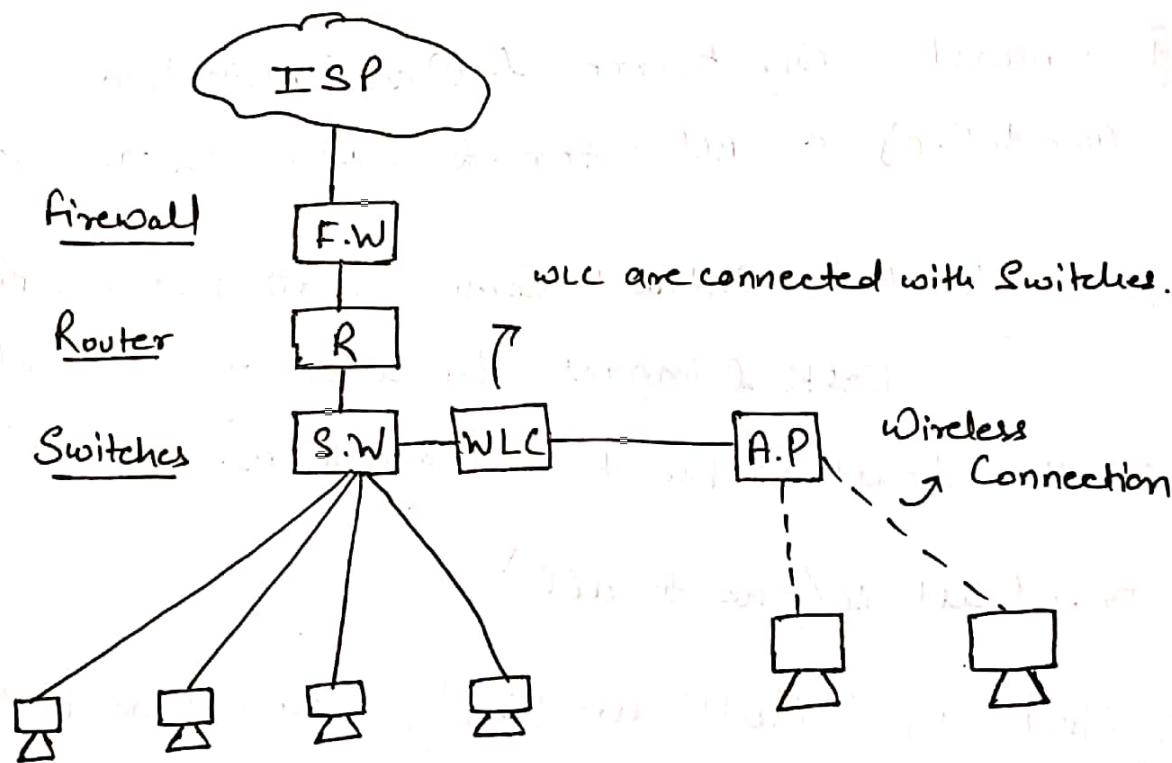


NETWORK :- Interconnection of Network devices that are used to share data or resources.

ex Router , switches, firewall , Access Point (AP's)

WLC (Wireless LAN controller) , end devices (PC, Server) etc



↳ Switch :- Provides centralized location & Connect Multiple devices in a network.

↳ Router :- Device Connecting two or More Network.

↳ firewall :- Protects Your network from unauthorized network access . Also we can say that it controls (filters) incoming & outgoing traffic in a network on the basis of some rules. (Like Company Policy).

Access Point :- Provides Centralized location to connect devices in a network but without wire using RF Signal.

WLC (Wireless LAN Controller) :- Provides Centralized management of all access points in a network.

### Types of Traffic (Communication)

① Unicast :- One Source + One Destination (One to One) ex All internet service we access.

② Broadcast :- Unicast Communication is a CPU intensive task & impacts Bandwidth as well So Broadcast is the best way to prevent both.

Broadcast is (One to all)

③ Multicast :- Multicast Simply means One to Many but why do we need it when we have Broadcast?

\* Router does not forward the Broadcast traffic by default & drops/limits it.

\* In Multicast only the user wish to receive gets it but How? That is because in backend all the user who wish to receive the packet joins that Multicast group & since it is multicast traffic so the router will not drop/limit it.

## NETWORK TYPES

### # LAN (Local Area Network)

Set of devices connected within a limited geographical area of upto 1 Km.

### # CAN (Campus Area Network)

A Computer network made up of interconnection of two or more LAN within a limited geographical area of upto 1 to 5 Km.

### # MAN (Metropolitan Area Network)

Set of devices connected within a city limits MAN covers a range of upto 50Km. (5Km - 50Km)

### # PAN (Personal Area Network)

Set of devices connected within a range of upto 10metre.

### # WAN (Wide Area Network)

Set of devices connected within wide geographical area.  
ex district, state, Country, Continent etc.

↳ IP Provides you an unique identity of a Network device over Internet or in your network.

\* we call it Internet Protocol as it is a protocol of a Internet layer.

## Version of IP

27-11-2019

(2)

/ \  
 IPv4 IPv6

\* Internet  $\rightarrow$  Public IP

In Our Network  $\rightarrow$  Private IP

↳ IPv4  $\rightarrow$  32 bit identity & is reps in decimal notation.

\* IPv4 is divided into 4 Octets.

ex 198.175.128.135  $\rightarrow$  32 bit IP  
①   ②   ③   ④  
↓ octet (8 bits)

$$\text{So } 8 \times 4 = 32 \text{ bit}$$

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

1 1 0 0 0 1 1 0  $\rightarrow$  198 (8 bits)

1 0 1 0 1 1 1 1  $\rightarrow$  175

1 0 0 0 0 0 0 0  $\rightarrow$  128

1 0 0 0 0 1 1 1  $\rightarrow$  135

more ex

235  $\rightarrow$  1 1 1 0 1 0 1 1

231  $\rightarrow$  1 1 1 0 0 1 1 1

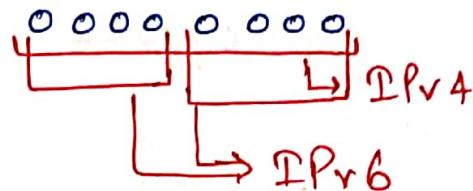
27-11-2019

(3)

↳ IPv6 → 128 bit identity & reps in hexadecimal notation.

Divided into 8 blocks

1 hexa = 4 bits.



<u>2001</u>	<u>0&gt;88</u>	<u>AC10</u>	<u>FEO1</u>	<u>0000</u>	<u>0000</u>	<u>0000</u>	<u>0000</u>
16 bit	16 bit	16 bit	16 bit	16 bit	16 bit	16 bit	16 bit

Adding all we get 128 bits.

↳ IP CLASSES

# Class A → 0 → 127

SUBNET MASK

255.0.0.0

Used in

Class B → 128 → 191

255.255.0.0

LAN &

Class C → 192 → 223

255.255.255.0

WAN

Class D → 224 → 239

Multicast } Reserved.

Class E → 240 - 255

Dept. of } Reserved for  
Defence      Research

27/11/2019

4

CLASS A  0 0 0 0 0 0 0 0 → 0

✓ common

## Class B

## Common

## class C

## Common

So that is why IP has different classes.

↳ SUBNET MASK :- 32 bit Identity

- \* S/m is a mixture of ~~not~~ Network id & host id.
  - N/w id is denoted by ON bit i.e 1 → fix
  - Host id is denoted by OFF bit i.e 0 → variable.
  - \* Subnet Mask tells the Network id & host id of a given ip address.

Ex 192.168.50.1 → so here 192.168.50 is a network id.

Part f . I is a host id part

27/11/2019

(5)

1 0 0 0 0 0 0 0 → 128

1 1 0 0 0 0 0 0 → 192

1 1 1 0 0 0 0 0 → 224

1 1 1 1 0 0 0 0 → 240

1 1 1 1 1 0 0 0 → 248

1 1 1 1 1 1 0 0 → 252

1 1 1 1 1 1 1 0 → 254

1 1 1 1 1 1 1 1 → 255

ex  $\frac{255}{N/W} \cdot \frac{255}{N/W} \cdot \frac{255}{N/W} \cdot \frac{0}{H}$  → S/m of class C.

$\frac{1111111}{N/W} \cdot \frac{1111111}{N/W} \cdot \frac{1111111}{N/W} \cdot \frac{00000000}{\text{Host}}$

Class A    0 - 127    255.0.0.0

Class B    128 - 191    255.255.0.0

Class C    192 - 223    255.255.255.0

\* **0.0.0.0** is a Reserved block/ip which we cannot configure on our PC. & it is used in the following

① Default Routing

② In DHCP during DHCP discover packet

→ [Windows + R & type npca.cpl] to give ip to Computer.  


\* **255.255.255.255** → Broadcast Ip.

↳ Loopback Ip address

Range → 127.0.0.0 — 127.255.255.255

In certain blogs the range is given as

(127.0.0.1 — 127.255.255.254).

→ Used for self pinging or troubleshooting.

\* Ping is a service helps in checking connectivity b/w two or more devices.

\* (ICMP protocol run in backend of ping.).

**Packet Internet group (PING)**

↳ APIPA Address :- (Automatic Private IP Address) APIPA

→ Even if we have ip assigned from DHCP & our NIC gets corrupted then the ip will not hold & we would not be able to use internet services.

→ Range → 169.254.0.0 — 169.254.255.255

169.254.0.1 — 169.254.255.254

→ When DHCP Server is unable to provide an ip Address then your PC automatically provides itself an IP which is APIPA

\* By default APIPA is enabled on client machine.

→ Used to control Broadcast packet (Broadcast flooding).

↳ Books ① How to master ccna (Rene' Molenaar)

② Routeralley.com (CCNA study guide)

③ Todd Lammle

↳ Websites ① www.omnisecu.com

② ccnablog.com

③ Networklessons.com (Paid)

④ gns3vault.com (fortaKs) (Free)

→ IP is divided into two parts based on working behaviour.

### Private IP

- ① Provided by network Admin
- ② Locally unique
- ③ Used for Internal Communication LAN
- ④ Free
- ⑤ Unregistered

### Public IP

- ① Provided by ISP
- ② Globally unique.
- ③ Used for Internet (WAN)
- ④ Paid
- ⑤ Registered.

### Private IP Range :-

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

\* Except all these ranges All are Public IP's.

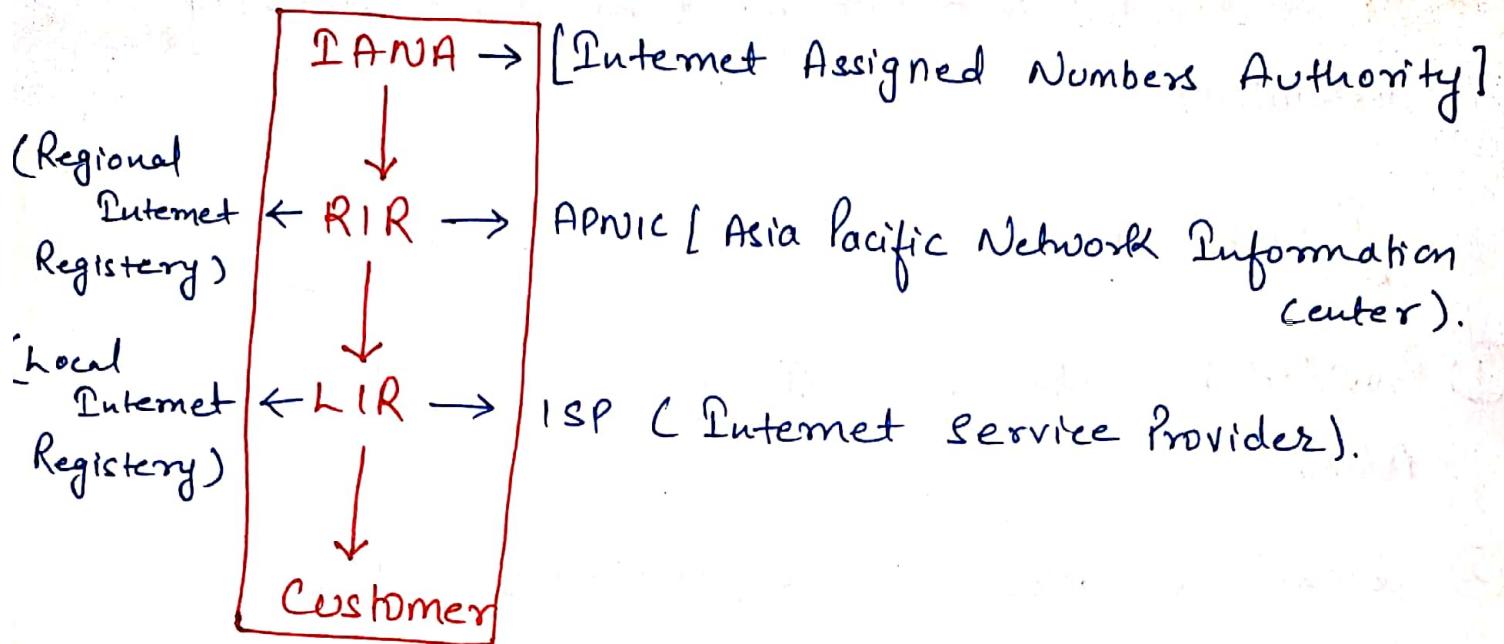
1.0.0.0 — 1.~~255~~.255.255

11.0.0.0 — 172.15.255.255

172.32.0.0 — 172.167.255.255

192.169.0.0 — 192. — — —

All are public



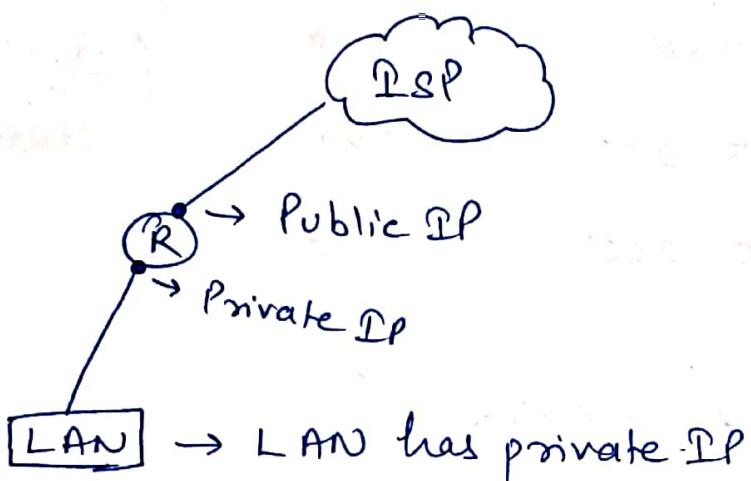
- \* IANA works on global level
- \* RIR works on continent level.  
(Total 5 RIR)
- \* LIR like airtel etc.

29/11/2019

①

LECTURE - 4

\* NAT Replaces private IP with Public IP



↳ SUBNETTING :- A method where we divide a large or complex network into small network & that small network is called Subnetwork.

↳ CIDR :- Classless Inter-Domain Routing

- \* Another way of representing subnet mask.
- \* CIDR is represented by slash (/) notation where every single bit represents one bit.
- \* ISP uses CIDR notation to allocate IP address to its clients.

CIDR			
Class A	0 - 127	255.0.0.0	18
Class B	128 - 191	255.255.0.0	16
Class C	192 - 223	255.255.255.0	124

classfull.

29/11/2019

(2)

S/M

CIDR

 $255 \cdot 128 \cdot 0 \cdot 0$ 

19

 $255 \cdot 255 \cdot 224 \cdot 0$ 

119

 $255 \cdot 255 \cdot 255 \cdot 254$ 

131

 $255 \cdot 255 \cdot 255 \cdot 255$ 

132

classless

↳ Conversion S/M  $\leftrightarrow$  CIDR

#  $\boxed{\text{No. of Subnets/network} = (2)^{\text{no. of extra on bit}}}$

#  $\boxed{\text{No. of host/ip/host/subnet} = (2)^{\text{no. of off bits}} - 2}$

ex  $192 \cdot 168 \cdot 1 \cdot 5 / 28$

$$\text{S/M} = 255 \cdot 255 \cdot$$

$$\text{no. of Subnet} = 2^4 = 16$$

$$\text{no. of host/subnet} = 2^4 - 2 = 16 - 2 = 14$$

\* we can calculate on & off with the help of each other

ex here no. of off =  $32 - 28 = 4$

$$\text{So no. of on bits} = 8 - 4 = 4$$

29/11/2019

(3)

ex class C - CIDR /29 , CIDR /26

$$\begin{aligned} \text{no. of host/Subnet} &= 2^3 - 2 \\ &= 8 - 2 \\ &= 6 \end{aligned}$$

$$\begin{aligned} \text{no. of Subnet} &= 2^5 \\ &= 32 \end{aligned}$$

$$\begin{aligned} \text{no. of host/Subnet} &= 2^6 - 2 \\ &= 64 - 2 \\ &= 62 \end{aligned}$$

$$\begin{aligned} \text{no. of Subnet} &= 2^2 \\ &= 4 \end{aligned}$$

ex class B - CIDR /18 , CIDR /23 , CIDR /27

$$\begin{aligned} \text{no. of host/Subnet} &= 2^{14} - 2 \end{aligned}$$

$$\begin{aligned} \text{no. of Subnet} &= 2^2 \\ &= 4 \end{aligned}$$

$$\begin{aligned} \text{no. of Subnet} &= 2^7 = 128 \end{aligned}$$

$$\begin{aligned} \text{no. of host/Subnet} &= 2^9 - 2 \\ &= 512 - 2 \\ &= 510 \end{aligned}$$

$$\begin{aligned} \text{no. of Subnet} &= 2^{11} \\ &= 2048 \end{aligned}$$

$$\begin{aligned} \text{no. of host/Subnet} &= 2^5 - 2 \\ &= 32 - 2 \\ &= 30 \end{aligned}$$

↪ Complete Process (Step by step).

ex 192.168.1.25 /28

Step 1 → S/m → 255.255.255.240

Step 2 → 4<sup>th</sup> Octet Block Size = 256 - 240 (Gives no. of IPs in a block).  
= 16

29/11/2019

(4)

Step 3

$$192 \cdot 168 \cdot 1 \cdot 0 \rightarrow .115$$

$$192 \cdot 168 \cdot 1 \cdot 16 \rightarrow 31 \quad 192 \cdot 168 \cdot 1 \cdot 25 \text{ lies in this.}$$

$$\cdot 32 \rightarrow 47$$

|

|

$$224 \rightarrow 239$$

$$240 \rightarrow 255$$

So

$$192 \cdot 168 \cdot 1 \cdot 16$$

$\rightarrow$

$$192 \cdot 168 \cdot 1 \cdot 31$$

$\downarrow$

network address

$\downarrow$

Broadcast address

\* First & last ip of a Block is a network ip & Broadcast ip respectively.

So

$$192 \cdot 168 \cdot 1 \cdot 17 \rightarrow 192 \cdot 168 \cdot 1 \cdot 30$$

It is our valid ip range with 192.168.1.17 is first valid ip & 192.168.1.30 is the last valid ip.

\* [www.subnetting.org](http://www.subnetting.org) → To practice subnetting.

↳ SUBNETTING CLASS B

ex 172.19.144.0 / 20

Step 1 S/m  $\rightarrow$  255.255.240.0

Step 2 Block Size  $\rightarrow$   $256 - 0 = 256$  (4<sup>th</sup> Octet)

$$256 - 240 = 16 \text{ (3}^{\text{rd}} \text{ Octet)}$$

Step 3

172.19.144.

$$172 \cdot 19 \cdot 0 \cdot 0 — 15 \cdot 255$$

$$16 \cdot 0 — 31 \cdot 255$$

$$32 \cdot 0 — 47 \cdot 255$$

$$\begin{array}{c|c|c|c} & & & \\ \hline | & | & | & | \\ | & | & | & | \\ | & | & | & | \\ | & | & | & | \\ | & | & | & | \\ \hline 144 & 0 & — & 159 & 255 \end{array}$$

So we have range/Block

n/w address

172.199.144.0 — 172.19.159.255

172.19.144.1 — 172.19.159.254

Valid ip Range

Broadcast address

So last Valid host is 172.19.159.254

02/12/2019

(2)

\* IP in class B flow like below

172.19.0.0

0.1

|

|

|

|

0.255

172.19.1.0

1.1

|

|

|

|

1.255

172.19.2.0

2.1

|

|

|

|

2.255

172.19.3.0

3.1

|

|

|

|

172.19.159.255

①

03/12/2019

\* Uptill now we have read FLSM

FLSM [Fixed length ~~Subnet~~ Subnet Mask]

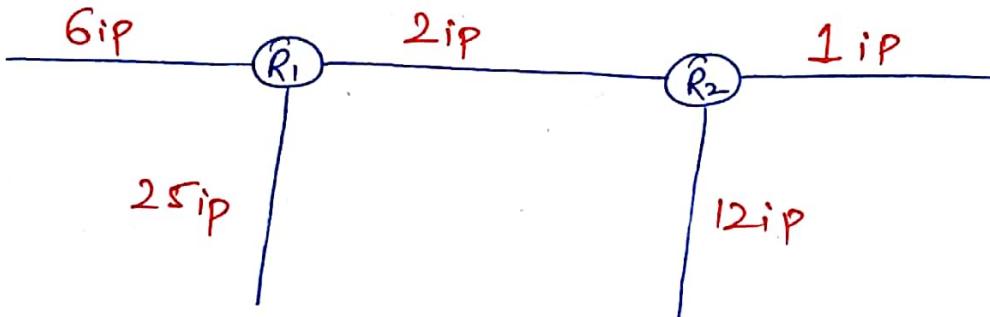
& Now we will read VLSM

VLSM [Variable length Subnet Mask]

\* Broadcast address: This address is used to broadcast in its own network. (Both are different)

Universal Broadcast id → 255.255.255.255

ex



\* There is a kind of rule that we have to go in Descending Order to avoid ip conflict.

\* Suppose here ISP gave us one subnet of 192.168.10.0/24 from which we have assign ip to various subnets.

$$\rightarrow 25 \text{ ip} = 192.168.10.0 - 31$$

For 25 ip we need a block of 32 means no. of off bits = 5

$$\begin{aligned} \text{no. of host/Subnet} &= 2^5 - 2 \\ &= 32 - 2 = 30 \end{aligned} \quad \therefore \text{no. of on bits} = 3 \quad \therefore \text{CIDR} = 27$$

03/12/2019  
In the Same way

$$\text{for } 12 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot \underline{32} - \underline{47} / 28 \quad \leftarrow$$

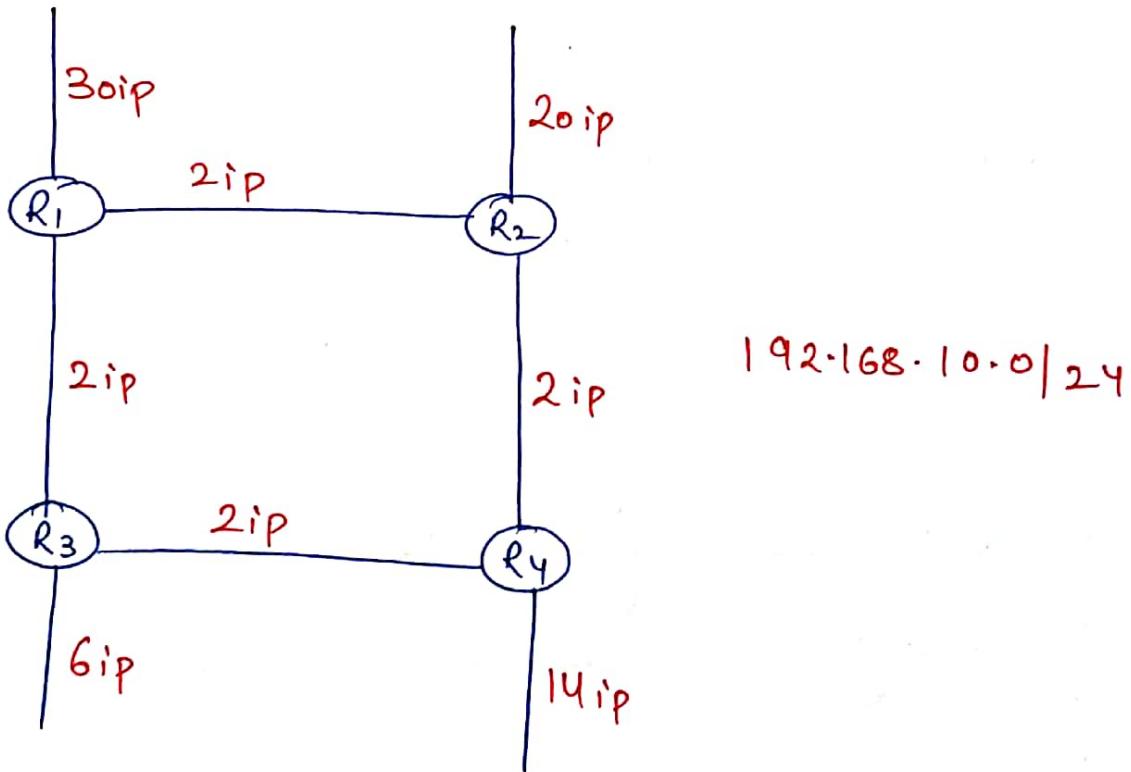
no. of off bits = 4  $\therefore$  no. of on bits = 4 hence CIDR

$$\text{for } 10 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 48 - \cancel{64} 63 / 28$$

$$\text{for } 6 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 64 - 71 / 29$$

$$\text{for } 2 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 72 - 75 / 30$$

ex



$$30 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 0 - 31 / 27$$

$$20 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 32 - 63 / 27$$

$$14 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 64 - 79 / 28$$

$$6 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 80 - 87 / 29$$

03/12/2019

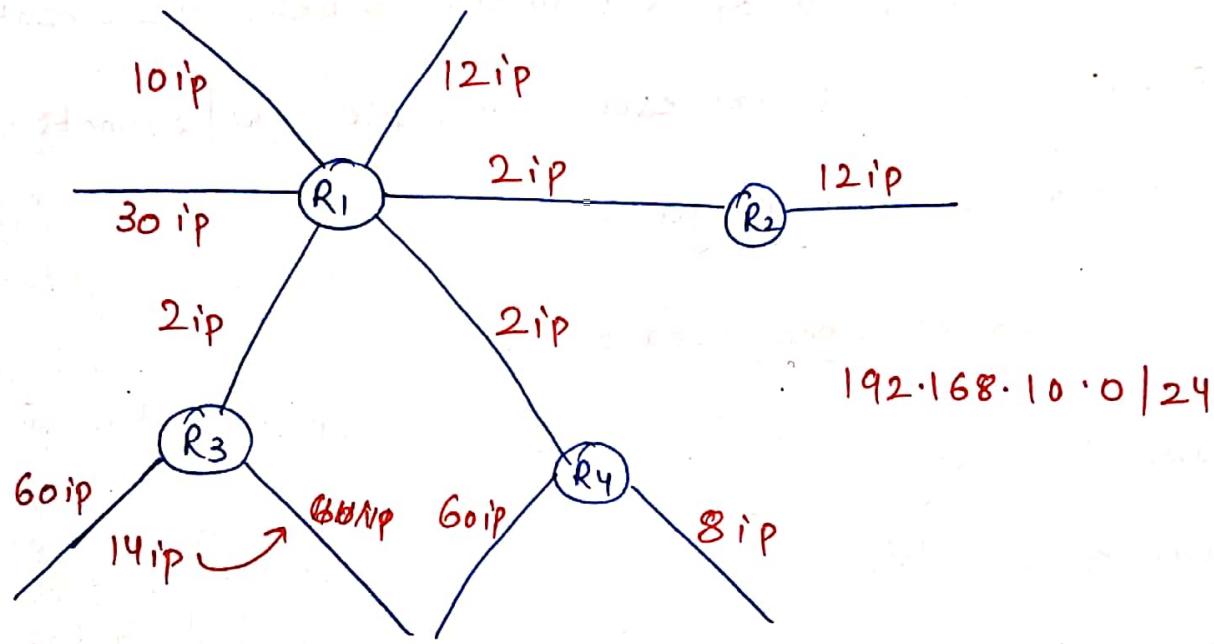
(3)

$$2 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 88 - 91 / 30$$

$$2 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 92 - 95 / 30$$

$$2 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 96 - 99 / 30$$

ex



$$60 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 0 - 63 / 26$$

$$60 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 64 - 127 / 26$$

$$30 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 128 - 159 / 27$$

$$14 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 160 - 175 / 28$$

$$12 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 176 - 181 / 28$$

$$12 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 192 - 207 / 28$$

$$10 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 208 - 223 / 28$$

$$8 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 224 - 239 / 28$$

$$2 \text{ ip} = 192 \cdot 168 \cdot 10 \cdot 240 - 243 / 30$$

④

03/12/2019

$$2^{\text{ip}} = 192 \cdot 168 \cdot 10 \cdot 2^{24} - 247 / 30$$

$$2^{\text{ip}} = 192 \cdot 168 \cdot 10 \cdot 2^{24} - 251 / 30$$

## ↳ SUPERNETTING :-

Supernetting / Summarization is a method where we create one summary route that represent multiple n/w / subnets. It is also called route aggregation.

→ Supernetting is done because :-

- ① Saves Memory
- ② Saves Bandwidth
- ③ Saves CPU Cycles
- ④ Stability.

ex

172	.	16	.	0	.	1	/24
172	.	16	.	1	.	1	/24
172	.	16	.	2	.	1	/24
172	.	16	.	3	.	1	/24

\* In Supernetting we have to see which block is changing & then convert that block in Binary

This Octet is changing

0 →	0	0	0	0	0	0	0	0
1 →	0	0	0	0	0	0	0	1
2 →	0	0	0	0	0	0	1	0
3 →	0	0	0	0	0	0	1	1

So first 6 bits are common

Now  $\frac{172}{8\text{bit}} \cdot \frac{16}{8\text{bit}} \cdot 0 \cdot 0$

6 bits from above

So CIDR will be  $172 \cdot 16 \cdot 0 \cdot 0 / 22$  ( $8+8+6=22$ )

So  $172 \cdot 16 \cdot 0 \cdot 0 / 22$  reps above all 4 Networks.

ex

10	·	0	·	0	·	0	0
10	·	0	·	1	0		
10	·	0	·	2	0		
10	·	0	·	3	0		

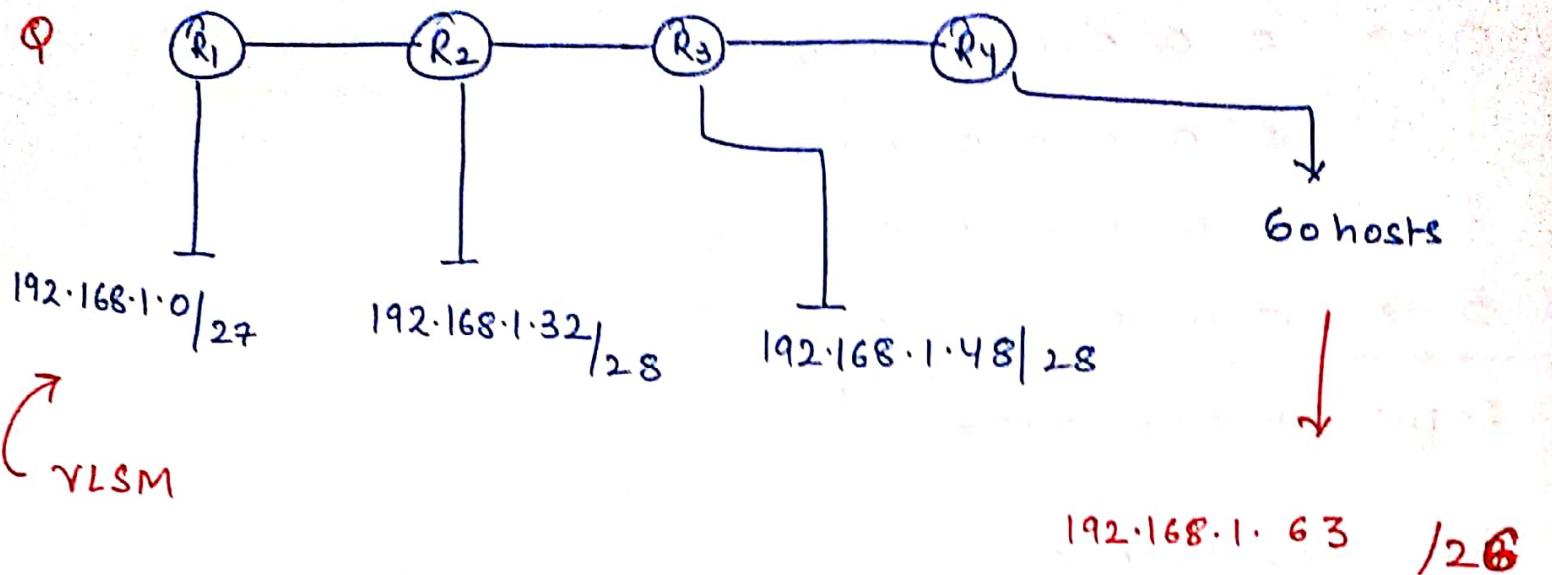
→ class is A but change is in 3rd Octet

\* So we do not go by class, we go by the actual block in which change is occurring

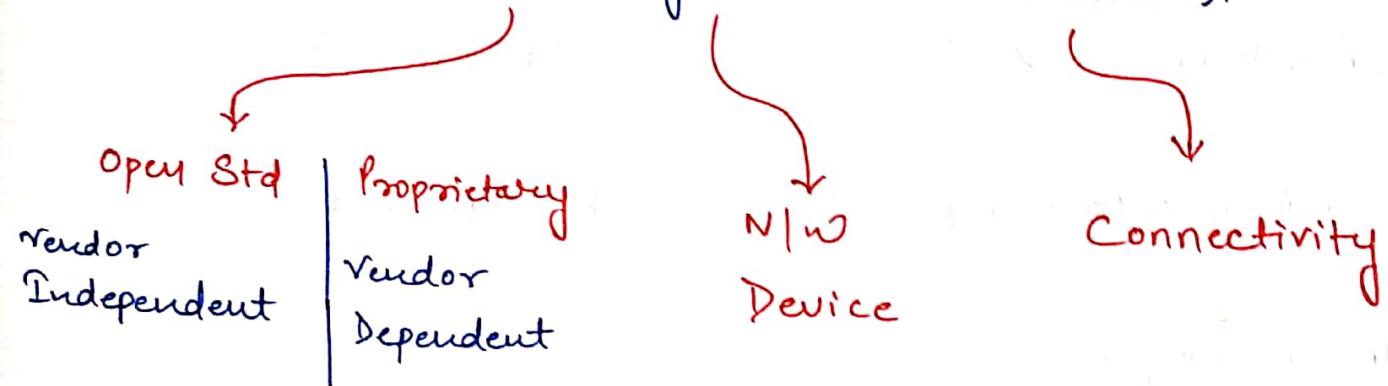
So  $\frac{10}{8\text{bit}} \cdot \frac{0}{8\text{bit}} \cdot \frac{0}{6\text{bit}} \cdot 0 / 22$  Ans.

03/12/2019

(6)



↳ OSI, → (Open System Interconnection).



↳ OSI MODEL :-

It has 7 layers.

- L7 → Application layer
- L6 → Presentation layer
- L5 → Session layer
- L4 → Transport layer
- L3 → Network layer
- L2 → Data link layer
- L1 → Physical layer.

↳ L7 → APPLICATION LAYER

→ Acts as an Interface between user and Application layer Protocol

\* Protocols works at Application layer are as follows :-

ex    FTP (Data)      20    (TCP)

          FTP (control)    21    (TCP)

(Remote login    SSH - 22    (TCP)  
Protocol)

          Telnet - 23    (TCP)

04/12/2019

(Simple Mail Transfer Protocol)

SMTP - 25 (TCP)

Domain Name System (DNS) - 53 (TCP/UDP)

Trivial File Transfer

Protocol (TFTP) - 69 (UDP)

HTTP - 80 (TCP)

POP3 - 110 (TCP)

SNMP - 161/162 (UDP)

Internet Mail Access Protocol (IMAP) - 143 (TCP)

Border Gateway Protocol (BGP) - 179 (TCP)

HTTPS - 443 (TCP)

DHCP - 67/68 (UDP)

\* Application layer interacts as an interface b/w user & protocol.

\* All above ports are logical ports / port numbers.

04/12/2019

(3)

↳ DNS → Port no. 53

# Layer 7 Protocol

# Works over TCP / UDP

Translate

# Used to Resolve name to IP and IP to Name

Ex https://www.google.com

↳ URL

www.google.com → This is in terms of DNS.

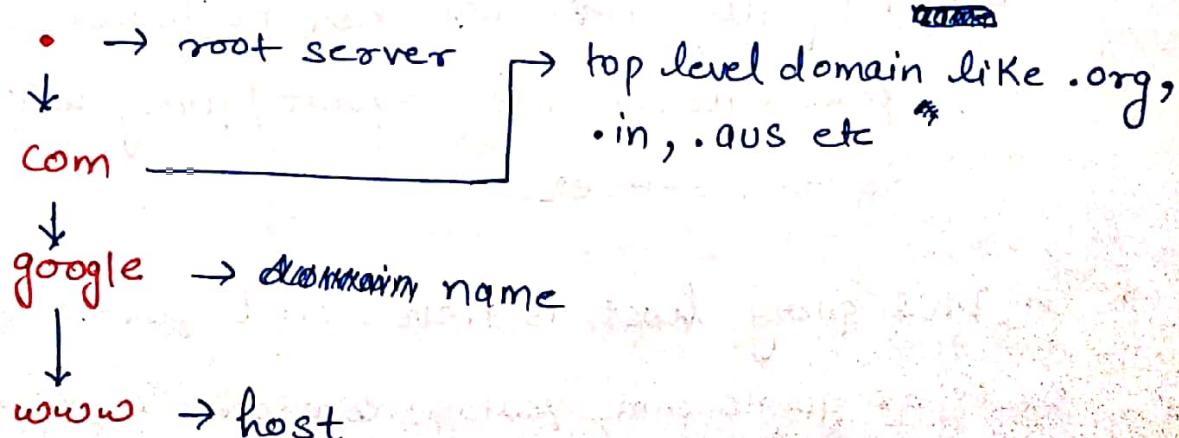
↓  
host + domain

↓  
→ FQDN (Fully qualified Domain name)

\* Earlier or we can say before DNS another method was used in which we had to do manual entry in host.txt file

→ DNS Hierarchy :-

→ We never type www.google.com  but it is there and it is called root server



04/12/2019

④

Based on Above Hierarchy we will study DNS working or DNS lookUp.

cmd # ip-config /Display-dns

It is used to check DNS entry / Request

Pc

① if we try to access any website or make any DNS query then it first go to the local PC only & gets checked in DNS Resolver Cache.

cmd # ip-config /flushdns

It is used to delete DNS entry.

② if the PC is rebooted or DNS cache is deleted then the request will go to DNS forwarder.

like company server

→ DNS forwarder is an IP provided by DHCP

③ If the <sup>DNS</sup> entry will not be found in any of the two places above the request/query will be forwarded to root server.

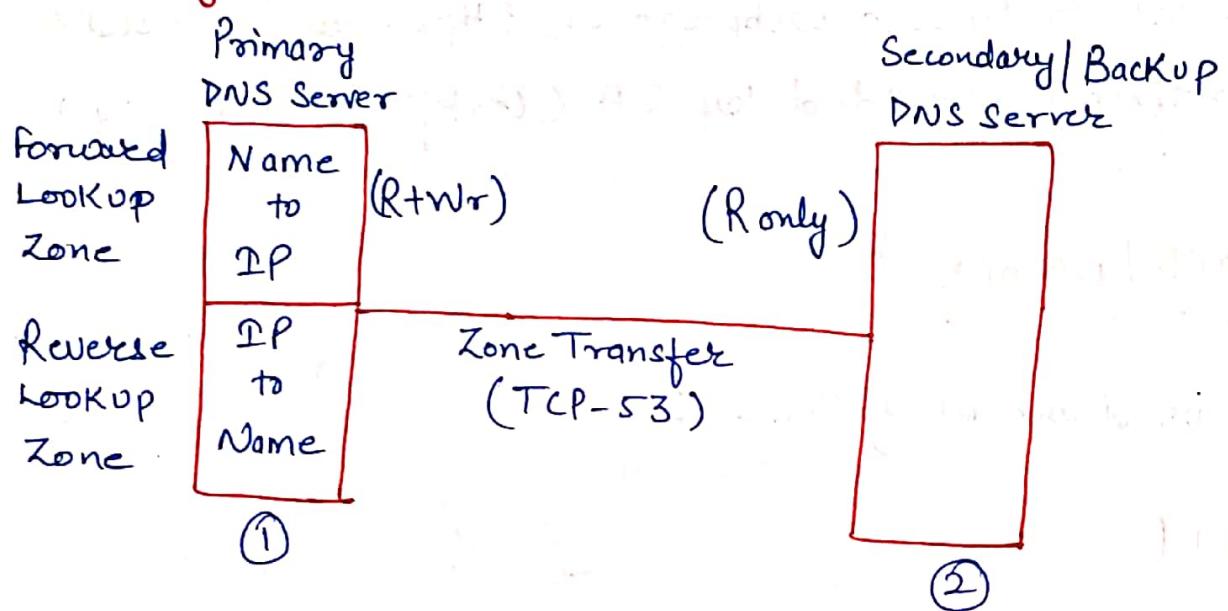
\* In DNS query host is never sent just the domain is sent ex google.com, youtube.com etc.

04/12/2019

(5)

- \* 8.8.8.8 is an open DNS.
- \* whenever DNS Server is installed then in that all the ip's of all root server gets installed in that (Roughly there are 13 root servers in the world).

→ In System we see two DNS Server IP because:-



- \* There are mainly two DNS server installed with one primary & other secondary / Backup. [At company level we have backup]
- \* Primary DNS Server is Read + Write whereas Secondary DNS Server is Read only.
- \* In Zone transfer or we can say in transfer of Database for Primary to Secondary server needs (TCP Port-53).
- \* By Default DNS query is made on UDP Port 53 but Problem occurs in case of Iprb as query length usually gets increased above 512 bytes then it sends DNS query on TCP Port 53.

## WEB SERVICES :-

Protocols used are as follows :-

↳ **HTTP** : Plain Text data transfer.

**HTTPS** : Encrypted packet (Ciphon text)

\* If we want to host a webpage on https then we need to get certificate provided by CA (Certificate Authority).

## DOWNLOAD / UPLOAD :-

Protocols used are as follows :-

### FTP

- ① File transfer protocol
- ② Works over TCP port no. 20/21
- ③ Support Authentication
- ④ Support directory based browsing

### TFTP

- ① Trivial file transfer protocol
- ② works over UDP port no. 69
- ③ Doesn't support Authentication
- ④ Must Know the exact path of the file as doesn't support directory based browsing.

\* In Zone transfer is done on TCP 53 not UDP 53 as high speed transfer is required as UDP only support max 512 bytes/sec & 2ndly in DNS query UDP Port 53 is used by default but in case IPv6 is used & length goes over 512 bytes then TCP 53 is used.

↳ L6 → PRESENTATION LAYER

→ Presentation layer presents data into standard format also perform encryption, decryption, compression and decompression.

↳ L5 → SESSION LAYER

- Responsible for maintaining the session and terminate the sessions.
- Whenever a user creates sessions a unique port no. is created alongwith ip address.
- with the help of unique port no. session is identified.

# Port no. → 16 bit identity

(1 - 65,536)

↓  
(1 - 1023)

Well Known  
port numbers)

↓  
(1024 - 65536)

↓  
(Random port no.)

cmd # Net stat

↳ to check all traffic & port no. on your pc.

## L4 → TRANSPORT LAYER :-

TCP

- ① Transmission Control Protocol
  - ② TCP works over protocol no. 6
  - ③ Connection oriented
  - ④ Provides windowing, ACK, Segmentation
  - ⑤ Slow
- ex Telnet, FTP, ssh etc

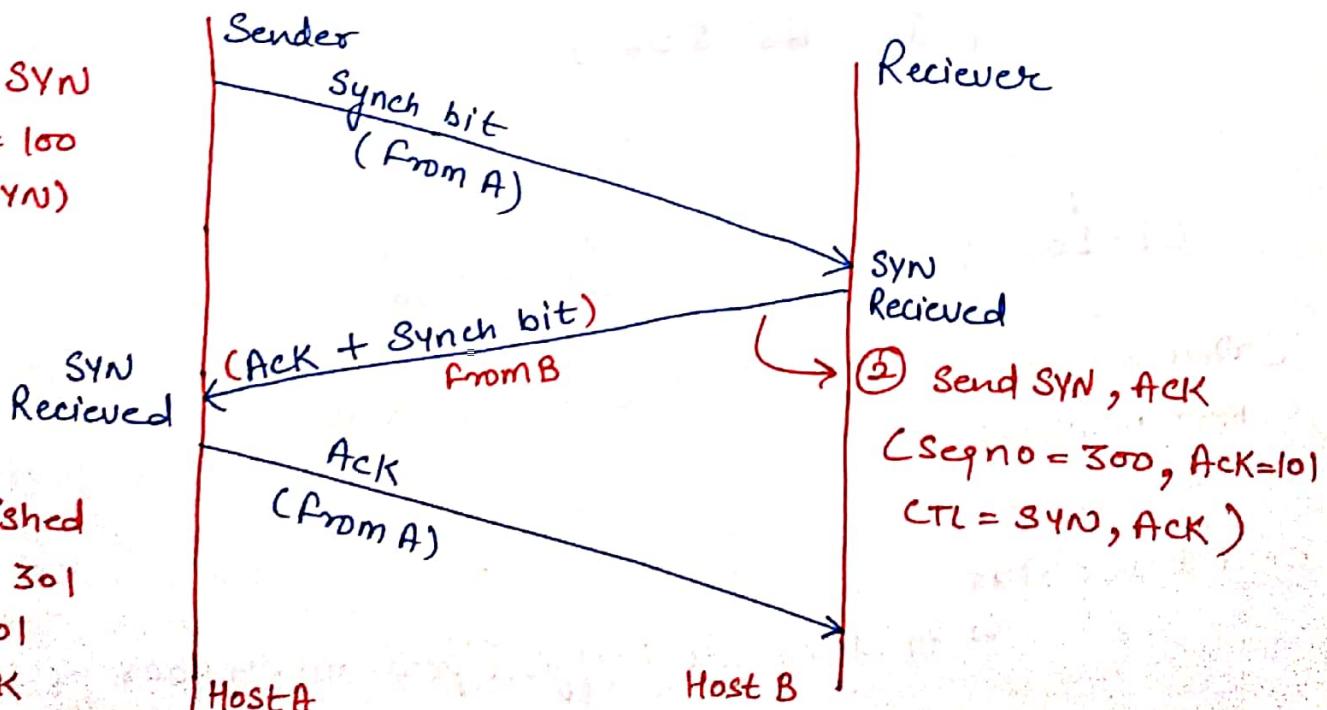
UDP

- ① User Datagram Protocol
  - ② UDP Protocol no-17
  - ③ Connection Less
  - ④ No
  - ⑤ Fast
- ex DHCP, TFTP etc.

\* DNS works on both TCP & UDP

## 3 WAY HANDSHAKE :-

- ① Send SYN  
 $\text{Seq no.} = 100$   
 $\text{CTL} = \text{SYN}$



05/12/2019

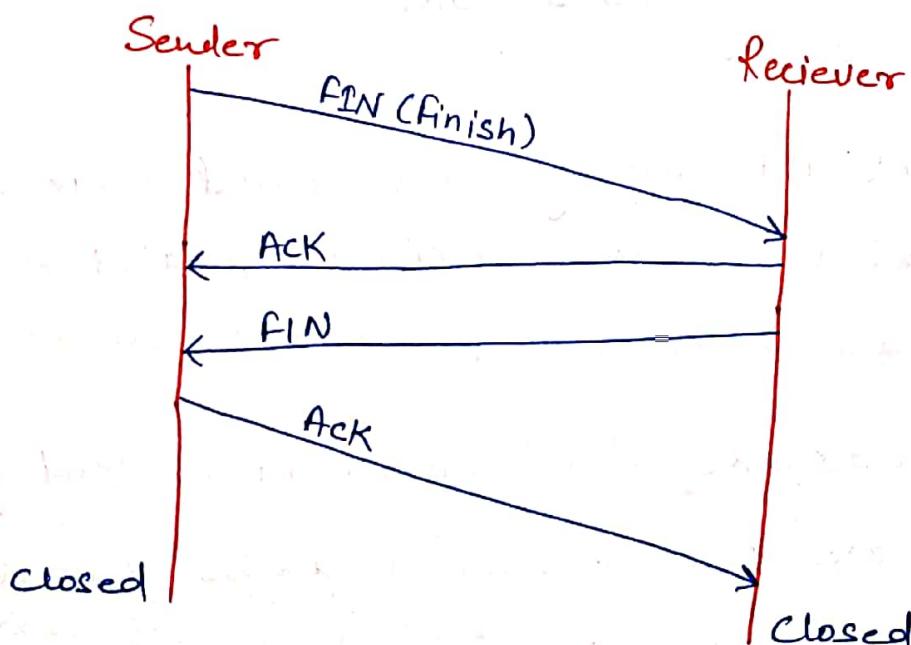
(3)

- \* Protocol work on L7 has port no. & protocol work on L3 & L4 has protocol no.
- \* Because all protocols on L7 works on TCP & UDP port so can't be protocol nos., Also we can say the protocol work on L7 are basically services.

Now, In TCP, 3 way handshake is required to establish the connection, 4 way handshake is required to terminate the connection.

- \* Data is transferred only after connection is established through 3 way handshake.

↳ 4 way handshake :-



- \* In 3 way handshake of TCP the Seq no. generated can be a random one. but the acknowledgement is Seq.no + 1 i.e here Seqno was 100 & the ACK was 101.
  - \* In 3 way handshake & Actual data transfer Seq & Ack no. works in a different way.  
also
  - \* In Data transfer Random Relative Sequence no.'s generated in relation to Actual data which can be in billions.
  - \* Data gets added to initial Seq no. to generate next Seq no. in Data transfer

Random Seq no.  $\rightarrow$  1

Data → Q

Next Sequence.  $\rightarrow$  1+9

→ 10

In Data transfer not 3-way handshake

- \* In Data transfer acknowledgement received is the same seq no. not ~~seq~~ +1, because receiver updates sender that correct seq no or correct data has been received.
  - \* In 4 way hand shake FIN(Finish) bit is sent from sender to indicate that connection can be terminated now.

05/12/2019

↳ SEGMENTATION :- Process of dividing a chunk (large block) of data into a small block & that small block is called segment.

MSS (Maximum Segment Size)

↳ Helps in determining the size of the small block.

→ In other words we can say maximum amount of data that can be allowed in a single segment.

By Default,

$$\boxed{\text{MSS} = 1460 \text{ bytes}}$$

\* It's just a by default size of MSS not a size of segment.

So

$$\boxed{\begin{array}{c} 1460 \text{ bytes} + 20 \text{ bytes} \\ \text{MSS} \qquad \qquad \qquad \text{TCP} \\ \qquad \qquad \qquad \text{Header} \end{array}}$$

$$\rightarrow \boxed{1480 \text{ bytes}}$$

Now it is called Segment.

↳ WINDOWING :- Maximum amount of data that a receiver is willing to receive before sending a ~~KILLER~~ back an ACK.

By default,

$$\boxed{\text{Window Size} = 4128 \text{ bytes}}$$

\* Window size (Windowing) is decided at the time of 3 way handshake and during each segment successful ACK.

05/12/2019

- \* Suppose we get 5000 bytes of Data from N/w layer then it will be segmented as  $1460 + 1460 + 1460 + 620$  bytes.
- \* Windowing depends on the Buffer size as ex receiver can share window size of 10000 bytes during 3 way handshake 10000 bytes will be transferred & now next window size will be informed during Acknowledgement.

**Accediam → TCP Series #4 (Blog)** to study TCP R/ACK

### ↳ What is Zero Window?

when a client advertises a zero value for its window size this indicates that the TCP receiver buffer is full & it can't receive any more data.

It may have <sup>a</sup> stuck processor or be busy with other task, which can cause the TCP receiver buffer to fill.

\* Window length is maximum of 65,536 bytes i.e  $(2^{16})$

\* Window scaling factor can increase window length for Data transfer (16 bit.)

↳ Flow Control :- It solves the problem of fast sender & slow receiver.

Use windowing, ACK to control the flow of data

## L3 → NETWORK LAYER

- Device :- Router, L3 Switch
- Protocol :- IP, ICMP, OSPF, EIGRP etc.

### Function :-

- ① Packet Forwarding
- ② Path Determination
- ③ Fragmentation.

\* If packet received at interface is more length than of interface then there is need to divide large packet into small packet called fragments.

\* Fragment size depends upon or we can say divided by MTU

## MTU (Maximum Transmission Unit).

→ Maximum amount of Packet that can be allowed through a router (L3) Interface.

MTU = 1500 bytes by default but can be altered.

$$\frac{\text{Data Segment}}{1480 \text{ bytes}} + \frac{\text{IP Header}}{20 \text{ bytes}} = \frac{1500 \text{ bytes}}{\text{Packet}}$$

- \* IP header length can also be altered up to 60 bytes.
- \* Suppose if at Router R<sub>1</sub>, 5000 bytes packet/segment is received then it would be divided into 4 packets of  $1500 \times 3 + 500$  bytes at R<sub>2</sub>

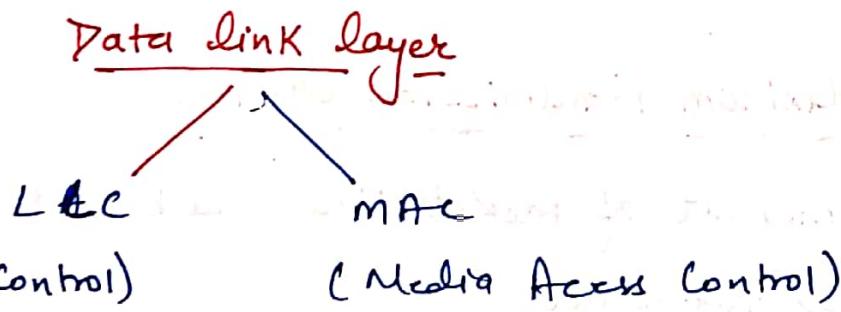
## ↳ DATA LINK LAYER

Device → L<sub>2</sub> Switches.

Protocol → MAC, PPP etc

### function:-

- ① Frame Switching
- ② Error Control



- \* for higher layer like L<sub>3</sub> etc
- \* for lower layer.

## ↳ MAC (Media Access Control)

- ① 48 bit
- ② Represented in Hexadecimal Notation.

06/12/2019

(3)

ex.

### MAC

00	1A	3F	F1	4C	C6
24 bit			24 bit		

48 bit identity

Rps → OUI (Vendor)

Rps → NIC (Hardware)

organizationally Unique  
Identifier

Network Interface Controller  
Specific

cmd # getmac

\* If in any MAC address the 8<sup>th</sup> bit is

0 → then Unicast

1 → then Multicast

+ FFFF.FFFF.FFFF their Broadcast.

↳ L1 → PHYSICAL LAYER

→ Device :- Hub, NIC etc

$$\# \frac{1500 \text{ bytes} + 14 \text{ bytes}}{\text{Data}} = 1514 \text{ bytes}$$

Data → L2 (Ethernet Header)

→ Data → Bits.

06/12/2019

## ↳ ARP FAMILY

### → ARP (Address Resolution Protocol)

- \* Combination of L2 & L3 Protocol
- \* Called 2.5 protocol, Also works on L3 & L2 both.
- \* Used to Resolve IP to MAC
- \* Check on CPT with 2 pc practical.

### → RARP (Reverse ARP)

- ↳ Used to Resolve MAC to IP.

### → GARP (Graftions) ARP

- Used to check IP duplicacy or IP Conflict
- In this Source IP & Destination IP are same for packet broadcasts.
- \* In today's world we do not use RARP as Boot protocol & then DHCP was launched & DHCP does the same thing as RARP if MAC binding is done with DHCP.

## → P ARP (Proxy ARP)

It is a technique by which a proxy device on a given network answers the ARP queries for an IP address that is not on that network. The Proxy is aware of a location of the traffic's destination, and offer its own MAC address as the lastly final Destination.

## ↳ PRACTICAL

Yellow Color :- Data port to which IP is given

Blue Color :- Console port for Device manager to take physical access of device

\* Console Cable is used with Serial to USB Converter

Software to take access of Physical Device :-

Secure CRT, Putty

These tool are an interface if we want to take the access of Real Hardware

↳ Access of R,S is taken in two ways :-

① CLI Command line Interface

② Physical Access → console port

06/12/2017

② Remote Access → Telnet, vty port, ssh

② http → Http, Https → curl tool.

## CABLING :-

### Co-axial Cable :-

#### Drawback:-

- ① Cross talk
- ② High Interference.
- ③ Degradation of Signal Quality.

\* These drawbacks are mainly due to the copper metal used in the ~~wire~~ as it produces E.M Waves which causes hindrance.

↳ Twisted Pair Cable :- It Overcomes the drawback of the Co-axial Cable so we use this nowadays.

\* It overcomes to large extent but not fully.

\* With Twisted Pair Cable we make two cables ↗

Cross-over Cable & Straight-talk Cable

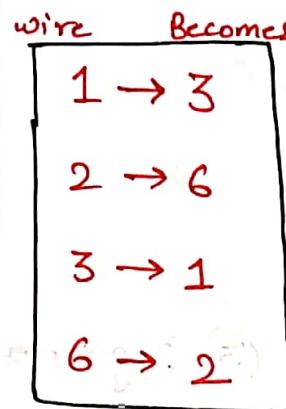
→ Inside both above cables the wire is still twisted but at connected end we connect them in two ways which divides it into cross over & straight through. & the difference can be checked by color coding.

## ↳ Color Coding of Cross-Over Cable

(2)

09/12/2019

Pin 1	Orange/white
Pin 2	Orange
Pin 3	Green/white
Pin 4	Blue
Pin 5	Blue/white
Pin 6	Green
Pin 7	Brown/white
Pin 8	Brown



Pin 1	green/white
Pin 2	green
Pin 3	Orange/white
Pin 4	blue
Pin 5	Blue/white
Pin 6	orange
Pin 7	brown/white
Pin 8	brown.

\* Used to Connect Similar Devices → R-R, SW-SW

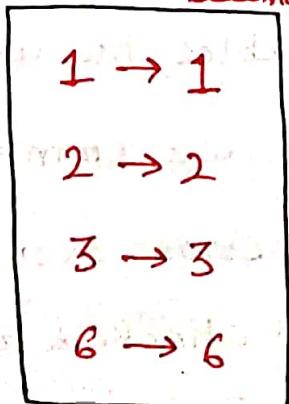
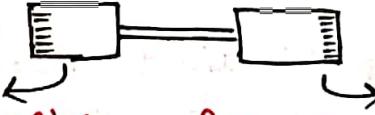
R=PC (Server), etc

\* Used to Connect Non-Similar Devices → R-SW

SW-PC etc

## ↳ Color Coding of Straight-Through Cable

Pin 1	Orange/white
Pin 2	Orange
Pin 3	Green/white
Pin 4	Blue
Pin 5	Blue/white
Pin 6	Green
Pin 7	Brown/white
Pin 8	Brown



Pin 1	Orange/white
Pin 2	Orange
Pin 3	Green/white
Pin 4	Blue
Pin 5	Blue/white
Pin 6	Green
Pin 7	Brown/white
Pin 8	Brown

ex →

PC  $\longleftrightarrow$  PC  
↓  
crossover cable

(3)

09/12/2019

Transmit [ 1 3 ] Receive  
2 6

Receive [ 3 1 ] Transmit  
6 2

\* Other 4 pins are unused & are used for POE (Power over ethernet)

PC  $\longleftrightarrow$  SW  
↓  
straight through cable

Transmit [ 1 1 ] Receive  
2 2

Receive [ 3 3 ] Transmit  
6 6

\* Other unused 4 pins are used for POE.

\* Nowadays we use Auto MDIX but not in old devices as not supported by old OS which was in old Routers.

\* (Automatic Medium-dependent interface crossover) detects the wrong cable and cause the switch to swap the pair it uses for transmitting and receiving, which solves the cabling problem. This feature is not supported on all Cisco devices.

## PRACTICAL

(4) 09/12/2019

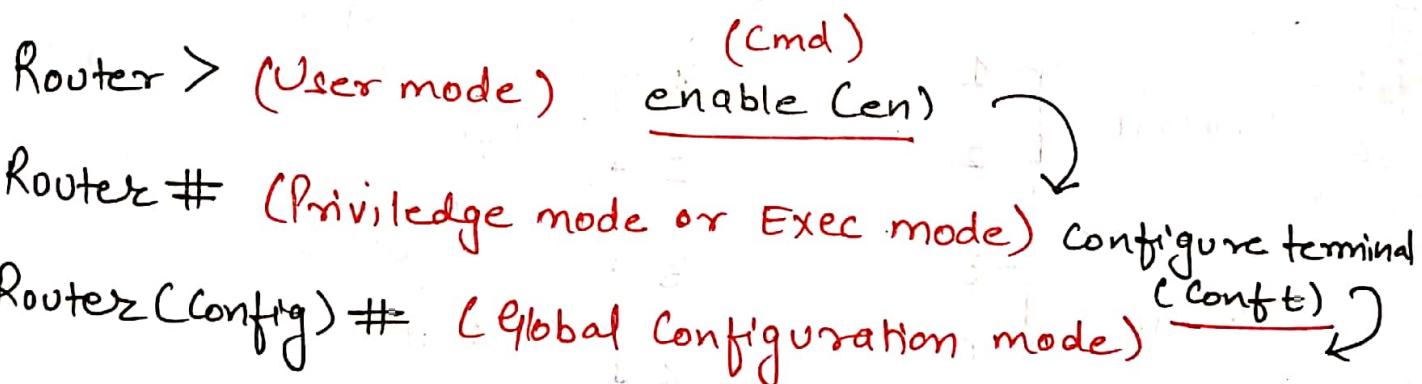
- ↳ We use two tools
- CPT
  - GNS3

In lab there will be mainly 3 router series at CCNA level

- ① 2811 Series
- ② 2911 Series
- ③ 2681 Series
- ④ 1841 Series

Up to CCIE level couple of more routers will add up.

### TOS [Router/Switch] Modes :-



- \* With 'exit' command or 'Ctrl+Z' you can exit or come out of ~~any~~ <sup>global</sup> mode and User Mode.
- \* To come out of Privilege mode type ~~an~~ 'disable' not 'exit' with exit you will be logged out.

### USER MODE :-

- ① Read only mode as it can't be configured
- ② Basic Show Command.
- ③ Telnet
- ④ SSH
- ⑤ Traceroute etc

## ↳ Privilege Mode :-

(5)

09/12/2019

- ① Kind of Read only mode as we can't configure but yes can read database.
- ② All Show commands.
- ③ All Debug Commands.
- ④ All Copy Commands.
- ⑤ All Erase Commands.

## ↳ Global Configuration Mode :-

- ① Allowed to modify the Database [Add & delete <sup>any</sup> End's]
- ② We can also Run previous mode Commands but we have to type 'do' at the beginning of commands.

## ↳ Shortcut Keys :-

- ① TAB Key → Autocomplete the command.
- ② Ctrl + A → At the beginning of line / command.
- ③ Ctrl + E → At the end of line / command.

## ↳ How to change Hostname?

Cmd → hostname\_R1

↳ How to Set up Username & Password?

cmd → Username \_ KK \_ Password \_ ccna ↴

ctrl + z

cmd → Show running - Config ↴ ← Pre. Mode

- \* Show running - config will show database that Username is KK & password is ccna in plaintext. But we can encrypt password by 'service password-encryption' cmd in Config mode

\* Service password cmd encrypt password with md5 algo so and it is still Vulnerable and can be decrypted so always set password with enable secret.

\* Type 'no' before command to delete the command , use in Config mode.

\* Enable Secret cmd Use md5 Algo.

↳ How set up Username & password with Secret ?

cmd → Username \_ KK \_ secret \_ ccna.

\* RAM

running - config

ROM

Startup - config

On reboot running config gets deleted so in order to save data we need to copy it from running config to startup config in Rom.

So, Cmd → Copy - Running-config - startup config  
file will be copied.

We can check by show running-config / startup-config  
or Simple Cmd is 'write'.

## LECTURE - II

10/12/2019 ①

Cmd → show\_version

↳ for software version

cmd → Show\_history

↳ for previous command used.

(By default display 10 commands only).

cmd → Show\_terminal

↳ to check history buffer/length.

cmd → terminal\_history\_size\_(0-256)

↳ choose any size to change buffer/length.

cmd → Show-ip-interface-brief

↳ to check interface summary

↳ TELNET :-

→ L-7 Protocol

→ works over TCP port no. 23

→ Used to remote access of network device (R, Sw, F etc).

\* Data is sent in plain text.

→ How to give ip to an interface?

# Interface\_FastEthernet\_0/0

# No\_Shutdown

# ip\_address - 192.168.1.1 - 255.255.255.0

ip

Subnet Mask.

}  
Global  
mode

\* We can give ip to pc by clicking on it.

### ↳ Steps to Configure telnet

- ① Username & password [ for user mode ] } to Secure user &
- ② Privilege mode password. } privilege mode.
- ③ Go to Vty line and allow telnet.

→ # username\_KK\_secret\_ccna (for user mode)  
# Enable\_secret\_ccna (for privilege mode).

→ # line\_vty\_0\_2 (to allow no. of user who can access your router).  
# login\_local

- ↳ (i) Router will prompt username & password.
- (ii) And that username & password.

\* For only login → Router will prompt password only.

# Telnet \_ 192.168.1.1 ] → on the pc or router you want to take access on.

↳ Then it will ask for username & password on User mode & then again password on privilege mode.

↳ After that you will have access of Router

cmd → show\_users

↳ display no. & name of user who are presently accessing the device.

cmd → exit (on PC)

↳ To exit Remote login.

- \* By default idle timeout is 10 minutes so if system remains inactive after remote login the it exit after 10 minutes.

cmd → line\_clear\_326 (no. written before vty in show-user cmd).

↳ to terminate telnet session from router.

cmd → Transport-input-telnet



↳ SSH :- (Secure Shell)

- ① LT Protocol
- ② works on TCP port no. 22
- ③ Used to remote access of network devices.

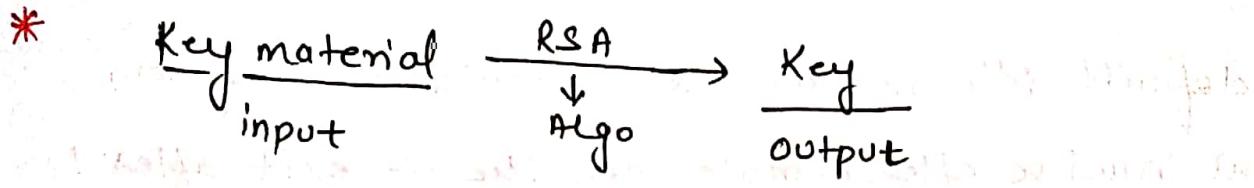
\* Data sent in cipher text

↳ (unreadable or encrypted)

↳ Steps to Configure ssh

- ① Change your hostname
- ② Create username & password
- ③ Create privilege mode password.
- ④ Define a domain name
- ⑤ Generate crypto key

⑥ Go to vty line and allow SSH.



# Username - KK - secret - ccna

# Enable - secret - ccna

# crypto-key-generate-rsa

↳ then it will ask for to change hostname & domain name as after that only key will be generated.

# Hostname - R1

# ip-domain-name - guftgu.com

↳ it ask for bit in modulus [512-2048] choose any in between them.

# line-vty-0-2

# login-local

# exit.

On pc

# ssh -l KK - 192.168.1.1

↳ then it will ask for user & privilege mode password.

① DHCP :- ① L-7 Protocol

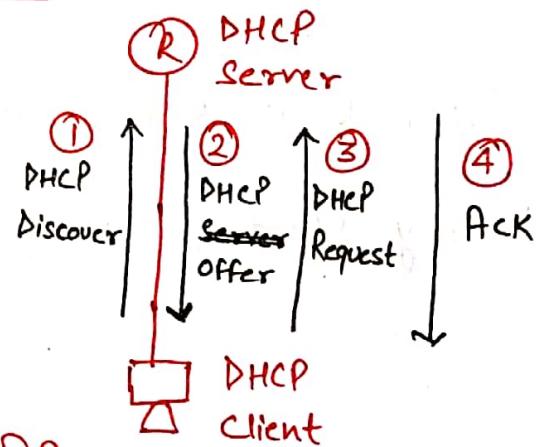
② Works over UDP port no. 67 & 68

③ Used to dynamically distribute ip addresses to its client

DHCP (Dynamic Host Configuration Protocol)

- \* To access Internet we need the following things:
  - IP, Subnet Mask, Default gateway & IP of DNS server.
- \* Messages gets exchanged b/w DHCP Server & DHCP Client which we can learn through DORA

D → Discover  
 O → Offer  
 R → Request  
 A → Acknowledgement



- ① In DHCP Discover packet source IP will be 0.0.0.0 & Destination IP will be 255.255.255.255
- ② In DHCP offer packet → S. IP → DHCP Server IP  
                             D. IP → 255.255.255.255

- \* There is lease time for which DHCP Server offers IP to a client [ex for cisco ios it is 24 Hours]
- ③ In DHCP Request packet client may ask for lease time ext' or/and may sent the ip it has chosen with DHCP Server IP to update which server ip it has selected [In case of multiple DHCP servers]

## ↳ How to Configure DHCP?

```
# int_fo0
# ip-add_ 192.168.1.1_ 255.255.255.0
# no shutdown
# ip-dhcp-pool_Networkbulls
# Network_192.168.1.0_ 255.255.255.0
# Default-router_ 192.168.1.1
# DNS-server_ 8.8.8.8
# exit
# ip-dhcp-excluded-address_ 192.168.1.1_ 192.168.1.10 ]
```

It's to exclude the  
ip's we give manually

## ↳ How to Backup Startup Config?

```
# copy_startup-config_tftp:
```

↳ Then it will ask for ip & the name you want to save the file with.

Cmd → Erase startup-config

↳ To delete startup config.

## ↳ How to restore startup config?

```
# copy-tftp:_ startup-config
```

↳ used to restore startup config to ~~the~~ from tftp server if deleted.

## ↳ How to Backup IOS?

11/12/2019 (3)

\* show version → To copy IOS file name

# copy - flash: - tftp:

↳ Then it will ask for source file name, host server ip & destination file name.

## ↳ How to Restore/ update IOS?

# copy - tftp: - flash:

↳ Then it will ask for ip of remote host, source ~~addr~~ filename & destination file name.

## ↳ How to Reset Password?

- \* By default Configuration Register value of Router is 0x2102
- \* Register Value 0x2102 performs two things:
  - ① It Boots IOS
  - ② It copies startup config in Running config.
- \* But if we forgot password & startup config file gets copied in running config then it will ask for password.
- \* So we break boot process to enter into Rommon mode by  $\text{ctrl}+\text{c}$  /  $\text{Pause}$   $\text{Break}$  to change the register value & set up new password.

0x2142 (New)

### → Steps →

- # Restart your Router
- # Press  $\text{ctrl}+\text{c}$  /  $\text{Pause}$   $\text{Break}$  to abort boot sequence
- # Rommon1> confreg\_0x2142
- # Rommon2> reset
- # Router> enable
- # Router# copy-startup-config - Running-config.
- # R1# Conf t
- # R1(Config)# Change password (ex enable\_secret\_ccna).
- # R1(Config)# Config-register\_0x2102
- # R1(Config)# do\_write
- # R1# reload.

## ROUTING

→ When we want to connect two or more n/w's using different n/w addresses then we have to use IP Routing technique. The router will be used to perform routing b/w the networks.

→ A Router will perform following function for Routing:

- ① Path determination
- ② Packet forwarding

① The process of obtaining path in routing table is called path determination. There are different methods to which router can learn path.

- Static & Default Routing
- Dynamic Routing

② It's a Process that is by default enable in routers. The router will perform packet forwarding only if route is available in the routing table.

## STATIC ROUTING :-

### Syntax

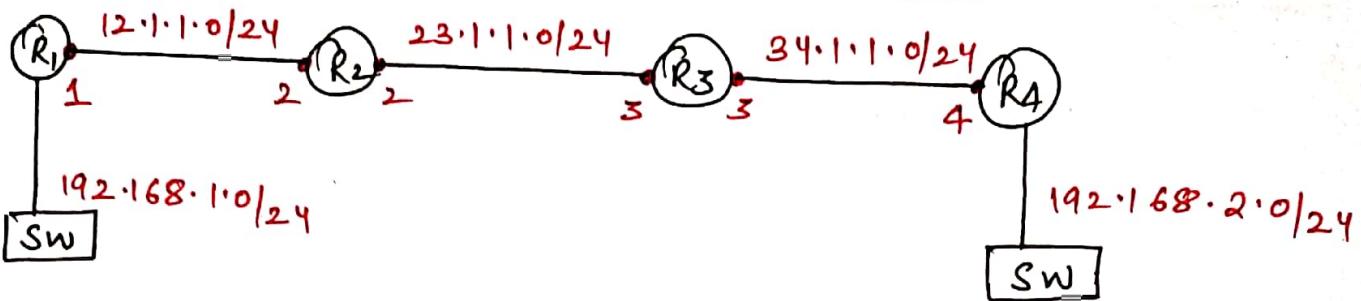
```
# Router(Config)# ip_route -<dest n/w> <s/m> <next hop ip>
```

\* Next hop Ip is the <sup>ip</sup> address of neighbor router that is directly connected to our router.

12/12/2019

(3)

hop = Router  
next hop ip = nextRouter.ip



\* No-ip-domain-lookup command ↴

when we type incorrect command

it gets checked in CLI command & if any command does not match then it checks the domain server if its is any Computer name configured on DNS Server

So if we want to ~~stop~~ that then we can use the above command.

cmd # Show-ip-route

↳ To check routing table

In Routing table:

C → directly connected

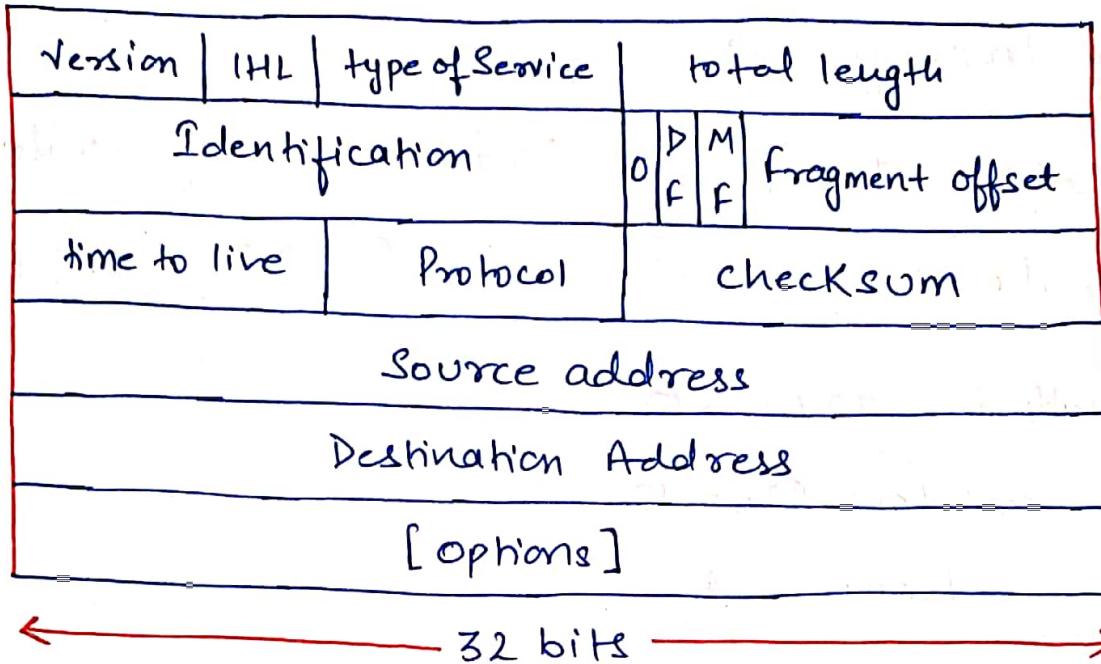
S → static Routing

1

## IP HEADER FORMAT

LECTURE-14

13/12/2019



\* The ip datagram header has a minimum length of 20 bytes & maximum length is of 60 bytes [20-60 bytes]

# Version → IPv4 or IPv6

# IHL → Internal Header length (Here 20 bytes) but can be  
 ↳ But total<sup>length</sup> = Data length + Header length [20-60 bytes]  
 $1500 = 1480 + 20$

# type of Service → used for traffic prioritization

# Time to live (TTL) → The TTL sets an upper limit on the number of routers through which a datagram can pass. It limits the lifetime of the datagram. It is initialized by the sender to some value (often 32 or 64) & decremented by one by every router that handles the datagram.

13/12/2019

(2) When this field reaches 0, the datagram is thrown away, and the sender is notified with an ICMP message. This prevents packet from getting caught in routing loops forever.

# Protocol :- This field indicates the higher level / upper layer protocol. ex TCP, UDP, OSPF, EIGRP etc.

\* Default Ios TTL = 255

Window TTL = 128

Linux = 64

\* TTL Decrements on the sending port not receiving port.

# Check Sum → Used for Error Detection.

↳ It is an Algorithm

\* Sender runs checksum & attach value to sender header & when ~~data~~ packet is received at receiver then it again runs checksum & matches value.

\* So if Value matches then it means there is no error.

# Identification :- A unique number assigned by the sender to aid in reassembling a fragmented datagram. Each fragment of Datagram has the same identification number.

③ # Flags → This field contains control flag

0: Reserved, must be zero

DF (Do not fragment)

OFF : 0 means allow fragment

ON : 1 means do not allow fragment.

MF (More fragment)

OFF : 0 means that this is the last fragment of the datagram

ON : 1 means that additional fragments will follow.

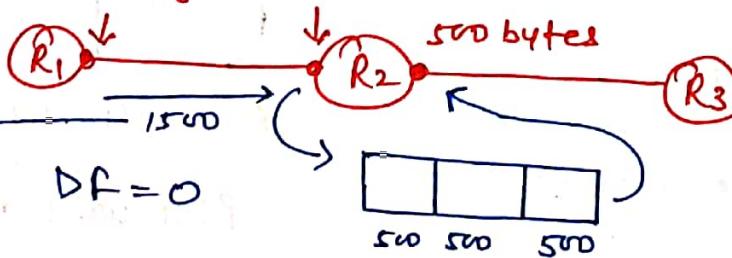
# Fragment offset → This is used to aid the reassembly of the full datagram.

is the

If this first (or only) fragment, this field contains the value of zero.

1500 bytes 1500 bytes

ex



complete  
1500 bytes

get forwarded

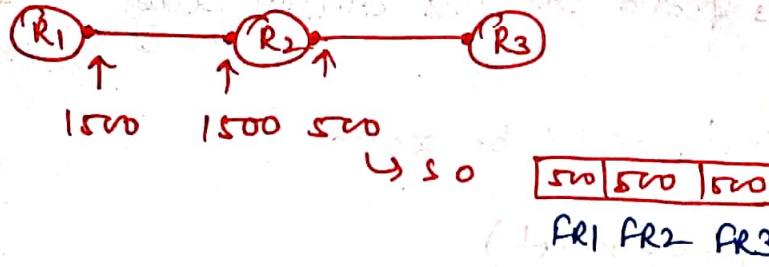
$DF = 1 \rightarrow$  Packet drops if MTU size is 500 but received is 1500 moreover  $DF = 1$

$DF = 1$  also does not make a difference

4

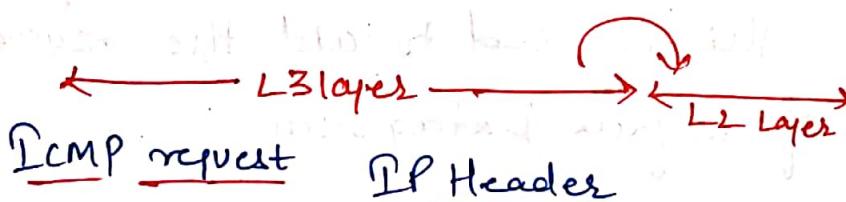
ex

13/12/2019



$M_F = 1$  at R<sub>3</sub> input terminal which means more fragment will follow

, when FR<sub>1</sub> is received which is a last fragment so  $M_F = 0$  will be sent



Type-8	S.IP 192.168.1.1	S.Mac PCA
Code-0	D.IP 192.168.1.2	D.Mac PCB

S/M  $\rightarrow$  255.255.255.0

A	B	Y
0	0	0
0	1	0
1	0	0
1	1	1

\* with AND operation

PCA will verify that if PCB is in a same network or in a different network

(5)

13/12/2019

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

1 1 1 0 0 0 0 0 → 192

1 0 1 0 0 0 0 0 → 168

0 0 0 0 0 0 0 1 → 1

0 0 0 0 0 0 0 1 → 1

1 0 → 2

S.I.P

11000000 · 10101000 · 00000001 · 00000001 → 192.168.1.1

1111111 · 1111111 · 1111111 · 00000000 → 255.255.255.0

11000000 · 10101000 · 00000001 · 00000000 → AND

↓              ↓              ↓              ↓              ↓              operation  
192    ·    168    ·    1    ·    0    → Network.

D.I.P

11000000 · 10101000 · 00000001 · 00000010 → 192.168.1.2

1111111 · 1111111 · 1111111 · 00000000 → 255.255.255.0

11000000 · 10101000 · 00000001 · 00000000 → AND

↓              ↓              ↓              ↓              ↓              operation  
192    ·    168    ·    1    ·    0    → Network.

→ In this way we can see that both the IP's are of same network.

- \* Since PCA & PCB are in same n/w so we need the MAC address of PCB , But if they would have been in different n/w then we would have needed default gateway MAC.
- \* ICMP first packet drops as we do not have MAC of PCB & ARP Comes in to resolve MAC from IP.

\* So,

ICMP reply .	IP header	etherenet header
ICMP reply type -0 Code -0	S·IP → 192.168.1.2 D·IP → 192.168.1.1	S·MAC PCB D·MAC PCA

## STATIC ROUTING WITH SELF EXIT INTERFACE

- \* It is same as static routing with just one difference that instead of next hop ip we put exit interface self name.

### Syntax

Router(Config)# ip-route- <Dest^n/w> - <mask> - <self exit interface name>

ex ip-route- 23.1.1.0 - 255.255.255.0 - fastethernet 0/0  
 Router self exit interface name

- \* In static Routing with self exit interface show all n/w directly connected but with next hop ip it shows via --- connections.
- \* Next hop ip is used in real time but self exit interface is not as self exit has proxy arp enabled [even router has proxy arp enabled by default]
- \* Proxy arp resolution is a cpu intensive task & not enabled due to security purposes.
- \* Next hop ip routing resolve arp which is good if used in real time

cmd → #interface - fastEthernet 0/0

# no-ip-proxy-arp → to disable proxy arp.

## DEFAULT ROUTING :-

Default Routing means route for any n/w.

### Syntax

```
Router(Config)# ip-route-0.0.0.0-0.0.0.0-<next hop>
or
Router(Config)# ip-route-0.0.0.0-0.0.0.0-<exit interface>
```

- \* Any traffic from any n/w will be forwarded to next hop in default routing & it is used in following scenarios

### Scenario 1

A n/w which has only one exit interface

### Scenario 2

- Internet Connectivity - On internet, million of n/w are present. So we have to specify default routing on our router.
- Default route is also called gateway to last resort. This route will be used when no other routing protocol is available.

16/12/2019

## DYNAMIC ROUTING

Administrative Distance :- AD is used to specify one route as primary and mark other route as backup. Router will select lower AD route to forward the traffic.

### Protocols

	<u>AD</u>
Directly Connected	0
Static	1
BGP	20
EIGRP	90
OSPF	110
RIP	120

- \* In dynamic routing we will enable routing protocol on router. This protocol will send its routing information to the neighbour router. The neighbour will analyze the information & write new routes to the routing table.
- \* The router will pass routing information received from one router to other router also. If there are more than one path available then routes are compared & best path is selected.

ex of dynamic protocol :- RIP, EIGRP, OSPF.

## Types of Dynamic Routing Protocol

Acc<sup>n</sup> to working there are two types

- ① Distance Vector - RIP
- ② Link state - OSPF
- ③ Hybrid - EIGRP

According to the type of area in which protocol is used there are again two types.

- ① Interior Routing Protocol (IRP) - RIP, EIGRP, OSPF
- ② Exterior Routing Protocol (ERP) - BGP

## Metric of Dynamic Routing

Metric are the measuring unit to calculate the distance of destination n/w. A protocol may use a ~~one~~ or more than one at a time to calculate the distance.

Different type of metric are:

- ① Hop count
- ② Band width
- ③ Load
- ④ Reliability
- ⑤ Delay
- ⑥ MTU

RIP - hop count

OSPF - Bandwidth

EIGRP - B.W

Load

Delay

Reliability, MTU

16/12/2019

(5)

→ Method to solve routing loops in distance vector routing protocol.

There are 4 different methods to solve or reduce the problem of routing loop:

- ① Maximum Hop Count
- ② Flash updates / Triggered update
- ③ Split Horizon
- ④ Poison Reverse

(There are 5 actually  
but 5th one will be  
covered in CCNP &  
on.)

## ↳ RIP (Routing Information Protocol)

# Features of RIP :-

- ① Distance Vector
- ② Open Standard.

\* Metric

Hop Count

\* Timers

Update - 30 sec

Invalid - 180 sec

Hold - 180 sec

Flush - 240 sec

\* Maximum Hop Count - 15

\* Administrative Distance - 120

\* Equal path Cost load Balancing

RIP ver1

1) Doesn't support VLSM

2) Send periodic updates in every 30 sec by using broadcast address  
( $255.255.255.255$ )

RIP ver2

1) Support VLSM

2) Send periodic updates in every 30 sec but by using multicast address (224.0.0.9)

↖ Here periodic  
↙ updates mean  
periodic routing  
updates.

17/12/2019

(2)

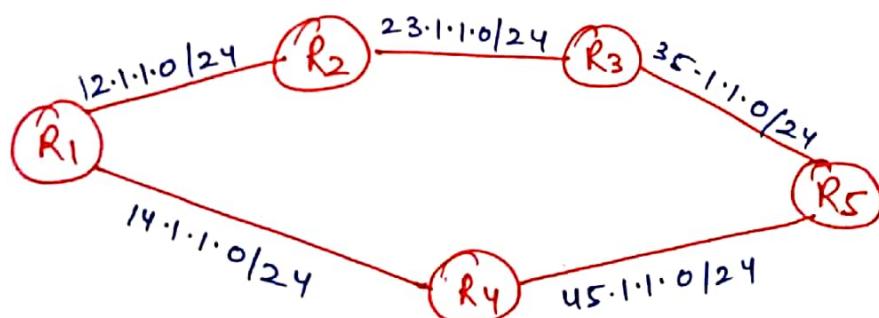
### RIP v1

- 3) Doesn't send subnet mask information in routing updates.
- 4) Classful routing protocol
- 5) Does not support Authentication

### RIP v2

- 3) Send subnet mask information in routing update.
- 4) Classless routing protocol
- 6) Support both plain text & MD5 Authentication.

### Lab



### cmd's

```
router(config) # router_rip
```

```
router(Config-router) # version2
```

→ need not to type version 1  
in case of version 1

(If not used then it will → # no\_auto\_summary [ Here it is used to  
Keep it in classfull nature] ↳ convert classfull  
behaviour into classless]

(ex for R1) {

```
# network - 12.1.1.0 → [ own network  
# network - 14.1.1.0 → [ Address ]  
# exit
```

17/12/2019

Cmd → Show-ip-route-rip [This command is used to see filtered routes for any protocol]

\* In rip routing table we will see [120/2] if there is 2 path to any n/w so here 120 is AD  
2 is metric [hop count]

\* Also here comes the concept of equal packet load balancing as metric value is same for two routes.

Cmd → traceroute (to track packet route)

traceroute - n/w (where we need to reach.)

Cmd → Debug-ip-rip  
↳ Helps in showing packets on console window for updates which does not happen by default.

Cmd → undebug-all

↳ to disable debug-ip command.

↳ Loop Control/avoidance method :-

① Split horizon :- It states a route that update receive from an interface cannot be send back to same interface.

\* It is enabled by default.

cmd# no-ip-split-horizon

↳ to disable split horizon.

cmd# ip-split-horizon

↳ to enable split horizon

(But enable by default).

↳ Route Poison :-

\* Maximum hop count is 15 so total no. of router is 16

\* So we can say that n/w becomes unreachable when hop count reaches 16.

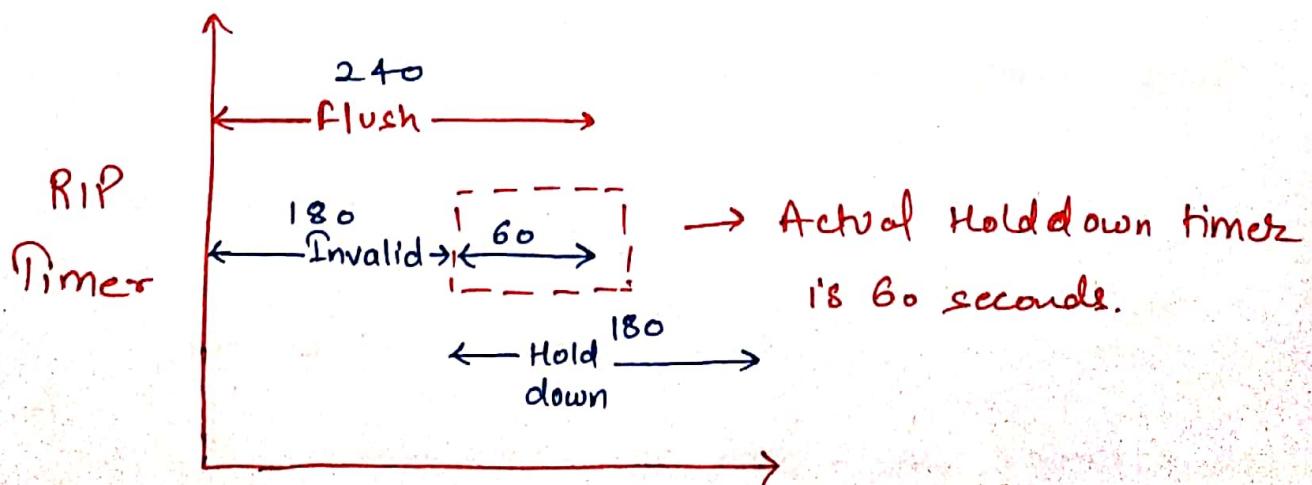
\* Therefore if any network/Router becomes dead then ~~the~~ its hop count value ~~is~~ becomes 16 & update is sent to all neighbouring routers. to indicate n/w unreachability

↳ Triggered update :- In this method a partial update is sent to all the neighbours as soon as there is topology change.

\* We do not wait for periodic update after a change & only update specific to change is sent.

## RIP Timers

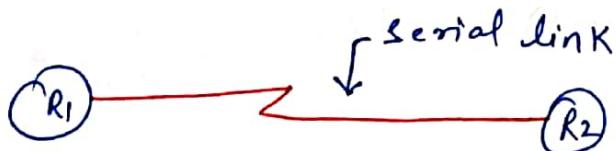
- ① Update :- this is how often we send routing updates, the default is 30 seconds.
- ② Invalid :- the no. of seconds since we received the last valid update, once this timer expires the route goes into holddown, the default is 180 seconds.
- ③ Holddown :- The no. of seconds that we wait before we accept any new ~~new~~ updates for the route that is in holddown, the default is 180 seconds.
- ④ Flush :- How many seconds since we received ~~that~~ the last valid update until we throw the route away, the default is 240 seconds.



## ↳ OSPF (Open shortest Path first)

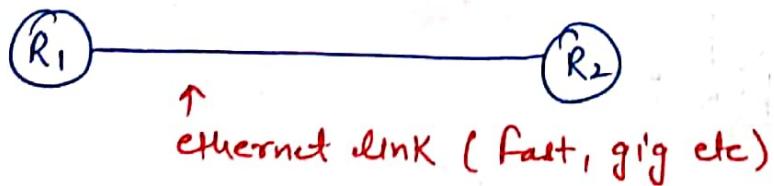
- # Link state routing Protocol
- # Open standard Routing Protocol
- # Works on Protocol no. 89
- # Metric → Bandwidth
- # Multicast address → 224.0.0.5, 224.0.0.6
- # OSPF uses SPF algo for best path calculation.
- # Support equal cost load balancing.
- # Supports Unlimited hop counts.
- # Uses hierarchy structure.

## ↳ Point to Point Network



\* Serial link is also called WAN link

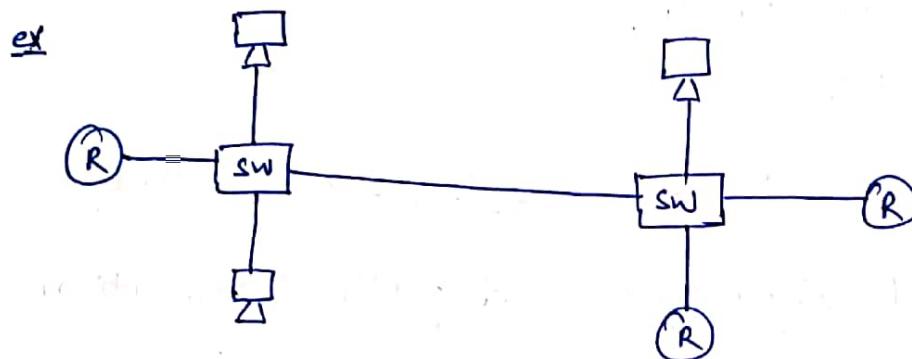
↳ Cisco consider it point to point n/w.



↳ Cisco consider it as Broadcast n/w not point to point n/w.

## Broadcast n/w [Multi-access n/w]

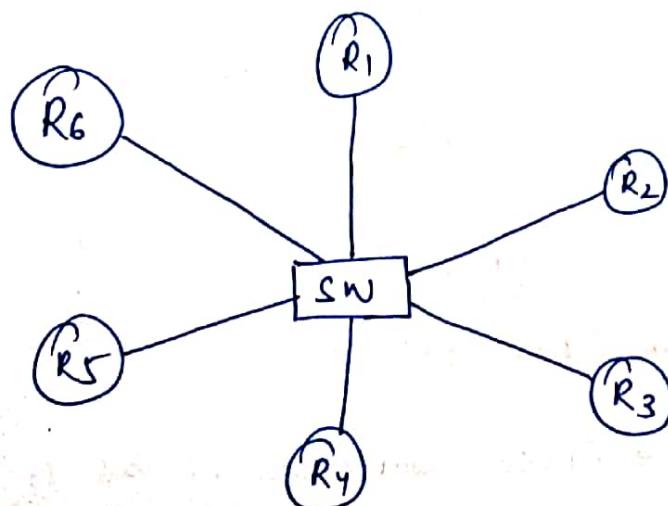
Multi access n/w consist of more than 2 devices sharing the same media.



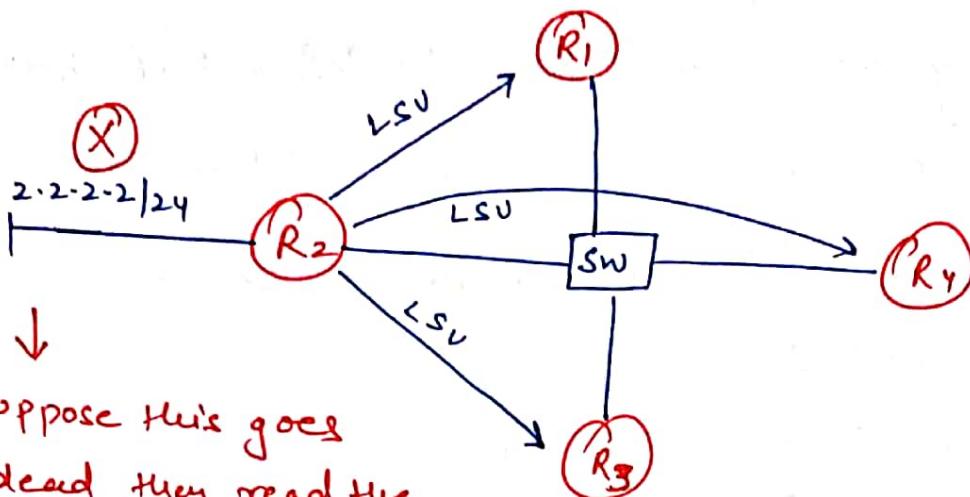
## Challenges in Broadcast n/w [Multi-access n/w]

- ① Multiple adjacency (neighbors)
- ② flooding of LSA (data)

→ Total no. of neighbor =  $\frac{n(n-1)}{2} = \frac{6(6-1)}{2} = \frac{6 \times 5}{2} = \frac{30}{2} = 15$



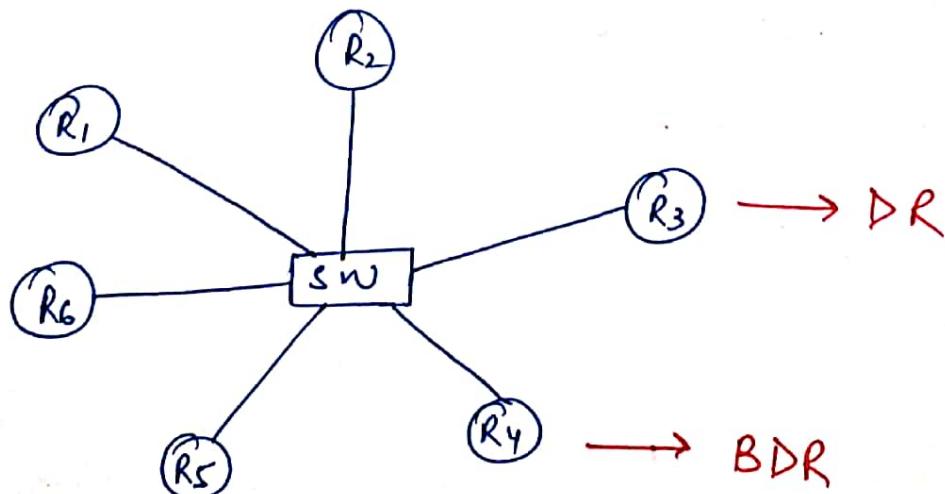
11



- \*  $R_2$  will update  $R_1, R_3, R_4$  & then  $R_1$  will update  $R_4$  &  $R_3$  & then  $R_3$  will update  $R_4$  so data which is same getting transmitted / flooded in the n/w which is one of the challenges of Broadcast n/w.

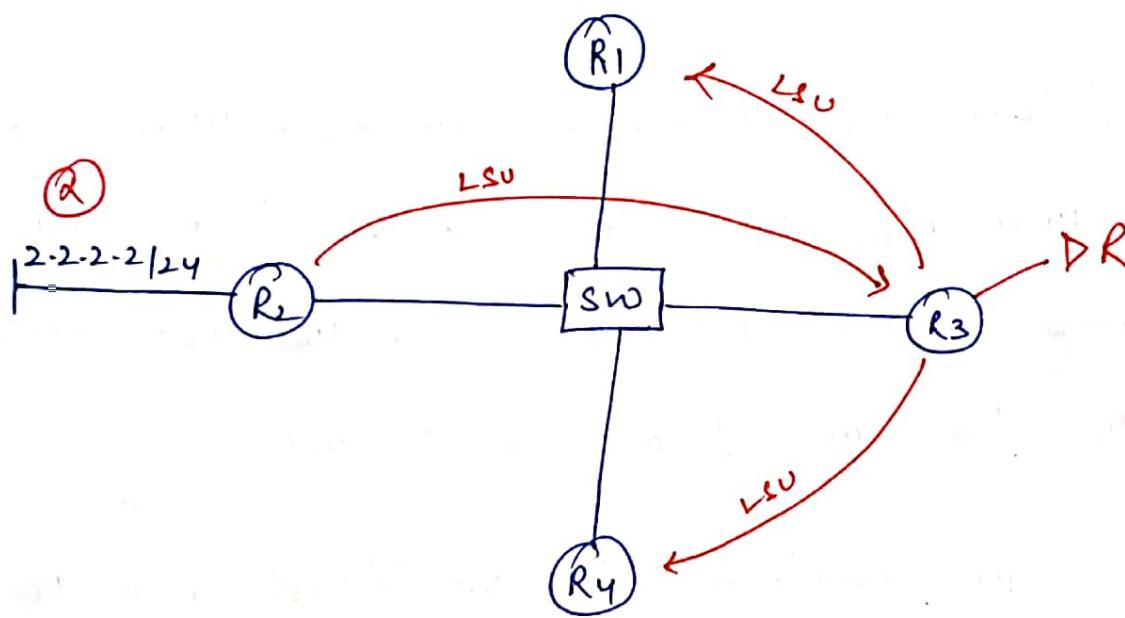
# To overcome the challenges of Broadcast or multi-access n/w, we use the concept of DR & BDR

- DR (Designated Router)
- BDR (Backup Designated Router)



- \* So here every router will update DR & BDR ~~but~~  
not every router so total no. of neighbor will be 9 as DR & BDR will also be neighbor. so we can see challenge<sub>1</sub> is controlled.

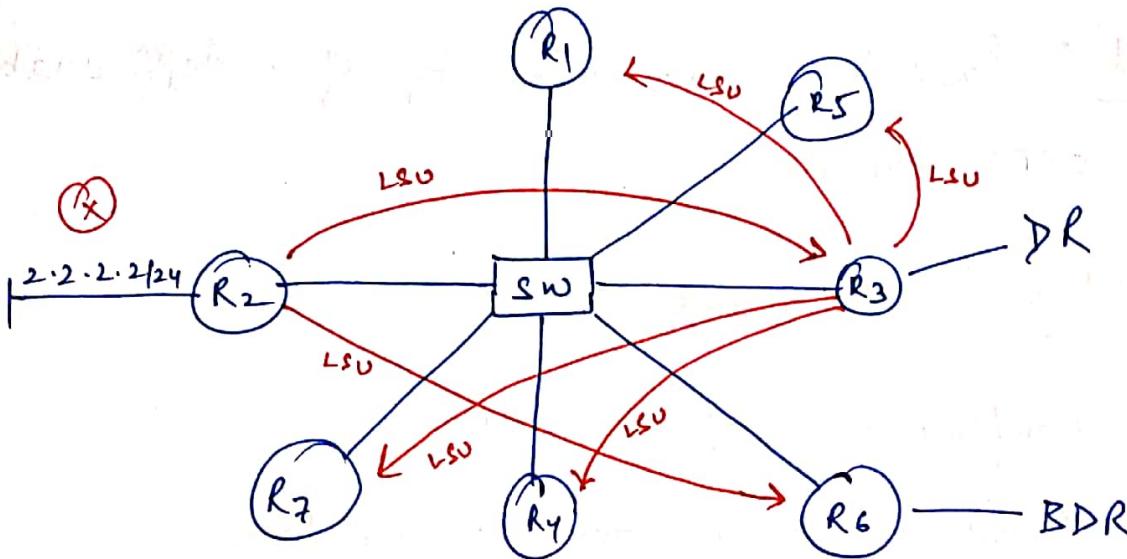
Now assume 2nd challenge scenario



- \* Here if n/w of 2.2.2.2/24 on R2 goes dead then R2 will update DR & then DR will update R1 & R4 so there's controls LSU flooding.

\* Extra Case for explanation

\*



↳ DR & BDR election

- ① DR is one having highest priority & BDR is one having second highest
  - ② If priority is ~~tie~~, then DR is one having highest router id & BDR is the one with second highest router id.
- \* By default router priority is 1 but if we make any router priority 0 then router becomes 'DR Other'. This happens in the case we do not want any router to become DR or BDR.

↳ Router id :- Provides unique identity of a OSPF enabled router in OSPF domain.

↳ Router-id Election Process :-

- ① Manual Configuration of the router ID.
- ② Highest IP address on a loopback interface
- ③ Highest IP address on a non-loopback interface.  
(Physical)

\* Among Loopback & physical interface we choose loopback over physical as loopback will not go down until & router is down.

↳ Wildcard Mask :- Opposite of Subnet Mask.

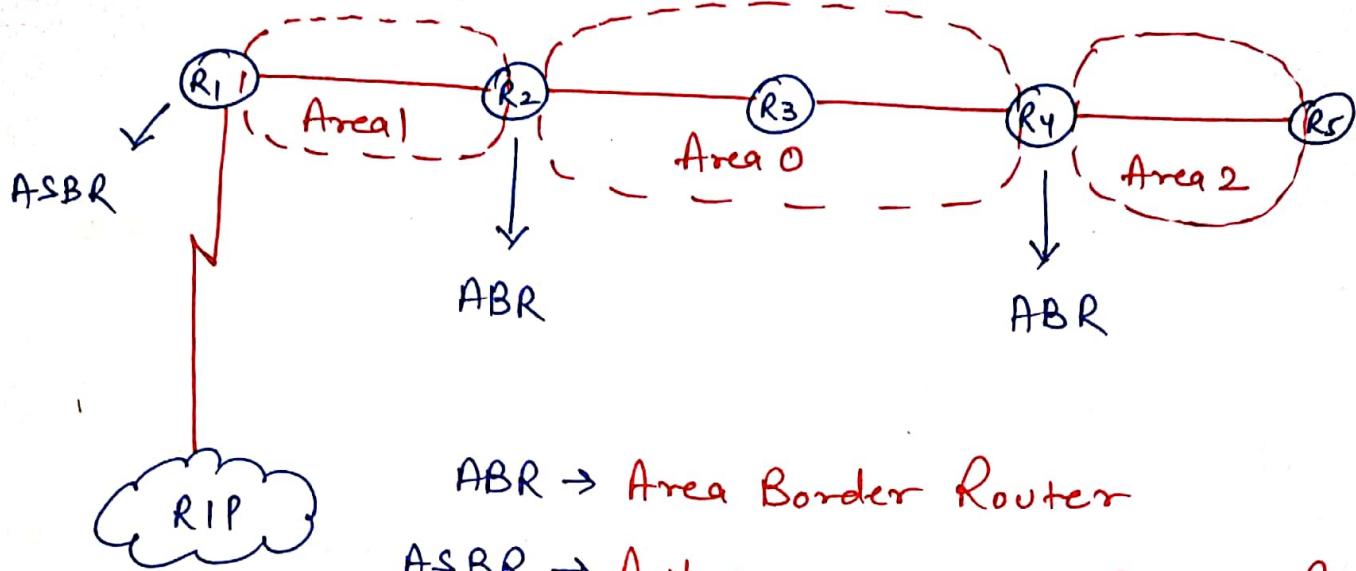
Class C  $\rightarrow$  255.255.255.0 - S/M

Wildcard  
Mask  $\rightarrow$  0.0.0.255

Class C  $\rightarrow$  255.255.255.192

wildcard  
mask  $\rightarrow$  0.0.0.63

↳ In W/M    0  $\rightarrow$  Matching bit  
                  1  $\rightarrow$  don't care bit.



$\text{ABR} \rightarrow$  Area Border Router

$\text{ASBR} \rightarrow$  Autonomous system Border Router

- \* Area 0 is called Backbone Area.
- \* ASBR is router whose both interface is connected to different domain like here is RIP & OSPF
- \* ABR has both interface in same domain like OSPF here
- \* For All Area it is important to have connectivity/link to Backbone Area otherwise they would not be able communicate even if directly connected.
- \*  $R_3$  is Backbone router as it is in complete Backbone area.

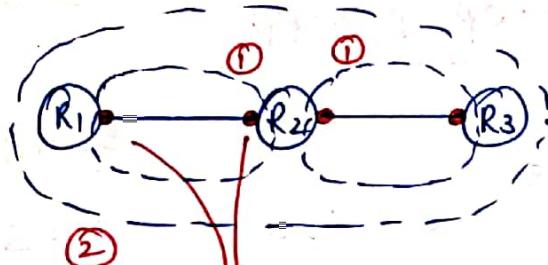
LECTURE-18↳ Neighbour Requirements for EIGRP & OSPF

	<u>OSPF</u>	<u>EIGRP</u>
→ Interfaces primary IP addresses must be in same subnet.	→ YES	YES
→ Must not be passive on the connected interface	→ YES	YES
→ Must be in same area.	→ YES	N/A
→ Hello Interval / Timer, plus either the Hold (EIGRP) or Dead (OSPF) timer must match	→ YES	NO
→ Router ID must be unique.	→ YES	NO
→ IP MTU must match	→ YES	NO
→ Must pass neighbour authentication (if configured)	→ YES	YES
→ K-values (Used in metric calculation) must match	→ N/A	YES
→ Must use the same ASN (EIGRP) or process ID (OSPF) on the router configuration command.	→ NO	YES

\* Above requirement defines when two routers should be neighbours.

19/12/2019

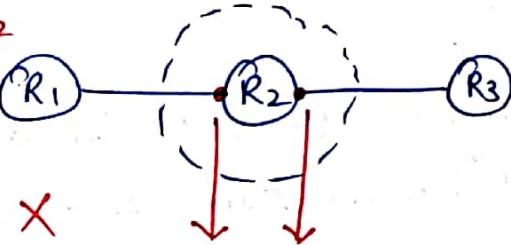
\* Same subnet must be a member of same area.

Case 1

① ✓

Both interface  
are same subnet

② X

Case 2

X

Both are diff subnet  
so choice of Area is  
wrong.↳ Syntax

```
Router(config) # router_ospf - P. ID (Process Id)
```

```
# network _ own_nfw_id _ wildcard  
Mask — Area — Area-id
```

ex Area 2

#

#

# Exit.

↳ Process Id → 16 bit identity (1-65536)

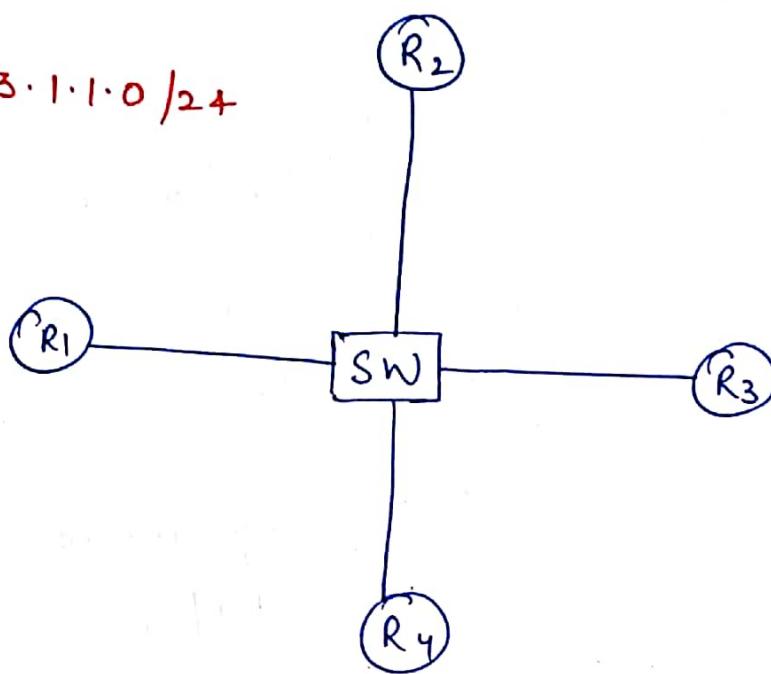
→ Locally Known

→ Used to identify no. of ospf process running on a router.

19/12/2019

## Class practical

$\text{N}|\text{w} \rightarrow 13.1.1.0/24$



\* It's Broadcast n/w so  
n/w will be same but  
ip will be diff.

\* If we match ip we keep all 0 i.e. 0.0.0.0 & in case  
we want to match n/w in/24 we put 0.0.0.255 in  
wildcard mask.

↓  
(don't care)

↓  
so it will match  
first 3 block only.

cmd `Show_ip_ospf_interface_fastethernet0/0` ↴  
↳ to check ospf enable or not & it also shows  
DR, BDR status.

\* When ospf is enabled with the above command we can see  
that after enable a router waits for 40 sec to elect DR  
& BDR as might be other router may go live in n/w.

\* But if router gets assigned as DR being a lowest ip also  
then after highest ip goes live the already assigned  
router will stay DR until its dead.

19/12/2019

(4)

- \* if DR goes down then BDR is promoted to DR & then BDR will be the router with highest ip.

cmd # router OSPF\_1  
# router\_id - 4.4.4.4 ] global mode  
Then it will ask to clear/reload  
OSPF process.

# clear\_ip OSPF\_process ] Privilege mode.  
then enter Yes/No

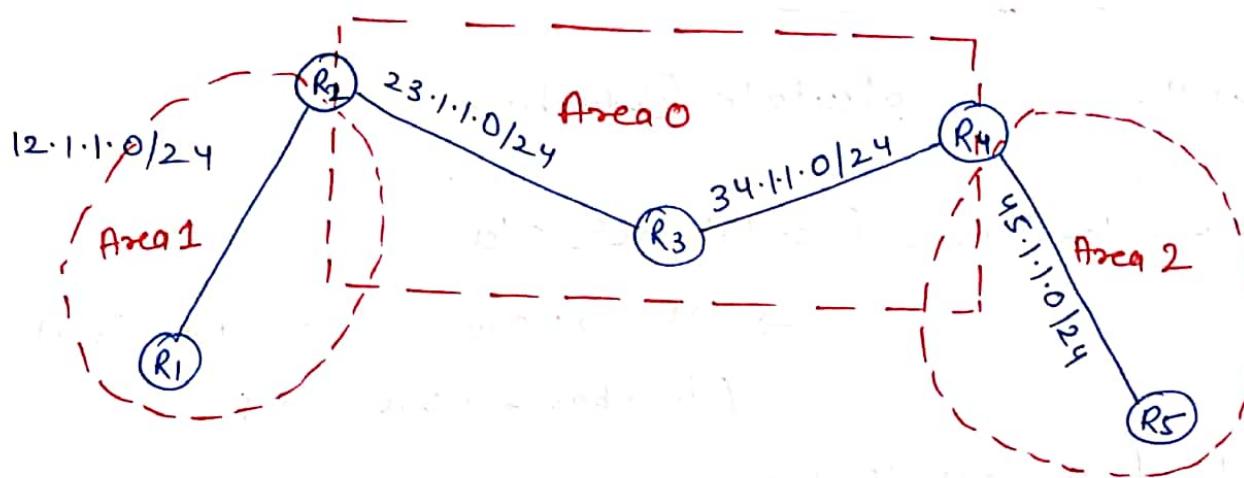
- \* Manual router id is preferred so we set it up manually above & after reload router id will change to 4.4.4.4

↳ 224.0.0.5 is a multicast address used in below scenarios.

- ① Hello packets
- ② Point to point n/w
- ③ Goes to all OSPF routers on a link/Broadcast n/w subnet

↳ 224.0.0.6 is also a multicast address used in below scenarios.

- ① Broadcast n/w [ Goes to DR & BDR on a link]



R1# router ospf 1

# network 12.1.1.0 0.0.0.255 area 1

R2# router ospf 1

# network 12.1.1.0 0.0.0.255 area 1

# network 23.1.1.0 0.0.0.255 area 0

For all Router

cmd# show ip route ospf → This can also be checked for other protocols.

→ It will show ospf routes.

O → OSPF

O IA → OSPF Intra Area

O E1/E2 → OSPF External route (from another domain)

Could be RIP, EIGRP or OSPF also.

Here we see in routing table that routes.

110/20 or 110/30 for diff  
AD ↓ Metn'c

$$\text{Metric (Cost)} = \frac{\text{reference B.W}}{\text{Interface B.W}}$$

20/12/2019

(2)

Reference B.W = 100 mbps by default

If we will learn to calculate Interface B.W.

cmd# show\_interfaces\_fastEthernet\_0/0

→ It will show Interface B.W  
(in Kbps & mbps both)

Here in practical it was 10mbps

$$\text{So Metric} = \frac{100}{10} = 10$$

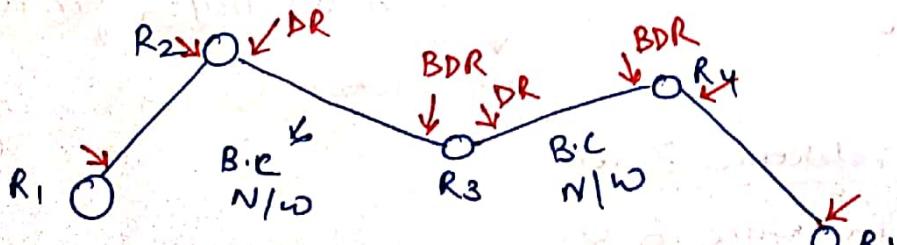
→ OSPF Maintains 3 types of Tables:-

- ① OSPF neighbor table → Maintain neighbors information.
- ② OSPF Database table → Database of LSA.
- ③ OSPF Routing table → Best Route.

cmd# show\_ip\_ospf\_neighbor

→ It will show the neighbor routers.

\* DR & BDR election depends on network not on Area



(Conn b/w router's B.C n/w so it will have its on DR & BDR)

20/12/2019

(3)

Cmd# show-ip-ospf-database

↳ to check database table

Cmd# show-ip-route-ospf

↳ to check routing table.

Cmd# show-ip-ospf

↳ to check ospf details like spf algorithm run count.

\* OSPF behaves as link state routing protocol within area but outside area it behaves like distance vector routing protocol.

↳ OSPF Packet types:

# HELLO: Neighbor discovery, build neighbor adjacencies and maintain them.

# DBD: This packet is used to check if the LSDB b/w 2 routers is the same. The DBD is a summary of the LSDB.

# LSR: Requests specific link-state records from an OSPF neighbor.

# LSU: Sends specific link state records that were requested. This packet is like an envelope with multiple LSAs in it.

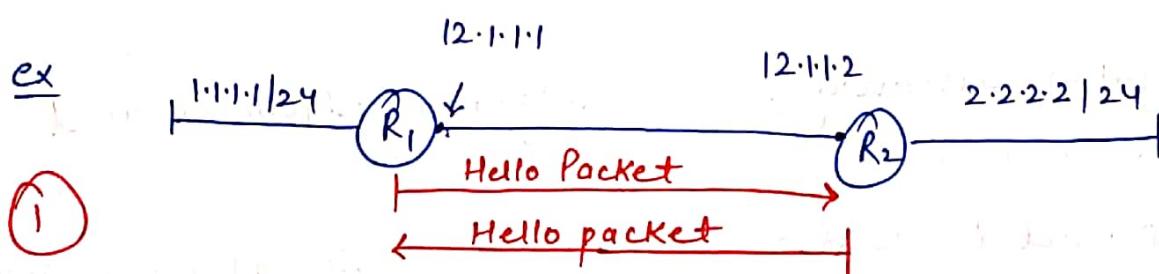
# LSAck: OSPF is a reliable protocol so we have a packet to acknowledge the others.

20/12/2019

(4)

↳ OSPF has to go through 7 states in order to become neighbors. :-

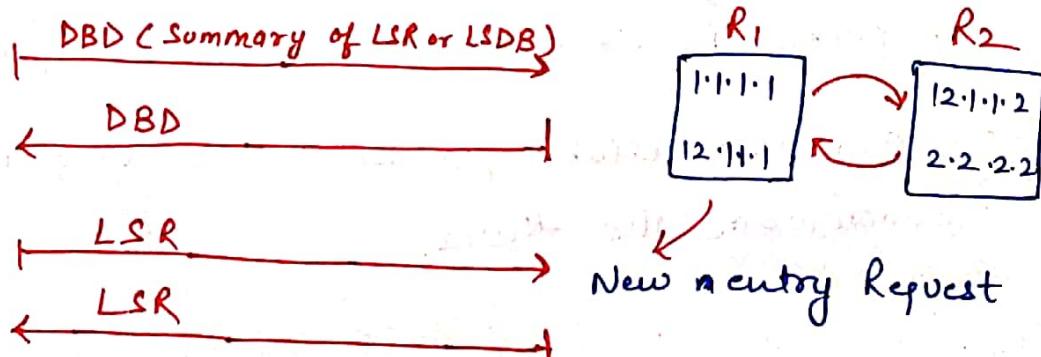
- ① Down: no ospf neighbors detected at this moment.
- ② Init: Hello packet received.
- ③ Two-way: Own router ID found in received Hello packet.
- ④ Ex start: Master & slave roles determined.
- ⑤ Exchange: Database description packets (DBD) are sent.
- ⑥ Loading: Exchange of LSRs (Link State Request) & LSUs (Link state update) packets.
- ⑦ Full: OSPF routers now have an adjacency.



\* if suppose R<sub>1</sub> does not send Hello packet the R<sub>2</sub> will hold last sent hello packet

hello timer = 10 sec  
dead timer = 40 sec

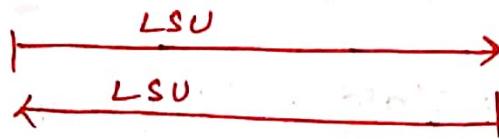
for 40 sec & if still not new hello packet received then R<sub>2</sub> will consider R<sub>1</sub> dead & neighborship will be lost.



20/12/2019

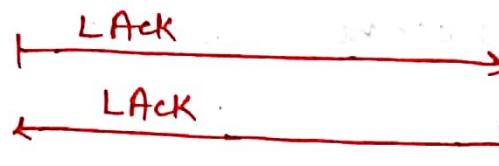
(5)

(4)



update regarding request  
will be sent

(5)



Ack for updates.

LSA → Link State Advertisement

↳ status of a particular link (Interface)

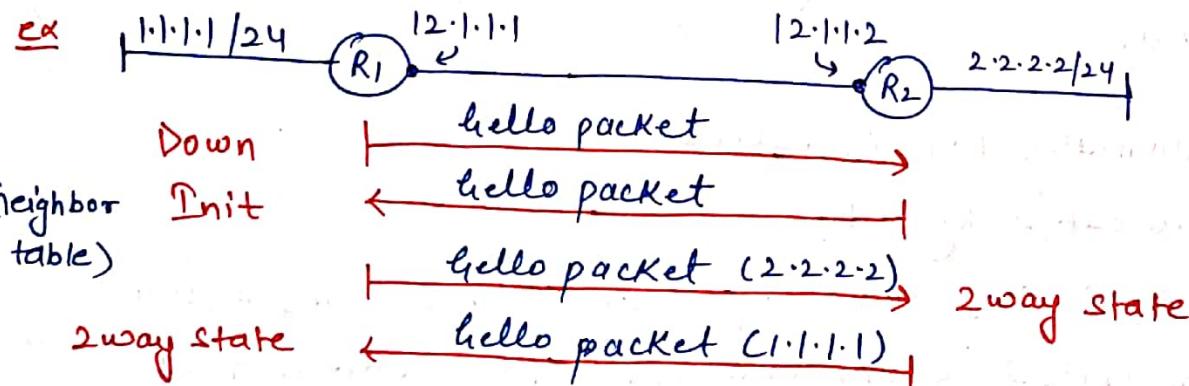
LSDB → Link state database

↳ Database of LSAs.

LSA timer = 30 minutes

= 1800 sec

LSA Dead timer = 60 minutes  
= 3600 sec

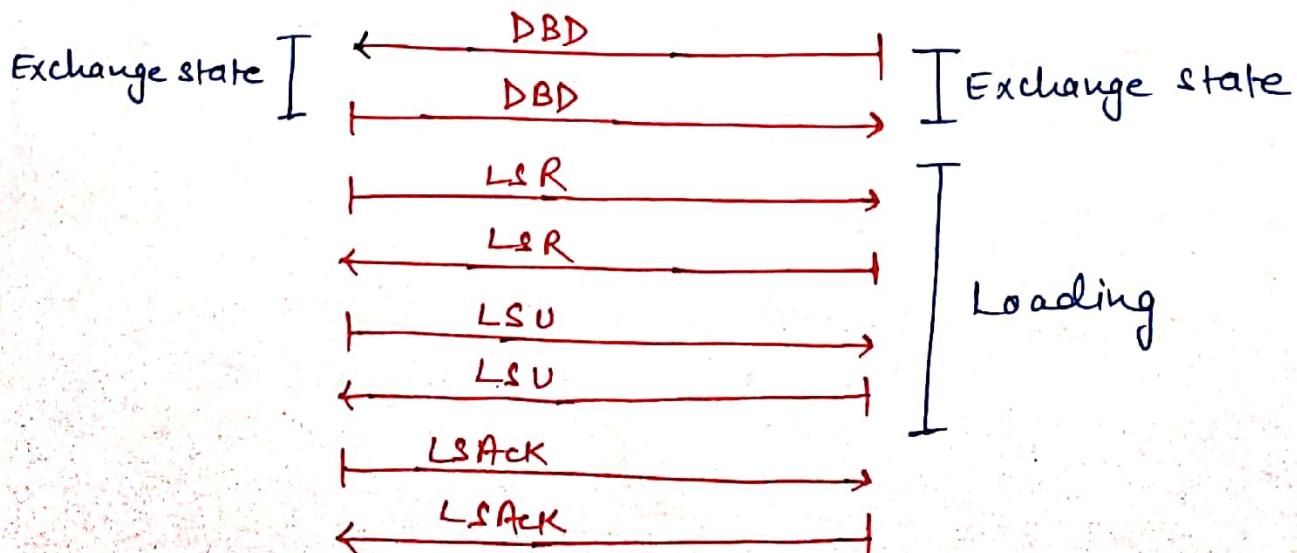


→ Router with lower ip

| Master & slave election | ex start state

Here R2

Router with higher id ↗



20/12/2019

\* Neighbor is just 2 way state of Adjacency is set up when DBD is exchanged b/w routers so both are different.

### ↳ Types of LSA :-

Total 11 but we will study only 3

LSA1 → (i) Router LSA is called LSA1

(ii) Router LSA is generated by every router that belongs to a area. LSA1 is limited within Area.

LSA2 → (i) N/W LSA is called LSA2.

(ii) LSA2 is generated by DR. LSA2 is also limited in a area.

LSA3 → (i) Summary LSA is called LSA3.

(ii) Generated by ABR

(iii) LSA1 & LSA2 are repackaged into LSA3 & then forwarded from one area to another Area.

## EIGRP (Enhanced Interior Gateway Routing Protocol)

- \* EIGRP is also called Advance distance Routing protocol and also hybrid routing Protocol
- \* EIGRP works on protocol no. 88
- \* EIGRP uses Dual algo. for best path calculation.
- \* Multicast address - 224.0.0.10
- \* Metric - Bandwidth, load, Delay, Reliability & MTU.
- \* Supports both equal & unequal cost load balancing.
- \* By default, EIGRP supports 100 hops but we can extend it up to 255.
- \* Classless Routing Protocol.
- # We will not find B.W, load, delay, written in EIGRP instead there are  $K_1, K_2, K_3, K_4$  &  $K_5$

$K_1$  = Bandwidth (1)

$K_2$  = load (0)

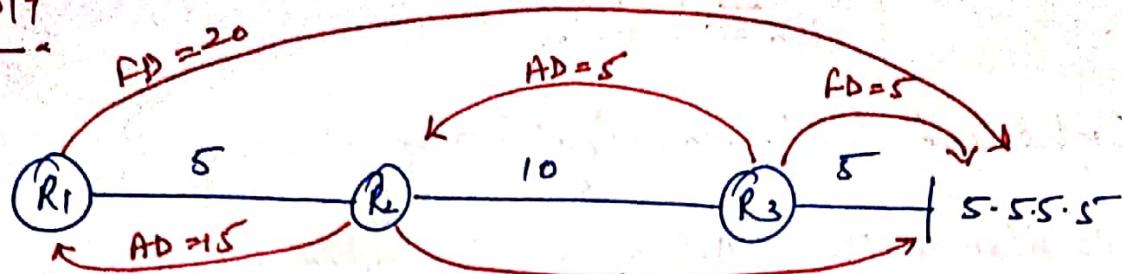
$K_3$  = Delay (1)

$K_4$  = Reliability (0)

$K_5$  = MTU (0)

→ Bandwidth & Delay are static value

→ load, MTU & Reliability are Dynamic value.



For  $R_3$   $AD = 5$  for  $5 \cdot 5 \cdot 5 \cdot 5$  n/w  $FD = 15$

if  $AD = 5$  will be advertised to  $R_2$

So for  $R_2$   $FD = 5 + 10 = 15$

if  $AD = 15$  will be advertised to  $R_1$

So for  $R_1$   $FD = 20$

Advertised Distance :- How far the dest is away for your neighbor.

Feasible distance :- The total distance to the destination.

# Backup path is called feasible successor.

# Best path to destination is called successor.

↳ Feasibility condition for a Backup path. ↴

$AD$  of feasible successor  $\leq$  Feasible distance of Successor.

↳ EIGRP maintains 3 Tables :-

① Neighbor Table → for neighbors entry

② Topology Table → for Best path and Backup path entry

③ Global Routing Table → only for Best path entry.

23/12/2019

## ↳ Syntax

```
Router(Config) # router-eigrp-As.no
    # no-auto-summary
    # Network Network — own n/w address
    #
    # Exit
```

As.no. (Autonomous System no.)

- ↳ 16 bit identity (1-65,535)
- ↳ Globally Known
- ↳ Group of Router controlled by single n/w admin.

cmd # show-ip-eigrp-neighbors

↳ To check Routing Table

cmd # show-ip-eigrp-topology

↳ To check topology tables.

P - Passive - Route is reachable & synchronized

A - Active - Unreachable & unsynchronized & actively finding its alternate path.

↳ # Hello timer → 5 sec

# Hold timer → 15 sec

1

## ↳ Metric Calculation :-

$$\text{Metric (cost)} = \left[ \frac{10^7}{\text{Slowest B.W along a path}} + \frac{\text{Cumulative Delay}}{10} \right] \times 256$$

Cumulative Delay :- Delay of (sum) every exit interface along a path.

B.W  $\rightarrow$  Bandwidth.

ex Metric = (i)  $\frac{10^7}{10^5} = 10^2$  (ii) Cumulative delay  
 $\downarrow$   $= 100$   $= \frac{300}{10} = 30$

BW checked By command

3 interfaces with 100 delay in each = 300

$$so \quad [100 + 30] = 130 \times 256 \\ = 33280$$

23/12/2019

cmd # show\_int\_serial 0/0/0

↳ to check B.W

However for serial link BW is 1.54 mbps & Delay is 20000 ~~usec~~

$$= \left[ \frac{10^7}{1544} + \frac{20000 + 100 + 100}{10} \right] \times 256$$

$$= \left[ \frac{10^7}{1544} + 2020 \right] \times 256$$

$$= [6476 + 2020] \times 256 = 2172416 \text{ Ar.}$$

ex

$$= \left[ \frac{10^7}{10^5} + \frac{200}{10} \right] \times 256$$

$$= [100 + 20] \times 256$$

$$= 30720$$

## ↳ Distance Vector :-

How far away  
is your Post"

Direction  
(Exit Interface)

totally

- \* This type of routing is <sup>totally</sup> dependent ~~on~~ neighboring router updates only & does not know about topology beyond neighbor
- \* In contrast <sup>in</sup> the link state routing protocol router is aware of the topology like how it looks. (Map).

24/12/2019

(2)

## ↳ ACL (Access Control List)

→ A feature available on ios that limits (controls) incoming and outgoing traffic in a network.

### ↳ Types of ACL :-

#### ① Numbered ACL

→ ④ Standard ACL

→ ⑥ Extended ACL

#### ② Named ACL

→ ④ Standard ACL

→ ⑥ Extended ACL

\* Numbered ACL is identified on the basis of Numbers.

\* Named ACL is identified on the basis of Names.

~~st. ACL~~ :- Numbers Ranging from (1-99, 1300-1999)

→ Filters traffic on the basis of Source ip address.

→ Applied Near to the Destination.

→ Only one ACL can be applied on the Interface and per direction.

Ext ACL :- Numbers Ranging from 100 -199, 2000 - 2699

→ Filters traffic on the basis of both source and destination ip address and also on the basis of port no. (TCP/UDP/ICMP/HTTP)

24/12/2019

\* Basically Ext ACL filters L3 & L4 traffic.

→ Applied Near to the Source.

→ Only one Access list can be applied on an interface and per direction.

# Everything is same in Named ACL just names are used in place of numbers.

cmd # Access-list -1 - deny - host - ip

↳ to deny any host

(But we can deny any n/w also)

(check help?)

cmd # Access-list -1 - permit - any

cmd # int - f0/0

↳ to allow any n/w except ↗

# ip-access-group -1 - out/in

# exit

↳ Based on incoming / Outgoing interface.

cmd # show - access-lists

↳ to check access list (deny/allow)  
hit count

cmd # no - access-list -1

↳ to delete access list

\* 24/12/2019

(4)

cmd# access-list -1 - deny - 192.168.1.0 - 0.0.0.255  
# access-list -1 - permit - any  
# int - f0/0  
# ip - access - group - 1 - out

↓  
we use wildcarded  
mask to block any  
subnet.

## ↳ Loopback Interface

cmd# int - loopback - 0  
# ip - add - 2.2.2.2 - 255.255.255.0  
# exit

- \* By default up
- \* Different Subnet is required.

① 30/12/2019

LECTURE - 22

## ↳ EXTENDED ACCESS LIST

statement

- \* By default implicit deny is enabled in Access List i.e it blocks all traffic

cmd # access-list\_100\_permit\_icmp\_host\_192.168.1.3\_host\_192.168.3.3

# access-list-100-deny-ip-any-any  
Source Destination

cmd# Router (config) # int\_f0/0

# ip-access-group=100-in

cmd# Router# show-access-lists

- \* We can also block service based traffic in the Access list.

cmd# access-list-100\_permit\_tcp\_host\_192.168.1.3\_host\_192.168.3.3

eg - 80  
↓

to indicate the http protocol

cmd# access-list-100\_permit\_udp\_host\_192.168.1.3\_host\_192.168.3.3

eg 53  
↓

To ~~block~~ due service.  
allow

## → NAT (Network Address Translation)

\* Main function of NAT is to enable private IP address networks to connect to the Internet. NAT replaces a private IP address with a Public IP address, translating the private address in the internal private n/w into legal, Routable addresses that can be used on the public Internet.

### → NAT Types :-

- ① Static NAT (Manual NAT)
- ② Dynamic NAT
- ③ NAT- PAT

### → Static NAT :-

- One to One Mapping
- Used for Servers.
- Permanent Entry in NAT Table.
- Static NAT initiates bidirectional flow.

Ex

192.168.1.2 — 12.1.1.1



Permanent Entry in NAT Table

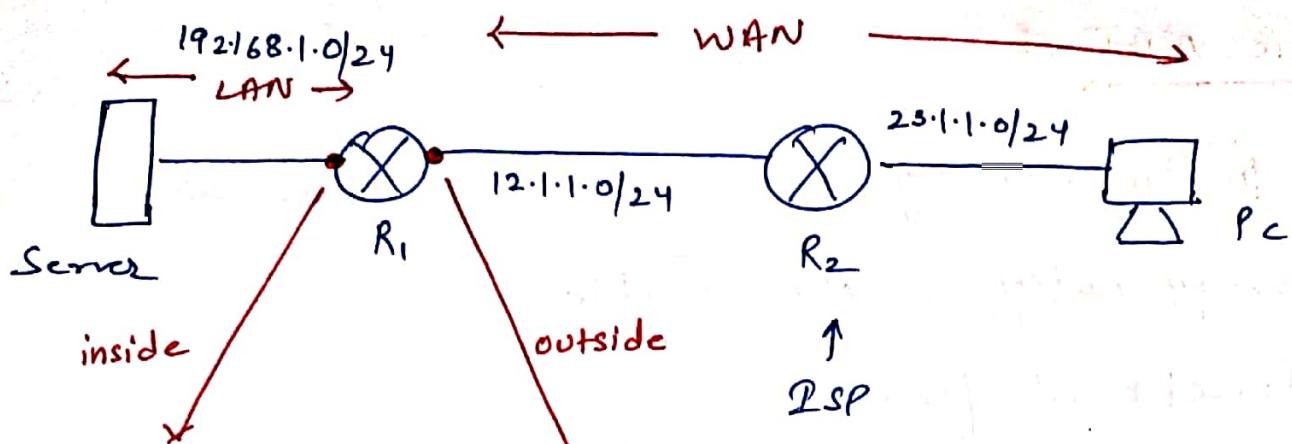


Bidirectional flow.

①

31/12/2019

LECTURE-23



# Int-f0/0

# ip-nat-inside

# ex

# Int-Sec0/0/0

# ip-nat-outside

# ex

# ip-nat-inside-source-static - 192.168.1.2 - 12.1.1.10

\* Nat applied above is on the inside interface which will convert private ip to public ip.

\* On the outside interface the rule gets applied automatically i.e. public to private conversion / translation would be done automatically.

# show-ip-nat-translation

↳ to check NAT Table

# debug-ip-nat

↳ to enable debugging & see each conversion / command one by one.

31/12/2019

(2)

## ↳ Dynamic NAT :-

- ① One to One mapping
- ② Temporary entry in NAT Table.
- ③ Unidirectional flow
- ④ Used for end user

\* Not used nowadays, because suppose 10 user/pc want to access internet then 10 public ip would be required.

- \* We need Access list in dynamic NAT as to identify the internal/private network.
- ① We need to define <sup>nat</sup> ip pool to define public ip range
- ③ Define NAT rule and integrate ACL and ip pool.

### Commands:-

```
# Int_Fo/o  
# ip-nat-inside }  
# ex  
  
# Int_Se0/0/0  
# ip-nat-outside }  
# ex
```

31/12/2019

(3)

# Access-list-1 permit 192.168.1.0 - 0.0.0.255 } (2) ACL

# ip-nat-pool-guftgu-12.1.1.10 - 12.1.1.11 network 255.255.255.0 } (3) pool

# ip-nat-inside-source-list-1 - pool-guftgu } (4) integration

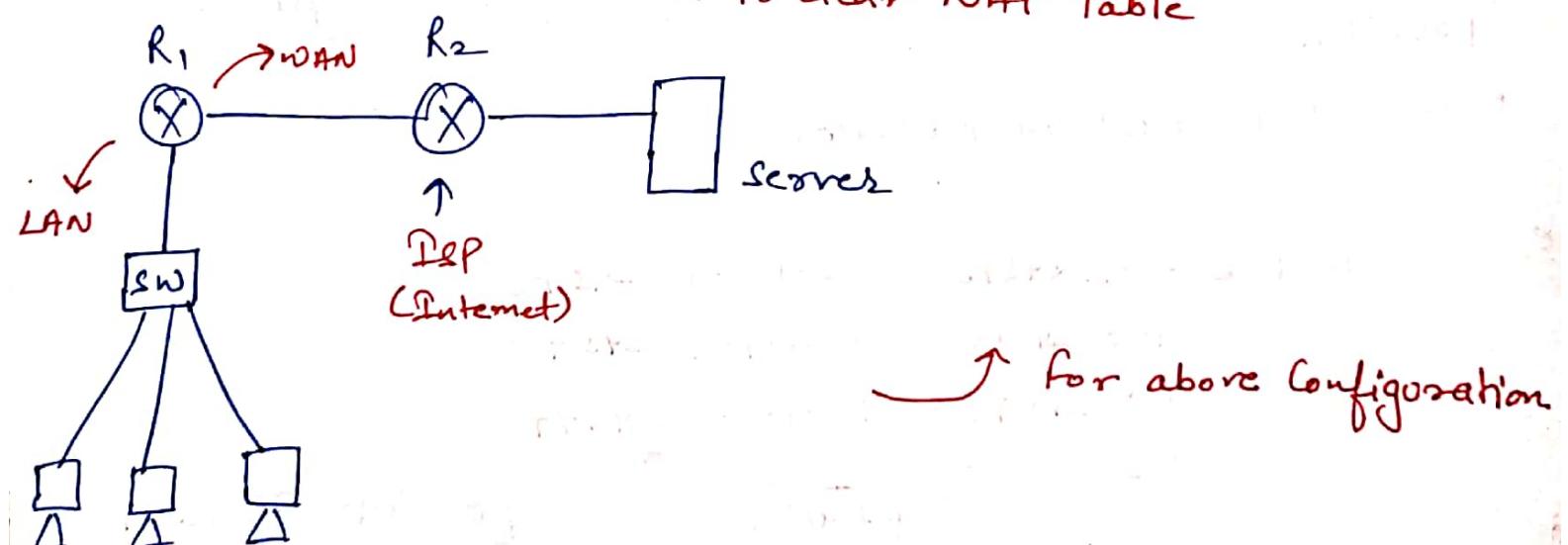
# Show-ip-nat-translation

↳ to check NAT Table

\* Data is saved in table when translation is done or we can say request is made.

# Clear-ip-nat-translation

↳ to clear NAT Table

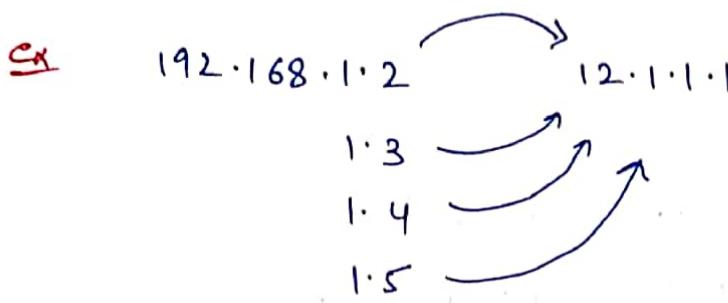


31/12/2019

④

↳ NAT - PAT (Port Address Translation).

- ① Used for end users
- ② Unidirectional flow.
- ③ Temporary entry in NAT Table.
- ④ One to many NAT



\* If we bind this single public ip with each private ip then the traffic which 12.1.1.1 will bring would be different to decide that which ip it is for so we have NAT-PAT in Rescue.

Ex

192.168.1.2	24576	12.1.1.1	24576
1.3	24598	12.1.1.1	24598
1.4	24576	12.1.1.1	24999
1.5			

Translation.

86999 86939

\* So in NAT-PAT Port no. is attached with ip & when the traffic is brought by public ip then it can be easily identified that which ip it is for.

\* Port no. is random & if it matches for any ip then port no. is also translated like in ip 1.4

31/12/2019

5

# int\_folo

# ip-nat\_inside

# ex

# int-sc/01010

# ip-nat-outside

# ex

```
# access-list -1 -permit - 192.168.1.0 - 0.0.0.255
```

# ip nat pool null\_admin\_ 12.1.1.1-12.1.1.1 netmask 255.255.255.0

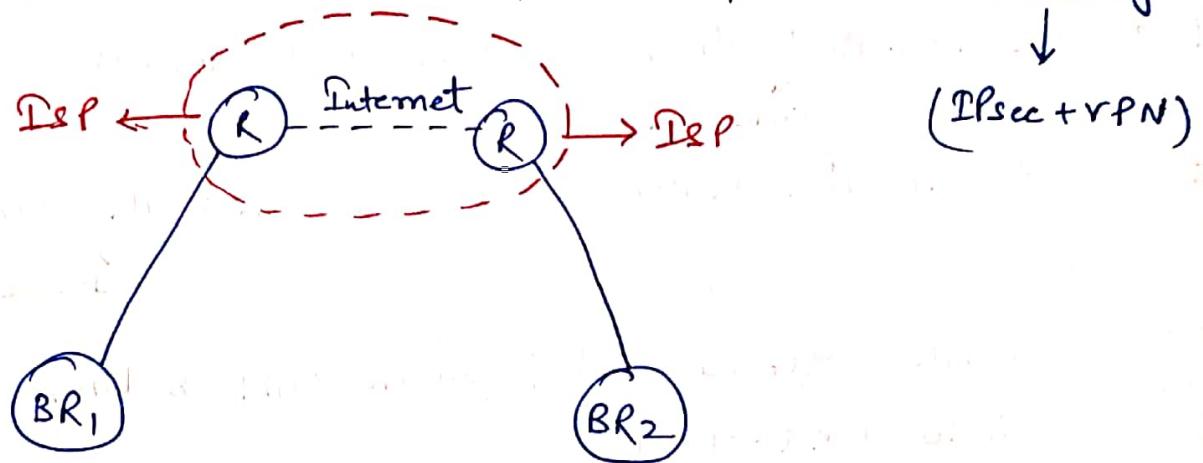
# ip-nat-inside-source-list-1-pool-null-admin-overload  
↓  
undersrc  
↓

with overload and dynamic NAT behaviour connects into NAT-PAT

## GRE TUNNEL

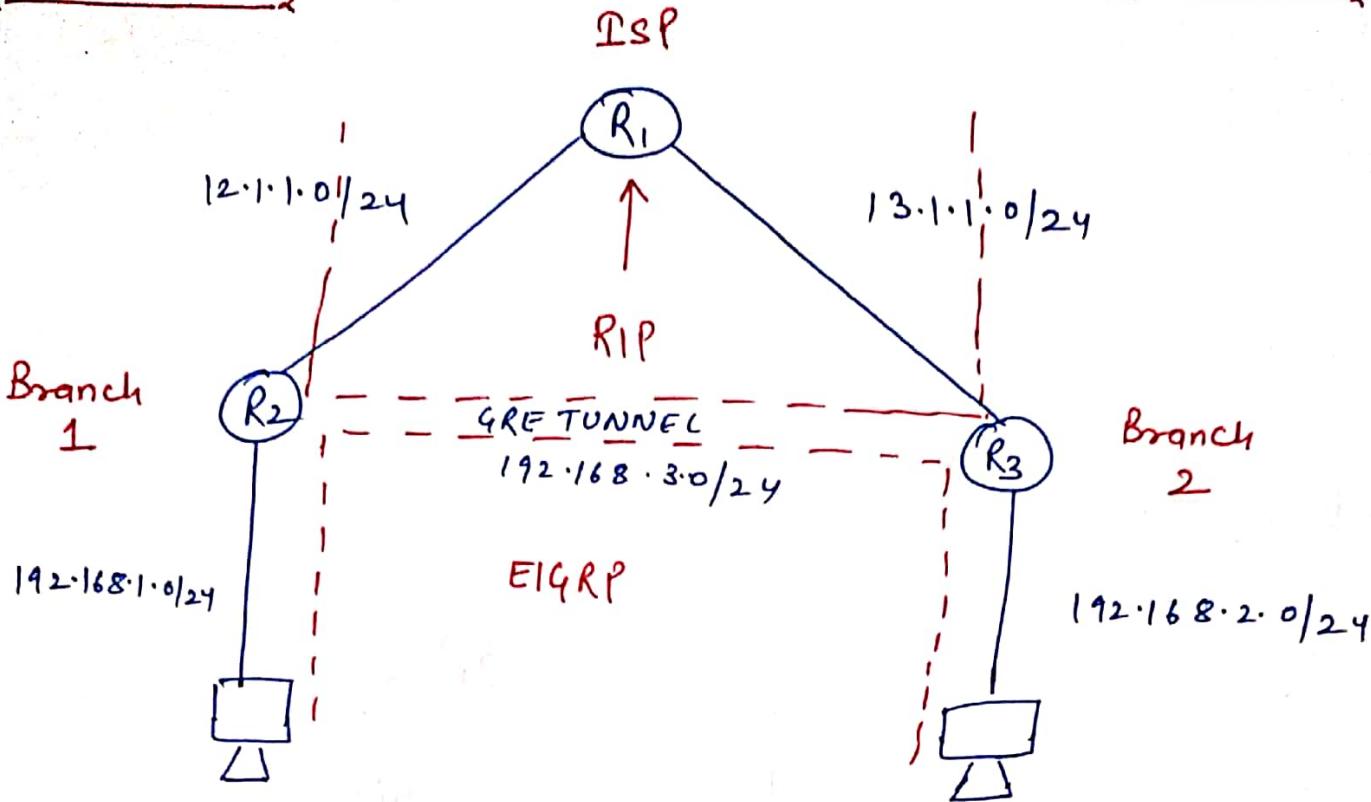
- ① L-3 Protocol
- ② Works on protocol no. ~~46~~ 47
- ③ GRE adds 24 bytes of extra overhead to the original ~~header~~ packet.

VPN :- logical channel over public n/w [Not Security]



\* Earlier Physical link was used b/w Branches which was costly & required high maintenance but now we use VPN :- connecting two or more branch offices over a public n/w.

\* Connected virtually but seems like connected directly.



\* Tunnel n/w interfaces also will be advertised in EIGRP

R<sub>2</sub> # interface - tunnel\_0

# ip - address - 192.168.3.1 - 255.255.255.0

# tunnel - Source - Serial 0/0/0

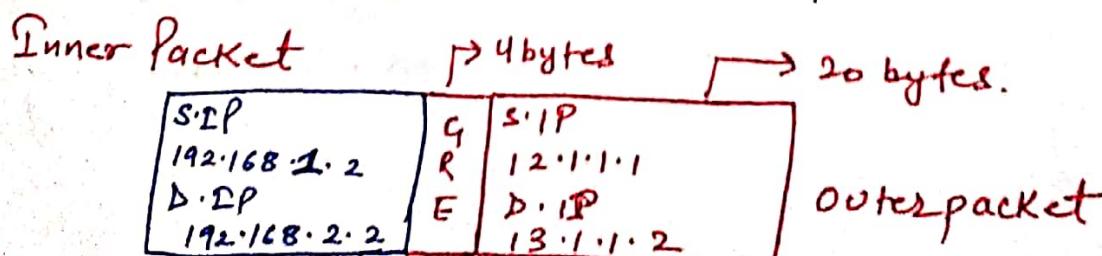
# tunnel - Destination - 13.1.1.2

# exit.

→ In config we use int no.  
→ In real device use IP only for source also

R<sub>3</sub> # Same as R<sub>2</sub> & just change

ip, source & destination as per network.



## ↳ IPv4 - :

### IPv4

- ① 32 bit
- ② written in Decimal format
- ③ 4 Octet (8 bit each)
- ④ Octet are separated with dot (.)
- ⑤ five classes  
A, B, C, D, E
- ⑥ Has N/w bits & host bits according classes
- ⑦ It uses subnet mask

### IPv6

- ① 128 bit
- ② written in hexadecimal format
- ③ 8 groups (each 16 bit)
- ④ groups are separated with colon (:)
- ⑤ No classes
- ⑥ It has mostly fixed N/w bits (64 bits) & Host bits (64 bits)
- ⑦ It does not use subnet mask. It uses prefix

## ↳ Benefits of IPv6

- ① Large no. of IP address
- ② Simplified Header (Fix Header length = 40 bytes).
- ③ Extension Header
- ④ Fragmentation & Security is applied implemented by Extension header.
- ⑤ Broadcast is not available
- ⑥ Anycast is introduced.

Ex: 2001: 0DB8: AC10: FE01: 0000: 0000: 0000: 0000  
                16 bit

1 hex = 4 bit

4 hex = 16 bit (1 group)

8 group  $\times$  16 bit = 128 bit

\* Good Explanation is given in How to master CCNA.

\* OSPF & EIGRP support IPv6 but those are separate protocols. If you have a n/w with IPv4 & IPv6 you will run a routing protocol for IPv4 & another one for IPv6.

Running IPv4 & IPv6 at the same time is called over stack.

01/01/2020

④ Original : 2041: 0000: 140F: 0000: 0000: 0000: 875B: 131B

Short : 2041: 0000: 140F: ! 875B: 131B

Shorter : 2041: 0: 140F: ! 875B: 131B

Another way

Original : 2001: 0001: 0002: 0003: 0004: 0005: 0006: 0007

Short : 2001: 1: 2: 3: 4: 5: 6: 7

So the Rules were :

① A string of zeroes can be removed leaving only a colon(:)

You can only do this once.

② 4 zeroes can be removed leaving only a single zero.

③ leading zeroes can be removed within a block.

\* In IPv6 we use prefix length in place of CIDR

ex

2001: 1234: 5678: 1234 : 2001: 1234: 5678: 1234  
Prefix host id / interface id

So, 2001: 1234: 5678: 1234: 2001: 1234: 5678: 1234 / 64

(5)

↳ Some of the Prefixes are reserved :-

① 2000::/3 - Global Unicast

② FD : Unique local → if ip starts with this it would be

③ FF : Multicast

④ FE80 : Link local

\* Global Unicast is just like public IP & Unique local is just like private IP.

Cmd # Int-f0/0

# no-shut

# IPv6-add-2001::2/64

# exit

\* For IP use IPv6 everywhere for IPv6

# show-ipv6-int-brief

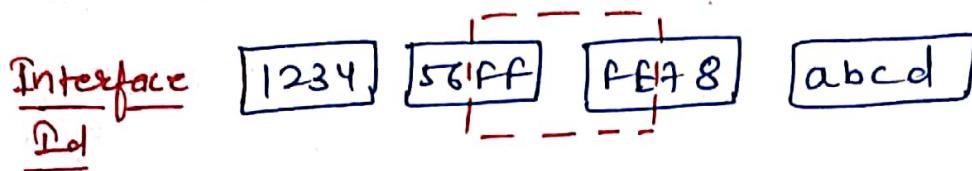
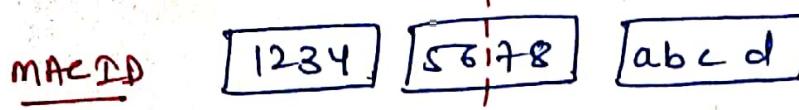
↳ EUI 64 (Extended Unique Identifier)

\* It is used to configure id as it can be used to make the router generate its own interface id instead of typing 128 bit complete ip ourselves. [it generates interface id of fix length 64 bit]

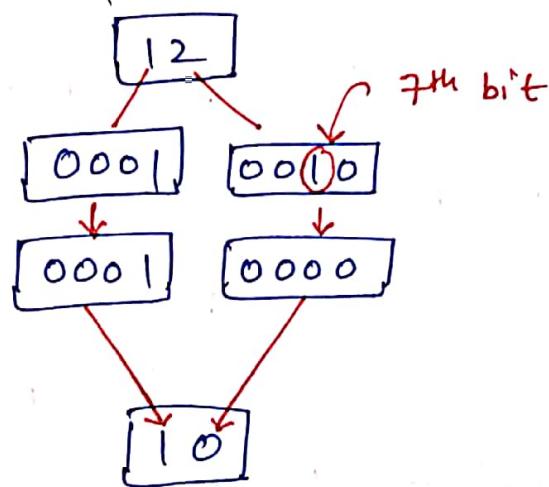
\* It generates ip with the help of MAC id but MAC id is of 48 bits & ip interface id is of 64 bits so we do the following for remaining 16 bits

01/01/2020

(6)



Now we invert the 7<sup>th</sup> bit from starting in the interface Id.



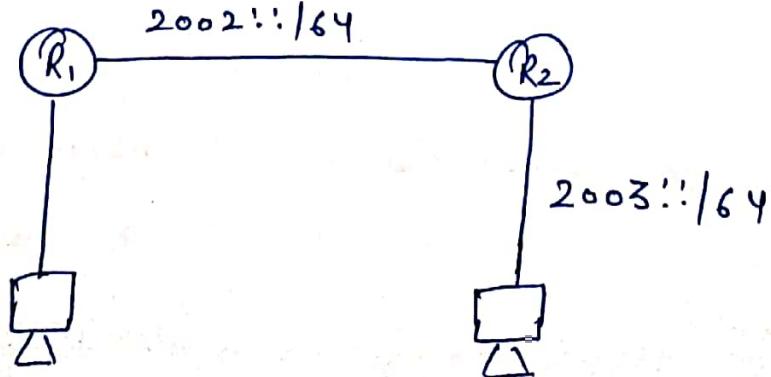
So we did following steps :-

- ① We take the MAC address & split it into two pieces
- ② We insert FFFE in b/w the two pieces so that we have a 64 bit value
- ③ We invert the 7<sup>th</sup> bit of the interface Id.

cmd # int\_folo  
# no\_shut  
# ipv6\_add\_2000::/64-cvi 64  
# exit

- \* Each device that has IPv6 enabled will automatically generate a link local address. These addresses are unicast can't be routed and are only used with Subnet, which is why they are called link-local.
- \* A no. of protocols use the link local addresses instead of the global unicast addresses, a good example is NDP (Neighbor Discovery protocol) which is used to discover the MAC addresses of other IPv6 devices in the Subnet (NDP replaces ARP for IPv4)
- \* Routing protocols also use these link local addresses to establish neighbor adjacencies and also as the next hop for routes.
- \* Multicast address - EIGRP uses ff02::1 & OSPF uses ff02::5 & ff02::6.

ex for  
Default/static  
Routing: 2001::/64



- \* Routing Command are exactly same just use IPv6 instead of IP & by default Router does not maintain routing table for IPv6 so we use an extra command.

### #. IPv6\_unicast-routing

→ for dynamic Routing :-

- \* We used to advertise networks with Network commands in IPv4 but in IPv6 we enable network on the interface itself
- \* Also we need to give router id manually in IPv6.

R1# IPv6\_unicast-routing

# IPv6-router ospf-1

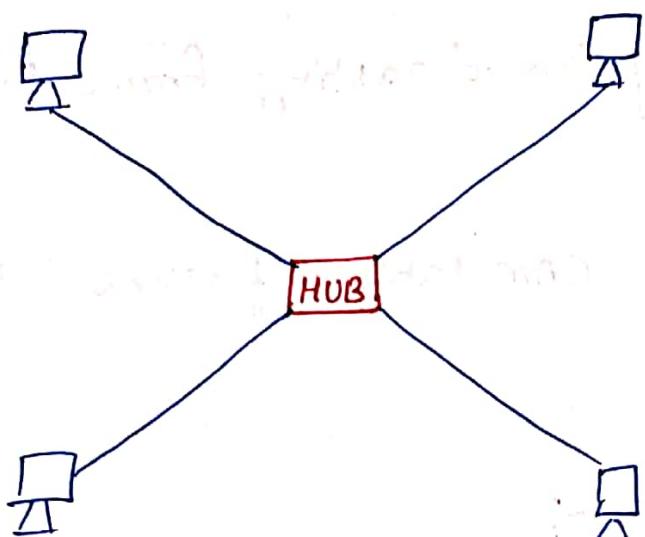
# router-id 2.2.2.2

# int\_f0/0

# IPv6\_ospf-1\_area\_0

→ Same for other interfaces & other routers.

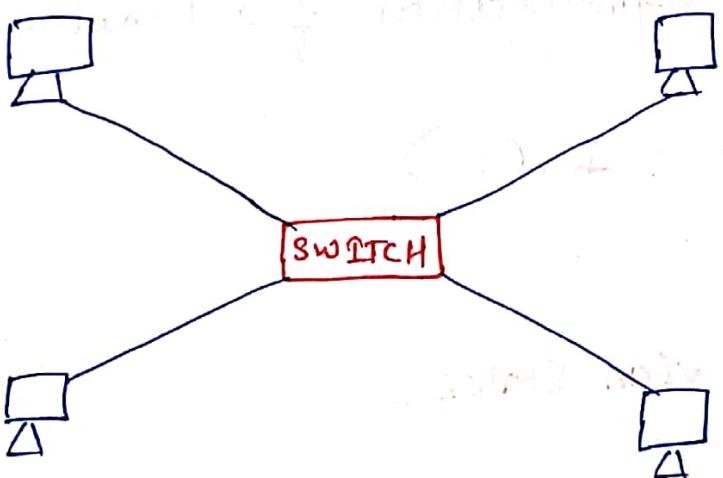
## SWITCHING :-

ex

① Single collision domain  
② Broadcast device

③ Layer 1 device

④ CSMA/CD is used to avoid collision based on clock timing.

ex

Switch :- \* It is a layer 2 device.

- \* It takes forwarding decision on the basis of CAM table (Content Addressable Memory).
- \* CAM table maintains the database of MAC address, port id, VLAN id etc.
- \* So basically it's a smarter device as compared to HUB.

02/01/2020

(4)

# show - mac\_address\_table

↳ to show mac address table

- \* After resolving ARP by broad casting frame Switch shows unicast behaviour.
- \* After every 5 minutes CAM table refreshes & if remain idle then deleted.

↳ VLAN (Virtual Lan) :-

\* VLAN is a virtual segmentation of a broadcast domain.

(1 Broadcast domain = 1 VLAN)

# show\_vlan

↳ to check VLAN status.

→ Why we need VLAN?

- ① Broadcast Control
- ② Security - logically separates users & departments, allowing administrators to implement access-list to control traffic b/w VLANs.
- ③ Flexibility - removes the physical boundary of a network, allowing a user or device to exist anywhere

③

## ↳ VLAN Ranges :-

### ① Standard VLAN Range :-

Range from 1 - 1005

(Standard VLAN Range)

### ② Extended VLAN Range :-

Range from 1006 - 4094

cmd # Conf-t

```
# vlan - 10      (VLAN no. from 1-4094)
# name - hr    (name for VLAN)
# exit
```

To give VLAN a name & create VLAN

cmd # int\_f0/1

```
# switchport_access_vlan - 10
# exit
```

To assign port to VLAN.

\* Interfaces can be assigned in individual, in groups with random no. or in ranges.  
(1,10,12 etc)                          (ex 1-10).

cmd # int\_range\_fastEthernet - 0/2-10

```
# switchport_access_vlan - 10
# exit.
```

Assigning interfaces in ranges.

02/01/2020

⑥

cmd # int-range - fa0/12, fa0/15, fa0/18

# switchport-access-vlan - 21

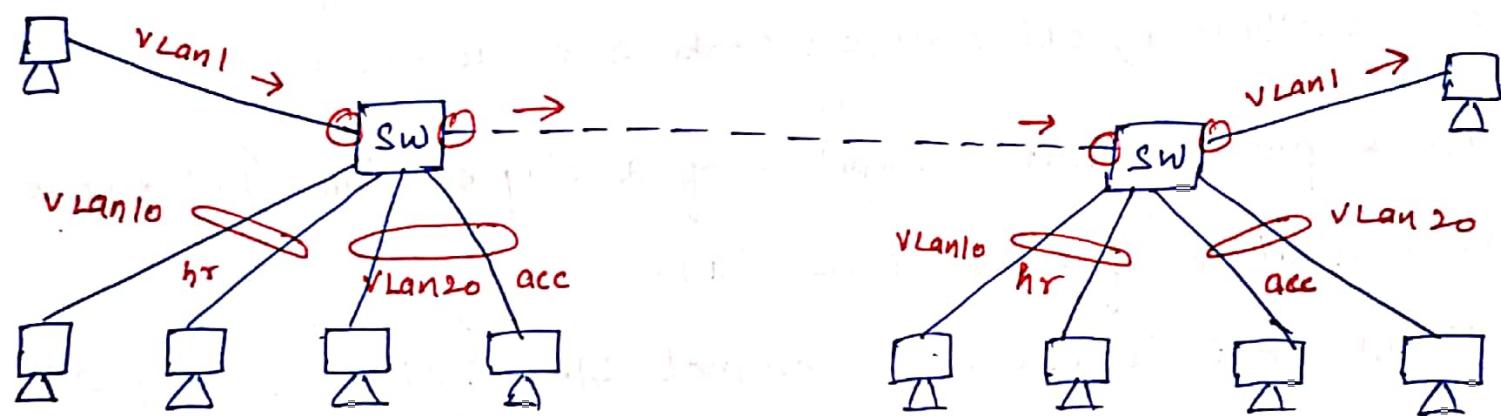
# exit

→ if we write 21 instead of 1  
then it will see that no  
vlan 21 exist so it will create  
one.

# ① LECTURE-26

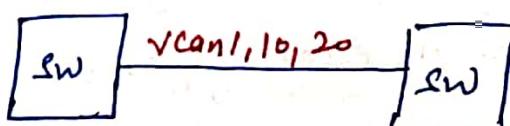
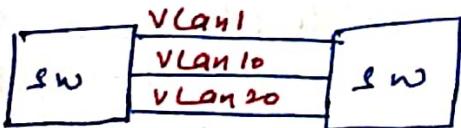
03/01/2020

- \* Different vlan should have different network, we can give same but then it would not be differentiated while communicating b/w different vlan.
- \* By default we can communicate ~~b/w~~ in intra vlan (Same vlan) only.
- \* We would be needing routing or L3 switch to communicate b/w different vlan.



\* Vlan1 will ping Vlan1 on other switch as Broadcast domain is same & frame will travel through link.

But in case of other vlan ping will not work as the Broadcast domain will be different. So how to make it happen we have two methods.



So either we can connect port for diff vlan with diff media but not practically feasible

So we use only one media & ~~connect separate~~ for vlan group.

## Port

↳ Vlan Types :-

- ① Access port
- ② Trunk port

① An access port is a member of only a single vlan.

Access ports are most often used to connect host devices. Such as computers and printers. By default on Cisco switches, all switch ports are access ports.

② Trunk port is not a member of a single vlan. Trunk port is a member of a multiple vlan.

Trunk port is used to connect b/w switches & b/w switch & router.

(Sw to Sw)

↳ Vlan Frame - Tagging :-

\* When vlangs span multiple switches, a mechanism is required to identify which vlan a frame belongs to. This is accomplished through frame tagging, which places a vlan id in each frame.

\* Tagging only occurs when a frame is sent out on trunk port.

(8)

## Frame Tagging Protocols :-

① Inter-Switch Link (ISL)

② IEEE 802.1Q

① ISL encapsulates a frame with an additional header (26 bytes) and trailer (4 bytes). Thus, ISL increases the size of a frame by 30 bytes.

\* ISL increases the frame size by another 30 bytes. Thus, most switches will disregard ISL-tagged frames as being oversized & drop the frame.

\* ISL is also almost entirely deprecated - most modern Cisco switches no longer support it.

② IEEE 802.1Q or referred to as dot1Q is an industry-standard frame-tagging protocol.

\* 802.1Q is supported by nearly all switch manufacturers, including Cisco.

\* 802.1Q embeds a 4 byte VLAN tag directly into the Layer 2 frame header.

Imp\* Both sides of the trunk must be configured with the same tagging protocol. Otherwise, a trunk connection will not form.

If the switch only supports 802.1Q, the switchport trunk encapsulation command will not be available.

03/01/2020

↳ Configuring interface as a trunk:

```
# int_f0/6
```

```
# switchport_trunk_encapsulation_dot1q
```

```
# switchport_mode_trunk
```

Switch - 2960  
2950 } L2 Switch

(any switch of series above 3000  
all are L3 switch.)

SW - 3750  
3850  
3560  
3850  
6500  
6800 }  
4 L3 Switch

```
# show_int_f0/6_switchport
```

↳ to check trunk/access port.

↳ Inter Vlan Routing (IVR)

R - Router on a stick (if routing is done with the help of router)

S - Switching virtual Interface. (if done on switch).

Router # int\_f0/0  
cmd

```
# no_shwt
```

```
# ex.
```

```
# int_f0/0.1 (for vlan 1) subinterface.
```

```
# encapsulation_dot1q
```

```
# ip_addr_192.168.1.3_255.255.255.0
```

```
# ex.
```

03/01/2020

(8)

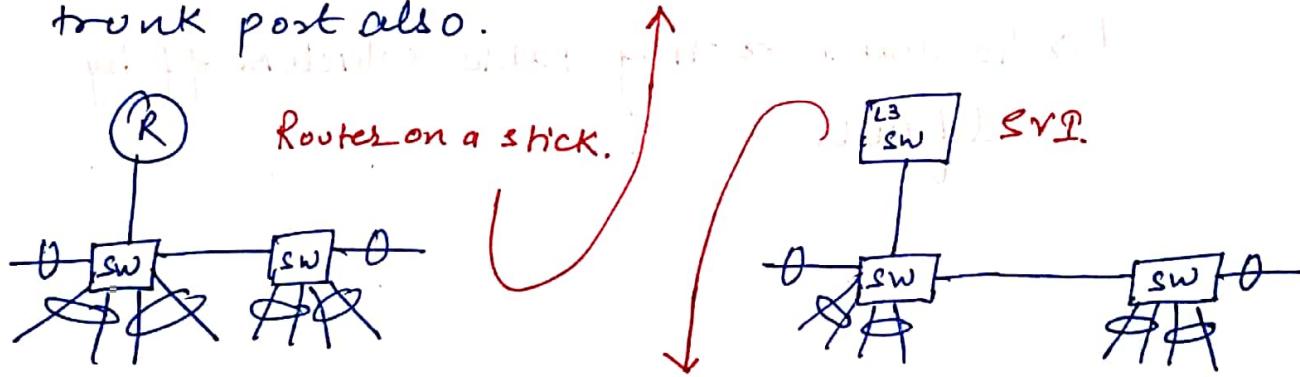
```
# int_f0/0.10 (for vLan10) Subnet int
# encapsulation_dot1Q_10
# ip_addr_192.168.10.10_255.255.255.0
# ex
```

(\* If add gateway to router interface will be a gateway)

```
# int_f0/0.20 (for vLan20) Sub interface.
```

```
# encapsulation_dot1Q_20
# ip_addr_192.168.20.10_255.255.255.0
# ex.
```

\* Interface of switch connected to Router has to be made trunk port also.



Switch cmd # vLan\_10

[vLan1 created by default]

```
# ex
```

```
# vLan_20
```

```
# ex
```

```
# int_f0/1
```

```
# switchport_trunk_encapsulation_dot1Q
```

```
# switchport_mode_trunk
```

```
# ex
```

```
# int_vLan1
```

{ shut by default for security purpose }

```
# no_shut
```

03/01/2020

# ip - add - 192.168.1.3 - 255.255.255.0

# ex.

# int - vlan10 (for vlan10)

# ip - add - 192.168.10.10 - 255.255.255.0

# ex.

# int - vlan 20 (for vlan20).

# ip - add - 192.168.20.10 - 255.255.255.0

# ex.

# ip - routing

↳ To enable routing table which is off by default.

- \* Trunk port can be made manually by `vlan` command & the other method would be automatically with the help of DTP.

### ↳ DTP (Dynamic Trunking Protocol) :-

- \* Trunk's frame tagging protocol can be autonegotiated, through the use of the Dynamic Trunking Protocol (DTP).
- \* DTP can also negotiate whether a port becomes a trunk at all.
- \* Trunk ports send out DTP frames every 30 seconds to indicate their configured mode.
- \* A Trunk will form in the following configuration:

Manual trunk  $\leftrightarrow$  Manual trunk

Manual trunk  $\leftrightarrow$  Dynamic Desirable

Manual trunk  $\leftrightarrow$  Dynamic auto

Dynamic desirable  $\leftrightarrow$  Dynamic Desirable

Dynamic desirable  $\leftrightarrow$  dynamic auto

- \* A trunk will never form if the two sides of the trunk are set to dynamic auto, as both port are waiting for the other to initialize the trunk.

- \* It is best practice to ~~not~~ manually configure trunk ports to avoid DTP.

06/11/2020

(2)

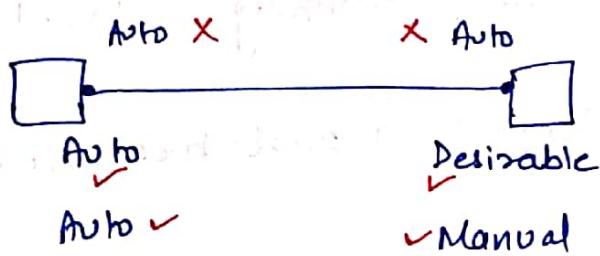
→ negotiation error. DTP is also vulnerable to VLAN spoofing attacks.

\* Switchport mode trunk → send & receive DTP packets.

Desirable → ↑

Auto → Only detects DTP Packets.

Access → Doesn't understand DTP Packets.



Cmd # int -f -0/1

← interface connecting to end host.

# switchport access vlan 10

# switchport mode access

# exit

\* Switch ↔ end device (Access port)

Switch ↔ Switch (Trunk port).

# int -f -0/2 → Interface connecting to switch.

# switchport\_trunk\_encapsulation - Dot1Q

# switchport\_mode\_trunk

# switchport\_nonegotiate → to turn off DTP packets

# ex.

08/11/2020

(3)

## ↳ VTP ( VLAN Trunking Protocol )

- ① Cisco proprietary protocol
- ② By default, enabled on Cisco switches
- ③ L-2 protocol

\* VLAN Trunk protocol reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain.

## ↳ VTP Modes :-

### ① VTP Server :-

- ① Allowed to create and delete VLAN.
- ② VTP Server, distributes VLAN database from one switch to another switch in a domain.

### ② VTP Transparent :-

- ① Allowed to create & delete VLAN.
- ② It maintains its own local database. → 

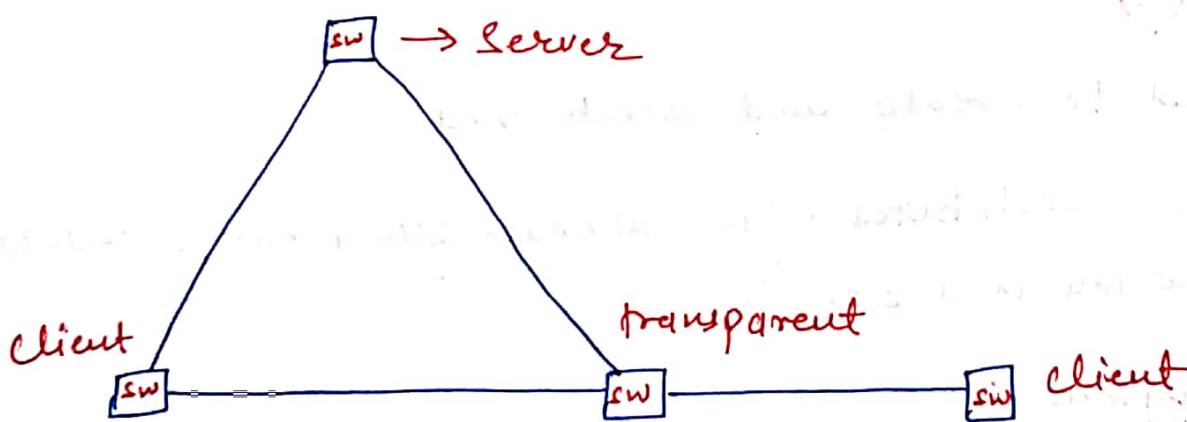
Avoid flooding of data from one SW to other SW
- ③ Acts as a transparent switch, when it receives VLAN database from VTP server and forward to the other switch in a domain.

### ⑧ VTP Client :-

- ① Not allowed to create & delete VLAN.
- ② It forwards its VLAN database to other switch in a domain.

### ↳ VTP Versions :-

- ① VTP version 1
  - 1 } Only supports standard VLAN range  
C1-1005
  - 2 }
  - 3 } Supports both extended & standard  
VLAN range (1-4094).
- ② Supports only limited hardware. (Switch).



\* By default VTP is enabled on switch & is by default on server mode

# `show vtp status`

↳ To check status.

08/01/2020

cmd (Server) # conf-t

# vtp-domain-abc.com

# vtp-mode-server / transparent / client.

(By default all switch are in server mode).

\* We must take care of Revision Number.

# show-vtp-status

↳ It will show Configuration Revision no.

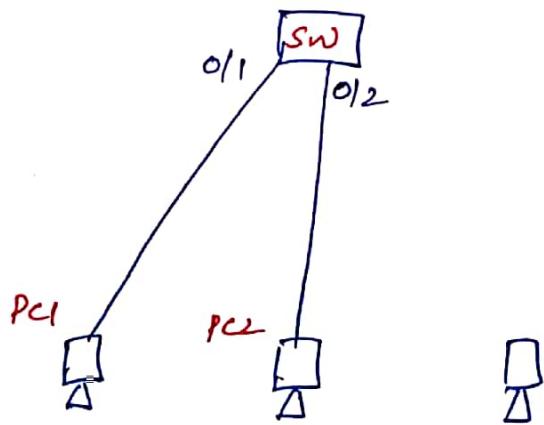
↳ How to Reset Revision No.?

# change your mode to transparent (Preferred).

# change your domain name.

## Port Security :-

- ① L-2 Security feature.
- ② Used to allow limited no. of MAC-address on a interface (MAC-Binding).
- ③ By default disabled on Cisco switches.
- ④ Protect switched nets from MAC flooding attack.
- \* Port security is always enabled on the port <sup>to which</sup> of your end device. is connected.



(two mac-address allowed in table)

```

# int - F_0/2
# switchport - port-security-maximum - 2
# switchport - port-security - mac-address - sticky (Automatically)
# switch - port-security - violation - protect / restrict
               / shutdown
               / default
  
```

Seek help for each?)

\* Do wr after sticky as it is stored in NVRAM.

06/01/2020

(7)

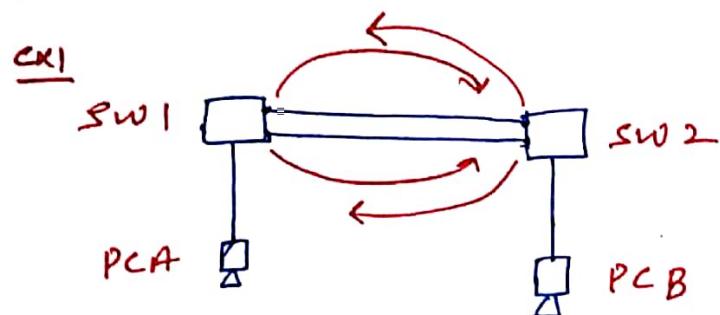
Cmd# Show - port - Security

# show - port - Security - int - Fo/2

\* Error Disabled state.

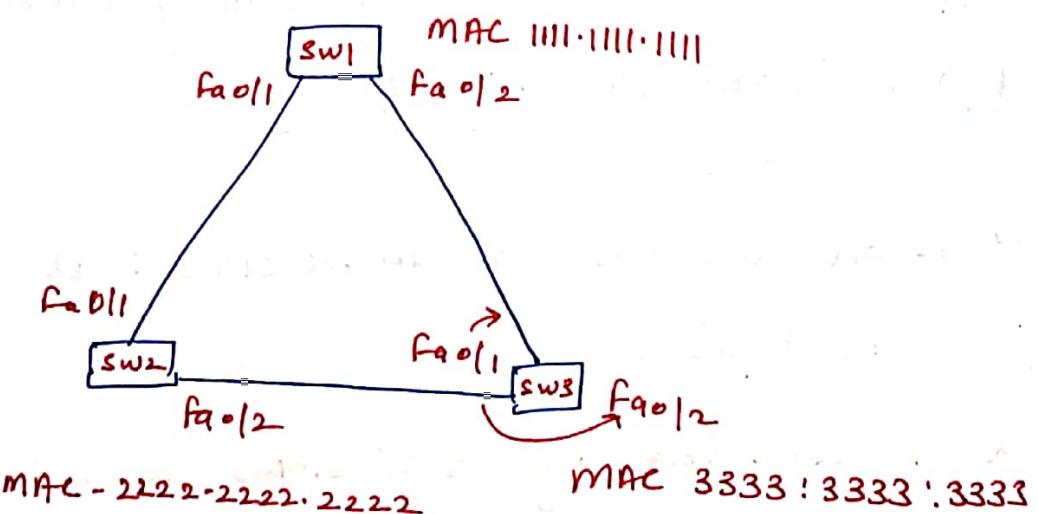
## SPANNING TREE PROTOCOL (STP)

- ① L-2 Protocol
- ② By Default, enabled on Cisco switches.
- ③ used to prevent (avoid) loop in switched n/w.



\* To overcome the problem of single point of failure, we bring redundancy in our switched n/w & redundancy brings loop in our switched n/w.

ex2



07/01/2020

## STP Calculation (Working)

Step 1 : Root Bridge (switch)



Best Bridge id



(Priority + MAC address)

↑ Least

↑ Least

- \* By default Priority for every switch is same (32768).
- \* All ports on root bridge are in designated ~~state~~ port.
- \* Designated ports are not blocked.

Step 2 : Root port : Root port is one having shortest path (best path) to take the root bridge.

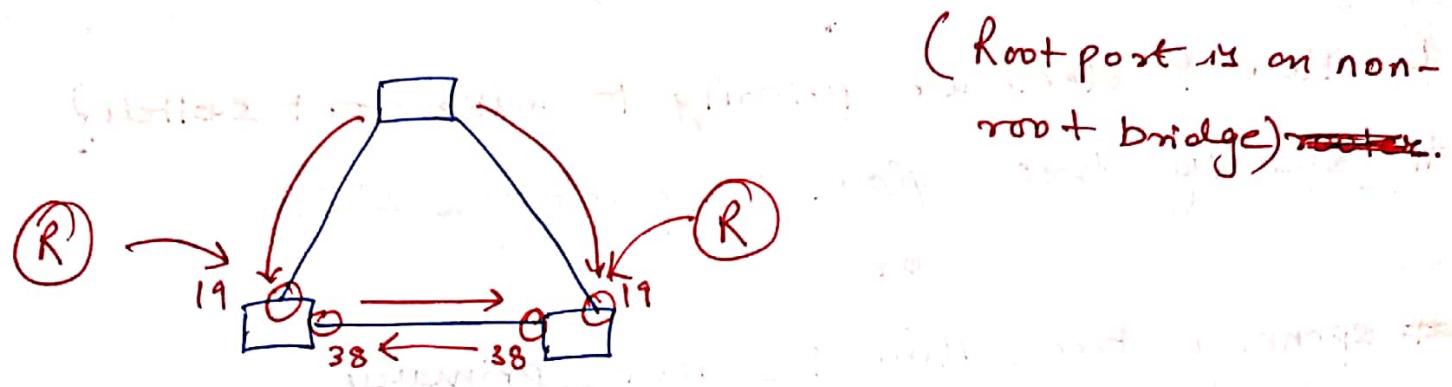
or.

Root port is one where we can receive best BPDU (Bridge protocol Data Unit).

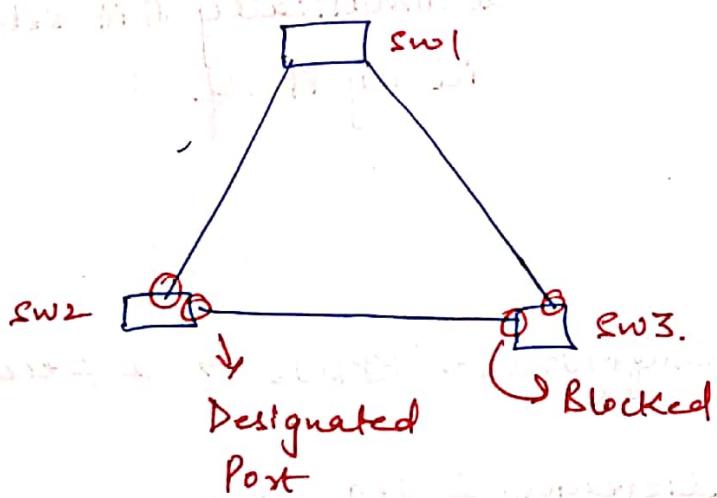
- \* Root port is decided by BW(LINK) & cost.

eth	100
Fast eth	19
Ether	4
10 Gb	2

- \* When BPDU generated from Root Bridge its cost is 0 & it's added when received at other switch port & the cost is based on link.



### Step 3 : Designated Port :-



- \* sw2 has designated port as it has best BPDU & also because it has least MAC id.

# Show - spanning - tree

↳ To check root bridge database.

Root Id → show database of Root Bridge

Bridge Id → show database of local switch.

↳ How to decrease priority to make root switch?

# spanning-tree vlan 1 priority 24576  
or

# spanning-tree vlan 1 root primary



By this we can make root bridge automatically & it select root id by itself.

↳ STP Timer :-

Hello → Interval b/w configuration BPDUs. → 2 seconds.

Forward Delay → Time spent in listening & learning states before transitioning toward → 15 seconds. forwarding state.

Max Age → Maximum length of time a BPDU can be stored without receiving an update.

Time expiration signals an indirect failure with designated or root bridge → 20 seconds.

07/11/2020

## ↳ STP States and Port Activity

STP State	The Port Can	The Port Can't	Duration
Disabled	N/A	Send or receive Data	N/A
Blocking	Receiving BPDU's	Send or receive data or learn MAC addresses	Indefinite if loop has been detected.
Listening	Send & Receive BPDU's	"	Forward Delay timer (15 seconds)
Learning	Send & receive BPDU's & learn MAC addresses	Send or Receive Data	"
Forwarding	Send & receive BPDU's learn MAC addresses & send & receive data		Indefinite as long as port is up & loop is not detected.

## ↳ Port Fast

\* Port fast is enabled on access port (Port connecting to end device)

\* Improves convergence time and directly put interface into forwarding state.

your

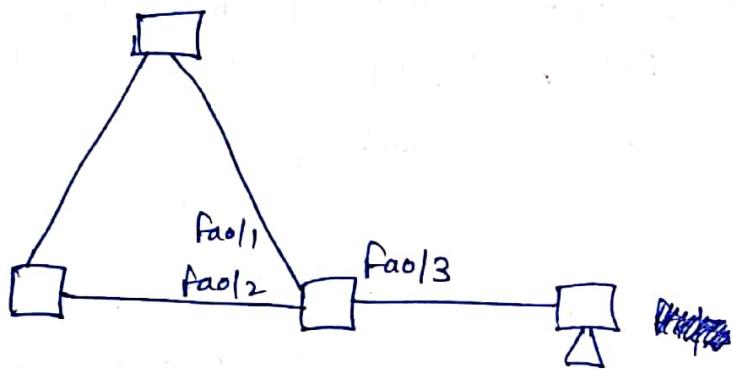
07/1/2020

# int - F\_0/3

# switchport - mode - access

# spanning - tree - PortFast (Should be on access port without end devices).

# ex



↳ BPDU Guard :-

# int - F\_0/3

# switchport - mode - access

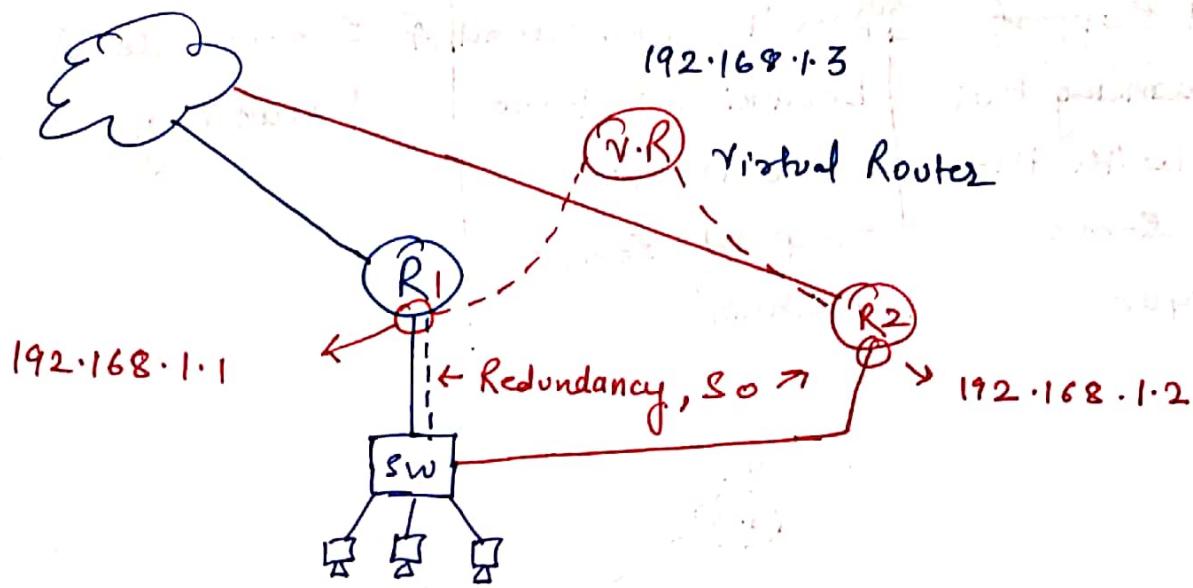
# spanning - tree - bpduguard - enable

# ex.

\*

1  
08/01/2020

## fHRP (First hop redundancy Protocol)



- \*  $R_1 \rightarrow$  Active Router.

- $R_2 \rightarrow$  Standby Router

- $R_3 \rightarrow$  It is created with the help of  $R_1$  &  $R_2$

- \* Active Router is the one having highest priority

↳ To create virtual Router we have 3 protocols :-

### HSRP

- ① Hot standby Routing Protocol
- ② Cisco proprietary Protocol.

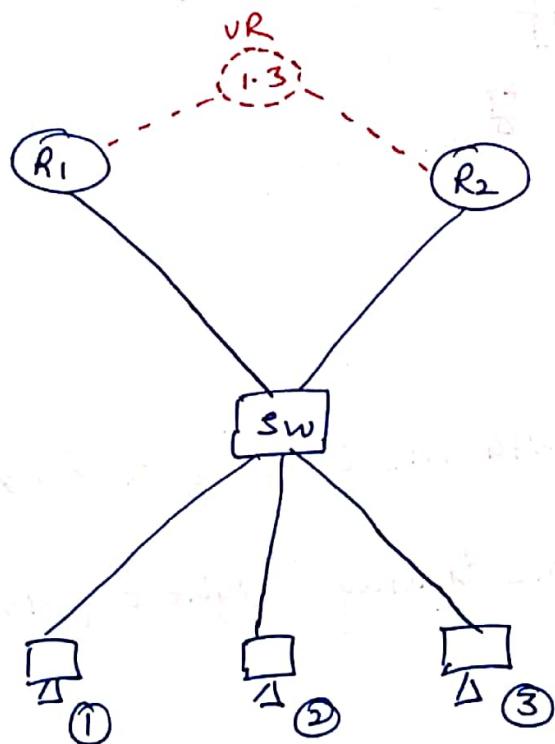
### VRRP

- ① Virtual Router redundancy Protocol
- ② open standard

### GLBP

- ① Gateway load Balancing Protocol.
- ② Cisco prop. protocol.

③ Hello timer = 3 sec Hold timer = 10 sec	Hello timer = 1 sec Hold timer = 3 sec	Hello timer = 3 sec Hold timer = 10 sec.
④ Doesn't support load balancing but we can with the help of some technique.	④ Doesn't support load balancing but we can with the help of some technique.	④ Support load balancing.



(R<sub>1</sub>) # Give ip

# Standby - 1 - ip - 192.168.1.3

(R<sub>2</sub>) # Same

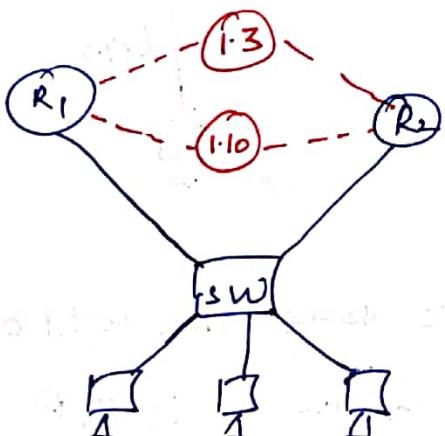
Group no. should be same in both routers

\* if R<sub>1</sub> becomes dead then R<sub>2</sub> will be active & to make R<sub>1</sub> active we need to increase priority with preempt command.

08/01/2020

**R<sub>1</sub>** # standby - 1 - priority - 180 } to make R<sub>1</sub> active from  
 # standby - 1 - preempt } standby

- \* Priority if the highest ip will be compared for active router but normally router configured first will be active.

ex

**R<sub>1</sub>** & **R<sub>2</sub>** Same as Before

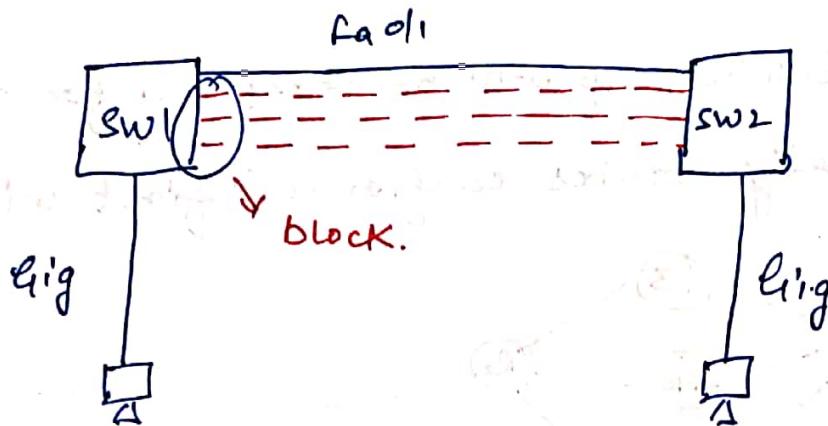
then **R<sub>1</sub>** # standby - 2 - ip - 192.168.1.6  
 # standby - 2 - priority - 60  
 # standby - 2 - preempt

**R<sub>2</sub>** # standby - 2 - ip - 192.168.1.6

Cmd # show standby

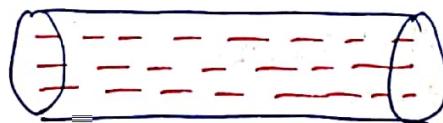
↳ To check the status of Active & standby routers,  
 Group no & Timers and Virtual Router  
 ip's.

## ↳ Etherchannel (link aggregation)



Since  $\text{Gig} > \text{Fa}$  so traffic congestion will occur.

- \* So we can add multiple links but STP will block all the redundant port tree in that case all the redundant link will be included in a channel.



- \* Maximum no. of links you can use: 8 physical interfaces for etherchannel.

If  $> 8$  then only 8 will be active.

## ↳ Etherchannel Requirement :-

- ① Duplex has to be the same.
- ② Speed has to be the same.
- ③ Same native & allowed VLAN's
- ④ Same switchport mode (Access or trunk).

↳ We can create etherchannel with the help of two protocols :-

① PAgP (Cisco proprietary)

② LACP (IEEE Standard).

① PAgP mode :-

→ ON (Interface becomes member of the etherchannel but does not negotiate).

→ Desirable (Interface will actively ask the other side to become an etherchannel).

→ Auto (Interface will wait passively for the other side to ask to become an etherchannel).

→ OFF (no etherchannel configured on the interface).

② LACP mode :-

→ ON (Interface becomes member of the etherchannel but does not negotiate).

→ Active (Interface will actively ask the other side to become an etherchannel).

→ Passive (Interface will wait passively for the other side to ask to become an etherchannel).

→ OFF (No etherchannel configured on the interface).

8/01/2020

(6)

sw1

sw2

(prototyping switch)

sw1 # Int-range-fa-0/1-6

# channel = Protocol - pagp

# channel-group-1-mode-desirable

# ex

# int-post-channel-1 → same as group no.

# switchport-trunk-encapsulation-dot1q

# switchport-mode-trunk

# ex

} make  
Trunk port

sw2 # Same as sw1

\* mode can't be auto-auto & check for other condition.

& protocol used should be same

& Port mode should be same ex trunk here

} for both  
Switches

↳ CDP (Cisco discovery Protocol) :-

① L-2 protocol

② By default enabled on Cisco devices.

③ Cisco prop. protocol

④ Used to discover directly connected devices (Cisco devices)

↳ It discovers :-

- ① Platform
- ② ip - address
- ③ interface
- ④ Duplex
- ⑤ Capabilities.
- ⑥ ios version etc.

# show\_cdp

↳ to check if it is enabled.

# show\_cdp\_neighbors

↳ to check basic neighbor info.

# show\_cdp\_neighbors\_detail

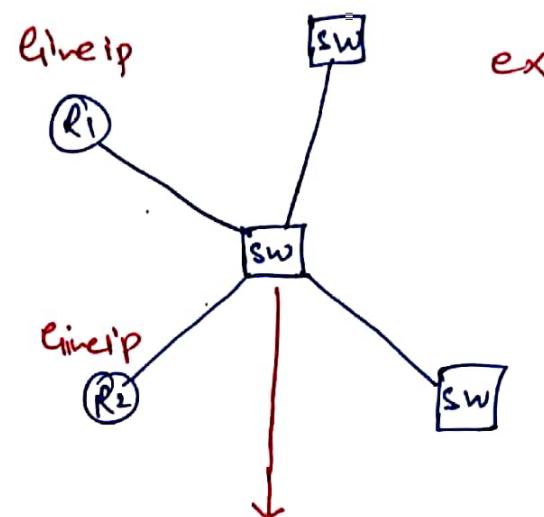
↳ to check detailed neighbor info.

# no\_cdp\_run

↳ to disable cdp.

# cdp\_run

↳ to enable cdp.



## \* Just Overview.

- ① CST
- ② PVST
- ③ PVST+ +
- ④ RSTP
- ⑤ MST

STP Types.

## \* LLDP (Link layer discovery protocol).

- ① L-2 Protocol
- ② Open std. Protocol
- ③ By default, disabled on cisco devices
- ④ Used to discover directly connected devices.

cmd# show\_lldp

↳ To check if it is enabled or not.

cmd# lldp-run

↳ To enable lldp.

cmd# show\_lldp\_neighbors

↳ To check neighbor status.

cmd# show\_lldp\_neighbors\_detail

↳ To check neighbor status in detail.

## BGP (Border Gateway Protocol).

- ① L-7 protocol
- ② Works over tcp port no. 179
- ③ Static neighbors
- ④ AD no. 20 (ebgp)  
200 (ibgp).
- ⑤ Used b/w different AS no  
 ↓  
 (Autonomous System).

### When to use BGP :-

- ① the Autonomous system allows packet to travel through it to reach other autonomous system. Ex ISP (As a transit AS)
- ② the Autonomous system has multiple connection to other autonomous systems.
- ③ Routing policy and route selection for traffic entering and leaving the Autonomous system must be manipulated.  
 (for path manipulation).

### When not to use BGP :-

- ① A single connection to the Internet or another autonomous system
- ② Lack of memory or processor power on edge routers to handle constant BGP updates.

09/11/2020

③ You have a limited understanding of route filtering and the BGP path selection process.

↳ BGP has two flavors:-

① External BGP: Between Autonomous system

② Internal BGP: within Autonomous system.

\* BGP guarantees loop free routing information.

\* BGP is a Path Vector Routing Protocol.

ex



(R1) # Give ip & loopback

```

# router bgp 1
# neighbor 12.1.1.2 remote-as 2 → Manually set up
# network 1.1.1.0 mask 255.255.255.0
# ex
  
```

(R2) # Give ip & loopback

```

# router bgp 1
# neighbor 12.1.1.1 remote-as 2
# network 2.2.2.0 mask 255.255.255.0
# ex
  
```

09/11/2020

④

cmd# show\_ip\_bgp\_summary

↳ Bgp neighbor table.

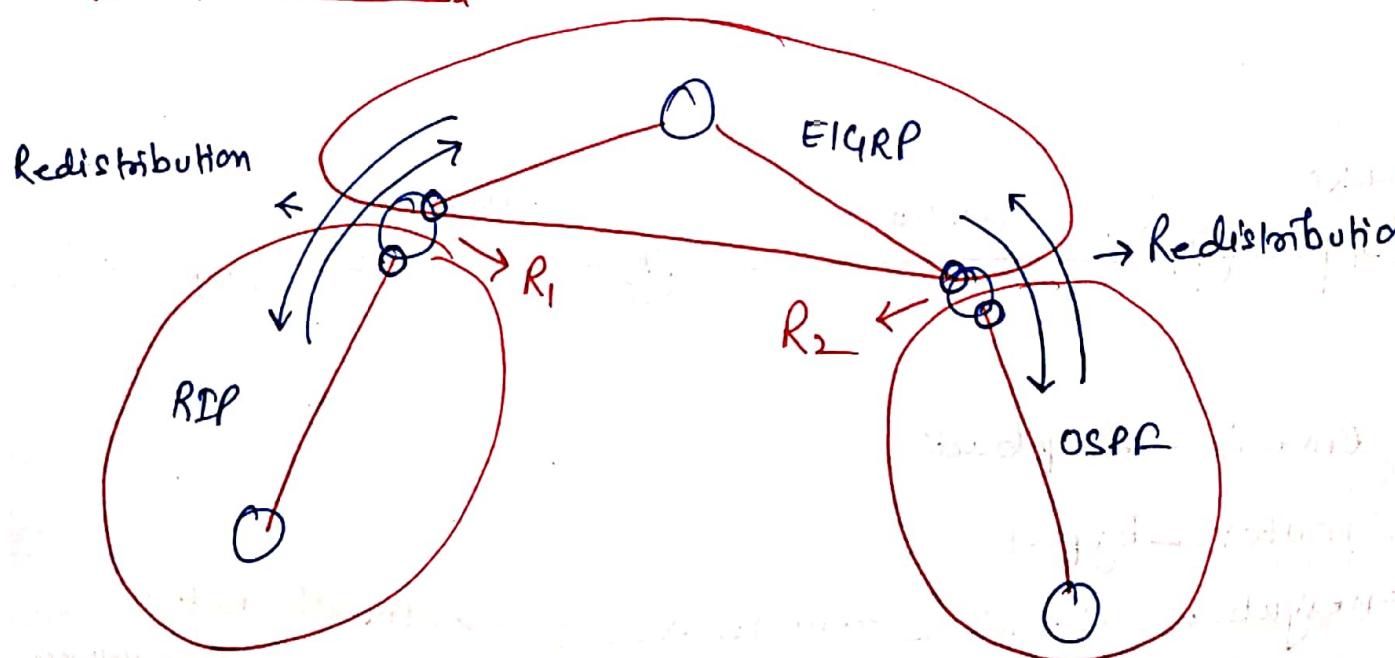
cmd# show\_ip\_bgp

↳ Bgp table.

cmd# show\_ip\_route\_bgp

↳ for Bgp routing table.

↳ REDISTRIBUTION :-



R1 # After enabling Rip f EIGRP proceed for redistribution  
# router\_rip  
# redistribute\_eigrp\_1\_metric\_2  
# ex ↗ Rip metric

R1 # ~~# router\_eigrp\_1~~  
# redistribute\_rip\_metric\_1\_1\_1\_1\_1

↳ eigrp metric.

09/11/2020

(3)

\* (R2) # router\_ospf\_1

# redistribute eigrp-1 - 1 Subnet

# ex.

→ we use subnet instead  
of metric because

# router\_eigrp\_1

# redistribute ospf-1 metric - 1-1-1-1-1

# ex.

ex # router\_rip

# redistribute connected

# redistribute static

# ex.

} Check for this as it is for  
directly connected.