- Network is the linkage or connection.

- Internet is the network of networks.

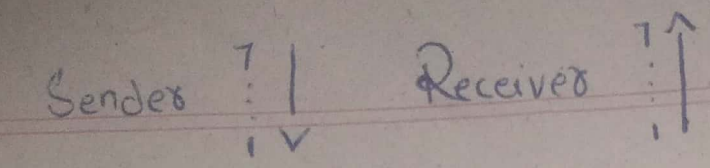
- The Physical Address of Network Interface Controller -> Hardware Address / MAC Address

- Fibre Optics is a cable that is used to connect the network of networks. High speed, made of glass.

- ISP (Internet Service Provider) invests in cable and provides internet service to consumers by charging fees.

- MODEM (Modulator - Demodulator) used earlier

- MAC Address -> for local identification
  IP Address -> for global identification



Open System Interconnected Model (OSI):

7 - Application Layer: Provide Interface

6 - Presentation Layer: Type of file

5 - Session Layer: Data & info about it.

4 - Transport Layer: To ensure end-to-end reliability.
TCP / UDP -> Protocols

3 - Network Layer: Routers, IP Address
L-> Logical Address.

2 - Data Link Layer:
- Network Switch
- MAC Address
↓
Media Access Control
- Data Error checking
- CRC -> Cyclic Redundancy Check
Checks Data Integrity

TCP/IP H.W

1 - PHYSICAL LAYER: Physical Devices

DNS (Domain Name Server/System):

DNS Service Port = 53

Google Server DNS = 8.8.8.8
or 8.8.4.4

↳ Reachable to destination?

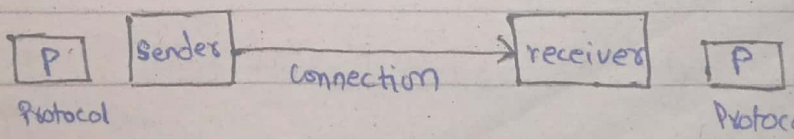
* Ping works on ICMP Protocol

Full form
ICMP -> Internet Control Messaging Protocol.
↳ Packet

Internet	Echo Request	Completes 1 Packet
Groper	Echo Reply	

↳ Kis kis jaga se guzr kr destination pr phacha

* tracert (Trace Route)



The concept says that the data sent by the sender, must be understood by the receiver. For this, we use some kind of protocol that is running on sender's & receiver's machine.

Wireshark Putty Tool

Brutal Attack -> Ransomwhere

Common Ports:

HTTP = 80 (Hyper Text Transfer Protocol)

HTTPS or HTTP/SSL = 443

↓

(Secure Socket layer)

POP (Post Office Protocol) = 110

TALNET = 23

FTP = 21 & 20

Secure Shell = 22

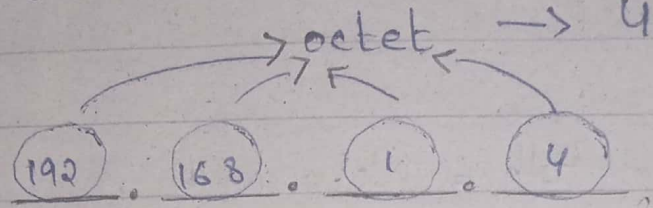
(Secure version of Talnet)

DHCP -> Dynamic Host Control Protocol

IP ADDRESSES: → 32 bits hi hti h
2^{32} = 4.2 billion
→ contains: ① Network portion
② Host portion

DHCP → Dynamic Host Control Protocol

Physical Address → MAC Address



→ 4 octets

4 x 8 = 32 bits

IPv4 addressing

Each octet = 8 bits

2^8 = 256 → 0 - 255 → Range of each octet

Max value of an octet

An IPv4 address is 32 bits long.

IPv4 address range:

0.0.0.0 - 255.255.255.255

IPv4 address

IPv4 Subnet Mask

IPv4 Gateway → Tells you the end point of your network to go to another network.

(Jhn se aap network se bahir ja skte)

Subnet mask

255.255.255.0 /24

8 8 8

+

Subnet = Subnet Path = Network ID

Subnet Mask = Network Mask

IP Address given

Subnet mask given

Network ID = ?

IP Address = 10.57.65.1

Subnet mask = 255.255.252.0

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

IP = 00001010 . 00111001 . 01000001 . 00000001

SM = 11111111 . 11111111 . 11111100 . 00000000

IP & SM

NI = 00001010 . 00111001 . 01000000 . 00000000

10.57.64.0 -> Network ID

IP Address Classification:

① Class A → 0.0.0.0 – 127.255.255.255 → (0-127) 128
② Class B → 128.0.0.0 – 191.255.255.255 → (128-191) 64
③ Class C → 192.0.0.0 – 223.255.255.255 → (192-223) 32
④ Class D → 224.0.0.0 – 239.255.255.255 → (224-239) 16
⑤ Class E → 240.0.0.0 – 255.255.255.255 → (240-255)

Subnet mask of Class A, B, C
↳ Default subnet masks

Class A → 8 bits → 255.0.0.0
Class B → 16bits → 255.255.0.0
Class C → 24bits → 255.255.255.0
↳ Main classes we use.

Class D → Used for multicast
Class E → Used for research

→ Default Subnet masks will be taken

192.168.1.4 ——→ 192.168.1.0 } Network IDs

192.168.1.13 ——→ 192.168.1.0

* These IP addresses will communicate with each other because there Network IDs are same. (without any router)

* If Network ID is different then Devices will communicate with each other through router.

* Gateway is the part of your network

Gateway: (Subnet mask is same throughout the network)

Gateway : 10.57.64.1
Subnet : 255.255.252.0
Network ID : 10.57.64.0

in bits ⇒ 22 bits

IP Address:

① Host Portion
② Network Portion

Host -> Kitne devices connect hokte us network m. $2^n - 2$ -> useable hosts
↳ no. of hosts.

1st IP of 1st octet] not usable / not assignable
Last IP of last octet]

192.168.1.0 / 24 -> 86.86.86.0
Network
↳ identified by
host

-> Total bits IPv4 = 32
Subnet mask = 24 - 8
8 x 3 = 24 bits

$2^8 = 256$ hosts

First usable IP of this address
192.168.1.1
⋮
last usable " " "
192.168.1.254

192.168.1.255 -> Broadcast ID.
11111111 -> Host k saray on.

Network ID may host portion saray zero.

Host k saray on hjyen two -> Broadcast IP
(1)

10.57.64.0

255.255.252.0

11111111.11111111.111111|00.00000000

Network bits — 22 bits + = 32

Host bits — 10 bits ← 32 - 22 = 10 Host

↓ Subnet mask.

2^{10} = 1024 hosts

First IP -> Reserved ID / Network ID
Last IP -> Broadcast ID } not useable

1024 - 2 = 1022 -> Useable IP's

Network ID

- 10.57.64.0 — 10.57.64.255 (256)

+1 ←

10.57.64 256 → 10.57.65.0 ~~(256)~~

- 10.57.65.0 — 10.57.65.255 (256)
- 10.57.66.0 — 10.57.66.255 (256)
- 10.57.67.0 — 10.57.67.255 (256)

Broadcast ID

+ 1024

10.57.65.255 ←

00001010 . 00111001 . 01000001 . 11111111

All are neither 0 (Network ID) nor 1 (Broadcast ID) so it is useable IP

Separate Network ID & Broadcast ID.

IP = 10.57.65.1

Subnet = 255.255.252.0 /20
240

IP= 00001010.00111001.01000001.00000001

S = 11111111.11111111.11110000.00000000

NI = 00001010.00111001.01000000.00000000

Network ID = 10.57.64.0

S = 11111111.11111111.1111|0000.00000000

Network bits 20 | Host bits 12

32 - 20 = 12 bits → Host bits

2^{12} = 4096 hosts

4096 - 2 = 4094 useable IPs

Network ID		
10.57.64.0	—	10.57.64.255
10.57.65.0	—	10.57.65.255
10.57.66.0	—	10.57.66.255
10.57.67.0	—	10.57.67.255
10.57.68.0	—	10.57.68.255
10.57.69.0	—	10.57.69.255
10.57.70.0	—	10.57.70.255
10.57.71.0	—	10.57.71.255
10.57.72.0	—	10.57.72.255
10.57.73.0	—	10.57.73.255
10.57.74.0	—	10.57.74.255
10.57.75.0	—	10.57.75.255
10.57.76.0	—	10.57.76.255
10.57.77.0	—	10.57.77.255
10.57.78.0	—	10.57.78.255
10.57.79.0	—	10.57.79.255

Broadcast ID

BI = 00001010.00111001.01001111.11111111

All Host bits are 1's

Commands:

<Huawei>

↓ Indicates user mode / limited mode.
No configuration is allowed.

Interface -> jism (LAN card / cables lgti hn.
(Bridge to connect network)

<Huawei> system-view (enter)
(tab)

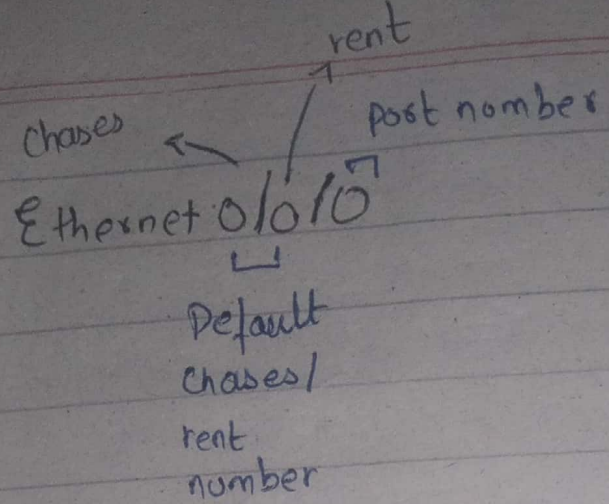
[Huawei] -> system view

↓
system configuration mode

[Huawei] display ip interface brief

↓
legends are displayed

Ethernet	vs	Gigabit Ethernet
Total capacity bandwidth is 100 Mbps (throughput)		Total capacity bandwidth is 1000 Mbps = 1K Mbps (throughput)



IP Assignment

[Huawei]

Interface Ethernet0/0/0 (Enter)

[Huawei-Ethernet0/0/0]ip address 192.168.3.250

? agr agy ka ←

syntax nhi pata.

X.X.X.X

[Huawei-Ethernet 0/0/0]ip address 192.168.3.250
255.255.255.0

[Huawei-Ethernet0/0/0] display ip interface brief

(physical)

down → interface is by-default disabled
(cable connect nh kiya)

(Protocol)

down → for-end interface is disabled

4 + 8 + 8

172.16.0.0 — 172.31.255.255

Network Bits: Start from left to right

Host Bits: Start from right to left.

16 = 00010000 31 = 00011111

```
  00010000
& 00011111
  --------
  00010000
```

← right to left for hosts

8 + 8 + 4 = 20 host bits

Every interface of a router has a unique network ID.

VLSM -> Variable Length Subnet Mask

24.23.5.0/24

③ 16 = 2^5 = 32
③ 24 = 2^5 = 32
④ 03 = 2^3 = 8
① 100 = 2^7 = 128
⑤,6,7,8 2 = 2^2 = 4 -> 4 hosts of 2

151
254

① 100 H = 255.255.255.128

11111111.11111111.11111111.10000000
255 . 255 . 255 . 128

② 24 H = 255.255.255.224

11111111.11111111.11111111.11100000
255 . 255 . 255 . 224

company will grow 20% of 128 after few years = 15.6 ≈ 16

128 + 16 =

$\frac{20}{100} \times 128$

(3) 16 H = 255.255.255.224

(4) 3H = 255.255.255.248

11111111.11111111.11111111.11111000

255 . 255 . 255 . 248

(5) 2H = 255.255.255.252

(6)

(7)

(8)

11111111.11111111.11111111.11111100

255 . 255 . 255 . 252

(1) 24.23.5.0 — 24.23.5.127

(2) 24.23.5.128 — 24.23.5.159

(3) 24.23.5.160 — 24.23.5.191

(4) 24.23.5.192 — 24.23.5.199

(5) 24.23.5.200 — 24.23.5.203

(6) 24.23.5.204 — 24.23.5.207

(7) 24.23.5.208 — 24.23.5.211

(8) 24.23.5.212 — 24.23.5.216

+ IP && Subnet = IP then IP is NI
+ In IP if all host bits are off (0) then it is NI and if On (1) then it is BI

Commands: (2)

arp stores MAC Address through IP Addresses

arp -a (arp space -a) -> Tells Interfaces

Advanced Resolution Protocal

ping 192.168.1.2 (find address to which we want to connect our system)

PC1 has no info (switch will broadcast to all PCs)

Ping PC1 to PC2

Check if IP of both has same NI then need MAC Add not Network Add.

PC2 in reply gives MAC Address to switches.

Sb PCs k ps <- request jaegi

reply sirf jiski IP hai whin se aega ie PC2

u t m

to turn off the commands in switch

OUI -> Organizationally Unique Identifier

CID -> Company ID

MAC ADDRESS: -> Total combination of bits = 48 bits (12x4)

$2^{(4)}$ — bits = 16 bits

4 bits

9B - 3B - 8F - 5D - 9D - 8A

8 bits OUI — Device (CID)

(- Identifies company

8 x 6 = 48

- Switch is Layer 2 device by defaults (i.e saves ^ MAC Address, ports)

MAC Address

Static type: ^ that we enter manually

dynamic type: that we enter by learning a reply

ff - ff - ff - ff - ff - ff -> Broadcast ID for MAC Address

01 - 00 - 5e - 00 - 00 - 02

Multicast Address

- Switch k VLAN k upar ID dikh k port pr nhi

sniffing through wireshark

Unicast -> one to one

Multicast -> one to many

Broadcast -> one to all

Commands (2)

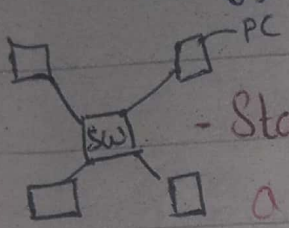
display mac-address

- By default switch aik hi VLAN ko support krta h (aik hi NI chlrhi hoti).

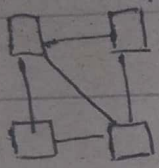
PC 1 wants to contact PC 4
PC 4 is already pinged
then PC1 will unicast instead of broadcast.

Mesh -> mila hua

Topology -> network arrangement



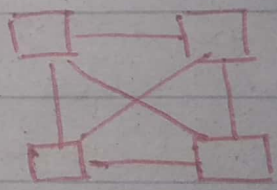
- Star topology (Every thing is connected to a same device) costly bcz of switch.



- Mesh topology (PCs are connected to each other without switch). agr koi cable khrb hoa tw sirf wo connection tute ga

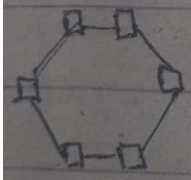
Full Mesh Topology $= \frac{n(n-1)}{2} = \frac{4(4-1)}{2} = 6$

n = no. of nodes

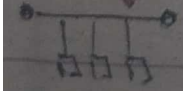


Full mesh

(aik cable khrb hui to pura connection tut jaega)



- Ring topology (Circular connection)



- Bus topology

Transmission Media:

- Coaxial Cable
  (TV, not for digital transmission)

- Ethernet Cable
  - UTP (unshielded twisted)
  - STP (costly) (shielded twisted)
    ↓
    shield for wave protection

- Twisted Pair (4 pairs 8 cables)
  4 · for data transfer
  4 for backup

Transmission Modes:

Ethernet 3 Modes

- Simplex (can decide direction of data, TV eg.) one-way

- Halfduplex (Two-way) but one at a time.

- Fullduplex (Two-way at the same time)

SNMP protocol. To link 1 PC to multiple.

Switch (Layer 2)
if switch is given an IP it will become Layer 3 switch. (router)

Loopback address: 127.0.0.1 (Local Host)
- used for loopback testing
- indicates OS is not corrupted and device's stack is intact
- Cannot be assigned to any PC
  - more bandwith consume
  - security issues

Cascading: Switch to Switch connection
- cascaded switches will also receive 'ping' requests (broadcast)
- Request will be broadcasted to every PC in switch as well as PCs in cascaded switches

IPs
1.X Finance — 4
2.X HR — 4
3.X Admin — 5
4.X Marketing — 4

Not handling the broadcast issue. For this we use VLAN

(1.X)
Request will be sent to all the PCs present in different networks (1.X, 2.X, 3.X, 4.X) then PC will reject it knowing that request is not for its network (2.X)

VLAN (Virtual Local Area Network):

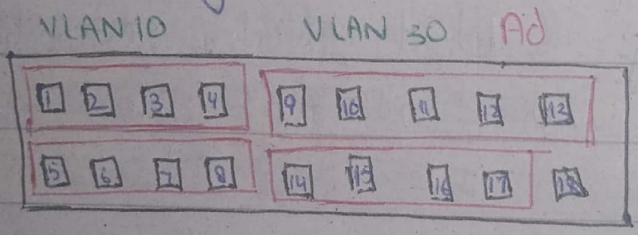
(Segmenting networks).

Switches:

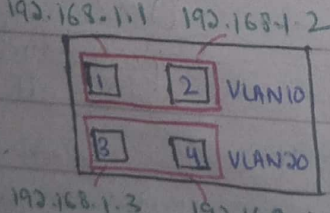
- Manageable Switch (can do configuration)
- Unmanageable Switch (cannot do configuration)

Huawei switches are manageable:

1–4	Finance – 4	Same network IP.
5–8	HR – 4	
9–13	Admin – 5	
14–17	Marketing – 4	



Task



1) ping all from PC 1.
2) user mode to admin mode
3) display VLAN (How many vlans are there in switch and their ports)

4) vlan 10

system view > admin mode > vlan 10

H.w -> What is the length of Ethernet? (100m).

1) Switch -> turn on -> <Huawei> -> System-view -> (usermode)

sysname Malaika (change user name)
(system mode, config mode, admin mode)

2) Save and close topology (user name wapi: huawei hjyega).

3) Again open ensp and load same topology.

display current-configuration (checks current configuration).
in system (like RAM)

display saved-configuration (display saved configurations).
(like ROM)

run -> save
<Huawei> save

- Length of Ethernet is 100m.
- Maximum VLANs in a switch 4096.
- By default, one switch has one VLAN i.e VLAN 1

[redacted] to go back in user mode quit or Ctrl+Z or undo.

- VLAN tag is of 4 bytes.

5) quit

6) vlan 20

// assigning ports.

7) display vlan (vlan 10 vlan 20 will be displayed but ports will be blanked).

i) vlan 10

L-> port eth 0/0/1

ii) display internet brief

interfaces can be:

a) giga

b) ethernet

For giga:

interface ge 0/0/1

L-> vlan 10

Private IP Address

Class A : 10.0.0.0 — 10.255.255.255

Subnet = 255.0.0.0 8

2^{24} Host & 2^{8} Network

Class B: 172.16.0.0 — 172.31.255.255

Subnet = 255.~~255~~.~~224~~.0 12

240.0.0

2^{20} Host & 2^{12} Network

Class C: 192.168.0.0 — 192.168.255.255

Subnet = 255.255.0.0 16

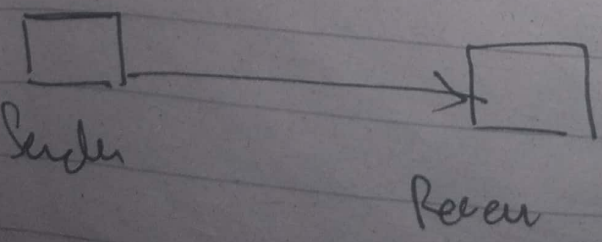
2^{16} Host & 2^{8} Network

Transmission modes:

Define the direction & flow of data transmission between devices.

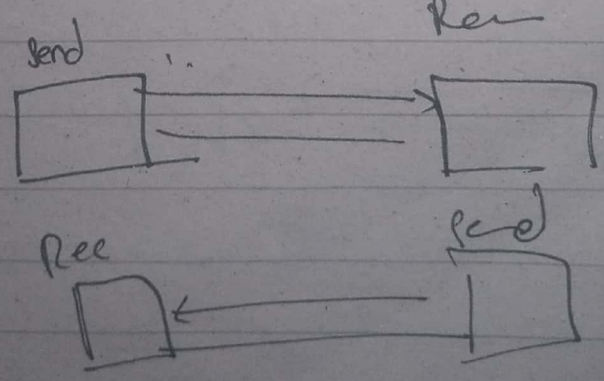
Simplex Mode:

- Data transmission only in one direction.
  - One device (sender) Other (receiv
  - Receiver receives data
    Sender transmits data
  - No bidirectional communication
  - E.g.:
    - Television Broadcast
    - One way paging system



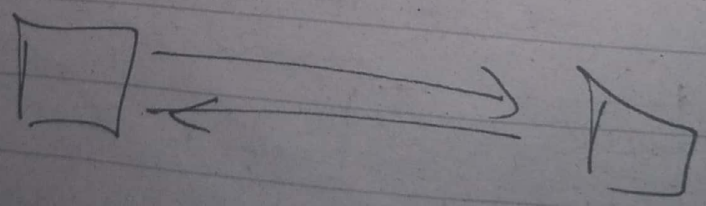
Half Duplex:

- Both direction data transmission but not simultaneously.
- Devices can both send and receive data but not at the same time on a single communication channel.
- One transmitting, other waits to receive & vice versa.
- "Walki-Talki communication", devices takes turns transmitting & recieving.
- Example:
  - Two way radio comm
  - Ethernet hubs.



Full - Duplex:

- Simultaneously in both directions.
- Can send and receive data simultaneously, utilizing separate communication channel for each direction.
- Allows for simultaneous bidirection communication.
- Enables faster & more efficient data transfer
- Commonly used in
  - Modern Ethernet networks
  - Wireless comm "wifi"
  - Fibre optic connections.



Transmission Media:

refers to physical pathways or channels through which data is transmitted in a computer network.

Twisted Pair Cables:

- Unshielded Twisted Pair (UTP):
  - most common
  - Used in Ethernet network
  - consists of:
    - pair of twisted copper wires
    - terminated with RJ-45 connector.

- Shielded Twisted Pair (STP):
  - Additional layer of shelding to reduce
    - Electromagnetic interference (EMI)
    - Cross-talk

blue cables:
- costly
4 pair 8 cables
4 for data transfer 4 for backup

Coaxial Cable:

- Central Conductor surrounded by a layer
  - Layer of insulation
  - metallic shield
  - outer protective covering.
- Commonly used in:
  - cable television (CATV) networ
  - high-speed data transmission appli

Fibre Optic Cable:

- Use thing strands of glass or plastic fibers to transmit data as pulses of light.
- provide
  - high bandwith.
  - long dist transmission
  - immunity to EMI.
- Widely used in:
  - Telecommunication,
  - Internet backbone network (BN)
  - high speed data transmission

Wireless Media:

- Use electromagnetic waves to transmit data.
- No physical cables.
- Examples:
  - WIFI
  - Cellular networks (3G, 4G, 5G)
  - Microwave & satellite

Power Line Communication (PLC):

- utilizes existing electrical power line for data transmission.
- Enables communication over the electrical power distribution network.
- Used for:
  - home networking
  - Industrial applications.

Packet Switching vs Circuit Switching

Concept

Data is divided into small units called packets, which are individually routed from source to destination.

A dedicated physical path or circuit is established b/w source & destination before data transmission.

Transmission

Each packet is transmitted independently and can follow diff paths through the network.

Packet may arrive at destination out of order

Once the circuit is established, data is transmitted continuously along the fixed path without interruptions or sharing with other connections.

Resources

Allows multiple packets of different sources to share available network resources such as bandwidth, routers and links.

- Requires dedicated resources for the duration of connection even when there is no ongoing data transmission.

Efficiency.

More efficient in utilizing network resources as it allows for
- shared utilization
- dynamic allocation based on demand.

- Less efficient in utilizing network resources since the dedicated circuit remains reserved even during periods of inactivity

Example.

- Internet & Modern Computers
  Data is broken into packets and sent independently

- Traditional Telephone network (PSTN), where a physical conn is established for duration of a call.

TCP/IP Model:

Application Layer:

- Used by end user software (browser & email clients)
- Provides protocols allowing software to send and receive info & present meaningful data to users.

PDUs transmitted at network layer called 'data'.

Transport Layer.

- Receives data from application layer protocol.
- Encapsulates data with corresponding transport layer protocol header
- establishes end to end connection.
- PDUs transmitted at transport layer are segments.
  - TCP UDP

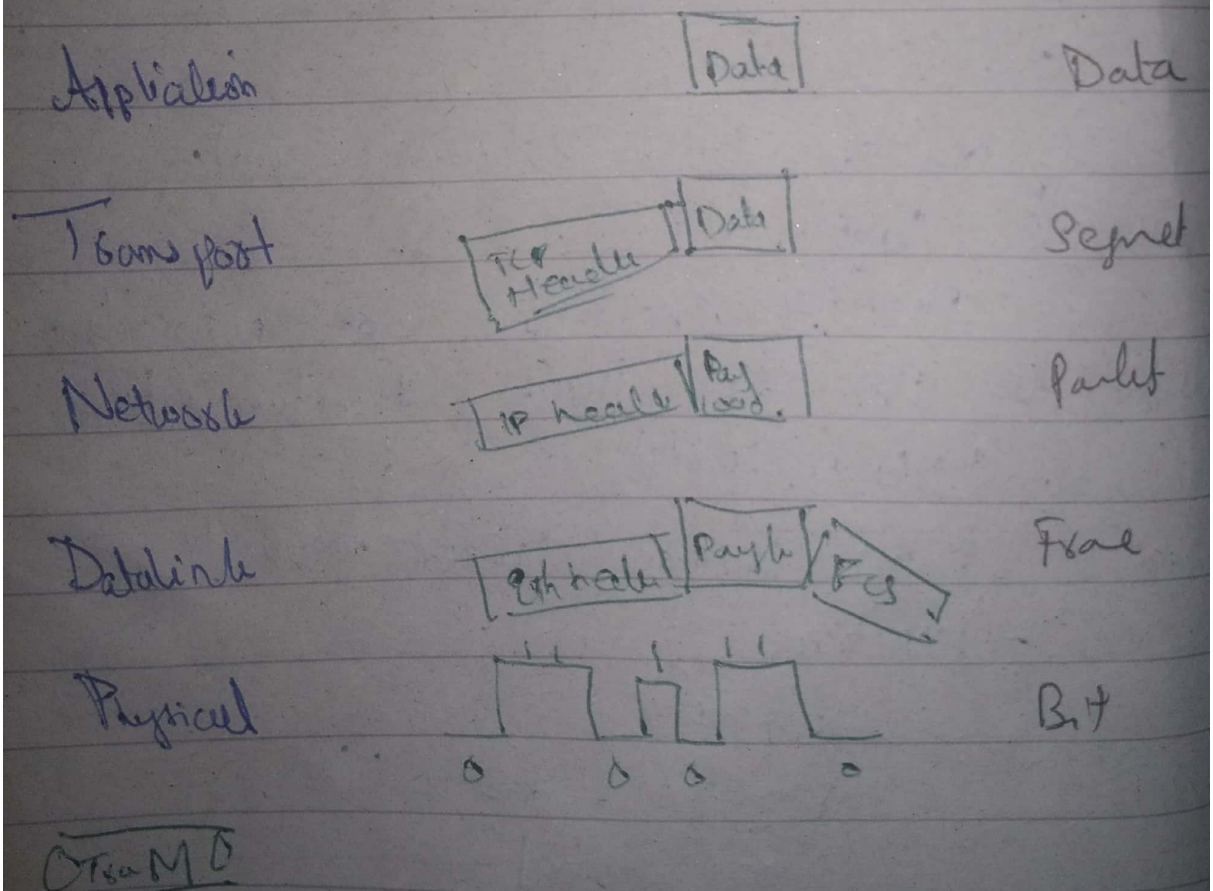
- Network layer:
  - Responsible for transmitting data from one host to another.
  - PDUs -> packets
  - send packets from source host to to destination host
  - Provide logical address for network devices

- Data link layer:
  - located b/w network and physical layer.
  - provides service for protocols such as IP and IPvG at network layer.
  - PDU -> frames
  - Most common protocol Ethernet
  - function:
    - framing
    - physical address
    - Error control

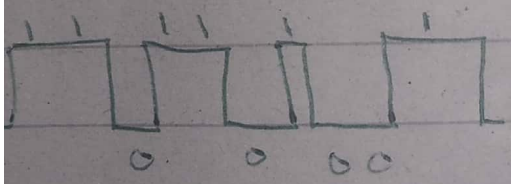
Physical layer:

- After data arrives, convert digital signal to optical, electrical or electromagnetic wave signal based on physical media.
- PDU → bit stream

DATA DECAPSULATION ON THE RECEIVER



Data Encapsulation On The Sender

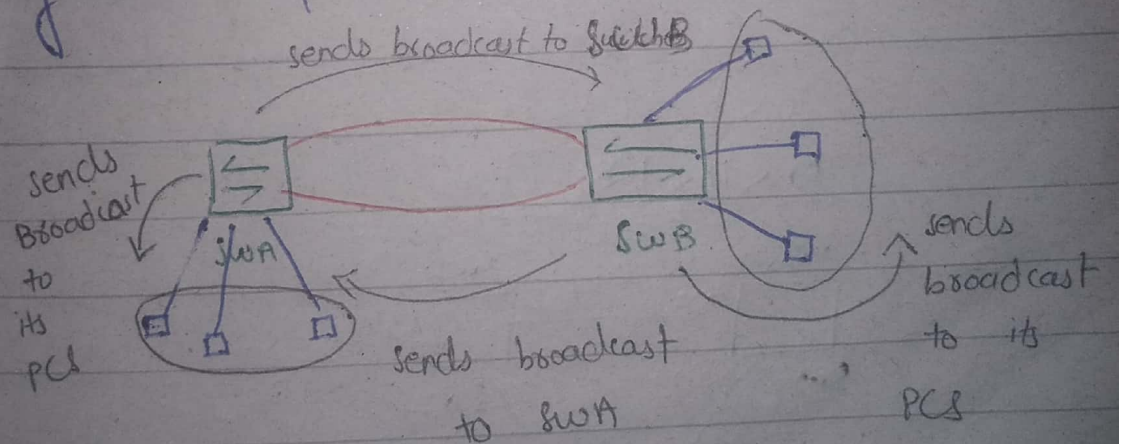
DATA	Application layer	Data
TCP Header | DATA	Transport	Segments
IP Header | Payload	Network	Packets
Eth header | Payload | FCS	Data Link	Frame
	Physical → Transmission media.	bits

STP (Spanning Tree Protocals)

Works only at switch. Switch is also known as bridge.

When switch turn on, ~~the switch~~ STP protocol is by default enabled and every switch consider itself as root bridge.

When connected switches starts its process, they will first select their root bridge.



Creates loop

MAC Address:

Priority for root bridge | Mac Address

4096/- 4c1f - aabc - 102b

16x4 = 64

Number ↓ Priority ↑

Bridge ID

first priority will be checked then Lowest MAC Address will be selected.

802.1D → IEEE standard of Bridge ID. (BID)

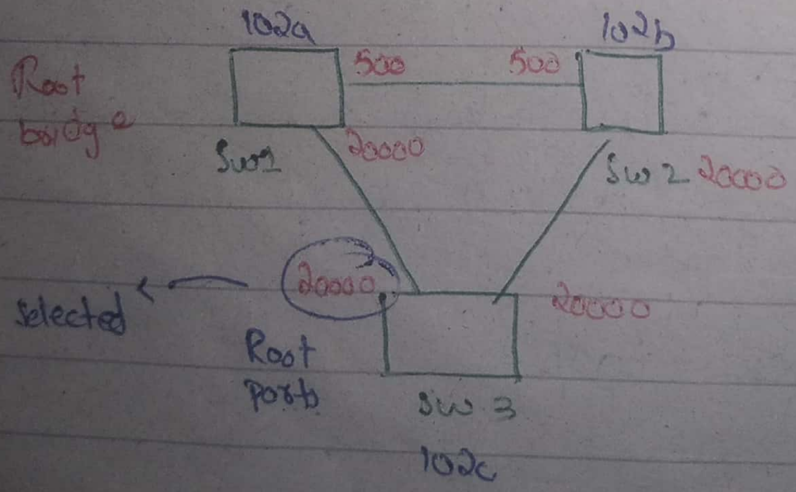
Compare MAC addresses from left to right for BID.

~~4096-4c1f-aabc-102~~

4096-4c1f-aabc-102a priority matches,
102b Compare MAC Add
102c → Bridge ID

a < b < c

10 < 11 < 12



100 & 1000 wi cost yd hum h

Three types of ~~post~~ port:

- Root port
- Designated port
- Alter or blocked port

When Switches are connected they communicate by using ~~BDPU~~ BPDU

Sends ~~BDPU~~ BPDUs after every 2 seconds.
to switch k

Port k upon priority hti h or default priority 128 h.

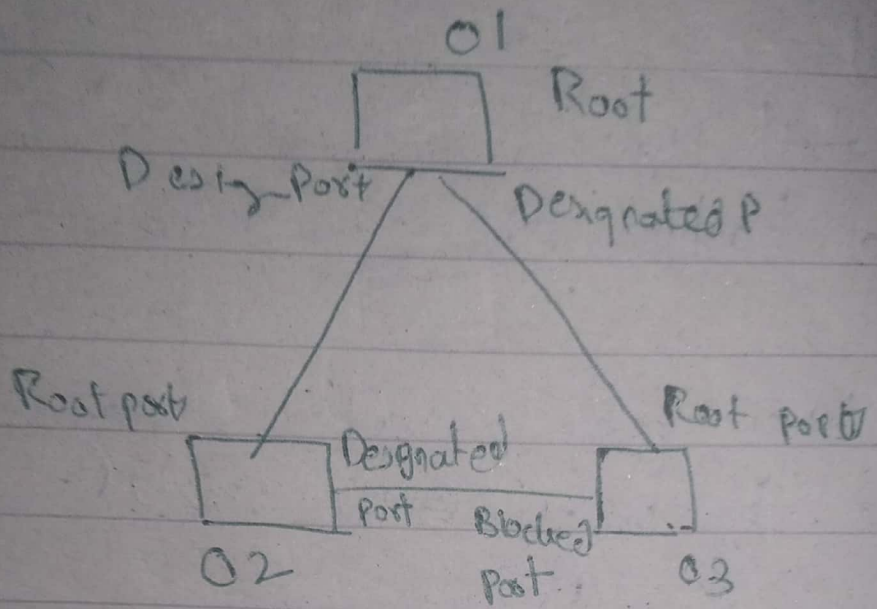
PID: 128.24

Port priority — Port no.

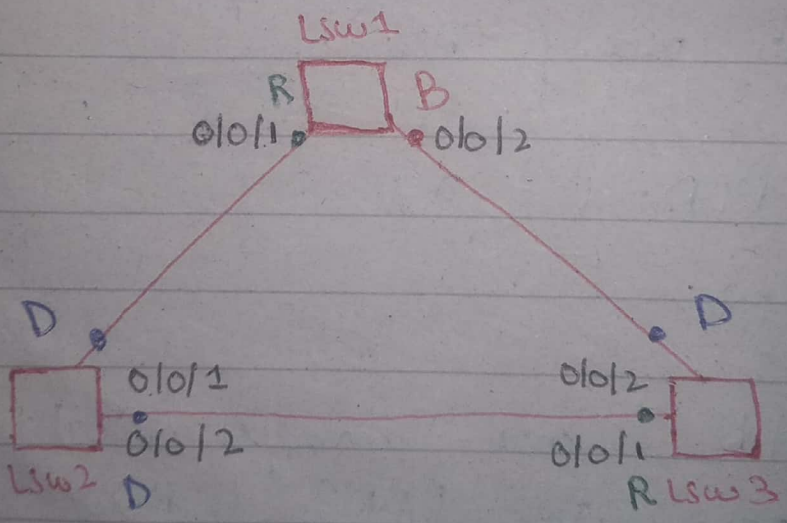
Switches sends messages that are known as ~~BDPU~~ BPDU.

Pg 24 Slide STP

STP Calculation



Default priority of switch 32768



when switches are not connected, every switch considers itself as root bcz bdpdu are not sent.

display stp

LSW1: (Global Info)

CIST Bridge : 32768.4c1f-cca1-194e
CIST Root/ERPC : 32768.4c1f-cc1b-34d3 / 20000
CIST RootPortId : 128.1

GE 0/0/1 (Forwarding)

Port Role : Root Port
Port Priority : 128
Port Cost : Config = auto / Active = 20000
Designate Bride/Port : 32768.4c1f-cc1b-34d3/
128.1

GE 0/0/2 (Discarding)

Port Role : Alternate Port
Port Priority : 128
Port Cost : " / Active = 20000
Designated Bridge/Port : 32768.4c1f-cc98-6e7f/
128.2

LSW2: (Global Info)

minimum MAC

CIST Bridge: 32768.4c1f-cc1b-34d3
CIST Root/ERPC: 32768.4c1f-cc1b-34d3/0
CIST RootPort Id: 0.0

GE 0/0/1 (Forwarding)

Port Role: Designated Port
Port Priority: 128
Port Cost: Config = auto / Active = 20000
Designated Bridge/Port = 32768.4c1f-cc1b-34d3
128.1

GE 0/0/2 (Forwarding)

Port Role: Designated Port
Port Priority: 128
Port Cost: // / Active = 20000
Designated Bridge/Port: 32768.4c1f-cc1b-34d3
128.2

LSW3: (Global Info)

CIST Bridge: 32768.4c1f-cc98-6e5f
CIST Root/ERPC: 32768.4c1f-cc16-34d3/20000
CIST RootPortId: 128.1

GE 0/0/1 (Forwarding)

Port Role: Root Port
Port Priority: 128
Port Cost: Config = auto / Active = 20000
Designated Bridge/Port: 32768.4c1f-cc16-34d3/
128.2

GE 0/0/2 (Forwarding)

Port Role: Designated Port
Port Priority: 128
Port Cost: 4 / Active = 20000
Designated Bridge/Port: 32768.4c1f-cc98-6e5f/
128.2

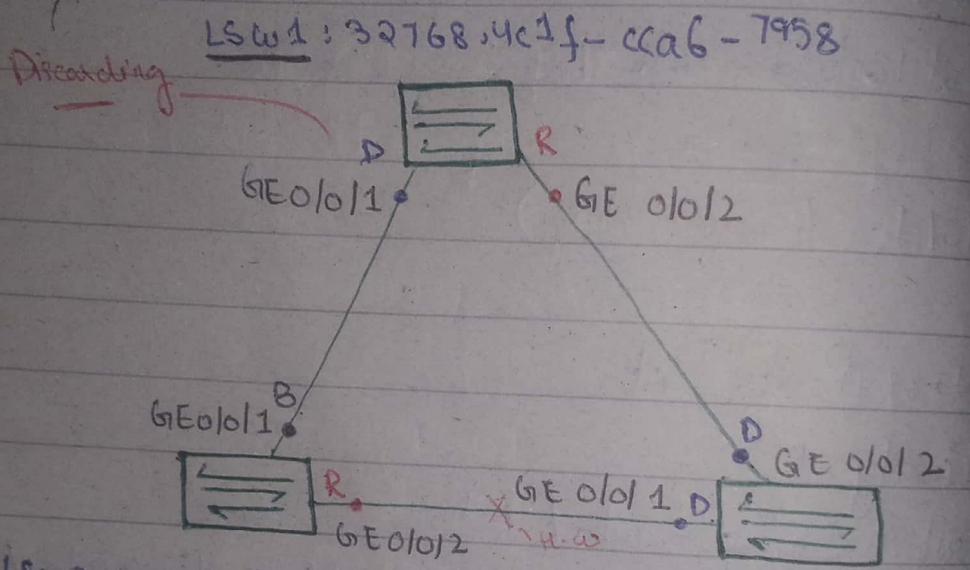
Max length of Eth cable 100m

Switch After every 100m.

Disabled -> there is no cable connected

DOWN VS DISCARDING:

hai to up, system ny down kra hua

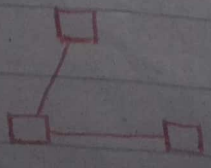


O > a > c

R B

(1)

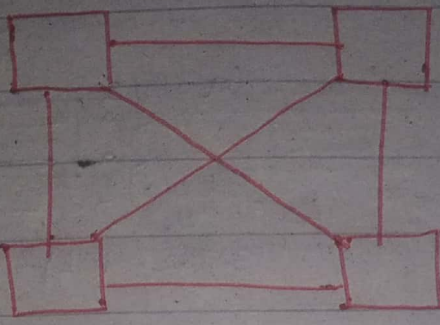
Remove the opposite cable of blocked port (main of root) and change the gig with ethernet cable



6 Switches

(2)

Full Mesh:

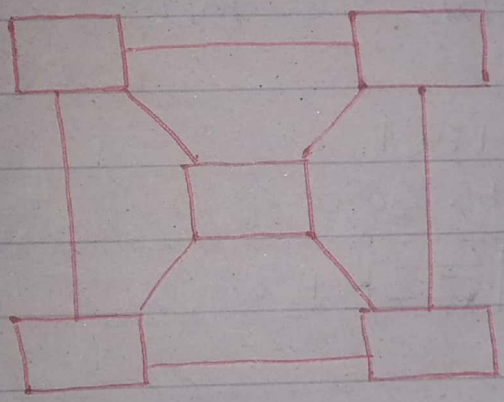


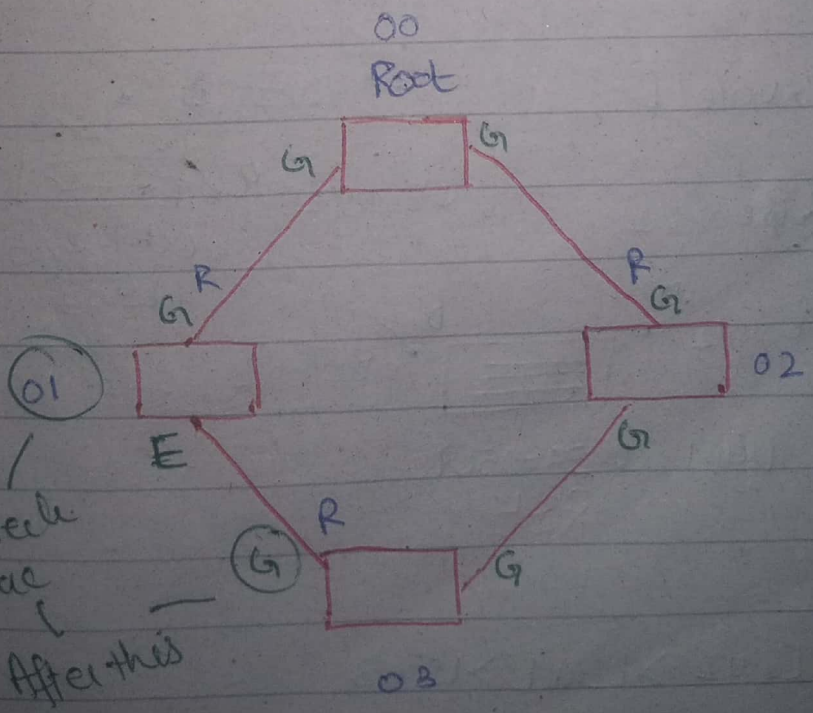
Take all ports as Gigabit Eth

loop zyada blocked ports zyada

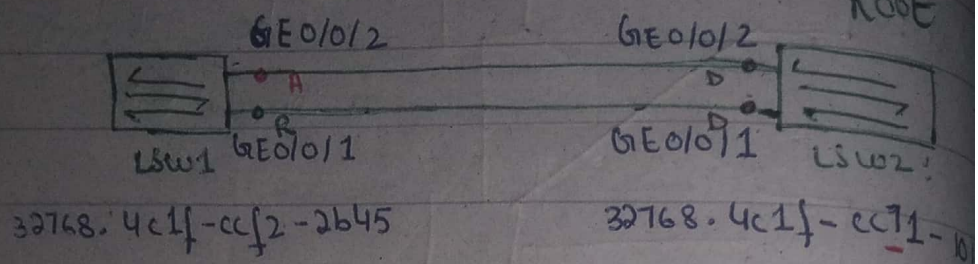
(3)

Not full Mesh



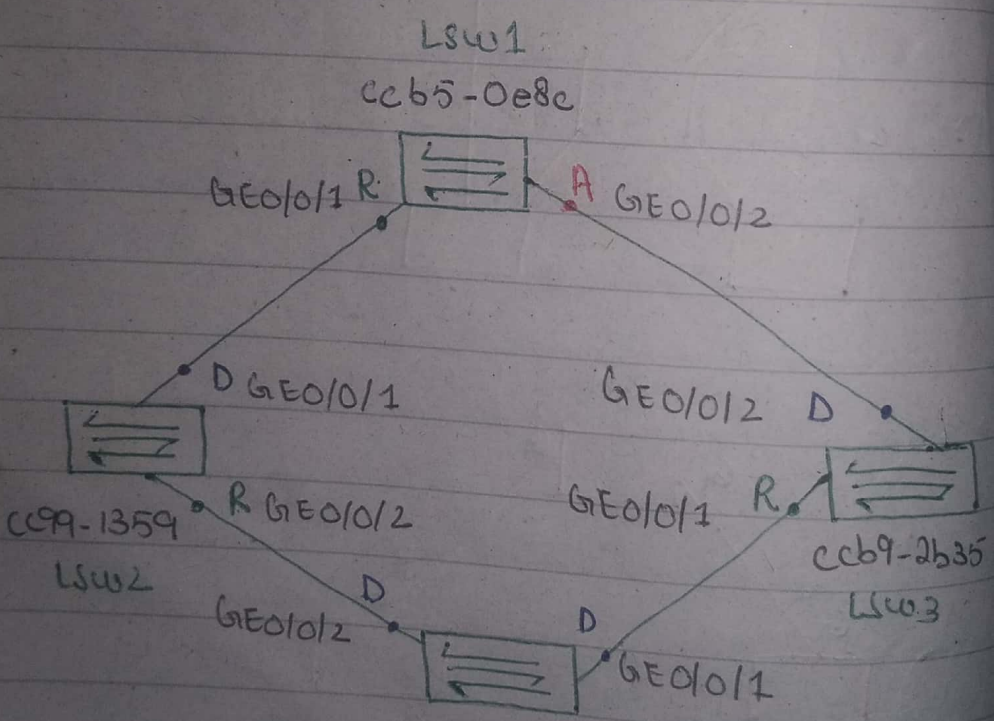


Check Mac table after this



LSW2 > LSW1

Alternate port has been decided by comparing GE0/0/2 < GE0/0/1

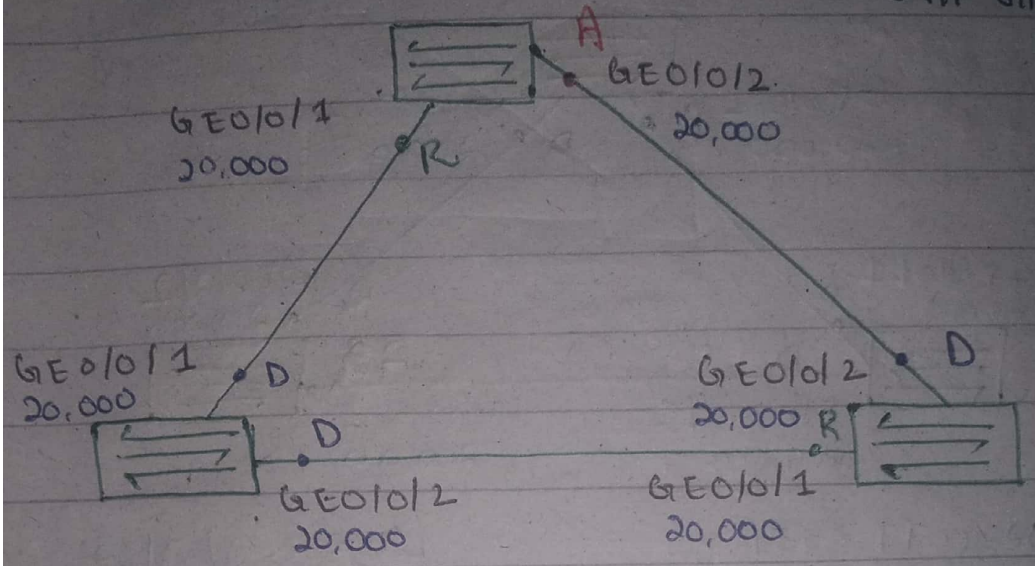


LSW4 > LSW2 > LSW1 > LSW3

CABLE CHANGE:

LSW1 : cc90 - 7027

All Gig



SW2: cc77 - 5539

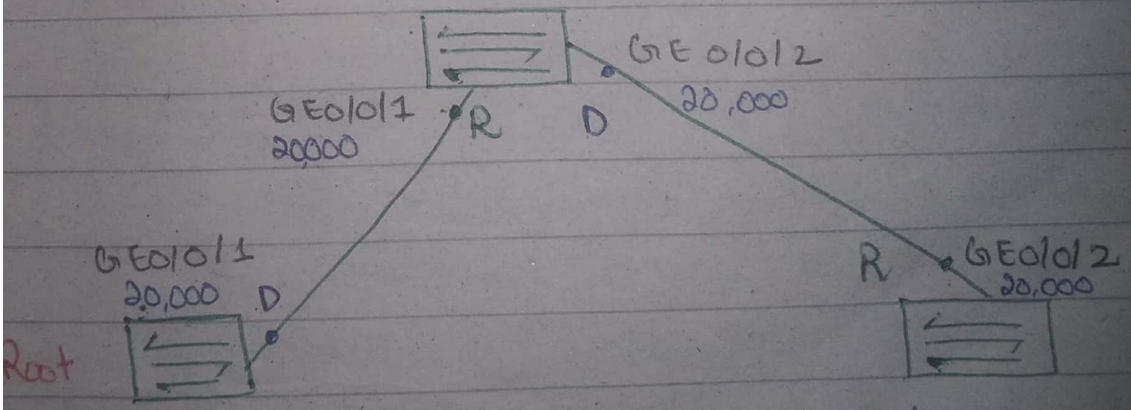
Root

LSW3: cc8d-0f83

LSW2 > LSW3 > LSW1

Cable Removed

LSW1 : cc90 - 7027



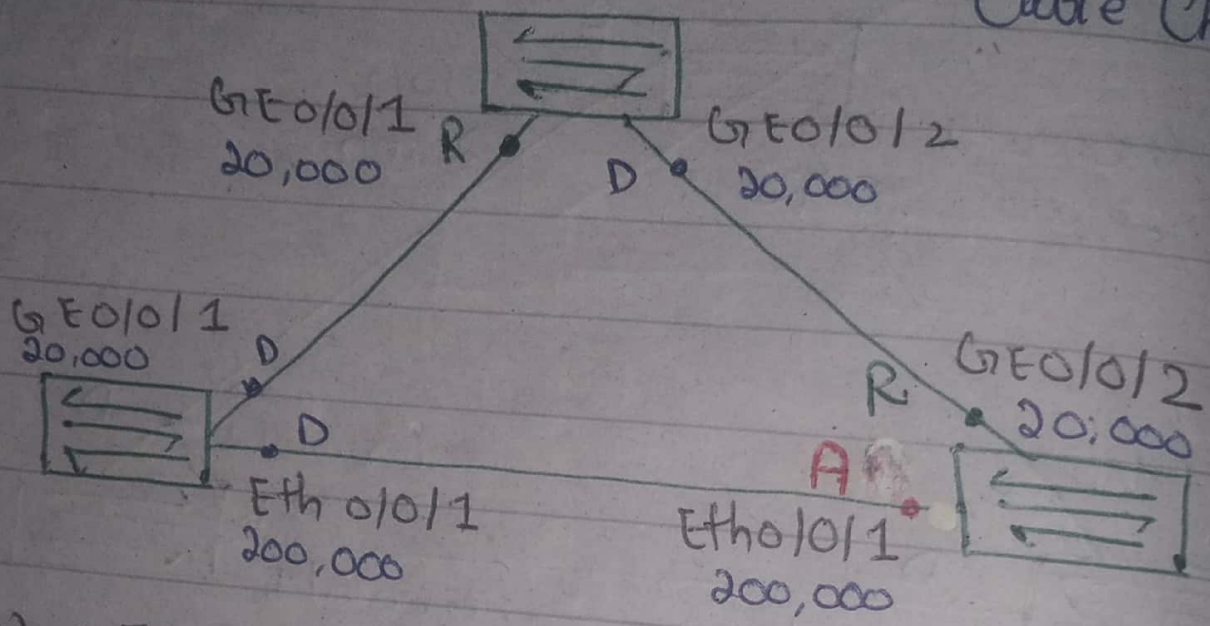
Root

SW2: cc77-5539

LSW3: cc8d-0f83

LSW1 : cc90-7027

Cable Change



LSW2: cc77-5539

Root

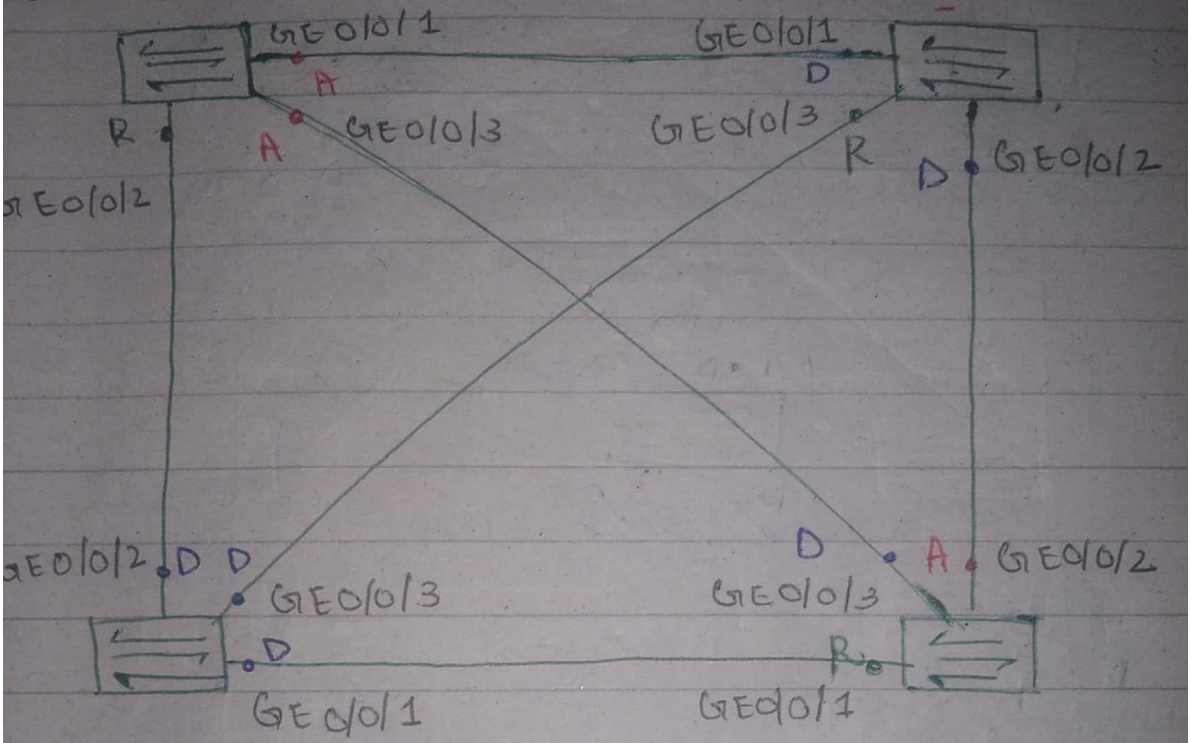
LSW3: cc8d-0f83

LSW3 -> LSW2 = 200,000

LSW3 -> LSW1 -> LSW2 = 40,000

('p').on({'click':fu...
{ },
{'dblclick'},
}

LSw3 > LSw2 > LSw4 > LSw1



A

First, check loop in max number of switches which is 4 in this case. then LSw1 is larges, has two ports from which we have to select alternate port the port with lowest priority (0/0/3) will be blocked

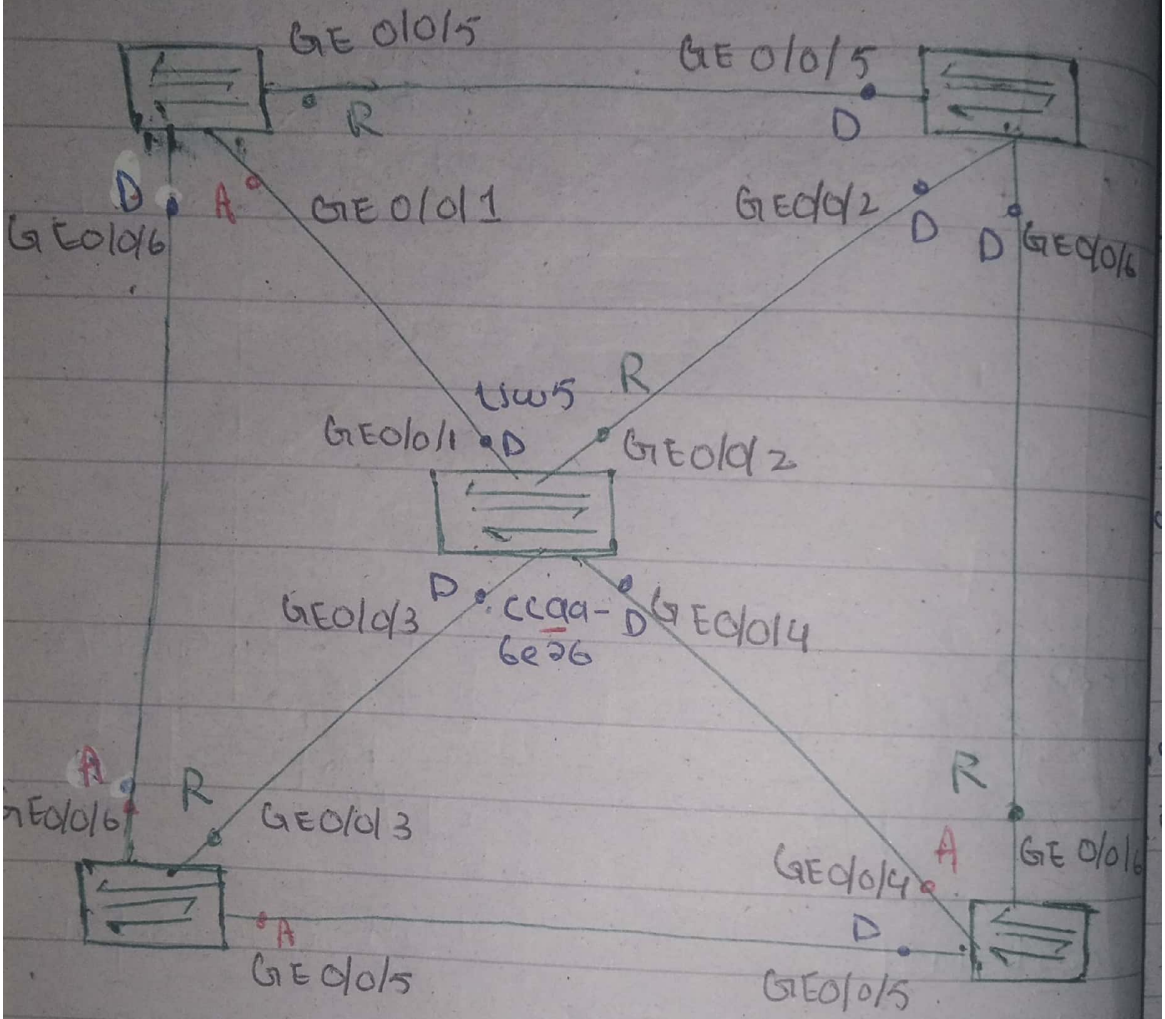
Then, check loops in 3 switches one by one.

Confusion???

Root

Lsw1: cccd-20e2

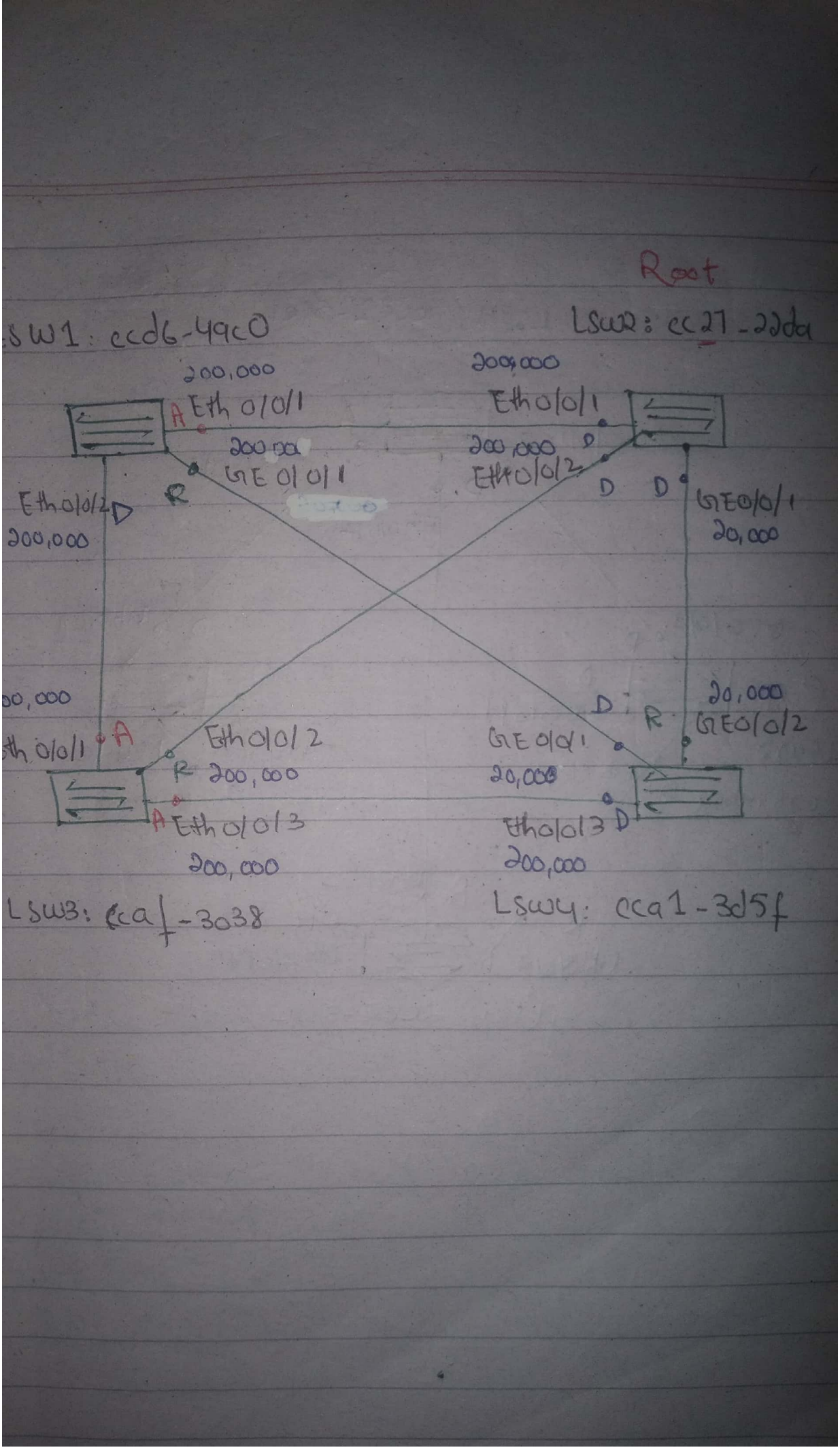
Lsw2: cc82-5a36



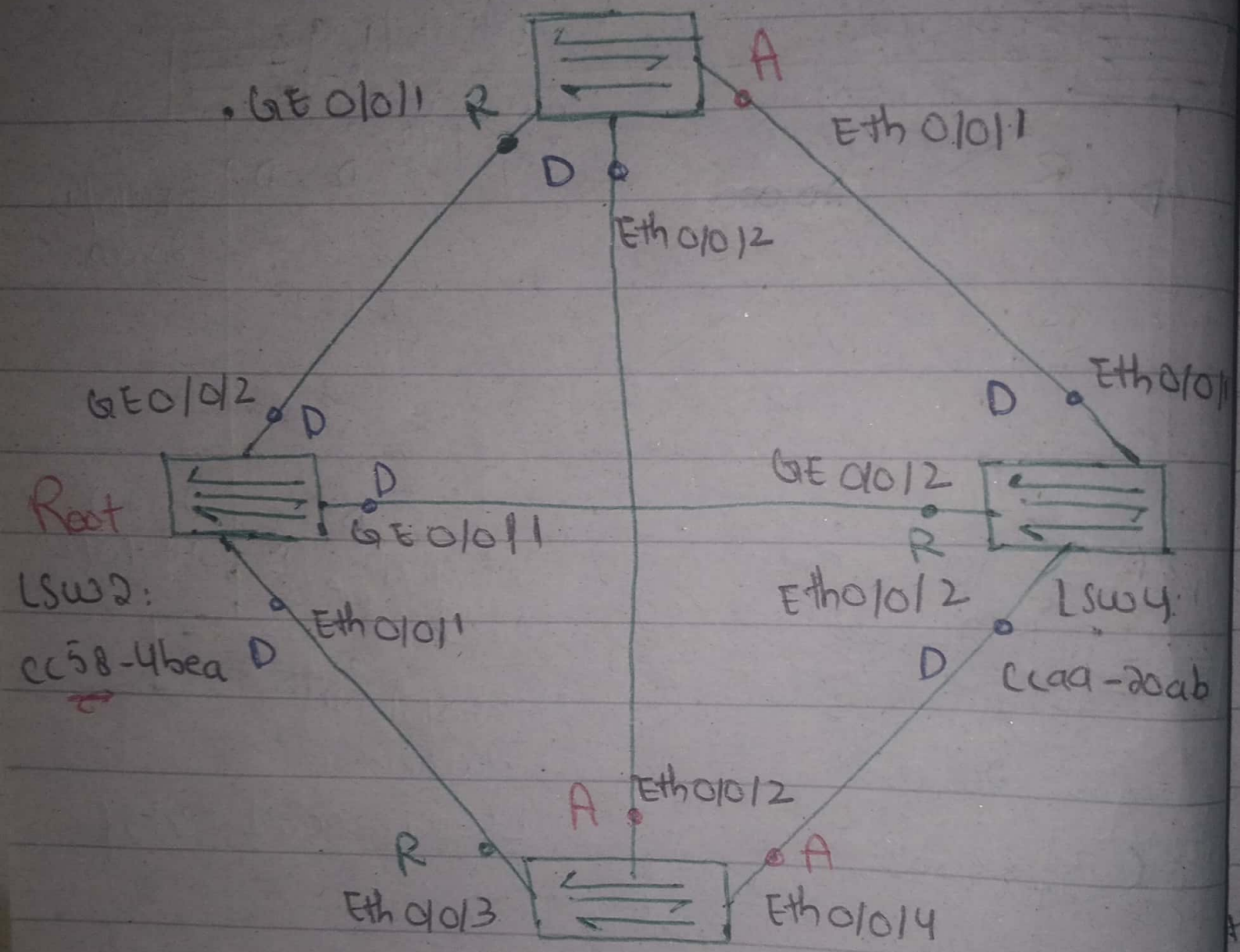
Lsw3: cc85-0a9f

Lsw4: ecf9-53da

Lsw2 > Lsw3 > Lsw5 > Lsw1 > Lsw4


Root
SW1: ecd6-49c0
LSW2: cc27-22da
200,000
Eth 0/0/1
A
200,000
GE 0/0/1
R
Eth 0/0/2
D
200,000
200,000
Eth 0/0/1
200,000
Eth 0/0/2
D
D
D
GE0/0/1
20,000
00,000
th 0/0/1
A
Eth 0/0/2
R
200,000
A
Eth 0/0/3
200,000
D
R
20,000
GE0/0/2
GE 0/0/1
20,000
Eth 0/0/3
D
200,000
LSW3: cca1-3038
LSW4: cca1-3d5f

LSW1 : cccc2-58e1



LSW3: cce8-3012

new bridge > old bridge for root bridge
MAC high MAC low

use config to make new bridge as root

STP PORT STATES:

- Disabled
- Blocking
- Listening
- Learning
- Forwarding

It takes atleast 15 seconds to convert from one state to another.

Huawei supports MSTP by default hr vlan ka
MSTP: Multivlans Spanning Tree Protocol alg stp nikalta h
RSTP: Rapid spanning Tree Protocol.
timing of state conversion is less.

H.W
- Edge Ports
- STP config

bridge priority is set with multiples of 4096.

Cost
Priority
Port number

ip config /all
cmd

II Domain Name Server (DNS):

IPv 4 : 10.57.65.16
pvt IP

- Service DNS Server: 192.168.1.4
pvt IP
- DNS Server (resolves DNS queries)

ping www.facebook.com
on cmd to check FB ip address

nslookup
Default Server: ns1.neduet.edu.pk
Address: 192.168.1.4

ns lookup mode me ajyenge
ab direct ping krskte (no need to write ping)

> www.facebook.com

"

192.168.1.4
↳ is ny bh kisi or server se reply lay hai (we are not owner)

actual facebook server ka name

Non-authoritative server
Name: star-mini.c10r.facebook.com
Addresses: ipv4 add
ipv6 add
Aliases: www.facebook.com

ab → reason: different countries (judge on the basis of ip address)

> www.geo.tv

Name: www.geo.tv

Addresses: 104.16.123.91
104.16.122.91

Two ips isliye use krti q k Load balancer krna hta a

> www.neduet.edu.pk

Server:

Address:

Name:

Address: 192.168.2.219

private ip

Non-authoritative likha nhi aya (we are the owner)

Two types of network
- on the basis of ip
- Physical boundaries (LAN, WAN, MAN

↓

ISP ko use kse bghte aik hi network pr communicate kr skte (same network on the basis of physical boundary)

tracert 192.168.1.4 kon kon si jaga se guzrs k jo the

Request timed out (hop)

ping ki request ko block krta hua

Famous DNS server -> Google 8.8.8.8

Koi chz bahir se access krwani h us k 2 interfaces bnte hn (internal & external)

Server 8.8.8.8 (ye google DNS server not mine)

apna dns server change krdega

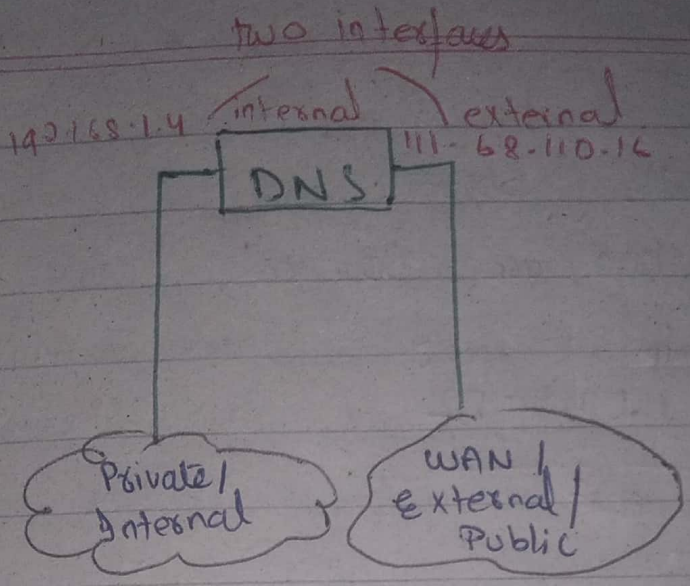
www.nedunet.edu.pk

Non authoritative answer:

Address: 111.68.110.16

ned public server ki ip

Prefix -> subdomain



prefix suffix

> cct.neduet.edu.pk

Non authoritative :

Name:

Address: 111.68.110.235

Aliasis

cct > se.neduet.edu.pk

"

"

Address: 111.68.110.235

"

Same sb aik hi server px hosted hain how to distinguish?

Configuration level: Alias defined folders of cct, se after ip.

Port level:

Total ports 65535

Starting 1000 are reserved

ip port

192.168.1.3 : 82

socket

home address : ip

home gates : port

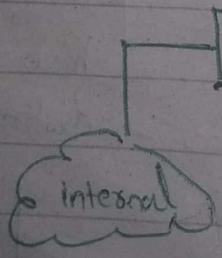
ip address & port -> socket

hacking is done through ports.

www.neduet.edu.pk : 8080

www.neduet.edu.pk : 53

] Two diff service but same domain name same IP diff Port



This scenario can be made for high confidential service / servers and Bahir wala jye and wala bahir na jye.

↑ records saved in the Domain servers bain

13 Top level DNS servers known as TLD. a to m

saves records in form NS

DNS server registers to TLD
(google /donya ko btany ki liye)
8 hours for maximum convergence.
DNS updates at

TLD saves records in form of NS

NS ns1.nedoet.edu.pk 111.68.111.22

NS nust2.edu.pk 112.68.11.3

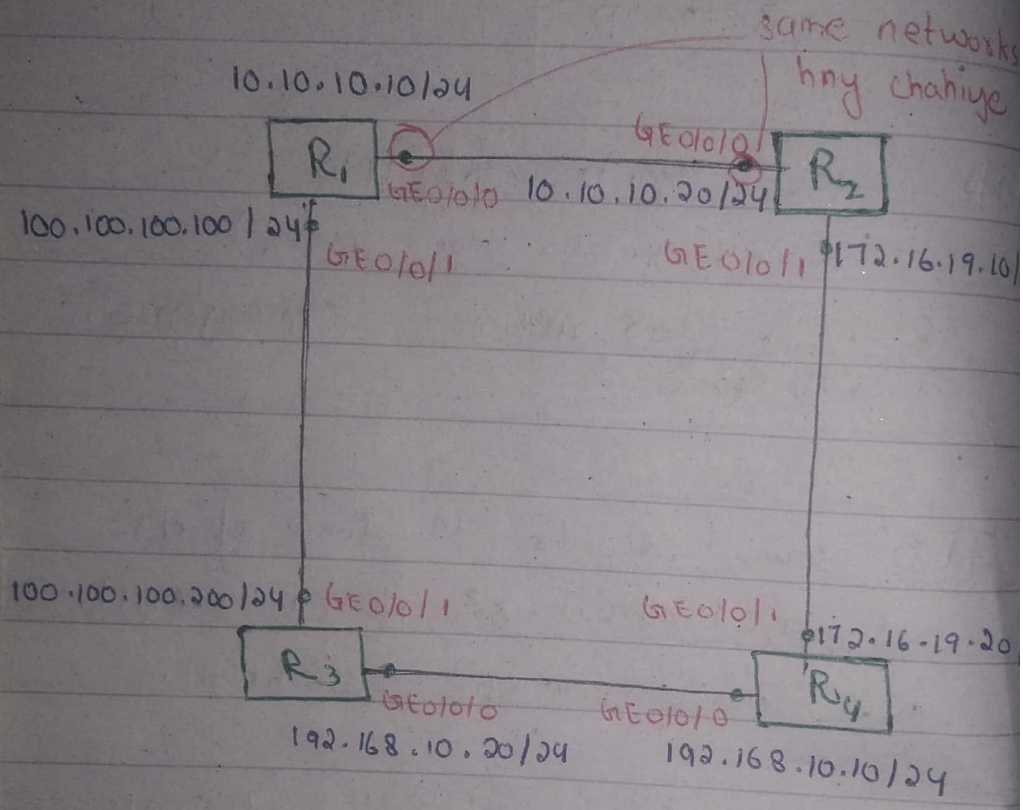
NS -> Name Server Record of DNS Server.

Small Network -> Static Route

Large Network -> Default Route
or
Dynamic Route

STATIC ROUTE:

Used jhn limited resource ka network ho.



- Ping each interface.
- Router doesnot support broadcasting.
- Router turns down broadcast.
- Router itself is Gateway.

To check IPs on interfaces:

[R1] display ip interface brief

alternate way -> display current-configuration

Patten matching:

[R1] display current-configuration | ?

to know further command

include exclude begin

[R1] display current-configuration | include address

copy bna k routing table ki jb ko dedi means. routing-table exchange.

To check what info router has:

[R1] display ip routing-table

Proto -> direct

Itself or that is directly connected.

Nexthop

Where to send for next interfaces.

10.10.10.10/32 -> exactly yhi ip

10.10.10.0/24 -> Network ID.

127.0.0.0/8 -> Loopback address

127.0.0.1/32 -> Loopback ip

- Router ko btana pta hai k knsa route krna hai.

- OR xyz khn se accessible hgi

Communicate with 192.168.10.X from R1.

R1

↓ send

192.168.10.X to 100.100.100.200

[R1] ip route-static 192.168.10.0 255.255.255.0 100.100.100.200

[R1] ping 192.168.10.20

ping 172.16.19.10/24 from R3

R3

↓

172.16.19.X to 100.100.100.100

reverse path -> give reverse static route
wapis jany ka rasta bh hna chahiye.
ping 10.10.10.10 from R4

[R4] ip route - static 10.10.10.0 255.255.255.0
192.168.10.20

[R3] ip route - static 10.10.10.0 255.255.255.0
100.100.100.100

Task :- ha router dusre interface ko
ping ka paye

[R4] tracert 10.10.10.10

All Routers Should Be able To Ping All Interfaces:

[R1] ip route-static 172.16.19.0 24 10.10.10.
[R1] ip route-static 192.168.10.0 24 100.100.10

[R2] ip route-static 100.100.100.0 24 10.10.10.10
[R2] ip route-static 192.168.10.0 24 172.16.19.20

[R3] ip route-static 10.10.10.0 24 100.100.100.100
[R3] ip route-static 172.16.19.0 24 192.168.10.10

[R4] ip route-static 10.10.10.0 24 172.16.19.10
[R4] ip route-static 100.100.100.0 24 192.168.10.2

10.10.10.10
10.10.10.20
100.100.100.100
100.100.100.200
192.168.10.10
192.168.10.20
172.16.19.10
172.16.19.20

On what basis routing table chooses a route?

192.168.0.0/16
192.168.1.0/24 ✓

192.168.1.1 ↑ chooses bcz of longest match.

Two cables:

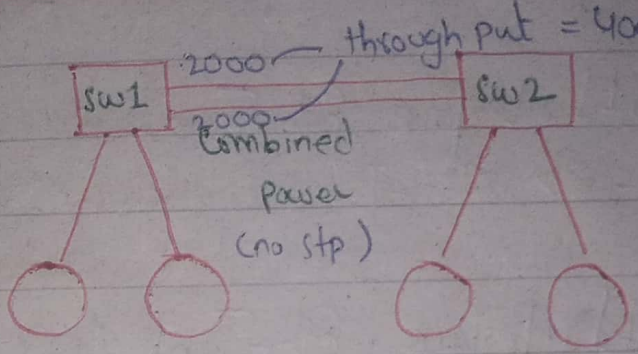
Either use as a fault tolesant

or Combined Power.

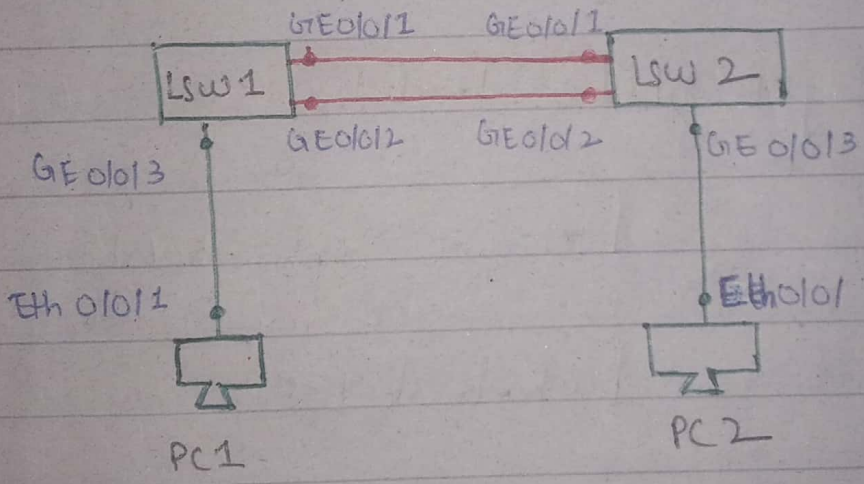
Stp won't effect,

Static combine treat as a single connection

LINK AGGREGATION:



ENSP



IP Address: 10.10.10.10/24 IP Address: 10.10.10.20/24

[PC1] ping 10.10.10.20

- Aggregation in Huawei → Ethernet-trunk
- It is logically created and linked to physical ports.

[LSW1] display interface brief

[LSW1] interface Eth-Trunk ?
  <0-63> Eth-Trunk interface number

[LSW1] interface Eth-Trunk 1

[LSW1-Eth-Trunk1] interface GigabitEth 0/0/1

[LSW1-GigEth0/0/1] eth-trunk 1

[ ] interface GigabitEth0/0/2

[ ] eth-trunk 1

[LSW2] interface Eth-Trunk 1

[LSW2-Eth-Trunk1] interface Gigabith Eth 0/0/1

[LSW2-GigEth0/0/1] eth-trunk 1

[ ] interface GigabitEth0/0/2

[ ] eth-trunk 1

[LSW2] display interface brief

Trunk number should be same.

[PC1] ping 10.10.10.20 -t
will not stop after 5 packets

PC1 and PC2 both have ethernet cables while the switch ports have Gig. The capacity of PC1 and PC2 have less throughput 100MBps. Therefore, the link aggregation is not beneficial here.

Link aggregation will be beneficial in switch connection.

- Remove the connection during ping. (only one)
  It will recalculate and restate the packet transmission. delay
  fault tolerant.
- Add the connection again.

This was static link aggregation.

Self-Study

LACP mode of Link Aggregation / Ethernet Trunk:

for

- It will not delay / recalculation, immediately continue the packet transmission.

- Port Priority.

- 4 Ports -> 3 Packet Transmission
  1 fault Tolerance

Link Agg:

Default Precedence of Direct Route is 0.

Default Precedence of Static Route is 60.

Preference In Link Agg:

R1]ip route-static 172.16.19.0
" " 192.168.10.0 24 10.10.10.20
" " 100.100.100.200
preference 50.

To turn off interface:
shutdown
to turn on interface
undo shutdown

If the preference of two same routes is same. The one which is configured first (i.e. on top of routing table) will be chosen by the router.

Static route will be used in small networks.

Default Route:

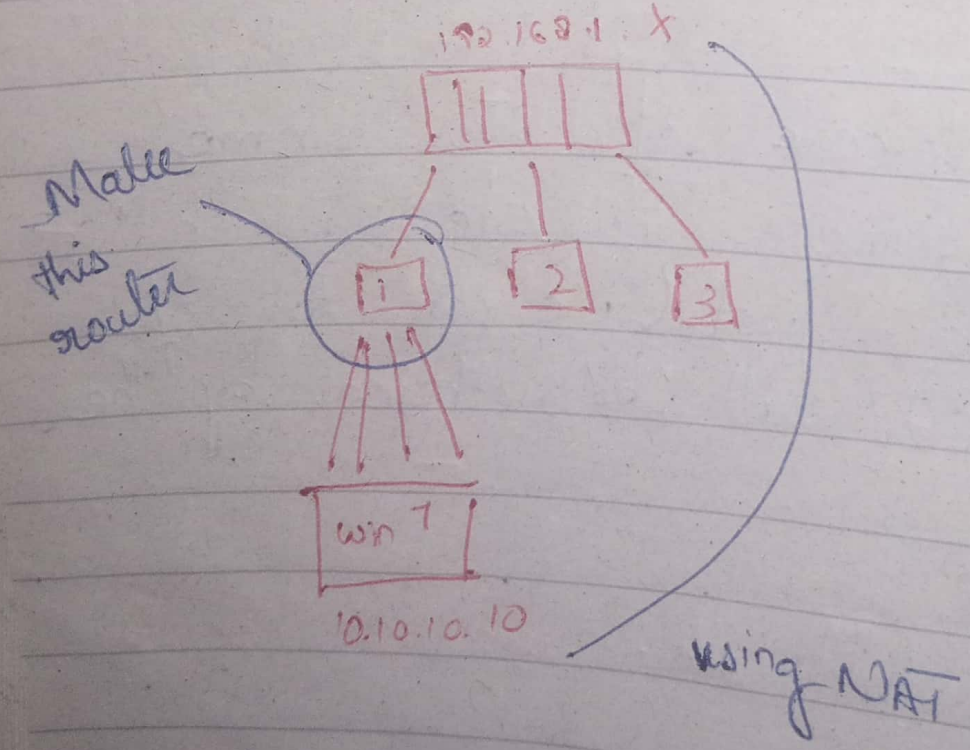
R1]ip route-static 0.0.0.0 0.0.0.0 10.10.10.20
First checks entry in routing table then chooses default route if entry is not present.

cmd > route print

TASK:

- virtual machine of windows 10 on vm ware
- NAT

outside machines ping the virtual machine ip using NAT



CONSOLE:

Real world configuation on console by connecting Router to PC using CTL.

- Telnet connected
- Console with putty

CTL -> console cable

Console Security -> restrict user not to come without password.

interface console 0.

user-interface console 0.

authentication:

1) password based
2) user id + password
3) NO authing.

① login which mode

[Huawei-ui-console 0] authentication mode password

~~Privelege level~~ (Huw)

② How much privelege?

[ ] use privilege level 15

[ ] set authentication password?

③ How to store its password?

cipher (display encrypted)

simple (display as it is in cussent only)

[ ] set authentication password cipher huawei123.

Password:

Task:

Telnet or SSH

config same through telnet

TELNET:

- It will be connected based on ip addresses.

Connect PC to R4 using copper cable

Telnet all routers from PC.

(config all routers from PC)

vty:

if default route is not used in large network

II) DYNAMIC ROUTING: Used in large network

RIP -> Routing Protocol

Routing Protocols:

RIP, ERGP, EIGP, BGP

* RIP is a dynamic routing protocol.

ENSP: (Same topology)

Remove all static routes from previous 4 router topology.

* RIP is a distance vector protocol.

Ye koi apna routing table dusre k sath share krta hai (Dynamic Routing)

Tables are matched and the best reachability is selected and updated in routing table.

[R1] rip ?

INTEGER -> processor id
ak processor k upar multiple chzen
Processor id will be unique in different PCs. that's why they are locally significant.

65535 -> maximum ports

Port id config with IP address
They are known as socket.
MAC Add + IP

Every router is taking responsibility of other 3 routers and itself.

RIP are of two types:

- Networkless
- Network ful

cr -> carriage return
cannot

- Classless Any subnet mask
- Classful (Addition of network -> consider default subnet mask)

[R1-rip] network 100.100.100.0

Error

Huawei supports Classful

[ ] network 100.0.0.0

No Error

Each router will advertise its networks to its neighbor

[ ] network 10.0.0.0

if don't want to exchange a specific network of a router from other routers no need to run this cmnd.

Routing tables is not updated yet.
Do same thing on all routers then share with each other

[R2-rip] network 192.168.10.0

[ ] network 100.0.0.0

[R3-rip] network

[ ] network

[R4-rip] network

[ ]

Msgs will come which means routing tables are being exchanged

Proto RIP - learnt through RIP

Pref

~~Cost~~ of Dyamic route 100

" " Static " 60

Static route will always be preferred

COST

Each router will advertise its networks to its neighbours.

Neighbours of R1 -> R2 & R3

Attach one more router to R3 (i.e, R5)

33.33.33.33 R3

33.33.33.34 R5

Info of R5 will not be given to any other router.

[R5-rip] network 33.0.0.0.

[ ] display ip routing-table

entry of 33 only on R3 route-table of R3 will be updated only

[R3-rip] network 33.0.0.0

[ ] display ip routing-table

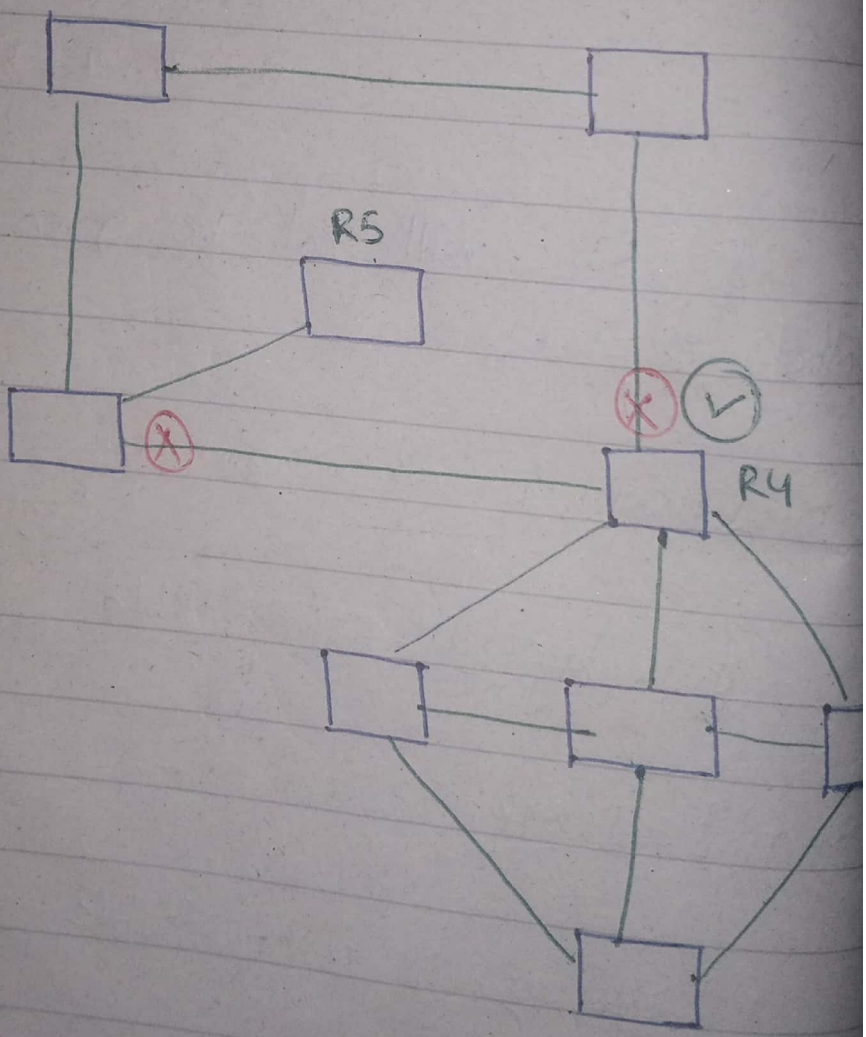
all route-table updated.

Shutdown interface 172.16.19.20/24

[R2] display ip routing-table

(Cost)
distance of 192.168. will be increased. (i.e, 2)

Khud identify krta jaega kisko
Populate krna & kisko nae krna.



Add 5 more routers on R4.
Enable rip on all and address networks
display routing table

Turn on . 172.16.19.20/24

display routing table

Shut down 192.168.10.20/24

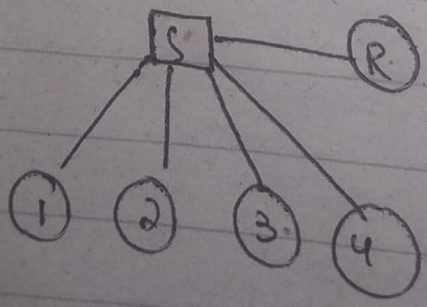
display routing table.

DHCP: (Dynamic Host Control Protocol)

Jo Jo devices request krskhin hn unko ips automatically assign krdeta hai.

DORA

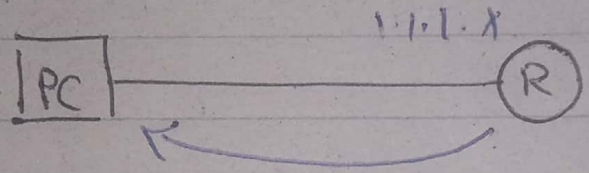
D = Discover
O = Offer
R = Request
A = Acknowledge



acl number standard 2000

Servers ko hmesha fixed ip rkhna prta h

ip assignment last se shuro hti h
1.1.1.254



will assign ip of 1.1.1.X to this interface.

Relay:

Std ——> Teacher ——> chairman

ipconfig /renew

0.5 lease renewal message

IPv6 Basics:

128 bits Hex format $128/4 = 32$

Basic IPv6 Header:

2001:0D88. . . .

Hextet

0000 1011

Padding

0000 : 0000 : 0000

0 : 0 : 0

::

:: sirf aik bar aata hai abbreviated m

0000 : 0000 : 0008 : 0000 : 0000

:: 8 : 0 : 0

0000 : 0000 : 0008 : 0000 : 0000 : 0000

0 : 0 : 8 ::

choice k kisko double colon likha h

0000:0000 ya 0000:0000:0000. The pref

is zyada Zeroes jahan hon wo ::

starting hextet of GUA

GUA -> public IP 2000:/3

ULA -> apny network pr jo chz FD00:/8 unique ho (private ip).

LLA -> APIPA FE80:/10
Automatic private IP address

Check static IP
if no DHCP server
if no APIPA (apny ap ko khod IP dedeta) 169.X.X.X
is subnet ki
169.X.X.X class B.

64 | 64
Network Host

Convert MAC address into EUI

Interface ID of an IPv6 Unicast Address

To get unique identifier in Link local Address

· EUI-64

① Break MAC Address in two:

MAC (hex) : 3C-52-82 | 49-7E-9D

② Insert FFFE in between

3C-52-82-FF-FE-49-7E-9D

8 8 8 8 8 8 8 8 = 64 bits

③ Convert 3C into binary

3 C

0011 1100 See what's written on 7th location and toggle.

0011 1110

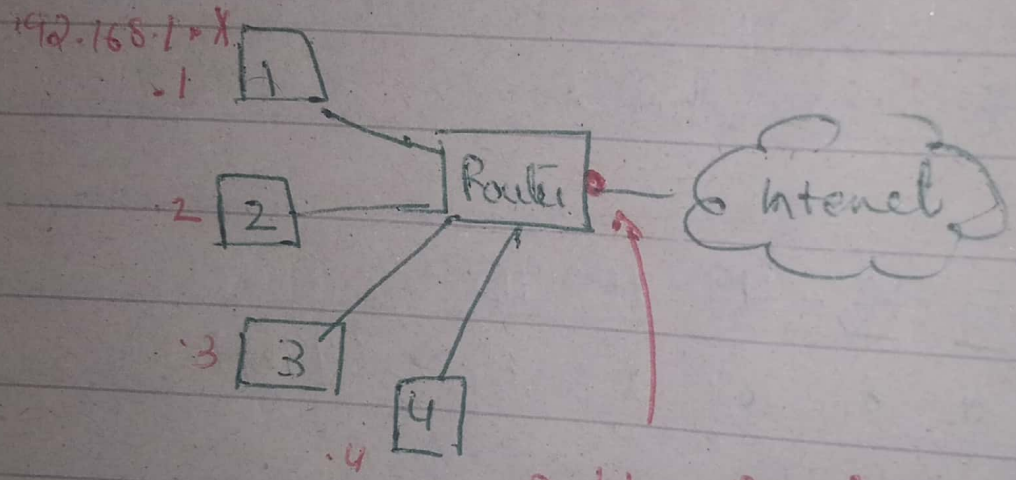
3 E

3E-52-82-FF-FE-49-7E-9D

Network Address Translation (NAT)

used in homes

Private IPs donot work at internet
Public IPs are used for internet



Public IP of router = 111.111.123.32

All 4 routers have same public IP →

Convert network address into public as NAT (private to public)

Translate

① Static NAT: one to one mapping

Different public IP for each private IP (IP Pool)

Disadv: we will have to buy public ~~private~~ IPs for every private IP.

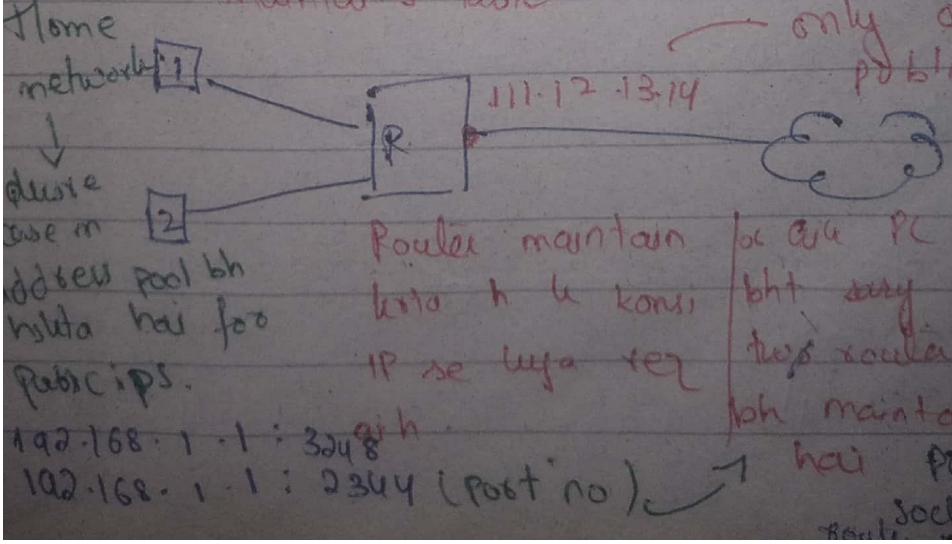
② Dynamic NAT:

Address pool se jo available hgi wo dedega private IP ko.

③ PAT (Port Address Translation)
(In huawei NAPT)

Network address and port translation

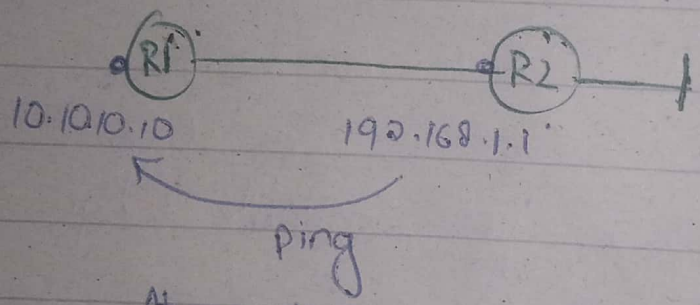
Maintains Table



cmd> netstata -a

H.w Read
- Link State protocol
- Distance vector protocol.

Loopback



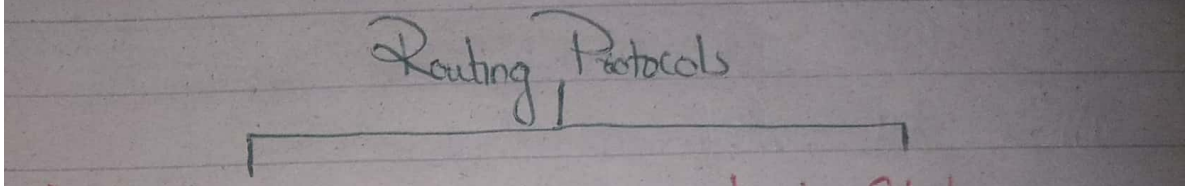
It won't ping
in this case we will use loop back

loop 1
loop 2
:

Loop back is virtual and always up or kisi se connect krne ki zrurat nhi (cable)

Usage of loopback in ospf.
ospf classless
rip classful

Routing Protocols (Dynamic)



- BGP
- EIGRP
- RIP

- OSPF
- ISIS

Checks distance

Router send info about their directly connected networks only to neighbours

Checks distance + bandwidth

- Router send info about their links to all other routers.

Each router selects best routes from the perspective of the neighbours.

- Each router makes router selection decision itself.

Slow Convergence

- Fast Convergence

Lower CPU and Memory Usage

- Higher CPU and Memory usage

Prone to Errors loops, tables are not updated

- Reliable

OSPF (Open Shortest Path First)

Classless

When all routers are deployed on OSPF:

LSA (Link State Advertisement)

- Links ki info advertise krna

LSDB (Link State Data Base)

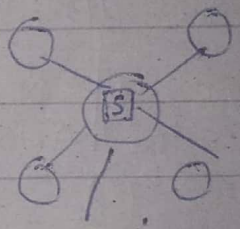
- LSA stored on LSDB
- Saray routers k pas aik jesa database LSDB bnega

Routing Table:

- LSDB se shortest le k Routing table update.

Neighbourship
neighbours
(directly Connected)

Adjacency
neighbours +
info share
Directly connected
+
- Same Subnet
- Same Area



Same subnet

- Routers ko choty choty areas my tor dety hn.
- Area 0 is must as it is backbone in OSPF

Routers have router IDs.
- Either manually configured
- or automatically.

Automatic Selection for Router ID:

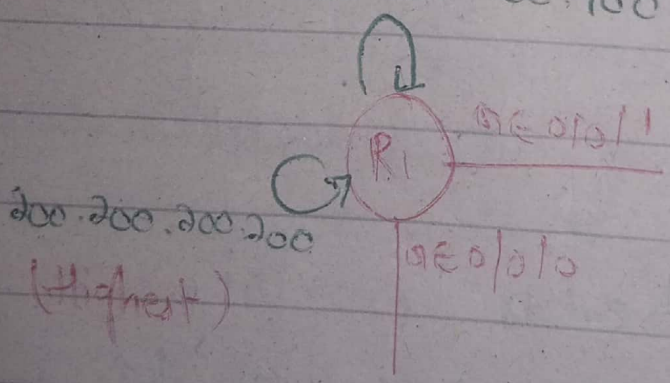
1st Case:

- Checks loopback Addresses

- Highest IP of available loopback Address

Router ID = 100.100.100.100

in case of only one loopback address



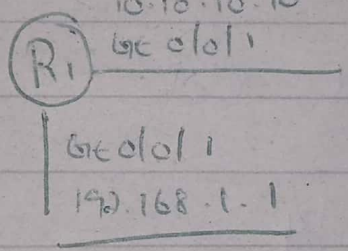
Router ID = 200.200.200.200

Adminstatively down (shutdown)
Down (far end PC) khod bnd krna
50 > Router -> dusra area bnyega

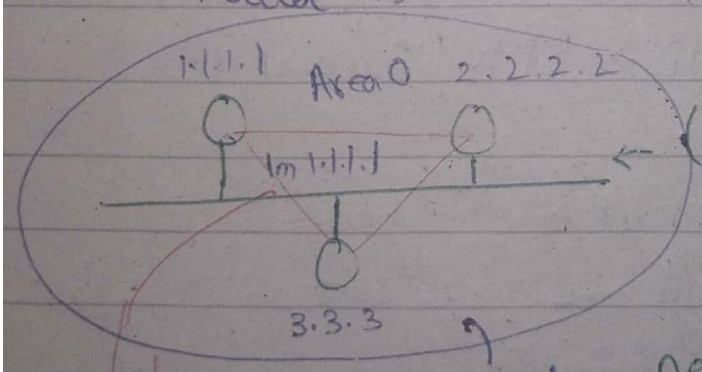
2nd Case: (Interface based)

- Interface should not be down.
(far end side pr pc down ho)

- Highest IP of the up interface



Router ID = 192.168.1.1

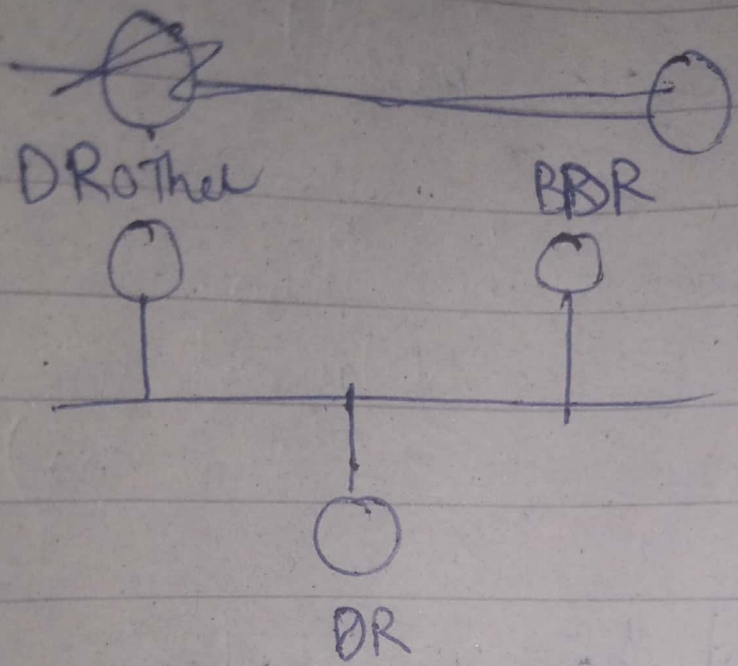


(sab ka LAN pr hona)
means sab ki network hga
subnet same, area same -> adjacency

Virtual mesh

1.1.1.1 -> broadcast network create
DR BDR.

fast solve mesh prob



DR, BDR, DROther will be selected based on:

1) Priority
2) Router ID

Higher Router ID -> DR (Designated Router)
2nd Higher Router ID -> BDR (Backup DR)

Jha ~~DR BD~~ Broadcast domain ^ nhi hnd
no DR BPR will be selected

Read -> Master Slave

Transport Layer:

A transport layer receives data from an application layer protocol, encapsulates the data with the corresponding transport layer protocol header, and helps establish an end-to-end (port to port) connection.

PDUs transmitted at the transport layer are called segments.

Role Of Transport Layer:

1) End-to-End Delivery (Port-to-Port Delivery)
2) Uses two protocols:
   - TCP (Connection Oriented)
   - UDP
   - TCP provides reliability, in-order delivery, (proper guarantee)
     No loss of data
   - TCP first establishes connection.
3) Error Control using Checksum Method
5) Congestion Control ~~& Flow Control~~

6) Flow Control

- At what speed and which size of the message, sender is sending to receiver?

- We use method Advertising the wind

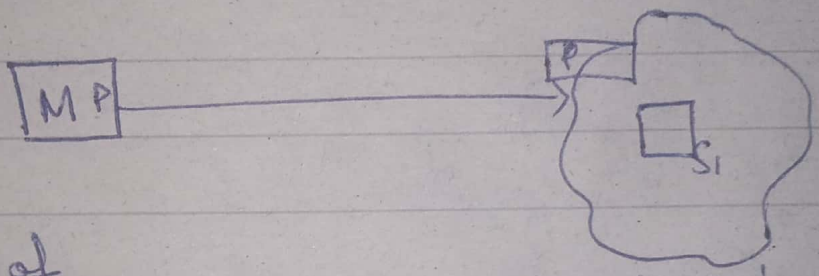
- Receiver at first sends the size of window to sender/and size of message.

7) Multiplexing / Demultiplexing

TCP:
Socket Address (48 bit address

IP Address + Portnumber
(32 + 16 = 48)

- To uniquely identify a connection.



TCP of Host A

- Establish connection first.

Port numbers:
0 - 65355 out of which
- 0 - 1023 well defined
- 1024-49151 reserved
- 49152 - 65535 Assigned by OS of servers

- TCP stores connection in buffer.
Only IP address is not sufficient.
" Port no. " "
To uniquely identify we need Port no + IP.

TRANSPORT LAYER:

PORTS & SOCKETS:

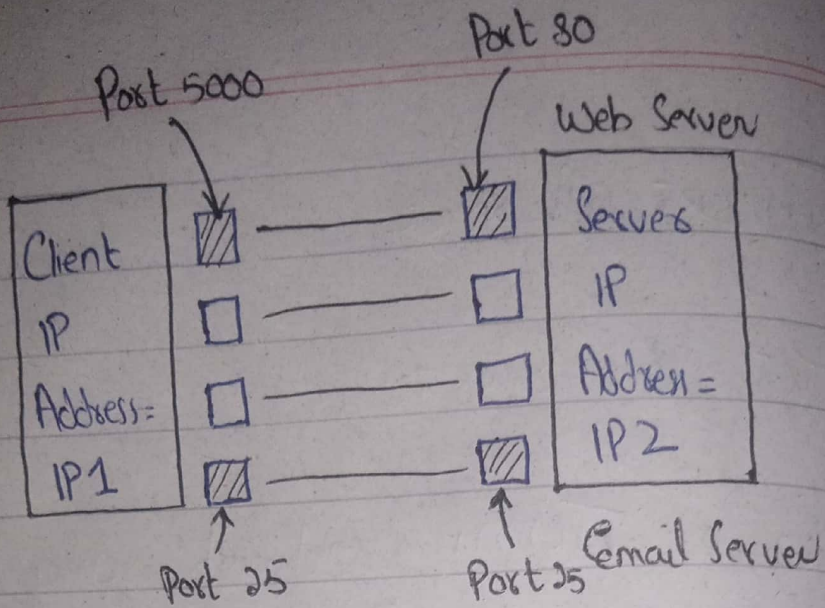
On a TCP/IP network every device must have an IP address.

The IP address identifies the device/computer.

However, an IP address alone is not sufficient for running network applications, as a computer can multiple applications or services.

The use of ports allow computers/devices to run multiple services/applications.

Just as the IP address identifies the computer, the network port identifies the application or service running on the computer.



IP + Port number = Socket

Port Number Ranges & Well Known Ports:

Ports are represented by 16-bit unsigned integers, allowing a range of values from 0 - 65535.

- Well-known ports: 0 - 1023
  Allocated to server services by IANA.
- Registered ports: 1024 - 49151
  Registered for services with IANA. (Semi-reserved)
- Dynamic & Private ports: 49152 - 65535
  Used by client programs.

Following are some well-known ports:

FTP (port 21)
Telnet (port 23)
HTTP (port 80)
HTTPS (port 443)
RIP (port 520)
DNS (port 53)

Socket:

A socket is one endpoint of a two-way communication link b/w two programs running on the network.

It is a communication b/w two computers uses a socket.

Each end of connection will have a socket.

Port no or IP Address are not lonely sufficient that's why we need their combination to uniquely identify a established connection

b/w client server.

Hence, Socket is the name given to the combination of IP Address & port.

Socket address is 48 bits address, containing 32 bits IP address & 16 bits port number.

A socket is the interface b/w the application layer & transport layer, also referred to as API b/w application & network.

Client port numbers are dynamically assigned and can be reused once the session is closed.

TCP Connection Establishment:

Connection establishment is a crucial step in communication b/w two devices using a reliable Transport Layer Protocol such as TCP. It involves a series of steps to setup a reliable communication channel before actual data transmission can begin. The process is known as "Three-way handshake" in TCP.

TCP Handshake involves following steps in establishing the connection:

Step #1 (SYN):

The initiating device (client) sends a SYN (Synchronize) packet to the receiving devices (server) to request a connection. SYN Request segment contains the following information in TCP Header:

1- Initial Sequence number
2- SYN bit set to 1
3- Maximum Segment size
4- Receiving window size.

STEP #2 (SYN-ACK):

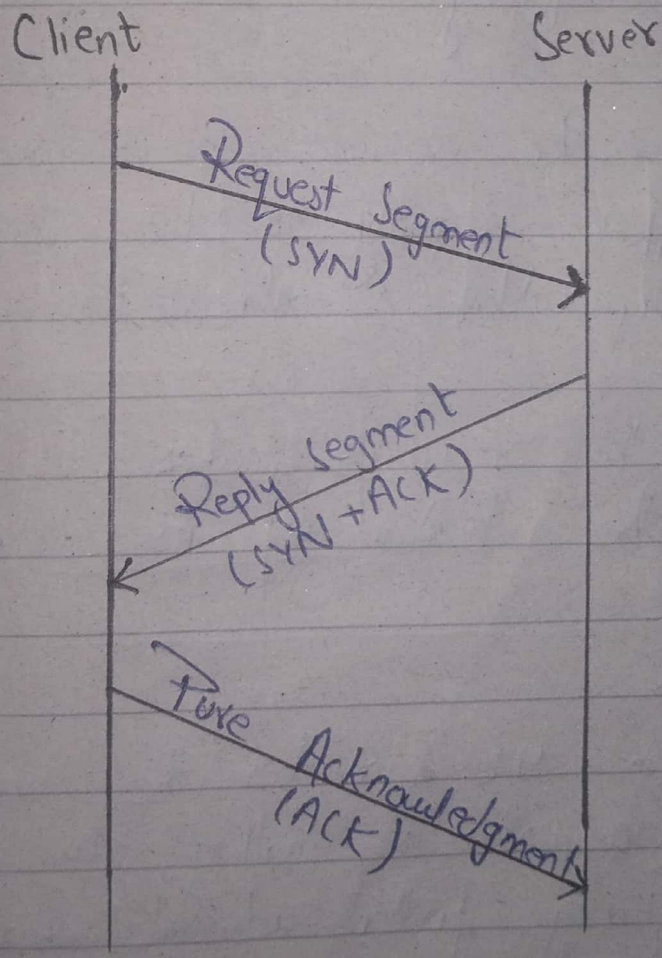
Upon receiving the SYN packet, the receiving device responds with a SYN-ACK packet. The SYN-ACK packet acknowledges the receipt of the SYN packet and also contains a randomly generated acknowledged number. The receiving device also allocates resources for the connection.

SYN-ACK reply segment contains the following info in TCP header:

1- Initial Sequence number
2- SYN bit to 1
3- Maximum segment size
4- Receiving window size
5- Acknowledgement number
6- ACK bit set to 1.

Step #3 (ACK):

Finally, the initiating device acknowledges the receipt of the SYN-ACK packet by sending an ACK (acknowledgment) packet to the receiving device. This completes the three-way handshake, and both devices are now connected and ready to exchange data.



With these, a Full Duplex Connection is established.

Flow Control:

Flow control deals with the amount of data sent to the receiver side without receiving any acknowledgement.

Flow control ensures that the sender doesnot overwhelm the receiver by sending data too quickly.

It allows the receiver to communicate its buffer's capacity to the sender, preventing packet loss & data overflow.

In TCP, the receiver specifies a window size in the header of its acknowledgment packets.

This window size indicates the amount of data the receiver is willing to accept before requiring further acknowledgement.

Congestion Control:

Congestion control refers to techniques & mechanism that can:

- Either prevent Congestion before it happens.
- Or remove congestion after it has happened

TCP reacts to congestion by reducing the sender window size which is determined by the following two factors:

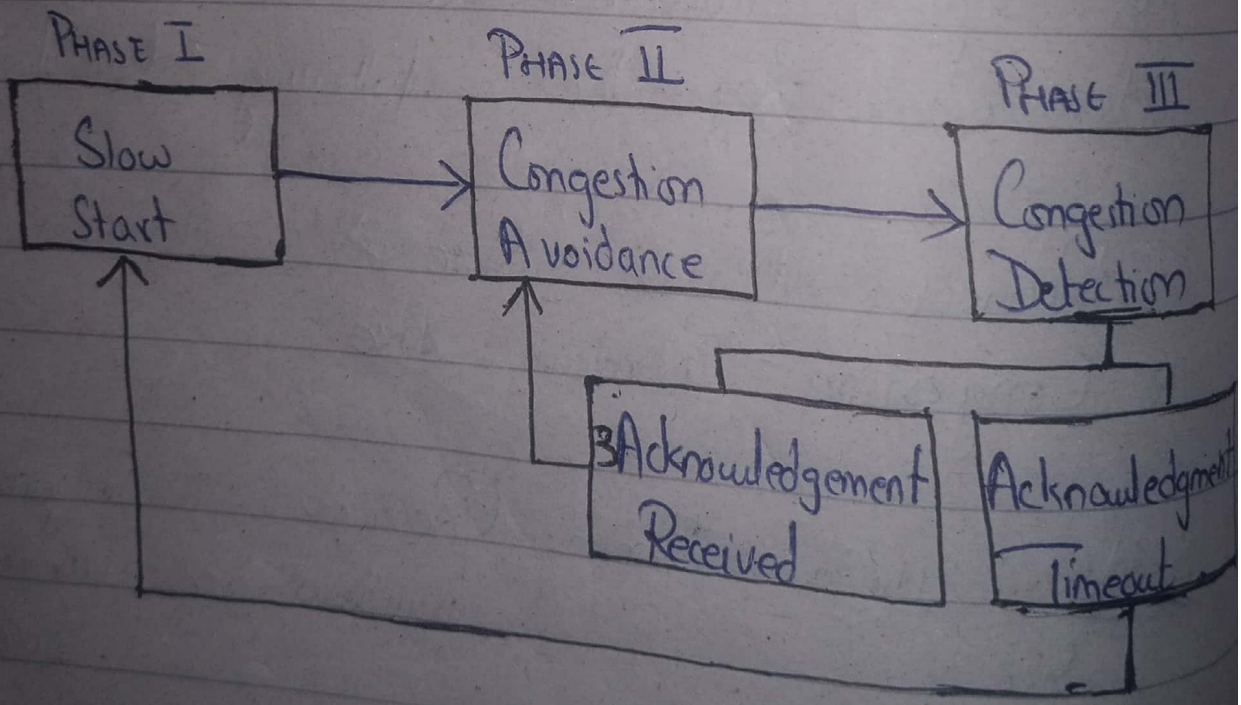
- Receiver Window Size
- Congestion Window size

Sender Window Size = Minimum (Receiver window size, Congestion window size)

TCP Congestion Policy:

TCP's congestion policy has following three phases:

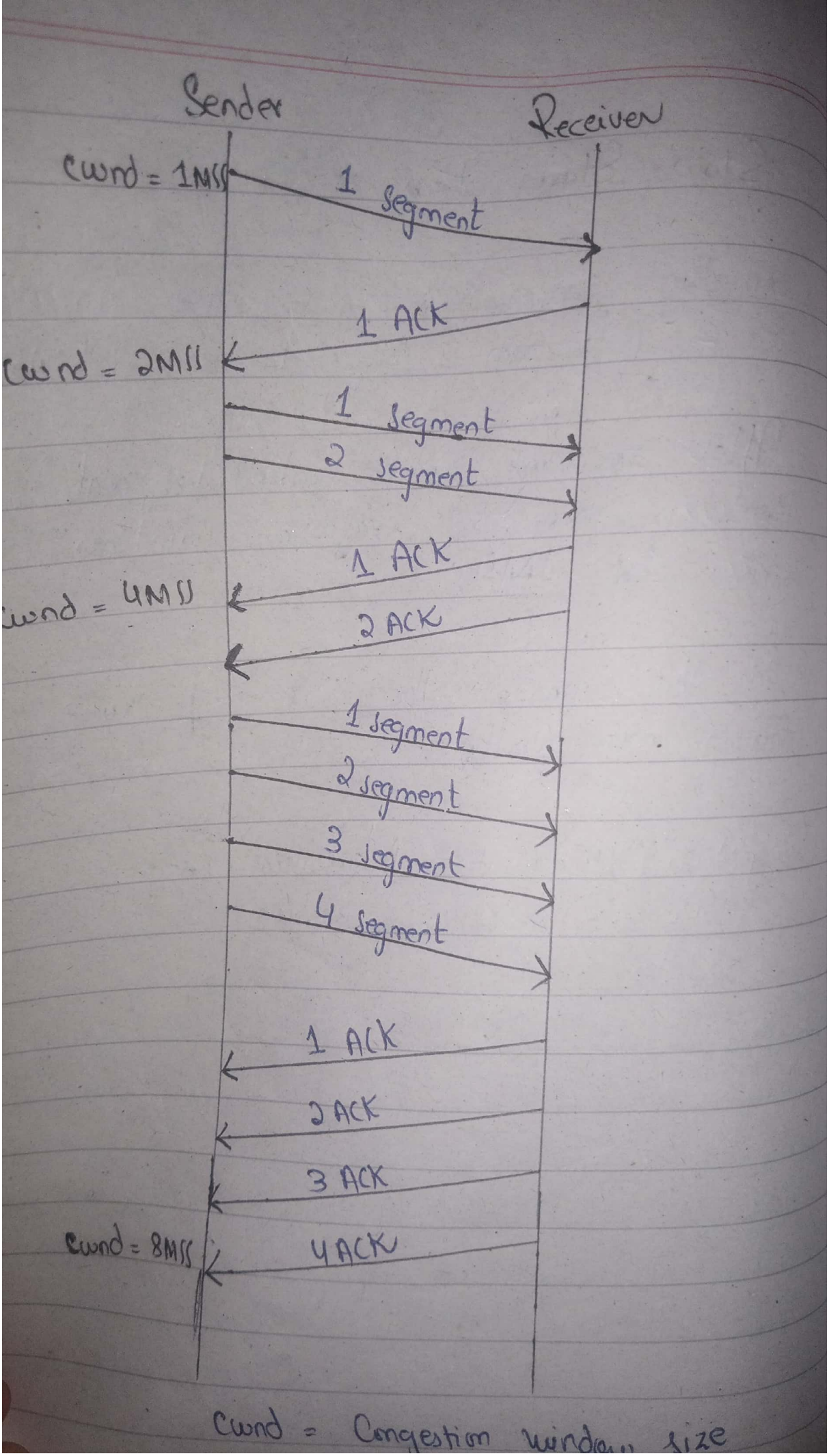
1- Slow Start
2- Congestion Avoidance
3- Congestion Detection



1. Slow Start Phase:

- Initially, sender sets congestion window size = Maximum Segment Size (1MSS).
- After receiving each acknowledgment, sender increases congestion window size by 1MSS.
- In this phase, the size of window increases exponentially.

Congestion Window Size += Maximum Segment Size.


Sender
Receiver
cwnd = 1MSS
1 Segment
1 ACK
cwnd = 2MSS
1 Segment
2 segment
1 ACK
cwnd = 4MSS
2 ACK
1 segment
2 segment
3 segment
4 segment
1 ACK
2 ACK
3 ACK
cwnd = 8MSS
4 ACK
Cwnd = Congestion window size

- After 1 round trip, cwnd = $(2)^1$ = 2MSS
- " 2 " " " = $(2)^2$ = 4MSS
- " 3 " " " = $(2)^3$ = 8MSS

and so on.

This phase continues until the congestion window size reaches the slow start threshold.

Threshold = Maximum no. of TCP segments that receiver window can accomodate / 2

= (Receiver window size / MSS) / 2

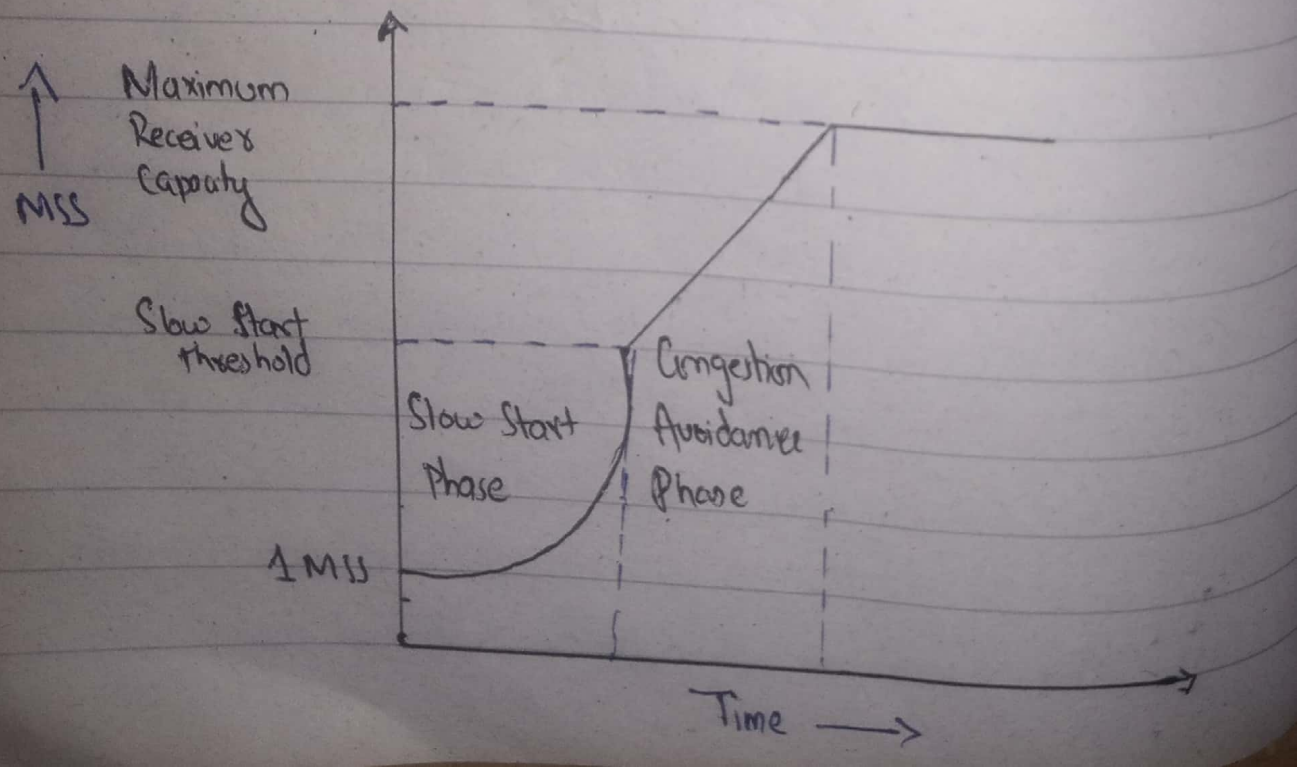
2. Congestion Avoidance Phase:

After reaching the threshold:

- Sender increases the cwnd linearly to avoid congestion.
- On receiving each acknowledgment, sender increaments the cwnd by 1.

Congestion Window Size + = 1

This phase continues until the cwnd becomes equal to the receiver window size.



3. Congestion Detection Phase:

When sender detects the loss of segments, it reacts in different ways depending on how the loss is detected.

Case #01 Detection On Time Out:

- Time out timer expires before receiving the acknowledgement for a segment.
- Stronger possibility of congestion in network.
- Chances that a segment has been dropped in the network.

Reaction:

In this case, sender reacts by:

- Setting the slow start threshold ≠ ~~cwnd~~ to the half of current cwnd.
- Decreasing the cwnd to 1MSS.
- Resuming the slow start phase.

Case # 02 Detection on Receiving 3 Duplicate Acknowledgments.

- Sender receives 3 duplicate acknowledgments for a segment.
- Weaker possibility of congestion in network.
- Chances that a segment has been dropped but few segments sent later may have reached.

Reaction:

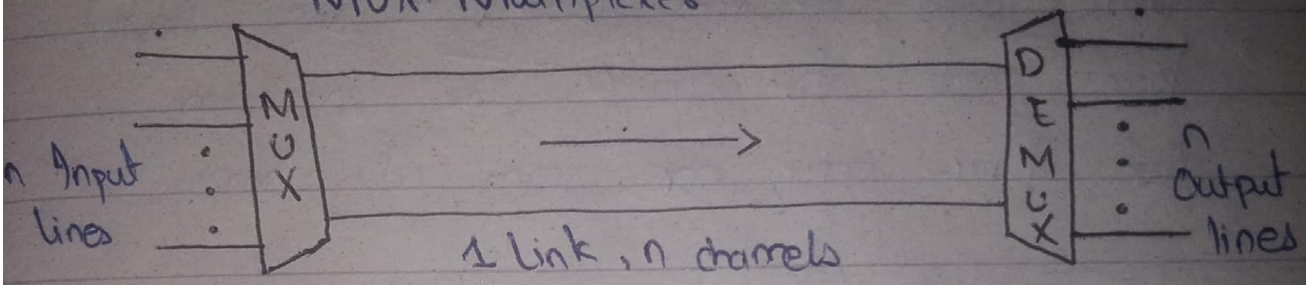
In this case, Sender reacts by:

- Setting the slow start threshold to the half of current cwnd.
- Decreasing the cwnd to slow start threshold.
- Resuming the congestion avoidance phase.

Multiplexing & Demultiplexing:

DEMUX : Demultiplexer

MUX: Multiplexer



- Multiplexing:

  - Process of:
    - Collecting data from multiple application processes of the sender.
    - Enveloping the data with headers.
    - Sending them as a whole to the intended receiver.

  - Achieved by using a device called Multiplexer (MUX) that combines n input lines to generate a single output line

  - Follows Many to one.

Why Multiplexing?

- Transmission medium used to send signal from sender to receiver. The medium can have only one signal at a time.

- Multiple signals to share one medium, divide medium so that each signal is given some portion of the available bandwidth.

- When multiple portions share common medium, there is a possibility of collisions.

- Multiplexing is used to avoid collisions.

Types of Multiplexing Techniques.

Each type offers adv and is suitable for specific applications. The choice depends on factors:

- nature of signals
- bandwidth requirements
- no. of devices sharing medium.

1. Analog:

- Frequency Division Multiplexing (FDM): Suitable for analog signals & multiple users sharing a common medium.
- Wavelength Division Multiplexing (WDM): Suitable for high-speed data transmission over fiber optic cables.

2. Digital:

- Time Division Multiplexing (TDM): Suitable for digital signals & provides

fair access & efficient utilization of available bandwidth.

- Demultiplexing:

- Achieved by using a device called Demultiplexer (Demux).

- At receiving end.

- Seperates a signal into its component signals (1 input, n ouputs)

- Follows one to many approach.

Why demultiplexing?

- At receiving end → multiple receipient to receive specific data.

- Demux extracts relevant data from combined signal and sends to appropriate output channel.

- Uses control signals to determine which output channel receives data.

- By demultiplexing, each receipent receives data with out interference from other signals.

Types of Demultiplexing Techniques:

1. Analog:
   - Frequency Division Demultiplexing
   - Wavelength Division "

2. Digital
   - Time "

ANALOG AND DIGITAL DATA TRANSMISSION:

1. Analog Data Transmission:

- Involves continuous signals that vary in amplitude & frequency.

- These signals can represent either analog data, like voice or digital data, which may pass through a modem.

- Analog signals achieve attenuation, becoming weaker as they travel over distance.

- To achieve longer distances, amplifiers are used to boost the signal energy.

- However, this process also amplifies noise components.

- As amplifiers are cascaded to achieve longer distances, the signal undergoes increasing

distortion. While analog data can tolerate some distortion & remain intelligible, cascade amplifiers introduce errors in digital data. ~~transmission~~

Advantages:

- Suitable for continuous data
- More tolerant of signal degradation over long distances.

Disadvantages:

- Susceptible to interference & noise, can distor signal & reduce data accuracy.

- Not efficient for handling discrete or digital info.

2. Digital Data Transmission:

Uses binary signals (1s and 0s) to represent information.

A digital data can be transmitted only a limited distance before attenuation, noise & other impairements endanger data integrity.

To achieve greater distances, repeaters are used.

A repeater:

- receives digital signal
- recovers pattern of 0s and 1s
- retransmits a new signal

Thus, the attenuation is overcome.

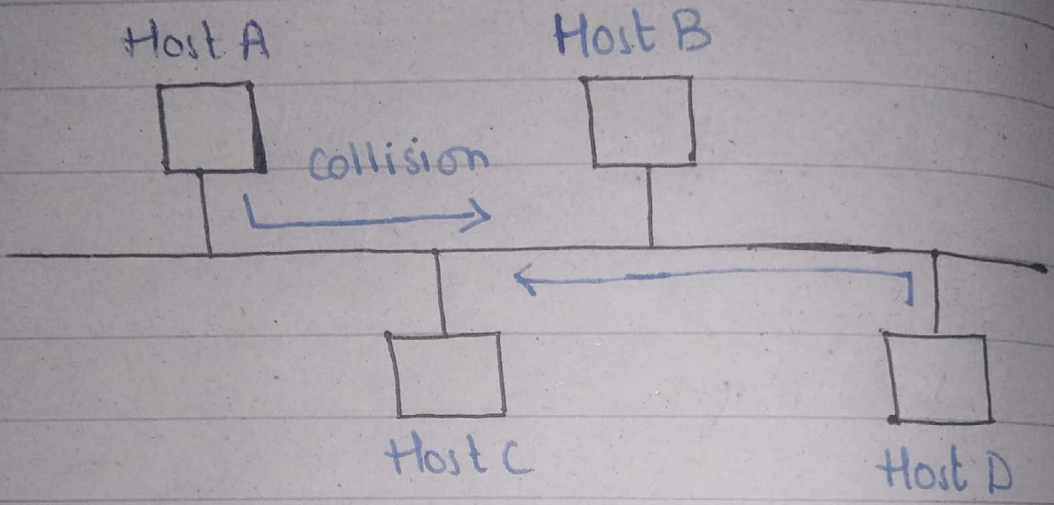
Advantages:

- Less susceptible to signal degradation, providing more reliable data integrity.
- More efficient in handling discrete data & complex info.

Disadvantages:

- Require higher bandwidth compared to analog.
- Processing and encoding digital signals can add some overhead.

Carrier - Sense Multiple Access With Collision Detection:



CSMA/CD is MAC Layer protocol. It defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision.

It defines how long the device should wait if a collision occurs. The medium is used by multiple data nodes, so each data node receives transmission from each of the other node on the medium.

Working Principle:

On a shared network, the Ethernet uses the CSMA/CD technology to avoid collisions. The CSMA/CD process is as follows:

1. A terminal continuously detects whether the shared line is idle or not.

   a) If the line is idle, the terminal sends data.

   b) If the line is in use, the terminal waits until the line becomes idle.

2. If two terminals send data at the same time, a collision occurs on the line, and signals on the line becomes unstable.

3. After detecting the instability, the terminal immediately ~~sends data~~ stops sending the data.

4. The terminal sends a series of disturbing pulses. After a period of time the terminal resumes data transmission.

The terminal sends disturbing pulses to inform other terminals, especially the terminal that sends the at the same time, that a collision occured on the line.

The working principle of CSMA/CD can be summarized as follows:

- Listen before send
- Listen while sending
- Stop sending due to collision
- Resend after random delay.

IPv6:

- Length = 128 bits
- Colons are used to divide the IPv6 address into 8 segments.
- Each segment contains 16 bits and is expressed in hexadecimal notation.
- Each segment is known as hextet

IPv6 Advantages:

1- Nearly Infinite Address Space:

The 128-bit address length provides numerous addresses, meeting the requirements of emerging services such as IoT and facilitating service evolution & expansion.

2- Hierarchical Address Structure:

Allocated more properly than IPv4, facilitating route aggregation (reducing the size of IPv6 routing tables), fast route query.

3- Plug & Play:

Supports Stateless Address Autoconfiguration (SLAAC), simplifying terminal access.

4- Simplified Packet Header:

The simplified packet header improves forwarding efficiency.

5- Security Features:

IPsec, source address authentication & other security features ensure E2E security, preventing NAT from damaging the integrity of E2E communication.

6- IMobility:

Greatly improves real-time communication & performance of mobile networks.

7- Enhanced QoS Features:

A flow label field is additionally defined & can be used to allocate a specific resource for a special service & data flow.

IPv6	IPv4
Address Length	
128 bits	32 bits
Packet Format	
A fixed 40 byte basic packet. header + variable length extension headers	A basic header containing the optional field to support extended features
Address Type	
Unicast, Multicast, Anycast	Unicast, Multicast, Broadcast
Address Configuration	
Static, DHCP, SLAAC	Static and DHCP

DAD

ICMPv6 - Gratuitous ARP

Address Resolution

ICMPv6 - ARP

Characteristics

- Unlimited no. of addresses - IPv4 address depletion
- Simplified packet header - Inappropriate packet header design
- Automatic IPv6 address allocation. - ARP dependency - induced flooding.

Need Of IPv6:

The world's population has reached 8 billion, with each person owning multiple devices such as PCs, mobiles, laptops and computers in public places like labs & libraries. Due to this exponential growth in the no. of devices, there is a severe shortage of IPv4 addresses, which are limited to approximately 4.3 billion.

To address the problem of IPv4 address exhaustion, technologies like Network Address Translation (NAT) & Classless Interdomain Routing (CIDR) were introduced in the 1990s. While these transition solutions have temporarily slowed down the rate of address depletion, they have not provided a permanent & comprehensive solution to the issue. To address the growing demand for unique IP addresses & overcome the

limitations of IPv4, a new version called IPv6 was introduced.

IPv4:

- 32 bits long
- Dotted decimal notation
- Address Range: 0.0.0.0 - 255.255.255.255

IP Address Structure:

- Network Part: identifies a network
- Host Part: identifies a host & is used to differentiate hosts on a network.
- Network Mask: is used to distinguish network part from host part in an IP address.

IP Address Classification (Classful Addressing):

Class A: 0.0.0.0 – 127.255.255.255

Class B: 128.0.0.0 – 191.255.255.255

Class C: 192.0.0.0 – 223.255.255.255

Class D: 224.0.0.0 – 239.255.255.255

Class E: 240.0.0.0 – 255.255.255.255

Class A, B, C → Assigned for hosts
Class D → Used for multicast
Class E → Used for research

Default Subnets of Class A, B, C:

Class A: 8 bits
Class B: 16 bits
Class C: 24 bits

IP Address Types:

- **Network Address:** Identifies a network. All ~~network~~ host bits are 0.

- **Broadcast Address:** A special address used to send data to all hosts on a network. All host bits 1.

Network & Broadcast cannot be directly assigned to hosts.

- **Available Address:** IP addresses that can be allocated to device interfaces on a network.

No. of available addresses = $2^n - 2$

Public IP Addresses:

An IP address is assigned by the Internet Assigned Numbers Authority (IANA) & this address allocation ensures that each IP address is unique on the internet.

Private IP Addresses:

In practice, some networks donot need to connect to the internet. In the IP address space, some IP addresses of class A, B and C addresses are reserved for such situations. These IP addresses are called Private IP addresses

Class A : 10.0.0.0 — 10.255.255.255
Class B: 172.16.0.0 — 172.31.255.255
Class C: 192.168.0.0 - 192.168.255.255

Special IP Addresses:

1) Limited Broadcast Address: 255.255.255.255

2) Any IP address: 0.0.0.0

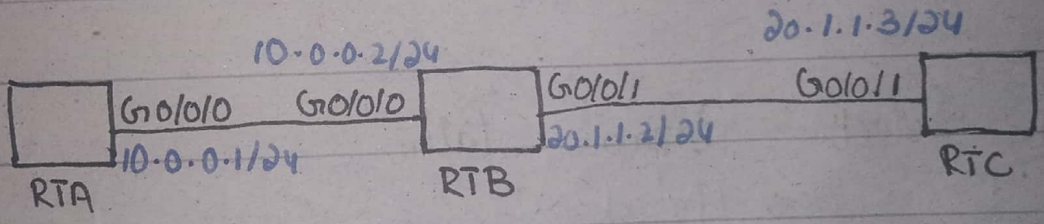
3) Loopback Address: 127.0.0.0/8

4) Link-Local Address: 169.254.0.0/24

Common Methods Of Obtaining Routes:

- Direct Routes:

Direct routes are automatically generated by devices and point to local directly connected networks:



RTB:

Destination/Mask	Protocol	Next Hop	Outbound Interface
20.1.1.0/24	Direct	20.1.1.2	GE0/0/1

Fields In The IP Routing Table:

- Destination / Mask
- Proto (Protocol)
- Pre (Preference)
- Cost
- Next Hop
- Interface (Outbound)

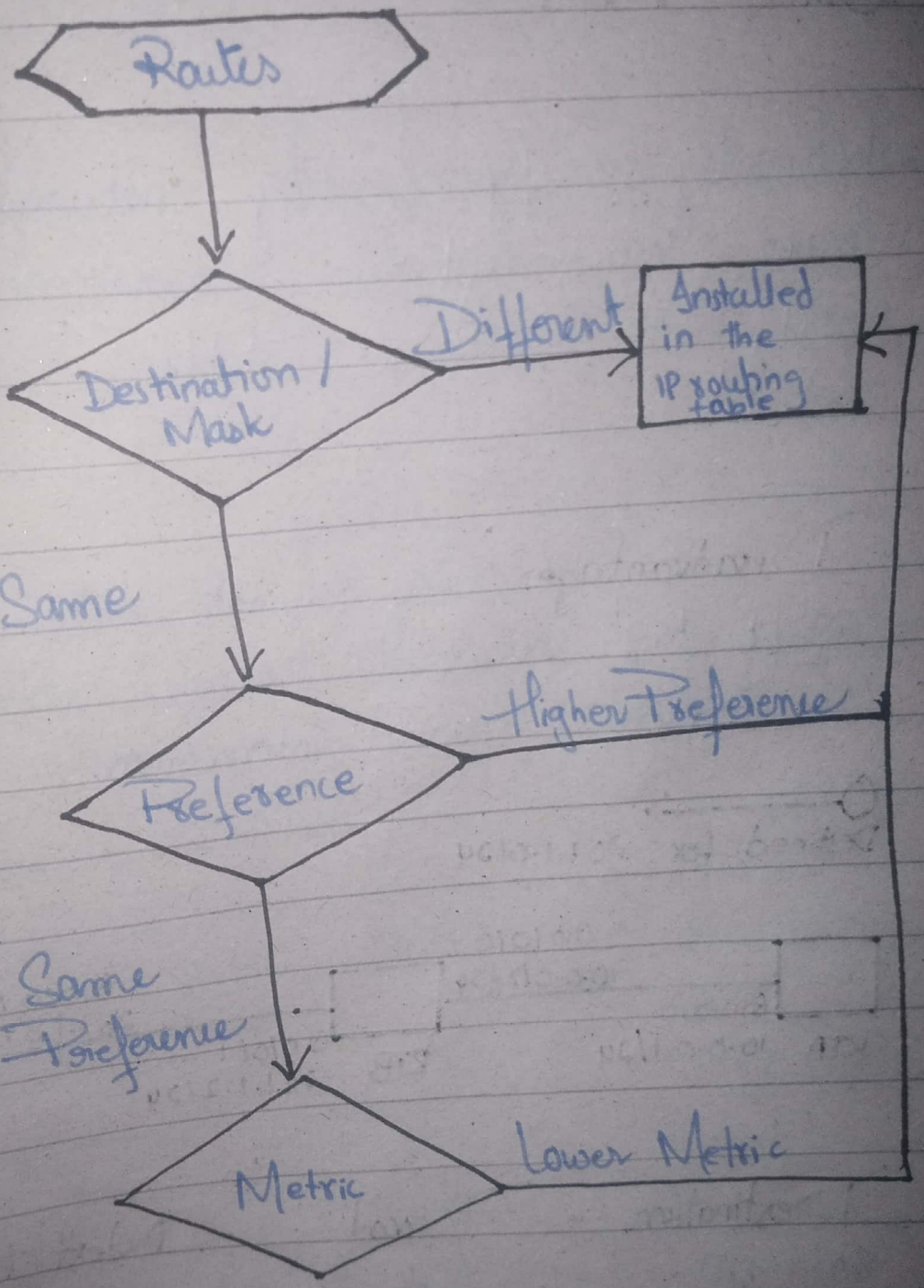
To Select Optimal Path:

- Destination / Mask (Longest Matching)
- Route Preference
- Metric (Cost)

Route Preference - Common Default Values:

Protocol	-	Route Type	-	Default Preference
Direct	-	Direct Route	-	0
Static	-	Static Route	-	60
Dynamic	-	OSPF internal	-	10
"	-	OSPF external	-	150

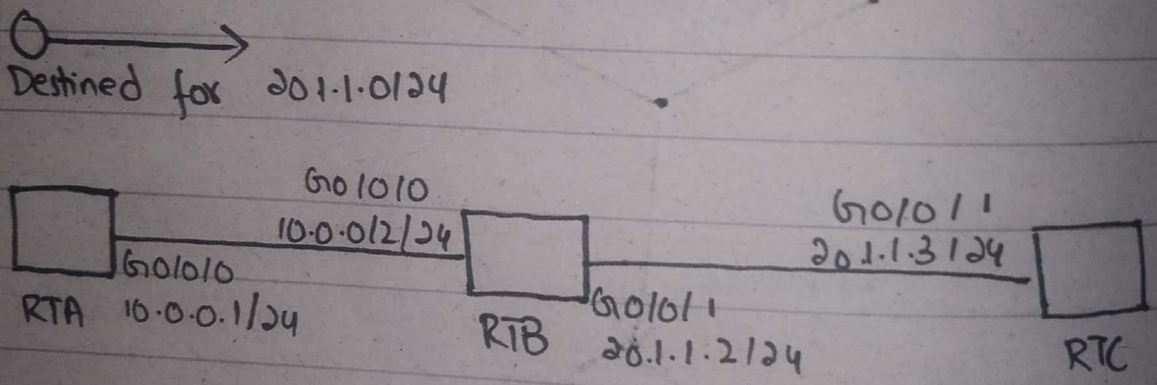
Comparison : Flow chart



- Static Routes:

- Manually configured by network administrator, have low system requirements, and apply to simple, stable & small networks:

- Disadvantage: They cannot automatically adapt to network topology changes & so require manual intervention.



Destination	Protocol	Next Hop
20.1.1.0	Static	10.0.0.2
10.0.0.0	Direct	10.0.0.1

ip route-static 20.1.1.0 255.255.255.0 10.0.0.2

x 1 Default Routes:

- Used only when packets to be forwarded donot match any routing entry in an IP routing table.

- In an IP routing table, Default route is the route to the network (with the mask 0.0.0.0), - 0.0.0.0

namely, 0.0.0.0/0

ip route - static 0.0.0.0 0 10.0.0.2

- Dynamic Routes:

Learned by dynamic routing protocols running on routers.

Dyamic Routing Protocols are classified as:

- Classification By Application Scope:

- Interior Gateway Protocol (IGP):
  - RIP
  - OSPF
  - IS-IS

- Exterior Gateway Protocol (EGP):
  - BGP

Classification By Working Mechanism & Routing Algorithm:

- Distance - Vector Routing Protocol:
  - RIP
- Link-State Routing Protol:
  - OSPF
  - IS-IS

• Routing Information Protocol:

- Distance Vector Protocol: Uses hop count as its metric to measure the distance b/w routers. Max hop count is 15.

- Versions: RIPv1 and RIPv2. RIPv2 supports subnet info & is more efficient.

- UDP port 520: messages are sent through UDP port 520.

- Convergence Time: RIP's slow convergence time can lead to transient loops during the updates.

- Limited Scalability: Best for small to medium-sized networks due to its hop count limitation & slow convergence.

- RIPng: RIP next generation supports IPv6.

- Classful Routing:

RIPv1 -> Classful Routing
RIPv2 -> Classless Routing

- Triggered Updates: Send immediate update when topology changes to speed up convergence.
- lacks support for VLSM.

RIP config:

[ ] rip <process-id>
[Huawei] rip 1

[ ] network <network-ip>
[Huawei] network 10.0.0.0

OSPF (Open - Shortest Path First)

- Link State Routing Protocol.

- OSPF routers exchange Link-States information, but not routes. Link States information is key information for OSPF to perform topology & route calculation.

- An OSPF router collects link status information on a network and stores the information in LSDB. Routers are aware of the intra-area network topology and be able to calculate loop-free paths.

- Each OSPF router uses the SPF algorithm to calculate the shortest path to a specific destination. Routers generate routes based on the paths and install the routes to routing table.

- Supports VLSM & manual route Summarization.

- The multi area design enables OSPF to support a larger network.