Page No.:
Date: 5 | Sept.

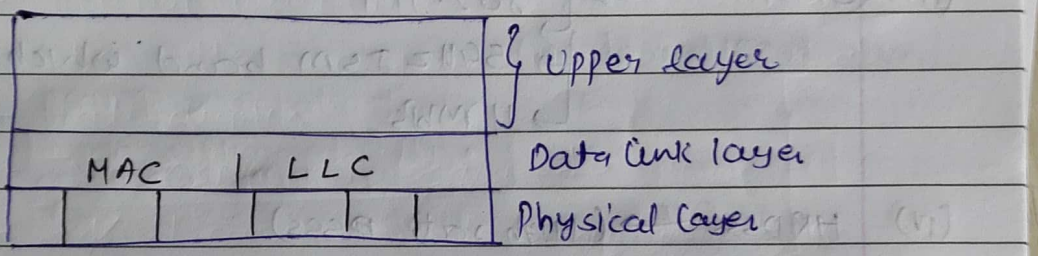
Wireless Communication

802.11 IEEE 802.11 → wifi standard

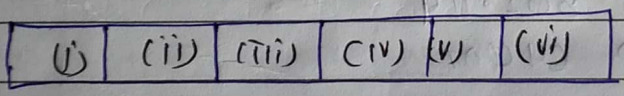
- protocol stack
- frame
- services

Protocol Stack:

- reference model is "OSI model". bcoz of IEEE standard is there.



- only two layer are different for any nw
- physical layer:



infrared → diffuse IR
→ omni directional
→ 1/2 MbPs
→ it can't propagate through walls

(i) DSSS (Direct sequence spread spectrum)
FHSS (freq hoping spread spectrum)
OFDM
→ both are used 2.44 GHz ISM band, which are freely available. we have

faced the High interferenced through many n/w.

(ii) FHSS → 79 channels of 1 MHz wide
- Due to that interference is less.
- Pseudo random seq is used and seed seq is used at Tx and Rx which are same.

(iii) OFDM → 802.11g
→ 5GHz ISM band, which is unlicensed payable
→ 11 Mbps

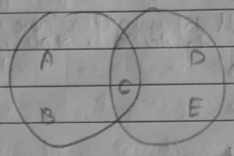
(iv) HRDSSS → (High rate DSSS)
- 1/2/5.5/11 Mbps
→ 802.11g B

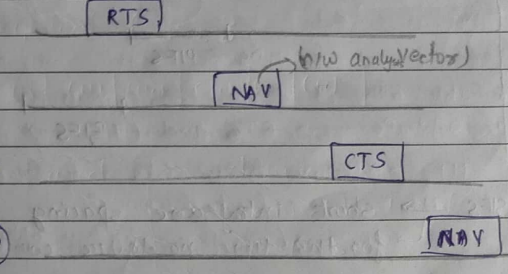
(v) OFDM → at 2.4GHz ISM
→ 802.11g
→ 64 QAM
→ 54 Mbps speed achievable
(With given the max speed of 54 Mbps which used 802.11g → at 2.4GHz ISM band)
└ device are movable

(vi) 802.11M → OFDM + MIMO
→ many links are present each with 54 Mbps ⇒ speed 1Gbps
→ used now a days (2009)

LLC
(logical link control)
- LLC is responsible for the frame conversion blw lower layer to upper layer.
- 802.3 to 802.11 → for data link layer
→ By LLC conversion is there

two mode of comm:
- (i) DCF (Distributed coordination function)
CSMA / CL
- hidden and exposed station are solved



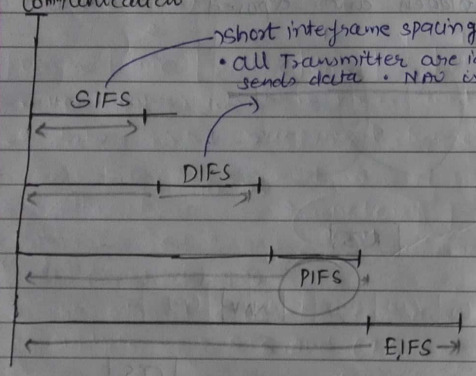


A, D both wants to communicate with 'C'.

NAV → n/w analysis vector
└ contains the info about for how much time A and C will communicate
- direct comm blw nodes.

(ii) PCF (Point coordination function)
- Client server type model
- there should be base station.
- Base station will decide, who is Tx or Rx.
- Ex: - xender (PCF) if one user is send and two or more user receive data than xender → PCF
if b/w two user than xender → DCF

⇒



SIFS → short Interframe spacing
└ for this time no device comm^n present after NAV is over.

DIFS ┬ Distributed Interframe spacing
└ DCF is used

PIFS ┬ Point IFS
├ PCF is used
└ server polls who will Tx/Rx of anyone

wants to do.

EIFS ┬ extended IFS
└ control signal, ack or any extra frame which is left during other spacing (SIFS, DIFS, PIFS) is done then.
- This happens only when both DCF & PCF are present. - This spacing is always present after comm^n gets over.

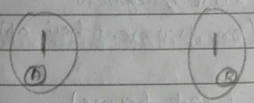
frame :

Byte #	2	2	6	6	6	2	6	0-2312	4
	Control	~~Destination~~ Duration	Ad1	Ad2	Ad3	seq	Ad4	data	CRC

Duration → for generate the NAV, required time is provided into duration.

Ad1, Ad2, Ad3, Ad4 → 4 MAC addr
- in ethernet we are having 2 MAC only for source and destination.

[4 mac addr → 2 addr (customer), 2 addr (Base station)
DCF → 2 MAC addr
PCF → 4 MAC addr)



1 - destination } individual computer
2 - source }

3 - destination } to which tower
4 - source } (central terminal)

- sequence (2B)

  16 → 12 + 4
  - 4 → fragment no.
  - 12 → tells about the frame no.

  0000 0000 0111 1001
  7 frame, 9 fragment no.

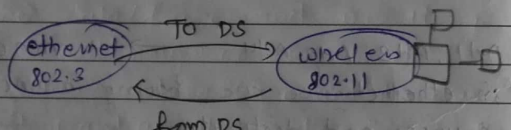
  frame can be divided into fragments and then transmitted.

- control (2B)

bits → 2 2 4 1 1 1 1 1 1 1 1

Version	type	subtype	To DS	From DS	MF	R	Power	MORE	W	O

- version → which version is used
- data, control, managment frame → type



- b/w ethernet & wireless comm is there.
- subtype → RTS and CTS
- MF → more fragments
  - MF = 0 → last fragment
  - MF = 1 → (or fragment hai abhi)
- MORE → 0 (last frame)
  MORE → 1 (more frame are coming)
- Power
  - Power = 1 → sleep mode (for a particular Base station goes to sleep mode)
- W → WEP (wire equivalent privacy)
  - W = 1 encryption is there.
  - W = 0 → normal msg, no encryption is there
- O → order
  - O = 1 → strictly received the data in order
  - O = 0 → data received in any order.

12-Sept

Services:

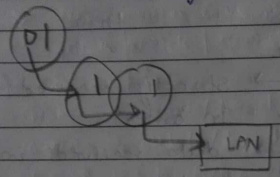
(i) intercell (b/w cells)
(ii) intracell (within the cell)

(i) Intercell:

It provide 5 services in intercells:

* Association
  PC is in the cell but in off state and when it is switched ON → given addr.
* De-association → PC getting power offered and removing from the network
* Re-association → moving from 1 base station to other Base station → w/o switching off the device. • Handshaking.
* Intigration → converting the frame, when distribution is done, eg:- LLC
  - for distribution, integration is important.

* Distribution → if multiple n/w are there whereas we want to send the data, is allowed. Distr of data should be allowed.



• if a device in base station A want to send data to LAN n/w device then it should be allowed.

(ii) Intracell :

* Authetication → if we properly decode the data/frame and are it properly to the Base station then and only we can used the services
• Base station sends a frame and the device has to decode it and ans. it correctly - then only the device is authenticated in that Base station n/w.
* De-authetication → If ans given is wrong by device - then de-authetication takes place.

* Data dilvery → same as distribution within the cell in proper format.

* Privacy → WEP (wire equivalent Privacy)
- provide security to data
- if hacked, then also data is not capable of to be decoded. Eg: WEP

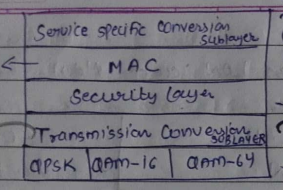
⇒ 802.16 :
Wireless LAN and MAN

802.11	802.16
- LAN ↳ wireless	- Wireless MAN
	- its covered large area.
- 2.4 GHz	- 10 - 66 GHz (Upper ISM Band) (noise interference is very high bcoz f is High)
- error detection	- Error correction/ Deletion
- Mobile (moving devices, we can used this)	- Stationary devices (bcoz data is very large)
- Omnidirectional comm^{n}	- line of sight comm^{n}
- Phy layer → FHSS, OFDM many diff^{t} Phy layer	- FDD, TDD in Physical layer
- DCF, PCF	- PCF
- Ex: wireless LAN - Half & Full Duplex	- Ex: wireless cable n/w - Full Duplex

• Wireless cable n/w is the example of 802.16

Protocol stack :
- layer and work of each layer
- OSI model is used

Upper layers



- QOS ←
- error correction ↓

Physical layer:

- QPSK → 2 bits/baud (for large distance)
  16-QAM → 4 bits/baud
  64-QAM → 8 bit/baud (for small distance)
- Transmission Conversion sublayer → conversion of frame - for data link layer to understand.
  • Haffman error correction is done by Trans. conv. Sublayer
- Security layer → encryption of data is must
  Security - encryption - many algorithms present.
- MAC →
  • it provide the QOS (quality of service)
  (i) Constant bit rate service
  (used for voice comm^n → slot time is fixed so that Bandwidth & data rate is fixed → no one can change if initialization of comm^n is happened)

  (ii) real time bit rate
  • (used for video file)
  • DPCM — only difference b/w frames is sent.
  • change of bit rate is possible with the predefined time
  • During polling → It is asked if bit rate is to be used or not by central terminal during a specific time period.

(iii) Non-Real time bit rate
• Base station may or may not ask for bit rate from
• depends on if BW is available with base station or not
• asks user whenever BW is available ⇒ no specific time fixed

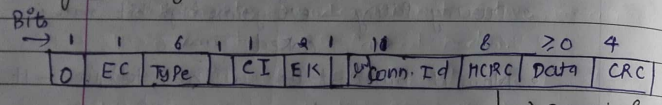
(iv) Base effort
• it available in all the n/ws.
• During Polling — every time high bit rate is asked
• Now if base station is able to give — it gives else not.
• No security of getting high bit rate.

• PCF is used so
MAC — does not has to decide where and when who will transmit.
• Central terminal decides time slots
• FDD, TDD is used → for user & Base station
• full Duplex
• in wifi - half duplex is possible
• MAC does uplink & downlink time division b/w users.

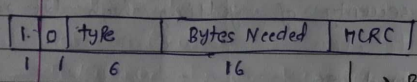
- Service specific convergence sublayer →
  • actual LLC
  • converts the frame into the frame format of data link layer.

- Physical layer provide the frame conversion and also error correction is done at this layer → in 802.16 standard.

frame format :



↳ generic frame



↳ BW request frame when BS asked for more data rate, then this frame has to send by user to Base station (BS).

EC → encrypted msg
can be present or not, mostly absent

type → type of frame (real, non real, informed, supervisor)

HCRC → header CRC
Huffmann coding, for error detection

CI = 1 → CRC is there
CI = 0 → CRC is not there

EK → encryption key

HCRC → used as error correction for header
→ 0 (then no extra CRC for data ~~data~~ present)

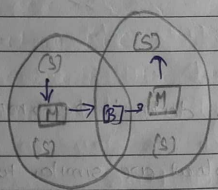
CRC → may be omitted as Huffman code is used

- customer and Base station is always Half duplex.
- HCRC → header CRC → used for 1st (24 bits)
- Byte needed → BW request is been done
- CI → check sum indication

⇒ 802.15.1 Bluetooth

SIG → special interest group
INTEL, TOSHIBA, NOKIA, IBM, ERICSSON

- does something which is not present for themselves
- cheap comm^n w/o wire
- IEEE standardized only two layer data and physical layers for BT.
- So BT is not followed the OSI model.
- range → 10m



- 8 active slave node and 1 master node in the range of 10m

- every 10m BT device having the master node.

- Slave node having the capability to become the master node.
- Two Slave can't comm^n directly, if present in diff Piconel.
- Bridge node b/w two master node.
- Scatter node → more than 10m range

- Park node → nodes are not active, in a Piconel there can be 255 Parked nodes.
- In one Piconet (10m), 255 Parked node is there
- 10m area is called "PICONET"
- Bridge node behaves as master node b/w 2 more nodes of diff Piconel.
- Total nodes present in Piconel - 255 + 8

Services / Profiles :

Slave - client; master -

(1) Generic Access :
is for initially link management.

(2) Service Discovery :
- what kind of device and which are active
- what service is provided by them.

its compulsory in all the cases if present BT application can't perform

(3) Serial Port :
- Through BT, data is transmitted serially. only.
- Serial comm^n protocol are similar to wired serial comm^n

(4) Generic Object Exchange :
- link management - client service model connection done.

Xender → 802.11
Hotspot → 802.11
BT → 802.15.1

- Control and Hand shaking is done. 1, 2, 3, 4 → link management.

(5) LAN
We have to comm^n with the existing n/w as 802.11 or 802.3

(6) FAX
- specially used for FAX.
- similar to modem

(7) Modem
- bT established for modem comm^n
802.11 → modem — then through this device, by BT for internet wifi can be shared.

(8) Telephony
- using BT, we can comm^n via walkie-talkie
- uses very low ISM Band - RF comm^n

(9) Cord-less
using BT, headset and BS are connect

(10) Head Phone
- using BT.
- wireless ear phones, BT speaker etc.

(11) Object Push
for small data is been transferred.

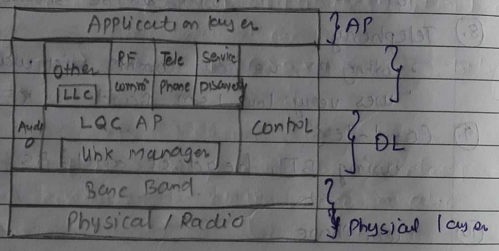
(12) File transfer
for large data is been transferred.

(13) Synchronisation
BT device and stationary device →
Ex: google drive

25-Sep

- it uses stop and wait protocol → speed is very less in BT.
- only changes are updated in the file which are already present in the other device - connection done through BT.
- Required when BT connection gets on and off.
- BT is cheapest comm^n.

⇒ protocol stack & frame format



*Physical radio :

- 2.4 GHz
  79 channels — 1 MHz each
  FHSS is used
  comm^n b/w BS and user occurs.

max. time on which we stay on at a particular frequency → dwell time

- dwell time = 6.5 sec
- 1600 hopping in @ 1 sec

- for 802.11 → dwell time = 400 ms
- a user can hop to other freq. before dwell time but cannot hop after dwell time
- Tx and Rx have to change / hop to simultaneously

*Base band :

- BS initiate the comm^n as user doesn't have power.
  every even slot → BS
  every odd slot → user

→ slots in time

when data is long, then odd no of slots are combined

0, 2, 4, 6 → Base station (Tx in the mobile when BT comm^n is happening)
1, 3, 5, 7 → user end

When we download the data, then 0th slot and 1st slot and 2nd slot can be used by the user for long data transmission.

- if data to be send is long and BS requires more no. of slots then it uses 0th slot taken 1st slot and as 2nd is of BS ⇒ BS can use 0, 1, 2 slots.
- similarly 0, 1, 2, 3, 4 slots for longer frame
- if 0, 1, 2 slots — 2nd is not needed by BS then it goes waste but not given to users

- 625 µs ⟶ 1 Mbps speed

625 bits

BS ——— end user

Settling time = 260 µs

625
- 259
366 → bits

126 ⟶ Header

240 bits

For longer frame → as 5 slots

(Header) 126 bits + 259 bits (setting time) are only required for once

long data ⟶ 240 bits + 625 × 4 = ____ bits can be Tx

* when slot is change and hop is changes (Tx and Rx changes) → then everytime settling time is also changes

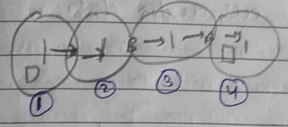
(when both device hop and changing the role (Tx and Rx))

- Only in hop (once we sync the Tx and Rx) we don't required settling time again and again.

- Service provided by Bcne station →
  - Connection less (Asynchronous) (ACL)
  - Connection oriented (synchronous) [SCO]

(bridge node) (based on clock)

SCO → reliable comm, path is pre-defined



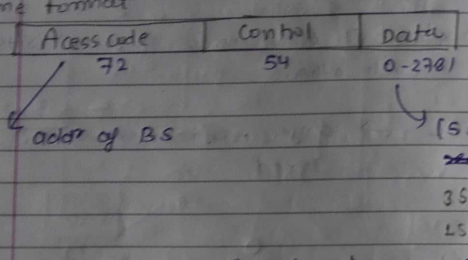
device ① & device ④ → comm with each other.

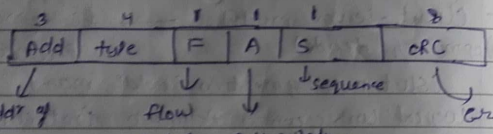
ACL → asyn connection is not fixed.

- Client-server model ⟶ link manager protocol (hoping seq. decide) (slot mandigment or add mam)
- logical link control Adaptation Protocol (L2 CAP)
  - converts the ~~data~~ frame which can understood by uppes layer
  - frames other than control & audio are taken care off.
- Other LLC
  - Bluetooth to other frame conversion as ethernet, wifi
- RF comm & telephony
  - codeless
- service discovery →
  - available service provided by devices which are nearby

Control → control frames
Audio → all audio data

frame format





F = 1 → Rx is ready
F = 0 → " is not ready

A → +ve acknowledgement, when Rx data is correct

S → seq. no., which data is Tx
(Stop & wait are used)

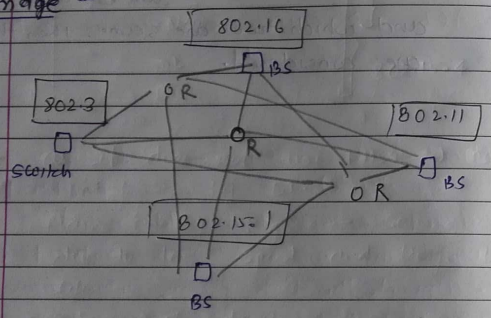
- 18 x 3 = 54
  $x_1\ x_2\ x_3$
  for error detection & error correction $x_1 x_2 x_3$ three time control is transmitted.
  If $x_1 = x_2 = x_3$ → correct data is Rx there is no error
  $x_1 = x_2 \neq x_3$ → then error ~~detection~~ can easily detect
  and which two are same, then they are considered.

Bridge :

- Modem → Physical medium
- Hub → Physical layer
  (its not intelligent device. connecting the all user by star topology, then collision will occurs and its not provide the add°)
- switch → DL layer – works on MAC addr
  intelligent device

- Router — n/w layer
  - many user and multiple path are present for deciding the path.
  - has all OSI layer present in it
  - very intelligent device
  - main algorithm it has — is of routing

- Bridge -



- frame format is different for every n/w then bridge required
- frame conversion is done by bridge
- whole LAN is connected in bridge which in s/w individuals component is connected.
- else act's similar to a s/w.

Ex:- A n/w operating for BT is improvised to provide speed of 2 MbPs. It has a BS wishes to send 9000 bits of data to a device. Then find out the no of slots in the frame.

Sol:-

625 μs ⟶ 2 MbPs

625 × 2 = 1250 bits

Settling time = 260 μs

Header = 126

1250 − 259 − 126 = 865 bits

865 + 1250 × 6.5 = 9000

7

7 + 1 = 8 Slots are required

Bcoz in BT, we are having always odd slots

So Ans. = 9 Slots. Ans.

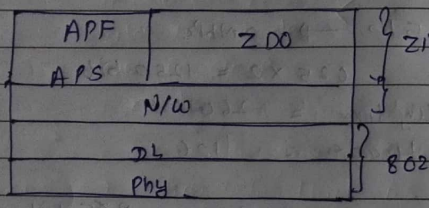
Zigbee:

- 802.15.4
- Physical and data link layers are standardized.
- 2.4 GHz ⟶ data rate (data rate is very less, so Power is also less)
- DSSS
- Short range comm (10m)

- physical layer also 3 bands :-

			data rate
(i)	2450 MHz	16 channels → QPSK	250 Kbps
(ii)	915 MHz	10 " → BPSK	40 Kbps
(iii)	868 MHz	1 " → BPSK	20 Kbps

= 27 channels in total.



- as it does not use FHSS ⇒ no interference by BT.
- Main use of zigbee - sensor n/w → due to less speed and large battery life.
- 2 types of device :-

(I) RFD (reduced function device)

(II) FFD (full function device)

RFD → . Sensor nodes where only data is collected.
. does not have all the layers.

FFD → . Base station
. has all the layers
. decides where & when to send
. comm^n to cloud
. 2 types (roles)

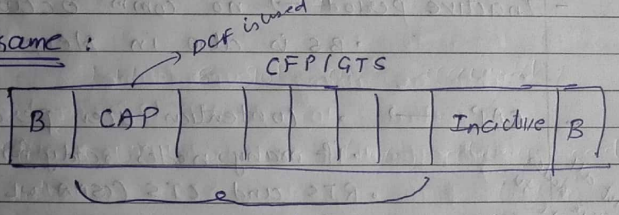
① Router (serve as routing

- RFD
  - ~~reduced func device~~
- FFD → full " "

② PAN coordinator
↓
FFD

- Nodes does not have all the layers so cannot comm^n with each other w/o Base station ⇒ PCF is supported
- Base station comm^n using two methods
  ① Superframe
  ② w/o superframe

Superframe :



B - Beacon

- nodes are in sleep mode normally
- Superframe is generated by BS time to time for node to get to know that BS wanted to communicate or would like to communicate.
- Superframe is gen^r by BS after specific interval

- Nodes comes out of sleep mode → looks for superframe → if not then waits for superframe

node in active mode till superframe is there → if no emergency data, then node goes in sleep mode

- Becon → • has info that BS wants to communicate
  • is a frame gen^{r} by BS
- Inactive period → no comm^{n} occurs
  • BS is also in sleep mode.
- CAP → • contention acen period
  • if many nodes ready for comm^{n}
  • RTS and CTS (CSMA/WL) is used for comm^{n}

(not all active nodes are able to comm^{n})

- CFP → • contention free period
  • BS itself gives time slot for energy station (similar to TDMA)

• all active nodes are able to comm^{n}
• BS sends a polling frame to each node → if node does not respond then time is not given.

- GTS → Guaranteed time slot

- W/O superframe:
  • comm^{n} is done through CAP.
  • CSMA/WL is used

frame

W/O superframe — frame is called as "Generic frame"

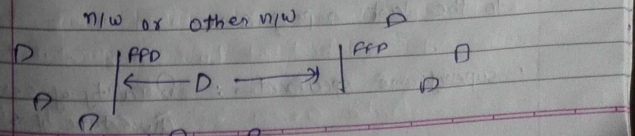
bytes →	1	1	2/8	2	2/8	≥0	4
Control	Seq	Dest PAN ID	Dest Device ID	Source PAN ID	Source Device ID	Data	CRC

• can be of 2 or 8 byte
• initially of 8 byte once set then 2 byte ID is used.

Frame type	SE	FP	ack	Intra PAN	Reserved	Source device mode	Reserved	Dest. device mode

Frame type → RTS/CTS/ack
SE → Security enable. If encryption then 1.
FP → Last frame

- ack — reliable & unreliable comm^{n} possible
  ack = 1 ack = 0
  ack is req to be sent by Rx
- intra PAN — BS gets to know whether node is in n/w or other n/w

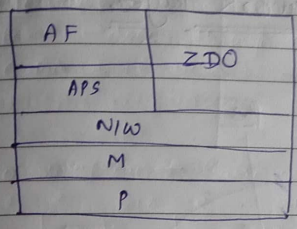


- RFD, FFD, FFD routes → device is in which mode → present in source/Dest. device mode.

byte →

2	1	4/10	8	Var.	Var.	Var.	0
Control	Seq.	Addr	Superframe Spec	GTS	Pending Addr	Data	MIC

- Beacon frame (similar to Generic frame)
  - ↓ Seq. of frame
- in generic frame we have four addr
  - 8 — DD (Destination Device)
  - 2 — D PAN
  - 8 — SD (Source device)
  - 2 — S PAN (Source PAN coordinator).
- when we are using superframe in initial 10 byte addr (2 PAN coord. & 8 DD) and after that 4 byte addr is required
- GTS tells the slot, in which comm^n is done or user has provided for the comm^n.
- Pending addr → in sleep mode, if data is sent and due to sleep mode, that's not Rx. So in pending addr that's tell which device does not respond to the last superframe.
- superframe specification: Quality of service gives type of superframe



* NIW layer → routing, if area is large

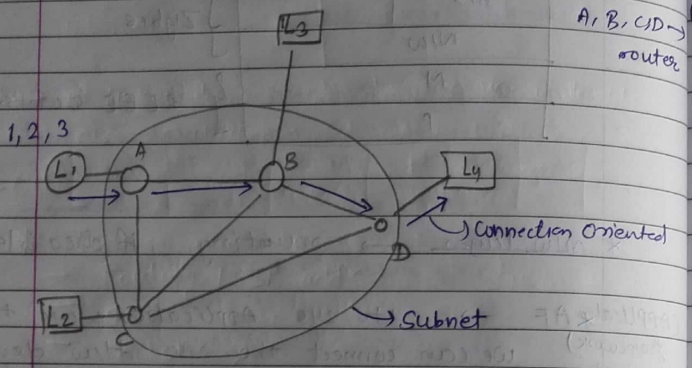
* AF → 1 to 240 Application's are there (Application framework) we can connect the 240 H/w device with zigbee. and every H/w having diff^t-2 applications.

* ZDO → (Zigbee device object) information is stored about which nodes are comm^n each other
  - protocol specification service etc about the H/w or device is present in ZDO.

* APS → (Application Sublayer)
  - provide service through which ZDO & AF can communication.

Page No.:
Date: 5 Oct 20

Network layer



- connection b/w routers → Subnet
- Subnet can be connection oriented (CO) and connection less (CL)
- if L_1 wants to sent data 1, 2, 3 to L_4 L_1 send the request to A → B → D → L_4 and then data is sent that's connection oriented.
- Virtual ckt subnet → which uses the CO
- in connectionless, path is not fixed. at the time of transmission of data, router will decide the path as either A send to B or C.
- in CL, there is possibility that data is not reached at L_4. bcoz data is in b/w A to D.

Data Gram → Connectionless

Page No.:
Date:

	Data - Gram	Virtual Circuit
① Addr state	- less	- large data in frame
② Link	- more data required all the addr of link has to saved	- less data required Addr of specific link is to be saved
③ Router failing	- not effected	- effected
④ speed	- (when data is less then it may preferable)	- (when data is large then speed is high bcoz we have to consider the link making time)

- Every router having the tables in which they have information about the when they are connected or not. → (immediate router data is saved)

① - In Data gram we are considered only the destination frame but in Virtual ckt ~~all~~ complete Path have to consider so large data in frame → VC

② - VC link is decided, so less data but in Datagram more data is required as all the addr of link has to saved.
no of router through which data passes is High in Data gram and less in VC.

④ - depending on the data and no. of user's, speed may varies so we can't say anything.

⑤ Order	not in order	Data is ~~not~~ in order
	less reliable	more reliable

Page No.:
Date: 9/10/20

Congestion control	X	✓
QOS	QOS changes router to router	QOS same throughout the path.

- If link is to remembered the VC is better else Datagram

9-Oct

* Task of nw layer:
  - Routing / IP addr
  - QOS
  - Packetizing

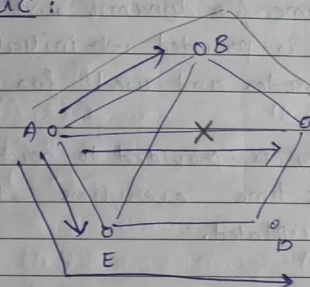
Routing Algorithm:

- deciding a path for Packets b/w two routers
- features of algorithm:-
  - optimality (the result it is provide that's optimum in all the aspects as BW, speed, delay etc.)
  - ~~conversion~~ convergence (it should reach to equilibrium state)
  - Security
  - Stability (it should be stable, after stability router reach to convergence)
  - fairness (it should not be biased, ex: should not choose Fiber optic path everytime - it should depends on situation)
  - Simplicity

Page No.:
Date: / /

- Router Types:-
  - Static / non-adaptive (no of cables, BW, no. of devices and traffic) — routing table — simple and fast
  - Dynamic / Adaptive

(i) Static:



- taking source and table is stored on that node already on papers

- routing tables are fixed, non-adaptive
- while making nw on paper and decide the routing table
- the shortest path, least cost of path etc, all parameter are considered.
- if any link breaks then the other path is not used unless it is programmed again
- does not considered traffic on path.

(ii) Dynamic:

- path changes depending upon situation during run time.
- Considered traffic on path.
- Adv:- when router is fails, then path changes automatically
  - QOS is better than static
  - updating time is required ⇒ slow compared to static
  - complex compared to static

- In dynamic, tables at nodes gets updated after specific time automatically while in static it is done manually ⇒ lines get added or deleted manually in static ~~and used for~~ while automatically in dynamic

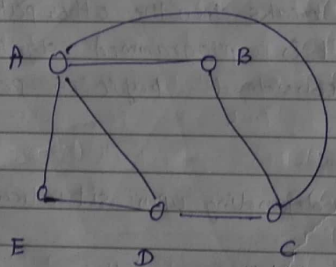
- Algo are same for dynamic and static

Static – data is provided ~~or~~ initially - tables are made at nodes and used for all comm.

dynamic – data is provided to routers after specific time everytime – thus tables gets updated.

Data – speed, physical distance b/w nodes, B.W, congestion, delay

(A) Flooding:



- A packet is generated and then the packet is broadcasted to everyone – the addr of nodes which broadcasted and through which nodes it passed through – all these data is collected – and then routing path is decided.

Eg:- A's packet broadcasted — B, E, D, C received

- all Parameters/data is collected. — they broadcast their packet and as packet

- Repeation of broadcasted packets ⇒ thus causing congestion.

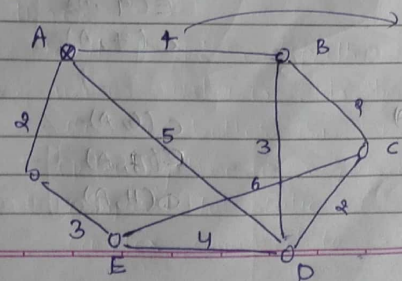
Eg:- 'A' will gets its own packet again & again till the algo stops and 'A' will broadcast its packet again ⇒ congestion occurs.

(B) Selective Flooding:

In this B takes care that A's packet is not sent to A by B again.

Shortest Path:

Shortest path may be in terms of any as phy. shortest path, max. speed, delay, cost no. of nodes connected to router.



– A — C
↓ ↓
source Destination

- We have to set the parmanent node and temporary node.
- permanent node is source node.

P	T
A(–, A)	~~F(2, A)~~
	B(4, A)
	D(5, A)

shortest will become next Permanent node

F(2, A)	~~B(4, A)~~
	D(5, A)
	E(3, A)

shortest B(4, A)

B(4, A)	→ D(5, A)
	E(5, A)
	C(6, A)
	→ D(7, A)

in b/w D & E, we have to selected that permanent node which becomes first

(→ this will also cancel b/c it's short)

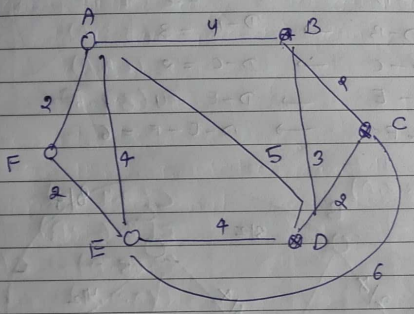
D(5, A)	~~E(5, A)~~
	C(6, A)
	~~E(9, A)~~
	C(7, A)

E(5, A)	~~C(6, A)~~
	E(7, A)
	C(11, A)

C(6, A)

* A → B = A – B = 4
A → C = A – B – C = 6
A → D = A – D = 5
A → E = A – F – E = 5
A → F = A – F = 2

⇒



Source D

P	T
D(–, D)	~~C(2, D)~~
	A(5, D)
	B(3, D)
	E(4, D)

C(2, D)	A(5, D)
	E(4, D)
	~~B(3, D)~~
	~~E(8, D)~~

B(4, D)

B(3, D)	A(5, D)
	E(8, D)
	~~E(4, D)~~
	A(7, D)

P T

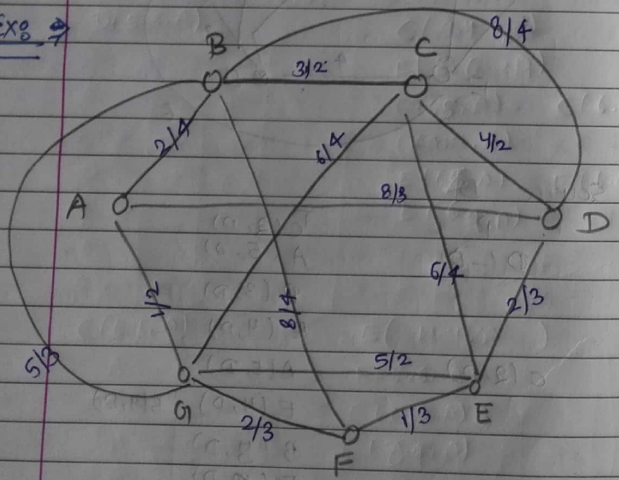
E(4, D) A(5, D) A(7, B) A(8, E)
F(6, E)

A(5, D) F(6, E)
F(7, A)

F(6, E)

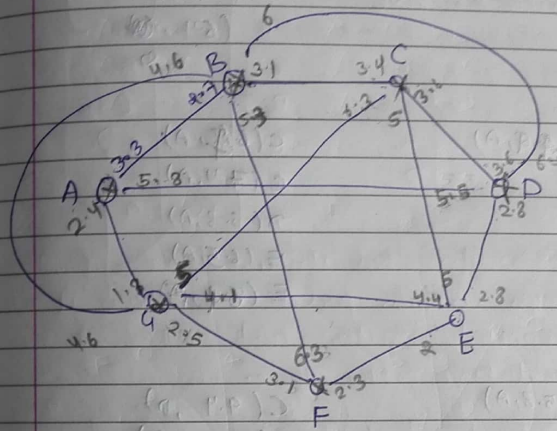
D − A ⟶ D − A = 5
D − B ⟶ D − B = 3
D − C ⟶ D − C = 9
D − E ⟶ D − E = 4
D − F ⟶ D − E − F = 6

Exp 7



* = PD/speed
PD → Physical distance

Cost = 0.5 (PD) + 0.2 (speed in m/s)
+ 0.3 (no. of Router Destination is connected)



A − B = 0.5 (2) + 0.2 (4) + 0.3 (5)
= 3.3

B − A = 0.5 (2) + 0.2 (4) + 0.3 (3)
= 2.7

A − G = 0.5 (4) + 0.2 (2.4) + 0.3 (3)
= 2.9

Source
A

P
A(−, A)

G(2.4, A)

T
B(3.3, A)
G(2.4, A)
D(5.8, A)
B(3.3, A) F(4.9, G)
D(5.8, A) C(7.4, G)
B(7, G) E(6.5, G)

B(3.3, A)

C(7.4, ~~6~~)
D(5.8, A)
E(6.~~5~~, ~~A~~)
F(~~5.9~~, ~~A~~)
~~F(9, A)~~
C (6.4, ~~A~~)

F(~~5.9~~, A)

C(6~~.5~~, A)
C(7.4, A)
~~D(5.8, A)~~
E (6.5, A)
E (~~8.9~~, ~~A~~)

D(5.8, A)

~~C(9.4, D)~~
E[8.6, A)
~~C(6.5, A)~~ C(6.~~5~~, A)
C(7.4, A)
~~E(6.5, A)~~ E(6.5, A)
E(~~8~~.9, A)

C(6.4, A)

E(11.4, A)
E(8.6, A)
E(6.5, A)
E(~~8.9~~, A)

E(6.5, A)

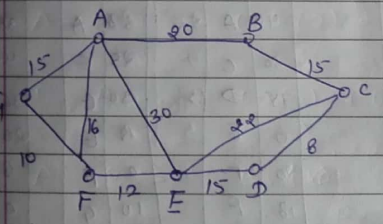
A — G → A — G = 2.4
A — B → A — B = 3.3
A — F → A — G — F = ~~5.8~~ 4.9
A — D → A — D = 5.8
A — C → A — B — C = 6.4
A — E → A — G — E = 6.5

30-Octo

© Dynamic Routing Algorithm :

Two main routing algorithm :
(I) distance vector
(II) link state

(i) Distance Vector :



Every router has its own table which has a distance vector (contains delay, cost, Bw etc. parameters)

Eg:- A's table

A	0	A
B	20	B
C	35	B
D	60	E
G	50	G
F	72	D
G	40	A

→ (not acc to diagram)

This table gets modified after a pre-defined time.

- every router generates packets.

Router A's table

A	0	–
B	20	B
C	35	B
D	45	E
E	30	E
F	26	F
G	15	G

- Each router has its own table - for this it design its own packet and shares it with connected routers and others to calculate the distance blw them.

B

A	18	A
B	0	B
C	12	C
D	98	C
E	35	C
F	36	A
G	30	A

E

30	E	
40	A	
20	C	
15	D	
0	E	
20	F	
18	F	

F

18	A	
38	A	
25	E	
30	E	
15	E	
0	F	
10	G	

G

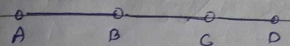
17	A	
35	A	
45	F	
36	F	
20	F	
8	F	
0	G	

A → E = 28
A → B = 18
A → G = 12
A → F = 14

A

A	0	–
B	18	B
C	12	B
D	43	E
E	28	E
F	14	F
G	12	G

Problems – practically routers are not aware about geographical connections blw them.

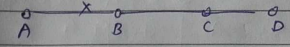


– – – } when A is not connected then distance = 0

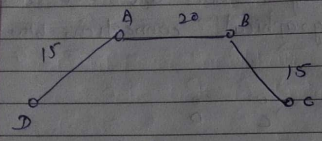
1 – – }
1 2 – } when A is connected to
1 2 3 } the S/S
– 1 2 3 → when A is not working and it stops

– 1 2 3
1 2 3
3 2 3
3 4 3
5 4 3
5 4 5
5 6 5
7 6 7

This is known as count to infinite. It occurs bcz the router is unware about the link of its neighbouring routers.



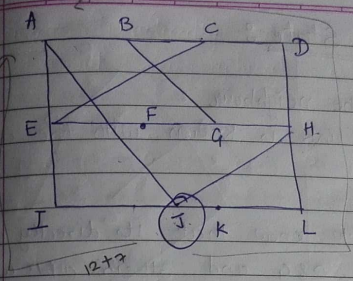
A	B	C
B 1 B	C 1 C	B 1 B
C 2 B	D 2 C	D 2 D
D 3 B	A 4 C	A 3 B
		A 5 B



	A		B		D	
A	0	A	20	A	15	A
B	20	B	0	B	35	A
C	35	B	15	C	50	B
D	15	D	35	A	0	D

When D is not working, only A is aware about it. If ~~the~~ D's table is removed, then A's modified table is :-

	A		B	
A	0	A	20	A
B	20	B	0	B
C	35	B	15	C
D	55	B	35	A



JA - 8
JH - 10
JI - 12
JK - 6

node J

12+7

	A's	J's			I	H	K
A	0	8	A	L	33	9	9
B	12	20	A	A	24	20	21
C	25	29	H	B	36	31	28
D	40	18	H	C	18	19	36
E	14	19	I	D	27	8	24
F	23	29	H	E	7	30	22
G	18	16	H	F	20	19	40
H	17	10	H	G	31	6	31
I	21	12	I	H	20	0	19
J	9	0	J	I	0	14	22
K	24	6	K	J	11	7	10
L	29	15	K	K	22	22	0

Create the table for J !

	A	I	H	K
J	8	12	10	6
B	12	36	31	28
	+ 20	46	41	24
C	25	18	19	36
G	18	31	6	31
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40

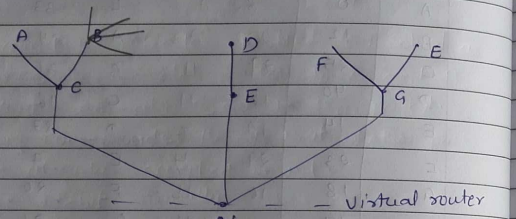
A to B & B to A links are not same they either be fiber link or ~~twisted~~ pair

(10) Link Table State :

(i) Identify the neighbour :

- the whole link is known with the cost values.
-

C is come to know that its directly connected to A, B, D & G and their addr will stored in the table.



(ii) Find out cost :

- cost is dependant on the delay
- (a) with load
  (b) without load

there would be two ~~load~~ ways to find the delay b/w the nodes, by sending the packets.

(a) without load

└ in this if cost of C to B Path is to be found — then the router connected to B, their effect is not been considered in that path.

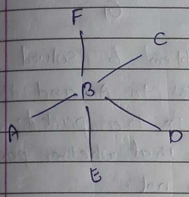
└ so to find cost, C would send packet to B and get the cost.

└ in w/o load cost is not exactly found

└ ideal condition.

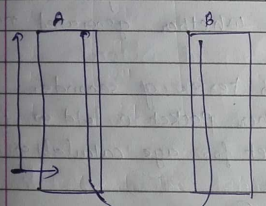
(b) with load

└ in this the other connected nodes to B are also considered at C for cost calculations.



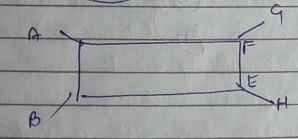
To find A-B cost with load — queuing time and propagation time at A and B are calculated using a time and then at the end queuing time are removed.

— in w/o load queuing time is not removed.



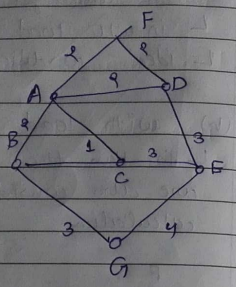
w/o load → ideal condition

with load → oscillations occur



(iii)

A	
Sequence	
age	
B	2
C	1
D	9
F	2



- count to infinite problem is solved as here the connected routers to A and their cost are also sent in the packet.
- Seq. no. – provides the info that whether packet is already accepted or not.
  - 32-bit normally
  - also provides whether the packet is old or new – i.e, whether generated now or before.
- Age – given in terms of seconds.
  - provides whether packet is old or new.
  - a time is set for age calculation of packet.

(iv) Distribution
- Using selective flooding each packet is sent to each router.
- wherein, the packet is not sent to router from where it is received.

(v) Shortest Path

Congestion Control:

(• Buffer size, speed)

- Congestion happens in the subnet where router and their connection b/w router is there.
- Congestion – means traffic – data is not lost but the speed ↓ ses.

-(i) Slow Processor
-(ii) Slow Lines – EOC
-(iii) Buffer Size - more data, less size or has filled caused cong.
- Congestion reduced by:
  - increase the queque length (↑ed the memory) due to memory ↑ed congestion ↑ed bcoz
  - speed of Processor ↑ed

- How to reduce/decrease congestion:
  - Use High end processor and high BW length cable
  - ↑se queque length (memory) - does not ↓se congestion impact ↑se it bcoz if memory is large then routers would save it to the last packet would take greater time to get transmitted ⇒ time out may occur at receiver and transmitter
    ∴ we may ↑se time out which is not preffered ⇒ speed ↓ ses.

Hence, Improving hardware resources doesn't use congestion.

- Flow control is only at transmitter and receiver.
- Congestion is independent of flow control as it occurs due to all the other parameters of the n/w, Tx & Rx.

Congestion Control

Open loop	Closed loop
• Tx decide how to send the data but there is no guarantee that congestion gets controlled	• presence of feedback - congestion is controlled.

At Data Link layer —

① Selective repeat Protocol
② Time out policy
③ Error control — correction gives better congestion control compared to error detection while detection would cause re-transmission of data but correction would require greater overheads (tradeoff)
④ Acknowledgement
L piggy Backing
different frame for ack is not required.

At Network layer —

① Packet size
② Routing Algorithm
flooding - uses congestion
③ Aging
④ Discard Policies

Milk	Wine
- newer the packet better it is	- older the packet more important
- possibility of errors as depends on older packet	- possibility of time out

same policies at transport layer as for data link layer — D_L is for packets
T_L is for segments

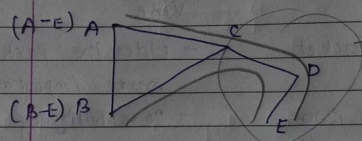
Close loop:

(I) No of repeated packets — if Yes ⇒ there is congestion occuring.
(II) delay of packets Yes
(III) Queue limits — if a packet takes a lot of time to get out of queue.
— no. of packets in the queue are Yes
(IV) No. of discarding packets →
(present due to any kind of packet data or audio)

All these shows congestion is occuring.

(1) Virtual Circuit:

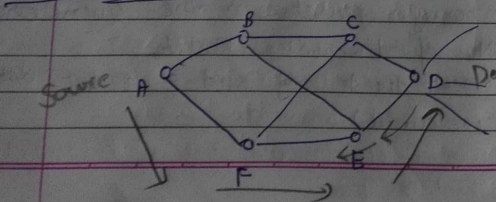
- Fixed Path



→ Part of both ckt
⇒ congestion may occur.

- admission control – do not allow new VC path to use it so that congestion occur.
  - if a node has single VC then it has to wait for a long time
  - telling others that the data is using only 1 MbPs and others can use 9 MbPs BW of cable – resource allocation.
- A node should have multiple VC Paths.
- its not used in datagram subnet.

Datagram Subnet:



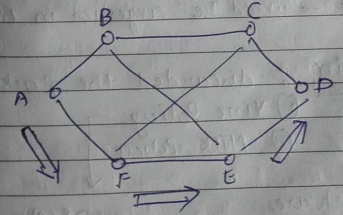
- if congestion b/w E & D happens ∴ A Tx the data to D and D feels that there is congestion.

* Warning Bit → D sends the 1 bit to A, and A comes to that line is congested But A don't know to know that either D itself (D's queue) is congested or line is congested. So A start to reduced the data rate, so that congestion can reduced.

- even if we get the warning ~~that~~ bit but that not reaches to A immediatly So it taken some time. So A can't respond to warning bit get immediately. So there should congestion is there. So A Tx the data at High rate
- Warning bit is ~~the~~ ack, when reverse frame is Tx.

* choke Packet →

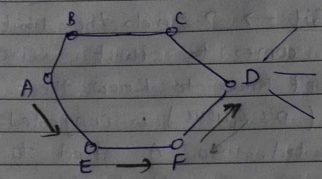
- D gen the choke Packet and transmit to A at the same time. and A reduced the data rate and congestion can reduced.



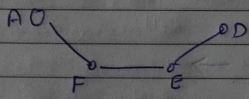
after predefined time A Inc the data rate where A comes to know that, there is no congestion.

* Hop-hop choke Packet →

at every router reduced the data rate



- path is changed whenever path is congested not the router. if router is also congested then path changed is not the solution.
- problem of delay for 1st choke packet to reach A is present ⇒ 'A' sends packets at high speed. So when choke packet reaches E & F then they also reduces their speed.



they won't rely on A to decrease speed.
∴ independent of Rx & Tx
This is called Hip-Hop choke Packet.

- choke packet — would see congestion in line & nodes.

Load Shedding : discarded the packets

① Wine Policy
② Milk Policy

Wine Policy → new Packets are kept and old are discarded

Milk Policy → old Packets are kept and new are discarded.

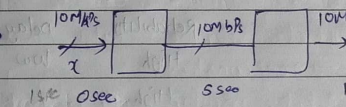
Random early detection (RED):

- Slow down packet rate at Tx
- Rx will discard packets before congestion rises to maximum ⇒ when re-transmission occurs then congestion would be less.

can or cannot be find destination

Jitters Control:

latency →



delay b/w two bits is same, but first bit takes some time to reach the Rx. so that's starting delay is → latency.

- If latency is not constant → jitter delay b/w data is not constant and latency is changes that's known as Jitter.

- the variation in the packet inter-arrival times is called jitter.
- latency is initial time taken by data to reach Rx.
- congestion control is difficult.

Page No.:
Date: 9 | Nov.

- In network layer - timestamps are present with sequence no., flow control, frame no. etc. Time stamp is not present at DL layers.
- Retransmission can be reduced by ~~fitt~~ jitter control & timestamp - by transmitting old packet immediately.
- Timestamp would also provide help to delay the data which is received earlier.

Quality of Service

QOS → Reliability, Delay, jitter & BW

	Reliability	Delay	Jitter	BW
Email	High	low	Low	low
File transfer	High	"	"	Medium
Remote login	High	Medium	Medium	low
Audio on demand	low	low	High	Medium

(Real time data, so reliability is not an issue
Reliability → by error control, data made reliable)
Audio required more Data rate as we required in video.

Video conferencing	Low	High	High	High

- reliability → error correction or detection
trade off would be there bcoz if data is more reliable then delay is also Used and jitter (If error correction → re transmission of data) is also Used.

1 user → One queue
10 different buffer for each user

Techniques for good QOS :

- Overprovisioning
  - (Supply more than demand)
  - In landline (telephone) → example
  - Supply more → Use the queue length of router
    → Buffer size is Used
    → Use the routes capacity

due to these delay is Used on time Used
So sis becomes more reliable but delay is Used → so tradeoff b/w reliable & delay
(congestion and time out problem will occur due to router cap. is Used → delay Used)

- Buffering
  - flow can be buffered on the receiving side before being delivered.
  - does not affect the BW and reliability
  - Used the delay
  - if buffer size is increases → delay is Used than timeout would be there and more buffer size expense more.
  - audio and video on hand → buffering is ~~more~~ important.

- Traffic shaping
  - Traffic shaping is about regulating the rate of data transmission.
  - at Tx side Buffer size, delay is considered
  - Service level agreement → Virtual circuit kind of comm" than provide or agree to the services
  - it reduces the congestion

Leaky Bucket :
- at Tx side
- If we don't used the VC, then leaky bucket algo is used.

- Bucket, outcome data is same or speed is ~~same~~ / constant
- Bucket, income data is ^speed not constant

- Output flow is constant → static
- Bucket is overflow → then data may discarded which we don't want.

problems

Token Bucket :

If no. of token is there, more data can comes and output flow of data also can there.

If token is full by the same data then more data is not paned into the bucket. So overflow / discard of data is not there.

- no of vacant buffer → no. of token gen"
  ↓
  Packet is stored in the token.

By this we can control the flow of input and output.

- if 1 token = 100 bit, and by seen the data input we have to wait for the token gen" ~~as~~ which we required to store the packet.

Resource Reservation :
- almost same as service level Agreement
- Disad → VC, we have to fixed the path.
- three kinds of resources can potentially be reserved
  - BW
  - Buffer space
  - CPU cycles

Link TDM, high priority interrupt sophisticated router eg.

- Reserved resource processes firstly

Admission control :
- Token bucket size
- " " rate
- by controlling them

Adm" cntrl → How much data is allowed

Proportional Routing :
- datagram subnet
- ~~multipath~~ multiple Path is provided ~~into~~ to ↓ses the congestion and jitter.
- more paths made - data sent by one the paths.

Packet scheduling :
- priority wise allocation
- fair queuing
- By providing the min packet size in byte so that time is not wasted for the small size of data.

- If data size is diff' by each router then data with less size will waste time and BW - so set byte that can be sent in a time

Resource Reservation Protocol (RSVP) :
- Group addr is provided for the nodes (Router) which demand for the same data.
- throughout the path

Differentiated services :
- VC (fixed the path)
① Expedited Packets
② Regular Packets

Expedited forwarding :
- b/w 1 router nearest router to router 1.

Assured forwarding :
- like round robin but with priority.

Network layer

Page No.:
Date: 13 | Nov.

IP Addressing :
- all router works on IP.
- logical addr → also name of IP addr
- IP addr → permanent or non-permanent

- IPV4 → 32 bit addr
they are unique, in the sense that each addr define one and connected to the internet access.
- decimal notation of IPV4
117 . 49 . 29 . 2 } each uses 8 bit for repr in binary
- Classful addressing :

(i) Class-A	2^8 → defined n/w 2^{24} → computers can be connected	(no. of n/ws are not sufficient)
(ii) Class-B	216 → n/w addr 216 → computer addr	(mostly used)
(iii) Class-C	2^{24} → n/w 2^8 → computer	(no. of computers are not sufficient)
(iv) Class-D	all addr are used for either n/w or computers. (multicast addr)	
(v) Class E	[Broadcast → all bits are '1'] reserved for future use.	

- Classless addressing:
use it to decide the n/w and computer IP addr.
- Addr must be contigous
- No. of addr in block must be power of 2.
- 32-bit addr converted into binary decimal must be divisible by no of comp possible.

Subnet mask:
- x.y.z.t/n
↳ n = 5 (subnet mask)
then we can says that 5 bit is for the network addr
& (32-5) bit → compr addr
- The first addr in block can be found setting the rightmost 32-n bits to 0's
- The last " " " " " to 1's.

Class-A
11111111 00000000 00000000 00000000
Subnet n = 8 → n/w addr
} subnet mask

Ex:- IP addr: 1100 1101 0001 0000 0010 0101 0010 0111
Mask 1111 1111 1111 1111 1111 1111 1111 0000
28 bit mask
By anding them, then first addr in blocks
first addr: 0001 0000 0010 0101 0010 0000
1101 1100
first (MSB) last

last 4 bit of is change in finding the first addr.

(i)- To find the last addr
By oring the given addr with the complement of the mask

(ii)- To find the first addr
By anding the given addr with the mask

(iii)- The no of addr can be found by complementing the mask, interpreting it as a decimal no and then added one.

Subnetting:
Ex: suppose an org is given the block 17.12.40.0/26, which contain 64 addr for computers. (32-26 = 6 → 26)
The organization has three offices and needs to divide the addr into three subnet blocks of 32, 16 and 16.

for subblock 1 → 32 addr for computer is required 25 = 32
32-5 = 27 ↳ mask subnet

mask: 1111_1111_1111_1111_1111_1111_1110_0000
first addr: 17.12.40.0/27 → given to the n/w
Last addr: 00010001_00001100_00101000_00011111

So that comp. first addr is
- 17.12.14.1/27 → first
- 17.12.14.31/27 → last

for subblock 2 → comp ⇌ $2^4 = 16$
32-4 = 28 for the n/w

28 mask is used
mask : 11111111 11111111 11111111 11110000
first : 17.12.41.32/28 → for the n/w
17.12.41.33/28 → for first comp of the subblock 2
17.12.41.49/28 → last addr

for subblock 3 →
17.12.41.48/28 → given to n/w
17.12.41.49/28 → given to 1st addr
17.12.41.63/28 → last addr

Page No.:
Date: 16 | Nov.

Internet Control message Protocol (ICMP) :

which is used in the IPV4

- if something error is occurs then it generate the packet which is send to either Tx or Rx (other than flow and congestion control)

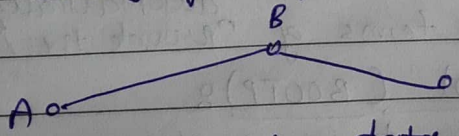
↳ Destination unreachable
- (due to larger size or small size)
- like count to infinite

↳ Time exceeded
- packet is discarded when time become 0 - source should be informed that the packet is discarded
- Happens rarely

↳ Parameter Problem
- header problems
- similar to frame reject (HDLC)

↳ Source quench
- choke Packet which used in congestion
- normally avoided

↳ Redirect
- Teach a router about geography
- changing the path



if B getting the data, which is not related the router which is not connected to directly with B, then B gen' the packet and send to all the sources, which are gen' or sending the data to B.

creation of routing table

- Echo
  - Hello msg for start - telling I'm there.
- Echo reply
  - find how many routers are directly connected.
- Timestamp request
  - similar to echo
  - helps to find the cost.
- Time stamp reply

if we access the internet from the LAN

Address Resolution Protocol (ARP)

- IP addr used for the internet.
- give MAC addr with help of IP addr.
- Eg: Center node (server) knows only IP addr. Then through ARP, MAC addr will be known.

Reverse Addr Resolution Protocol (RARP):

- getting the IP addr from the MAC
- useful in LAN.
- better in terms of automatically provide the IP addr

Bootstrap Protocol (BOOTP):

- better in terms of efficiency.
- IP list with MAC addr is already present so you will surely get IP addr.
- while in RARP free IP addr is given ⇒ sometimes you may not get.

Dynamic Host Configuration Protocol (DHCP)

- automatic
- no local server required
- broadcasting doesnot occur by router
- DHCP relay broadcasts the msg and routers connect through Point-to-Point connection.

⇒ IPV6 Goals

- Support billions of hosts (more no of IP's)
- reduce the routing table size
- security — 40 byte in IPV4 is not sufficient
- And multicasting
- real time QOS
- simplified header
- NAT is not req. bcoz no of IP is high.
- updation in future.

— data in sequence is take care by the transport and data link layer, not by the NW layer.

format —

- flow lable — no seq. present / not in sequence
- 40 byte header is fixed
- next header — can be the size.