EC357

ADHOC AND SENSOR NETWORKS

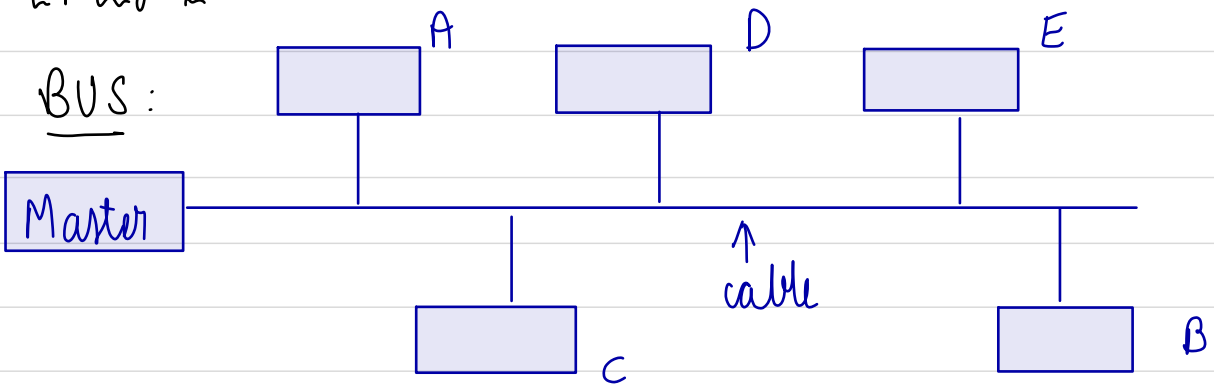
M MANVITH PRABHU 211EC228

ADHOC

Inter µP distance	Location of µP	Example
0.1 m	circuit board	Data flow in machine
1 m	System	Multi computer
10 m	Room	LAN
100 m	Building	LAN
1 km	Campus	LAN
10 km	city	MAN
100 km	country	WAN
1000 km	continent	WAN
10000 km	Planet	Internet

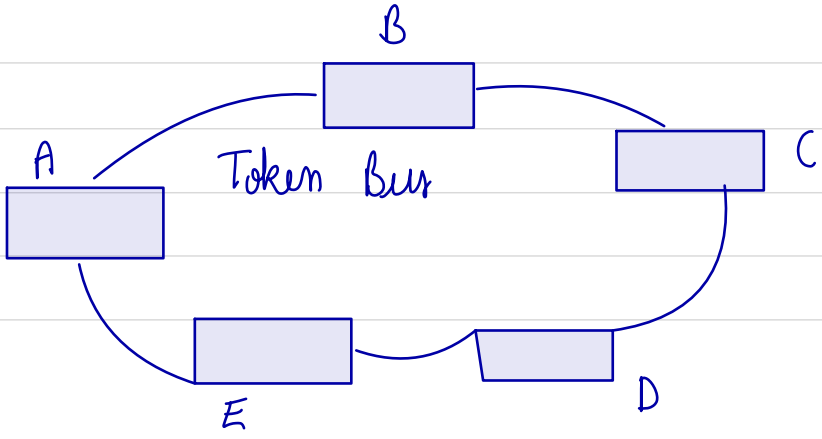
Topologies:

1) BUS:



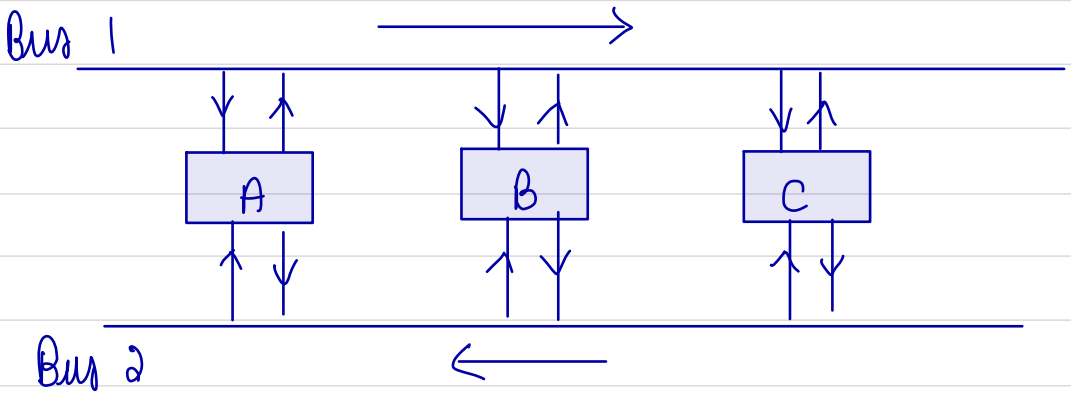
IEEE 802.3 (Ethernet) : 10 to 100 Mbps

2) Ring:

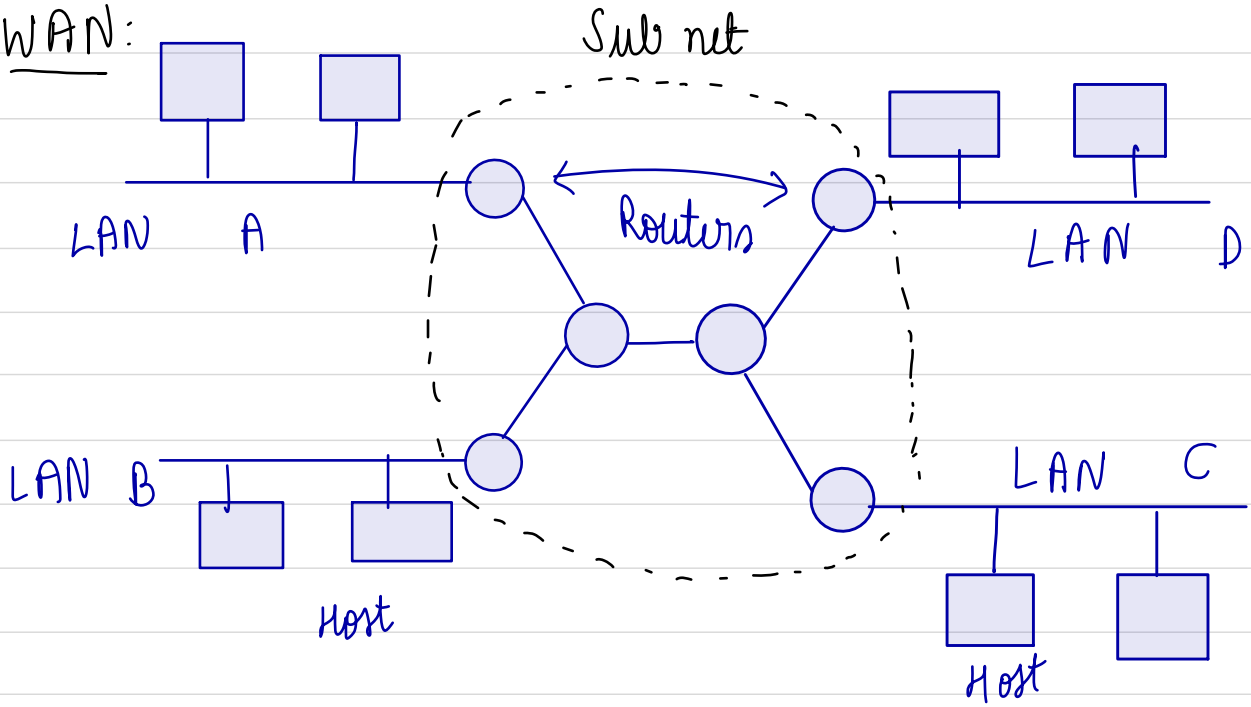


Token Bus is used to request for the permission to use data.

3> Distributed queue dual bus : DQDB



4> WAN:



LAN: • Several machines are connected to a bus and one of them acts as bus and others as slave.
• The master arbitrates use of bus.
• Arbitration is necessary when 2 machines try to transmit simultaneously.

- IEEE 802.3 is the standard used with a speed of 10 - 100 Mbps.
- If 2 or more than 2 packets, collide the sender of the sending machine may have to wait for random time before it re-transmits.

RING:

- In the topology, there is end to end connection for the bus.
- Machines are connected to this ring and are identified by some kind of address.
- A byte propagates through ring called token & token holder is authorised to use the ring.
- After completion a token passed on to the neighbours.
- IEEE 802.5 is the standard used here.
- The speeds range from 4 - 16 Mbps.

DQBD

- This standard is IEEE 802.6. Here there are 2 unidirectional bus, where the data flows in 2 different directions.
- All machines are connected to these 2 bus.

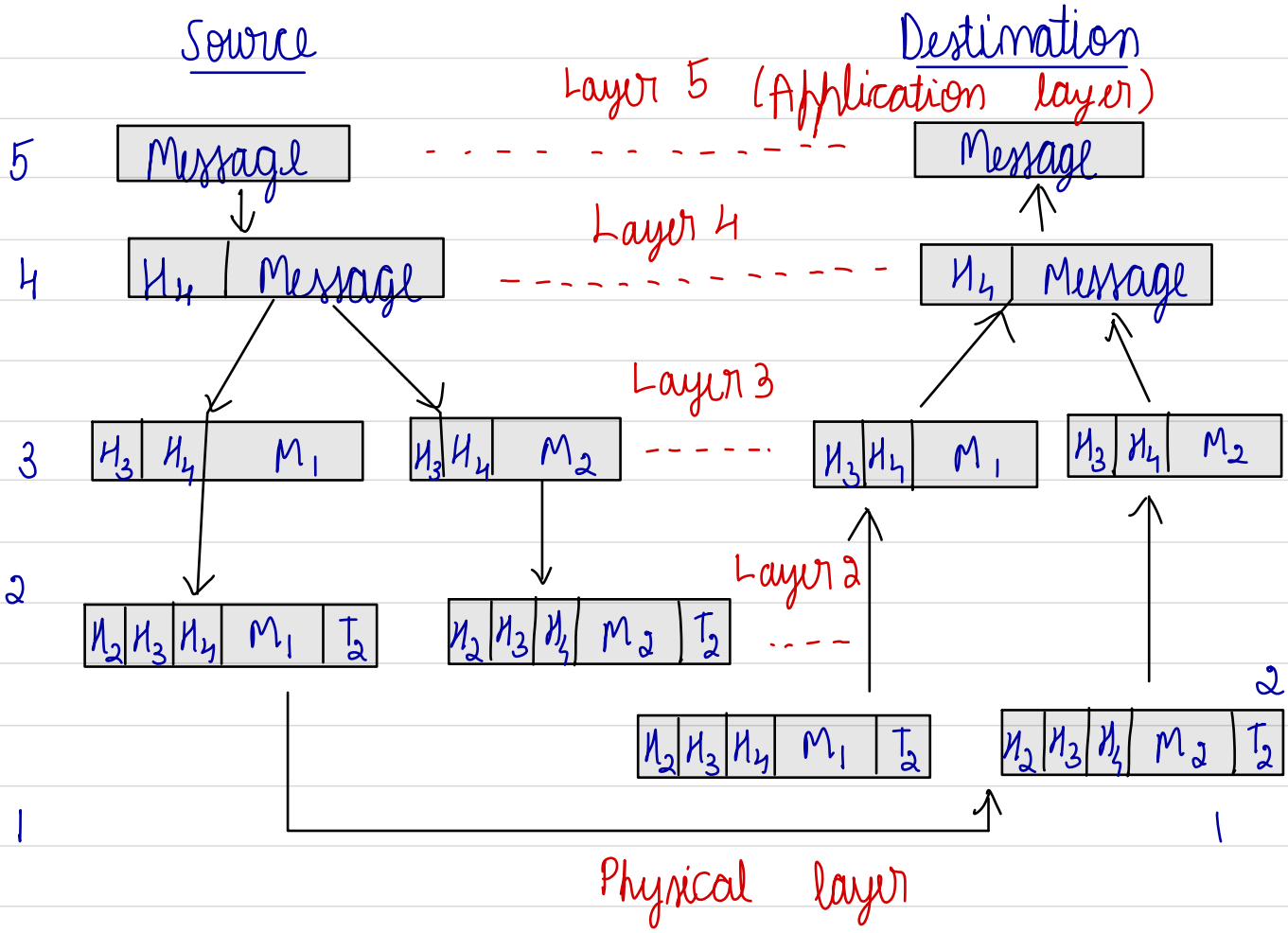
WAN: - It is a connection of several LANs.

- LANs are connected to routers. And the routers are connected to other routers.
- Routers form subnet.
- There could be more than 1 LAN connected to a router.
- WAN encompasses a large geographical area.

Internet:

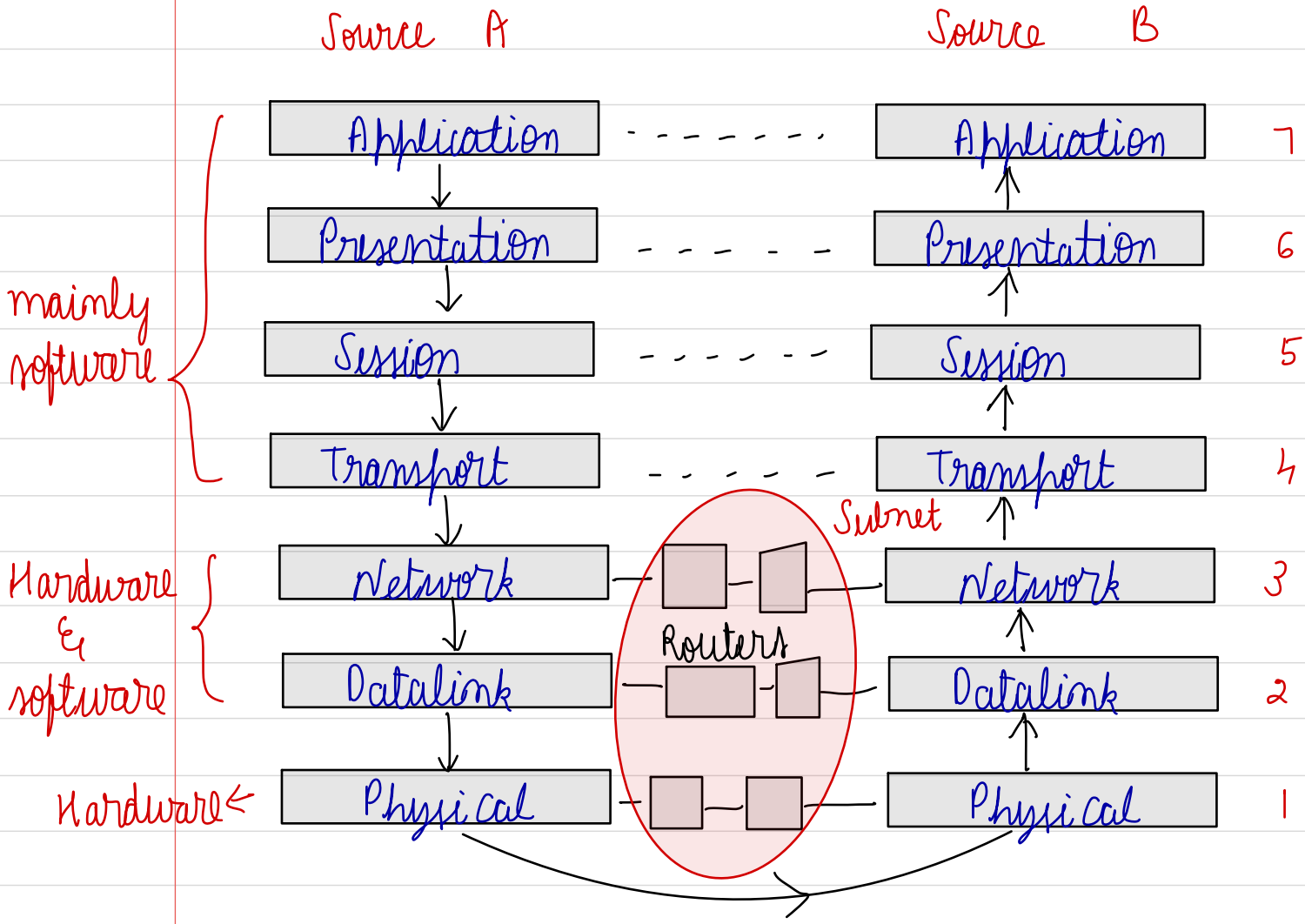
- It is a collection of WAN.
- It spreads across whole globe.

Protocol hierarchies



- A Message M is produced at the layer 5 which is the application layer and is the man machine interface.
- At layer 4, a header gets added to this message which has the destination address, control information, sequence information and other data.
- At layer 3 message is considered to be too long at split into several chunks and its own header, for eg: H3 is added.
- At layer 2 additional headers and trailers are added to prepare the message, so that they confirm to physical standard
- At layer 1 the actual physical transmission takes place via metal, fibre, wireless medium.
- On the return path, the header and trailer are removed one by one as the message proceeds through different layers.
- Finally message is reassembled such that it is meaningful and is submitted to application layer for man machine interface.

ISO - OSI Reference model



Principles applied to arrive at 7 layer model

→ Layers are needed when abstraction exists.
→ Each layer should perform well defined tasks.
→ Design of any layer should be such that it is globally accepted.
→ The layer boundary should be chosen such that it minimises information flow across interfaces.
→ The no. of layers should be optimally

chosen such that the functions are optimally achieved.

1) Physical layer: → It is a real life layer which is mainly used for man-machine interface.
→ It is concerned with sending raw bits so that a binary one should reach it's destination as binary one and not as binary zero.
→ Limits of voltages for binary 1's & 0's are standardised at this layer.
→ Issues like simultaneous communication, synchronization, simplex & duplex are handled here.
→ The no. of pins / wires, range of frequencies, type of modulation, encoding etc are some of the issues.

2) Data link layer
→ It takes in raw message from physical layer and detects error before sending it to next layer.
→ If the data has errors decisions like re-transmitting is dealt here
→ Traffic regulation to handle communication between slow & fast machine is sorted out here.

3) Network layer: The operations of subnet are controlled here.

→ Design issues include routing of packets.
→ Congestion control is handled here by storing extra data to be transmitted at a later time.
→ Since routers are the gateways, it is ideal to keep log of the data flow and hence accounting and building
→ Addressing issues are dealt with in this layer. However in a broadcast network the network layer maybe redundant.

4> Transport layer:
→ Large messages cannot be sent as it is and hence they need splitting into smaller messages, done at this layer.
→ Distinct connections between 2 machines is established here depending upon type of traffic.
→ It is called a true end to end layer since the source machine talks to distination machine and vice versa.
→ Connections are established & broken down as and when necessary.

5> Session layer:
→ It deals with token management, generation & passing of tokens to neighbours & recieving from neighbours is handled here.
→ Issues like synchronization to provide a

checkpoint in data stream is handled, so that unnessecory. Retransmission can be avoided.

6> Presentation layer:

→ It is concerned with syntax & semantics.
→ Encoding & decoding of data in a standard agreed upon way happens here.
Eg: ASCII, unicode, 1's compliment etc.

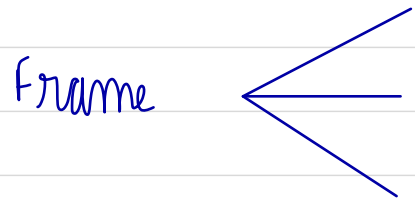
7> Application layer:

→ Contains variety of protocols to convert the output of presentation layer to user understandable pattern or mode.

Abbreviations

TCP = Transmission control protocol
IP = Internet protocol
UDP = User datagram protocol
TELNET = distant log in
FTP = File transfer protocol.
DNS = Domain name system.
HTTP = hyper text transfer protocol
MAC = Medium access control.

Data link layer



1> **Unacknowledged connectionless service:**
- Source sends frames to distination without waiting for acknowledgement.
- No connection is established.
- It is suitable for low error less noisy and real time applications like voice.

2> **Acknowledged connectionless service:**
- Each frame is acknowledged.
- If acknowledgement is not recieved within a specified, data is retransmitted.
- On a wired network this could be a burden but on a wireless network it is worth the cost, since wireless connections are not reliable

3> **Acknowledged connection oriented service:**
- The soure & distination establish a connection.
- Data of frames are number and then sent.
- Hence it is to identify loss of frames.

- At the end of communication, the connection is released.

Framing:

character count
Start and end with character stuffing
Start -11--11- with bit stuffing
Physical layer violation

CC

frame1 5 char 8 char 3 char
5 char

CS DLE 57X
DLE ETX
1100 1100 1

BS 0111 1110

a> 011 0111 1 1111 1111 1111 1 1 1 1111 0010
b> 011 011 1 1 1 10 11111 0 .....
↑ ↑
Stepped bits

PLV: Framing is essential when sending data in binary form. There as various methods of framming, to name a few:

1> Character count: A field in the header specifies number of characters. In this method, problem the header is in error.

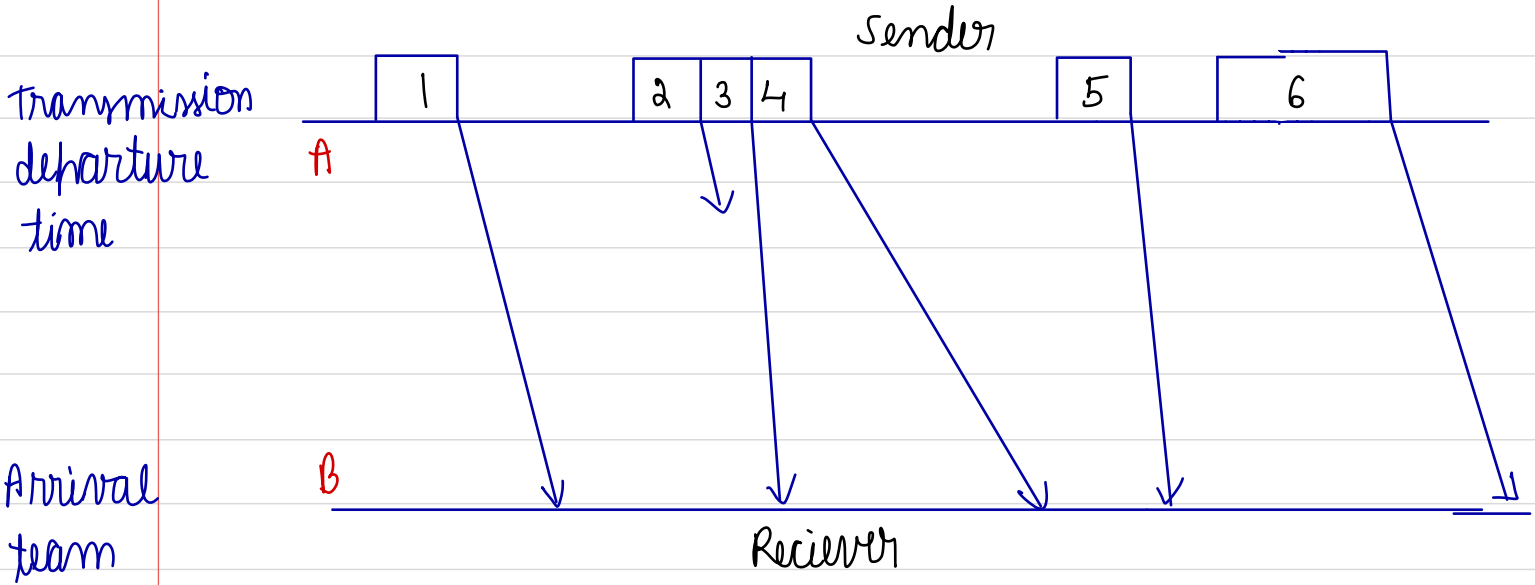
2> Character stuffing:
Starting and ending with character stuffing. The message starts and ends with ASCII characters like DLE STX & DLE ETX.
STX - Start of text
ETX - End of text,
Here while sending object program / floating point numbers the ASCII characters maybe present as data. Therfore the destination machine gets confused. However it is an 8 bit character code. Hence cannot accomodate arbitary sizes dataframe.

3> Bit stuffing:
Bits each frame begins & ends with a special bit pattern 01111110.
Here if there are more than 5 consecutive 1s in the data being sent, then a 0 is stuffed after 5 1s.
The flag pattern or bit pattern is not used as data. However of reciever looses track it searches for this pattern as flag.

4> Physical layer violation: This is applied in LAN. 1 maybe encoded using 2 physical ends.

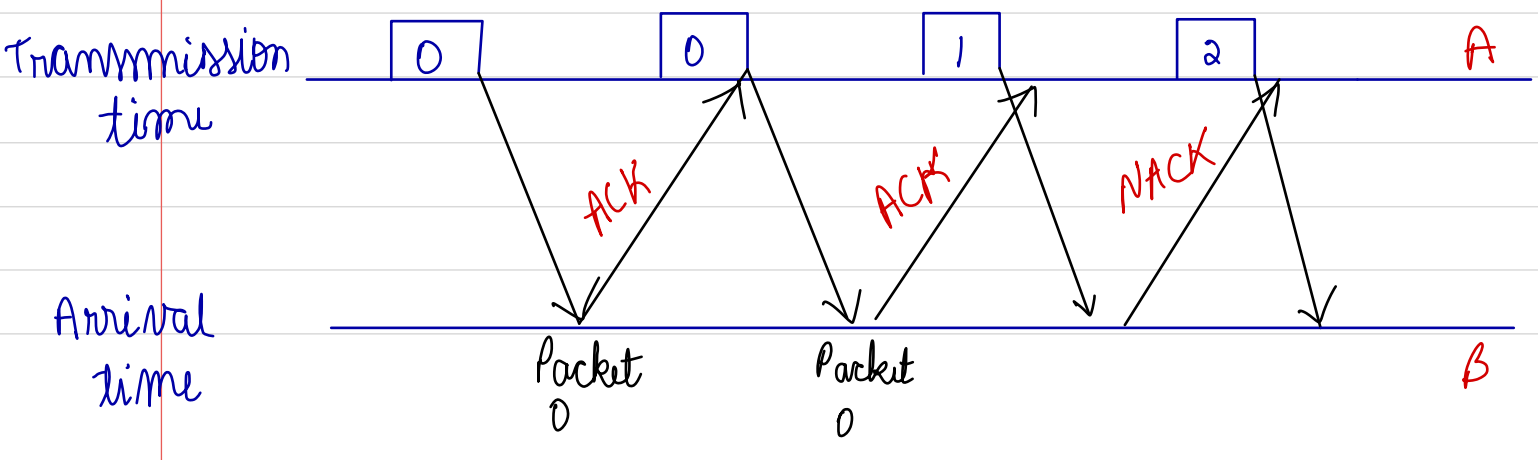
A binary one may be represented as a high high and zero may be represented as a low low, instead of a high low and low high pair.

Automated repeat request: (ARQ)



In the above example frame 2 is lost & never arrives. Frame 4 contains errors. Frames have variable transmission delay. But those that arrive do so in the order they are transmitted or sent.

STOP & WAIT ARQ

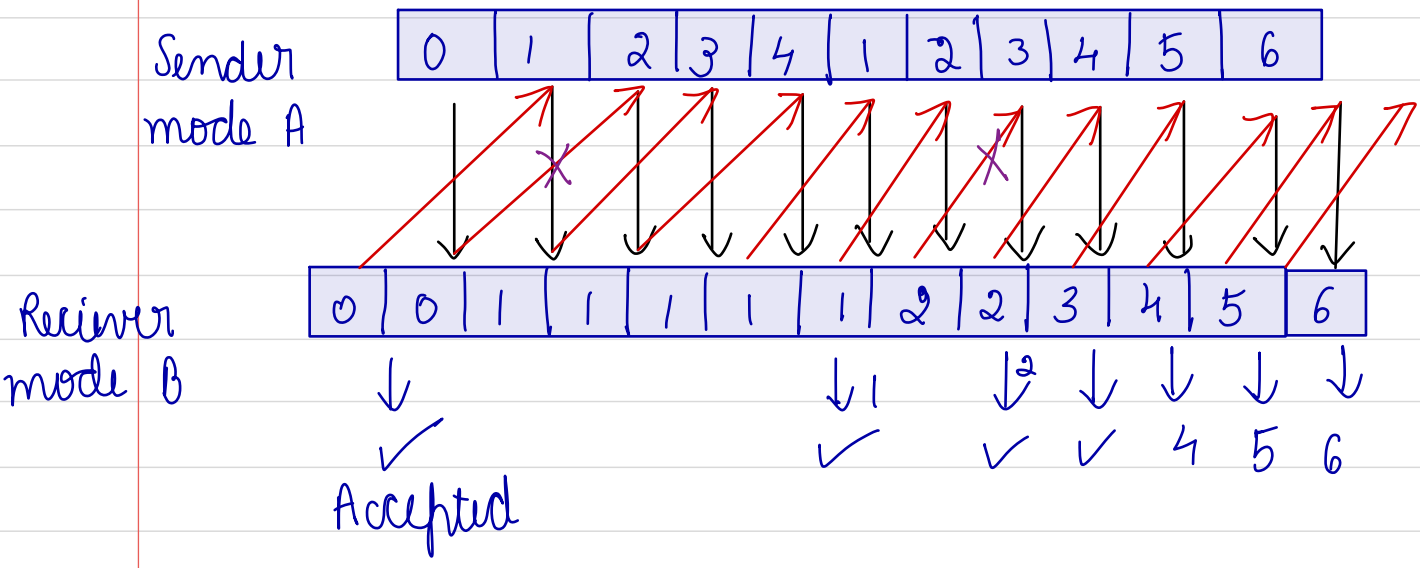


- The basic idea is to ensure that each packet is recieved correctly before sending next packet.
- A packet is transmitted and sending data link control waits
- If packet is recieved correctly at B, then B sends acknowledgement to A.
- If packet is recieved in error, then B sends a nack (no acknowledgement) to A.
- If acknowledgement of B at A is correct, then A will send next packet.
- Acknowledgement of B at A is delayed or in error then A retransmits same packet.
- If B recieves packet twice, it cannot detect whether it is a new or old packet which is retransmitted.
- The solution is Numbering these packets
- To avoid this B sends the number of the next packet awaited, which itself is an acknowledgement of previous packet. However the sender's sequence number SN and recievers request number RN is quite large as time progresses. Therefore the modulo 2 method of numbering is sometimes employed.

00 - initially first packet is recieved error free.
01 - Packet recieved at B error free
11 - A recieves requestor B's request
10 - B recieves packet from A.
00 - A recieves requestor B's request

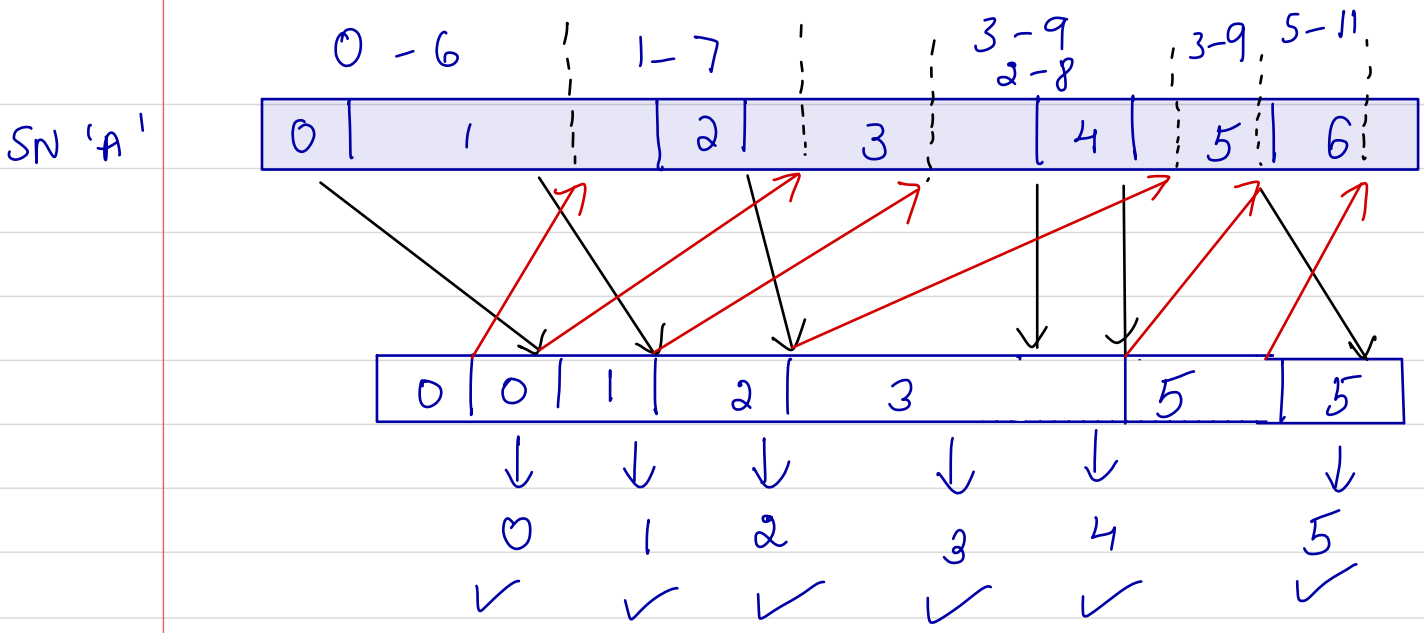
Go back (N) ARQ -

Go back N packets & retransmit those N packets



Go back 'dN' is a parameter that determines how many successive packets can be sent if i is not acknowledge
∴ go back N ARQ is called a sliding window protocol.

Go back 7 ARQ

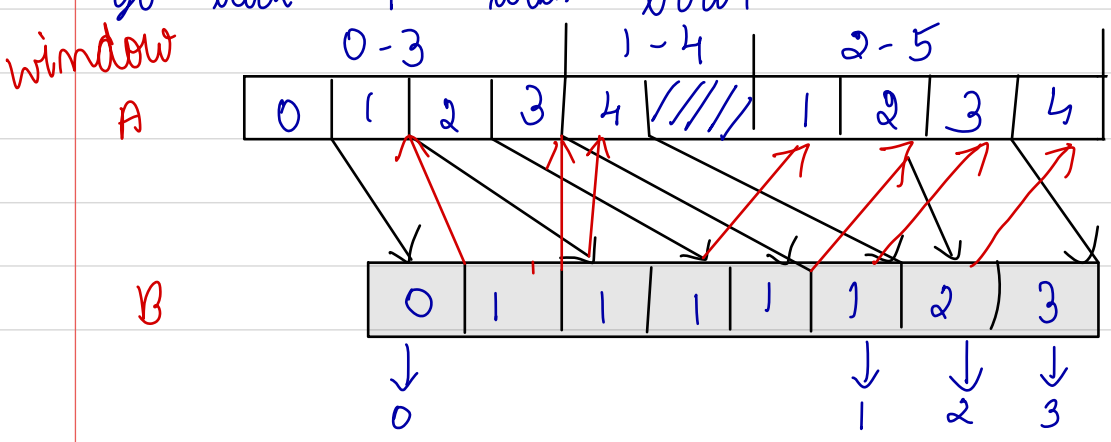


In go back 7 ARQ when I st francis 0 from A is recieved @ B is requesting for 0 again. Frame 1 is requested in 3rd slot slides from [0, 6] to [1, 7]. There it is allowed to send 7 packets at a time even if the acknowledgement are not recieved. There could be several types of errors

a> Text time error
b> prop delay error
c> waiting time error

when pack 3, 4 both recieved at B, B sends $R_N = 5$, to acknowledge with 3, 4

Go back 4 with error

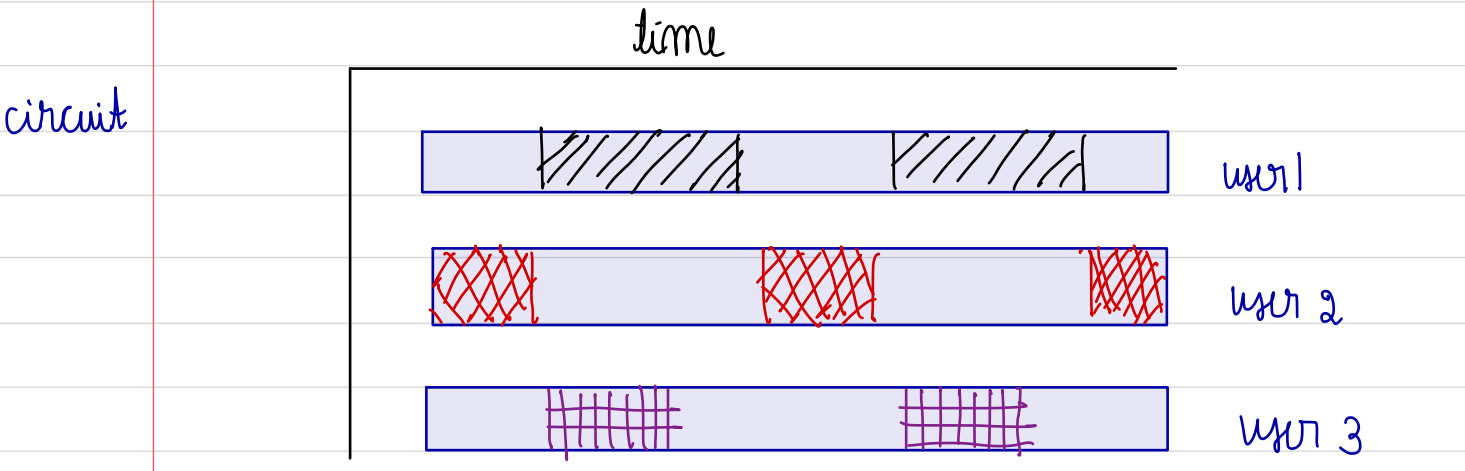


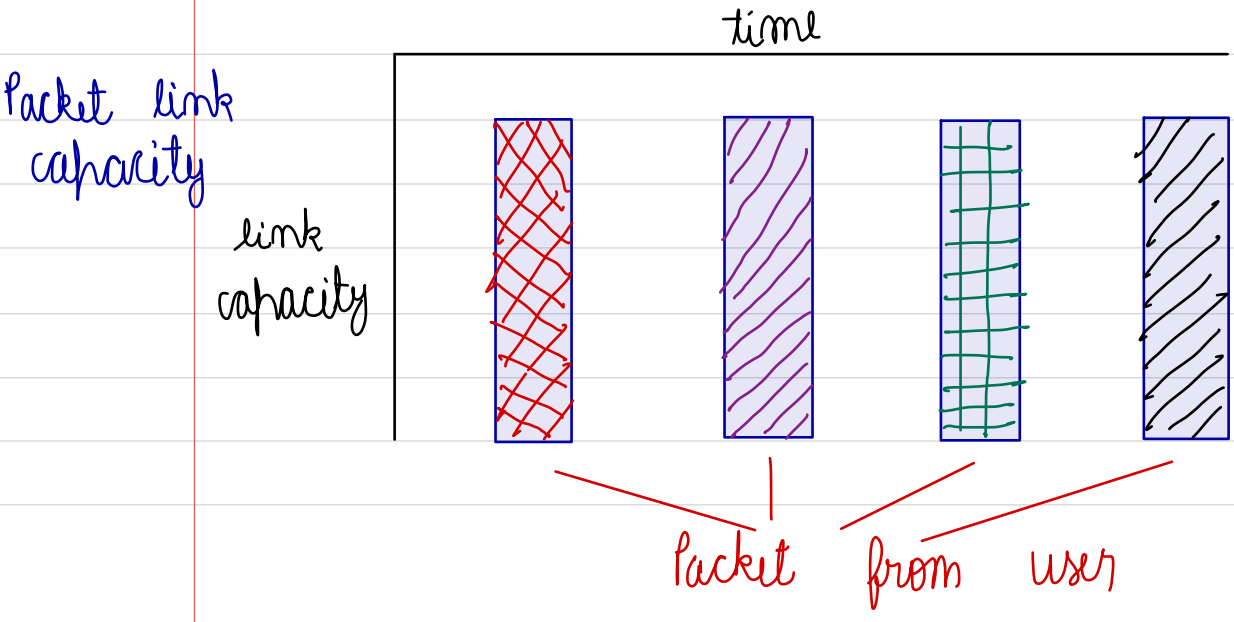
2nd frame in err, Node B looks for pack 1 & therefore $R_N = 1$ is sent repeatedly. However packet 2, 3, 4 are received error free but not accepted. 2, 3, 4, can be @ B. This techniques is called selective repeat request (SRQ). Node A re-tent pack 1. After the (1, 4) window is exhausted and after a time out.

Functional elements

1> Multiplexing

circuit
Packet link capacity





- Systematically merging several flows into a network is called multiplexing. It can be broadly classified into 2 types: circuit multiplexing & packet multiplexing

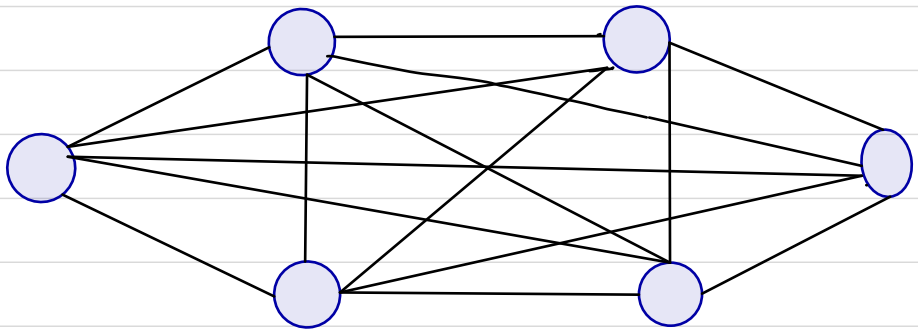
- In circuit multiplexing, allocations are partition as shown in 1st figure. In this multiplexing, the flow is determined by the number of channels. The link rates and channel rates confirm to some standards For eg: 30 channels of 64 kbps which totals to 1.92 Mbps per user of data. However the raw data could be more of 2.048 Mbps.

- In packet multiplexing the entire bitrate of the link is available to a user. Hence the burst of data is time interleaved into the link as shown in 2nd figure. Packet multiplexing has shorter bursts. Average data rate is less. But the peak data rate is high. Therefore, Queueing, delay and data loss might occur. Header and trailer is a must in packet transmission

- While measuring a packet multiplexer, delay & loss are the parameters that have to be measured.

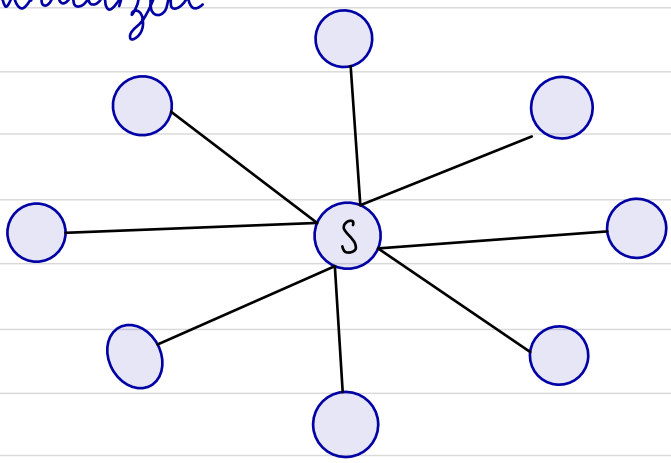
Switching

1>

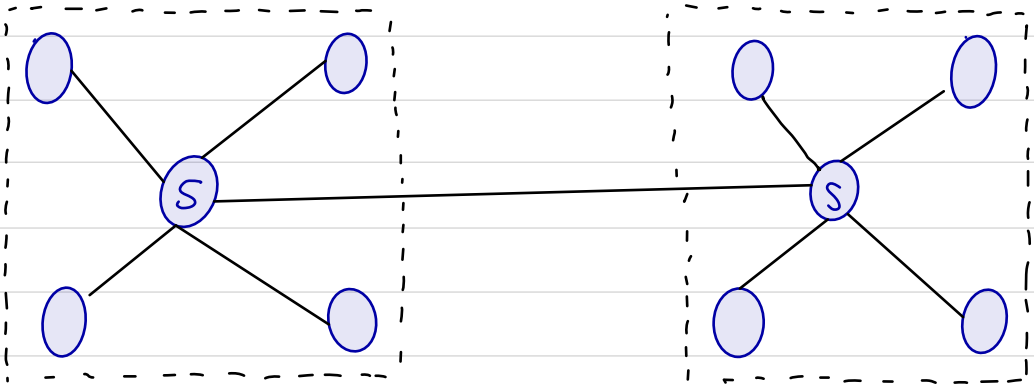


Fully connected : $\frac{N(N-1)}{2}$ links

2> Centralized



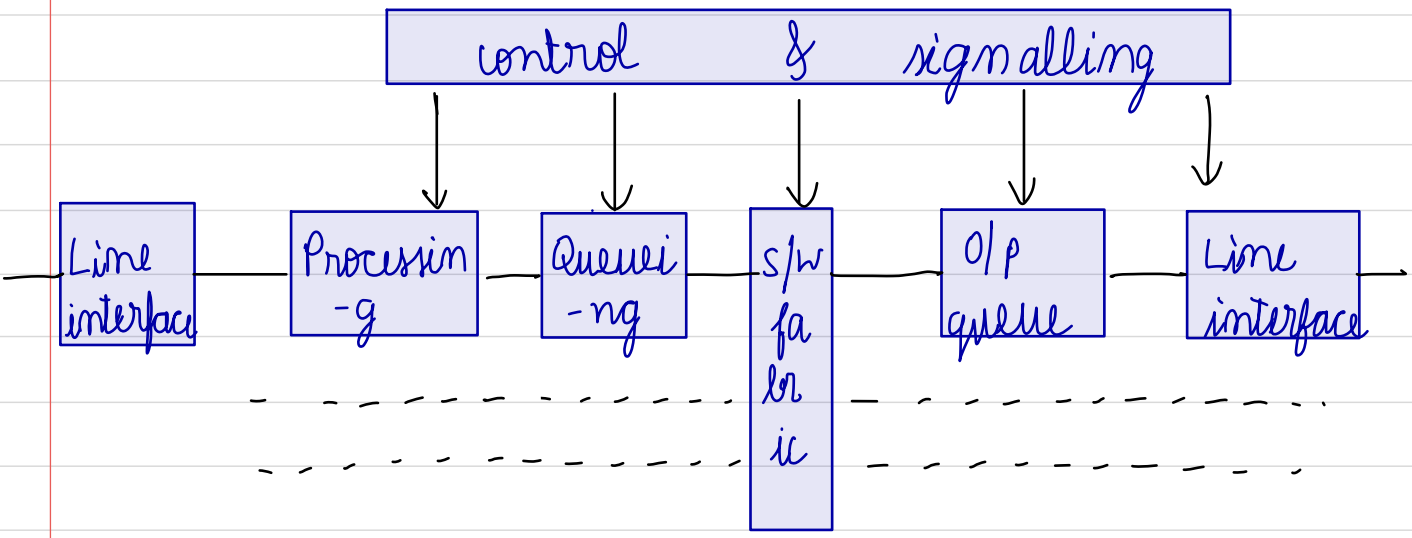
3> hierarchical :



- In a fully connected network, no. of links are more & uneconomical. Some links maybe rarely used and hence it is expensive.

- In centralised network, the physical distance between 2 nodes maybe less, but the distance the data needs to travel maybe more due to centralized architecture

Components of a Packet switch



- The line interface extracts the packet by identifying boundaries of the packet. (No. of bits.)

- Processor extracts the header & refers a lookup table for appropriate routing. The type of service like high & low priority is identified. If sending out is not possible

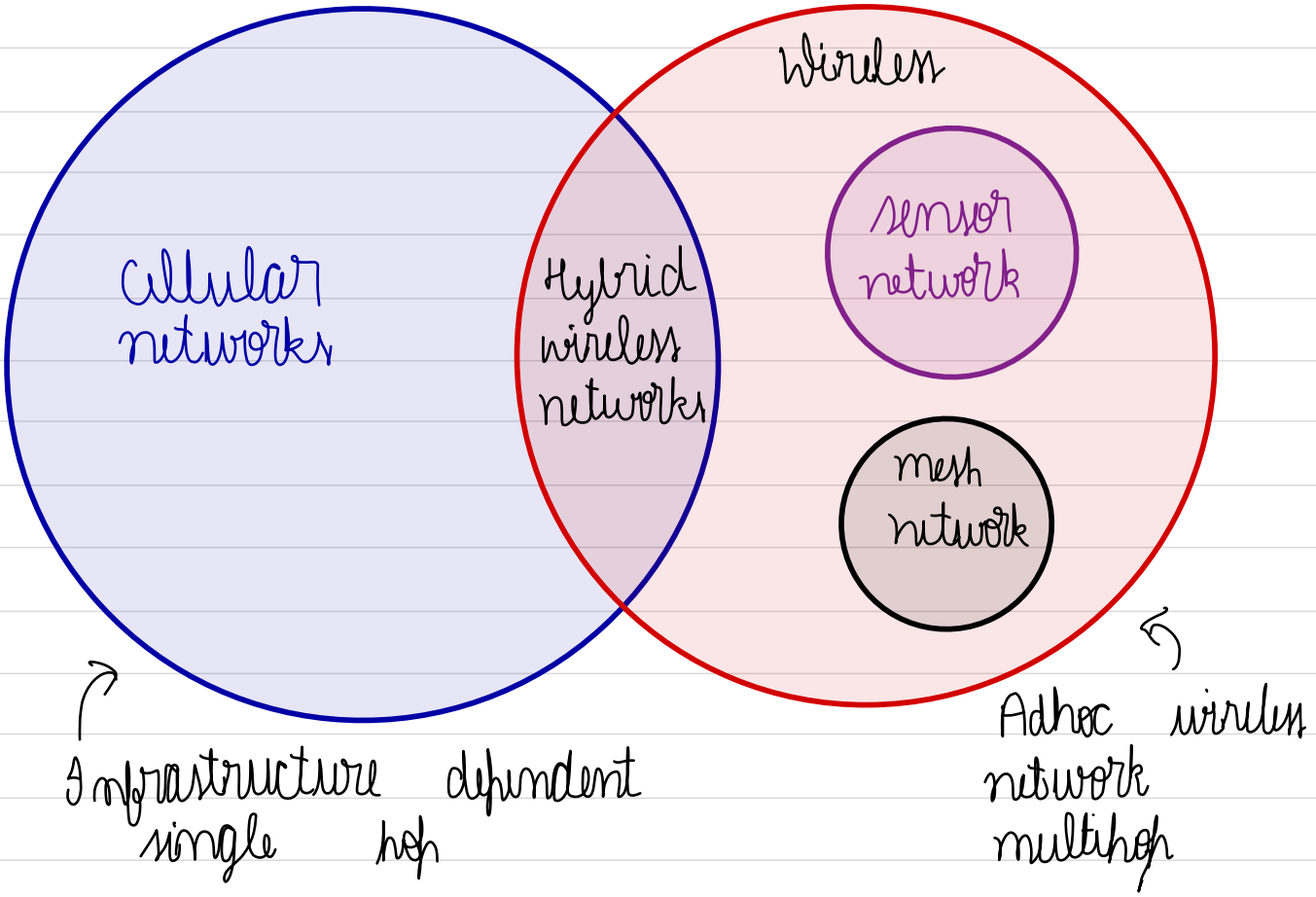
the data may have to be put in a queue.

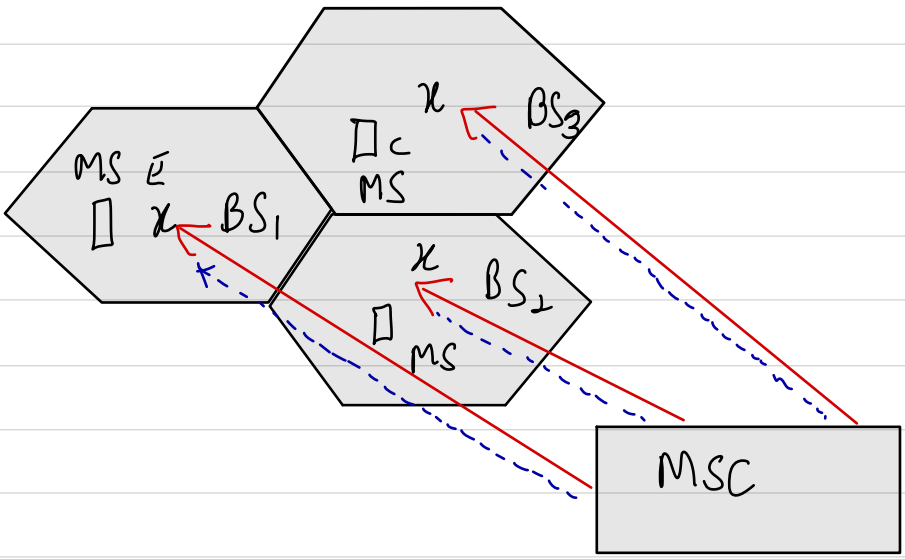
- Switching fabric determines the output queue. The switches also perform call setup in case of circuit multiplexer

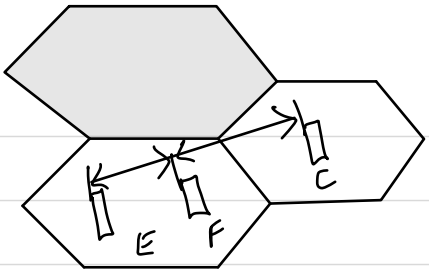
Adhoc networks

→ wireless networks which are temporary

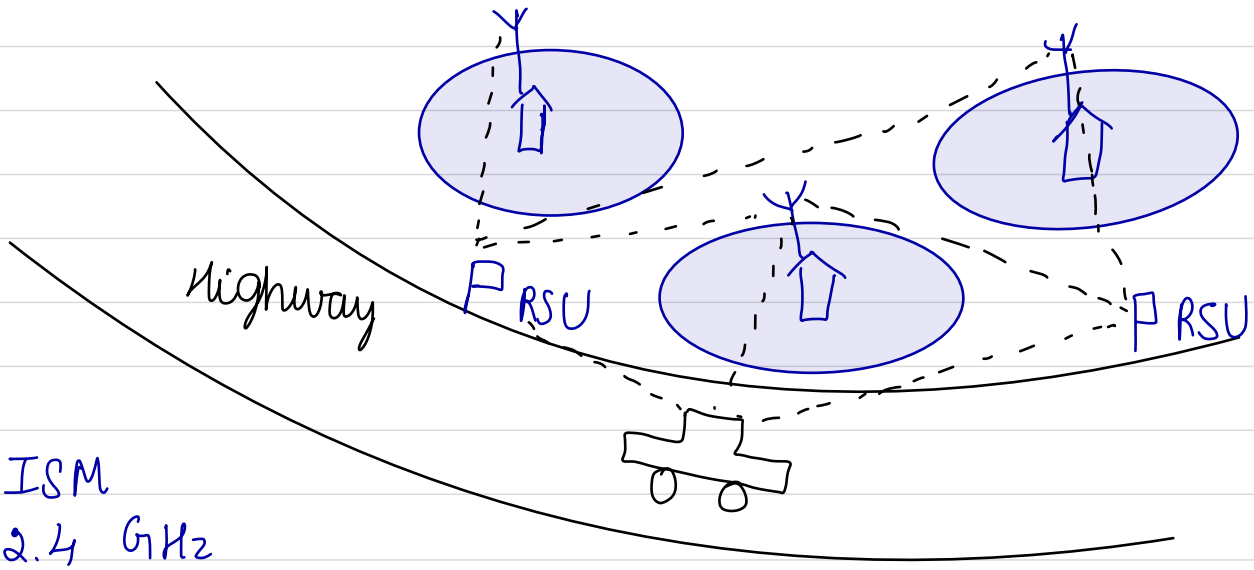
Cellular wireless networks.







Cellular network	Adhoc wireless network
1> Fixed infrastructure	1> Infrastructure less (No fixed infra)
2> Single hop wireless	2> Multitop wireless
3> Gauranteed bandwidth (voice)	3> Shared radio channel
4> Centralized routing	4> Distributed routing
5> Circuit switching	5> Packet switching
6> Seamless connectivity & low call drops	6> Frequent path breaks
7> High cost & time of deployment	7> Quick & cost effective
8> Reuse of frequency	8> Dynamic frequency use
9> Civil application	9> Military application
10> less complex	10> more complex



ISM
2.4 GHz
5.0 GHz

- A wireless mesh network is economical compared to cellular network. It provides an alternate path for data transfer.
- It operates in ISM band (2.4 - 5.0 GHz)
  ISM - Industrial, scientific, medical.
- Data rates : 2Mbps to 60Mbps.

Wireless sensor nodes

- Sensor nodes sense physical parameters, process them & communicate them to monitoring stations.
- Sensed data can be periodic or sporadic.

→ Periodic data eg: Temperature, humidity, radiation.

→ Sporadic data eg; stress level measurements of high rise building, border intrusion.

Issue distinct to sensor node networks

- Mobility of nodes is usually not existing in sensor networks. However, if the sensor nodes are mobile. They create additional problems like signal degradation & necessicity of more power.

- The size of sensor network is much larger compared to cellular & adhoc network.

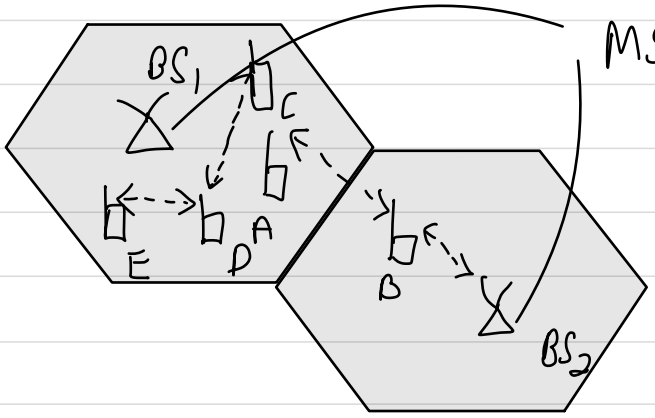
- Density of deployment depends upon the type of application. Power constraints are more stringent in sensor networks in comparison to adhoc & cellular network since sensors exist in harsh environment.

- Human supervision may not be possible. Since design should be rugged. In case of regenerative systems, power could be harnessed.

- Data fusion is necessary since bandwidth is limited. Reduction in no. of bits transmitted would be one of the solutions.

- The traffic distribution varies with application. Some applications may need faster delivery in case of intrusion and fire hazards.

Hybrid wireless networks



In hybrid wireless network communication between 2 entities can happen in different ways.

For eg: 1) A to B mobile stations can communicate directly

2) Communication between mobile stations C & E can be through D by avoiding base stations.

3) However base stations can keep a log of all it's node movements within that cell & update it regularly.

A few advantages are:

1) can have higher capacities than cellular networks

2) Efficient use of channels & reduced transmission mode.

3) Increased flexibility and reliability

4) Since failure of base station can still

provide a communication path, the coverage in areas of poor signal is better in a hybrid network.

Issues in adhoc wireless network.

1) Medium access schemes
2) Routing
3) Multicasting
4) Transport layer issues
5) Pricing schemes
6) Quality of service
7) Self organization
8) Security
9) Energy management
10) Scalability
11) Deployment

Medium access schemes

The performance of any wireless network depends on the MAC protocol. More so for adhoc wireless networks & sensor networks. Some of the issues are:

1) Distributed operation: There is no centralized coordination. Hence less control overhead may be needed for the packets transmitted.

2> Synchronisation: Time synchronisation is mandatory for TDMA systems to share scarce resources such as power & frequency.

3> Hidden terminals: These are those terminals which are not reachable by the transmitter but reachable by reciever. Hence collisions may occur.

4> Exposed terminals: These terminals are exposed both to transmitter & recievers and hence may interrupt when a transmission session is on.

5> Throughput: Maximizing throughput by reducing collisions & improving channel utilization is the motto here.

6> Access delay: It is the average delay a packet experiences. The target is to reduce this delay.

7> Fairness: It is an attempt to provide equal bandwidth to all competing nodes during data transfer.

8> Real time traffic: For traffic such as voice & video MAC protocols should be able to provide sufficient bandwidth such that quality is good.

9> Resource reservation: It is a planning criteria both for bandwidth and hardware The quality of service depends on this.

10> Power control:
It is essential to reduce interference and efficient use of energy.

11> Directional antenna: By use of this frequency reuse is better, reduced interfer-ence & reduced power consumption.

Routing:

1> Mobility: constant movement of nodes leads to path breaks, packet collision, stale routing information etc.

2> Bandwidth constraint: only fraction of total bandwidth is available to each user at a time, hence should be efficient.

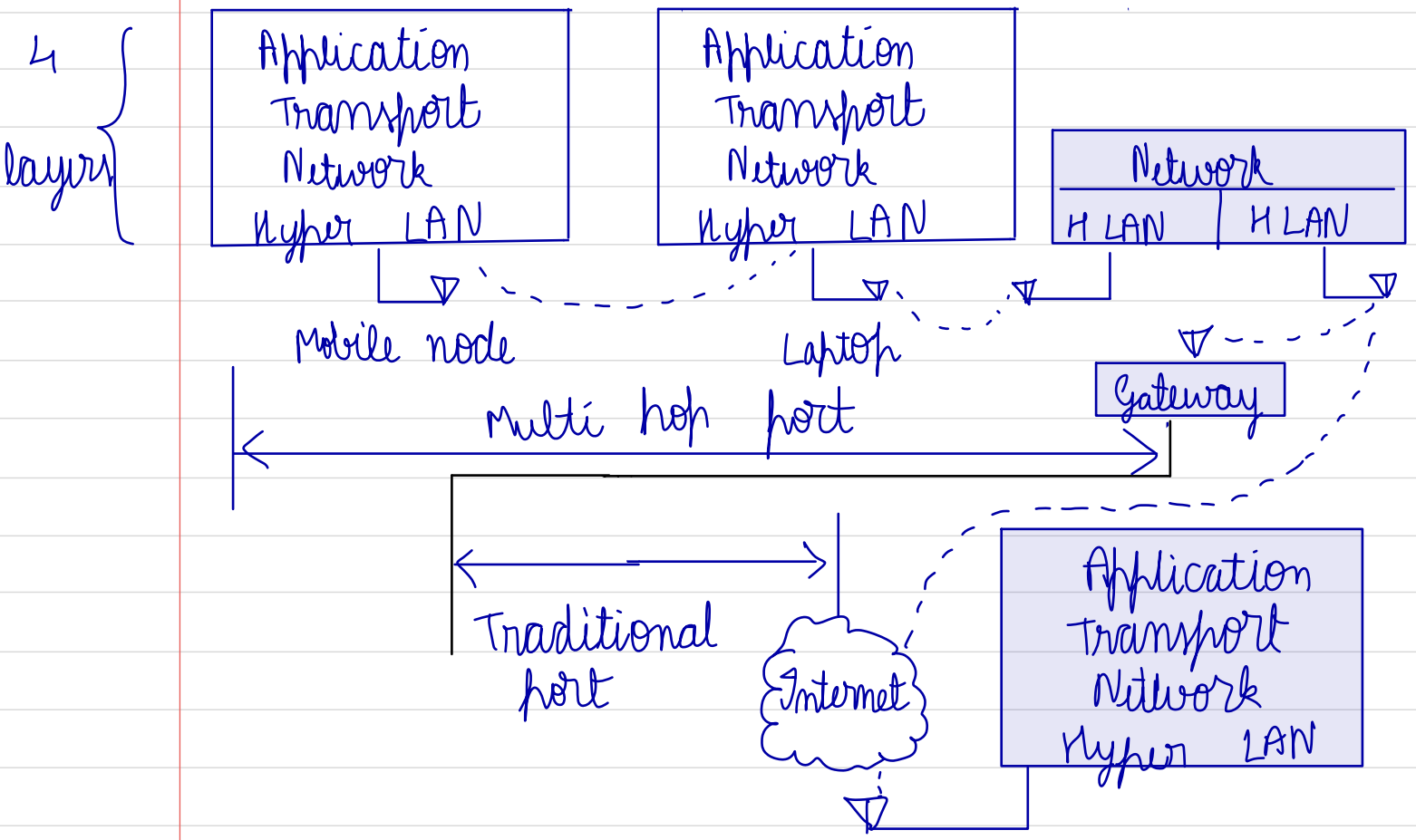
3> Error prone: Error rate in a wireless channel is quite high to extent of 10^{-5} to 10^{-3}. Wired channel error in range (10^{-12} to 10^{-9}). The SNR should be improved to reduce error

4> Location dependent: The higher the concentrati-on of nodes, the more chances of

collision and wastage of bandwidth.

5> Resource constraint: Computing power, battery power, buffer space limit the capacity of the nodes.

Adhoc wireless internet:



The above figure shows achoc wireless internet. It provides internet services to conferences, sport venues, military services, broadband in rural area.

Some of the issues faced by adhoc wireless internet are:

1) Gateways: Entry points to the wired internet or infrastructure network. They have to perform task like bandwidth management, load balancing, packet filtering and location discovery of end users.

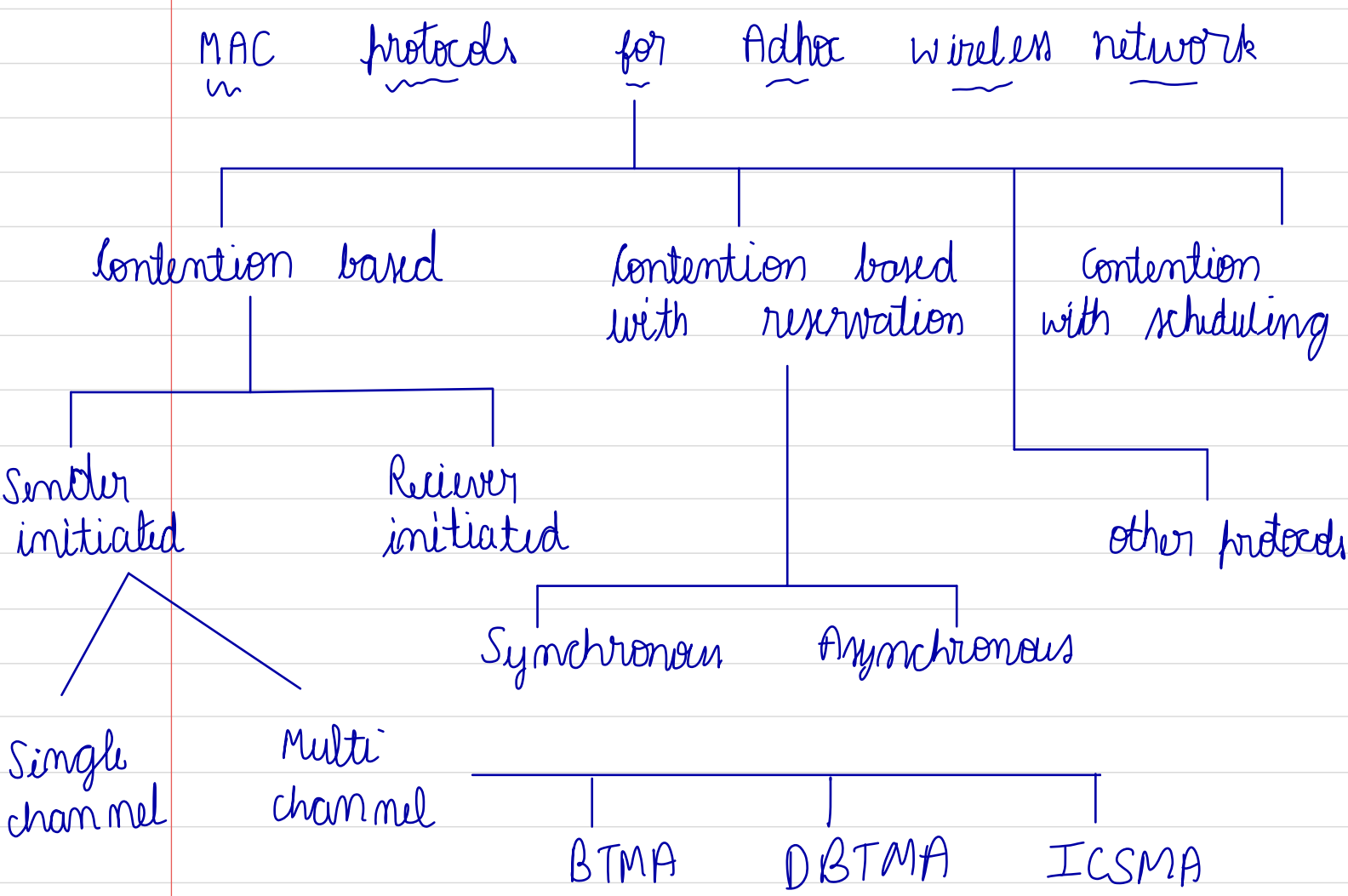
2) Address mobility: Since nodes are highly mobile, mobile internet protocol techniques may have to be employed.

3) Routing: It's difficult due to multi hop & dynamic nature of network

4) Pricing & billing: Gateways are ideal spot to keep track of incoming and outgoing traffic

5) Security: Since wireless medium is free for all, security is a prime concern.

6) Quality of service: The voice over Internet protocol (V.o.IP), quality of speech needs to be maintained.



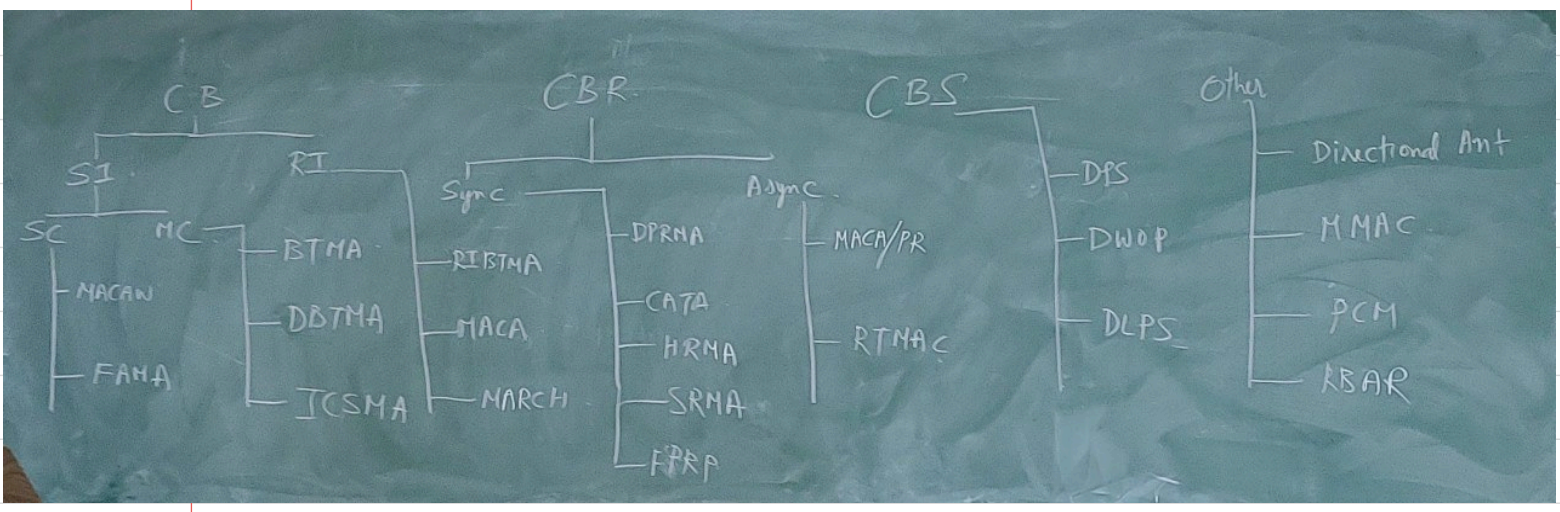
Can be classified into 3 main types:
1> Contention based
2> Contention based with reservation
3> Contention based with scheduling

1> Contention based: Nodes do not make any reservation in advanced. All neighbouring nodes take part using the shared channel. Quality of service cannot be gaurantee. There are 2 types:
a> Sender initiated
b> recived initiated
In (a), there are 2 types: single

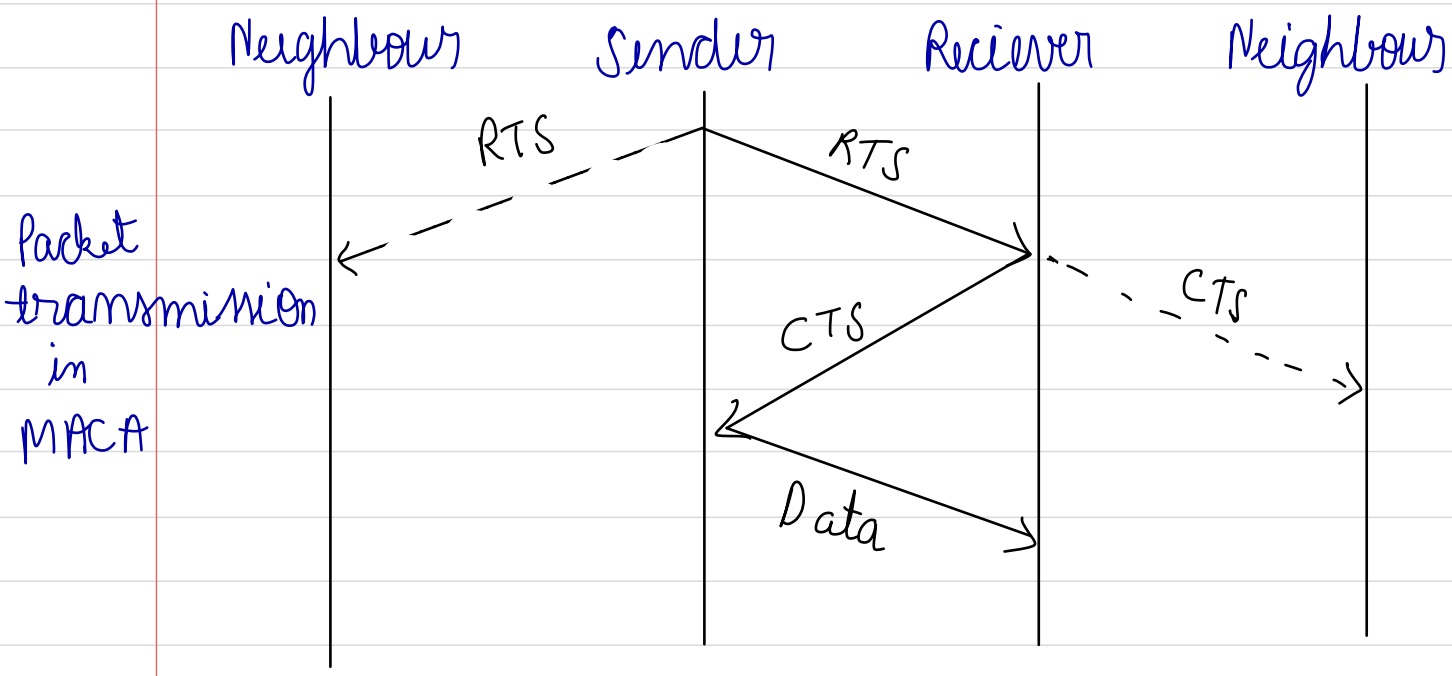
channel which uses entire bandwidth or multi channel where bandwidth is divided among nodes.

2> Contention based with reservation: It is mainly for real time traffic where QOS is needed. Here bandwidth & other resources are reserved in advance to support traffic. The traffic is usually time sensitive & hence synchrono-ous type requires synchronisation among all nodes. In asynchronous type the relative time information is used.

3> Contention based with scheduling: Here packets are scheduled at nodes. Nodes also need scheduling as to when they can access the channel. All the nodes are scheduled such that they get equal bandwidth. Scheduling scheme enforces priorities for the schemes at the nodes. Issues like remaining battery power is also considered before scheduling



MACAW: Medium access protol for wireless networks

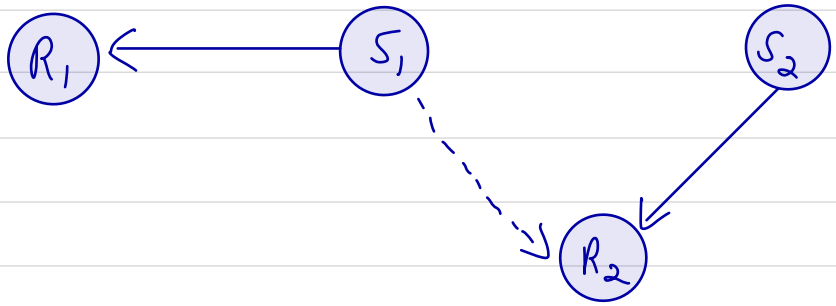


Packet transmission in MACA

RTS - Request to send
CTS - clear to send
BEB - Binary exponential backoff

MACAW is based on MACA (Multiple access with collission avoidance). MACA is an alternative for CSMA (carrier sense multiple access). In CSMA, the

carrier is sensed for activity and if it is busy it waits for a random time Hidden stations cause problems at receiver in CSMA due to collision. Here RTS & CTS are used to send packets. The transmitter sends data only after it receives CTS from the receiver. However if a packet is lost it uses BEB algorithm. In BEB the wait time is doubled very time a collision occurs. Here the neighbours wait for a long enough time after hearing RTS so that a CTS is also heard by the sender. If a CTS is not heard by the sender then neighbours may send their own data. The RTS and CTS packets carry the information of the expected duration of data transfer.



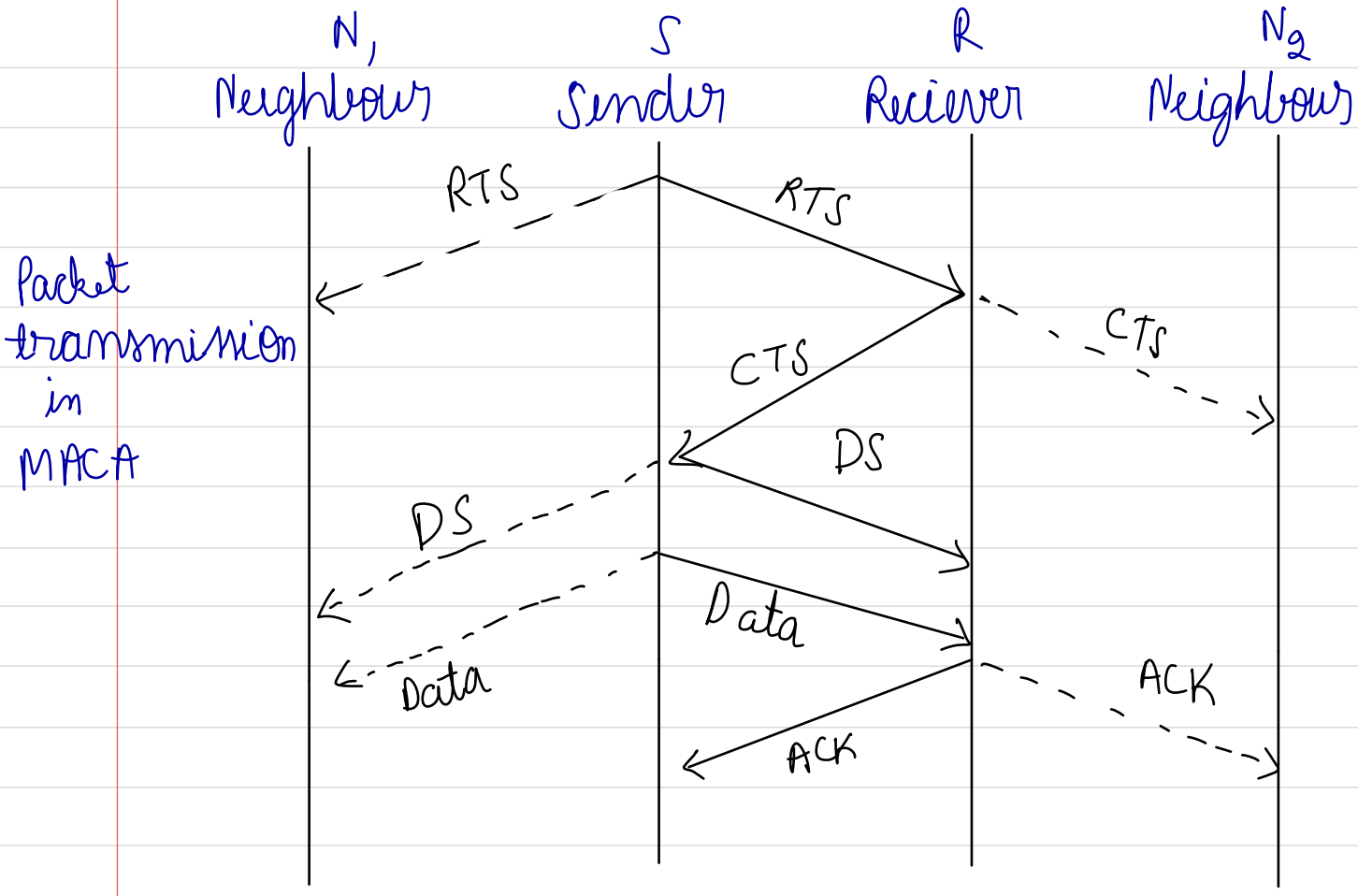
MILD - Multiplication increase and linear decrease.

In last example both S_1 & S_2 are trying to send data to R_1 & R_2 respectively. However R_2 is in the range of S_1 and is able to listen to the data transfer. Now S_2 has to backoff. It may so happen that S_2 may not be able to send data to R_2 because of BEB. An improvement over BEB is MILD. Here upon collission the backoff is 1.5 times and upon successful transition it is decrement -ed by a factor of 1.

RRTS (Request for request to send) is another type of data which is sent by the reciever to the sender when it is ready to accept data.

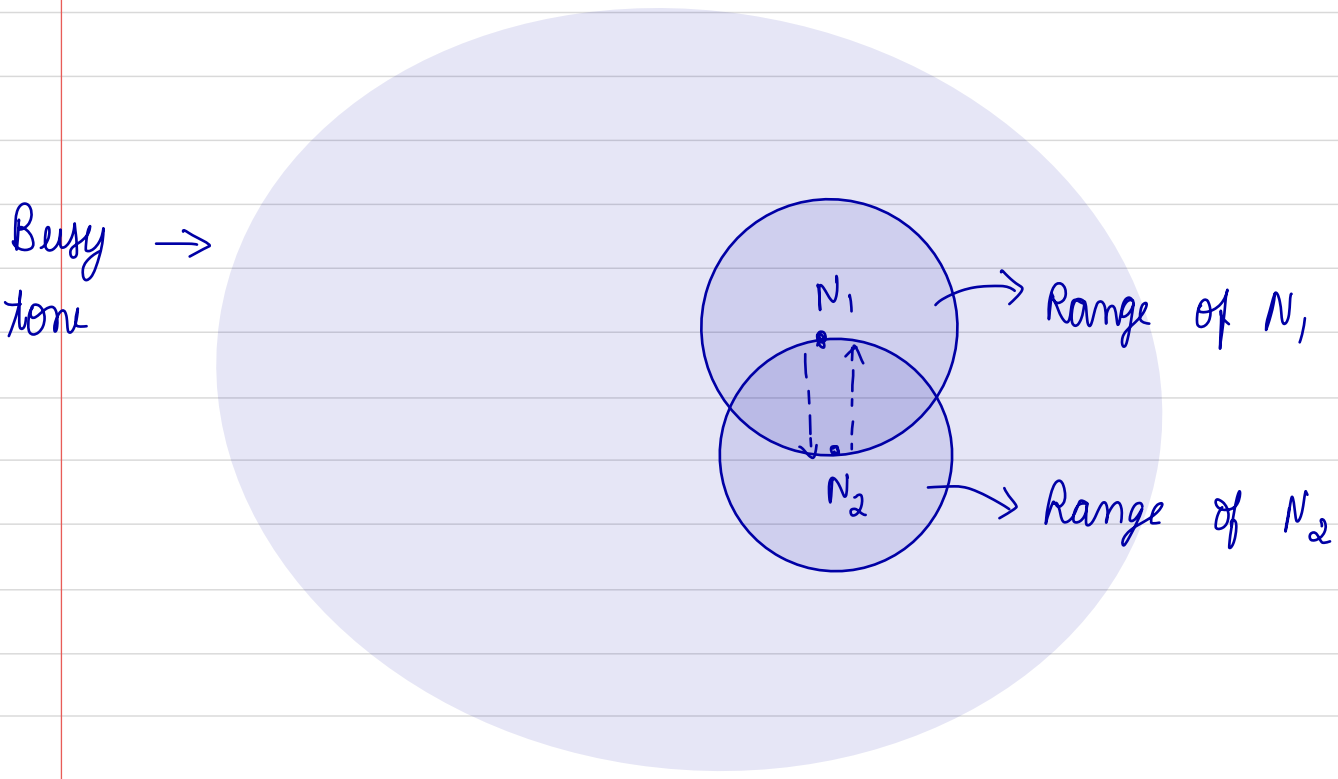
When R_2 finds out it can use the medium it sends an RRTS to S_2 initiating to send the data.

FAMA:



- When S transmits RTS, node N_1 avoids transmitting anything as it hears RTS.
- The moment R recieves RTS, it initiates CTS, this is heard by neighbour N_2. Hence N_2 avoids transmitting until reciever R recieves all the data from S. S also sends a DS message which is a kind of reservation informing neighbours. After R has recieved all data, it sends acknowledgment to S. And all in the neighbourhood know that the medium is free for transmission

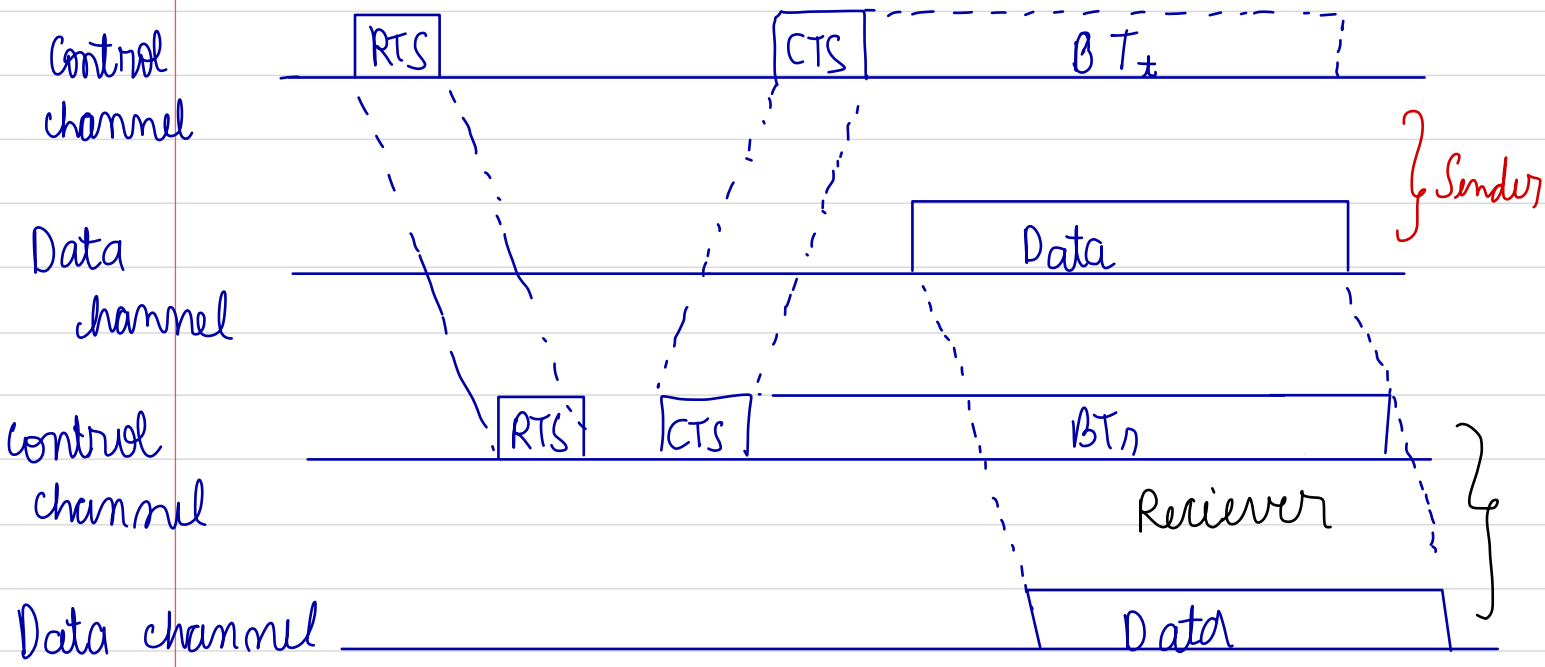
BTMA : Busy Tone multiple access



In BTMA, the available channel is split into 2 (frequency). One is called control channel & other is called data channel. Data channel is used for data transmission. Control channel is used to transmit the busy tone signal. When a node wants to transmit, it checks for busy tone signal in the medium. If the busy tone signal is not active then the transmitting node activates its busy tone & starts transmitting.

No other node in the neighbourhood is allowed to transfer. The above figure shows the worst case scenario where the node density is very high & the bandwidth utilization is poor.

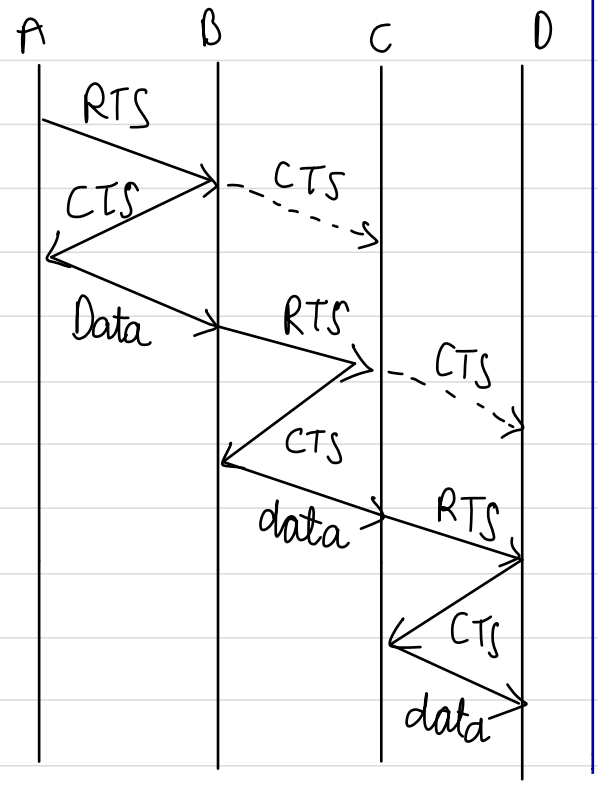
DBTMA: Dual Busy tone multiple access



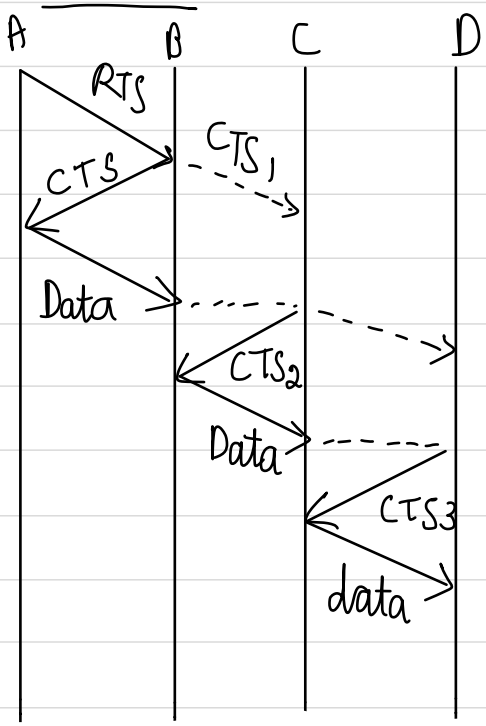
Similar to BTMA, but has an additional busy tone for the reciever also. BT_t is on while transmitting. BT_r is on during reception at the reciever. Here the network utilization is better since either the forward or backward channel is blocked as & when needed.

MARCH - Media Access with Reduced Handshake

MACA :



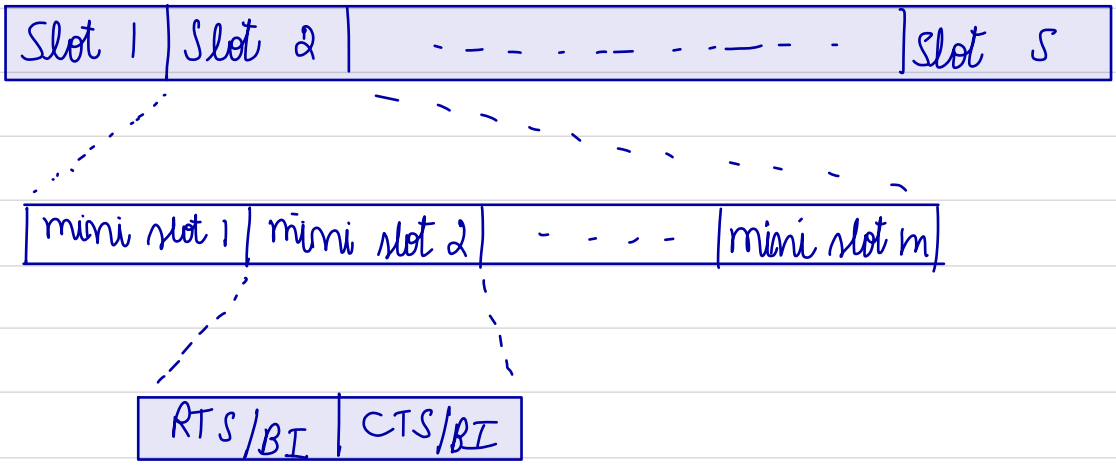
MARCH :



March exploits broadcast nature of omnidirectional antenna. Unlike MACA in MARCH, neighbouring node B generates its own CTS 2. After some time after it hears the CTS1 from B. Node C becomes ready to accept the forwarded data from B.

In the figure of MARCH, we observe that RTS is sent or generated by sender only once. After the first RTS, only CTS is generated by subsequent recievers to recieve data. Since the time required for end to end transmission of data is lesser compared to MACA. ∴ in March 2 way handshake is reduced to 1 way handshake.

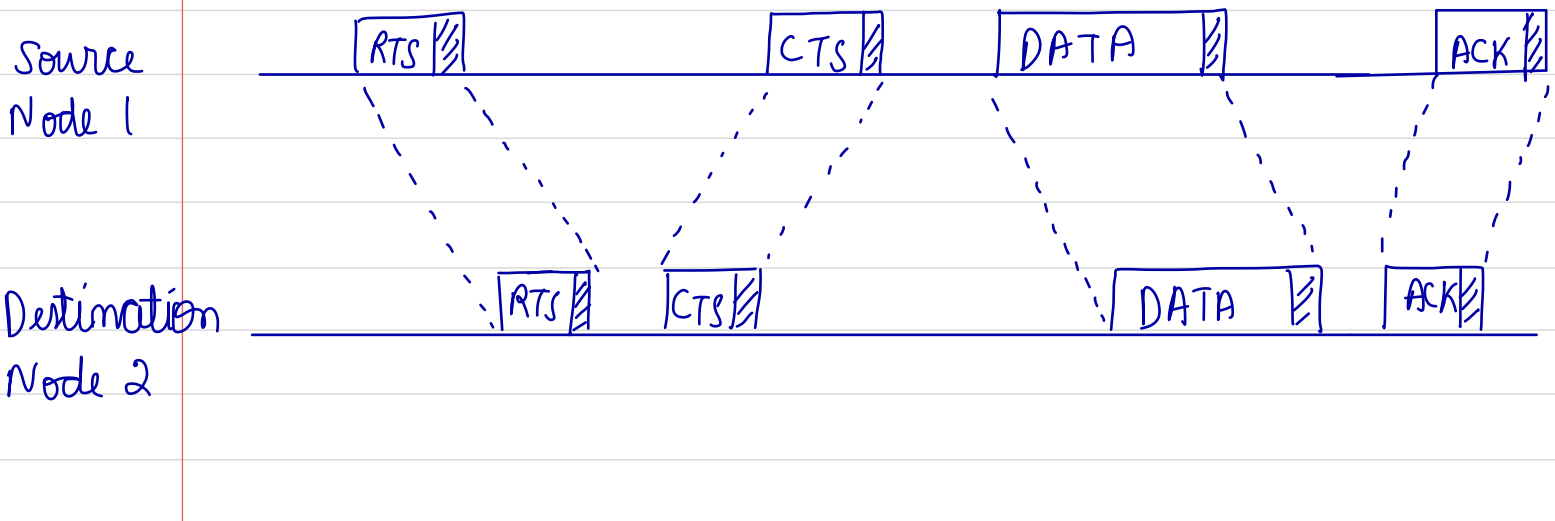
D-PRMA : Distributed packet reservation multiple accn



DPRMA is a TDMA (time division multiple accen) scheme. Channel is divided into fixed & equal sized time frames. Each time frame is further divided into mini slots. A frame could have S number of slots which is repeated in a cyclic fashion Mini slots are divided into 2 fields: RTS/BI & CTS/BI. BI indicates Busy indicator. All nodes that wants to transmit will contend for the first mini slot if it is a winner, it gets all mini slots for transmision. Sender sends the RTS/BI & reciever sends the CTS/BI when ready. If the sender is unable to win a slot it tries in the other subsequent slots for reservation. Here QOS can be gaurantee since the channel is reserved for only the winner.

Contention based with scheduling

DPS - Distributed Parity scheduling :



S	D	P
4	5	1
7	8	5

ST(a)

S	D	P
4	5	1
7	8	5
1	2	9

ST(b)

S	D	P
4	5	1
7	8	5
1	2	9
1	6	14

ST(c)

S	D	P
4	5	1
7	8	5
1	6	14

- Piggy banking is employed when RTS & CTS are sent. This will help neighbouring nodes to update their scheduling table.
- In this eg: node 1 wants to send to node 2 with a priority index 9. Hence in ST(b) there is an additional entry in 3rd row indicating this NAV.
- The CTS is sent in reponse by node 2 & neighbouring node 4 hears this CTS and extracts the piggy backed information, where it comes to know that node 1 wants to send to node 6 with priority. Hence node 4 updates its ST with entry in row 4 as shown in ST(c). Once the transfer of data from node 1 to node 2 is completed, this entry is deleted from ST as shown in ST(d).

Routing protocols for Adhoc wireless networks

Issues:

1> **Mobility**: Unlike wired networks, wireless networks are highly mobile. Therefore protocols should be efficient in mobility management.

2> **Bandwidth**: In wired networks, large bandwidth is available using optic fibres & wavelength division multiplexing. But in wired networks bandwidth is premium, hence routing protocols should use bandwidth optimally.

3> **Radio channel**: The time varying characteristics of a wireless channels lost problems. Routing protocols may have to find alternative path while there is congestion.

4> **Hidden & exposed station problems**: Routing protocol should take care of this issue.

5> **Resources**: Resources like battery power, memory hardware, computing power & frequencies should be used optimally. The size and weight of a node also depends on these resources.

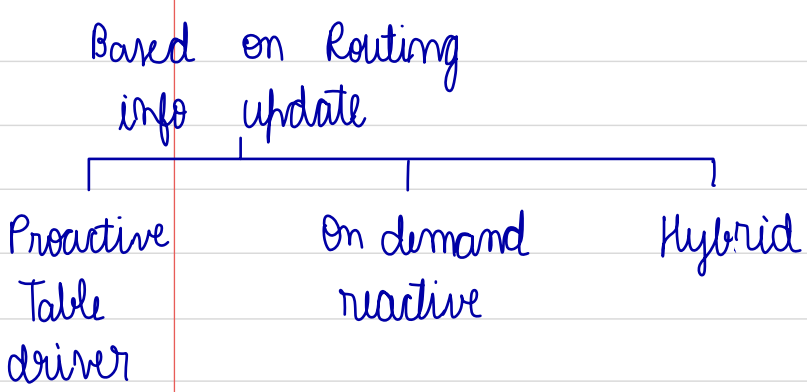
Ideal characteristics of routing protocol

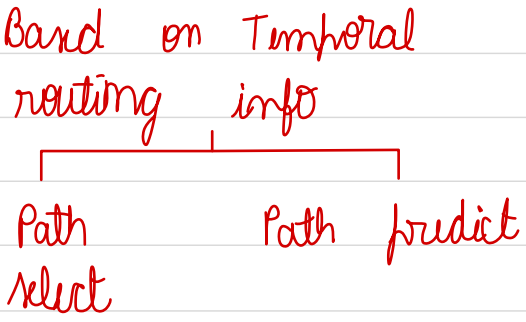
1> **Must be fully distributed**: Centralized behaviour

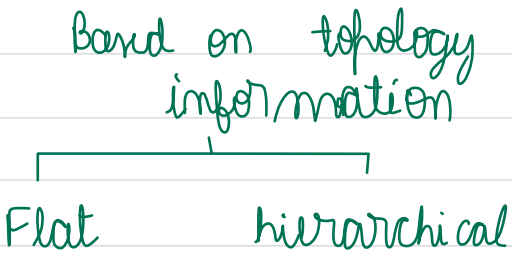
involves more overhead & is not scalable

- Topology changes are common in adhoc networks. Hence the protocols should be able to adapt.
- Localization is the requirement since globalization leads to more control overhead
- The setup between end to end nodes must be minimal
- Loop free behaviour is essential to avoid bounce back of messages.
- Collisions should be minimum such that resource and time is not wasted.
- Convergence to optimal root must be quick.
- QOS is needed.

Routing protocols for Adhoc wireless network classification:







→ This classification is not mutually exclusive.
→ They may fall into more than one category.

→ Routing information update:

1) Proactive (table driven):
Here the routing information is flooded on the network and every node maintains a routing technique by periodically exchanging routing information.

2) Reactive (on demand):
It does not maintain a routing table but obtains it as & when necessary through connection establishment.

3) Hybrid:
It combines the best features of the above 2. It uses proactive for nearby nodes and reactive for faraway nodes.

→ Temporal info based:

Whenever a path breaks the restablishment is done using fast and present information.

→ Routing topology based:

1) Flat:
It uses internet type addressing which is unique for every node.

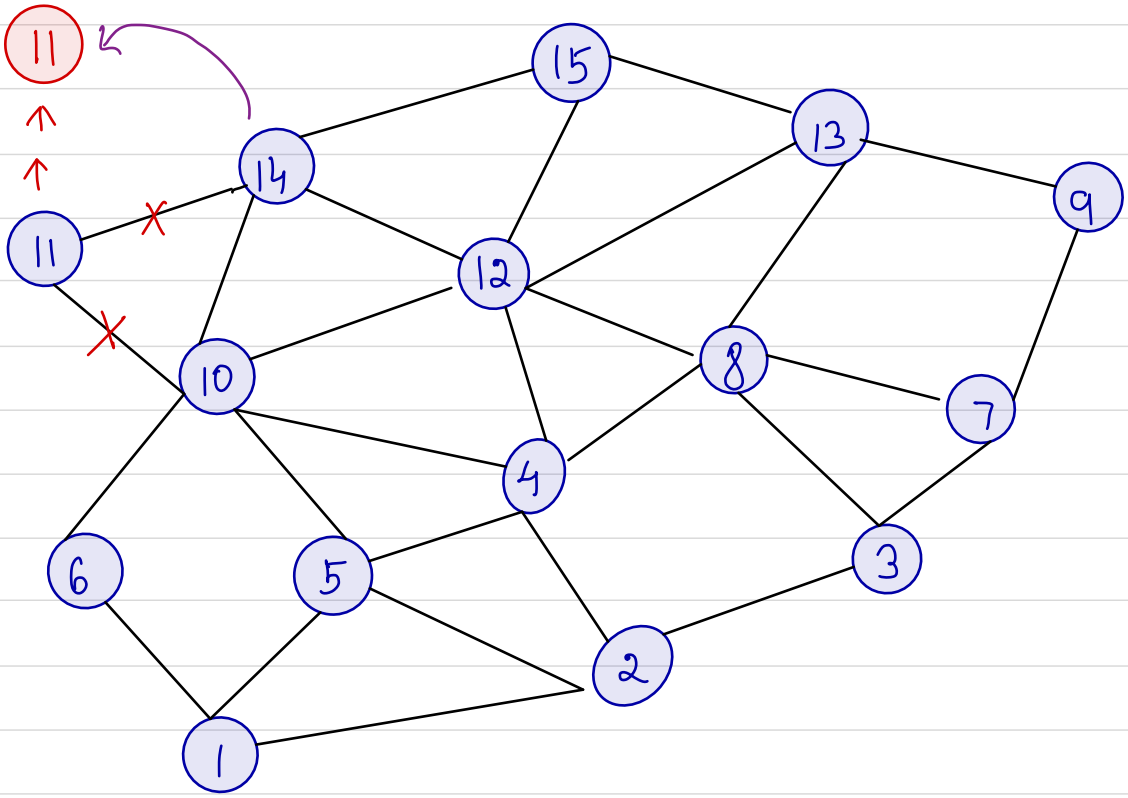
2) Hierarchy: Uses logical hierarchy based on the geography

→ Resource utilization:

1> Power aware:
The route is selected based on the residual power in every node

2> Geographical info based (GIS):
It uses GPS or GIS to locate nodes thereby reducing control overhead.

DSDV: (Destination sequenced distance vector)



This is one of the first routing protocols which was suggested for adhoc wireless networks.

Destination	Next node	Number of Hops
1	–	0
2	2	1
3	2	2
4	5	2
6	6	1
7	2	3
8	2	3
9	2	4
10	5	2
11	6	3
12	5	3
13	2	4
14	6	3
15	5	4

- This algorithm is an enhanced version of Bellman Ford algorithm. Every node maintai -ns a table of the shortest path of every other node.
- Sometimes a problem known as 'count to infini -ty' problem may arise whenever a node dies or awakens in the network. (eg 1) here)
- The table update could be incremental type for small changes in the topology or could be flooding type for major changes in topology network.
- For eg: If destination is 15, the route from source 1 can be via node 5 and number of hops needed is 4.

- If one of the nodes say 11 either dies down or moves away then the link to the neighbouring nodes 10, 14 is broken. Hence 10 and 14 inform it's neighbours that 11 cannot be reached. This info is broadcasted to entire network.
- However if one of the nodes recieves a link to 11 in this case 14, then this info is also passed to neighbouring nodes.
- The following table records that route to 11 is via node 5 and the number of hops change from 3 to 4

Destination	Next node	Number of Hops
1	–	0
2	2	1
3	2	2
4	5	2
6	6	1
7	2	3
8	2	3
9	2	4
10	5	2
11	5	4
12	5	3
13	2	4
14	6	3
15	5	4

Advantages: 1> Suitable for both wired & wireless networks.

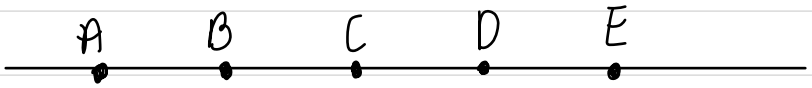
2> Routes available to all nodes, hence less setup time.

Disadvantages:

1> more overhead info if nodes are highly mobile.

2> Node update info may reach later when network is quite large.

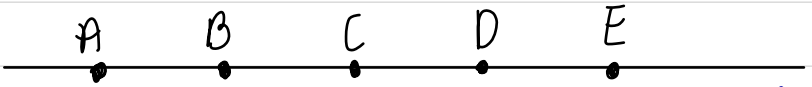
Count to infinity problem:



∞	∞	∞	∞	(Initially)
1	∞	∞	∞	(After 1st update)
1	2	∞	∞	(2nd update)
1	2	3	∞	(3rd update)
1	2	3	4	(4th update)

When A comes to life in network

When A dies;



1	2	3	4	(Initially)
∞	2	3	4	(1st exchange)
3	2	3	4	(B looks at C and concludes 3)
3	4	3	4	
5	4	5	4	
5	6	5	6	
⋮				
∞				

A B C D E are nodes placed in single row. The delay metric is number of hops.

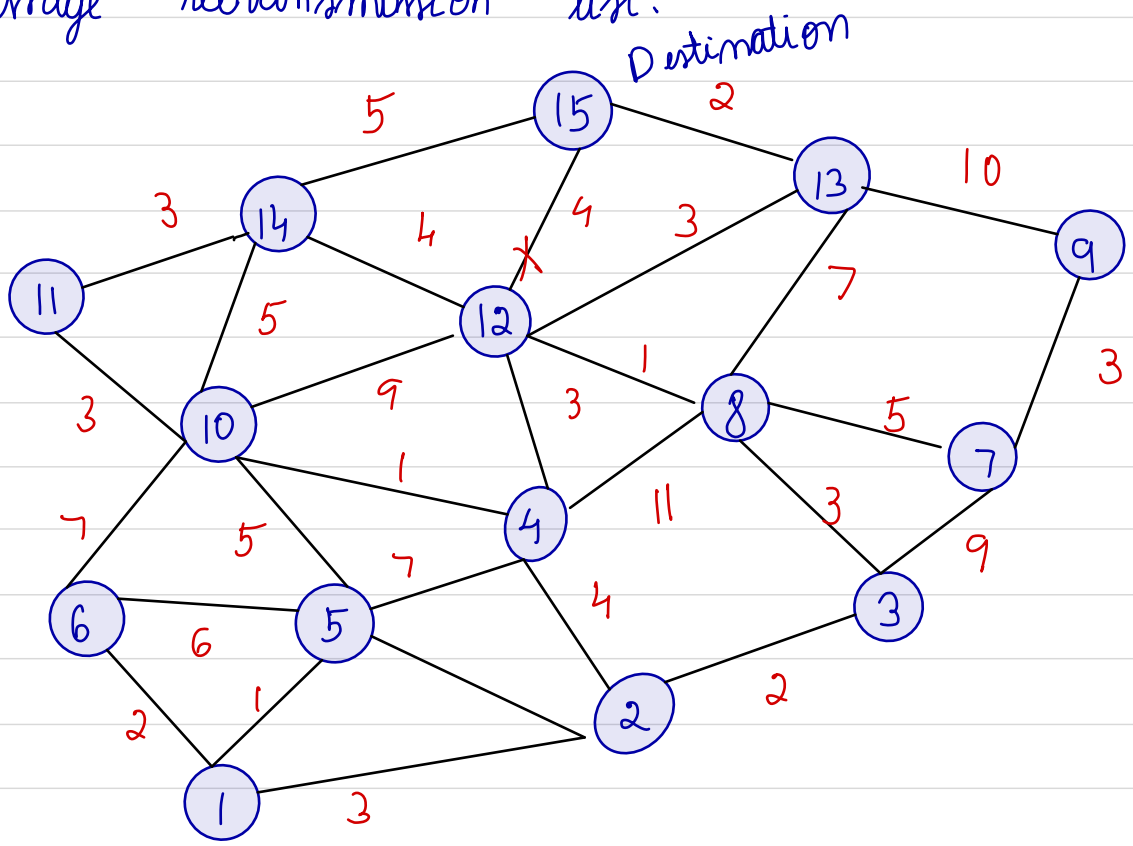
Initially A is down and all nodes record ∞ as distance. When A is energised B learns this & makes an intry into it's routing table that A is just 1 hop away from it. All other nodes still think that A is not reachable or down. On next update / exchange, C learns that B is 1 hop away from A and updates it's routing table as it is 2 hops away from A. This continues till N exchanges such that all nodes learn about A's existence.

However in second case when A suddenly goes down, B records ∞ distance from A. At random when it looks at C it assumes that there is a path to A via C and wrongly updates the distance of A as 3 hops. This continues with all other nodes untile all records the distance from A as ∞.

This problem is called as "count to infinity" problem. This can be avoided if every update has a time stamp or sequence.

WRP - Wireless routing Protocols :

→ Distance and routing table.
→ Link cost table
→ Message retransmission list.



After :-

Source node	Next node	Predecessor	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	13	13	5
11	14	14	8
10	4	13	9 (via 4)
9	13	13	12
8	12	13	12
7	8	13	11
6	10	13	16

5	10	13	14
4	12	13	8
3	4	13	11
2	4	13	12
1	2	13	15

WRP differs from DSDV by maintaining a set of tables instead of just one table.

Distance table: It contains information about neighbouring & predecessor nodes.

Routing table: It contains info about predecessor & next node. Info about condition of path is also maintained called flag.

Link cost table: It contains info about number of hops, path length, no. of update periods & probable delay.

Message transmission list: It keeps entry of every update by maintaining a decrementing count. Since more number of tables are maintained, convergence to optimal route is faster. The table shows the routing for the distination node 15. For eg: for route from 1 to 15 the next node is 2 & predecessor node is 12. The total cost to reach distination is 14. Predecessor node helps in faster

convergence. Shortest path algorithm is employed to reach destination.

Before:-

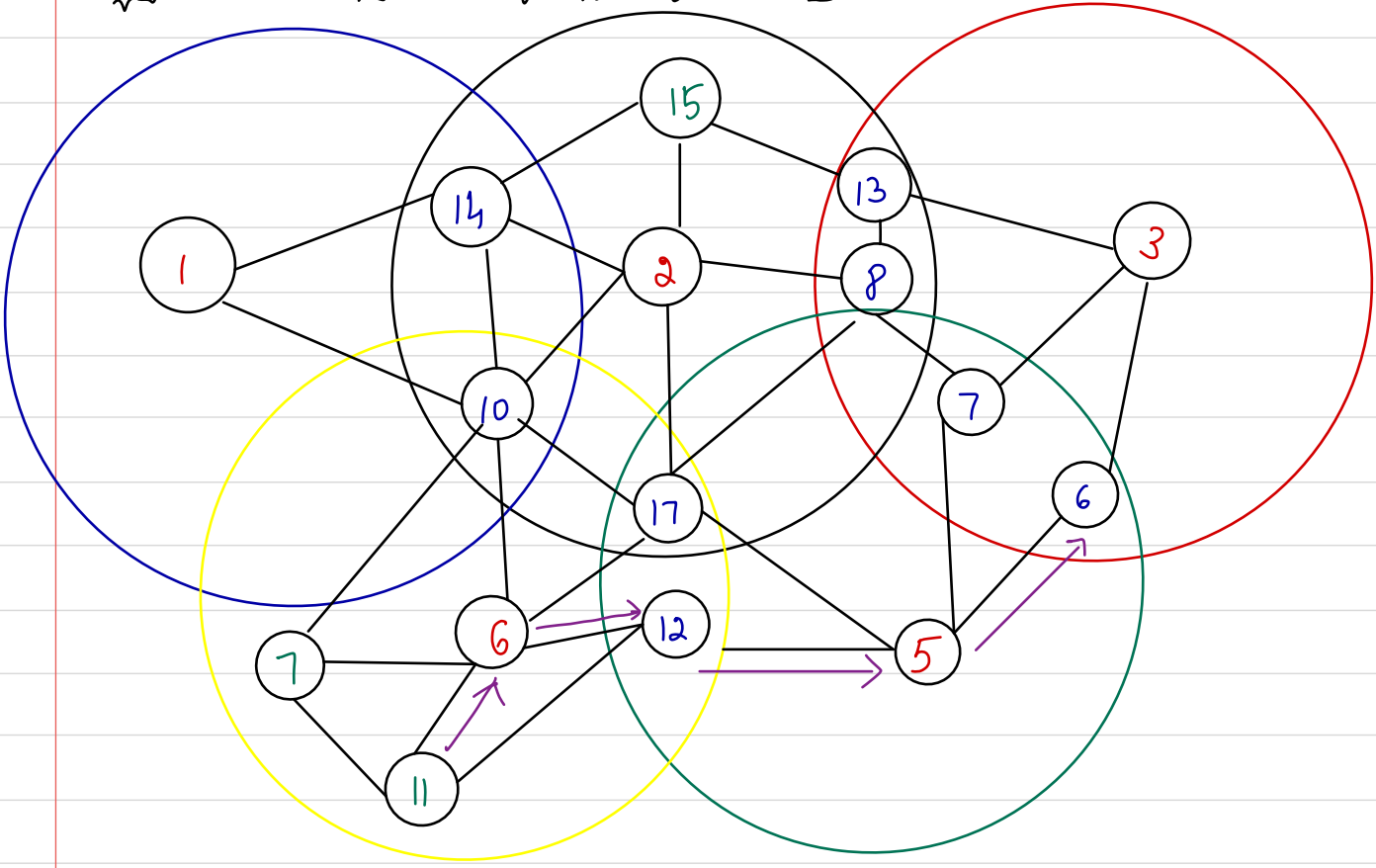
Source Node	Next node	Predecessor	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	12	4
11	14	14	8
10	4	12	8 (via 4)
9	13	13	12
8	12	12	5
7	8	12	10
6	10	12	15 (via 4)
5	10	12	13 (via 4)
4	12	12	7
3	4	12	10
2	4	12	11
1	2	12	14

If for example the link between node 12 & 15 breaks for some reason, then all entries with predecessor node 12 change entries to node 13 as the predecessor to destina-tion 15. The cost will accordingly change with new entries in routing tables

Advantages: 1> Convergence is faster
2> Needs fewer updates.

Disadvantages: 1) Complexity of maintaining tables is more. Hence needs more memory.
2) More processing is required & not suitable for highly dynamic networks.

cluster head gateway switch routing



— : Cluster heads
— : intersection nodes between clusters
— : other nodes

→ In CGSR, an hierarchical approach is used by organising the nodes into clusters. The cluster head behaves as the coordinator.
→ The cluster head is chosen by an algorithm called "least cluster change" → LCC. Cluster heads help in regulating the bandwidth

allocation. Network number nodes can access the network through the cluster heads with a single hop.

→ A token based algorithm is used within a cluster. Nodes which are common to clusters are called cluster gateways.

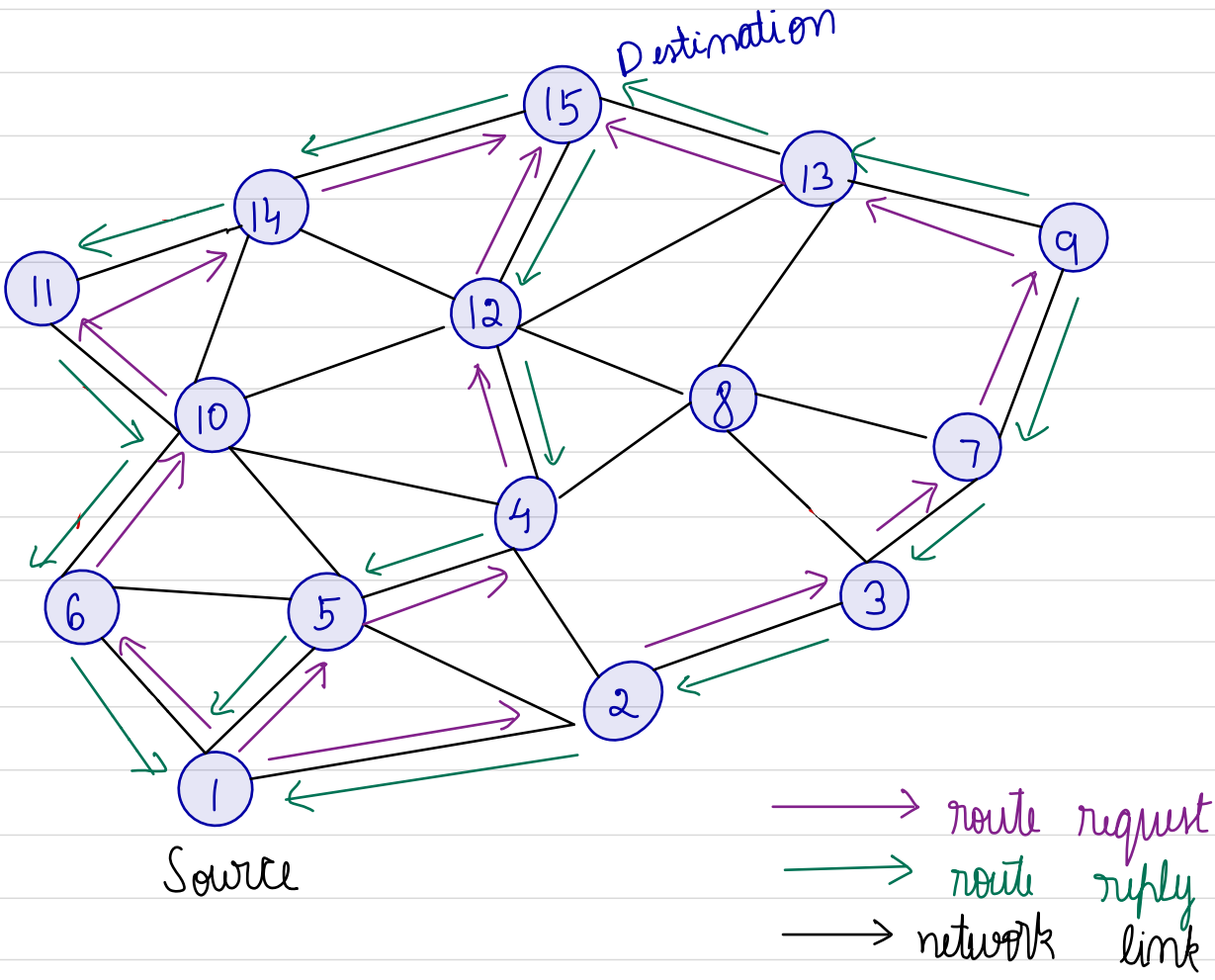
→ Gateway conflict may occur at times, when the gateway is catering to another cluster.

→ Similar to DSDB a table about the cluster head is maintained at every node. For eg: Path between 11 to 16 is 11 → 6 → 12 → 5 → 16 as shown in figure.

Advantages: 1> Better Bandwidth utilization.
2> Easy to implement priority scheduling for real time traffic at cluster head.

Disadvantages: 1> Path length may sometimes be increased.
2> More power consumption at cluster head.

DSR - Dynamic source routing → Beacon less



→ DSR protocol is designed to restrict the periodic updates & hence save bandwidth and computing power at all nodes.

→ It is also called a beacon less protocol since there are no hello packets generated repeatedly.

→ When a route request arrives, this flooded on to the network. If the destination node replies, then the root of the root

reply message is noted & the data is sent on the same route.

→ In the last example, several path to distination are formed like:
Path 1: 1-2-3-7-9-13-15
Path 2: 1-5-4-12-15
Path 3: 1-6-10-11-14-15

→ For eg: if 1 wants to send data, it sends route requests. The neighbours 2, 5, 6 recieve this & forward this.

→ Node 4 may get multiple copies from 2 & 5 however the late arrival is discarded

→ The route request reaches the distination & the destination initiates a route reply.

→ The source node will get multiple replies, but it will choose the best path in terms of no. of hops or delay etc.

→ If one of the links is broken, then the whole route discovery program has to be reinitiated.

Advantages: 1> Uses a reactive approach, hence saving memory.
2> Performs well on static & low mobility networks.

Disadvantages: 1) The route maintanance mechanism does not locally repair broken link issue.
2) Connection setup time is more compared to table driven or proactive methods.

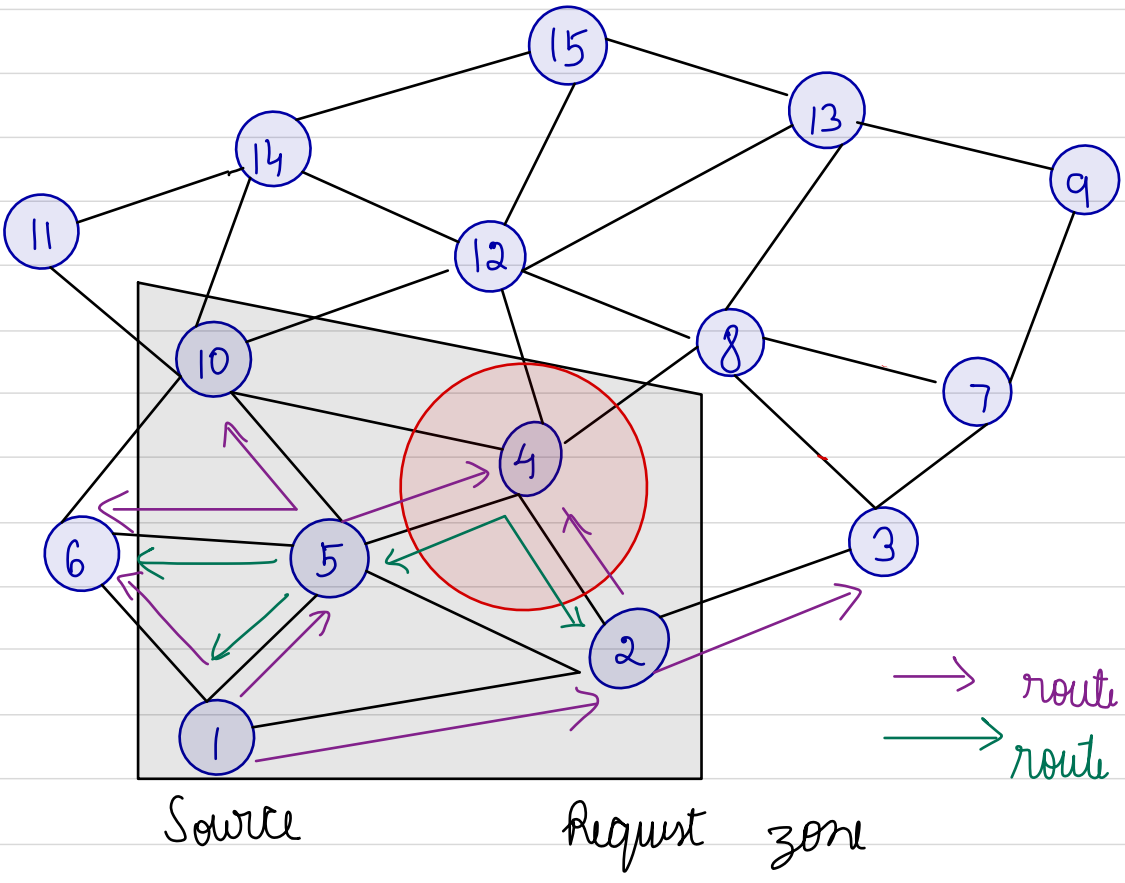
AODV : Adhoc on Demand distance vector Routing

- An improvement over DSR is AODV.
- The difference is additional control overhead is used to decide the path towards distination.
- A node updates it's path information only if the distination sequence number of current packet is greater than previous distination sequence number
- A route request will contain source id, distination id, source sequence number, distination sequence number & time to live (TTL).

Advantages : 1> Connection setup time is reduced.

Disadvantages : 1> Heavy control overhead is necessary for exchanging information.

Location Aided routing (LAR)



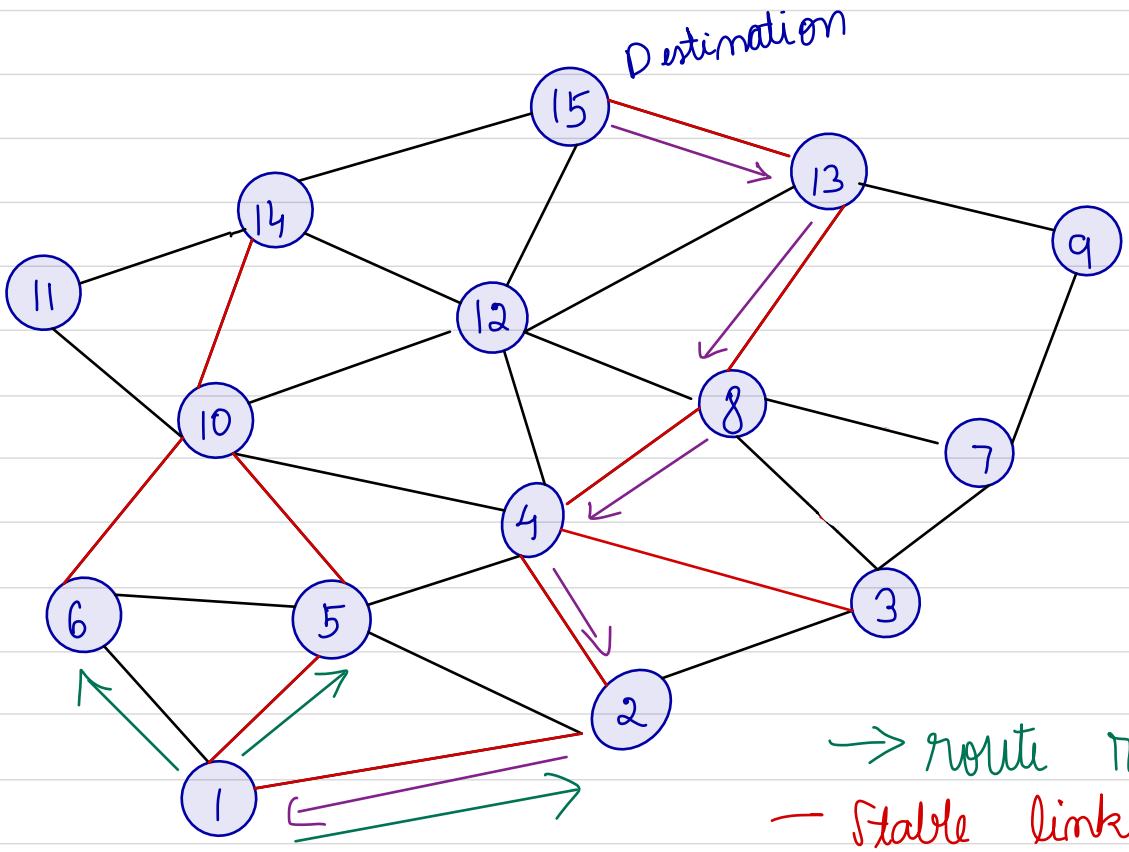
→ This protocol assumes that GPS is available.
→ There are 2 zones: request & expected.
→ Control & request packets are restricted from going beyond request zone.
→ Expected zone is a smaller area within which distination may be present.
→ However if destination node is not present in expected zone then request zone may increased.
→ The request zone is a square or rectangle which has both source & distination nodes.

→ However if source & distination nodes lie in expected zone then request zone may be reduced to expected zone.
→ Nodes which lie outside request zone discard the route request packet.

Advantages: 1) Search area is limited, hence reduced control overhead.

Disadvantages: 1) Relies heavily on GPS.

Associativity based routing (ABR)



→ ABR is based on stability of wireless links.
→ Every node keeps a count of no. of beacons recieved from neighbours.
→ More beacons ⇒ stable, less beacons ⇒ unstable.
→ When a route request packet is sent it reaches the destination via different routes.
→ The route with maximum stable links is chosen for the final path.
→ If a link is broken, a local repair mechanism is initiated to find an alternate path.

→ Intermediate nodes are not restricted from forwarding the route request packets depending upon the stability of a link.
→ The stability info is used only during final route selection process.

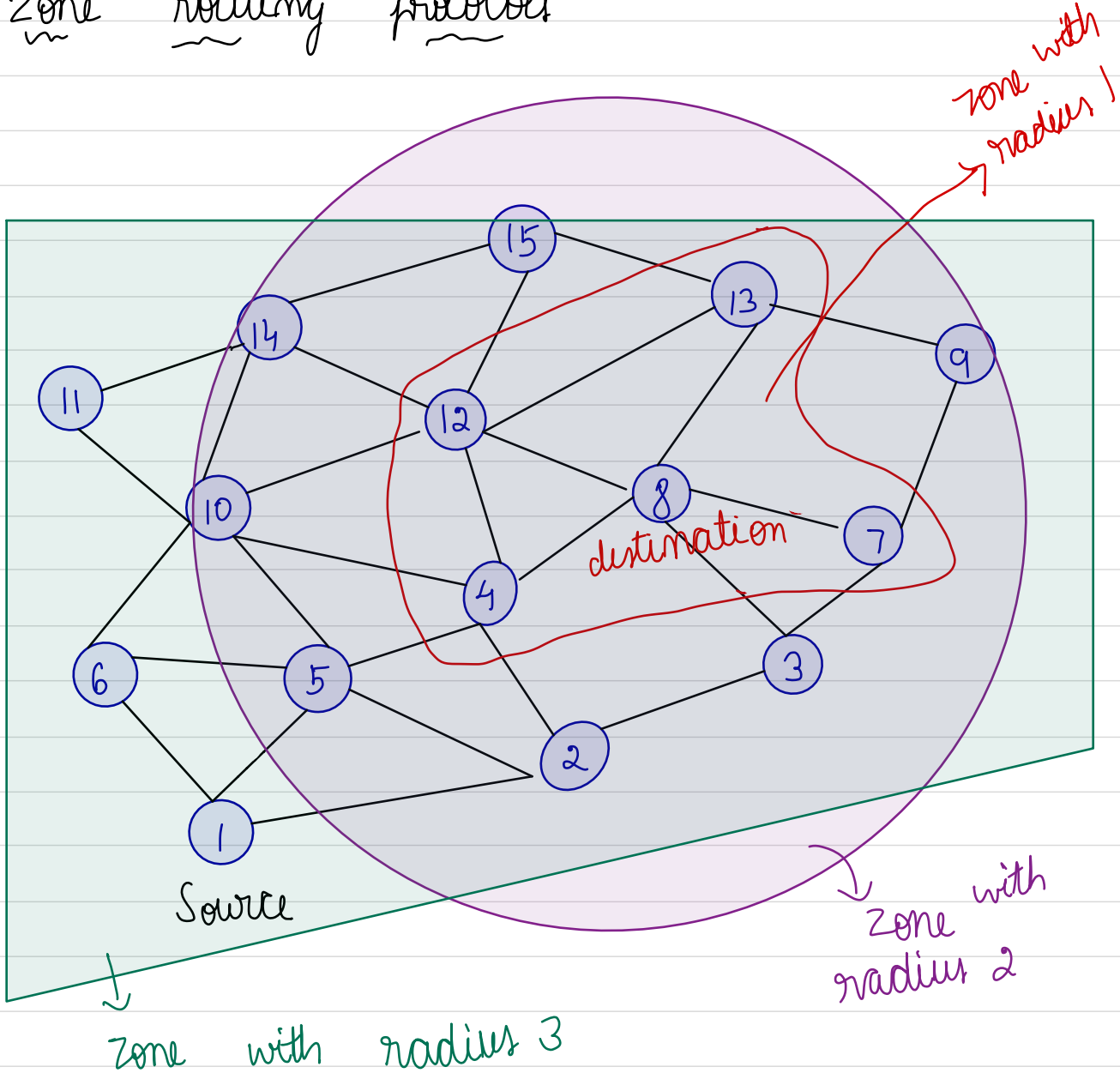
Advantages: 1> Stable routes have higher preference than shorter routes.
2> Fewer path breaks, hence reduced flooding.

Disadvantages: 1> The chosen path may be long.
2> Repeated local query may lead to delay.

In the last figure, the root request reaches destination via 3 different paths:
Path 1: 1 - 5 - 10 - 14 - 15
Path 2: 1 - 5 - 4 - 12 - 15
Path 3: 1 - 2 - 4 - 8 - 13 - 15.
However path 3 is selected as it has higher number of stable links.

Hybrid Routing protocols (HRP)

Zone routing protocols



- In the above example if node 8 is destination then 4, 7, 12, 13 are in the zone with radius 1 (intra-zone)
- Node 2, 3, 5, 9, 10, 14, 15 are in zone 2 with radius 2,
- The route to a destination is determined by identifying the zone; whether it is intra or inter zone.

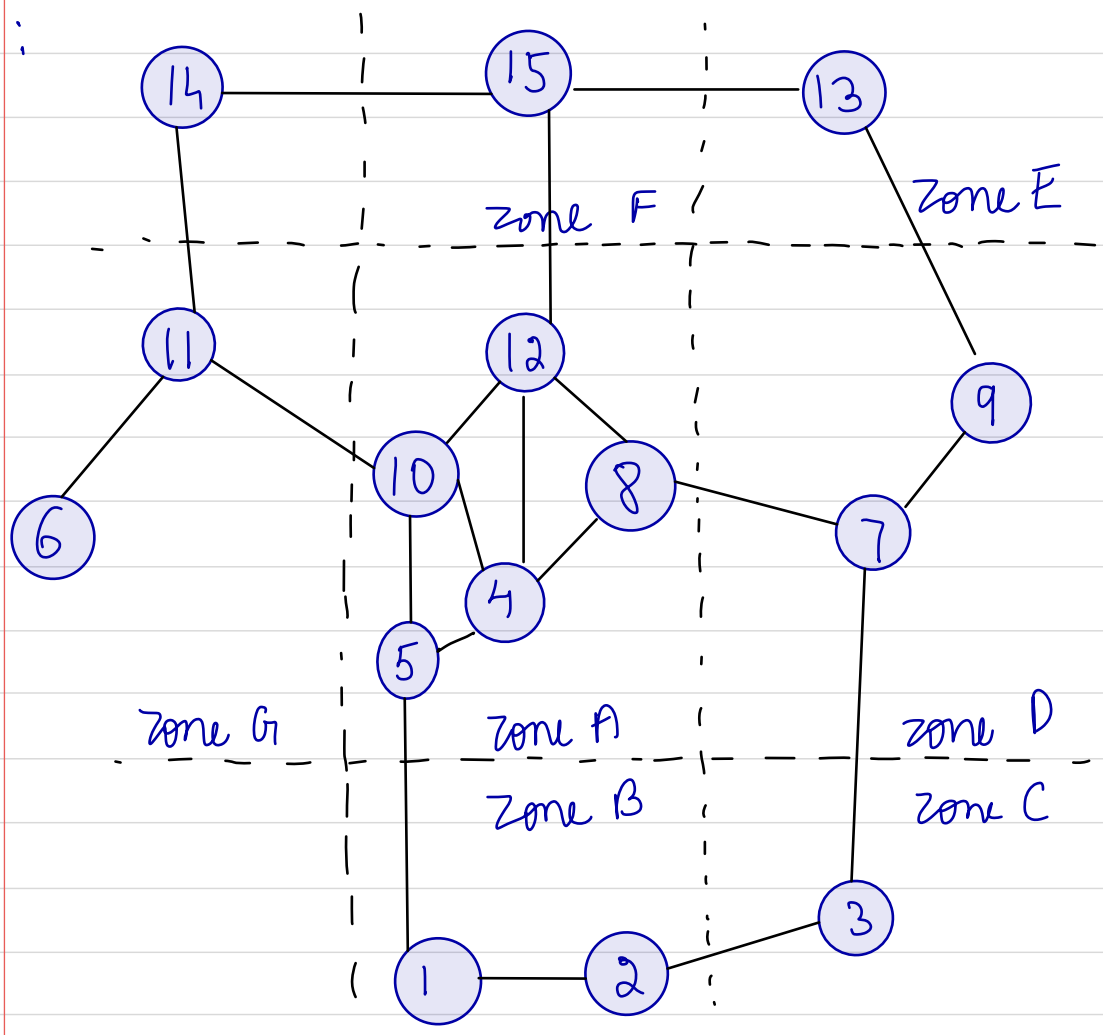
- However if 15 is distination & 8 is the source, 8 broadcasts to all the border nodes in zone 1 to find the destina-tion 15.
- If the distination 15 is not found, the border nodes re-broadcast to the next zone to find distination 15.
- If distination is still not found, re-broadcasting continues until distination is found.
- However in figure nodes 1, 6 & 11 are not in zone 1 or 2 but in zone 3 with radius 3.

Advantages: 1> Combines the best features of proactive & reactive routing.
2> Reduction of control overhead.

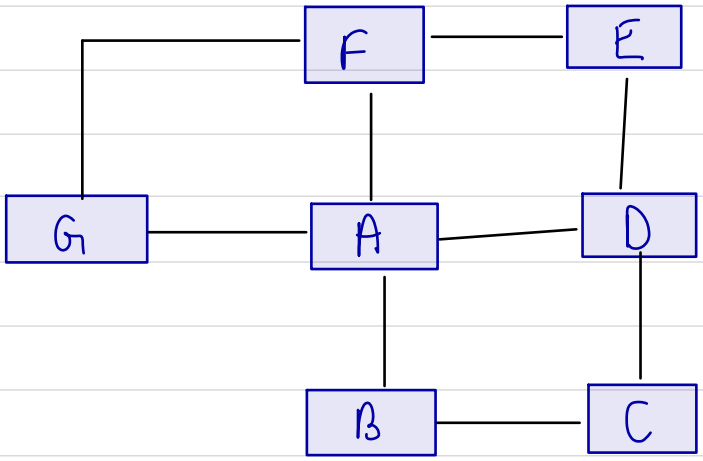
Disadvantages: 1> If zones overlap, then finding distination may be difficult and increase in control overhead.

Zone based hierarchical state routing :

node topology :



zone topology :



Source	Zone link state packet
A	B, D, F, G
B	A, C
C	B, D
D	A, C, E
E	D, F
F	A, E, G
G	A, F

- Uses GIS to form non-overlaping zones.
- Both zone ID & node ID are essential for hirarchical routing.
- Proactive approach for intra zone & reactive approach for inter zone routing is used.
- Every zone has a gateway which is linked to neighbouring zones.

Advantages: 1> Hierarchical approach reduces control overhead & memory requirements
2> Intra zonal changes do not affect the entire network.

Disadvantages: 1> GPS or GIS is a must.
2> The path to distination may be sub optimal.

Issues in designing multicast routing protocol

1) Robustness
2) Packet