Networking Models

(*) **Network Standards:**

It provides a framework on building a network.

Types: 1) **De facto standard:** — These are followed without any formal plan or approval by any organisation and these are usually unavailable to vendor.

eg: ~~http~~, Novell's Netware nw Operating system.

Further two types: — Open system = Published & accessible standard
— Close system = unpublished and unavailable stnd.

2) **Dejure Standard:** The are developed by not a single company rather developed by making specification available to all so that independent manufacturers can build hardware to such specification. They are adopted through legislation

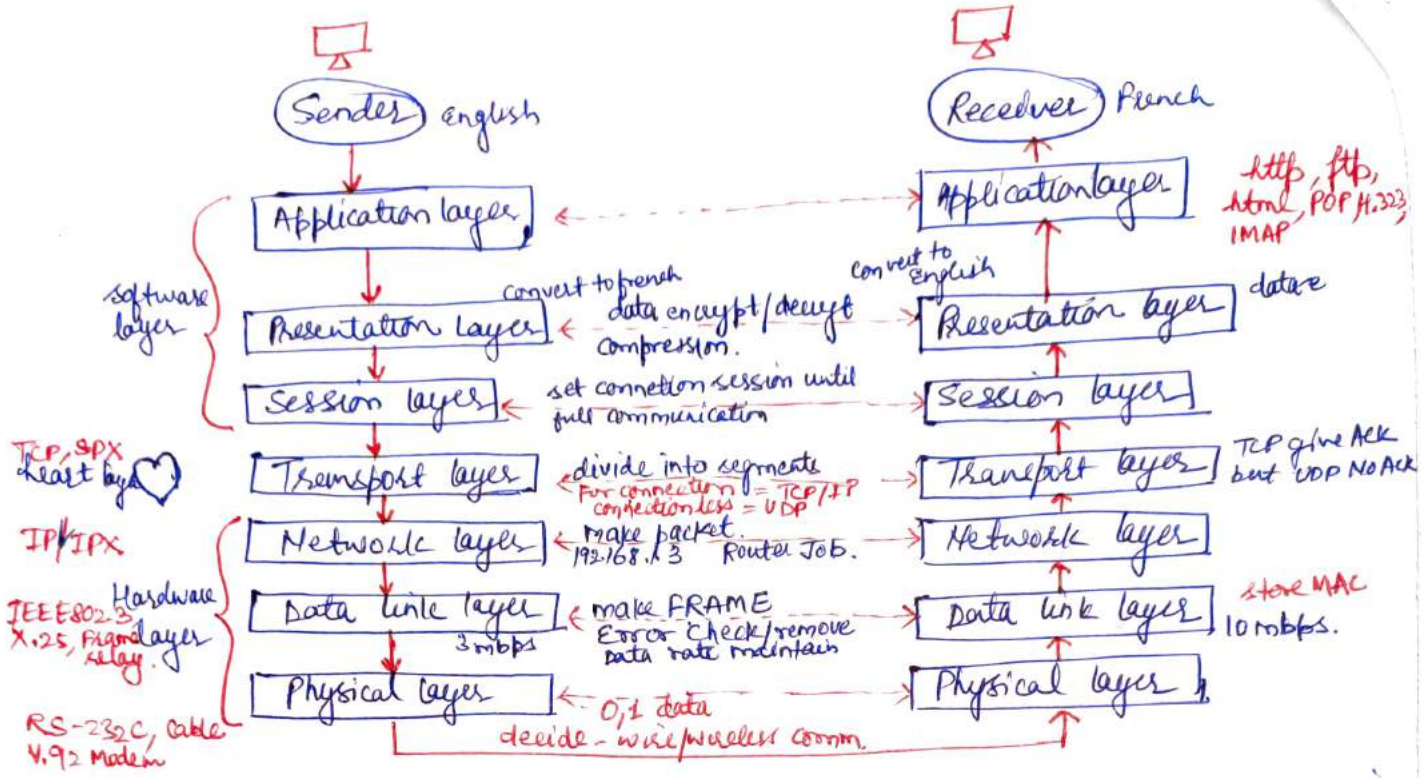
eg: TCP/IP.

(*) **OSI Reference Model:** open system interconnection model. It is a reference model only. means only conceptual not practical. It has been developed by ISO. (International Organisation for Standardisation) in 1984.

Shakti Raj Singh

Important:

1) It is a seven layer architecture where each layer is having specific functionality.
2) All these 7 layers work collaboratively to transmit the data from one network to another network across the globe.
3) ~~7~~



(*) If data is to send fast, then we use UDP in transport layer otherwise we use TCP.

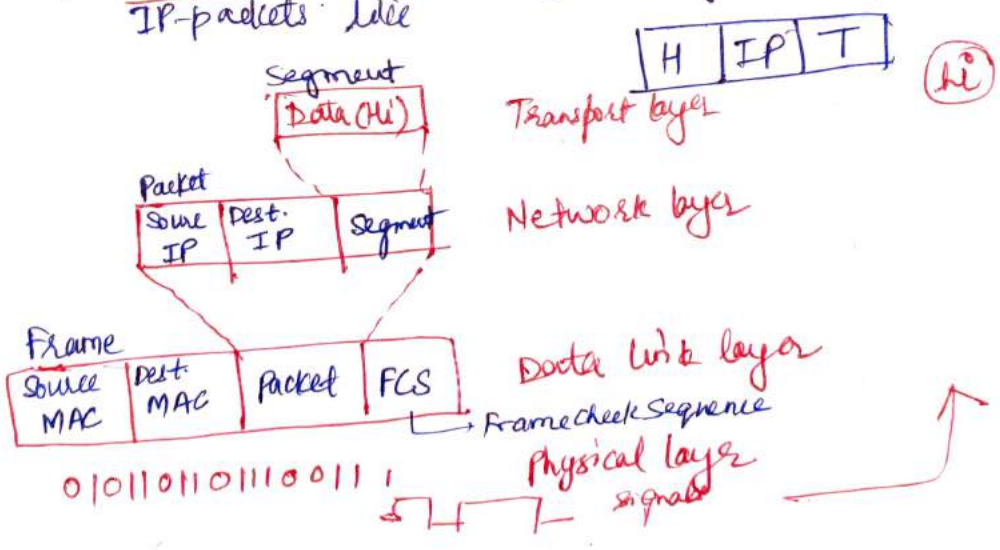
(*) N/W layer :→ 1) It has ~~to~~ do many jobs. So it carries the IP addresses of both sender and receiver

2) Router job is also done by it and choose the fastest path for data transfer.

(*) Data link layer :→ 1) if sender sends data @ 5mbps but receiver is receiving @ 10mbps. It maintains speed at both end.

2) Also store physical addres of both machines

3) Frames are made by adding certain information to the IP-packets like



Shakti Raj Singh

(*) Functions of Each Layer:

1) Physical Layer:
1) Represent data into bits (0, 1)
2) Define data rate.
3) Define transmission medium
4) Synchronization of bits between sender & receiver.
5) Line configuration (p2p, multipoint)
6) Physical topology
7) Transmission mode. (duplex/full duplex)

2) Data link Layer:
1) Framing
2) Physical Addressing (MAC)
3) Flow control. (between sender & receiver)
4) Error control. (if frame lost then retransmission takes place)
5) Access control. (if two devices are connected to same link then decide which device controls over the line)

3) Network layer:
1) Logical Addressing
2) Routing
3) It is responsible for end-to-end delivery of individual packets.

4) Transport layer:
1) while this layer is responsible for delivery of entire message. a message may contains many packets.
2) Service point addressing
3) Segmentation and re-assembly.
4) Connection control. = decides connection oriented or connectionless.
5) Flow control.
6) Error control.

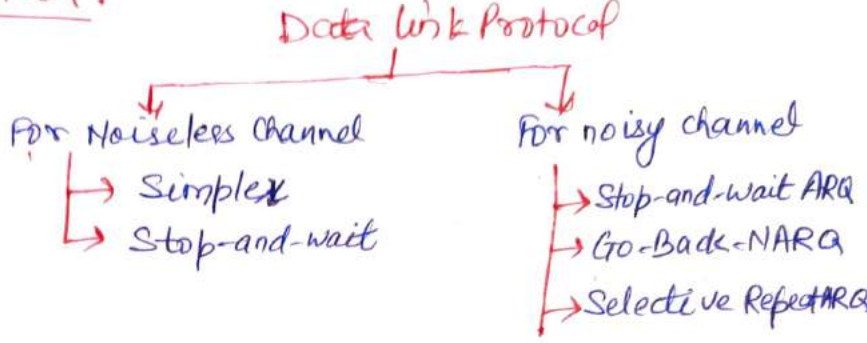
5) Session Layer:
1) Dialog control.
2) Synchronization

6) Presentation layer:
1) concerned with syntax of information
2) Translation
3) Encryption/decryption
4) Compression.

7) Application layer:
1) Provide user interface
2) Network Virtual terminal
3) File transfer, access & mngt in remote computer
4) Mail services
5) Directory services to provide distributed database access for global information.

* **Data link layer:** protocols in DLL are designed so that this layer can perform its basic functions – framing, error control and flow control.

* **Types of data link protocol:**



1) Simplex Protocol:

1. It is hypothetical
2. Designed for unidirectional data transmission over an ideal channel. ideal channel is that where transmission can never go wrong.
3. Distinct procedures for senders and recievers
4. All data send at a time and assume to be received all data instantly.
5. doesnot handle flow control and error control.

2) Stop-and-Wait:

1. It provides unidirectional data transmission without any error control facility.
2. However, it provides flow control. so fast sender & slow receiver balances.
3. For this balance, buffer is used.

3) Stop-and-wait ARQ: Automatic repeat request

1. It has error control mechanism.
2. Sender keeps a copy of the sent frame.
3. Sender waits for a finite time to receive a positive Ack from receiver.
4. If time expires/a negative Ack, then the frame will be re-transmitted.
5. If positive Ack received, then the next frame is sent.

4) Go-Back-NARQ:

1. It provides for sending multiple frames before receiving the Ack for the first time.
2. It uses the concept of sliding window. (SWP)
3. The frames are sequentially numbered and a finite number of frames are sent.
4. If Ack is not received within the time period, all frames starting from that frame are retransmitted.

Shakti Raj Singh

Selective Repeat ARQ:

1. This protocol also provides for sending multiple frames before receiving the ACK for the first time.
2. However, here only the erroneous or lost frames are retransmitted
3. while good frames are received and buffered

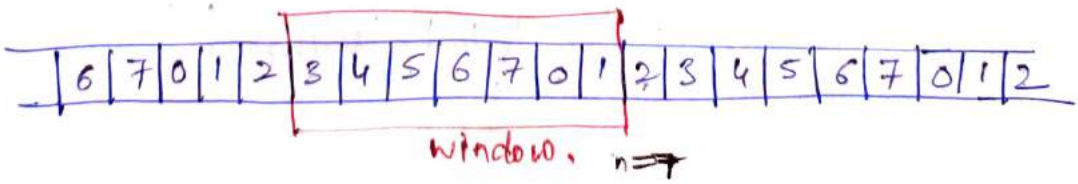
Sliding Window Protocol:

1. In DLL, this protocol is used in full-duplex data transmission
2. Two circuits are used each for a simplex data traffic.
3. Data frames are intermixed with the ACK-frames.
4. There is a "kind" field in the header of incoming frame which can tell the receiver whether the coming frame is data frame or ACK-frame.
5. sliding window refers to an imaginary boxes that hold the frames on both senders and receiver side.
6. It provides the upper limit on the number of frames that can be transmitted before requiring an ACK.
7. Frames may be ACK by receiver at any point even when window is not full on receiver side
8. Frames may be transmitted by source even when window is not yet full on sender side.

Concept of frame & window:

1) The window have a specific size in which the frames are numbered modulo-n, i.e. numbered from 0 to n-1. eg: if n=8, then frames are numbered as 0,1,2,3,4,5,6,7.
2) Size of window is 7 i.e. (n-1). i.e maximum of (n-1) frames may be sent before an ACK.
3) when the receiver sends an ACK, it includes the number of next frame it expects to receive.

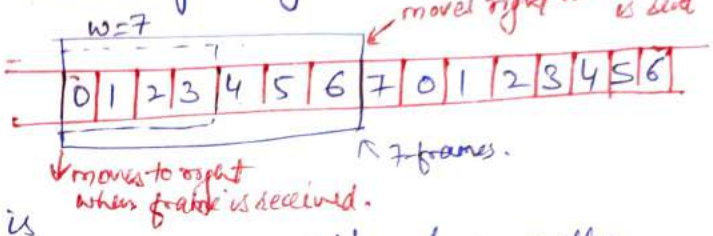
For eg: In order to ACK the group of frames ending in frame 4, the receiver sends an ACK containing the number 5. When sender sees an ACK with number 5, it means all frames upto 4 received.



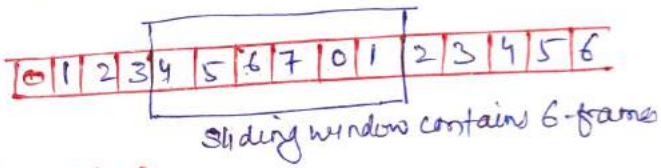
* Sliding window on sender side:

1) At beginning of transmission, the sender's window contains n-1 frames.
2) As frames are sent by source, the left boundary of window moves inward, shrinking the size of window.
   eg: if W = size of window, 4 frames are sent, then after last ACK, the frames left is W-4.
3) When receiver sends ACK, the source window will expand right boundary outward to allow in a number of new frames equal to the number of frames acknowledged by that ACK.

for eg: W = 7,
& 0 to 3 frame sent then sender's window will contain 4,5,6. (shrink)

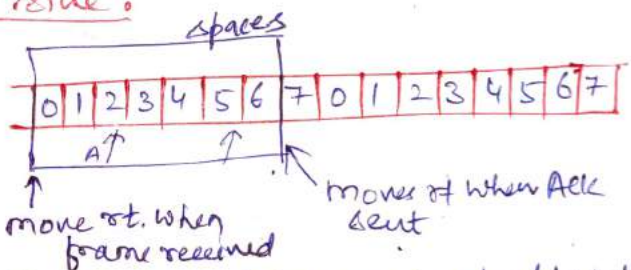


and after that, an ACK numbered 3 is received by source, it means 0,1,2 have been delivered correctly.
Now the sender window, will expand and includes next 3 frames.
ie. (4,5,6,7,0,1)

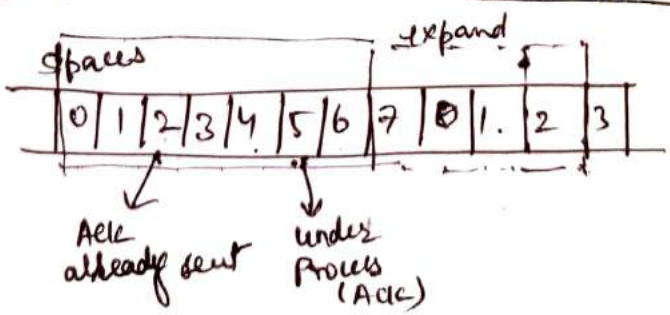


* Sliding window on receiver side:

1) In beginning, the receiver window contains (n-1) spaces for the frame but not the frames.
2) As the new frames come in, the size of the window shrinks.



3) The receiver window represents not the number of frames received but the number of frames that may still be received without an ACK must be sent.
   eg: W is window size, if 3 frames received without an ACK being returned, the no. of spaces in a window is (W-3)
   Now, as soon as ACK is sent, window expands to include the number of frames equal to the number of frames ACKed.
   If W=7, and a prior ACK was for frame 2 and the current ACK is for frame 5, the window will expand by (5-2 = 3)
   ↳ 0,1,2,3



Sliding Window Protocol

Sliding window protocol removes the shortcomings of simplex data communication types of protocol by creating windows of data frames and acknowledgements spaces on the receiver side

SWP is of 3-types;

1. One bit protocol or Stop and wait protocol.
2. Go back n protocol.
3. Selective repeat protocol.

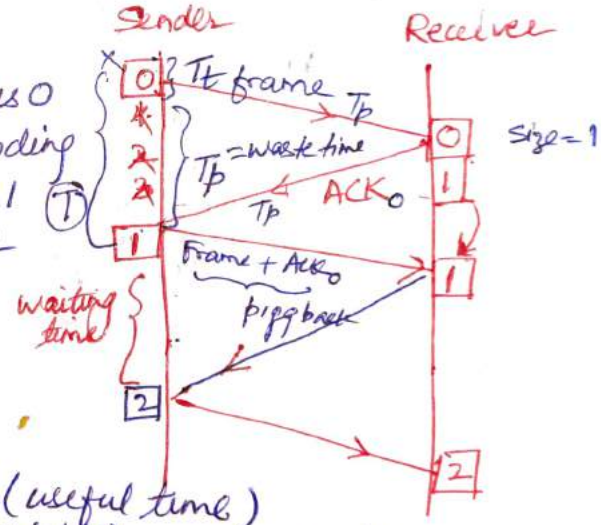
} SWP-main

They differ only in terms of complexity, efficiency, buffer requirements.

For all above cases, outgoing frame size is 0 to $2^n - 1$.

(1) **One bit / stop and wait protocol:** Here $n = 1$, hence it allows 0, 1 for out going frames. Here sender transmits a frame, waits for its ACK, then transmit the next frame. Thus it uses the concept of stop and waits for the protocol. This protocol provides for full-duplex communication. (Simplex also)

Hence, the ACK is attached along with the next data frame to be sent by piggybacking.



① initially, the size of sending window is 0
② After sending first frame, size of sending window = 1, and receiving window = 1
③ Next frame can be sent only after receiving of current frame ACK.

So efficiency, $\eta = \frac{T_t}{1+2a}$, $a = \frac{T_p}{T_t}$

where, T_t = transmission time, (useful time)

T_p = Propagation time (waste time)

so $T = T_t + 2T_p$

Mathematically,

T_t sec. sends pkt = 1 pkt

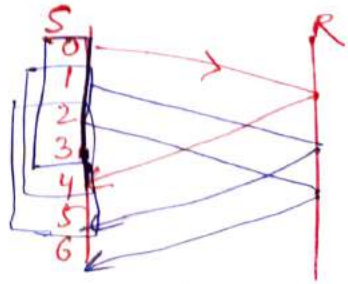
1 sec ⟶ $\frac{1}{T_t}$ pkt

$T(T_t + 2T_p)$ ⟶ $\frac{T_t + 2T_p}{T_t}$

$= 1 + 2a$

So to overcome this waste time, sliding window comes into picture.

$W = 4 = 1 + 2a$



Sliding window concept

Shakti Raj Singh

Sliding window Protocol

- Go back N
- Selective Repeat.

b) Go-back (N):

eg: If $T_t = 1$ msec, $T_p = 490$ msec, Go back (10) for n.

Now, total packets sent in total time, $T = 1 + 2a$

$= 1 + 2\frac{T_p}{T_t} = 100$

so $\eta = \frac{10}{100}$ } It is send 10 pkt but have capacity of 100 pkt

$\boxed{\eta = \frac{1}{10}}$

$\Rightarrow \eta = 10\%$

Now, calculate throughput = $\eta \times$ bandwidth

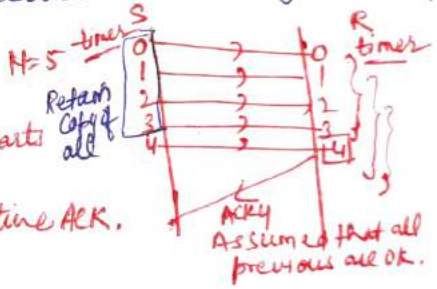
if bandwidth = 40 Mbps.

so, $Th = \frac{10}{100} \times 40 = 4$ Mbps.

Shakti Raj Singh

① In Gb'N', sender window size is 'N', and receiver window size = 1 always

② It uses cumulative Acknowledgements
- Receiver maintains an ACK Timer.
- each time the receiver receives a new frame, it starts a new ACK timer.
- After the timer expires, receiver sends the cumulative ACK.

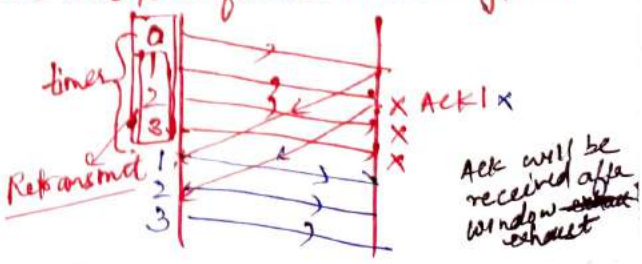


③ It uses independent ACK too.

④ It doesn't accept the corrupted frames and silently discard them.
- The correct frame is retransmitted by sender after the time out timer expire
- silent discarding a frame means- "simply rejecting the frame and not taking any action".

⑤ It doesn't accept out of order frames and silently discards them.
- all the following frames are also discarded
- this is because, receiver window size is 1. therefore out of order not accepted.

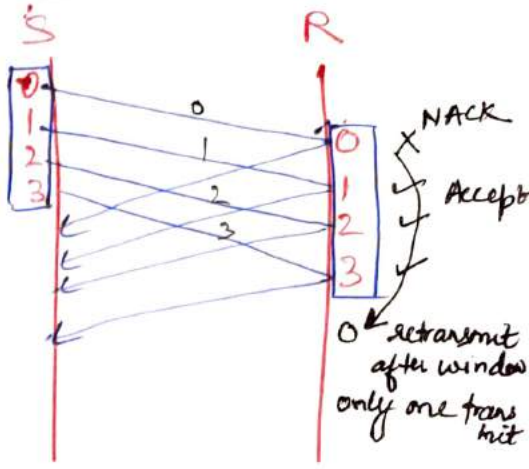
⑥ It retransmits the entire window, if for any frame, no ACK is received by the sender
- it will transmit all those frames again following the erroneous frame including the erroneous frame. That's why, its name is Go back N.



⑦ It retransmits the lost frames after expiry of time out timer.

η (Go back N) $= \frac{N}{(1+2a)}$

$W_S = W_R$



c) Selective Repeat SWP:

$$\eta = \frac{N}{H2a}$$

So, SR = S&W + GbN

1) Sender window size is always same as receiver window size.
2) It uses independent Acknowledgements.
3) It immediately sends the negative ACK for erroneous frame. It doesn't wait for timer.
4) It transmits only the erroneous frame just after completely exhaust of window of sender.
5) It accepts the out of order frames.
6) It requires sorting at the receiver's side
   - Receiving window follows linked list
   - As soon as, it gets retransmitted frame, sorting will start.
7) It requires searching at the sender side – it leads to its name.
   - For retransmitting the missing frame, it searches it in window and selected frame will be transmitted/repeated.
8) It leads to retransmission of lost frames after expiry of time out timer.

Shweta Raj Singh

⊛ Differences:

Go-back N ARQ	Selective Repeat ARQ
1. If a frame is corrupted or lost, all subsequent frames have to be sent again.	1) Only the corrupted or lost frame have to be sent again.
2. If it has a high error rate, it wastes a lot of bandwidth.	2) Low loss of bandwidth.
3. It is less complex.	3) It is more complex because it has to do sorting and searching as well. It also require more storage
4. It doesn't require sorting.	4) Sorting is required to maintain the frame order.

Network Layer:

It provides services to transport layer. Primary job is routing the messages across network/networks. It can operate both in connectionless mode as well as in connection oriented mode.

It is also known as inactive layer or Null layer because of its lack of functionality in local area networks. But if many different networks are operated then its role becomes complex.

Main goals:

1. Its service should be independent of subnet technology
2. It should shield the transport layer from type, topology and number of subnets present.

3. It is responsible for host to host delivery (source to destination).
4. logical Address is used. eg. IP < Host address / Network Address
5. Routing — using method RIP and OSPF method (Routing information protocol)
6. Fragmentation — large data packet is divided into small size pieces.
7. Congestion control. Although it is done by transport layer but N/w layer also maintain it using various methods.

Router / Bridge / (switch) / firewall / gateway → Network
Bridges → DLL → Physical L

Congestion control methods:

1) **Traffic Shaping**: It is mainly used in virtual circuit subnets. This methods smoothes out the traffic on server side rather than on client side. methods used — Leaky Bucket and token bucket. These methods are useful for real time data such as Audio and video.

Shakti Raj Sapkota

2) **Admission control:** It is also used in virtual circuits. When congestion is detected on part of subnets, no further virtual circuits are created until congestion is reduced.

3) **Choke packet:** This method is used in datagram as well as in virtual circuit subnets. Here router send a choke packet to host to reduce its traffic.

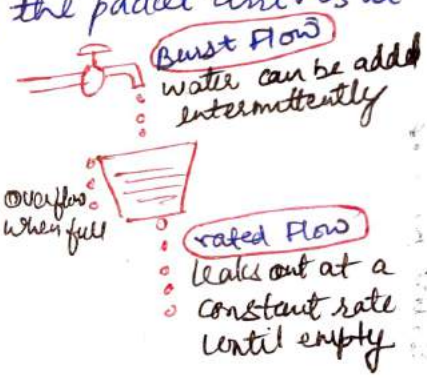
4) **Load Shedding:** When all methods fails to curb, then the router/switches start discarding packets to reduce the load of network.

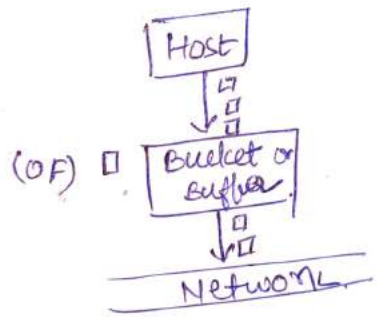
⊛ Various Algorithms Used to do it:

1) Leaky Bucket Algorithm: (buffering).

It comes under traffic shaping method.

- Each host is connected to the network by interface containing a leaky bucket. i.e. a finite input queue of the packet arrives at the queue. when it is full, the packet is discarded.
- The host is allowed to put one packet per clock cycle on to the network
- It regulates the flow at constant data rate.

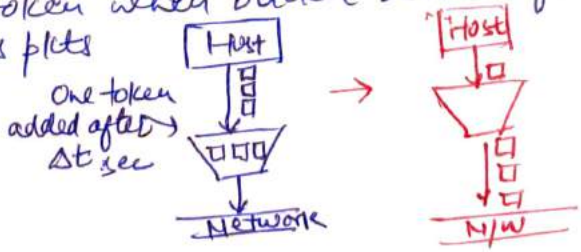




2) Token Bucket:

This method also used in congestion control. Congestion controlled by transport layer and network layer.

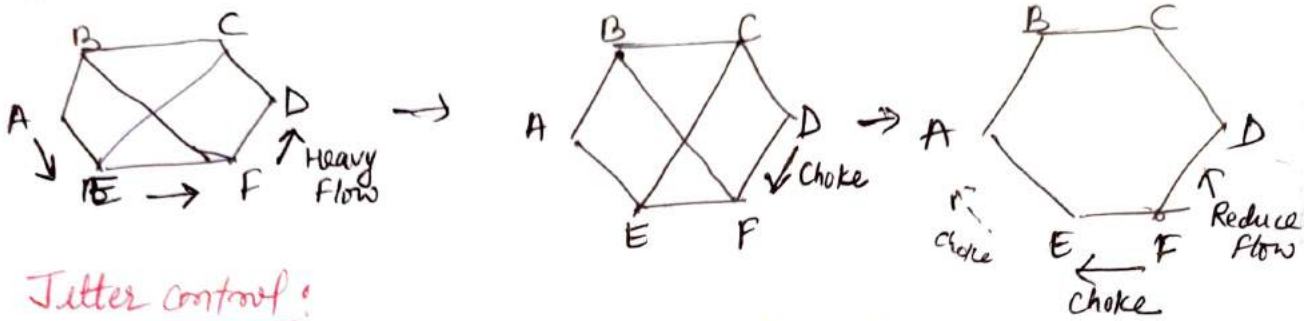
1) Since leaky bucket was rigid method in discarding excess pkts. but Token bucket doesn't do so.
2) In this algo, leaky bucket (buffer) hold tokens generated by a clock at the rate of every Δt sec.
3) It throws out token when bucket becomes full.
4) It never discards pkts



Shakti Roy Singh

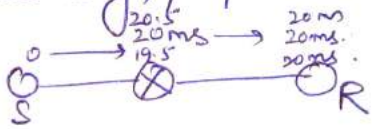
③ Hop-by-hop packet:

1) It is another method of choke packet method.
2) It is used to reduce congestion in a very long route.
3) Here choke effect takes place at every hop it passes through.



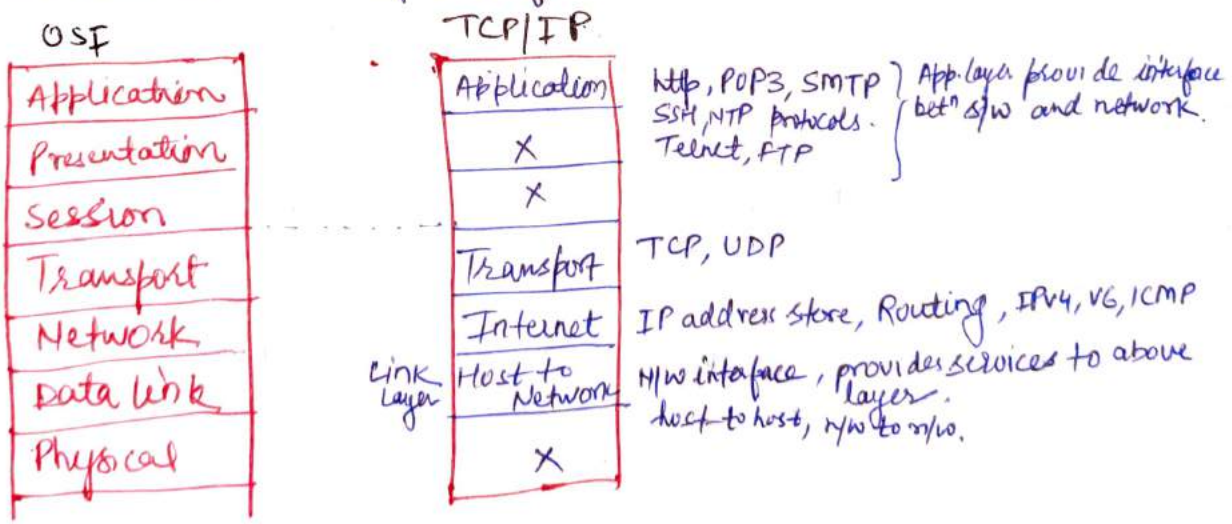
④ Jitter control:

1) The variation in the packet arrival time is called Jitter
2) It mainly apply in Audio/Video streaming where continuous data flow.
3) Router checks the data packet arrival time, if it is slow then router will speed it up. If it is fast then router will slow down the speed. In this way, proper data packet flow is maintained.



⑤ TCP/IP:

It is a client/server-model. Point-to-point communication. It has four-layers..
(Transmission control Protocol/Internet Protocol)
This suite was developed before OSI Model.



Shakti Raj Singh

Differences

OSI	TCP/IP
1) OSI has 7 Layers	1) It has 4-Layers.
2) Guarrantee delivery of packets	2) No guarrantee.
3) Separate session layer	3) No. S.L.
4) Separate Presentation layer	4) No. P.L.
5) Horizontal Approach	5) Vertical Approach
6) Protocols are better hidden and easily replaced as tech. changes.	6) Not easy to replace the protocol.
7) OSI is truly a general Model	7) It cannot be used for any other application
8) OSI is less reliable	8) It is more reliable
9) It has strict boundaries	9) doesn't have strict boundaries
10) OSI developed model then Protocol	10) It developed protocols then model
11) Network layer provide both connection oriented and connectionless services	11) It provides only connectionless services.

Chapter-3
TCP/IP Addressing

TCP/IP started with the introduction of ARPANET (Advance research Project Agency Network). After sometime, it became TCP/IP.
- A network in TCP/IP internetwork can be LAN, WAN, MAN.
- Data flow in form of datagram. i.e connectionless flow.
- Datagrams travel along different routes and they may arrive out of sequence.
- Datagrams contain all information sufficient for routing. without establishing a connection.
- Sometimes, datagrams may be duplicated.

So, for proper delivery of data, TCP/IP uses proper addressing methods.

✱ 3- Types of TCP/IP Addressing:

1) Physical Addressing
2) Logical Addressing
3) IP Addressing.

1) **Physical Addressing:** The address assigned to a network interface card by the original manufacturer or by n/w admin is called Physical address or hardware address.
- It is a unique identifier for a specific mode on a network.
- MAC (Media Access Control) is an identifier for the devices.
- It is a 48-bit address consisting of 6-hexadecimal blocks. MM:MM:MM:SS:SS:SS (manu.)
- First 3-bytes specify the NIC vendor, Rests give the serial number of device

Three types of Physical Address

1) Unicast Address
2) Multicast Address
3) Broadcast Address.

1) **Unicast Address:** It is permanently assigned to NIC and is unique for a machine. The card monitors the transmission and matches them against this address to identify the frames assigned to it. It helps the host.

2) **Multicast Address:** This address is given to a group of hosts instead a single host. Thus, to receive a datagram, they identify a group of stations/machines in the same domain. This technique is used when a common message is to be sent to a group of hosts.

3) **Broadcast Address:** This address is given to datagram to communicate to all hosts in the network. In this, address contains all 1's that points that all stations are to receive the given packet.

Shakti Roy

2) **Logical Addressing:** IP addresses assigned are the logical addresses which is allocated to an item in perspective of an application program.

3) **IP-Addressing:** It stands for Internet Protocol. An IP address is a unique number provided to each and every device. It is in the form of integric number which is separated by (.). eg: 192.168.10.29

IP-Address

IPV4
- Length 32-bit
- 4-octet (8-bit each)
- 0 to 255 (Range)
- 4 billion (2^{32})
- 192.168.10.26

IPV6
- Length 128-bit
- 8-octet
- 0 to FFFF (65536)
- 340 trillion (2^{128})
- 3FBB:1908:4646:2:100:L8FF:FE21:9738

Total pop = 7

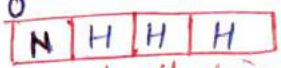
IPV4 is not sufficient for world's total population, that's why IPV6 comes into picture.

Shubh Raj Shukla Bay

✱ **Uses of IP:** 1) Private IP → It is for personal work.
2) Public IP → IP used on internet. like web address.

✱ **Classes of I.P:**

Class A → 0 to 126 (125.255.23.17) — 2 reserved: 0.0.0.0 default route, 127.0.0.0 loop back fun^n



127.0.0.1 → Private Address / Local server — for expmt purpose (hacking job)

Class B → 128 to 191 (191.23.28.144)

Class C → 192 to 223 (192.204.17.110)

Class D → 224 to 239 (used for multicasting) 1110 →

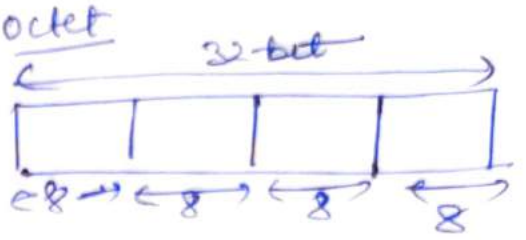
Class E → 240 to 255 (used for research) 1111 →

Class A: max 16777214 host, 126 Network
Class B: 65534-h, 16384-N
Class C: 254-h, 2097152-N

→ Host calculation = Total − 2
→ If all 0's (this network shows)
→ If all 1's (broadcast)

⊛ IP Address Structure:

- Network Id (1)
- Host Id (0)

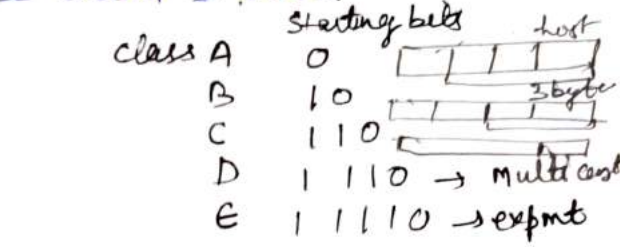


⊛ Special IP-Addresses:

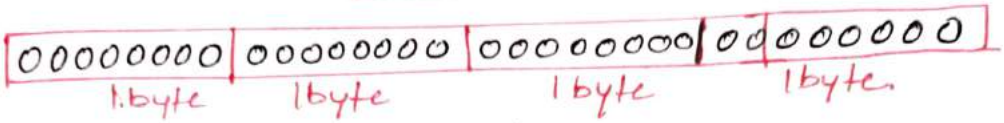
Special Addressing IP:

To identify class type, we use 0 and 1 bits.

0 → this network / this host
1 → broadcast address

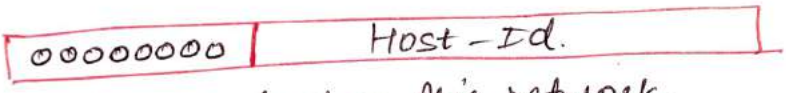


(1) 0.0.0.0 → This host



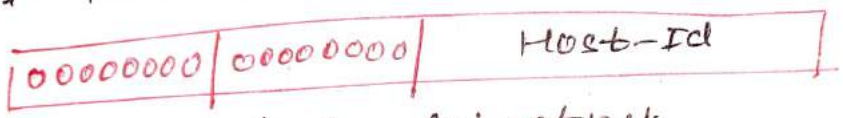
This is non-routable address
- the client is not connected to any TCP/IP Network.
- If netmask 0.0.0.0 used with it, then it means default route, pkts will be delived on given gateway.

(2)



- It means a host on this network.

(3)



- means a host on this network.

(4)

- Broadcast on local network. means msg will be broadcasted on the current network.

(5)

- Broadcast on a distant network as identified by given network id.

(6)

or 127.0.0.0/8

- Loopback → it allows a device to send msg to itself.
  - it is like a person talking to himself
  - They are used to check if the NIC functions properly.
  - This feature is also used for debugging of network software.

If we use 127.0.0.1 then 16777215 IP addresses are wasted.

Shakti Roy

IPV4 Link Local Address:

169.254.0.0 – 169.254.255.255 or 169.254.0.0/16 (Subnet mask)

Subnet mask separates the network id from host id.

- These are self-generated automatically.
  - when a host cannot find a DHCP server
  - when a communication problems occur between a host and DHCP server.
- A link local address means –
  - the host cannot access the Internet.
  - link local address is not routable.
  - the host can communicate with other devices on the same LAN.

IPV4 Private Address:

- Non-routable addresses
  - Routers would not deliver packets with private IP addresses
  - Free to use without anyone's permission

Shaikh Raj

* why do we need IPV4 Private Addresses
  - There are only 4.3 billion IPV4 address and these will be exhausted by 2011. as population/devices will increase so IPV6 will be required.

eg: Class A : 10.0.0.0 – 10.255.255.255 or 10.0.0.0/8
Class B : 172.16.0.0 – 172.31.255.255 or 172.16.0.0/12
Class C : 192.168.0.0 – 192.168.255.255 or 192.168.0.0/16

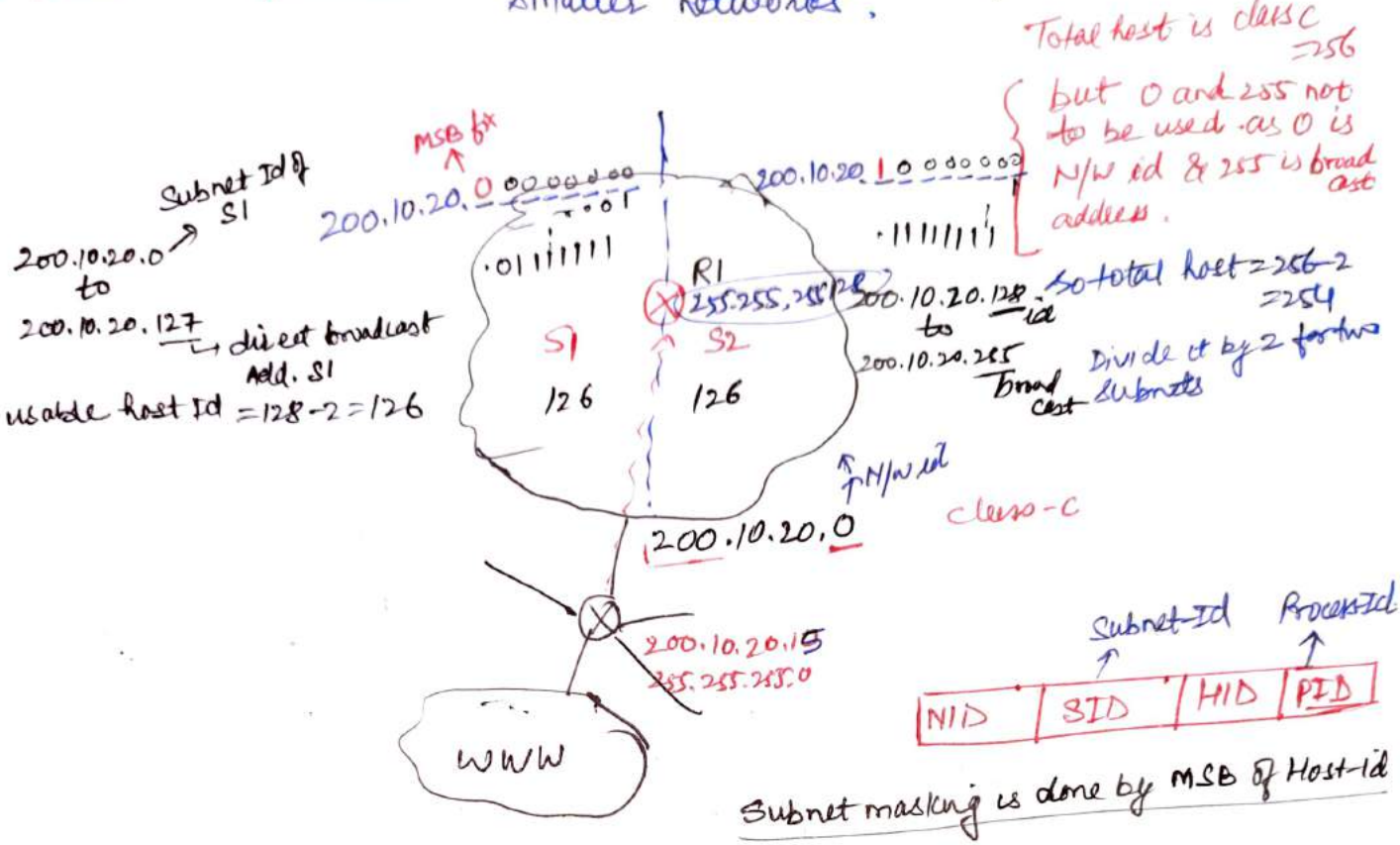
Why they are choosen so ?

They were given by Scientist Jonanthan Postel (1943–1998) since, he was died without unveil the fact behind it.

Benefits :- Security devices with private IP addresses cannot connect directly to the internet.
- Access to the internet must be brokered by a router.

Subnetting in IP:

means dividing the big network into smaller networks.



Subnet masking is done by MSB of Host-id

- for better control of network in a big organisation.
- For each job - class-C is used. Class A is difficult to maintain as it has many hosts.

special issue! Network id of S1 and complete N/W is same i.e. 200.10.20.0. (direct and broadcast address)

How to resolve it?

- Install one Router R1 in Network which filter the incoming packets for S1 and S2.
- Use subnet mask 255.255.255.128. (4th octet .10000000 in S1)
- pkt comes with IP 200.10.20.15 at R1. then it will AND with Subnet mask at R1 i.e.

```
  .10000000
  .10001111  AND
  .00000000
```

↳ it goes to S1

If pkt destination address is 200.10.20.130.

then

```
  .10000000
  .10000010  AND
  .10000000
```

↳ goes to right.

Shortcomings of Subnetting

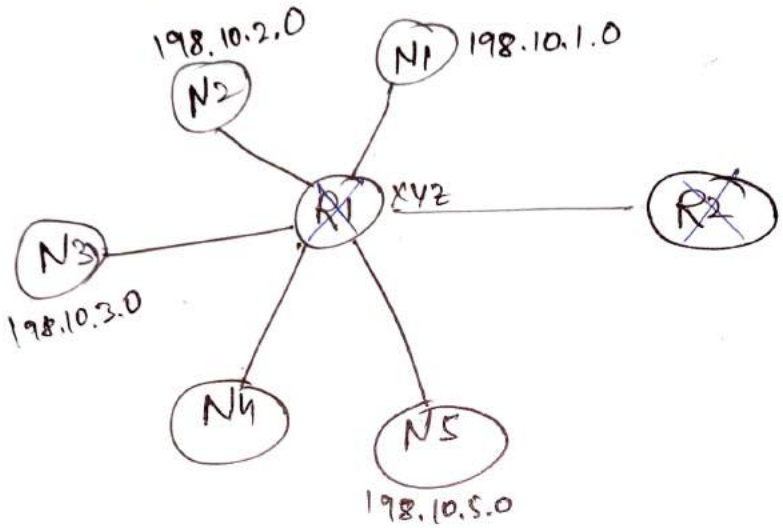
- Addressing will become a little bit complex.

Shakti Ray, Shakti Ray

(*) Supernetting:

It is reverse of subnetting. It also known as Prefix Aggregation / Route aggregation.

- Combining two or more IP Network / IP Sub-network with a common subnet mask or CIDR (classless Interdomain routing)
- It reduces Routing Table Entries. It makes router's job easy.



Routing table

NID	Subnet mask	Interface
198.10.1.0	X	
2.0	XYZ	
3.0		
4.0		
5.0		

Here, R2 will maintain a single IP of R1 and further mapping will be done by using R1 table

(*) condition for supernetting:

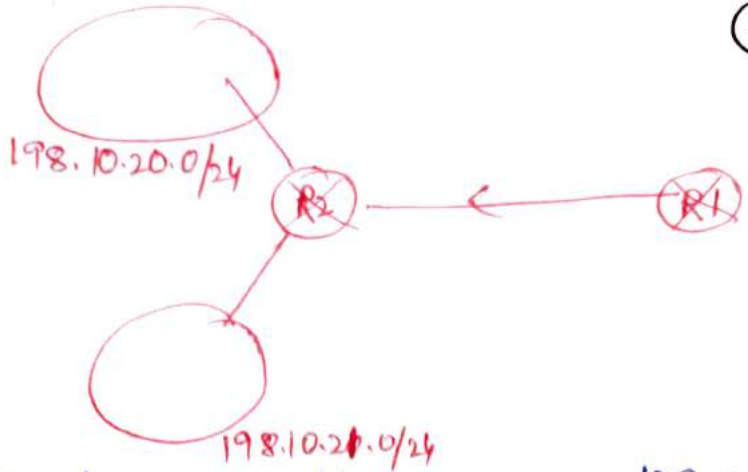
1) Contiguous in Nature
2) Size of all the networks should be same.
3) Network-Id should be divisible by total no. of host bit

(*) Practical Example:

① Let we have, 198.10.1.0/24 → 254 Host } → supernet
198.10.2.0/24 → 254 host. }

If we have install 500 computers in a lab, then class-C IP Addressing is not sufficient. So to do so, supernetting is another option to make network of 500 computers

② Let we have, 198.10.20.0/24
198.10.21.0/24



① Convert IP address into binary

Now it becomes

128+64+4+2 = 198

128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	
1	1	↓ 0	↓ 0	↓ 0	1	1	0	198
0	0	0	0	1	0	1	0	10
0	0	0	1	0	1	0	0	20
0	0	0	1	0	1	0	1	21

198.10.20.0 → 11000110.00001010.00010100.00000000

AND

198.10.21.0 → 11000110.00001010.00010101.00000000

11000110.00001010.00010100.00000000

N/W bit (23 bit) | Host (New)

198.10.20.0/23 — This supernet id.

1 ⊕ 1 = 1	AND
1 ⊕ 0 = 0	
0 ⊕ 1 = 0	
0 ⊕ 0 = 0	

In similar way, many ~~net~~ sub network can be taken but they should be in contiguous order like

198.10.98.0/24
198.10.99.0/24
198.10.100.0/24
198.10.101.0/24
198.10.102.0/24
198.10.103.0/24

Convert in binary as above. AND all these

01100001.00001010.01100XXX.00000000

N/W bit (21 bit) | Host (New) 11-bit

198.10.96.0/21

Shalini Roy

Loop Back: A loop back address is a special IP address, 127.0.0.1 to 127.255.255.254, reserved for testing network cards (NIC). This is the reliable method of testing the functionality of an ethernet card and its drivers and software, without a physical network.

ping 127.0.0.1 -t

Exception: 1) We cannot use 127.0.0.0, since it is current networkId when you use it, A message of "General failure" will be shown on screen.

2) We cannot use 127.255.255.255, it is broadcast address in this network. It shows msg "Request Time Out".

(*) NAT (Network Address Translation):

It is a process in which one or more local-IP address is translated into one or more global IP address and vice-versa in order to provide internet access to the local hosts.

Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding enteries of IP address and port number in the NAT table.

NAT generally operates on a router or firewall.

Shalabh Roy

(*) NAT Types: 3 types

1. Static NAT → a single unregistered (Private) IP is mapped with a legally registered (Public) IP
2. Dynamic NAT → a unregistered IP is translated into a registered (Public) IP address from a pool of Public IP addresses.
3. Port address Translation or NAT overload → In this, many local (private) IPs can be translated to a single registered IP address. Port nos are used to distinguish the traffic.

This is the best way of connecting thousands users to the internet by using only one real global (public) IP address.

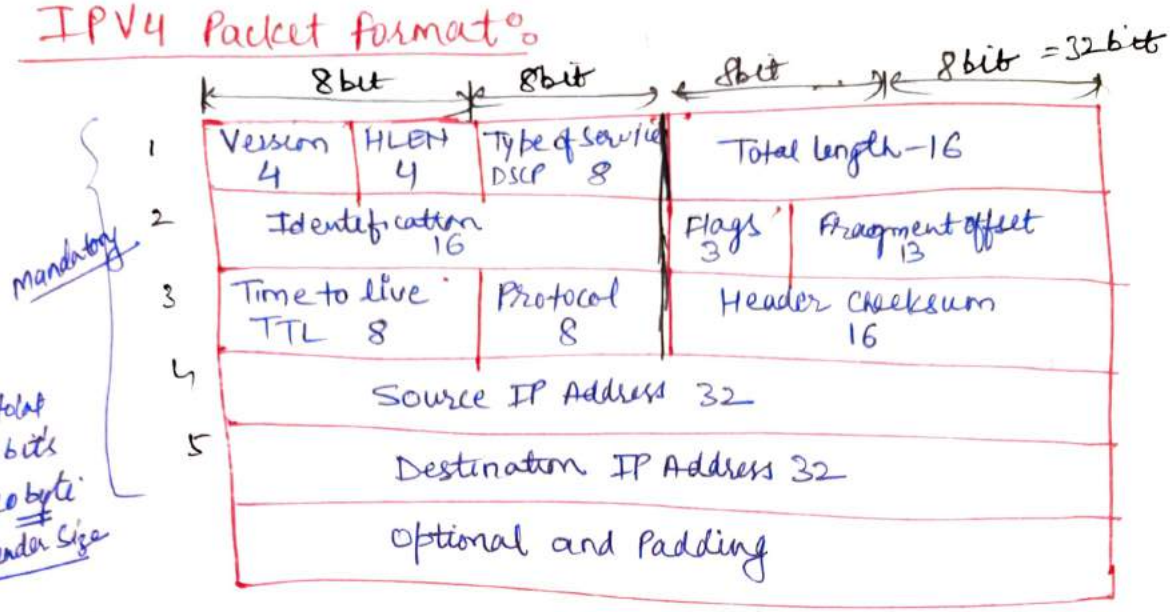
Advantages

1) NAT conserves legally registered IP Addresses
2) Provides privacy, as actual device IPs are hidden.
3) Eliminates address renumbering when a network evolves.

Disadvantages:

1) Translation results in switching path delays
2) Certain functions/applications will not function while NAT is enabled.
3) Complicates tunneling protocols as IPsec
4) Routers are tampered with port no, which makes it complex.

(*) IPV4 Packet format:



It contain - 12 fields of different length in its fixed 20 bytes part and one optional part that may contain 0 or more words alongwith padding.

- IPV4 works at network layer.
- IPV4 header is connectionless protocol.
- It is a datagram service. It means it is equiped with all information which is required to reach its destination point.
- Datagram (+)
  - Header Size = 20 - 60 Bytes (min - max.)
  - Payload = 0 - 65515 Bytes (Actual data to be sent)

Total Size of datagram = 20 + 65515 = 65535

max size of datagram = 2^{16}

Shatter Ring

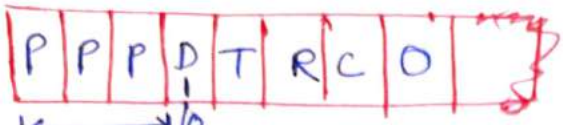
Fixed Parts:

1) **Version (4):** Values is 0100, → 4, for IPV6 - 0101
   It is just like engine of a train.
   It's range is 0000 to 1111 but only 2 are used.

2) **HLEN (4):** Header length, 0000 to 1111, 0 to 16, size 2^{16} = 65515
   Use multiple by 4 factor
   max value = 15 × 4 = 60 bytes.
   min value = 0 × 4 = 0 × Not valid., so avoid 0,1,2,3,4 values. If it is so, then invalid address

3) **DSCP (Differentiated Services code Point)**

3) DSCP : (8 bit)



↳ packet priority definition

other concept

Explicit congestion Notification

↳ denotes congestion

↳ Delay - it is '1' if less delay, otherwise 0; eg! VoIP - high delay. Normal call - less delay

T → throughput → 1 → If high data rate required, else → 0.

R → Reliability → 1 → if no drop in data, else 0.

C → Cost → 1 → for min cost (shortest path)

0 → Reserved for future purpose.

4) Total length : (16-bit)

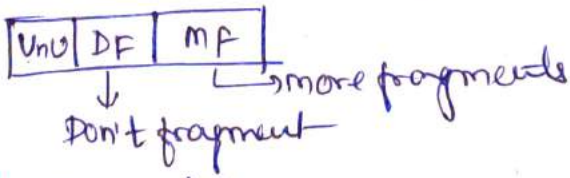
It gives the total size of a datagram i.e. $2^{16} = 65535$ out of it header size and payload make a proper proportion.

5) Level-2 related to data fragmentation and their identification

Identification : 16-bit

It allows the destination host to identify the datagram of currently arrived fragment. The fragments of same datagram contain same identification.

6) Flag : (3-bit) → One unused bit,



7) Fragment offset : (13-bit)

It indicates the position of fragment in the original datagram. max = $2^{13} = 8192$ fragments in a datagram and it may have total byte $8192 \times 8 = 65536$ bytes, which is one more than total length field. All fragments must be multiple of 64 bits except the last one.

8) Time to live: (8-bit)
It specifies the time for which a datagram can remain in the internet. Time is counted in seconds. and its range is 0 to 255 sec.
Every router decreases the TTL by at least one after processing it. It also works as hops counter. when it reaches 0. then the packet will be discarded.

9) Protocal: (8-bit)
If higher level protocols of upper layers are used in lower layer, then their details are provided in this field.

10) Header Checksum: (16bit)
checksum means identification of errors. It is verified the header. It detects the error that may occur during transit. It is rectified and recomputed at each hop. i.e. at each router. and it reaches to zero at its destination.
It is formed by taking 1's compliment addition of all 16 bits words in the header and then taking 1's compliment of the result

11) Source IP: (32-bit)
It contains class type, network id and host-id

12) Destination IP: (32-bit)

OPTIONAL PART

13) options and padding: & data
when extra bit is used to define data than it is used. It

a) Option: option field encodes the options requested by the source host. Five types—
1. Security 2. Strict source routing 3; Loose source routing
4. Record route 5) Time stamps.

b) Padding: is a variable number of bits used to ensure that the datagram header in a multiple of 32-bits in length.

c) Data: variable field ensures and integer multiple of 8 bits in length of data.

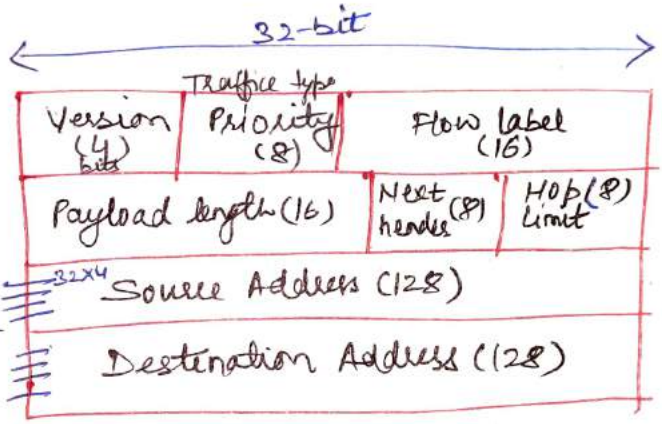
IPV6 Addressing: (128 bit)

For transmission of video and audio data, very high speed transfer is needed. So IPV6 designed.

Advantages:

1) Larger Address space (2^{128} bits) as compared to IPV4 (2^{32} bits)
2) Support for resource allocation
3) Address auto configuration
4) Increased addressing flexibility.
5) Improved optimal mechanism.
6) More security.

IPV6 - format: Packet (128 bit)



Total bits = 320
bytes = 40

1) Version: (4 bit)
i.e. 0110
It always remains 0110.
Fix

2) Traffic Class: (8 bit)
congestion control is done by giving certain priority to pkts.

3) Flow label: (16-bit)
Used in real time data, data should be reached speedy and no loss.
In this we convert datagrams into virtual circuits so that they can be speedily moved in a dedicated circuit (virtual)
It works like TCP.

4) Payload: (16 bit) It mean $2^{16} = 65535$ bit data can be send at time. It is a normal size. But we can also send jumbogram of 4 gb data size packets using hop-by-hop option in special cases.

5) Next header: (8bit)

It contains the addresses of extension headers which are above the limit of base header. If more information about a data is to be sent then it is used like in fragmentation.

6) Hop limit: (8bit): Time to live method. Counter decreased at every hop

Fixed
Base header = 40 byte (320 bits)

Shalabh Rai

7. Source Address : (128 bit)
8. Destination Address : (128 bits)

* Writing Method
8000:0000:0000:0000:0123:4583:89AB:CDEF
Written in 8 groups of 4 hexadecimal digits with colon between the groups

* IPV6 - Extension headers : They are defined in "Next Header" Option in main format of IPV6. They are 6 in number.

1) Routing Header : 43 bittle
Here sender decides that my data packet will travel through the routers of his choice.

2) Hop-by-Hop : 0 byte
In this, datagram will provide ~~in~~ certain information at every hop.

3) Fragment Header : (44 byte)
If we have large data pkt size, then it will be fragmented. Here, special point is that router will not fragment rather the sender has the power of fragment. in IPV6.

4) Authentication Header : (51 bytes)
Used for data integrity and authentication and verify sender's identity.

5) Destination options : (60 bytes)
In this, data packet will not checked for destination header at any hope. Only destination node can verify it.

6) Encapsulating / Encrypted Security Payload : (50 byte)
It contains the information about the encryption methods used in it.

Shaleen Roy

IPV4	IPV6
1. 2^{32} ways to represent Addresses	1) 2^{128} ways
2. Written in dotted decimal notation. 192.168.1.1	2) written in hexa decimal, consist of 8 gps containing 4 hexadecimal digits separated by colon
3. It has checksum which must be computed at each router	3) No header checksum
4. It has only Stateful Auto configuration	4) It has both a stateful and stateless address auto configuration mechanism
5. Security less.	5) Security high.
6. Source & destination address are 32-bit	6) 128 bit
7. IPSec supports is optional	7) IPSec support required.
8. Can be configured manually or DHCP	8) No such segmt
9. Header includes options	9) Extension headers are used for this purpose.

Network Architecture

(*) **Network Architecture:** It is defined as the physical and logical design of the software, hardware, protocols and media of transmission of data.

Simply, we can say that how computers are organized & how tasks are allocated to the computers.

Architecture includes the hardware, topology, design, software, signal characteristics and data representation.

(*) **Service Access point (SAP):**

A layer provides services to its upper layer by taking services from its lower layer. These services are available at some special point called SAP. Each SAP has unique address.

(*) **LAN Architecture:**

It has 4 Architectures —

1. Ethernet
2. Token bus
3. Token Ring
4. FDDI (fibre distributed data interface)

Shatty Raj

1. **Ethernet:** This LAN architecture is developed by "Xerox" and extended by joint venture of DEC, IC and XEROX. It is specified by IEEE 802.3. It defines two categories -

1. Baseband
2. Broadband.

1. **Baseband:** It uses digital signals (Manchester encoding) while broadband uses analog signals (PSK encoding).

Baseband is divided into 5-standards -

data rate Mbps ← 1. (10) base (5) → max cable length / type of cable.

2. 10 base 2
3. 10 baseT
4. 1 base 5
5. 100 base T

while Broadband is divided into 1-standard only!

1. 10 base (36) → cable length.

Access-method used in any ethernet is CSMA/CD. technique (carries sense multiple access with collision detection).

Collision: when multiple users access a single line then there is always a chance of overlapping and destroying of data which is called collision.

CSMA is used to control such collision when traffic increases

NIC: (Network Interface Card) :- Each device (computer, printer or any device) on ethernet network has its own NIC which is installed inside the device/station and provides a six byte physical address for the device/station.

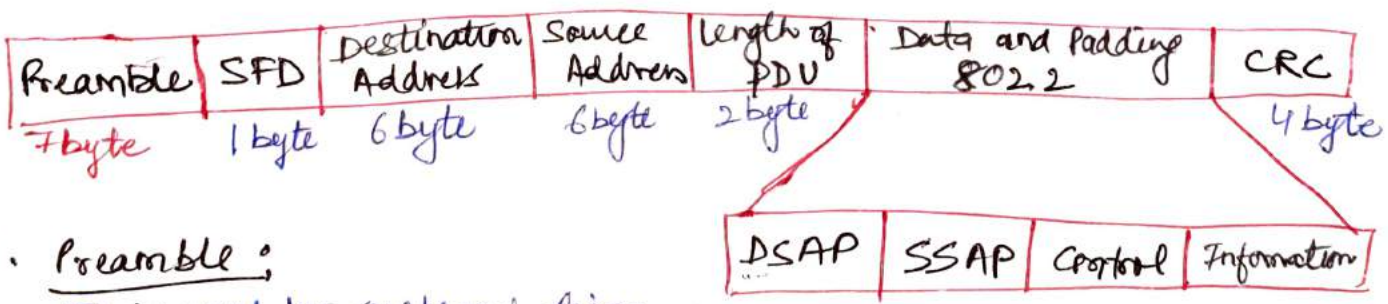
(*) Electrical specifications for Ethernet:

a) **Signalling:** Baseband uses Manchester digital encoding
Broadband uses differential PSK.

b) **Data rate:** Ethernet LANs supports data rate between 1 Mbps to 100 Mbps. Baseband = 1, 10, 100 Mbps
Broadband = 10 Mbps.

c) **Frame format:** IEEE 802.3 specifies only one type of frame format that includes 7 fields.

1. Preamble
2. SFD (start frame delimiter)
3. DA (Destination Address)
4. SA (Source Address)
5. Length/Type of PDU
6. PDU (802.2 frame)
7. CRC (cyclic Redundancy Code)



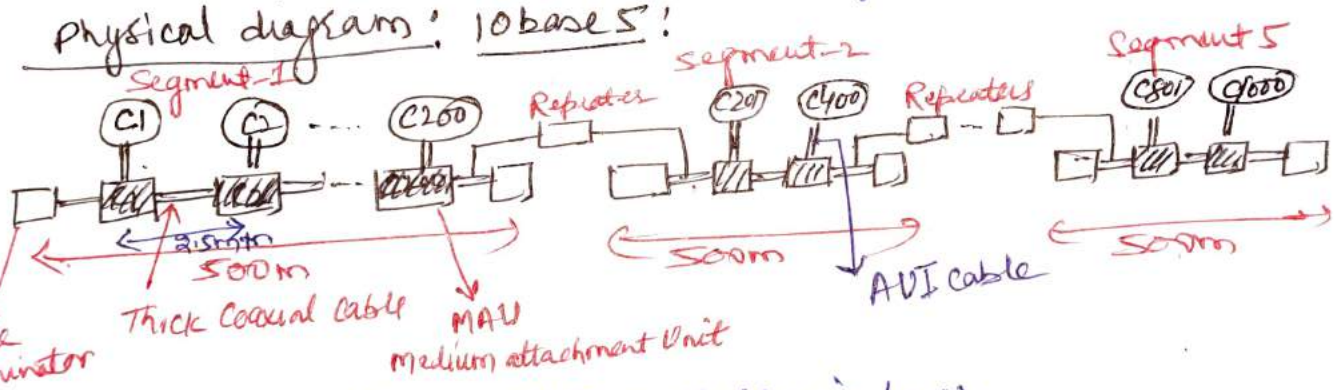
1. **Preamble:** It is used for synchronization.
2. **SFD:** used for signal beginning of frames.
3. **DA & SA:** contains address of source and destination as declared by NIC

4. Length of PDU: It gives length and type of PDU. It provides base for other protocols.
5. Data: It carries the data sent by the upper layers. This field has minimum length of 46 byte and maximum length of 1500 bytes.
6. CRC: It contains error detection code for the frame.

(*) Ethernet Specifications: 6 specifications

1. **10 base 5**: (Thick Ethernet or Thicknet):
   - It is a bus topology LAN with baseband signaling.
   - data rate 10 Mbps
   - max allowed segment length is 500m. To increase length repeaters can be used.
   - To reduce collision, total length of bus should not be greater than 2500m. i.e. 5 segments each of 500m length.
   - Each computer is separated by 2.5m so. 200 devices can be accomodated in each segment of 500m and total of 1000 devices in complete length of 2500m.

(*) Physical diagram: 10base5:



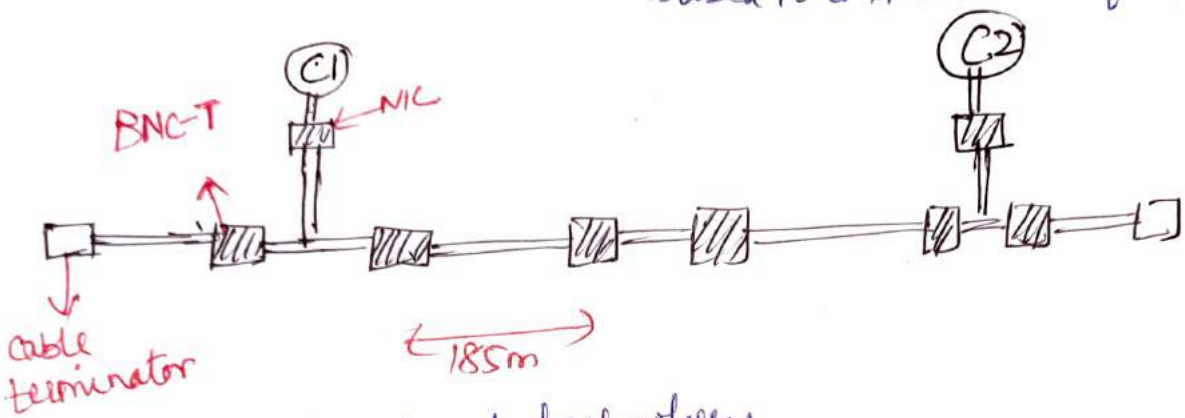
1. Coaxial Cable (Thick) - RG8 cable (main bus)
2. NIC
3. MAU or transceiver
4. AUI (Attachment Unit Interface) cable.

2. **10 base 2**: (Thin ethernet or thinnet or cheapnet or cheapernet)
   - it provides cheaper alternate to thicknet having same data rate i.e. 10 Mbps.
   - it uses thin coaxial cable
   - Segment length is 185m.
   - Less attaching devices.

- if small no. of computer are to be connected then this tech. is best.

⊛ Physical design:

- NIC
- Thin coaxial cable (RG-58) = Easy to install & move around
- BNC-T connectors = it is a T shaped device with three ports. One is used to connect NIC & 2 for i/p & o/p.



- it uses baseband technology.
- NO need of AUI cable.

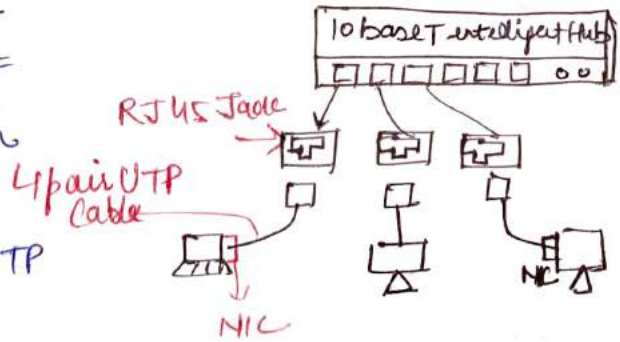
3. 10 base T ! (Twisted pair ethernet)

- Most popular ethernet standard defined in IEEE 802.3
- Uses STAR topology.
- UTP (unshielded Twisted pair) cables used
- Data rate 10 Mbps.
- max. cable length is 100 m.
- An intelligent hub is used.

Shakti Rep

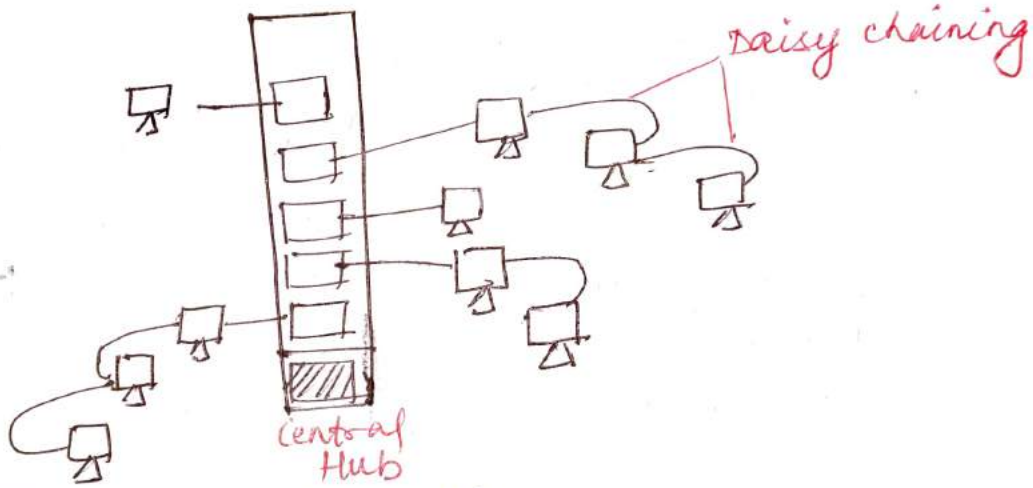
⊛ Physical Design

- An intelligent Hub = responsible to make connection between two stations.
- A 4 pair or 8-wired UTP
- RJ-45 Jack
- NIC



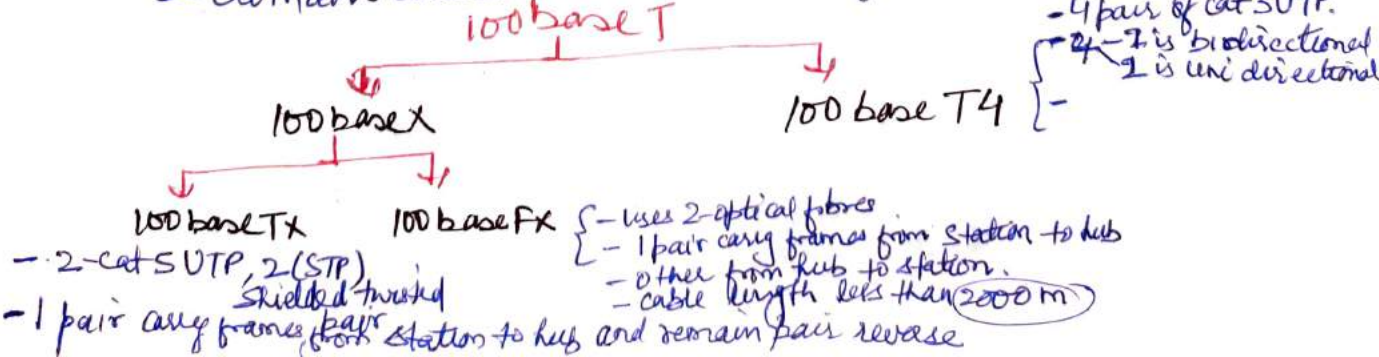
4) **1 Base 5 :** (Star LAN)

- Uses STAR topology.
- Uses HUB for connections
- AT & T product.
- Data rate is 1 Mbps (Very low)
- Least used ethernet.
- Allows cable length of 500 m in each segment.
- Range can be increase by using "Daisy chaining" method
- Only one device is connected to central HUB. and max 10 such devices to central HUB.



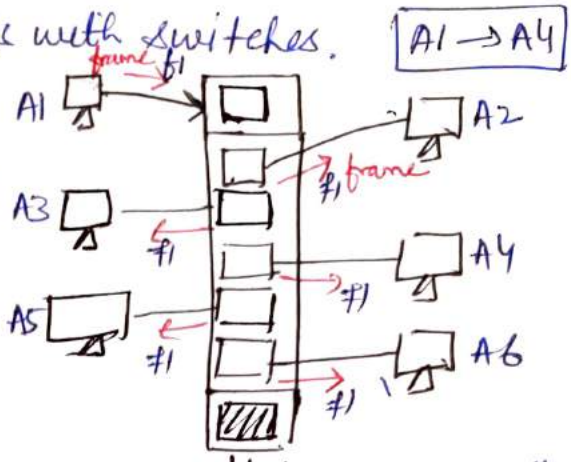
5) **100 base T :** (fast ethernet)

- Last Baseband
- Data rate 100 Mbps.
- Uses UTP
- Uses switches / central hub.
- STAR topology used
- max length of cable is 100 m.
- data speed is increased by factor 10.
- domain collisions is decreased by 10.

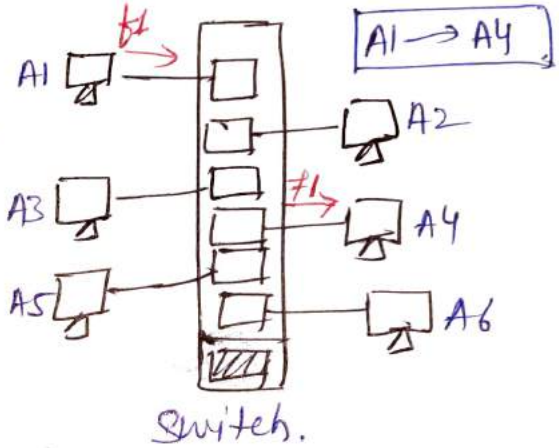


6) Switched Ethernet:

- It replaces HUB of previous methods with switches.
- If device A1 sends one data frame f1, then hub will receive it and send this f1 to all other 5 devices at a time, hence all cables will remain busy. and hence others will not be able to send any other frame at that time.
  To remove this issue, switched ethernet came into picture.

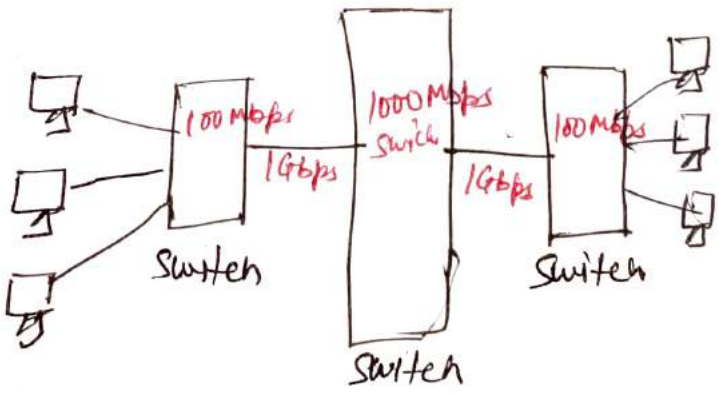


- If A1 sends frame to A4 then in switched ethernet, only one channel i.e. from A1 to Switch and Switch to A4 will be busy and others will be free for any communication.
- So in switch N/w, with N-devices, the capacity can be increased to N X 10 Mbps.



7) Gigabit Ethernet:

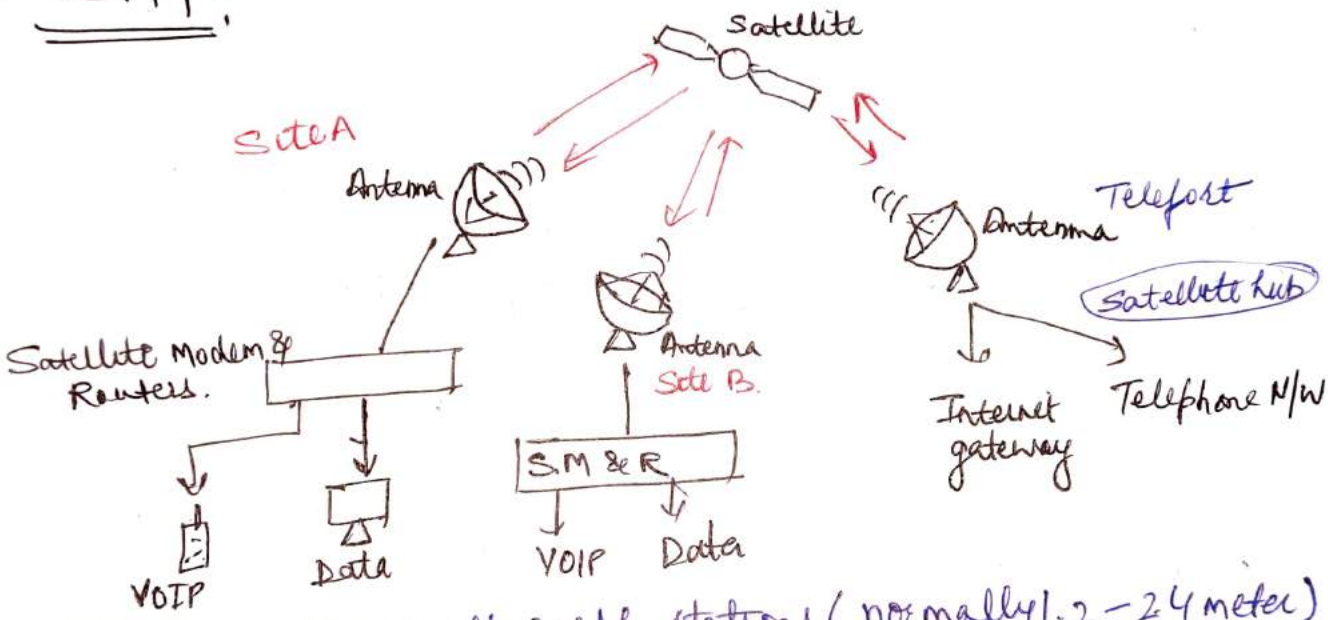
- Data rate 1000 Mbps or 1 Gbps.
- Collision domain is reduced.
- Uses optical fibres
- 4 categories are —
  - 1000 base LX } uses optical fibres. — 550m in multimode
  - 1000 base SX } — 550m — 5000m in monomode
  - 1000 base CX — 25m
  - 1000 base T — 25m.



Introduction to Media Connectivity:

1. VSAT: (Very Small Aperture Terminal)
2. PSTN (Public Switched Telephone Network)
3. DSL (Digital Subscriber line)
4. Optical Fibre
5. RF (Radio Frequency)
6. ISDN (Integrated Services Digital Network)

1. VSAT:



- VSAT are the small earth stations (normally 1.2–2.4 meter)
- utilised for reliable transmission of data, voice, and video via satellite.
- It consists of 2-units. One Indoor (IDU) which is installed in home for interfaces with user's communication devices
- ODU (outdoor unit) is place outside in a line of sight to the satellite.
- It is used to transmit narrow band data (ex. point of sale transactions such as Credit card, ATM, broadband data etc)
- It is used in remote location access.
- It is also used in mobile communication.

(*) **Configuration:** It can be configured in one of the following topologies:

1) Star topology - using a central uplink site to transport data back and forth to each VSAT terminal via satellite.
2) Mesh topology - each VST terminal relays data via satellite to another terminal by acting as a hub.
3) Mixture of above both technologies.

(*) **Characteristics:**

1) Band C having frequency 3 to 7 GHz used. The delivered power is low. Rainfall effect is minimum.
2) Band Ku having frequency 10 to 18 GHz used. The delivered power is medium. Rainfall effect is medium.

(*) **Advantages:**

1. Availability - services can be deployed anywhere.
2. Diversity - offers completely independent wireless link.
3. Homogeneity - gives same speed to all terminals.
4. Security - highly secure as they are private layer 2 network over the air.
5. Affordable -
6. Acceleration - delivers high quality internet performance

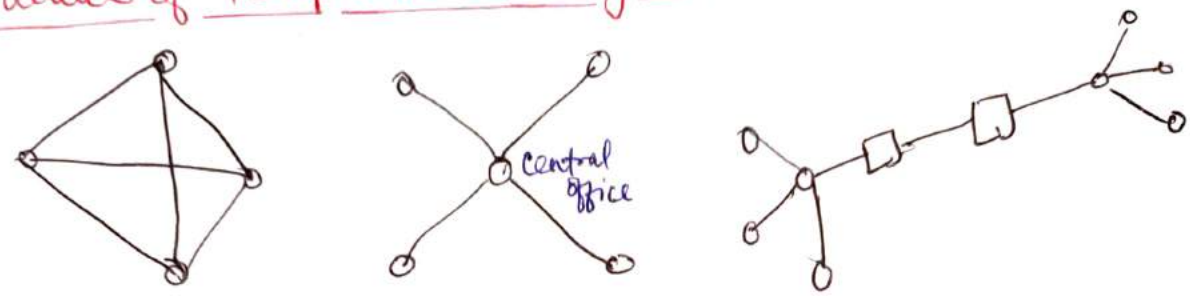
(*) **Disadvantages:**

1. Latency - since satellites is geosynchronous orbit, it takes minimum latency of 500 millisec. So it is a poor choice for online gaming.
2. Installation :- it require outdoor installation unit which is very difficult.

(2) PSTN : (Circuit switched Network.)

Our home telephone is connected to a circuit-switched network via an exchange through a local loop. PSTN is an example of it.

Structure of Telephone Exchanges :

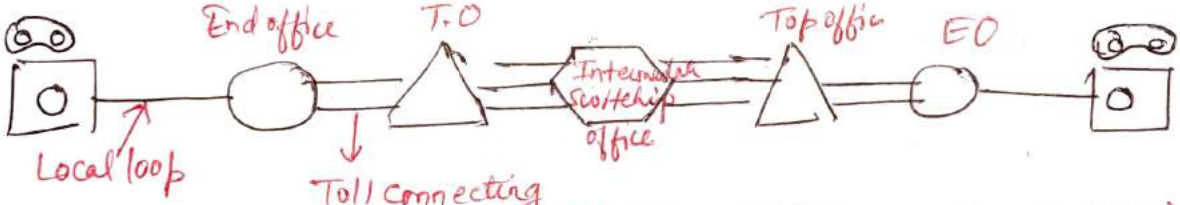


Fully interconnected
- as no of devices increased. It became difficult to manage.

Centralized switch
- It overcomes lacks of fully interconnected Model
- Here, operator in central office manually sets path using jumpers.
- Not suitable for long distances

Two ways hierarchy.
- to overcome previous model's shortcomings
- two wires goes to nearest telephone exchange makes a local loop.
- local loop distance is 1 to 10 km.

Local loop: The two wire connections between each subscriber's telephone and end office is known as local loop.



(digital fibre optics connecting switching)

Components :

1. Local loop = analog twisted pair cables going to houses.
2. Trunks
3. Switching offices.

(3) DSL : (digital Subscriber line)

It is the telephone line connecting end office to subscriber making a local loop for the purpose of high speed delivery of data, video, voice and multimedia. This is a analog line.

challenge is to make these links digital.

⊛ Technologies of DSL:

1. **ADSL**: It has higher bit rate in downstream (Network to subscriber) than upstream (subscriber to network).
   - This is most commonly ~~used~~ technology used by subscribers.
   - Modulation technology was CAP. (Carrier Amp/Phase) earlier, after this, DMT (Discrete Multi-tone) is using.
2. **HDSL**: (High bit rate digital subscriber line).
   - With this line, data rate of 2Mbps can be achieved without repeaters upto 3.6 km.
   - It uses two twisted-pair wires to achieve full duplex transmission.
   - It uses 2B1Q encoding, which is less susceptible to attenuation
3. **SDSL**: (Symmetric Digital subscriber line):
   - It is similar to HDSL but uses one single twisted pair cable.
4. **UDSL**: (Very high bit rate Digital Subscriber line):
   - It is similar to ADSL.
   - It uses coaxial, fibre optics, twisted pair cables for short distances (300-1800 m).
   - DMT modulation technique is used with downstream bit rate 50-55Mbps and upstream 1.5-2.5Mbps.

Shalini Roy

(4) Optical Fibre:

It is a medium to transmit data at high rate.

Advantage: Noise resistance, High bandwidths

Disadvantage: Expensive

(5) RF: (Radio Frequency):

- It can travel through air or space but requires specific transmitting and receiving mechanisms.
- It has frequencies between 3KHz to 300 GHz.

Features:

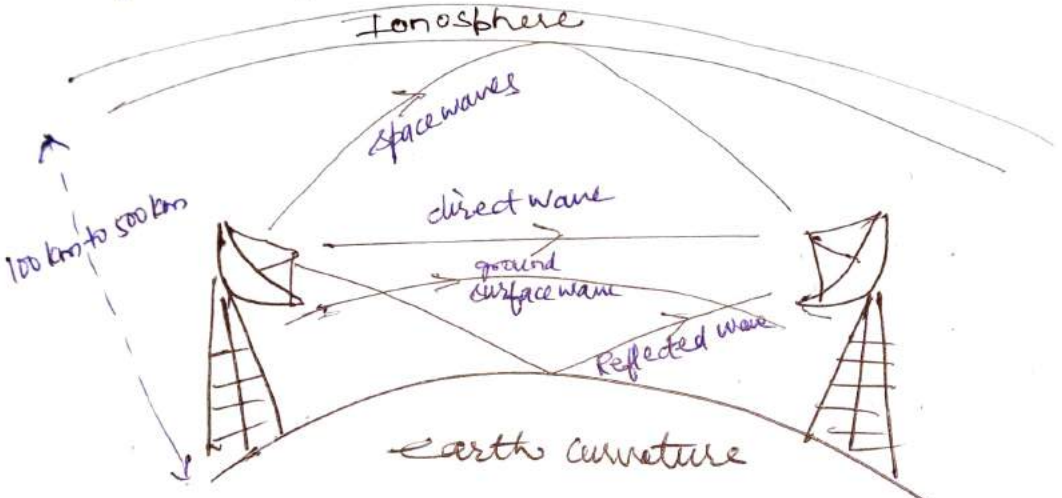
1. Easy to generate and can travel long distances.
2. Easily penetrate buildings.
3. Radio waves are unidirectional means they travel in all direction

i.e. no need to be careful about the setting of antenna.

4. It is frequency dependent.

⊛ Disadvantages:

1. At low frequencies radio waves pass through obstacles well but power falls off sharply with the distance.
2. At high frequencies radio waves tend to travel in straight line and bounce off obstacles.
3. At all frequencies radio waves are subject to interference from motors and other electrical equipment.



Ground waves :→ VLF (very low frequency), LF (Low freq.), MF (Medium waves freq)

Space waves :→ HF (High freq.), VHF (Very high Freq). These are refracted from ionosphere and return back to earth. These are used in military communication.

⑥ ISDN :- (Integrated services Digital Network)

- ISDN was developed by ITU-T in 1976.
- It is set of protocols that combines digital telephony and data transport services.
- It provides full integrated digital services to users

1. Bearer Services :- These belong to the first three layers of OSI model. It transfers information between users without the n/w manipulating the contents.
2. Teleservices : These belong to 4 to 7 layers of OSI model. Here N/W may change the data. They rely on bearer services.

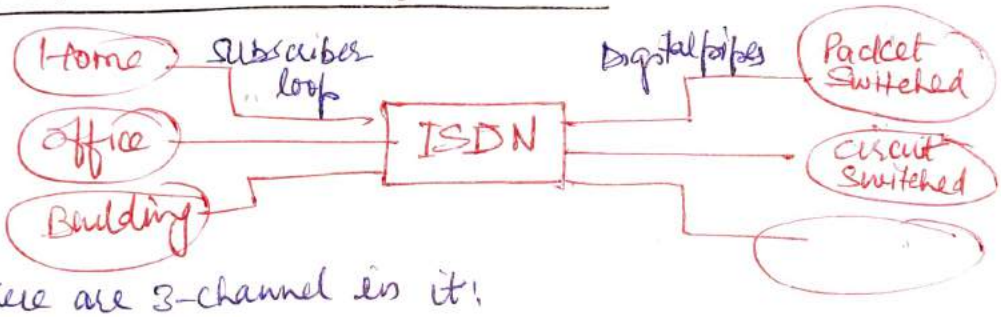
They include telephony, teletax, telefax, videotex, telex and teleconferencing.

3) Supplementary Services: Provides additional functionality to the bearer services and teleservices.

Advantages:

1) A copper line is used to transmit digital signals.
2) multiusers are connected using a single digital line with good speed.
3) ISDN can be plugged in through a traditional POTS (Plain old telephone service) line that can access both phone numbers at once.
4) digital modem is used to connect to ISDN.

(B) Access Mechanism of ISDN:



Shalini Roy

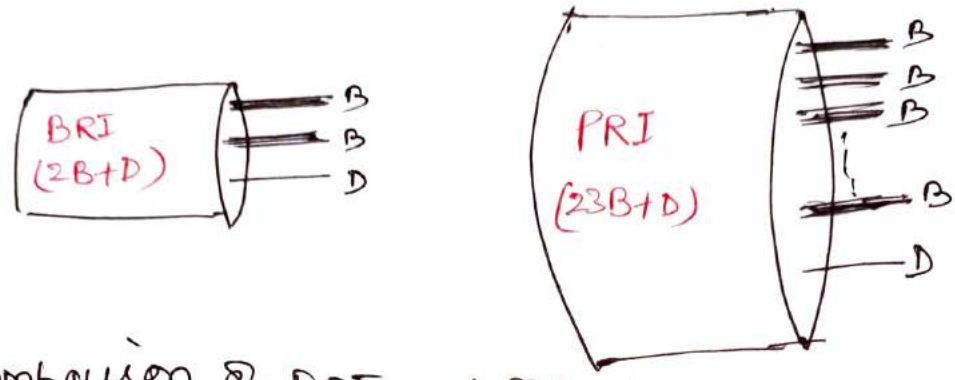
There are 3-channel in it:

1. B channel (Bearer) := Data rate 64 Kbps, it is basic user channel and can carry any type of information in full duplex mode.
2. D channel (Data) := Data rate 16-64 Kbps, its function is to carry control signals for B-channel
3. H channel (Hybrid) := Data rate 384, 1536, 1920 Kbps. It is used for high data rate applications such as video teleconferencing and so-on.

(A) Types of ISDN: Two types:

1. BRI :- Basic rate interface.
   - it consists of 2B channels and 1-D-channel of 16Kbps.
   - it is used for residential and small offices.
   - it require 48 Kbps of operating overhead.
   - it require 192 Kbps digital pipe.

2) PRI :-(Primary rate interface):
- it consists of 23 B channel and 1 D channel of 64kbps.
- it requires 8 kbps of operating overhead.
- it requires 1.544 Mbps of digital pipe.



(*) Comparison of BRI and PRI:

→ The major difference between BRI and PRI is the level of service and reliability.

→ BRI is the lower tier of service. It only provides basic needs at a lower cost.

→ PRI is the main service. It provides a better connection, more reliable service, and faster speeds.

→ BRI has max. speed of 128 kbps whereas PRI = 2.94 Mbps

Shakti Roy

(A) Differences:

ISDN	DSL
1. Data transfer rate is low	1. It transmit data faster than ISDN.
2. It is a dial-up service	2. It never needs a dialup of a number
3. They become active after dial-up.	3. They are "always-on connections".
4. Its top speeds is 128 kbps	4. Its top speed is 100 Mbps.
5. Two types - BRI & PRI	5. Two types - SDSL (symmetric DSL) & ADSL (Asymmetric DSL)
6. Some issue of interference	6. It reduces the interference of data with voice
7. It is replaced by DSL	7. It replaces ISDN

NETWORK ADMINISTRATION

NA-1

(*) Principles of Network Security:

Network security involves three key principles – confidentiality, integrity and availability.

1. **Confidentiality**: It specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if any unauthorized person is able to access a message.
2. **Authentication**: It is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. It is mostly secured by using username and password.
3. **Integrity**: Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it, but before reaching the intended receiver, then it is said that the integrity of the message is lost.
4. **Non-Repudiation**: It is the mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the Non-Repudiation doesn't allow the sender to refuse the receiver.
5. **Access Control**: The principles of access control is determined by role management and rule management.
   Role management determines who should access the data while rule management determines upto what extent one can access the data. The information displayed is dependent on the person who is accessing it.
6. **Availability**: It states that the resources will be available to authorize party at all times. Systems should have sufficient availability of information to satisfy the user request.

Shalini Rai

* **Cryptography:** It refers to the science and art of transforming messages to make them secure and immune to attacks.

It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

cryptography not only protects data from theft or alteration but can also be used for user authentication.

* **Components of Cryptography:**

1. **Plaintext and Ciphertext:** The original message, before being transformed, is called plaintext.
After the message is transformed, it is called Ciphertext.
An encryption algorithm transforms the plaintext into ciphertext. A decryption algorithm transforms the cipher-text back into plaintext.
The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

2. **Cipher:** ciphers are the encryption and decryption algos.
It may includes many such algorithms. and one Cipher can serve millions of communicating pairs.

3. **Key:** key is a number (or a set of numbers / passcode) based on which the cipher (algo) will be functional.
It is just like key of a lock. So -
So encrypt a message we need — 1) An encryption algo.
2) An Encryption key
3) A Plaintext.

So decrypt a message we need — 1) a decryption key
2) a decryption algo
3) the Ciphertext.

Then we will get the original text.

* **Types of Cryptography:** Two types -
1) Symmetric key Cryptography.
2) Asymmetric key Cryptography.

1. Symmetric key cryptography: Here, the same key is used by both parties (sender and receiver)

2. Asymmetric key cryptography: (Public key cryptography) Different keys are used at sender and receiver. Here a Public key is used by the sender for encryption while a Private key is used by the receiver for decryption.

The Public key is available to the public, and the private key is available only to an individual.

* Modern Cryptography objectives:
  1) Confidentiality
  2) Integrity
  3) Non-repudiation
  4) Authentication

* NMAP: (Network mapper)
  It is a free, open source tool for vulnerability scanning and network discovery. It is used to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

  It is a port scan tool, gathering information by sending raw packets to system ports. It listens the responses and determines whether ports are open, closed or filtered.

* Troubleshooting: It is a process of finding out the cause of the problem and eliminating the problem by identifying the cause.

  In any network, system may be down due to failure of machines, connecting lines, connectors or any other reason. so to locate the fault in case of network failure and remove it is called network trouble shooting. Various steps are -
  1. Problem Identification
  2. Fault location
  3. Fault Removal.

  } all of them

NAT

* **Troubleshooting Tools:** Sometimes your network shows error or not work. These issues can be resolved using following tools -

1. **PING:** most commonly used tool. This tools is used to test connectivity between requesting host and destination host.

   eg: ping 192.168.1.38 -t ; if it msg -

   1. Reply from 192.168.1.38 : byte=32 time=7ms TTL=255 then it means connection is proper.
   2. If messages shown is " Request time Out", then it means that is some break/issue in cable.

2. **Tracert / Traceroute:** It can be used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts.
   It is useful for trouble-shooting large networks.

   eg: tracert www.google.com ↵

   1. 4ms 12ms 5ms 10.131.81.1
   2. * 120ms 194ms 172.24.164.130
   3. — — — — —

   Note: Tracert command is used in windows.
   Traceroute command is used in LINUX.

3. **IPconfig / IFCONFIG:**
   This is used to determine IP config of host. It gives TCP/IP configuration details like IP Address, Subnet masks and default gateways of the computer.
   IP config command is used for windows
   IFCONFIG command is used in LINUX.

   eg: IPCONFIG ↵
   ≡ detail.

4. **NETSTAT:** This used to determine current state of active network connections on a host. when verifying the states of a listening port on a host or to check and see what remote hosts are connected to a local host on a specific port.
   eg: netstat ↵

5. **Wireshark:** It is a free open source packet analyzer used for troubleshooting network issues. It can be used for
   a) Slow webserver
   b) Analyse HTTP traffic.
   c) See the requests to the server, HTTP headers, commands and parameters
   d) See the responses to the client from the server, including HTTP headers, commands and HTML returned.

6. **Sniffer (PacketSniffer):**
   It is used to look inside header of packets. It helps if packets, route and path are, as expected. It can be used to:
   a) Find missing traffic.
   b) Find if sessions are proper
   c) Find the address used if system is using multiple addresses.
   d) Missing ping packets.
   e) Confirming route

7. **TCPDUMP:** It is a common packet analyser that runs under the command line. It prints the contents of network packets. It can read packets from a network interface card or from a previously created saved packet file. It can ~~create~~ write packets to standard output or a file.
   It can also be used in intercepting and displaying the unencrypted communications of other users/computers. Such as Telnet or http can use it to view login Ids, passwords, the URLs and content of websites being viewed.

8. **NSlookup:** It is used in locating IP addresses associated with a domain name and checking to see that DNS resolution is working for our host.
   eg: nslookup www.google.com ↵

9. **whois:** This is used to get information about who owns a given domain name or a range of public IP space. It gives all related information.
   benefit: Finding out who owns a range of IP space can help us to

Shakti Roy

determine where add traffic on our network is coming from.

10. Putty / Tera term: It is used for troubleshooting remotely. especially with LINUX/UNIX. It contains two sessions - Putty session and Tera term session

11. Subnet and IP calculator:

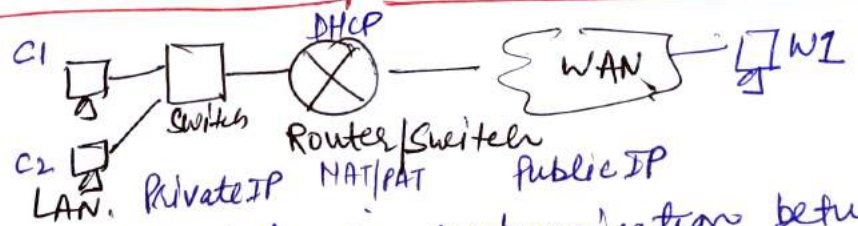
12. Speed Test: This is used to test the bandwidth. or speed of network.

13. IP Scanner: This is used when we donot have login credentials to the router. This can also help us to find devices that have mistakenly been configured with incorrect or duplicate IPs.

(*) DHCP Server: (Dynamic Host Configuration Protocol)

It is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as DHCP. to respond to broadcast queries by clients.

(*) How to use a Router/Switch as DHCP server:



DHCP has a key role in communication between private LAN to Public WAN. whenever system wants to communicate any system W1 in WAN, it's request will be routed through DHCP Server.

It is very easy to configure system manual if LAN is small. else DHCP is used.

~~most of the routers~~

Router must follow DORA process.

Shakti Raj

⊛ Working of DHCP : (RFC 2131) (Private always)

1) It automatically assign IP addresses to DHCP clients
2) It is based on client-server model.
3) DHCP works at Application layer
4) IP Address assigned is known as dynamic IP Address.
   (Address is assigned for a specific (lease time) — wait for renew request
5) DHCP IP address range is called scope.
   { Pool of total address available in DHCP server for allotment to the clients. It retain only one IP for itself
   eg: 172.16.0.0/16 , 172.16.3.0/24 , 172.0.0.0/8
6) BootP is the another method to allocate IP but MAC address must be entered manually in a BootP table. DHCP is advance version of BootP.
7) DHCP is a dynamic BootP.
8) It uses • UDP Port 67 & 68 at transport layer. It is for connectionless connection.
9) Besides DHCP server can provide us —
   1) IP Address
   2) Subnet mask
   3) Domain Name
   4) Default Gateway
   5) DNS Server Address
   6) WINS Server Address.

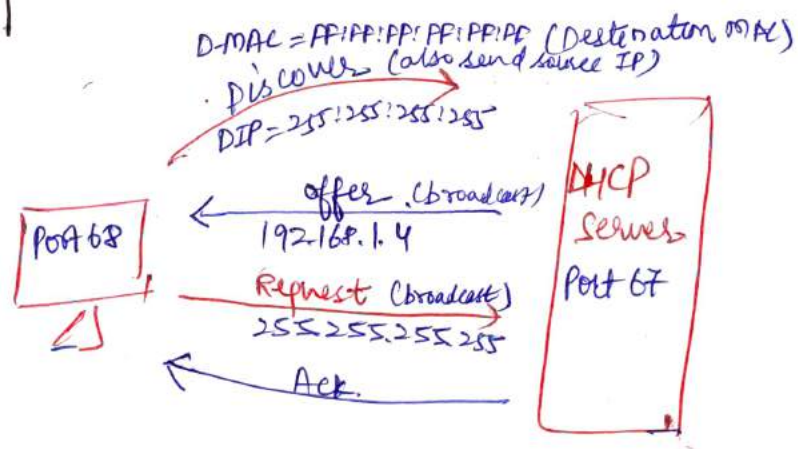
⊛ DORA Process: Discover, offer, Request, Acknowledge

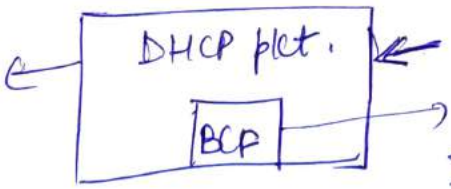
using this process, a client can get his IP address from server via when it will start further communication.

Initially client doesn't have any IP, then it starts broadcasting message that it has no IP. Then DHCP catches this signal and revert back with offer request, then

NA-8

DHCP message	Description
DHCP (68) Discover	UDP Broadcast from DHCP client to locate available server Layer 2: FF:FF:FF:FF:FF:FF → Server discovery. Data link - MAC (Hexa decimal) Layer 3: 255.255.255.255 → Network layer (IP)
DHCP (67) Offer	DHCP server to client in response to DHCP discover with offer of configuration parameter (IP Address of DHCP server, offer IP, MAC Address of client, subnet mask, lease length)
DHCP (68) Request	Client then broadcast to the server (It may have many DHCP servers) ~~and~~ with DHCP request message asking for the offered IP address and possible other info.
DHCP (67) Acknowledge	Server to client with configuration parameters including committed network Address.





Broadcast Flag
If BCF = 0 unicast
= 1 Broadcast

Video sent on 03/01/22.

NA-9

DHCP Scope:

A scope can be defined as a set of IP addresses which the DHCP server can allocate or assign to DHCP clients. Scope for DHCP server are configured by administrator.

Eg: 172.16.1.0/24, 10.0.0.0/8.

Superscope:

A superscope is the grouping of scope under one administrative entity that enables client to obtain IP address, and renew IP addresses from any scope that is part of the superscope.

Superscope used when:

1) The existing scope i.e. IP addresses are being depleted
2) You want to use two DHCP servers on the same subnet
3) You need to move client from one range of IP addresses to a different range of IP addresses.

Shakti Raj

Network Connectivity

(*) Connectivity: It is the degree to which any given computer can cooperate with other network computers/components.
without connectivity, network is of no use.

(*) In this chapter, we learn about hardware devices that are used in n/w connectivity.

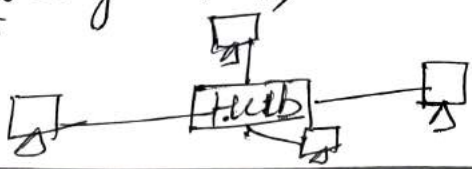
(*) Network Connecting Devices:
These are the devices used to connect two computers, two networks and deals with all intermediate jobs.

1. NIC
2. HUBS
3. Switches
4. Repeaters
5. Multiplexers
6. Modems
7. Routers & Bridges
8. Gateways, etc.

1) NIC:- (Network Interface card)
It is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also known as Network Interface controller, Network adapter, or LAN adapter.
It is of two types:

1. Ethernet NIC
2. Wireless Network NIC.

2) HUBS: A network HUB is a node/device that broadcasts data to every computer or ethernet-based device connected to it.
A HUB is less sophisticated than a switch. It is best suited for small LAN following STAR, TREE topology
- hub works in Physical layer of OSI
- it cannot filter data
- follows half duplex.
Broadcast job.

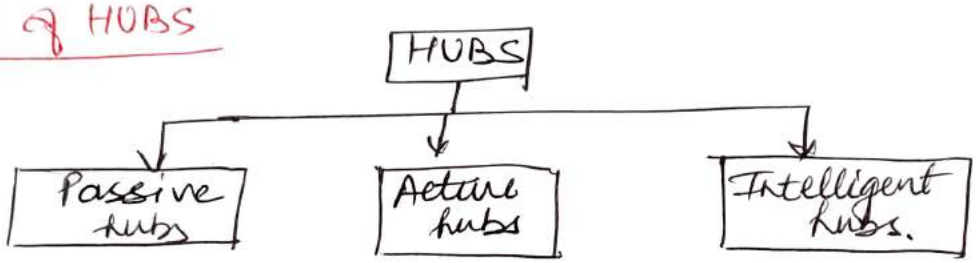


Hubs are of three types:

1. Active hubs
2. Passive Hub
3. Intelligent hub

- Collisions may occur during setup of transmission when more than one computers place data simultaneously in the corresponding port.
- Lack of intelligence
- Passive devices, they don't have any software associated with it.
- They have fewer ports of I/O.

(*) Type of HUBS



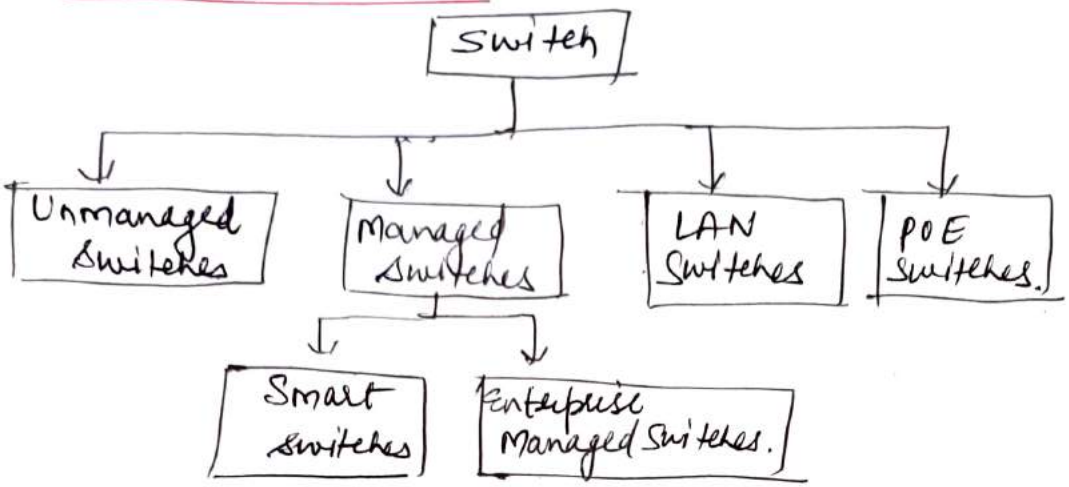
1. **Passive Hub:** It connects nodes in a star configuration They broadcast signals onto the network without amplifying or regenerating them. They limit the size of LAN.

2. **Active Hubs:** Active hubs amplify and regenerate the incoming electrical signals before broadcasting them.
   - They have their own power supply and serves both as repeater as well as connecting centre.
   - They increase the size of LAN.

3. **Intelligent Hubs:** - They are active hubs with additional n/w management facility like n/w management, switching, providing flexible data rates etc.

(*) **Switches:** They are networking devices operating at layer-2 or a data link layer of OSI-model.
   - They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.
   - It has many ports for connections.
   - They receive data from multiple input ports and send to its intended destination in the network.

⊛ Types of Switches:



1. **Unmanaged Switches:** They are mostly used in home networks & small business. They are plug and play. They do not need to be watched or configured. They are used locally. They are least expensive.

2. **Managed Switches:** They have many features —
   1) highest level of security, precision control and full managment of the network.
   2) These functionality can be customized.
   3) They are used in large organisation.
   4) They are scalable i.e. ideal for growing network

⊛ **Smart switches:**
- They have basic management features.
- They are called partial managed devices.
- It can accept configuration of VLAN.

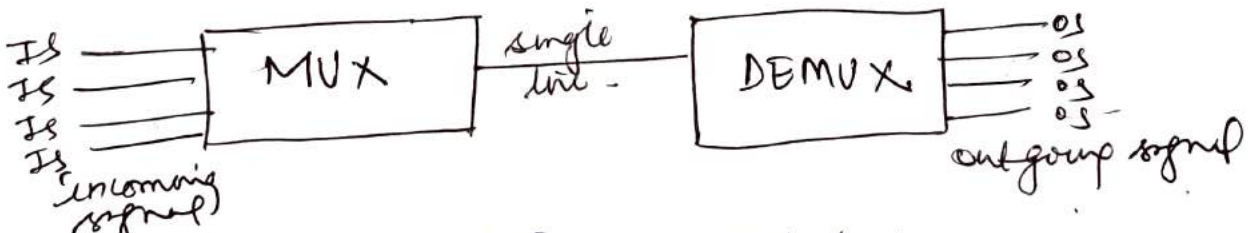
⊛ **Enterpeises managed switches:**
- They have ability to fix, copy, transform and display different network configurations alongwith a web interface and command line interface.
- Fully managed switches.
- More expensive.
- used in large organisations.

4) **LAN Switch:**
- These are known as Ethernet switches/data switches.
- Used to reduce network congestion.
- delivers packets of data only to its intended recipient.

5) **PoE switches:**
- Uses Power over ethernet technology. It integrates data and power on the same cable.
- simplifying the cable process.

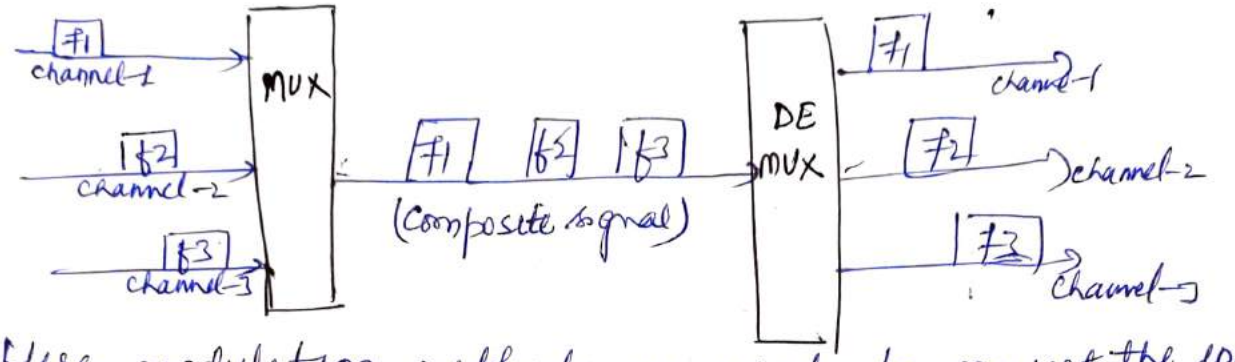
(4) **Repeaters:**
- They operate at Physical layer of OSI model.
- They amplify/regenerate an incoming signal before retransmitting it.
- They are used to expand the coverage area.
- They are also known as signal boosters.
- They have no intelligence.

(5) **Multiplexer:-**
- A multiplexer is a device that merges several lower speed transmission channels into one high speed channel at one end of the link and at the another end the low speed channels are reproduced from this one high speed channel by another multiplexers.
- It is done by multiplexer and De-multiplexer respectively.
- Multiplexers at both ends should be properly synchronized.



(*) **Types:-** Multiplexing is of 3 types:
1) FDM (Freqheney Division Multiplexing)
2) TDM (Time Division multiplexing)
3) WDM (Wavelength Division Multiplexing)

1) FDM: It is an analog technique that can be applied when the bandwidth of a link is greater than the combined bandwidths of the signals to be transmitted.



Here, modulation methods are used to convert the input signals into frequency bands, which are then merged by a multiplexer to produce a composite signal.

Guard bands are used to divide the channels. A guard band is a frequency that neither channel uses.

Uses: used in TV, FM, AM Networks.

Shakti Raj

2) ~~FDM~~

Drawbacks:

1) Guard bands consumes much of available bandwidth to prevent interfering with each other.
2) If all senders are not sending msg. regularly then much of bandwidth is wasted because of the idle channel conditions.

So to overcome such issues - TDM comes.

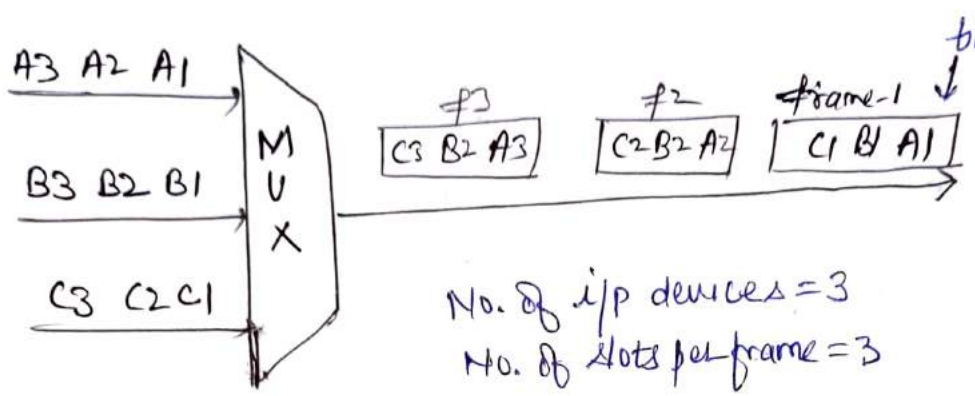
3) TDM: In TDM, the signals are such mixed that each signal is sent at a different time instant i.e. their clock cycle starts at different instants such that none of them falls into same time slot.

If a users is not transmitting at a particular time then that time is wasted.

TDM can be implemented in two ways -

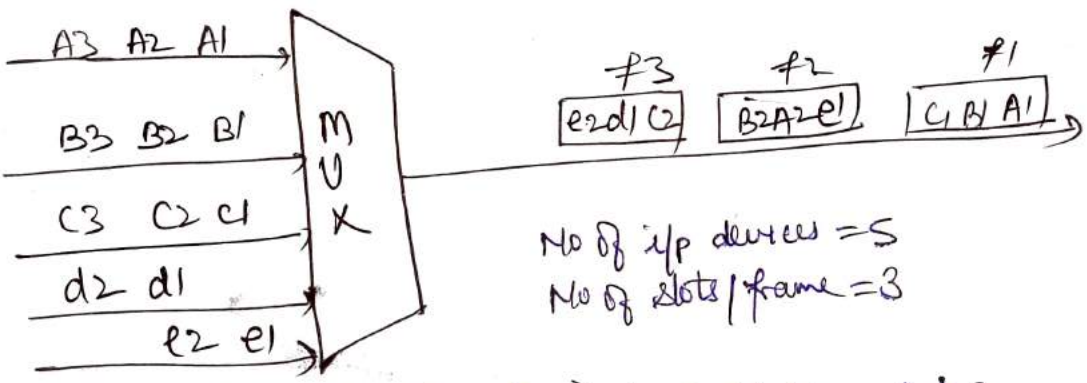
1) Synchronous TDM
2) Asynchronous TDM

1) **Synchronous TDM:** Here multiplexer allocates same time slot to each device at all times, whether or not a device has anything to transmit.



No. of i/p devices = 3
No. of slots per frame = 3

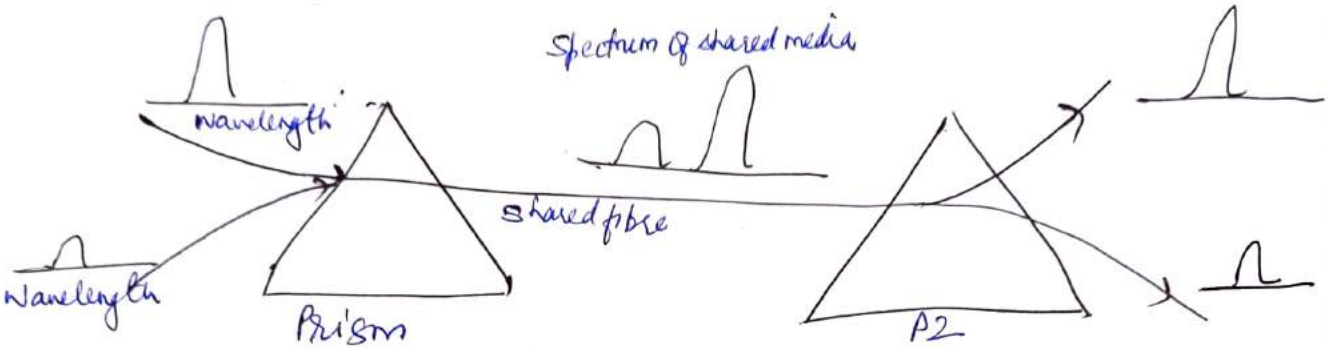
2) **Asynchronous TDM:** This overcome STDM shortcoming when nothing to transmit by a single device.
- This is also known as statistical TDM.
- It is designed to avoid the wastage.
- Here each time slot is available to any attached device when it has a data to send.
- Here total speed/number of input lines can be greater than the capacity of path.



No of i/p devices = 5
No of slots/frame = 3

3) **WDM:** (Wavelength division Multiplexing):
- It uses light signals and passed through fiber optical channels.
- A Prism/diffraction grating is used alongwith two fibres.
- Both fibres have different band energies.
- Beams from both fibres pass through the prism and then on a single fiber optical cable.
- Because of their different band energies, the spectrum

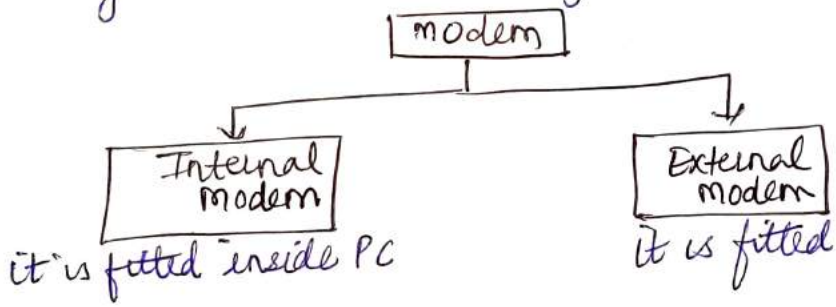
on this shared fibre is different from both of them. This multiplexed signal again passes through prism at receiving end and it splits back onto two fibres channels.
— This is highly reliable and popular.



(*) **Demultiplexing:** It is a technique that is inverse of multiplexing. It divides multiplexed signal into 'n' output signals to be sent on 'n' output lines.

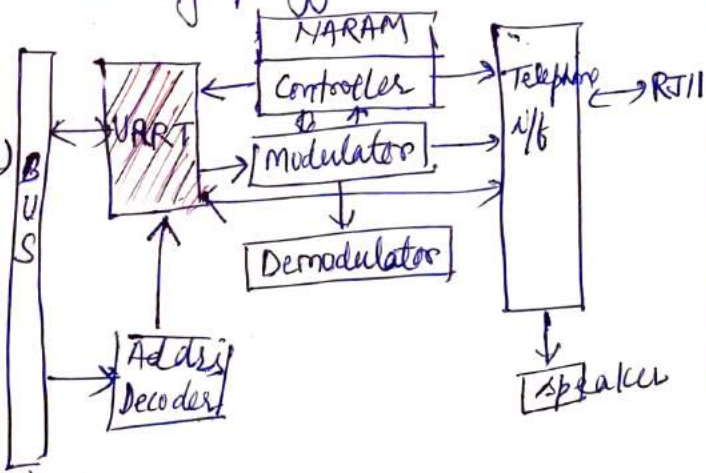
⑥ **Modem:**

Modem stands for modulation Demodulation. It converts the digital data signals into analog data signals. They can be connected using serial or USB port.



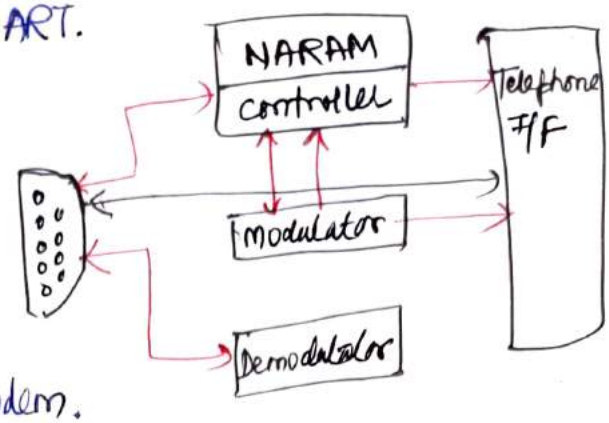
1) **Internal modem:** It is directly plugged in an ISA or PCI expansion Bus

- it contains its own UART (Universal Asynchronous Receiver/Transmitter) which is responsible for manipulating data into and out of serial form
- It converts parallel data into serial data.
- Then modulator converts serial data into analog signals.
- Demodulator converts it into data signals or serial data.



2) External Modem:

- It doesn't have an inbuilt UART. rather it relies on an existing serial port that is already configured in the computer.
- Faster and easier to operate than internal Modem.
- It needs external power adapter.



⊛ Features of modem:

1. They can be upgraded using software patches.
2. It enables high speed downstream data transfer while upstream runs at conventional rate of 33.6 kbps.
3. Some modems perform dual simultaneous voice and Data (DSVD).
4. Some modems ~~incorporate the~~ provide advanced voice mail features and these modem serves as intelligent answering machine
5. They can differentiate between a voice call, a modem call and an incoming fax.
6. They can detect callers originating telephone number and thus they can serve as caller ID.
7. The DSL modems allows transmission of voice, video and data over telephone lines at very high speed.

   1 DSL modem speed = 146 times of 56kbps modem.
   = 62 times than ISDN.

⊛ Types of modem:

Depending upon speed and functioning etc, different types are as under:

1. optical modem
2. Digital Modem
3. Acoustic Modem
4. Smart Modem
5. Short Haul Modem.

Shalotti Raj

① **optical modem:** It uses optical cables instead of metallic cable. It converts the digital data signals into pulse of light that are to be transmitted on the optical fibers used by it.

② **Digital modem:** It converts digital data into digital signals for transmission on digital transmission line.

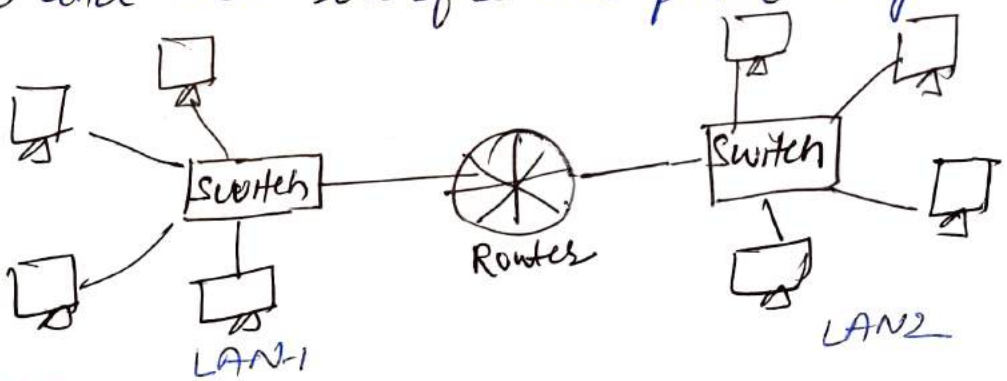
③ **Acoustic modem:** It can couple the telephone handset with a device that is used by traveling salespeople to connect the hotel phones. It contains a speaker and microphone.

④ **Smart modem:** It allows auto dial/radial and auto answer capabilities. It contains a microprocessor on board.

⑤ **Short haul modem:** They are present in your PC at home. They can transmit data over 20 miles or less. Generally, they are used to connect PC's in a building or office within this area.

⑦ **Routers:** Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysis and forwarding data packets among the connected computer networks.

When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.



✱ **Types of Routers:**

Basis on their function, they are of 6-types:

1. Central Router
2. Local Router
3. Remote Router
4. Internal Router
5. External Router
6. Peripheral Router.

(1) **Central Router:** It connects many LANs together.

(2) **Local Router:** It has a limitation to operate within the limits of its LAN drivers cable length limitations.

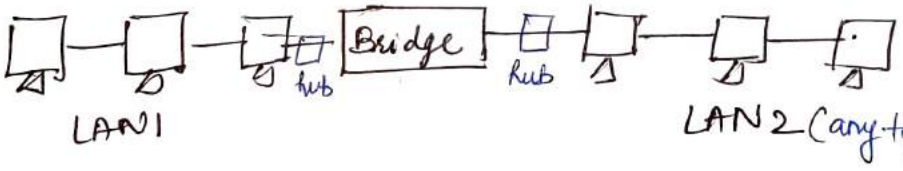
(3) **Remote Router:** It uses modems/remote connections to connect the LAN's beyond its device drivers limitations.

(4) **Internal Router:** It is a part of Network file server and it routes the data accordingly.

(5) **External Router:** It is located in a workstation on the network.

(6) **Peripheral Router:** It connects individual LANs to a central router or sometimes to another peripheral router.

(7b) **Bridges:** (Layer 2 Switch)



It connects multiple LANs together to form a larger LAN. The process of aggregating networks is called network bridging. It makes the combined network to appear as a single network. It operates at Data link layer. They are also known as Layer-2 switch. Subnetworks should have similar protocols.

Bridges Types: 3 types

1. **Simple:** It connects two segments and contains a table that lists the addresses of all the stations. It is cheapest.
2. **Multiport:** It connects more than two LANs.
3. **Transparent:** It starts with empty table. It is also known as learning bridge. It builds its table of station addresses on its own.

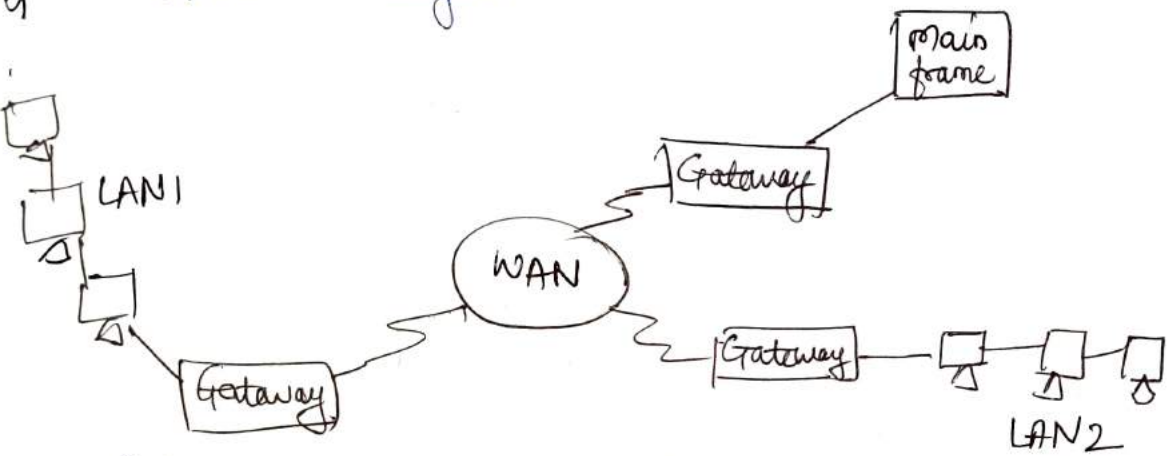
Shakti Roy

(9) Gateway: This device is used to connect two networks with different transmission protocols together. Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.

It operates at top most layer i.e. Application layer of OSI model. While routers operate on Network layer.

It converts data packets from one protocal format to another before forwarding it because it interconnects two dissimilar networks.

It incorporates a protocol conversion function at Application Layer.



- Gateways are slower than bridges and routers.
- Bridges cannot join dissimilar LANs

(*) Types of Gateways:

1. Default gateway: These are the computers used to access external networks when another gateway is not specified.
2. Media gateway: These are used with audio and video transmissions
3. Payment gateway: These are secure computers that receive and then accept or decline online payments.
4. VOIP gateway: These are used with voice over internet protocol communications such as phone calls made from PCs.

⊛ Configuration of Routers & Switches:

It is the most important part of the network basis on which it becomes fully functional.

Steps:

1) First switch ON router, connect router to network either via wire or wireless. Then open PCs web-browser such as IE. Then type http://192.168.0.1 or 192.168.1.1. or any other URL as given on the device.
2) Now it asked for user id & password, enter default user as "admin" & password "admin". Or any other mentioned on device
3) Then complete router informations will be opened for new settings. It can be set up automatically using quicksetup mode or can be done manually.
4) Enable the router's firewall if needed.
5) Set SSID (service set Identifier) for your wireless network. This is the name by which the wireless network is known.
6) Set WEP (wire equivalent Privacy) for encryption, means give your password just to protect your network
7) If you don't give the password then windows may not even connect to a wireless network that locks a password.
8) (optional) Configure to allow connections only from the known computers. This can be achieved by setting up/of binding of MAC address of each host to IPs at each hosts.
9) If not binding, then allow the router to issue IPs dynamically to all hosts on the network using enabling of DHCP (Dynamic Host Configuration Protocol)
10) Incoming and outgoing data speed can also be controlled via these devices.
11) Unauthorised websites can also be blocked using it.

Wireless Networking

(*) **WLAN:** A wireless LAN is a wireless local area network, which may be defined as connection of two or more computers without using wires. It utilises spread-spectrum technology based on radio waves to enable communication between devices in a limited area.

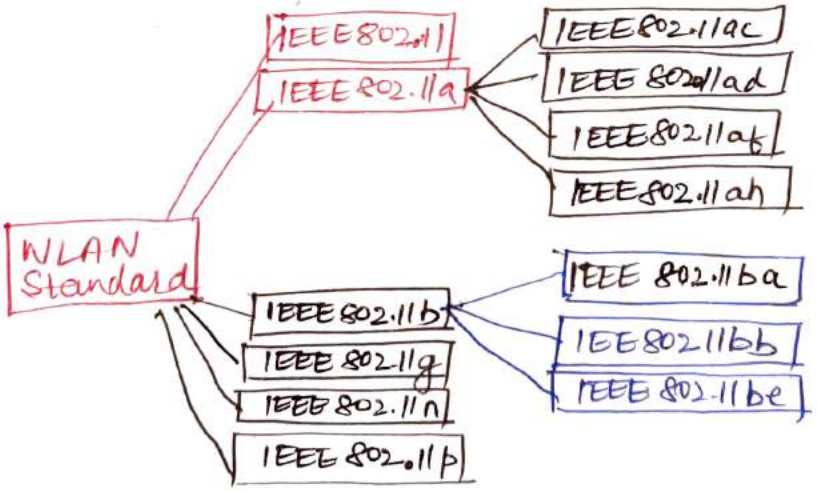
The main advantage of WLAN is that it helps us to get rid of all the cables and wires, and excellent device mobility.

Basically it is of 4-types:

1. WLAN - Wireless local Area N/w
2. WMAN - Wireless metropolitan Area N/w.
3. WPAN - Wireless personal Area Network.
4. WWAN - Wireless wide Area Network.

eg: 1. Mobile Phone N/w
2. Wireless sensor N/w
3. Satellite communication N/w
4. Terrestrial microwave N/w.

(*) **IEEE 802.11 standard:** This standard is popularly known as Wifi and lays down the architecture and specification of WLANs. There are several standard of IEEE 802.11 WLAN. All the standards use CSMA/CA (carrier-sense multiple access with collision avoidance). Also, they have support for both centralised base station based as well as adhoc networks.



① **IEEE 802.11:** originally released in A97. It provided 1Mbps or 2Mbps data rate in the 2.4 GHz band and used either FHSS (frequency-hopping spread spectrum) or DSSS (direct-sequence spread spectrum). It is obsolete now.

② **IEEE 802.11a:** comes in 1999. It uses OFDM (Orthogonal frequency division multiplexing). It provides max data rate of 54Mbps operating in 5GHz band. It provides error correcting codes also. It follows many new versions.

③ **IEEE 802.11b:** comes in 2000, it is a direct extension of the original 802.11 stnd. It uses same modulation technique DSSS. It operates in 2.4GHz band with data rate 11Mbps. It is still crowded so suffering with device interferences. It also follows many amendments.

④ **IEEE 802.11g:** comes in 2003, it operates in 2.4 GHz band with Average data rate of 22Mbps. It uses OFDM technique.

⑤ **IEEE 802.11n:** comes in 2009, operates in 2.4 GHz and 5GHz bands. It has variable data rate ranging from 54Mbps to 600Mbps. It uses MIMO antennas (Multiple Input multiple output).

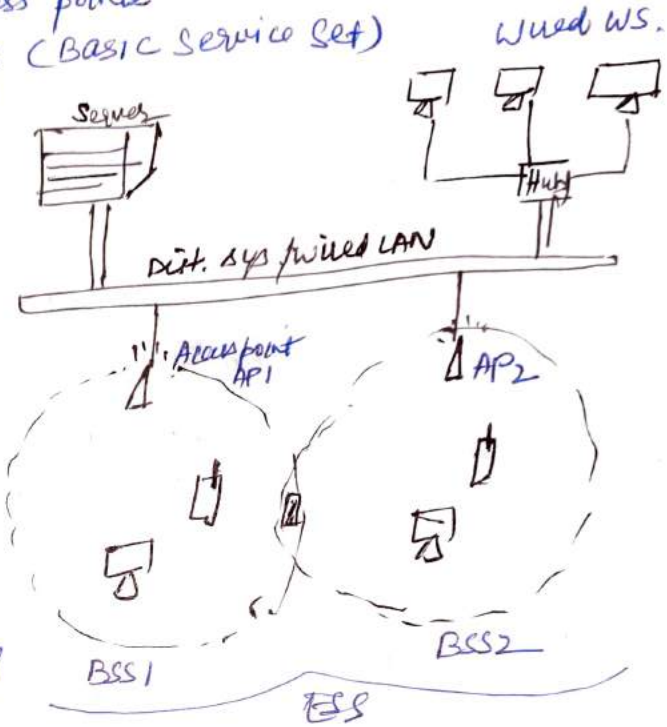
⑥ **IEEE 802.11p:** It includes network communications between vehicles moving at high speed and the environment. It uses WAVE (Wireless access in vehicular environments) to support ITS (Intelligent Transportation Systems). They have a data rate of 27Mbps and operates in 5.9 GHz band.

⑦ **Benefits of Wireless LANs:**

1) Convenience — in every manner
2) Affordable
3) mobility
4) Productivity
5) Speed & scalability
6) Remote areas accessibility
7) It has better chance of surviving disasters.

Architecture of a wireless LAN or 802.11 :

It consists of – 1) Stations
2) Servers
3) distributed system or wired LAN
4) Access points
5) BSS (Basic service set)
6) ESS



1) Stations: All components that can connect into a wireless medium in a n/w are referred to as stations. Two types:

1. Wireless & wired clients:
Wireless clients can be desktops, workstations, mobiles, laptops, PDA (personal digital assistant) etc. They should have NIC.
Wired clients are connected through cables.

2. Access point (A.P.): APs are the base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with.

3) BSS: It is a set of all stations that can communicate with each other. They are 2-types –
1) Independent BSS (without AP)
2) Infrastructure BSS (with AP)
Every BSS has an id called BSSID. and this is the MAC address of the AP servicing the concerned BSS.

4) ESS (Extended Service set): ESS is a set of connected BSS. APs in ESS are connected to each other and with stations as well as server by a distributed system.
Each ESS has an ID called SSID which is a 32-byte character string
eg: linksys is a default SSID for Linksys routers.

(*) Types of Stations in ESS:

Depending on the mobility, 3 types of stations are defined by IEEE 802.11.

1) No transition mobility
2) BSS transition mobility
3) ESS transition mobility

1) **No transition Mobility:** It is defined as a station which is no moving (stationary) or moving only inside a BSS.

2) **BSS transition mobility:** It is the one which can move from BSS to another but doesn't move outside one ESS.

3) **ESS transition mobility:** These types of stations can move from one ESS to another. Here, 802.11 doesn't gharantee a contenious communication when the station is moving.

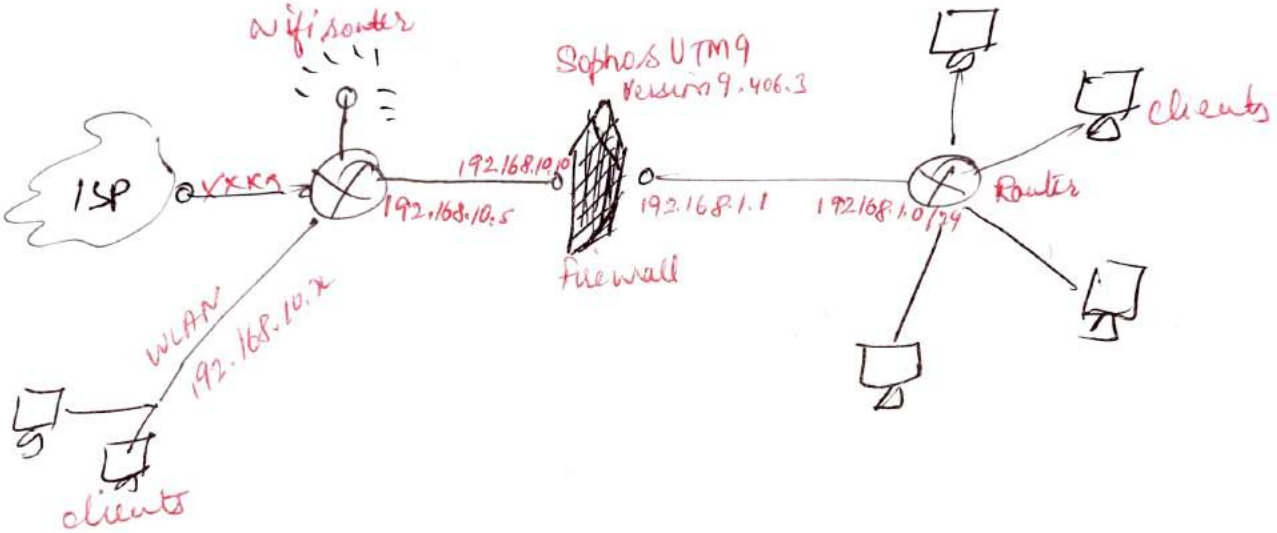
(*) WiMAX and Li-Fi:

S.No	Feature	WiMAX	Li-Fi
1.	Full form	World wide Interoperability for microwave Access.	light-fidelity
2	operation	Broadband wireless Access	It transmits data using light with the help of LED Bulbs.
3.	Interference	WiMAX communication poses a significant interference threat to satellite signals transmitted in C Band frequency	Do not have any interference issues similar to radio frequency waves.
4.	Technology	Wireless metropolitan Area N/w.	Present IrDA compliant device
5.	Application	Serves a large interoperable N/w	Used in airlines, undersea, operation theatre in Hospital office and home premises for data transfer & internet browsing
6.	Merits	can be used for long ranges upto 30 kms.	Interference is less, can pass through salty sea water
7.	Data transfer speed	works at 50 Mbps/Hz and can peak upto 1000 Mbps in a 20MHz	About 1 Gbps.
8.	Data density	Works in high dense environment.	Works in high dense environment
9.	Coverage distance	Upto 40 miles	About 10m
10.	power consumption	High	medium
11.	cost price	medium	Low
12	working concept	Request/grant	Direct binary data sending.

⊛ Wireless LAN security:

Wired network can be restricted to access by physical means. But it is not so in case of wireless network. So if security breaches result will be hacking of your data, bandwidth and resources. So some security feature are provided in wifi devices using WEP (wired equivalent Privacy) and WPA (Wifi protected Access).

Sometimes additional security is provided using firewall. WLAN users can be authenticated via MAC or Radius MAC authentication and access the corporate system via a VPN tunnel.



⊛ Bluetooth:

Its standard is IEEE 802.15.1. It is a WPAN (Wireless Personal Area Networks).

Bluetooth provides a way to connect and exchange information between devices like PDA (personal digital Assistants), mobile phones, laptops, PCs, printers and digital cameras via a secure globally unlicenced short range radio frequency.

⊛ Bluetooth fundamentals:

Bluetooth wireless technology is a short-range communication technology used to replace cables while maintaining high level of security. key features are:

1) Robustness
2) Low power consumption
3) Low cost.

Bluetooth technology is universal. Bluetooth enabled electronic devices connect and communicate wirelessly through short-range,

adhoc networks known as piconets.

Each device can simultaneously communicate with up to seven other devices within a single Piconet.

Also each device can simultaneous belong to several piconets.

Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave radio proximity.

Bluetooth wireless technology's strength is the ability to simultaneously handle both data and voice transmissions. This enables user to enjoy variety of innovative solutions such as!

1) A hands-free headset for voice calls.
2) Printing and fax capabilities.
3) synchronising PDA, laptop, and mobile phone applications.

(A) Bluetooth Power and Range:

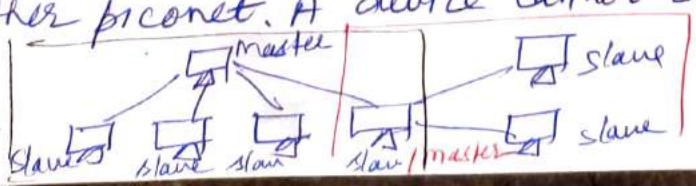
Bluetooth is a radio standard and communications protocols primarily designed for low power consumption, with a short range (1m, 10m, 100m) based on low cost transceiver microchips. devices will communicate when they come in range. They don't have to be in line of sight of each other. The transmission power levels fall in one of the 3-classes -

1) class-1 (100m) in industries - 100mW
2) class-2 (Range 10m) in mobiles - 2.5mW power consume
3) class-3 (Range 1m) - 1mW

(X) Architecture of Bluetooth:

Piconet: It consists of a master node and up to seven active slave nodes with in a distance of 10m and 255 parked nodes. Here slave-slave communication is not possible.

Scatternet: Multiple Piconets combined together to form one scatter net. A slave of a piconet can act as master in other piconet. A device cannot be master in two Piconets

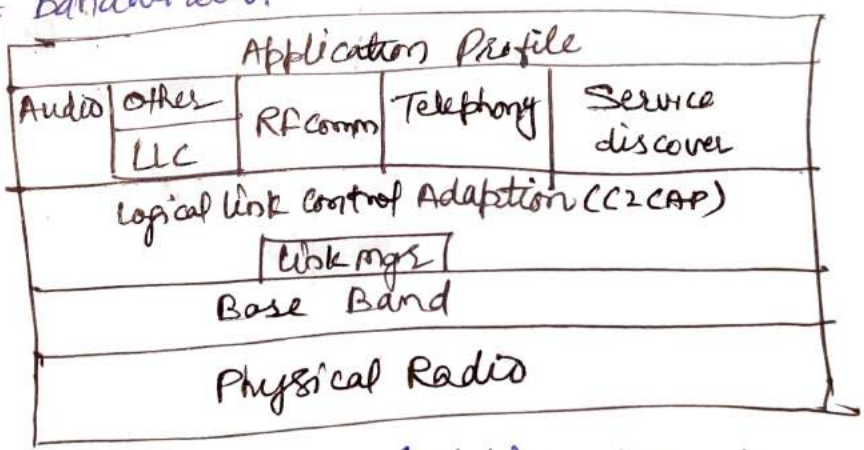


(A) **Bluetooth Applications:** Bluetooth was designed to be used at application level to improve the interoperability. Various applications are -

1) Wireless communications to PC output devices like printers.
2) Wireless networking between PCs in a small space where little bandwidth is required.
3) Wireless communications with PC input devices like Mice and K/board
4) Transfer of files between wireless devices.
5) Transfer of contact details, calender appointments and reminders between devices
6) Replacement of traditional wired serial communications in test equipments, GPS receivers and medical equipment.
7) W: control and comm. between a cell phone and a hands free headset or car kit.
8) For remote controls where infrared was traditionally used.
9) Sending small advertisements from bluetooth enabled advertisement hoarding to other, discoverable, bluetooth devices
10) W. control of a game console.

(*) **Bluetooth Protocol Stack:**

Every bluetooth device containing a radio transmission at rate of 1 mbps with 2.4 GHz bandwidth.



1) **Radio layer:**
It is similar to physical layer. Signals are transmitted through this layer by using very low power. FSK (freq. shift key) is used in modulation.

2) **Base band:**
It turns the raw bits stream to frames and defines some key formats. Each frame is transmitted over a logical channel called link between master and slave. It uses TDMA (Time division multiple Access) method.

③ L2CAP layer: 3-major functions:

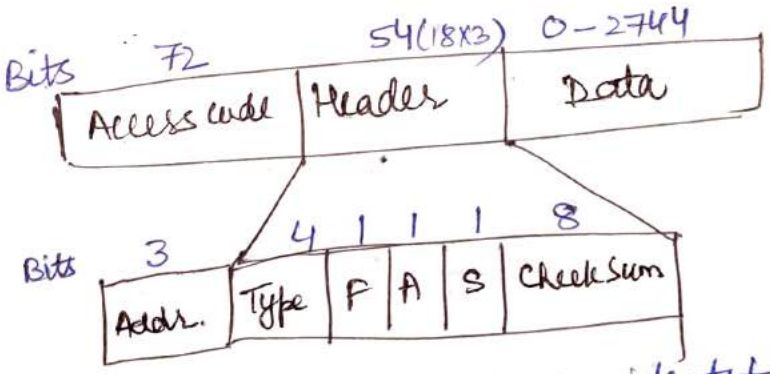
1. It accepts packets of upto 64KB from upper layer and breaks in to frames for transmission.
2. It handles multiplexing and demultiplexing.
3. It handles quality of service requirements both when links are established and during normal operation

④ Types of links between master and slave:

Two types:

1. Asynchronous connectionless: It is used when the correct delivery is preferred over fast delivery. In this, frame is only accepted when it is fully corrected.
2. synchronous connection oriented: For real time data such as telephone connections. This is used when fast delivery is needed. A slave has upto 3 links with its master.

⑤ Frame structure: (bluetooth)



1) Access code: These 72 bits are used to identify masters

2) Header: 54 bit field, it is futher divided into 3-parts, 18 bit each, and it has following subfields-

1) Address: 3-bits - identifies total slaves i.e. 1 to 7. and 0 means broadcast.

2) Type: 4 bits, identifies frame type and type of error correction in data.

3) F (Flow bit): it is 1 if slave is full buffer.

4) A (Acknowledge): it is used for Acknowledgement in piggybacking method.

5) S (sequence): it is used to number the frames to detect retransmissions.

6) Checksum: it is used to detect errors in header section.

3) Data: variable length field ranging from 0 to 2744 bits that contains data or control information from upper layer.

(*) Difference in bluetooth and wifi:

Bluetooth	wifi
1) Bandwidth is low.	1) Bandwidth is high
2) Simple to use and switching between devices is easier.	2) It is a little more complex.
3) max. range is 10m	3) max. range is 100m.
4) It is less secure	4) It has high security features
5) Power consumption is low.	5) P High
6) Freq. Range 2.4 GHz to 2.483 GHz	6) 2.4 GHz and 5 GHz (5.8)
7) Supports limited number of users.	7) Supports large nos.
8) Modulation Tech – GFSK (Gaussian Freq. shift keying)	8) OFDM – orthogonal freq. div. multiplexing. QAM – Quadrature Amplitude Mod.

(*) Lisbon: It is the new version of bluetooth. Its features are: 1) Atomic encryption change
2) extended enquiry response
3) sniff sub-rating
4) improvement in quality of service
5) simple pairing.