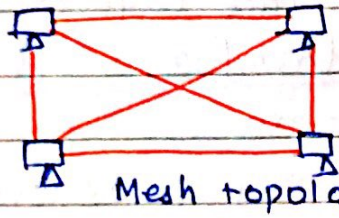
advantage: fast; easy to troubleshoot, setup, modify
: 1 fail ↛ whole n/w, hub can be upgraded easily.

disadvantage: cost high, if hub fails → whole n/w, depends on hub

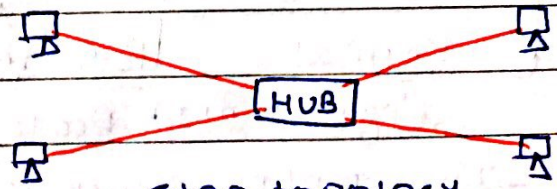
d. Mesh Topology: point to point connection to other device all n/w nodes are connected to each other.
- Mesh has $n(n-1)/2$ physical channel for n devices.
- Two techniques to transmit data a. Routing b. Flooding

routing: nodes have routing logic; to send data using shortest path

Flooding: same data is transmitted to all n/w, robust, -unlikely to loose data, unwanted load.



Mesh topology

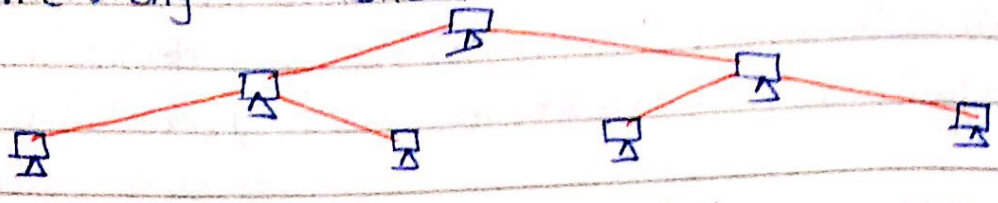


star topology

types: a. Partial Mesh topology: Some device connect to 2/3 devi
b. Full: each & every connected to each other

Features:	Advantage	DisAdvantage
fully connected	- each connection carry data	- more cable
Robust	- Fault dignosed easily	- Bulk wiring is req.
not flexible	- Secured, privacy	- difficult in installation

e. Tree Topology (hierarchichal topology):
It has root node and all other connected to it forming a hierarchy. It should at least have 3 levels.



-ideal if workstation are located in groups, used in WAN
advantage: extension of bus & star, easy to expand, error detect
disadvantage: costly, havily cabled, root node fail → wo

(11b) Discuss the TCP/IP protocol stack with suitable example
Compare TCP/IP with OSI

OSI Model	TCP/IP (protocol suite)			
Application	Telnet	FTP	DHCP	TFTP
presentation	HTTP	SMTP	DNS	SNMP
Session	Application Layer			
Transport	TCP			UDP
	Transport			
Network	ICMP	IGMP		ARP
	IP			
	Internet layer			
Data Link	Network Interface Layer			
Physical	Ethernet	Frame relay	ATM	Token Ring

Fig: TCP/IP Protocol Architecture

-The TCP/IP stack is a complete set of networking protocols. OSI model has 7 layers, TCP/IP
-TCP IP protocol map to 4 layer conceptual model known as DARPA model; Application, transport, Internet, Nlw interfa

Network Internet Layer: (N/w access layer) is responsible for placing TCP/IP packets on the n/w medium and receiving TCP/IP packets of the n/w medium. It includes the LAN and WAN technology details. it likes physical and data link layers. protocol is used to connect to the host, so that packet can be sent.

Internet Layer

- Selection of a packet switching n/w which is based on connectionless internetwork layer is called Internet layer. (it select the best path through the n/w).
- It is the layer which holds the whole arch^r together.
- IP defines a packet and an addressing scheme.
- transfers data bet^n the internet layer and n/w access layer.
- Routes packets to remote hosts.
- ICMP (Internet control message protocol): provides control and messaging capabilities.
- ARP (Address resolution protocol): determine dL layer, MAC Addr
- Reverse ARP (RARP): determine IP address for known MAC addresses

Transport Layer:

- provides logical connection bet^n source & dest^n host.
- breaks data into small unit, arrange data in sequence
- multiplexing, segmenting or splitting on data is done.
- uses port no to create process to process communication
- creates packet from bytes stream received from app layer

Application Layer:

- handles high-level protocol, representation, encoding
- TCP/IP protocol suite combines all application related issues into one layer

TELNET, FTP, SMTP, DNS

(Comparing TCP/IP with OSI)

TCP/IP	OSI
→ TCP/IP → Transmission Control protocol and Internet Protocol	→ OSI refers to Open System Interconnection.
→ It has 4 layer	→ has 7 layers
→ More reliable than OSI	→ less
→ doesnot have very strict boundaries	→ have
→ It follow horizontal approach	→ It follows vertical approach
→ TCP/IP is protocol dependent	→ OSI is protocol independent
→ it doesnot gaurantee the delievery of packet	→ It gaurantees the delievery of packet
→ is implementation of OSI	→ It is a reference model
→ Nlw layer of TCP/IP provides connectionless service	→ Nlw layer of OSI provides both connection oriented and connectionless
→ developed by Dept of defense(DoD)	→ developed by ISO
→ layers are:	→ layers are
→ It is a client-Server model	→ It is conceptual model
→ Bot Top to Bottom	→ bottom-up approach

→ TCP/IP is a standard protocol used for every nlw including internet whereas OSI is not a protocol but a reference model used for understanding and designing the system architecture

→ TCP/IP is used for end to end connection so as to transmit the data over the internet.

→ TCP/IP is robust, flexible, tangible

(Q10) Explain term: bandwidth, throughput, latency, Jitter. Explain working principle of Satellite Comm. System

Simply,

bandwidth : How big the pipe is ?

Throughput : How much data we can get through the pipe.

Latency : How long it takes to get there. A slow router can hold up the regardless of connections bandwidth

Jitter : Packets arriving out of order

Bandwidth is the amount of data that can be transferred from one point to another in a fixed amount of time (usually second) or range within a band of frequencies and wavelength.

20 Mbps : 20 megabits data can be uploaded/downloaded in a second. and it is not a speed.

Latency : is the time that a data packet takes to travel from one point to another. (delay). It is a natural phenomenon. everything needs time to travel even light.

Example : time takes a packet to travel from google's data centre to our computer.

bandwidth is like highway and speed of car (ie 60 mph) is latency.

By increasing bandwidth, you are increasing capacity not speed.

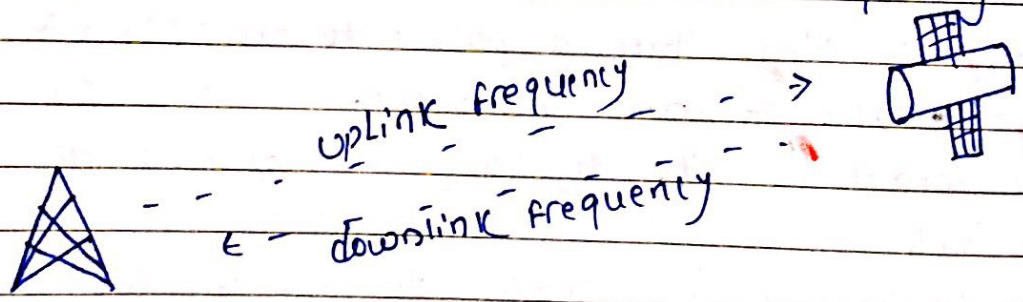
Throughput : The actual speeds at which data can be transferred by a device is called throughput.

bandwidth ≥ throughput. It is how much data actually does travel through the channel. it can be limited by bandwidth, latency.

when we speak about VoIP n/w, it can be issues.

→ Satellite is a body that moves around the earth in mathematically predictable path (orbit). A Communication satellite is microwave repeater station in space that is helpful in comm, radio, tv along with internet applications. Repeater is a device which increase the strength of signal it receives and retransmits it. Here, repeater work as transponder (which change the frequency band of the transmitted signal, from received one.

- The frequency with which the signal sent to space called uplink frequency and frequency with which it is sent by transponder is called downlink frequency.



(working Mechanism)

Satellites need power, receiver and antennas. Satellites are powered by solar panel. The data is The satellite is connected to computer system for processing of data. The data is received and sent back using satellites. These satellites can gather the

instruction from these system as well. Satellites constitute many sent back using satellites. These satellites can gather the instruction from these system as well. Satellites constitute many sensors, these sensor enable it to process the data and send it to the earth. Telemetry system is a key to the purpose and operation of satellite working. Satellite send encoded information to the earth based station. This information is decoded using transponders. The working of satellites is possible with power distribution to all the components connected to the satellites.
Example: GPRS Tracking.

2.1b) Compare ckt switching and packet switching. Illustrate with diagram.

– Packet switching and ckt switching are two ~~n~~ wing methods for transfering data betⁿ two nodes or hosts. ~~For a~~

	Circuit Switching	Packet Switching
1.	It has 3 phases a. Connection establishment b. Data Transfer c. Connection Released	1. In packet switching, directly data transfer taked place
2.	each data unit know the entire path address which is provided by source	2. each data unit just know the final destⁿ address. Intermediate path is decided by Route
3.	data is processed at source system only.	3. data is processed at all intermed node including source system.
4.	delay betⁿ data is uniform	4. not uniform
5.	more reliable	5. less reliable
6.	wastage of resources are more	6. less

7. Resource reservation is done	7. No
8. Connection oriented	8. Connectionless
9. message is received in order, sent from the source.	9. Packets of message are received out of order & assembled at the destination
~~10. Implemented at pl~~	
10. Implemented at physical layer.	10. Implemented at N/w Layer
11. Intially designed for voice communication.	11. Intially designed for data transmission.
12. Inflexible, once a path is set all parts of transmission follows same path.	12. Flexible, route is created for each packet to travel to destination
13. It is 2 types: ↳ Space division switching ↳ Time Division Switching Ex: PSTN, PBX	13. It has 2 types: ↳ Datagram approaches ↳ virtual circuit approaches

→ Packet switching is more efficient than Circuit switching whereas, when it comes to voice transmission, ckt switching is more efficient than packet switching.

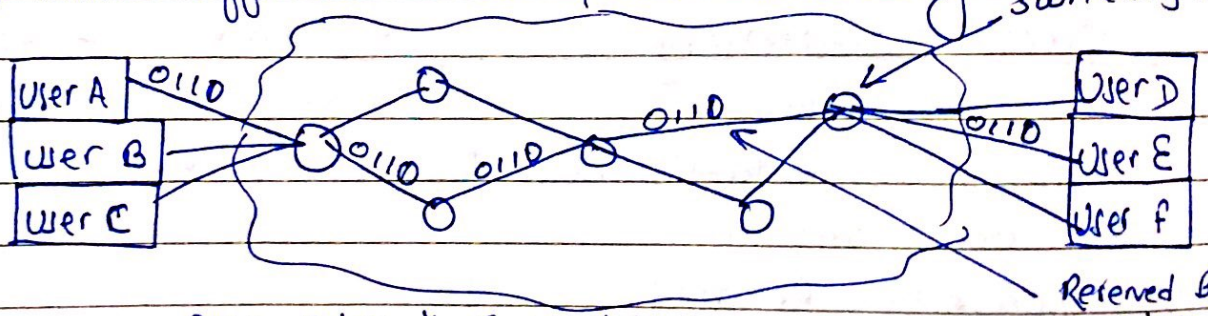


fig: Circuit Switching

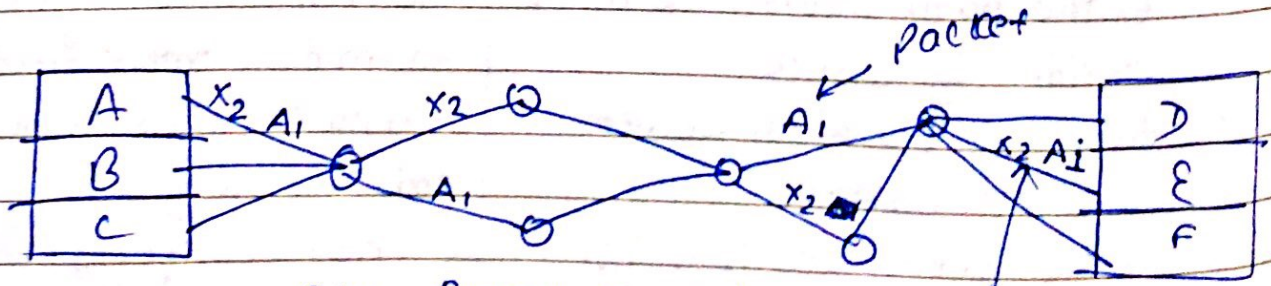


fig: Packet Switching

shared bandwidth

(310) Explain channel access mechanism in CSMA/CD

Short For Carrier Sense multiple Access / collision Detection, CSMA/CD is a Media Access Control (MAC) protocol. It defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision.

- The CSMA/CD rules define how long the device should wait if a collision occurs. The medium is often used by multiple data nodes, so each data node receives transmissions from each of the other nodes on the medium.
- To reduce the Impact of collision, Ethernet uses an algorithm called CSMA/CD which is a MAC protoo in which the station senses the carrier/channel before transmitting frame just as in persistent or

- If two or more computer should happen to send data exactly the same time through same medium then there will be data collision

⟹ CSMA/CD works by each node checking that media is not being used before placing its message to the line. The node will continue to listen throughout the transmission and if a collision occurs then sending station will stop transmission and put a jamming signal on the line to warn all other nodes to hold back. The transmitting nodes will apply a backoff algorithm to generate random time before they try to transmit again.

→ Due to the effect of attenuation, CSMA/CD is not effective beyon 1.5 miles (2500m).

→ In CSMA/CD, every host has equal access to the wire and can place data on the wire, when wire is free from traffic - when a node want to place data on the media, it sense the wire to find whether there is signal already. If traffic, wait until traffic is free.

→ Collisions destroys the data, then retransmission occu

Algorithm :

1. If (medium is idle) transmit; else step 2;
2. If (medium is buy) continue listen until channel is ready and transmit immediately
3. If (collision detected) transmit jamming signal and cease transmission
4. wait Random time then GOTO 1.

Traditional Ethernet uses CSMA/CD

[ecomputernotes.com]

(3)b) What is error control ? How forward error control (FEC) technique will help to detect and correct the error.

- Error control is the process of identification or correction of error occured in transmitted data.
- when data is transmitted over a cable or channel, always a chance that some of the bits will be changed/corrupted due to noise/signal distortion or attenuation.
- The purpose of error control is to ensure that information received by reciever is exactly the information transmitted by sender.

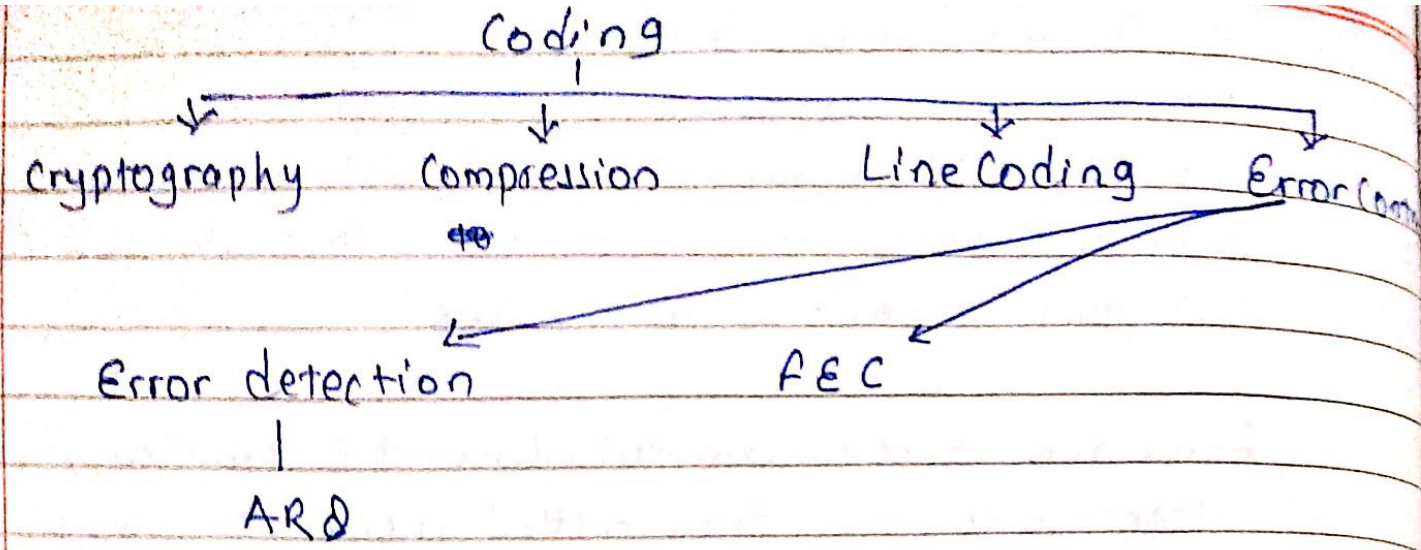
- Forward Error Control
- Backword (feedback Error Control (ARQ)

Note: In datalink layer, error control means detection of error and retransmission of data, this process is called Automatic repeat Request (ARQ).

Forward Error Control (FEC): Additional redundant information is transmitted along the useful data. Hence, the receiver not only detects the error, but also correct it. This method is not widely used because of the additional redundant information.

- Forward Error Correction (FEC) is a digital signal processing technique used to enchance the data reliability. It does this by introducing redundant data, called error correcting code or, prior to data transmission.
- FEC provides the receiver with the ability to correct errors without a reverse channel to request the retransmission of data. (Channel coding)
- The first FEC code, called Hamming code, it is a method adopted to obtain error control in data transmission where the transmitter sends redundant data only a portion of data without apparent error is recognized by receiver. This always broadcast to multiple dest^n from single source.
- possible for the receiver to detect and correct error without reference to sender

types
- Block code (BCH)
- Convolution Codes.



(4|a) Explain HTTP protocol. Describe the difference between SMTP, POP and IMAP services

→ HTTP Short for HyperText Transfer protocol, HTTP is a set of standards that allow users of the World wide web (WWW) to exchange information found on web pages. HTTP is the underlying protocol used by WWW and this protocol defines how messages are formated and transmitted and what actions web servers and browsers should take response to various Commands.

Example: when you enter a URL in your browser, this actually sends an HTTP Command to web server directing it to fetch and transmitting webpage. The other main standard that control How the WWW works is HTML, which covers how web pages are formated & displayed HTTP is an application protocol that runs on top of the TCP/IP suite of protocol. HTTP client is Chrome. latest version of HTTP is HTTP 11.

- when you enter URL, browser builds an HTTP request and sends it to the Internet Protocol address (IP address) indicated by the URL. The HTTP daemon in dest^{n} server response back.
- HTTPS (HyperText Transfer protocol secure) which uses

HTTP on connection encrypted by transport layer security
It is the default protocol for web transaction.

	IMAP	POP	SMTP
1.	Internet Message Access Protocol	Post office Protocol	Simple mail Transfer Protocol
2.	Retrieving emails	Retrieving emails	Sending emails
3	Email server Port : 143	110	25
4.	Limitations: Mailbox on server has definite quota and thus one needs to ensure that mailbox retains space for new mails	once the msg get downloaded on local computer, it remains accessible in that computer only.	It has no ways to verifying sender. This sometimes leads to Spam Issues.
5.	used in client & server	Used in client & server	used in client

→ If you are using email, you are using SMTP and (IMAP or POP) unknowingly.

1. POP : POP downloads email directly to your computer when this happens, the mail is deleted from server. This process occurs to prevent from reading same mail. That mail is available in your computer even no internet.

2. IMAP : It receives and held your email by your mail server. It requires small amt of data transfer, so could work with slow connection. Emails only dld when a specific email will be read. you can manipulate. It allows encryption. Ex : IMAP

SMTP: The way of mail transfer Agent (MTA) to deliever your email to receipts' mail Server. The SMTP protocol cannot receive.

Email forwarding: operation of re-sending on email message delievered to one email address to a possibly different address

(4|b) The existing nlw of PU (172.31.255.0/22) has 5 different schools, any 2 schools divided into 4 different department. provid IP plan which includes
- Network address, Broadcast address
- Usable IP pool
- Subnet mask and coild card Mask.

→ **Solution**

Given,

Network Address : 172.31.255.0/22

Subnet : 22

Host bit : 32 - 22 = 10

Total host : $2^{10} = 1024$

Usable host : 1024 - 2 = 1022

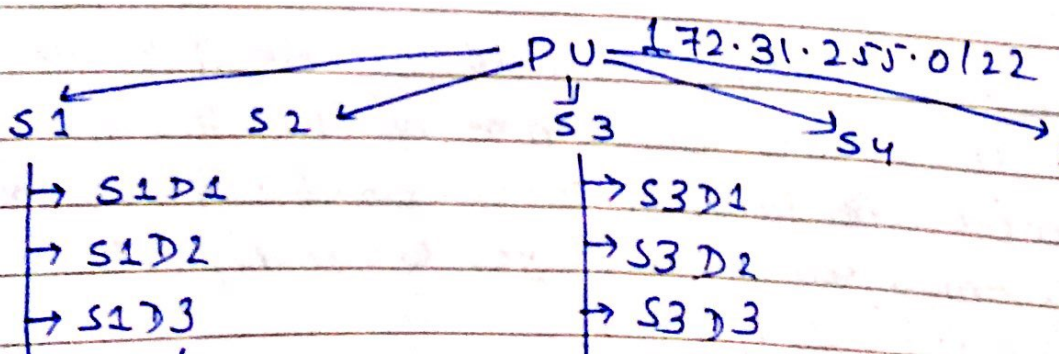
Now,

Requirement

Number of schools : 5 $(2^x > 5)$ $(x = 3)$

Network bit : 3

total network : $2^3 = 8$ (≥ 5)



So, Network bit is 3

000 → S1
001 → S2
010 → S3
011 → S4
100 → S4
101 } future use
110
111

New Subnet

172.31.111111|11.0|0000000 /25

22 + 3 = 25

125, subnet mask: 11111111.11111111.11111111.10000000

↳ 255.255.255.128

Wildcard mask

255.255.255.255
255.255.255.128
0.0.0.127

School 1: (000)

For Network Pool

172.31.111111|00.0| 0000000 → 172.31.252.0 /25 (NIW)
0000001 → 172.31.252.1 /25
⋮
1111110 → 172.31.252.126 } Host
172.31.111111|00.0| 1111111 → 172.31.252.127 (Broadcast)

/25, subnet → 255.255.255.128
wildcard → 0.0.0.127

School 2: (001)

172.31.111111|00.1| 0000000 → 172.31.252.128 → Network
0000001 → 172.31.252.129
⋮
1111110 → 172.31.252.254 } Usable Host
172.31.111111|00.1| 1111111 → 172.31.252.255 → Broadcast

125, Subnet mask: 255.255.255.128
wildcard mask: 0.0.0.127

School 3 (010)

172.31.111111|01.0|0000000 → 172.31.253.0 (N/w)
172.31.111111|01.0|0000001 → 172.31.253.1 } usable host
⋮
172.31.111111|01.0|1111110 → 172.31.253.126
172.31.111111|01.0|1111111 → 172.31.253.127 (Broadcast)

125, subnet mask: 255.255.255.128
wildcard mask: 0.0.0.127

School 4 (011)

172.31.111111|01.1|0000000 → 172.31.253.128 (Network)
172.31.111111|01.1|0000001 → 172.31.253.129 } Host
⋮
172.31.111111|01.1|1111110 → 172.31.253.254
172.31.111111|01.1|1111111 → 172.31.253.255 (Broadcast)

125 255.255.255.128 (subnet) / 0.0.0.127 → wildcard

School 5 (100)

172.31.111111|10.0|0000000 → 172.31.254.0 (N/w)
172.31.111111|10.0|0000001 → 172.31.254.1 } Usable
⋮
172.31.111111|10.0|1111110 → 172.31.254.126
172.31.111111|10.0|1111111 → 172.31.254.127 (Broadcast)

for sub department :

School 1, Department

total sub department : 4

Network bit : 2

total Nlw : $2^2 = 4$

New Subnet

Nlw address of school 1 is : 172.31.252.0/25

172.31.252.0 00000000 / 27

25 + 2

/25, subnet : 11111111.11111111.11111111.11100000

255.255.255.224

coildcard : 0.0.0.31

for department 1 of school 1 (S1D1) (00)

172.31.252.000 00000 → 172.31.252.0 (Nlw address)

172.31.252.000 00001 → 172.31.252.1

:

172.31.252.000 11110 → 172.31.252.30 } Usable host

172.31.252.000 11111 → 172.31.252.31 (Broadcast)

For S1D2 (01)

172.31.252.001 00000 → 172.31.252.32 (Nlw)

172.31.252.001 00001 → 172.31.252.33

:

172.31.252.001 11110 → 172.31.252.62 } HOST

172.31.252.001 11111 → 172.31.252.63 (BC)

SID3 (10)

172.31.252.010|00000 → 172.31.252.64 (Nlw)
172.31.252.010|00001 → 172.31.252.65
} HOST
172.31.252.010|11110 → 172.31.252.94
172.31.252.010|11111 → 172.31.252.95 (BC)

SID4 (11)

172.31.252.011|00000 → 172.31.252.96 (Nlw)
172.31.252.011|00001 → 172.31.252.97
} HOST
172.31.252.011|11110 → 172.31.252.126
172.31.252.011|11111 → 172.31.252.127 (BC)

for department of school 3

total sub department: 4
Nlw bit : 2
total Nlw : 4

new Subnet

Nlw address : 172.31.253.0/25
Ans → 172.31.253.000|00000/27
25+2
/27 → 11111111.11111111.11111111.111|00000 →
255.255.255.224 (subnet mask)
wildcard mask : 0.0.0.31

S3D1 (00)

172.31.253.000|00000 → 172.31.253.0 (Nlw)
172.31.253.000|00001 → 172.31.253.1
:
172.31.253.000|11110 → 172.31.253.30
11111 → 172.31.253.31

S3D2 : (01)

172.31.253.001|00000 → 172.31.253.32 (N/W)

00001 → 172.31.253.33 } HOST

11110 → 172.31.253.62

172.31.253.001|11111 → 172.31.253.63 (B/C)

S3D3 : (10)

172.31.253.010|00000 → 172.31.253.64 (N/W)

00001 → 172.31.253.65 } HOST

11110 → 172.31.253.94

172.31.253.010|11111 → 172.31.253.95 (B/C)

S3D4 (11)

172.31.253.011|00000 → 172.31.253.96 (N/W)

172.31.253.97 } HOST

172.31.253.126

172.31.253.011|11111 → 172.31.253.127 (B/C)

(S10) Explain Difference between distance vector Routing and Link State Routing

→ The primary responsibility of router is to direct packets destined for local local and remote networks by

a. Determining the best Path.

b. forwarding packets towards the destination.

A Routing protocol is the comm. used between Routers. A Routing protocol allows router to share information about networks and their proximity. Routers use this to maintain routing table.

Routing protocol

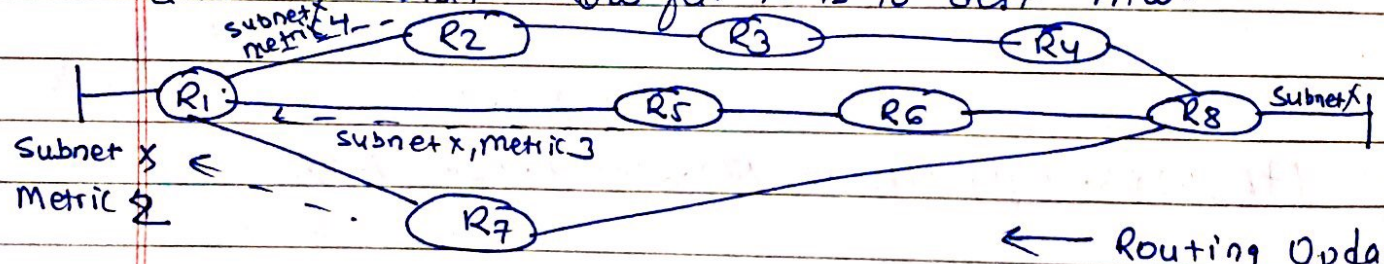
Static — Dynamic

Interior Gateway Protocol (IGP)
- Distance vector protocol
- Link state protocol

Exterior Gateway Protocol (EGP)

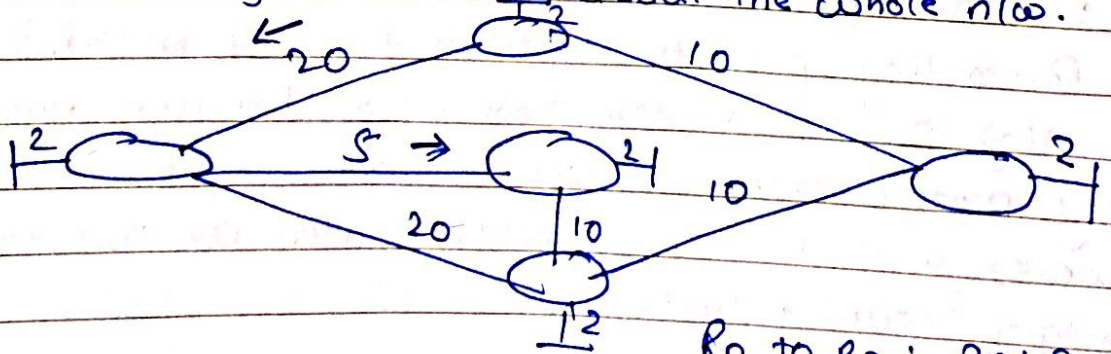
a. Distance Vector Routing Algorithm:

DV means that routes are advertised as vectors of distance and direction. Distance is defined as metric (hop count) and direction is simply the next hop router or exit interface. A router using this does not have knowledge of entire path to a destination; instead the router knows only the direction or interface in which packets should forwarded and the distance how far it is to dest^n nlw.



b. Link State Routing Algorithm (Shortest path routing)

Information about the state of Link (Network Interface) called Link state. Requires that all routers know about the paths reachable by all other routers in Network. Hence, They know more about the whole nlw.



R2 to R3 : 20+5+2 = 27

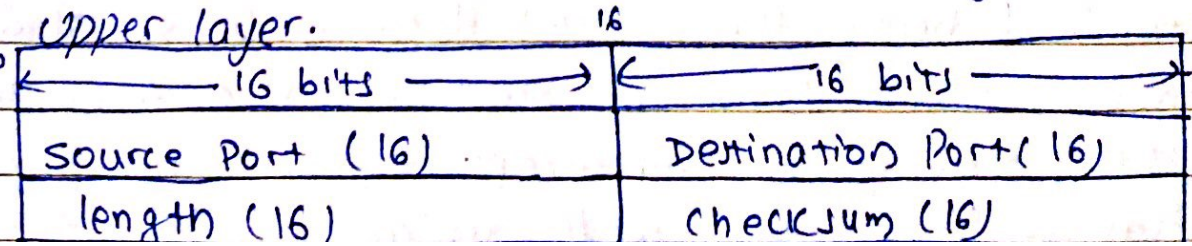
Distance Vector Vs Link State → Page: 120 (Photocopy)

Distance Vector	Link State
1. Uses hop count as metric	1. Uses shortest path
2. View the nlw from the perspective of neighbour	2. Get common view of entire network topology
3. Has frequent and periodic updates	3. has event triggered updates
4. Slow convergence	4. Fast convergence
5. Susceptible to routing loops	5. Not as susceptible to routingLoops
6. Easy to configure and administer	6. Difficult to configure & administer
7. Requires less memory & processing power of routers.	7. Requires more ~~power~~ processing power & memory than DV.
8. Consumes a lot of BW	8. consumes less BW
9. passes copies of routing table to neighbour router	9. Paves link-state routing updates to other routers.
10. Eg RIP	Eg: OSPF

(5)b) What is the role of UDP Protocol? Discuss TCP and UDP socket in terms of data transmission and security.

→ UDP (User Datagram protocol) is connectionless transport protocol in TCP/IP protocol stack. UDP is simple protocol that exchanges the datagram without gaurantee delievery. It is alternatives of TCP, combines with IP, it is UDP/IP. UDP uses internet protocol to get a data unit (datagram) from one computer to another.

UDP doesnot support reliability or ack so it is referred as unreliable Datagram protocol. Any reliability issues handled in upper layer.



	TCP	UDP
1.	Transmission Control Protocol	1. User Datagram Protocol
2.	Connection-oriented Protocol	2. Connectionless protocol
3.	Reliable (virtual circuit); check message delivery.	3. Unreliable; doesnot check message delievery.
4.	Divides outgoing msg into Segments	4. Divides outgoing message into Datagrams
5.	Provides flow control	5. provides no flow control
6.	More overhead than UDP (less efficient, slow)	6. less overhead than TCP (more efficient, faster)
7.	Example, HTTP, FTP, SMTP, Telnet	7. Example, DNS, DHCP, TFTP, SNMP, RIP, VOIP
8.	TCP rearrange data packets in order specified	8. Application layers has to manage since, no ordering in UDP
9.	TCP header size is 20 Bytes	9. It's header size is 8 Bytes
10.	Handshake : SYN, SYN-ACK, ACK	10. No Handshake (connectionless protocol)

6(a) What is Virtual circuit switching? Explain how Routers build routing table using RIP.

Switching

- Circuit switching
- Packet switching
  - → Virtual circuit PS
  - → Datagram PS

In virtual ckt pckt switching, a virtual path is made before the actual data is transmitted, but it is different from ckt switching in a sense that in ckt switching the call accept signal comes only from final dest^n to source while, in case of VC, this call accept signal is transmitted bet^n each adjacent intermediate node.

Virtual Circuit [Geeks for Geeks]

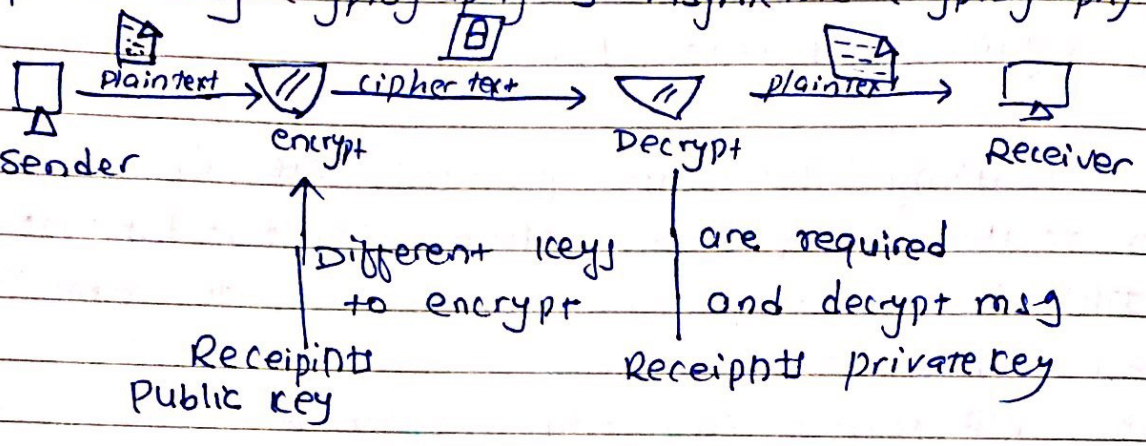
1. it is Connection Oriented ie reservation of resources like buffer, CPU, bandwidth etc for the time in which virtual circuit is used by data transfer session
2. First packet reserves resources and path and preceding packet follow same path. so that only first packet has a global header
3. All data (packets) reach in order [Highly Reliable]
4. At each time, new connection has to be setUp if again transmission happens

- The Routing Information protocol (RIP) defines a way for routers, which connect nws using the Internet Protocol (IP), to share information about how to route traffic among networks.
- Each RIP router maintains a routing table, which is a list of all the destination (nws). It knows how to reach, along with the distance to that destination. RIP uses a distance vector algorithm to decide which path to put a packet on get to dest^n.
- It stores in its routing table distance for each network it knows how to reach, along with the address of the "next hop" router, -- another router that is on one of the same networks -- through which a packet has to travel to get to that dest^n.
- If it receives an update on route, new path is shorter; it will update its table entry with the length and the next-hop address of shorter path; if new path is longer; it will wait through a hold-down period to see if later updates reflect the higher value as well and only update the table entry if the new, longer path is stable.

- Using RIP, each router sends its entire routing table to its closest neighbour, and neighbour in turn will pass and so on, until all RIP hosts within the network have some knowledge of routing paths, a state known as convergence

(6/b) Explain public key Cryptography. Explain Diffie-Hellman key exchange.

→ public key Cryptography is Asymetric cryptography



public key cryptography is an asymetric scheme that uses pair of keys for encryption: a public key, which encrypts a data, and a corresponding private or secret key for decryption. you publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can encrypt data that can be read by you. It is computationally infeasible to deduce the pvt key from public key and public key cannot decrypt it. Only the person who has corresponding private key can decrypt the information

- Different keys are required for encryption and decryption
- Receiver needs to publish an encryption key, public key.
- Each receiver posses a unique decryption key → pvt key.
- Three type of public key Encryption schemes
  - → RSA cryptosystem
  - → ElGamal CryptoSystem
  - → Eliptic curve cryptography

- The Diffie-Hellman key exchange is a secure method of transferring (exchanging) cryptographic keys. This method allows two parties which have no prior knowledge of each other to establish a shared, secret key, even over a insecure channel.
- The general idea of Diffie-Hellman involves two parties exchanging numbers and doing simple calculation in order to get a common number which serves as the secret key.
- Asymetric Encryption requires transfer of private key. The most challenging part in this type of encryption is to transfer the encryption key from sender to receiver without anyone intercepting this key in between.
- This transfer or rather generation on same cryptographic keys at both sides secretively was made possible by it.
- But, even though, it uses same principle as public key cryptography this is not asymetric coz, nothing was encrypted during exchange

Example: lets assume Alice wants to share secret with Bob

1. Alice and Bob agree on prime number, p and a base g in advance. For our example, assume $p=23$ and $g=25$
2. Alice chooses secret integer a, $a=6$ and computes $A = g^a \% p$
   A becomes 8
3. Bob chooses secret integer b, $b=15$ and computes $B = g^b \% p$
   B becomes 19
4. Alice sends A to Bob and Bob send B to Alice
5. To obtain share secret, Alice computes $s = B^a \bmod p$
   $s=2$
6. To obtain share secret, Bob computes $s = A^a \bmod p$
   $s=2$

→ This algorithm is secure because the values of a and b which required to derive s are not transmitted accros the wire

Company's private, internal network.
- VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources.
- To ensure safety, users must be authenticated using passwords, tokens and other identification methods -- to gain access to the VPN
- The first step to security is firewall betⁿ client and host server, requiring remote user to establish an authentica connection with the firewall. (point to private n\w).
- VPN uses a technique known as tunneling to transfer data securely on the internet to a remote access
- Sensitive data is hidden from public but accessible to appropriate ~~data~~ users through VPN.
- There are following ways to create VPN connection:

a. By dialing an Internet service provider (ISP)

- If you dial-in to an ISP, your ISP then makes another call to private networks remote access server to establish the PPTP or L2TP tunnel after authentication you can access private N\w.

b. By connecting directly to an Internet

- If you are already connected to an Internet, LAN, cable model, digital subscriber Line (DSL), you can make a tunnel through the internet and connects directly to the remote access server. After authentication, you can access the corporate network

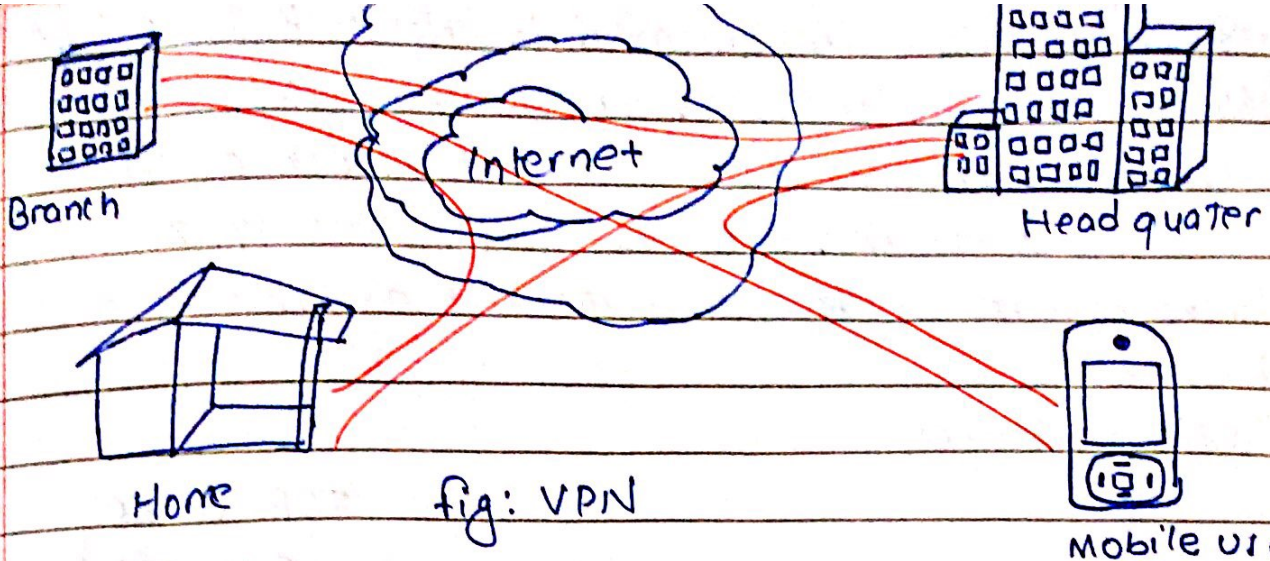


fig: VPN

(7.1.c) TCP Socket

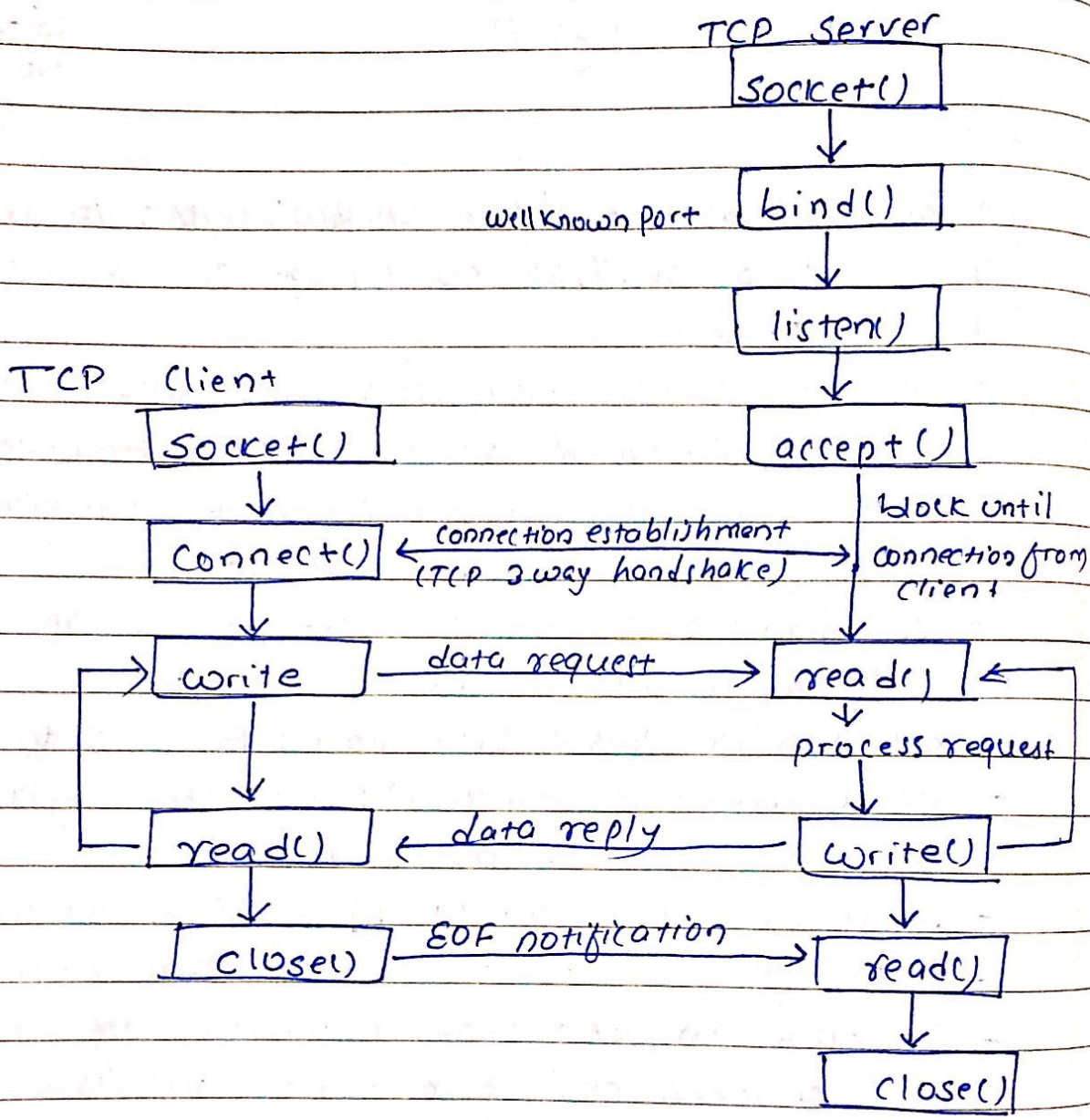
- The TCP Socket allows application makers to implement any protocol available on top of TCP such as IMAP, IRC, POP, HTTP etc
- on a TCP/IP nlw, every device must have an IP address (it identifies the device ie computer). However an IP address alone is not sufficient for running nlw applications as a computer can run multiple application/services.
- IP identifies the computer, port identifies application or services
  IP address + Port number = Socket
- Port number uses 16 bits, varies from 0 to 65535
- Well known ports (0-1023): registered by IANA.
  eg: web servers: 80, SMTP: 25
- Registered port (1024-49151) → semi revised
- Port (49152-65535) - Client program (free to use)
- A Connection between two computers uses a Socket
- each ~~connect~~ end of connection will have Socket
- One can open 2 browsers, one looking at google and other Yahoo website. the connection would be
  your PC - IP1 + port 60200 —— Google IP2 + 80 (standard)
  ie IP1 + P60200 = Socket of Client
  IP2 + 80 = Socket of google server
  Client port no. is dynamically assigned and reusable once session ends.

- IP address are implemented in Network layer (IP layer)
- Ports are implemented at transport layer - TCP and UDP
- The TCP/IP protocol support - TCP port or UDP port

TCP - Connection oriented, error checking, retransmit packets

UDP - Connectionless, no error checking, will not retransmit

Client Server



First server is started, sometimes later, client connects to server we assume that client requests to a server, server process request and responses back to client. This process continues until client closes its end of connect which sends end of file notification to server. The server closes the connection and either terminates or wait for new client.

1a) Client-Server Architecture. How is it more secure than P2P?

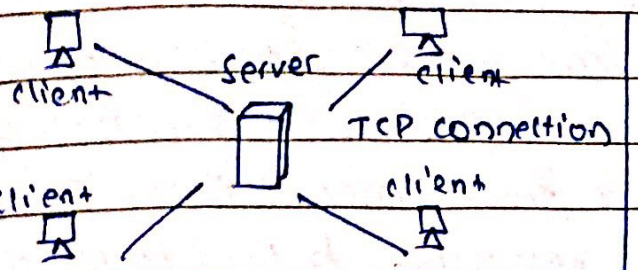


fig: client-server

Client server is a program relationship in which one program (client) requests a service or resources from another program (the server).

- The client-server model is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers and service requesters, called client.
- clients and servers exchange messages in a request-response pattern. The client sends a request, server responses.
- Clients /server example are: web browser, mail
- The client server architecture decreased traffic network by providing a query/response rather than a total file transfer.
- Remote procedure call (RPCs) or standard query language (SQL) are used to communicate between client and server.
- The performance is depends on processor speeds, memory, bandwidth, capacity, disk speeds, input-output devices
- The ~~etc~~ system is scalable, client can be added.
- The environment is Heterogenous and multivendor ie the os, hlw is not same bet^n client and server.
- client and server process communicate through API and RPCs.

• Another type of nlw architecture is peer to peer (P2P), in which computer is both client and server.

- Client Server is more secured than peer to peer N/W because client server can have passwords to own individual profiles so that nobody can access anything what they wa
- All the data is stored onto the servers which generally have far greater security than most client. Server can control the access and resources better to guarantee that only those clients with appropriate permissions may access and change data.
- P2P is less secure because security is handled by individual computers, not on the network as a whole.
- P2P doesnot have central storage or authentication of client, all clients are conversly dedicated servers

Client Server	Peer to Peer
1. Specific server and specific clients.	1. each node act as client or server
2. client request forserver responses.	2. each node can request for service and provide services
3. Focus on sharing Information.	3. Focus on Connectivity.
4. The data is stored in a centralized server.	4. Each peer has its own data.
5. When too many client request, server can be bottlenecked	6. As service are provided by several servers, not bottlenecked.
6. Expensive	6. Cheap
7. Secured	7. less secured
8. stable / scalable	8. unstable /

(11b) What are the reasons for using layered protocols? Explain the function of various layers in OSI reference model.

The reasons of using layered protocol are:

1. By breaking network communication into layers, it is easier to write programs to communicate with a standard 'presentation' level layer instead of something complicated like and entire protocol
2. By using layered protocol, it is easier to debug problems as you can easily identify what layer network fails
3. If someone writing message app, they can simply pass the info down to other layers, with necessary info, doesnot have to worry about anything like TCP connection etc.
4. One layer provides the service to upper layer so, one layer works independently
5. protocol layering is a common technique to simplify network design by dividing them into functional layers, assigning protocols to perform each task.

Ex: one protocol is designed to perform connection and another data delievery but doesnot concern about connection.

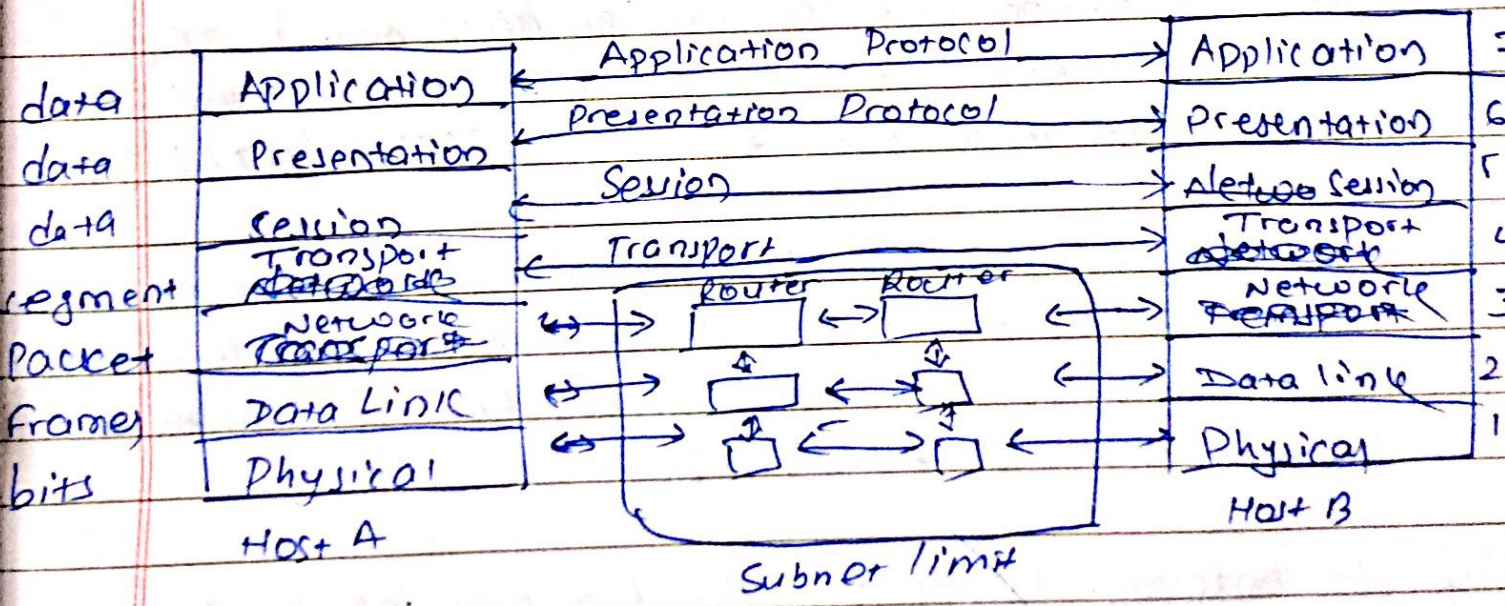


fig: OSI Reference Model

1. Physical layer: This layer conveys the bit stream through the network at the electrical, radio level. Data encoding is done. It provides the hlw means of sending and receiving data on a carrier network. Example: Ethernet, RJ45,

2. Data Link Layer: This layer set up links accross the physical nlw, putting packet into nlw frames. Its function is to make sure data transfer is error free from one to another. Transmitting and receiving data frames sequentially is managed by this layer (Ethernet)

3. Network Layer: This layers handles routing and addressing of the data, creating logical path for transmitting data from node to node. Routing, forwarding addressing, error handling, congestion control and packet sequencing are done in this layer. (IP)

4. Transport Layer: It provides transparent transfer of data between end systems or hosts and is responsible for end to end error recovery and flow control, it ensures complete data transfer. (TCP/UDP)

5. Session Layer: It Establishes, manage, terminates Connection bet^n application. It sets up, Coordinates and terminates Conversations, exchange dialogues bet^n application at each end (RPCs, SQL)

6. Presentation: Encryption, transform data into the form which application layer accepts. Called syntax layer. (ASCII, MIDI

7 Application: Supports one end user processes. Communication partners identified, authenticated. FTP, HTP, www browser

(8a) Compare Copper wire with fiber optics

Compare	Fiber	Copper
1. Bandwidth	10 Gigabit and beyond	Gigabit
2. Future-proof	Evolving towards the desktop	CAT7 under development
3. Distance	40km + @ 10,000 Mbps	100m @ 1000 mbps
4. Noise	immune to RFI, EMI	interfered.
5. Security	almost imposible to tap	susceptible to taping
6. Speed	fast	slower
7. Power	uses less power and provides less signal degradation	use more power. losses of data.
9. Sustainable	inflamable, suited for data transmission	-
10 Cost	Expensive	Cheap
11 Skill	needs skill ~~poo~~ to install	no need of skill engineer to install copper wire
12 Reliability	extremely reliable coz core is made of glass, no electric current (light)	less reliable than fiber optics
13 Durable	light in weight, more durable	heavy, less durable
14 Used	mostly backbone	in normal connection
15 Attenuation	low attenuation (less data loss)	high attenuation
16 lifecycle	30 - 50 yrs	5 - 10 yrs

(21b) What are the factors that affect (cause) Congestion? Explain Leaky and Token Bucket Traffic Shapping.

→ Congestion is a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss.

Congession in a network may occur if load on the network (no. of packet sent to nlw) is greater than the capacity of network (no. of packets a nlw can handle)

- Congestion control is a techniques to keep the load below the capacity

Congestion
- Open Loop (prevention)
  - Retransmission Policy
  - window policy
  - Acknowledgment Policy
  - Discarding Policy
  - Admission policy
- closed loop (detect, feedback & correct) (removal)
  - Back pressure
  - choke packet
  - Implicit Signaling
  - Explicit signaling

The factors that causes Congestion are:

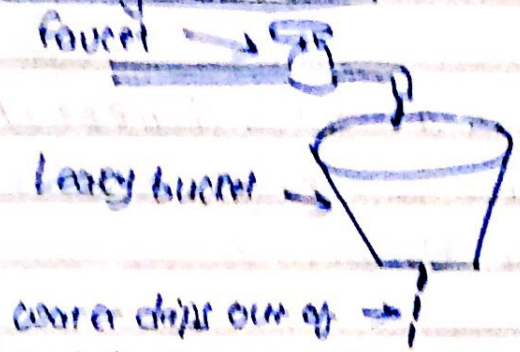
1. If routers are too slow to perform bookkeeping task (queuing buffers, updating table)
2. Congestion in a subnet occur if the processors are slow. Slow speed cpu results · queues even though there is excess line capacity
3. Too many hosts in the network ie network overload (too many request at once)
4. Broad cast storms (situation where there are unexpectedly too many request on a nlw); resuting nlw doesnot have ability to process all req. at once.
5. low bandwidth leads to traffic, becomes Congestion
6. multicasting (many computer speak each other simultaneously) leads to collision so, nlw becomes Congestion

Traffic shaping or packet shaping. Set of bandwidth mgmt. It is the manipulation and prioritization of network traffic to reduce the impact of heavy user or machines from affecting other users. It is done by delaying the flow of certain packets and prioritizing the flow of other preferred streams.

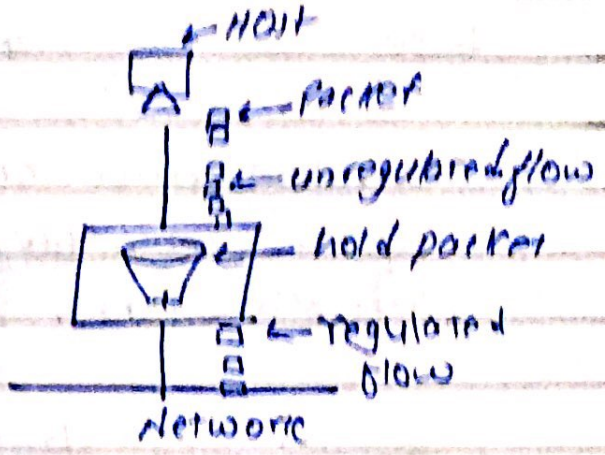
Traffic shaping algorithm

1. Leaky Bucket 2. Token Bucket

a. Leaky Bucket



(a)



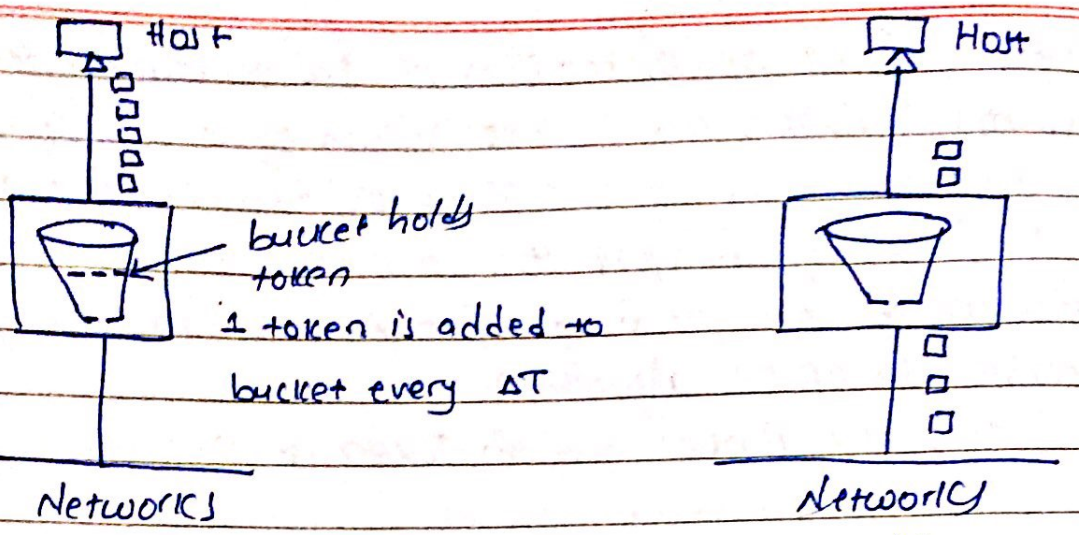
(b)

- Imagine a bucket with a small hole in bottom. No matter the rate at which water enters the buckets, outflow is at a constant rate when there is any water. And rate is zero. If no water once bucket got full, overflow incoming data lost. (as fig a)
- Conceptually, each host is connected to a n/w interface containing a leaky bucket (finite geriternal queue). If queue is full, and packet arrives lead to discarded of packet.
- implemented in a single-server queue with const-service time
- busy traffic into fixed rate traffic

b. Token Bucket.

- It allow output rate vary depending on size of burst.
- buckets holds token to transmit a packet, the host must capture and destroy one token.
- Tokens are generated by a clock at the rate of r token per sec
- Idle hosts can capture and save up tokens to the max size of bucket inorder to send larger bursts later.

a ⟷ b



before (a) fig: Token Bucket (b) after

token arrive at constant rate in token bucket. A packet from buffer can be token out only if a ~~token~~ in the token bucket can be drawn.

	Token Bucket	Leaky Bucket
1.	Token dependent	1. Token Independent
2.	Vary output rate	2. Constant output rate
3.	If bucket full, token are discarded not the packet	3. If bucket is full, packet are discarded.
4.	Packets only transmits when there are enough token	4. Packets are transmitted continously.
5.	It saves tokens to send large burst.	5. It doesn't save token

(31a) How ISDN interfaces and channel works ? wifinotes.com

→ ISDN (Integrated Services Digital Network) is a set of communication standards for digital telephone connection and transmission of voice and data over a digital line. These digital lines are commonly telephone lines and exchange established by the government

→ There are more ways to connect the device in Internet, dialup connection, DSL, wireless etc.. ISDN is another way.

- The landline ~~numb~~ are analogous line (ADSL), voice of speaker is picked up by telephone handset and transfer over phone line as an analogue.
- ISDN lines are digital communication and are capable of generating higher transmission speed of 1.4 Mbps. The medium used by ISDN is UTP cables.
- Communication methods of sending data, voice and video etc over digital telephones lines and these lines are ISDN lines. Types → BRI (Basic rate interface), Primary rate Intermace
- ISDN allow multiple digital channels to operate simultaneously through the same regular phone but transmits digital signal
- Latency is much lower on an ISDN line than on Analog line.
- The traditional PSTN was based on an analog connection bet? Customer premises and local exchange

BRI: It passes two 64B-channels, 1-D channel for controlled transmitting of information

PRI: It passes 23B channels and 1-D channel for United State and 30B channels and 1 D-channel for European

B-ISDN: uses broadband, uses fiber optic, 1.5 Mbps

regular ISDN: basband, UTP, upto 1.4 mbps

Advantage of ISDN (PSTN)

- speed Line, (commonly 56Kbps, ISDN faster)
- multiple lines for multiple device: FAX, telephone, video
- Connection Time (V34 modem take upto 60 sec, ISDN 2sec)

Disadvantage

- more expensive
- ISDN provider & ISDN users are require to have special dedicated line

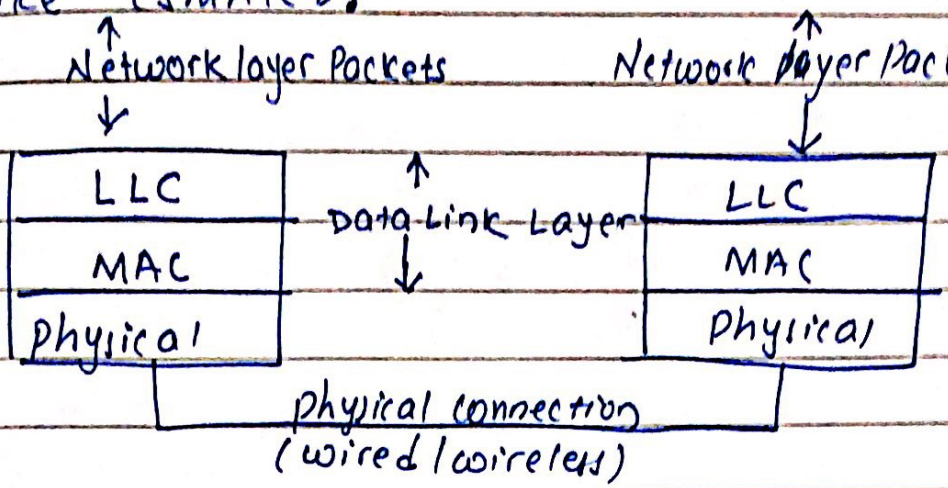
ADSL: only data Line, doesnot need local power
ISDN: 2 voice channel and one 128 kbps data channel need local power.

In ISDN lines, lines are logically divided into multiple channels - two main channels
(i) B-channel or Bearer, is defined clear digital path of 64 kbps for voice or data. Normally, ISDN posses 2 B channel one channel is dedicated for voice and other is data. in full duplex.
(ii) Delta channel or D-channel, it carries signaling messages, such as call setup, teardown, to control calls on B-channel. Traffic over D channel employs the Link Access Procedure on the D channel (LAPD) protocol. LAPD is data Link protocol based on HDLC.

(3)b) Explain use of Medium Access Control and Logical Link Control over LAN Architecture:

→ Media Access Control (MAC) is a sublayer of the dataLink layer on OSI reference model. MAC is responsible for the transmission of data packets to and from the network Interface Card (NIC) and to-and-from another remotely shared channel.
→ The main function of MAC is to provide an addressing mechanism and channel access so that each node available on nlw can communicate with each other.
Each computer has its own unique MAC address. Ethernet is an example of protocol that coore at MAC layer level.
→ MAC sublayer acts as an interface between the Logical Link Control (LLC) Ethernet sublayer and physical layer
→ MAC sublayer emulates a full duplex logical comm in multipoint
→ MAC is 12 digit Hex (48 bit in long).
MM:MM:MM:SS:SS:SS

MAC is responsible for framing / de-framing and collision resolution. MAC sub-layer add frames header and interact with physical layer processor to transmit the frame. MAC implements standard collision resolution protocol like CSMA/CD.



- LLC is responsible for handling multiplexing / demultiplexing and Link services (reliability and flow control)

The LLC multiplexing interface include following nlw protocol feature:

- multipoint network operation
- Flow control (specifies order using header)
- Frame sequence number assignment
- Acknowledgement tracking
- Error Control (LLC detect error, uses CRC).