IP ADDRESS :-

- IP Address is the identifier used in the network layer to identify each device connected on the internet or network.

- IP Address is 32 bit address.
- IP Address of every machine is unique, no 2 machines can have same IP Address.
- IP Address format is a universal format that has to be accepted by any host who is connected to the Internet.
- IP Address can be denoted in 3 ways :-
  1) Binary Notation — (Base 2 Notations).
  2) Decimal Notation — (Base 256 Notation).
  3) Hexadecimal Notation :- (Base 16 Notation).

In BINARY NOTATION, the address 32 bit is represented by 32 bits in a combination of 0's & 1s.

32 BITS are written in format of 4 octats. After every octates a space is inserted.

Ex :- 11111111 10111111 11111111 00011111

These is also known as 8 BIT NOTATION.

In DECIMAL NOTATION, 4 octates are converted into decimal format & each octate is separated by dot.

Ex :- 128.11.13.14

- It is also known as DOTTED DECIMAL NOTATION.
- It is the main most important notation & used generally.

In HEXADECIMAL NOTATION, the group of 4 bits are made & are converted in notation (0-9 & A-F).

$(2AF3)_{16}$

- Rarely used even in numericals.

ADDRESS SPACE :-

It is the total number of addresses used by protocol.

If the protocol uses n bits to define address then total address space is 2^n.

IPV4 → 2^{32} ~~bit~~ addresses

= 4,294,967,296 addresses

HOW TO FIND TOTAL ADDRESSES IN THE NETWORK :-

Q) Find the no. of addresses in the range for the network whose the first address of the network is 146.102.29.0 & last address of network is 146.102.32.255.

STEPS

1.) Subtract last address with the first address.

RESULT :- 0.0.3.255

2.) Convert the result to the decimal format i.e. base 256 & add 1 to the final result.

$3\ 2\ 1\ 0$

$0.0.3.255$

$(0 \times 256^3) + (0 \times 256^2) + (3 \times 256^1) + (255 \times 256^0)$

$= 3 \times 256 + 255$

$= 768 + 255$

$= 1023 + 1 = \underline{1024 \text{ addresses}}$

Q.) If the first address of the network is 14.11.45.96 & the total number of addresses in the network are 32. Find the last address in the network.

Ans) STEPS :-

1.) Convert the total no. of addresses in base 256.

2.) Minus 1.

$32-1 = 31$

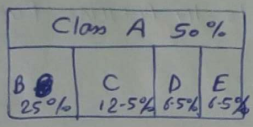
0.0.0.32

IPv4 ADDRESS

- Classful
- Classless

CLASSFUL IP ADDRESSING

In this, IP Addressing is divided into 5 classes :-



Class A covers 50% of the total address space

$= 2^{31}$ addresses.

$= 2,147,483,648$

(2^{32})

To recognize class of an address :-

~~For~~ only 1st octate is used.

→ First octate.

~~as in class A, 31 bits are free~~

	First byte	Second byte	Third byte	Fourth byte	Address space
Class A	0-------	- - - -	- - - -	- - - -	$= 2^{31}$
Class B	10------	- - - -	- - - -	- - - -	
Class C	110-----	- - - -	- - - -	- - - -	
Class D	1110----	- - - -	- - - -	- - - -	
Class E	1111----	- - - -	- - - -	- - - -	

~~Class A~~	Address space
Class A	2^{31} → as 31 bits are unoccupied in above table
Class B	$2^{30} = 1,013,741,824$ → (have to write in paper).
Class C	$2^{29} = 536,870,912$
Class D	$2^{28} = 268,435,456$
Class E	$2^{28} = 268,435,456$

Q.) How you can prove that we have 2,147,483,648 addresses are available in Class A?

Ans) Total address space of IPv4 protocol = 2^{32}

If 1 bit is reserved for class A.

So, 31 bit are unoccupied.

Hence, 2^{31} = 2,147,483,648 addresses are available in Class A.

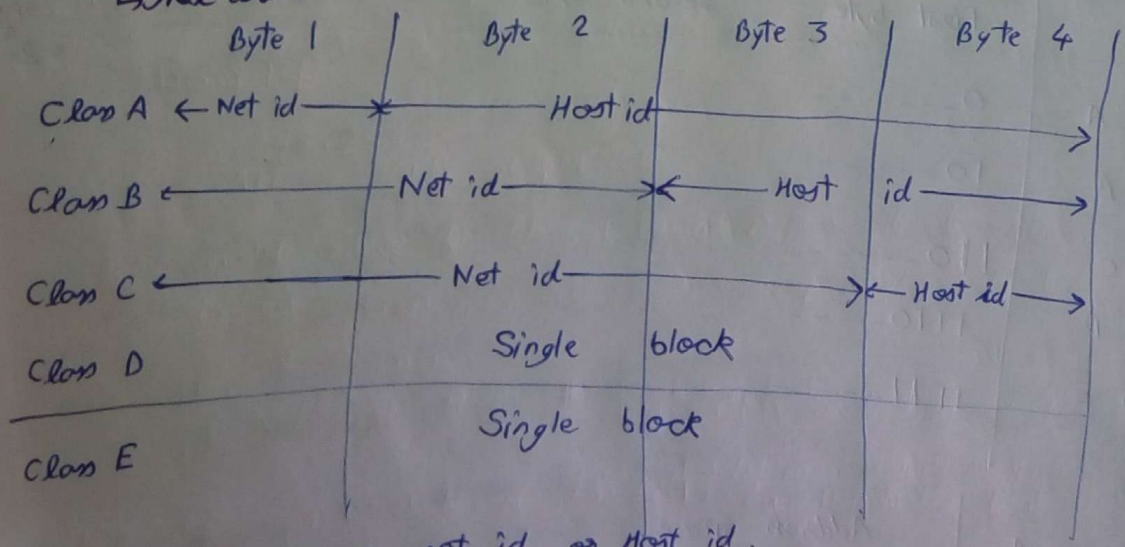
TO IDENTIFY THE CLASS IF ADDRESS IS IN DECIMAL FORMAT

	First byte
Class A	0-127
Class B	128-191
Class C	192-223
Class D	224-239
Class E	240-255

NET id & HOST id

Network id — to identify host

↳ these are n bits.



- In class D & E no net id or Host id.
- As D provides multicasting (~~multi~~ to provide multiple users).
- E is reserved ~~for~~ for future use.
- Here each class is sub-divided into blocks & each block has fixed size.

Q) 200.11.8.45

i) Create 32 subnets

ii) First & last address of first subnet

iii) First & last address of last subnet

iv) Divide first subnet in 2 subnets.

~~CLASSLESS A~~

SUPERNETTING:-

- Combine many blocks to form a single block.
- No of hosts inc. whereas in subnet no of hosts dec.

$n = 24$

→ Combine 8 sub-blocks in 1 super block

3 bits are required.

$x = 3$

Here $n = n - x$

$n = 24 - 3 = 21$

$32 - (n-x) = 11$

2^{11} hosts

Q) SUBNET

$n = 24$

$x = 3$

$n = n + x = 24 + 3 = 27$

$32 - (n+x) = 5$

2^5 hosts

CLASSLESS ADDRESSING

→ In classful addressing, lots of addresses are wasted.

→ All the blocks can have variable length. e.g. 32 bits → $2^0 - 2^{32}$ addresses

→ Here prefix is same as net id

→ suffix is same as host id.

→

→ prefix = n

suffix = 32-n.

prefix	Suffix
n	(32-n)

Q) What is the prefix & suffix length if the whole network is divided in a single block.

→ Prefix length = 0, Suffix length = 32. Total Addresses = $N = 2^{32}$

→ Here addresses are represented by SLASH NOTATION / CIDR (Classless Inter-domain routing)

byte . byte . byte . byte / n

Q) Find the block length if one of the address ~~230.84.~~ in the block is given as 230.84.56.6/16.

Ans) n = 16

32 - n = 16.

STARTING ADDRESS :-

1) Keep n left most bit as it is.
2) Rest i.e. 32-n, set 32-n rightmost bits 0.

So first address of block :- 230.84.0.0/16.

LAST ADDRESS :-

1) Keep n leftmost bit as it is.
2) Set 32-n rightmost bit 1.

So 230.84.255.255/16.

Q) Find the block length if one of the address in block is 230.84.56.6/20.

Ans)

n = 20

32 - n = 12

first address :- 230.84.48.0/20

last address :- 230.84.63.255/20

AF

ROUTING ALGORITHMS :-

1) First we create graph of internet. (weighted graph).

CONCEPT TO EVALUATE WEIGHTED GRAPHS :-

- Least Cost Routing

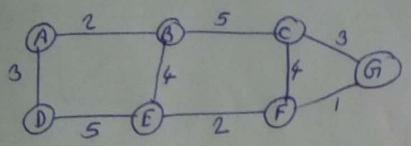
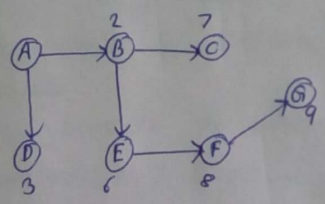


Fig 1

Convert it to LEAST COST TREES.

ALGORITHMS :- 1) DISTANCE VECTOR ROUTING -

We find the best route by creating the least cost trees for the each node & these trees are exchanged b/w the intermediate neighbours to create the complete tree of the given network.



Node A

A	0
B	2
C	7
D	3
E	6
F	8
G	9

→ Final vectors of Node A.

From Fig 1, n vectors of all nodes are :-

Node A

A	0
B	2
C	∞
D	3
E	∞
F	∞
G	∞

Node B

A	2
B	0
C	5
D	∞
E	4
F	∞
G	∞

Node C

A	∞
B	5
C	0
D	∞
E	∞
F	4
G	3

Node D

A	3
B	∞
C	∞
D	0
E	5
F	∞
G	∞

Node E

A	∞
B	4
C	∞
D	5
E	0
F	2
G	∞

Node F

A	∞
B	∞
C	4
D	∞
E	2
F	0
G	1

Node G

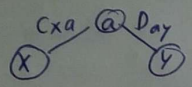
A	∞
B	∞
C	3
D	∞
E	∞
F	1
G	0

... are represented by SLASH NOTATION / ∞

To send packets from A to G.

→ First A will send packet to B. Here A will even sends its vectors. Now B will compare its vectors with vectors of A. Here if a node to create it we use BELLMAN FORD EQUATION.

$$D_{xy} = \min\left((C_{xa} + D_{ay}), (C_{xb} + D_{by}), (C_{xc} + D_{cy})\right).$$



	B
A	2
B	0
C	5
D	∞
E	4
F	∞
G	∞

	A
A	0
B	2
C	∞
D	3
E	∞
F	∞
G	∞

	New B
A	2
B	20
C	5
D	5 → 3+2
E	4
F	∞
G	∞

Now E had send its vectors of B.

	New B
A	2
B	20
C	5
D	5
E	4
F	∞
G	∞

	E
A	∞
B	4
C	∞
D	5
E	0
F	2
G	∞

	New B
A	2
B	10
C	5
D	5
E	4
F	6
G	∞

PROBLEM :-

1) COUNT TO ∞ PROBLEM :-

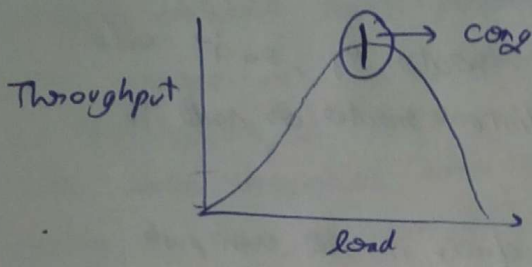
By any chance a link is broken b/w 2 vertex.

→ If in a vertex of destination contains an ∞ entry then it means that count to ∞ problem had occured.

OPTION :-

- Single byte option
- Multiple byte option

CONGESTION CONTROL



Congestion control is of 2 types :-

- Open loop → Prevent the congestion (before)
- Closed loop → remove congestion (after)

OPEN LOOP CONGESTION CONTROL :- (preventive measures)

1.) Retransmission Policy - fix time limit (for acknowledgement).

If ~~p~~ acknowledgement of ~~pac~~ ~~p~~ ~~re~~ sended packets is not received in fix time limit, sender will re-transmit the packets.

Receiver accepts by using piggy banking (a group acknowledgement)

DISADVANTAGE :- Duplicacy of packets.

2.) Acknowledgement policy :- Ack. policy of sender & receiver i.e. same policy before transmission of packets.

3.) Discard policy :- Sender has rights to discard packets (like for security issues, if they are bulky & can cause congestion).

4.) Admission policy :- → Same as discard policy but here router will discard as enters it.

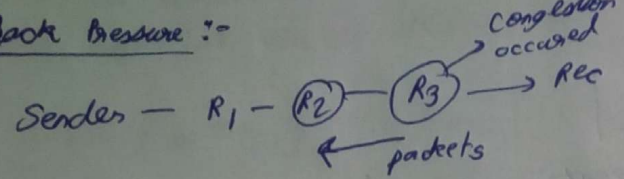
→ Here routes will provide permission to a packet to enter its network.

→ Here addresses are represented by SLASH NOTATION.

C) To send packets from A to G1.

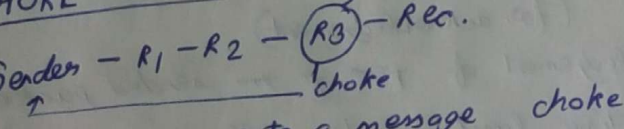
CLOSED LOOP CONGESTION CONTROL :-

1) Back Pressure :-



- Here since congestion had occured in router R3, so it will push back packets to previous intermediate routers or node to remove congestion.
- If congestion occured in R2 then forcefully it will even push back to R1 & then to sender.
- So, here sender ultimately all packets will reach to sender & then it will re-transmit to them.

2) CHOKE PACKETS :-



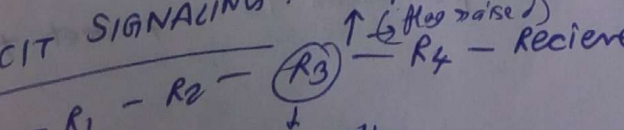
- Here R3 will create a message choke & then will send back the packets to sender.
- So, here sender will re-transmit the packets that are of router R3 to receiver directly without

ADVANTAGE :- R1 packets in R1 & R2 will get transmitted without pushing back to sender. Here R1 & R2 will find an alternative path & will transmits its packets to receiver.

3) IMPLICIT SIGNALING :- Increase the delay.

→ If receiver comes to know that congestion had occured, it i.e. acknowledgement is not received & to sender then it will inc. delay.

4) EXPLICIT SIGNALING :- Explicit signals are given by routers.



- Here R3 have recieved more packets than his capacity.
- R3 will raise a flag i.e. willingly withdraw the message.
- It will choose an alternative path to transfer packe

UDP
USER DATAGRAM PROTOOOL → ~~TRANS~~

TRANSPORT LAYER

- Process to process communication

→ whereas Network layer performs host to host communication.
→ When message is reached from sender to receiver i.e. it has reached to that system, it is known as host to host communication. Now when ~~user~~ receiver have the acces of that particular application or process only then, he can get data from that message which is already reached to him. This is known as process to process communication.

→ Transport layer uses the concept of **port number** for process to process communication.

Port No → ~~0-66~~ 0 → 65535

- Well known Ports → 0 - 1023
- Registered ports → 1024 - ~~4915~~ 49151
- Ephemeral ports → 49152 - 65535

→ Port No. are given by ICANN
(International Council of Assigned

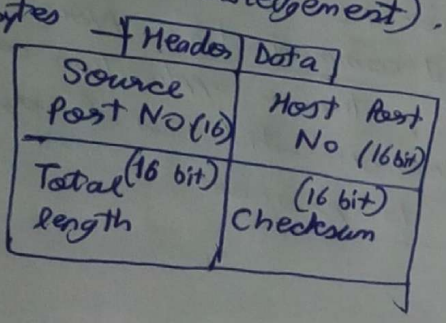
represented by SLASH NOTATION /

→ TCP & UDP are integrated with IP Address.

USER DATAGRAM PROTOCOL

→ A protocol of TRANSPORT LAYER
→ Connection-less protocol.
(No acknowledgement).

8 bytes



Header → 8 bytes

User Datagram of UDP

- Source Port No :- 0 - 65535
~~Host~~
- Total length defines total length of user datagram & header.
- Checksum is used for error detection & correction.

★★★

Q.) UDP header in hexadecimal format is :-

CB84 000D 001C 001C

is transmitted. Find the following :-

1.) Source port no
2.) Destination port no
3.) Total length
4.) Length of data
5.) Whether message is from client to server or server to client.

Ans.) 1.) $CB84_{16}$ → 52100 (client)
2.) $000D_{16}$ → 13 (server)
3.) $001C_{16}$ → 28 bytes
~~4.) 001C~~
4.) 28 - 8 = 20 bytes
5.) client → server.

routers will choose an alternative path to transfer packets.

→ Learn examples of few well known ser ports with their servers from BOOK.

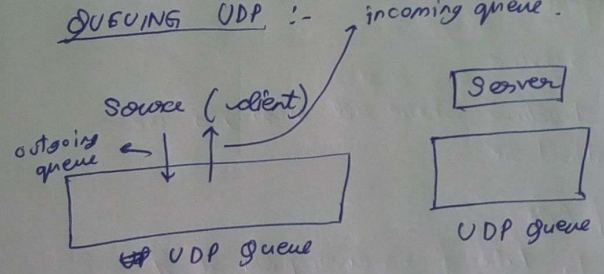
UDP Services :-

1.) Provides process to process communication
2.) Connection - less services
3.) No flow control in UDP.
4.) No error control except Checksum.
→ No specialized formula as we do not get acknowledgement.

TCP

- Widely used protocol of Transport layer.

QUEUING UDP :-



→ As soon as client wants to make a request to server, it first request for a port no. from ICANN (ephemeral port no).
[Ephemeral port no is only assigned on time basis, if time finishes then client either have option to renew it if possible otherwise have to request for new port.].

→ Now client will enquire for port no. of server by ICANN.

→ Now client will make 2 queue - outgoing queue (with port no of server) & incoming queue.

...ented by SLASH NOTATION / ...

→ TCP & UDP are integrated with IP Address.

→ Outgoing queue will have the request of client.

→ Outgoing queue will insert that request to UDP queue.

→ UDP queue will send the request to Server.

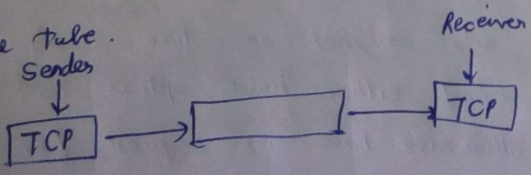
→ Server will process & send response or reply to UDP queue.

→ Now reply will be projected to client by incoming queue.

→ If incoming queue gets damaged or is broken down, then error will occur → HOST IS NOT REACHABLE.
(even due to its breaks down if time finishes earlier).

TCP

- process to process communication.
- Connection oriented protocol.
- It adds Stream Delivery service.
- It creates a tube-like structure where all messages are forwarded to tube-like structure.
- Technique used :- Push & Pull
- Sender pushes the message to tube & receiver pulls it.
- Now here even overflow of message can take place in the tube.



- To overcome this overflow, Stream Delivery Scheme with Buffer is used.