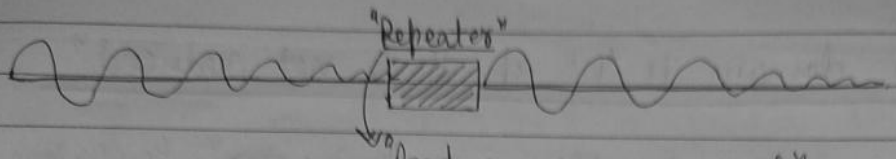
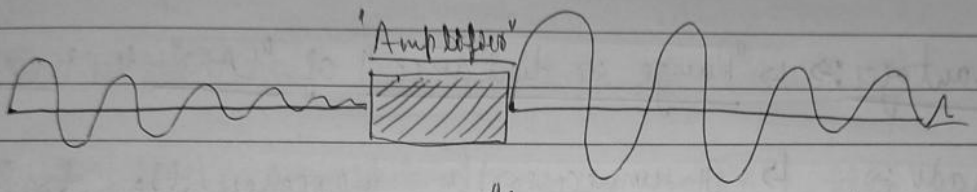
"Amplifiers & Repeaters are different".

PAGE No.
DATE : / 201

▷ "Repeater" :→ It will take a dying signal from one end & produce exactly the same signal at the other end.

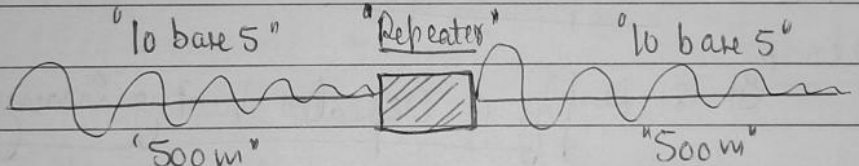




"Increases amplitude of a signal".

"Advantages of Repeater" :→

↳ We can increase "length of a LAN".



Total length of LAN = "1 KM".

Note:→ [Any thing less than "10 KM" is "LAN". Any thing less than "100 KM" is "MAN"; beyond "100 KM" we have "WAN".] Imp

"Repeater" knows nothing about "Sender & Receiver" it simply puts the "signal" on the other side.

Used to connect two "LAN-segments" & both "LAN-segments" should be of same type. (We cannot connect an "ethernet" with "Token ring".)

P.T.O.

:→ "Repeater" works at "Physical layer"

:→ "Collision" are possible at "Repeater".

:→ "Collision domain is "n" if it is not reduced"

Note:→ By placing a "repeater", "collision domain" remains unaffected.

Advantage:→ ↳ "Range or distance" of "LAN" is increased.

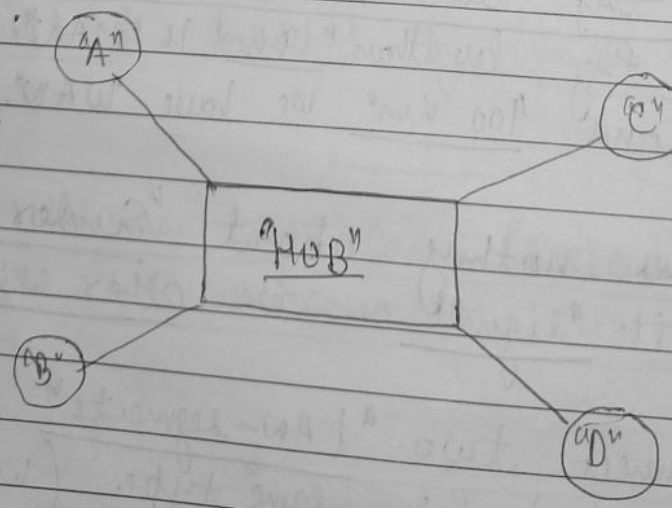
Disadv:→ ↳ It unnecessarily increases the traffic.

"Repeaters" were used long back, Now they are replaced with HUBS.

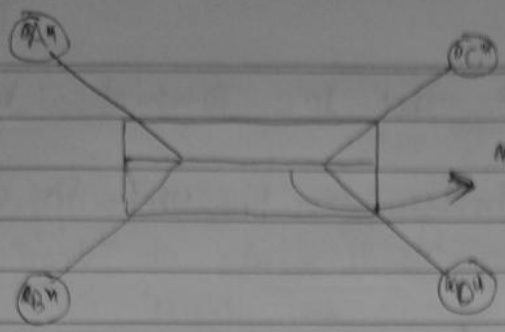
⇒ "Hubs" :→ It is a "multiport Repeater"

"It is simply a repeater having many ports".

For example, if we have a "four port HUB", we can connect stations as shown below:→



Externally there is only "one-channel" & all other stations are connected to this "channel".



Now, if "A" wants to send a message to "B", "A" will put the message on the channel, then message then be seen by each & every "station" connected to the Hub.

This is the main disadvantage of "Hub".

If "B" wants to send a message to "A", then everyone will get this message.

"Points about Hub" :=>

1> Traffic is very high.

2> It is having only physical layer. (This is the reason behind "broadcasting the message")

3> "Collision" are possible "inside Hub".

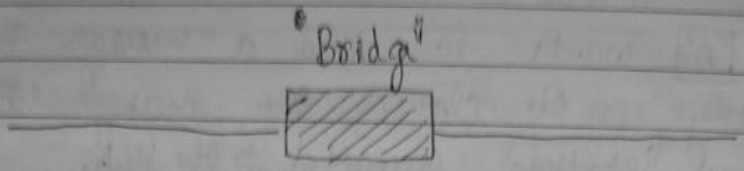
4> "Collision-domain" is "n". (All the "n-stations" connected to "HUB" are involved in collision)

"Bridge" :=> "Bridge" is a device used to connect "two LANs"

There is a difference between a "repeater" & a "bridge" & the difference is

"Repeater" is used to connect two "LAN segments" of the same type.

But "Bridge" can be used to connect too different "LAN-segments" i.e a bridge can be used to connect "ethernet" with "Token-ring"



"two diff. LAN-segments".

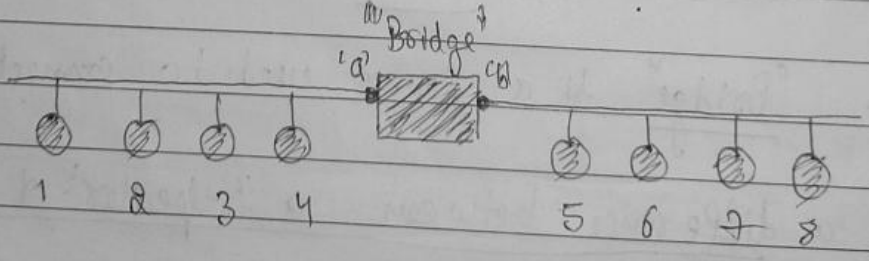
"Some important points about "bridge" :->

1> "Bridge" works both at "Physical layer" as well as "Data Link layer."

Hence "bridge" contains both "Physical-layer" as well as "Data link layer".

if "bridge" works at "DLL" then it can find out / detect "MAC addresses" of stations connected to it & hence it can take many important decisions.

Let us assume that a "bridge" is having "two ports" hence we can connect two "lan-segments" with it as shown below :-



Let "a" & "b" be port nos. & these numbers on the stations, assume them to be "MAC-addresses".

mapping table

"Bridge" will have a "~~Mapping-table~~" or a "forwarding-table"

mapping table

This "Mapping table" contains "MAC-address" of the "station" & the "port" to which it is "connected".

"Mapping-Table"

"MAC"	"Port"
"1"	"a"
"2"	"a"
"3"	"a"
"4"	"a"
"5"	"b"
"6"	"b"
"7"	"b"
"8"	"b"

If we want to send a packet to "3" station, bridge will send it to "port a".

There are two ways to construct the "Mapping table" at "bridge" :>

1> "Static Method" → Here we will manually write the "entries" in the "mapping table".

But the problem with this method is whenever a "MAC" Address of any "station" changes. ("MAC-add" of a "station" changes, when "NIC gets corrupted").

Now in Case if "MAC add." of any "station" changes, then we have to manually update it in the "Mapping-table".

& also whenever we want to move a "station" from "one LAN" to other. Again we have to manually update the "port numbers" in the "Mapping-Table"

P.T.O

So "manual intervention" is required, hence it is not a good option.

"2nd Method" is "Dynamic bridges"
or
Learning bridges or Transperant bridges

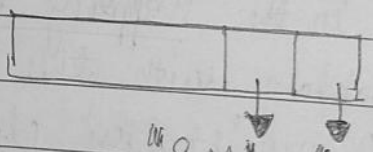
They are better than "static bridges" because we need not "manually configure this "mapping-table".

But it will take some time to construct this "mapping table".

Since "bridges" have both "Physical layer" as well as "data link layer".

So, "frames" are inspected at both there "layers".

a "frame" consists of both "source Mac-add" & "Destination Mac-address".



"Properties":->

1> Bridges are capable of "filtering the packets" Eg. If ① sends a packet to ③ & "bridge" knows that both of them are in the same LAN then it will not forward the packet to 2nd "LAN".

2> "Bridges" can also do "forwarding".

3> let us assume that a new station "9" is added to the "LAN segment" & it has not yet been identified by the bridge & if it entry is not present in the 'mapping Table'.

Then "bridge" will do "flooding of the message"

Note :> So "bridges" are capable of "filtering", "forwarding" as well as "flooding".

Note:> These capabilities of "filtering & forwarding" are present only in the "devices" which are having "data link layer in them".

4> "Bridges" are having the capacity of "store & forward".

So, a "bridge" can accept a "packet" intended for a "station", store it and then forward it.

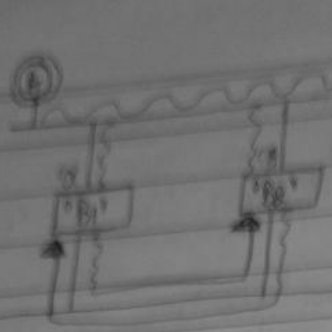
∴ there are "no collisions" inside the "bridge".

It means inside a "bridge" if "two packets" are coming from "two LANs" then both the "packets" will be present in the "bridge" without any collision.

Hence "Collision domain" is "reduced". Now collision can occur only in "one" LAN segment".

"Disadvantages of Bridges" :> Let us assume that, we are "connecting two "LAN segments"" using two bridges".

P.T.O

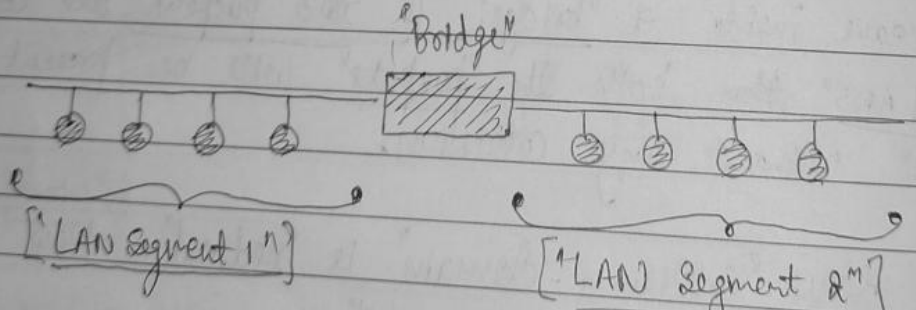


Suppose (A) wants to send a packet to (B), the packet would be forwarded to ["B1" & "B2"] & hence it will fall in an "infinite Loop".

Now in order to avoid the "packet" to fall into an "infinite loop", we use ["spanning-Tree"].

One more "problem" with "bridges" is that, theoretically we can use "bridges" to connect different type of "LANS".

But the problem with this is if ["MTU"] of both the "LANS are 'different".

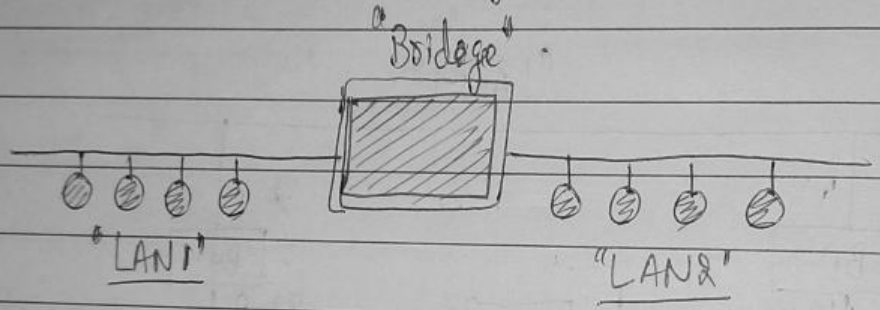


Now, suppose "LAN-seg 1" sends a "packet" to "LAN-segment 2", then bridge should be able to fragment this packet into "various 'fragments' of size "1000"

"Switch" ⇒ It is a "device".

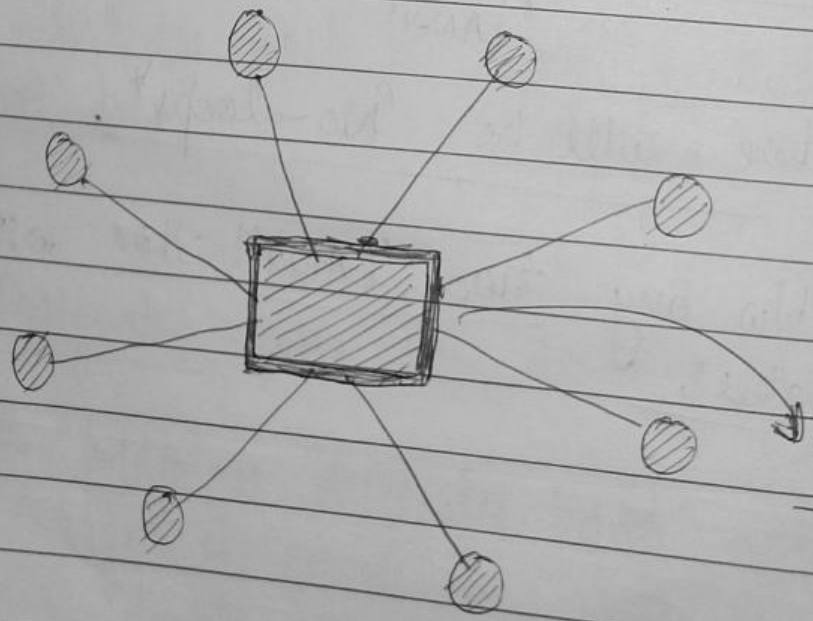
Till "1995" "bridges" were very popular, & people used to connect different "LANs" using "bridges".

Generally "bridges" are having "two ports" only and they are usually used for "connecting two "LAN segments".



Later "Capacity of the bridge" is increased in such a way that, bridges will have "lots of ports" connected to them, & instead of connecting a "LAN" to every port, we are directly connecting a "host/computer" to them.

"ports are sockets"



"This is a "switch"

"Switch" is a device which is basically an "extension" to the "Bridge"
& the main difference is actually in the "number of ports".

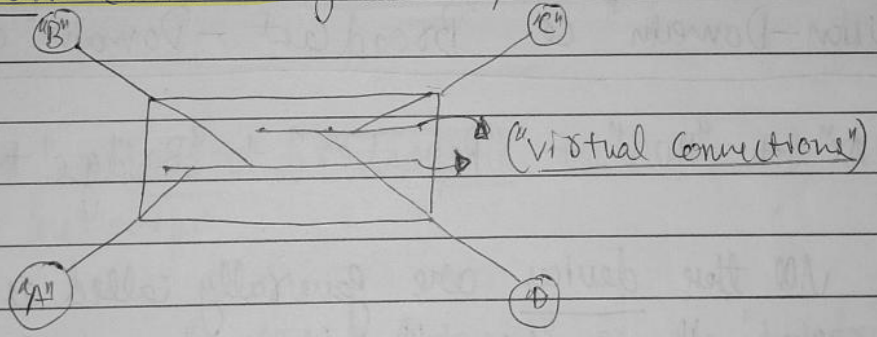
So, we can have either an "8 port switch", or "16 port" or "32 port", "64 port" switch.

"Some points about switch" :->

1> It contains both "Physical layer" & "DLL" "Data link layer".

∴ It can look into "MAC" addresses & is able to send "packets appropriately".

2> At a same time, more than "one communication" can happen using "switch". (without any collision).



Suppose "A" wants to send a message to "B" then a virtual connection is established & control/access is given to both "A" & "B"
Now at the same time.
Suppose "C" & "D" also want to communicate, so again a "virtual connection" is established & control/access is given to "C" & "D"

3> The links connecting "switch" to the "stations" are "full duplex links".

P.T.O.

"Switch" is highly efficient compared to "other devices" in the sense that "Collision cannot happen".

& "bandwidth is very very high"

⇒ "Collision domain is reduced to zero"

⇒ "MAC addresses" can be seen by a "switch" & appropriate messages are sent to "required host" efficiently.

⇒ "Traffic" is less compared to a "HUB".

"Disadvantages":⇒

↳ It is costly.

⇒ "Collision-Domain" & "Broadcast-Domain" of all Devices":-

"Wire" + "Hub" + "Repeater" + "Bridge" + "Switch"

All these devices are generally called as "LAN Components" beoz. even if we use all these devices the result will always be a "single-Network" or a "single-LAN".

Using all these "devices" the "Network" we obtain cannot be called as "an Internet".

According to the "rules of Networking" every broadcasting which is done within a Network at "Data link Layer" should be seen by everyone in the Network.

∴ "Bridge" & "Switch" should not stop any broadcast packets

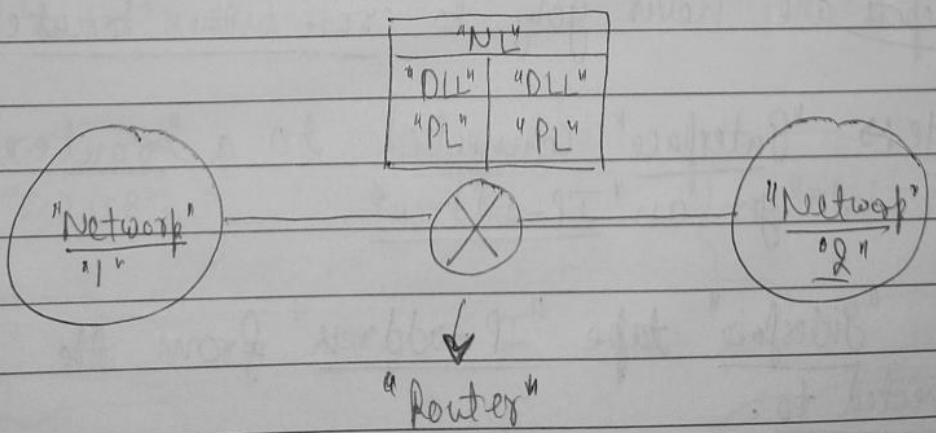
So, all these devices should not reduce the "broadcast domain".

i.e ("broadcast msg" has to be seen by everyone in the "network")

"Device"	"Broadcast-domain"	"Collision-Domain"
"Repeater"	"Same"	"Same"
"Hub"	"Same"	"Same"
"Bridge"	"Same"	"Reducer"
"Switch"	"Same"	"Reducer" infact it is "zero"
"Router"	"Reducer/decrease"	"Reducer"
"Gateway"	"Reducer"	"Reducer"

⇨ "Router" :⇒ A "router" is a "device" which is used to connect two "networks"

Note :⇒ We cannot call a "network" as an "internet" until we have "routers" included.



Router is having "PL", DLL & NL" & for every interface, it is having individual "PL" & "DLL".

P.T.O

["DLL" cannot do "fragmentation".]

We are having different "DLL" & "PL" because on one side of router or on one interface we having a different "protocol" working/running on "DLL" & on other side of the "router" we are having a different protocol running at "DLL"

∴ "Communication" ——— ∘
↳ will be easy.

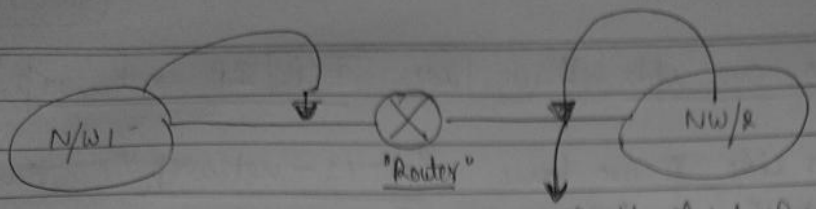
Since "Routers" work at "NL" ∴ "Routers" are capable of seeing both "MAC addresses" as well as "IP-addresses" & can take appropriate decisions.

Various decisions taken by Routers are :⇒

1) "Forwarding".
2) "Filtering" (Eg. "ARP packet," it is never send across a router, RARP, DHCP, Bootp all are filtered)
3) "Flooding" / "Routing"
4) No collisions inside a "router".
5) "Broadcasting domain" is also reduced because "broadcast packets" are never going to cross the "routers".

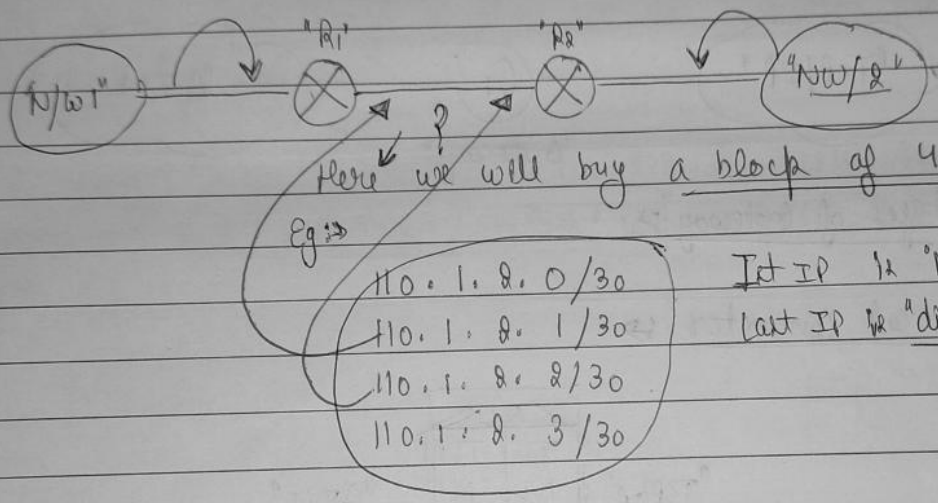
Note :⇒ "Interface" connected to a "routers" are going to get an "IP-address"

"Interface" take "IP-address" from the "network" it is connected to.



IP add of interface is taken from the N/w itself

If the "configuration" is like as shown below :-



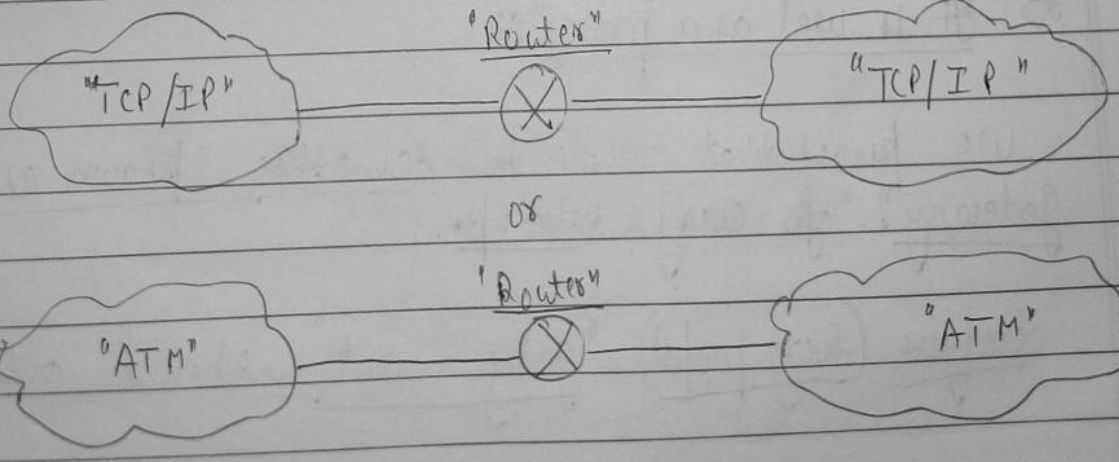
Here we will buy a block of 4 "IP address"

Eg :-

110.1.8.0/30
110.1.8.1/30
110.1.8.2/30
110.1.8.3/30

1st IP is "N/w Id"
Last IP is "directed broad cast address"

"Gateways" :- Main difference b/w "Gateway" & "Router" is if we have a "Network" & if we want to connect it with some other network, "Router" is used.

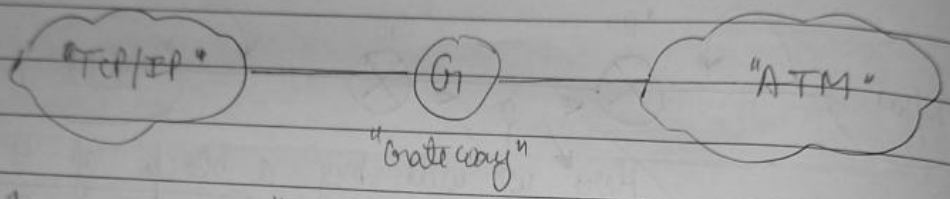


PT.O

Now on one side if we have "TCP/IP network" &

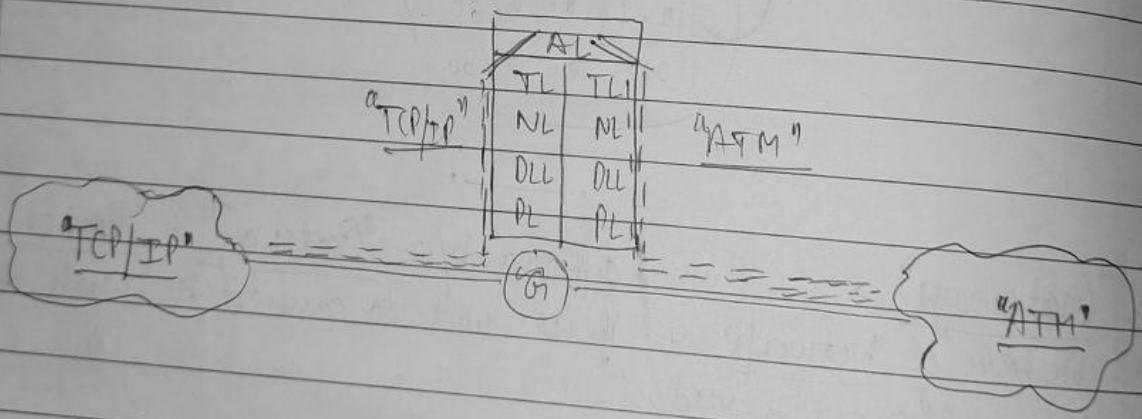
on other side if we have "ATM-network" then in between "Routers" will fail to provide connection b/w them. bcoz we have "diff-protocols" working at "Network layer" for "diff type of networks"

∴ In such cases "Gateways are used" to provide connections.



"Advantages of Gateway" :⇒

1> "Protocol convertor" :⇒

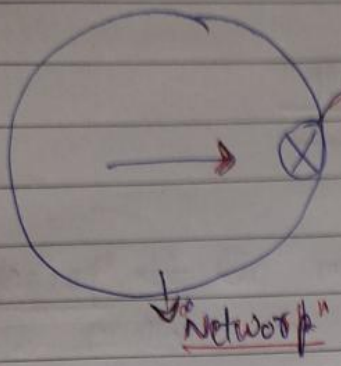


2> "It is used as a proxy" :⇒

We know that there is something known as "default-Gateway" for every networks.

Everyone (Every packet) "going out" should only go through

the "proxy" to the "outside internet".



[Now if we want to go out, we should go out through "proxy" only.]

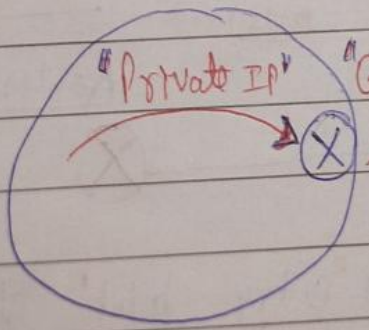
The adv. of the proxy is that, we can "monitor" every "single byte" we are sending out.

In many "organizations" & "educational-institutions" there is a restriction that no "user/student" use more than "2 GB of data" per week.

It means we want to count out how much amount of data every student used per week.

"Proxies will monitor everything going out."

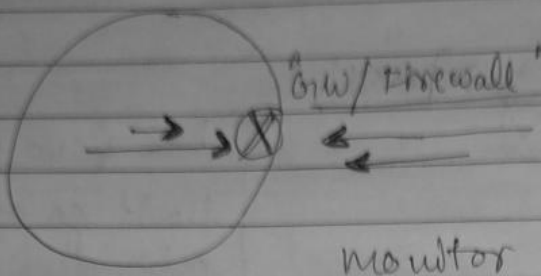
3> It can also be used as a "NAT Server". (Network Address Translation) :→ It is used to conserve the IP's



PTO

4) "It acts as a firewall"

Eg :- "Telnet can be blocked"



monitor all the "packets" going outside the network as well as those coming inside a network.

---

5) It can also be used for "DPI" ("Deep Packet Inspection")

Since "gateway" has all the "layers", it can look into "application layer data" also.

Eg:- "Many colleges" do not allow "videos" to be streamed during daytime.
