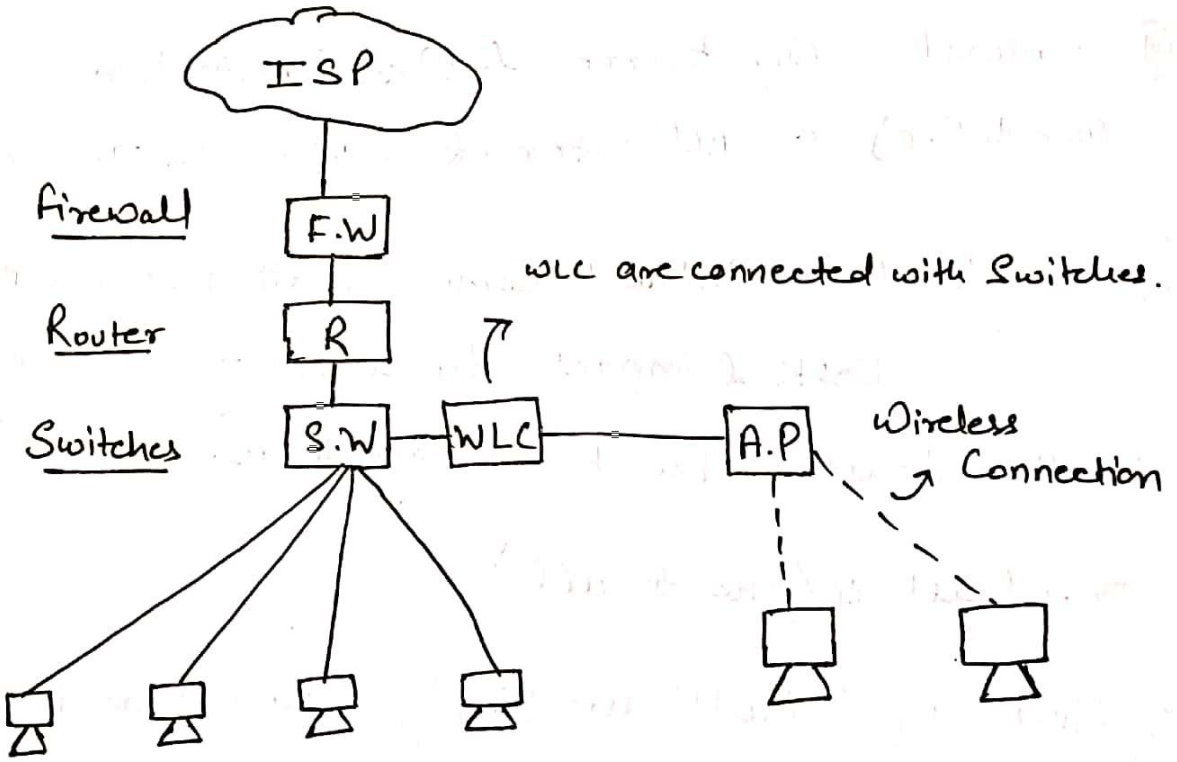
LECTURE - 1

26-11-2019

Sayed Hamza Jillani
Whatsapp: +923059299396

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 acess. 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 Sevice 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 recieve gets it but How? That is because in backend all the user who wish to recieve 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 1Km.

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. eg 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

IPv4 IPv6

* Internet → Public IP

In Our Network → Private IP

↳ IPv4 → 32 bit identity & is reps in decimal notation.

* IPv4 is divided into 4 Octets.

ex 198 . 175 . 128 . 135 → 32 bit IP

① ② ③ ④

↳ octet (8 bits)

So 8 x 4 = 32 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	→ 198 (8 bits)
		1	0	1	0	1	1	1	1	→ 175
		1	0	0	0	0	0	0	0	→ 128
		1	0	0	0	0	1	1	1	→ 135

more ex

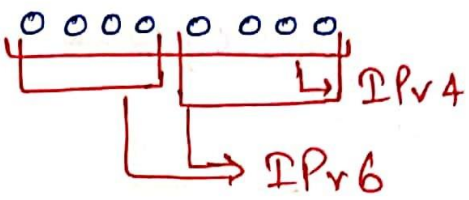
235 → 1 1 1 0 1 0 1 1

231 → 1 1 1 0 0 1 1 1

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

Divided into 8 blocks

1 hexa = 4 bits.



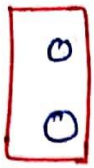
2001 : 0D88 : AC10 : FE01 : 0000 : 0000 : 0000 : 0000
16 bit 16 bit 16 bit 16 bit 16 bit 16 bit 16 bit 16 bit

Adding all we get 128 bits.

↳ IP CLASSES

#			SUBNET MASK	
	Class A	→ 0 → 127	255.0.0.0	Used in LAN & WAN
	Class B	→ 128 → 191	255.255.0.0	
	Class C	→ 192 → 223	255.255.255.0	
	Class D	→ 224 → 239	Multicast	Reserved.
	Class E	→ 240 – 255	Dept. of Defence	Reserved for Research

CLASS A

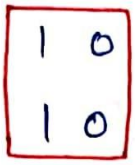


0 0 0 0 0 0 0 0 → 0

0 1 1 1 1 1 1 1 → 127

Common

Class B

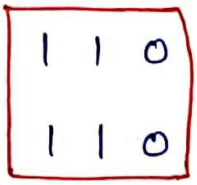


1 0 0 0 0 0 0 0 → 128

1 0 1 ——— → 191

Common

Class C



1 1 0 0 0 0 0 0 → 192

1 1 0 1 ——— → 223

Common

So that is why IP has different classes.

↳ SUBNET MASK :- 32 bit Identity

* S/M is a mixture of ~~of~~ 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 1 → 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 & .1 is a host id part

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 255 . 255 . 255 . 0 → S/m of class C.
N/w N/w N/w H

11111111 . 11111111 . 11111111 . 00000000
N/w N/w N/w 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

→ [Window + R & type ncpa.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.omniseco.com
2. ccnablog.com
3. Network lessons.com (Paid)
4. gns3vault.com (for tasks) (free)

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

Private IP	Public IP
(1) Provided by network Admin	(1) Provided by ISP
(2) locally unique	(2) Globally unique.
(3) Used for Internal Communication LAN	(3) Used for Internet (WAN)
(4) Free	(4) Paid
(5) Unregistered	(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.

9.0.0.0 — 9.255.255.255

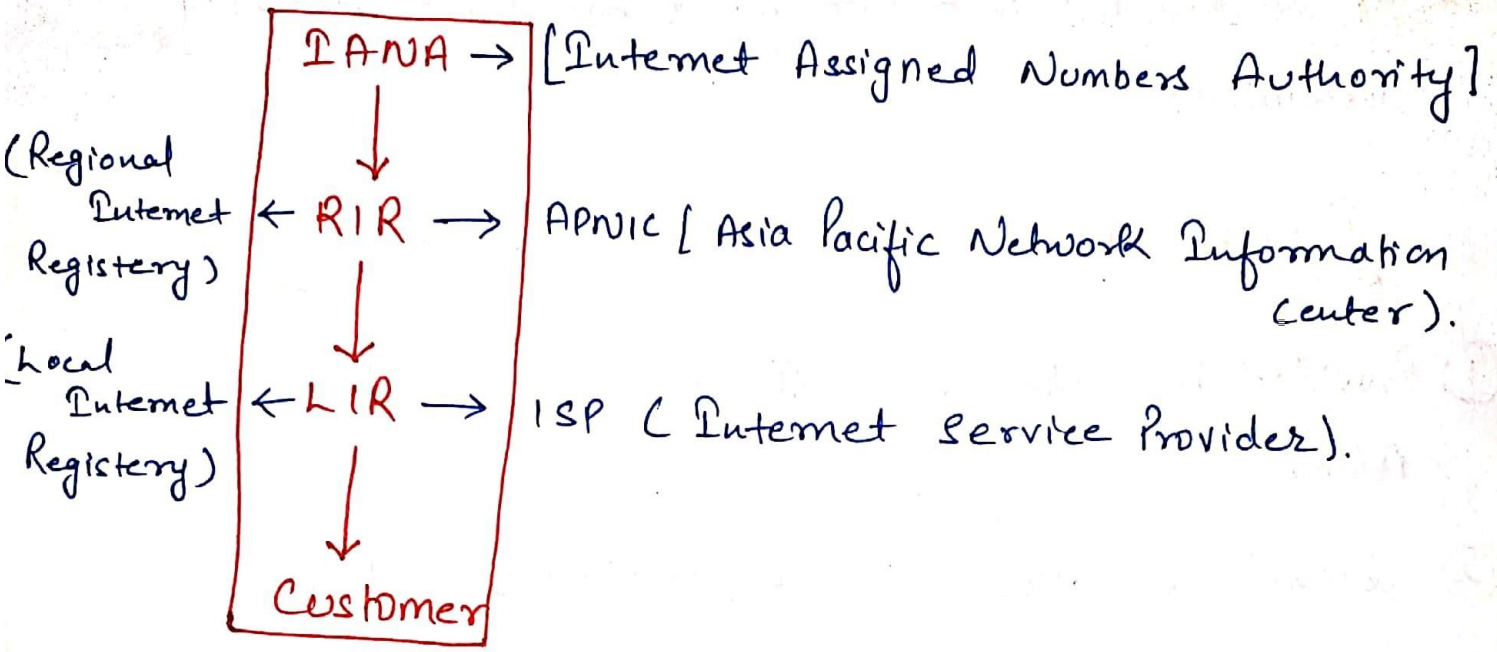
11.0.0.0 — 172.15.255.255

172.32.0.0 — 192.167.255.255

192.169.0.0 — 192.- - - -

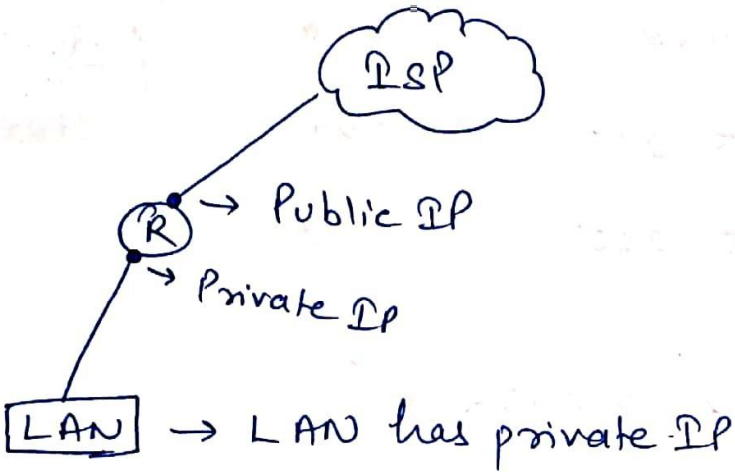
All are public

28/11/2019



* IANA works on Global level
* RIR works on Continent level.
  (Total 5 RIR)
* LIR like airtel etc.

* 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 on bit.
* ISP uses CIDR notation to allocate IP address to its clients.

			CIDR
Class A	0 - 127	255.0.0.0	/8
Class B	128 - 191	255.255.0.0	/16
Class C	192 - 223	255.255.255.0	/24

↓ classfull.

29/11/2019

S/M	CIDR
255.128.0.0	/9
255.255.224.0	/19
255.255.255.254	/31
255.255.255.255	/32

↓ Classless

↳ Conversion S/M ⟷ CIDR

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

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

ex 192.168.1.5/28

S/M = 255.255.

no. of Subnet = $2^4 = 16$

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

So no. of on bits = 8 − 4 = 4

29/11/2019

ex Class C — CIDR/29 , CIDR/26

no. of host/subnet = $2^3 - 2$
= 8 − 2
= 6

no. of Subnet = 2^5
= 32

no. of host/subnet = $2^6 - 2$
= 64 − 2
= 62

no. of Subnet = 2^2
= 4

ex Class B — CIDR/18 , CIDR/23 , CIDR/27

no. of host/subnet = $2^{14} - 2$

no. of subnet = 2^2
= 4

no. of subnet
= 2^7 = 128

no. of host/subnet
= $2^9 - 2$
= 512 − 2
= 510

no. of subnet
= 2^{11}
= 2048

no. of host/subnet
= $2^5 - 2$
= 32 − 2
= 30

↳ Complete Process (step by step).

ex 192.168.1.25/28

step 1 → S/m → 255.255.255.240

step 2 → 4th Octet Block Size = 256 − 240 (gives no. of ip's in a block)
= 16

Step 3 192.168.1.0 → .815

192-168.1.16 → 31 → 192.168.1.25 lies in this.

.32 → 47

224 → 239

240 → 255

So 192.168.1.16 → 192.168.1.31

↓ network address ↓ Broadcast address

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

So 192.168.1.17 → 192.168.1.30

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 → To practice subnetting.

↳ SUBNETTING CLASS B

ex 172.19.144.0 / 20

Step 1 S/m → 255.255.240.0

Step 2 Block Size → 256 − 0 = 256 (4th Octet)

256 − 240 = 16 (3rd Octet)

Step 3

~~172.19.144.~~

172.19.0.0 — 15.255

16.0 — 31.255

32.0 — 47.255

144.0 — 159.255

So we have range / Block

n/w address 172.19.144.0 — 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

* 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

172.19.159.255

① 03/12/2019

* Upto till now we have read FLSM

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

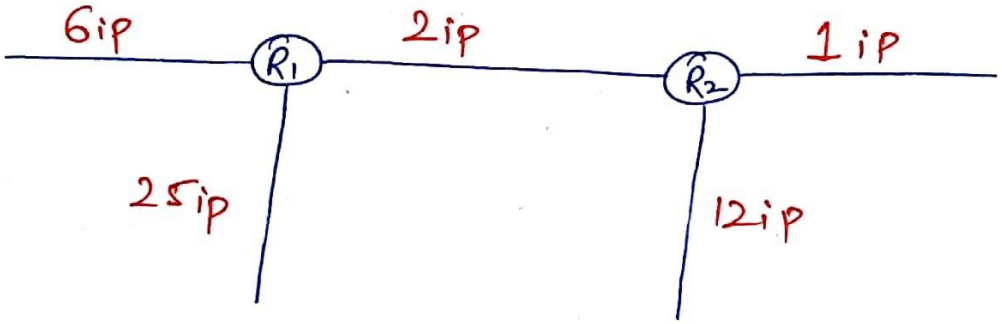
† Now we will read VLSM

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.

→ 25 ip = 192.168.10.0 —— 31

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

no. of host/subnet = $2^5 - 2$ ∴ no. of on bits = 3 ∴ CIDR = /27
= 32 - 2 = 30

03/12/2019

In the same way

for 12 ip = 192.168.10.32 — 47 / 28

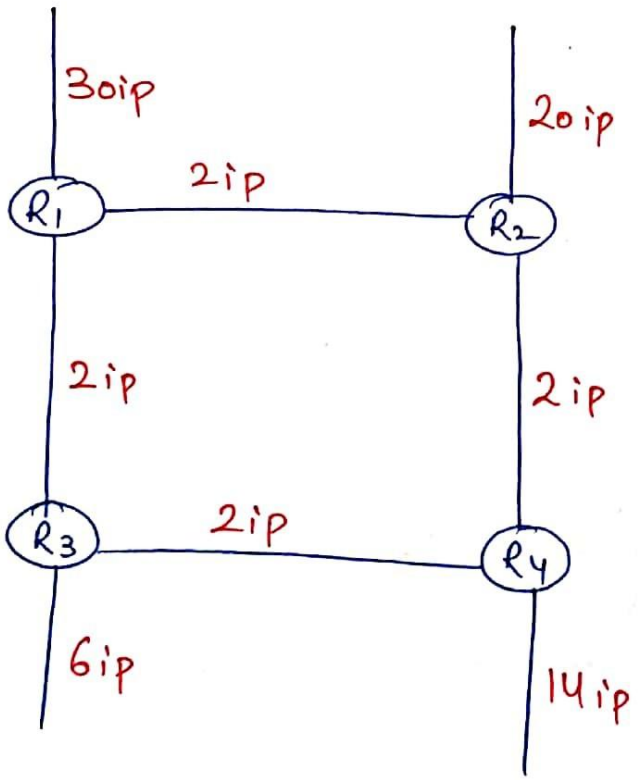
no. of off bits = 4 ∴ no. of on bits = 4 hence CIDR

for 10 ip = 192.168.10.48 — 63 / 28

for 6 ip = 192.168.10.64 — 71 / 29

for 2 ip = 192.168.10.72 — 75 / 30

ex



192.168.10.0 / 24

30 ip = 192.168.10.0 — 31 / 27

20 ip = 192.168.10.32 — 63 / 27

14 ip = 192.168.10.64 — 79 / 28

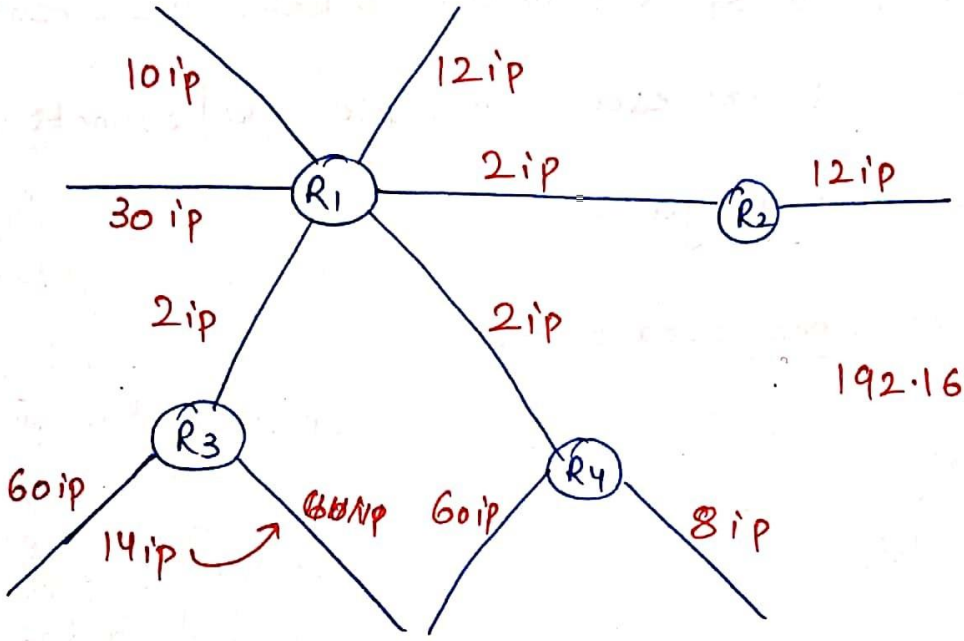
6 ip = 192.168.10.80 — 87 / 29

2 ip = 192.168.10.88 — 91 /30

2 ip = 192.168.10.92 — 95 /30

2 ip = 192.168.10.96 — 99 /30

ex



192.168.10.0/24

60 ip = 192.168.10.0 — 63 /26

60 ip = 192.168.10.64 — 127 /26

30 ip = 192.168.10.128 — 159 /27

14 ip = 192.168.10.160 — 175 /28

12 ip = 192.168.10.176 — 191 /28

12 ip = 192.168.10.192 — 207 /28

10 ip = 192.168.10.208 — 223 /28

8 ip = 192.168.10.224 — 239 /28

2 ip = 192.168.10.240 — 243 /30

④ 03/12/2019

2ip = 192.168.10.244 – 247 / 30

2ip = 192.168.10.248 – 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

↓

This octet is changing

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

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 172 · 16 · 0 · 0
8bit 8bit → 6 bits from above

So CIDR will be 172.16.0.0/22 (8+8+6=22)

So 172.168.0.0/22 reps above all 4 Networks.

ex

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

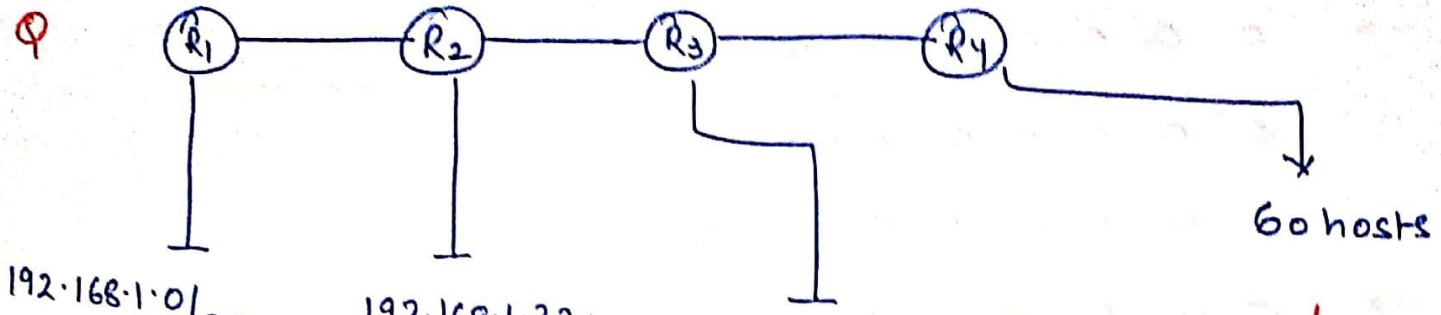
↳ class is A but change is in 3rd Octet

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

So 10 · 0 · 0 · 0 / 22 Ans.
8bit 8bit 6bit

03/12/2019

Q



192.168.1.0/27

192.168.1.32/28

192.168.1.48/28

VLSM

192.168.1.63 /26

↳ OSI → (Open System Interconnection).

- Open Std | Proprietary
  - Vendor Independent | Vendor Dependent
- N/W Device
- Connectivity

↳ 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 Protocol) SSH - 22 (TCP)
Telnet - 23 (TCP)

(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)

Interim 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

↳ DNS → Port no. 53

Layer 7 Protocol

Works over TCP/UDP

Used to (Translate)/Resolve name to IP and IP to Name

ex https://www.google.com
↳ URL

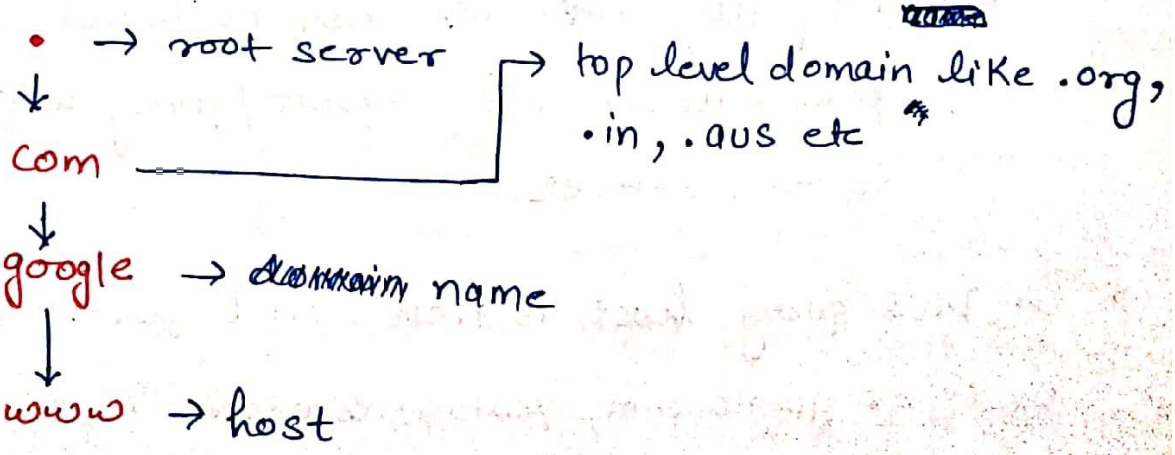
www.google.com → This is in terms of DNS.

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 entery in host.txt file.

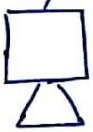
→ DNS Hierarchy :-

→ We never type www.google.com⊙ (or anything like that) but it is there and it is called root server



↳ Based on Above Hierarchy we will study DNS working or DNS lookup.

cmd # ip_config / Display_dns
↳ It is used to check DNS entory / Request



→ (1) if we try to access any website or make any DNS query then it first go to the local PC only t 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

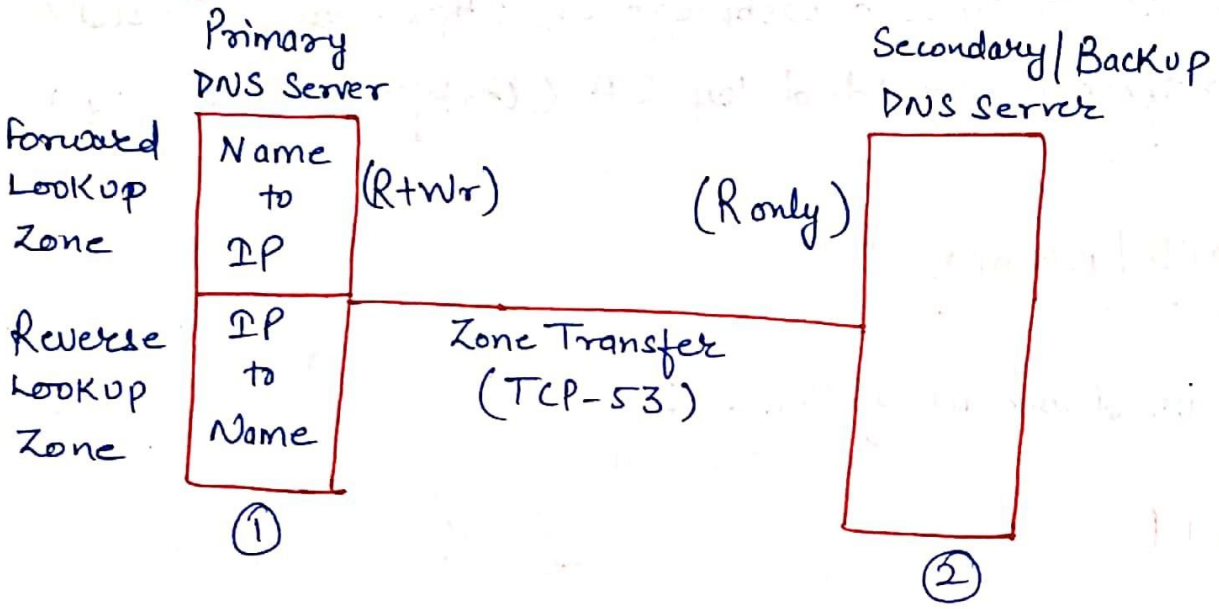
(*Also this will be the case when the website is accessed for the first time)

↳ (3) If the DNS 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.

* 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 IPv6 as query length usually gets increased above 512 bytes then it sends DNS query on TCP Port 53

04/12/2019

↳ WEB SERVICES -:

Protocols used are as follows -:

↳ HTTP : Plain Text data transfer.

HTTPS : Encrypted packet (Ciphor 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	TFTP
① File transfer Protocol	① Trivial file transfer Protocol
② Works over TCP port no. 20/21	② works over UDP port no. 69
③ Support Authentication	③ Doesn't support Authentication
④ Support directory based browsing	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 standered 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.

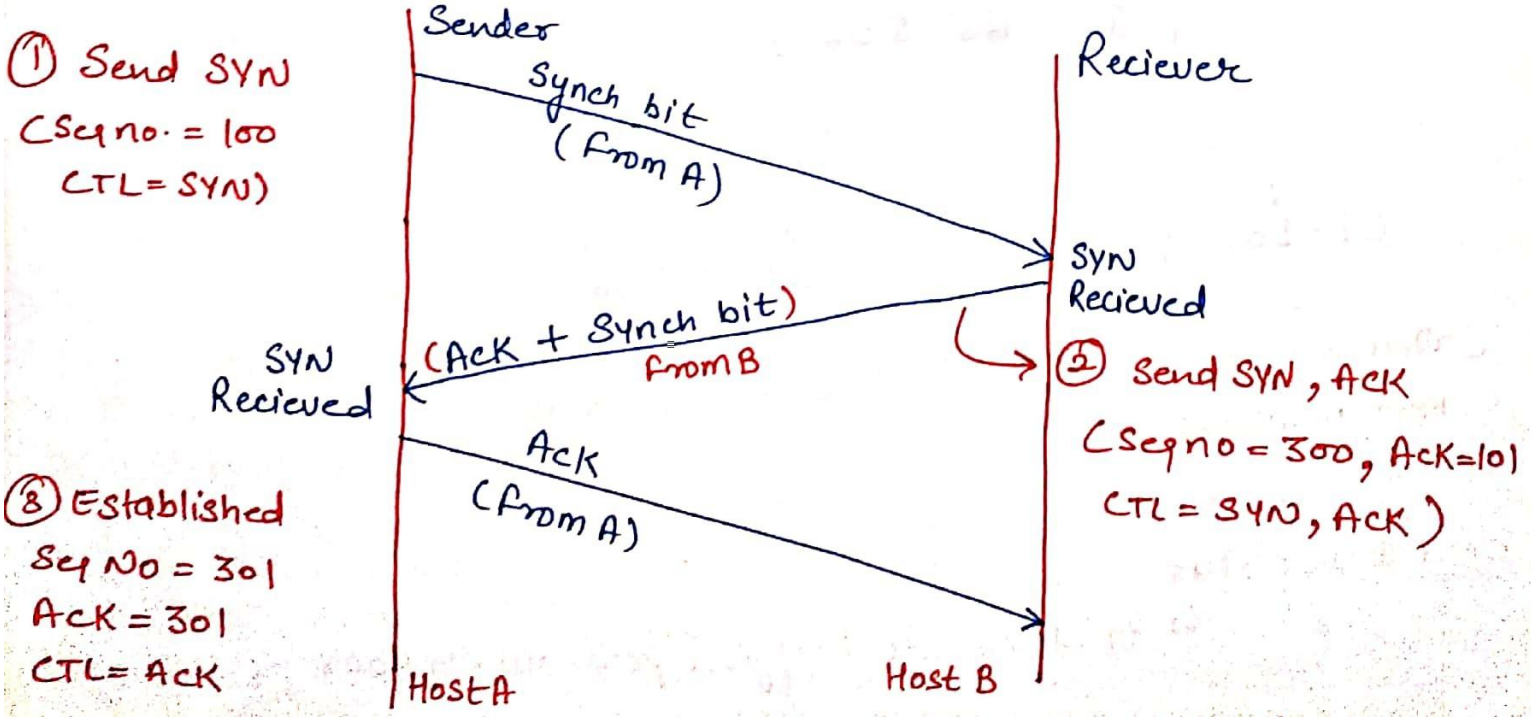
05/12/2019

L4 → TRANSPORT LAYER –:

TCP	UDP
① Transmission Control Protocol	① User Datagram Protocol
② TCP works over protocol no.6	② UDP Protocol no-17
③ Connection oriented	③ Connection Less
④ Provides windowing, Ack, Segmentation	④ No
⑤ Slow	⑤ Fast
ex Telnet, ftp, ssh etc	ex DHCP, Tftp etc.

* DNS works on both TCP & UDP

3 WAY HANDSHAKE –:



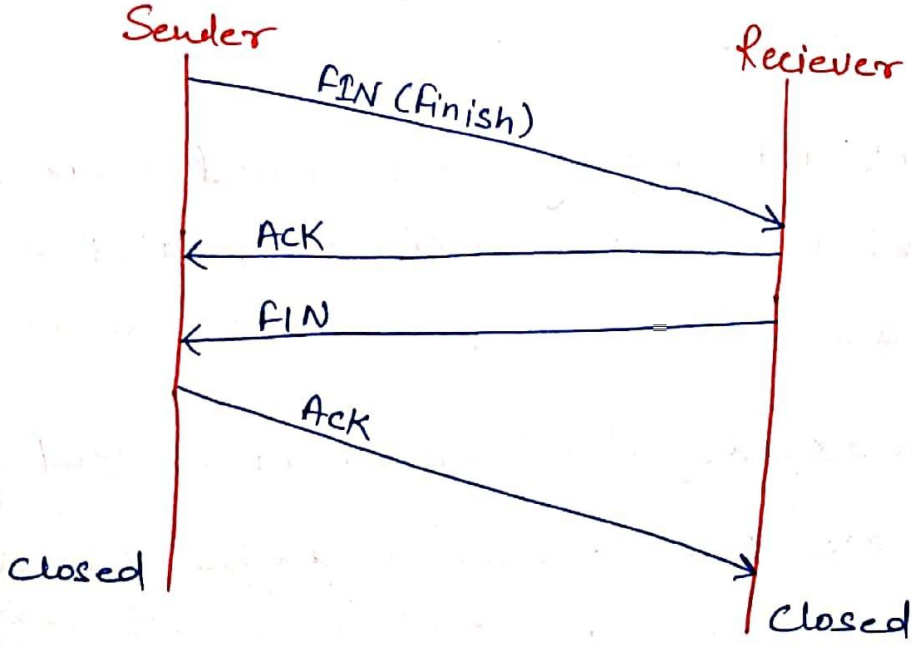
* Protocol work on L7 has port no. & protocol work on L3 & L4 has protocol no.

* Because all protocols on L7 works on TCP & UDP port so can't be protocol no.s, 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 :-



05/12/2019

* 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 Seq no was 100 & the Ack was 101.

* In 3 way handshake & Actual data transfer Seq & Ack no. works in a different way.

* In Data transfer also Random Relative Sequence no. is 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 → 1

Data → 9

Next Seq no. → 1+9

→ 10

} In Data transfer not 3way handshake

* In Data transfer Acknowledgement recieved is the same Seq no. not +1. because reciever updates sender that correct seq no or correct data has been recieved.

* In 4 way handshake FIN (finish) bit is sent from sender to indicate that connection can be terminated now.

↳ **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, **MSS = 1460 bytes** * It is just a by default size of MSS not a size of segment.

So **1460 bytes (MSS) + 20 bytes (TCP Header)** → **1480 bytes**

↓

Now it is called Segment.

↳ **WINDOWING** :- Maximum amount of data that a reciever is willing to recieve before sending a back an Ack.

By default, **Window Size = 4128 bytes**

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

* 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 shake window size of 10000 bytes during 3 way & now 10000 bytes will be transferred & now next window size will be informed during Acknowledgement.

Accedian → Tcp series #4 (Blog) to study TCP & IP packet

↳ What is Zero Window?

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

It may have a stuck processor or be busy with other task, which can cause the TCP reciever buffer to fill.

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

* Window scaling factor can increase window length for Data transfer

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

Uses 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 recieved at interface is more length than of interface the there is aneed 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.

$$\underbrace{\text{Data (Segment)}}_{1480\text{ bytes}} + \underbrace{\text{IP Header}}_{20\text{ bytes}} = \underbrace{1500\text{ bytes}}_{\text{Packet}}$$

* IP Header length can also be altered upto 60 bytes.
* Suppose if at Router R_1 5000 bytes packet/segment is recieved then it would be divided into 4 Packetes of 1500 x 3 & 500 bytes at R_2

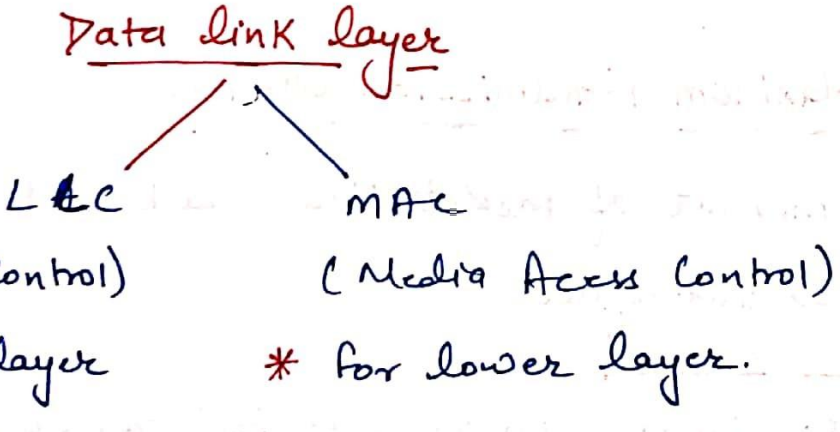
↳ DATA LINK LAYER

Device → L2 Switches.

Protocol → MAC, PPP etc

function-:

① Frame Switching
② Error Control



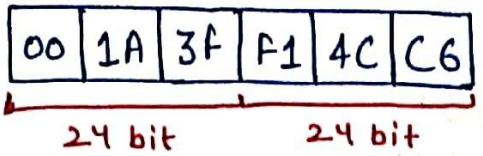
* For higher layer like L3 etc
* For lower layer.

↳ MAC (Media Access Control)

① 48 bit
② Represented in Hexadecimal Notation.

ex

MAC



48 bit identity

Reps → OUI (Vendor)
Organizationally Unique Identifier

Reps → NIC (Hardware)
Network Interface Controller Specific

Cmd # getmac

* If in any MAC address the 8th bit is

0 → then Unicast

1 → then Multicast

& ffff.ffff.ffff then Broadcast.

↳ L1 → PHYSICAL LAYER

→ Device :- Hub, NIC etc

1500 bytes + 14 bytes = 1514 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 as work 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 (Gratitious ARP)

→ Used to check Ip duplicacy or Ip Conflict

→ In this Source IP & Destination IP are same & packet broadcasts.

* In today's world we do not use RARP as Bootp protocol & then DHCP was launched & DHCP do the same thing as RARP if MAC binding is done with DHCP.

→ PARP (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 costensibly 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

① Physical Access → console port

② Remote Access → Telnet, vty port, SSH

② GUI → HTTP, HTTPS → CCP tool.

LECTURE - 10
09/12/2019

↳ 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 ~~red~~ wire as it produces E.M Waves which causes hinderance.

↳ **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 Connector end we connect them in two ways which divides it into Cross over & straight through. & the difference can be checked ~~at~~ by color coding.

↳ Color Coding of Cross-Over Cable

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

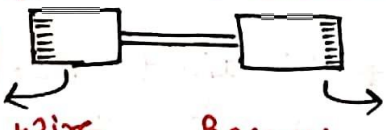
wire	Becomes
1	3
2	6
3	1
6	2

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

wire	Becomes
1	1
2	2
3	3
6	6

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 ⟷ PC
↳ Crossover Cable

Transmit [1, 2] ⟷ [3, 6] Recieve

Recieve [3, 6] ⟷ [1, 2] Transmit

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

PC ⟷ SW
↳ Straight through Cable

Transmit [1, 2] ⟷ [1, 2] Recieve

Recieve [3, 6] ⟷ [3, 6] Transmit

* Other unused 4 pins are used for POE.

* Nowadays we use Auto MDIX but not in old devices as not support 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 recieving, 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

Upto CCIE level couple of more routers will add up.

↳ IOS [Router/Switch] Modes :-

Router > (User mode) enable (en) (Cmd)

Router # (Priviledge mode or Exec mode) configure terminal (conft)

Router(Config)# (Global Configuration mode)

* With 'exit' command or 'Ctrl + Z' you can exit or come out of Global Config mode and User Mode.
* To come out of Privelge mode type en '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. Tracer route etc

↳ Privelege Mode :-

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 any cmd'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 Commaud.

② Ctrl + A → At the beginning of line / commaud.

③ Ctrl + E → At the end of line / commaud.

↳ 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 plain text. But we can encrypt password by 'service password-encryption' cmd in Config mode

* Service password cmd encrypt password with md7 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	ROM
running-config	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

f file will be copied.

We can check by show Running-config / startup-config

or Simple Cmd is 'write'.

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 & Privelege mode.
② Privelege mode password.
③ Go to vty line and allow telnet.

username_KK_secret_ccna (for user mode)
Enable_secret_ccna (for privelege 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 privelege mode.

↳ After that you will have acess 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 L7 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 privelege mode password.
④ Define a domain name
⑤ Generate Crypto Key

(6) Go to vty line and allow SSH.

* Key material (input) → RSA (Algo) → Key (output)

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.

LECTURE - 12

11/12/2019

① ↳ DHCP :- ① L-7 Protocol

② Works over UDP port no. 67 & 68

③ Used to dynamically distribute ip addresses to its client

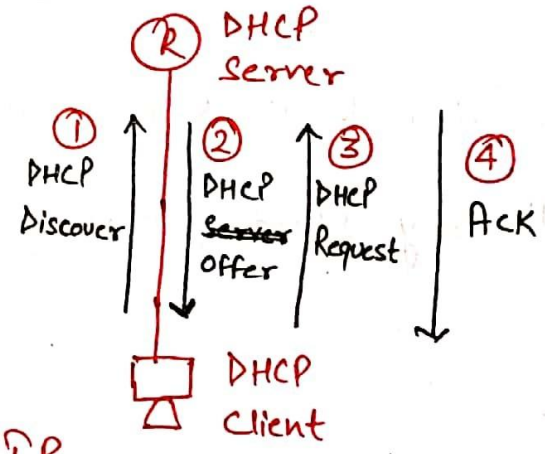
DHCP (Dynamic Host Configuration Protocol)

* 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 server]

How to configure DHCP?

```
# int_fo/o
# 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 is 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 ~~sta~~ 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~~ file name & 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 ctrl+c / Pause Break to change the register value & set up new password. 0x2142 (New)

→ Steps ↓

Restart your Router
Press ctrl+c / Pause Break to abort boot sequence
Rommon 1> Confreg_0x2142
Rommon 2> 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

12/12/2019 ②

→ 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 Routes 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 routes can learn path.

→ Static & Default Routing

→ Dynamic Routing

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

↳ STATIC ROUTING :-

Syntax

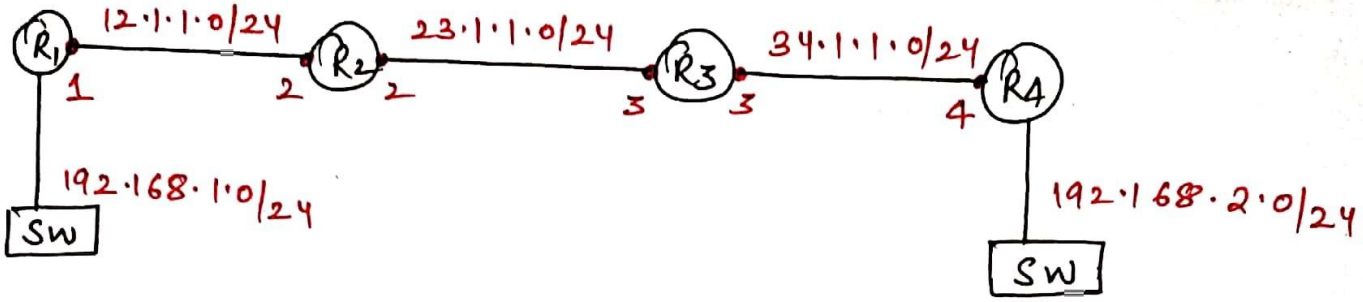
Router(Config)# ip_route _<dest^n n/w>_<s/m>_<next hop ip>

* Next hop Ip is the i.p address of neighbor router that is directly connected to our router.

12/12/2019

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 ~~break~~ stop that then we can use the above command.

cmd # show_ip_route

↳ To check routing table

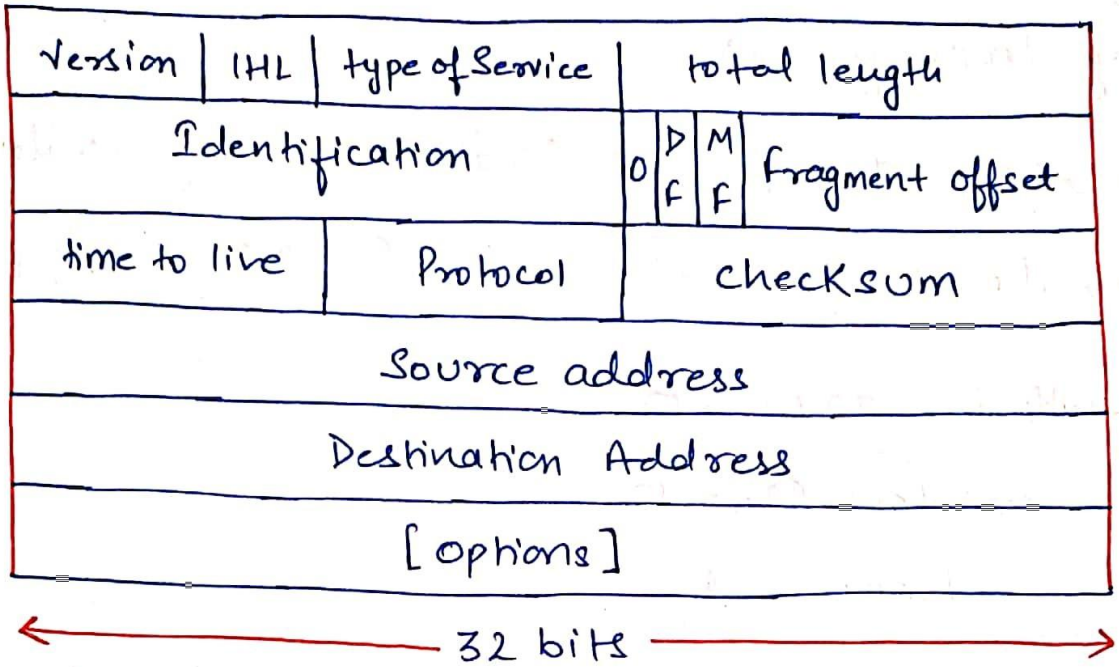
In Routing table:

C → directly connected S → Static Routing

↳ 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 [20-60 byte]

↳ But total length = Data length + Header length

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 recieving port.

Check Sum → Used for Error Detection.

↳ It is an Algorithm

* Sender Runs checksum & attach value to sender header & when ~~data~~ packet is recieved at reciever 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 fragmanted datagram. Each fragment of Datagram has the same identification number.

13/12/2019

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)

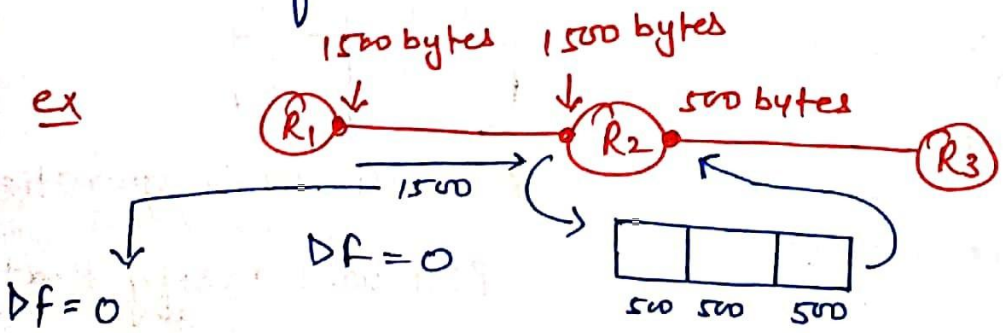
Off : 0 means that this is the last fragment of the datagram

ON : 1 means that additional fragments will follow.

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

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

ex



Complete 1500 bytes get forwarded

Df=1 ∴ Packet drops & MTU size is 500 but recieved is 1500 moreover Df=1

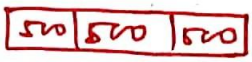
Df=1 also does not make a difference

(4) ex

13/12/2019

1500 1500 500

↳ so

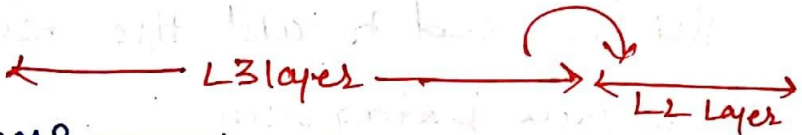


FR1 FR2 FR3

MF = 1 at R_3 input terminal which means more fragment will follow

, when FR1 is recieved which is a last freagment so MF = 0 will be sent

↳ PACKET FLOW



ICMP request IP Header

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

S/M → 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

13/12/2019

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	0	0	0	→ 192
1	0	1	0	1	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.IP

11000000 . 10101000 . 00000001 . 00000001 → 192.168.1.1

11111111 . 11111111 . 11111111 . 00000000 → 255-255-255-0

11000000 . 10101000 . 00000001 . 00000000 → AND operation

↓ . ↓ . ↓ . ↓

192 . 168 . 1 . 0 → Network.

D.IP

11000000 . 10101000 . 00000001 . 00000010 → 192.168.1.2

11111111 . 11111111 . 11111111 . 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	ethernet header
ICMP reply type -0 code-0	S·IP → 192·168·1·2 D·IP → 192·168·1·1	S·MAC PCB D·MAC PC A

16/12/2019

LECTURE-15 (1)

↳ STATIC ROUTING WITH SELF EXIT INTERFACE

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

Syntax

Router(Config)# ip-route _ <Dest^n 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 & 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
<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 many other route as backup. Router will select lower AD route to forward the traffic

Protocols	AD
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 routers. The neighbour will analyze the information & write new routes to the routing table

* The router will pass routing information recieve from one router to other routes 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^n 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 (IGP) – RIP, EIGRP, OSPF
   Gateway
2. Exterior Routing Protocol (EGP) – BGP
   Gateway

↳ 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

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

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

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

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

↳ 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

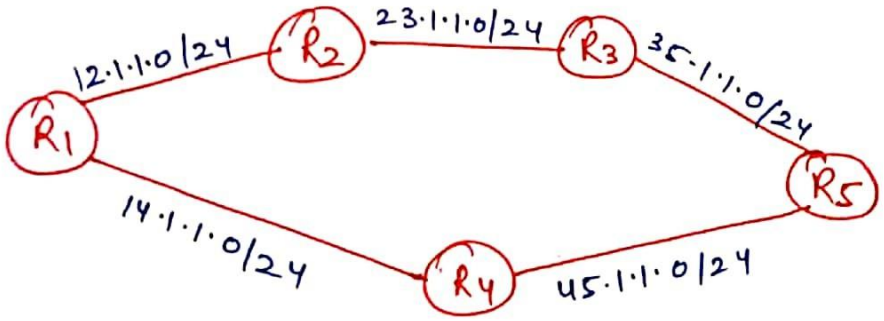
* Equal path Cost load Balancing

RIP ver1	RIP ver2
1) Doesn't support VLSM	1) Support VLSM
2) Send periodic updates in every 30 sec by using broadcast address (255.255.255.255)	2) Send periodic updates in every 30 sec but by using multicast address (224.0.0.9)

← Here periodic updates mean periodic routing updates.

RIP v1	RIP v2
3) Doesn't send subnet mask information in routing updates.	3) Send Subnet mask information in routing updates.
4) classful routing protocol	4) classless routing protocol
5) Doesnot support Authentication	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 Keep it in classfull nature)

```
# no_auto_summary
```

[Here it is used to convert classfull behaviour into classless]

(ex for R1) {

```
# network_12.1.1.0
# network_14.1.1.0
```

[own network 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 routers is 16
* So we can say that n/w becomes unreachable when hop count reaches 16.
* Therefore if any network/Routers becomes dead then hop count value 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.

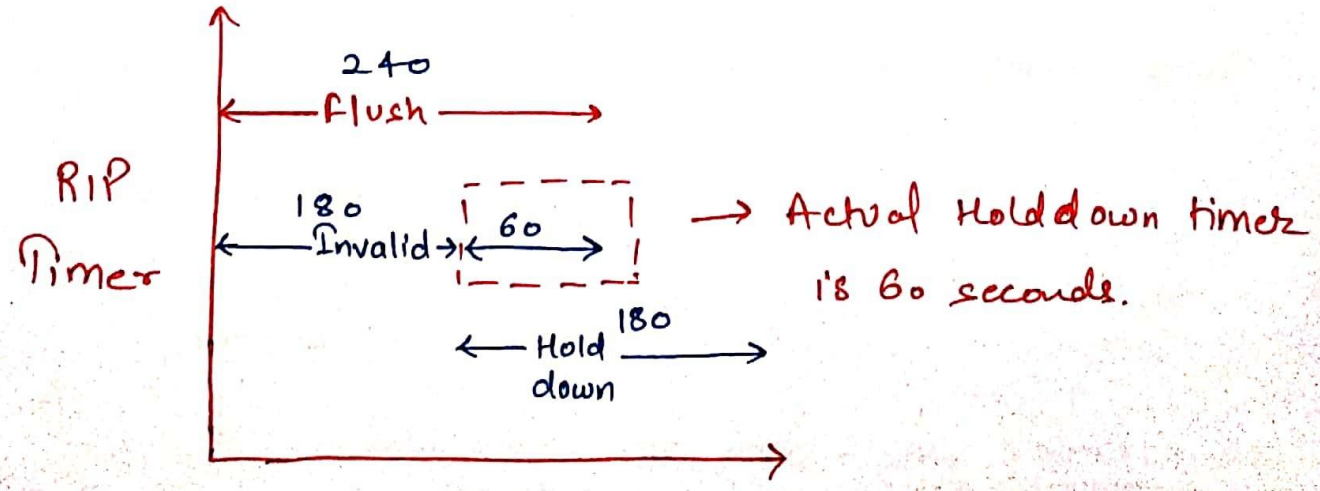
↳ Rip Timers

① **Update** :- this is how often we send routing updates, the default is 30 seconds.

② **Invalid** -:- the no. of seconds since we recieved 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.

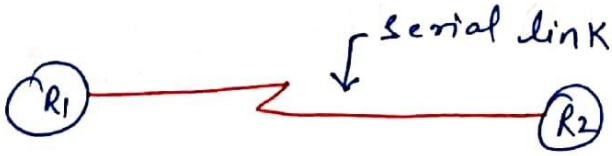
④ **Flush** -:- How many seconds since we recieved ~~that~~ the last valid update untill we throw the route away, the default is 240 seconds.



↳ OSPF (Open shortest Path find)

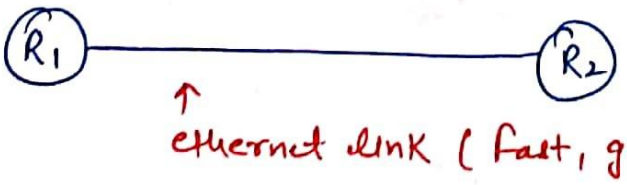
Link state routing Protocol
Open standard Routing Protocol
Works on Protocol no. 89
Metric → Bandwidth
Multicast address → 224.0.0.5, 224.0.0.6
OSPF uses SPF algo for best path Calculation.
Support equal cost load balancing.
Supports Unlimited hop counts.
Uses hierarchy structure.

↳ Point to Point Network



* Serial link is also called WAN link

↳ Cisco consider it point to point n/w.

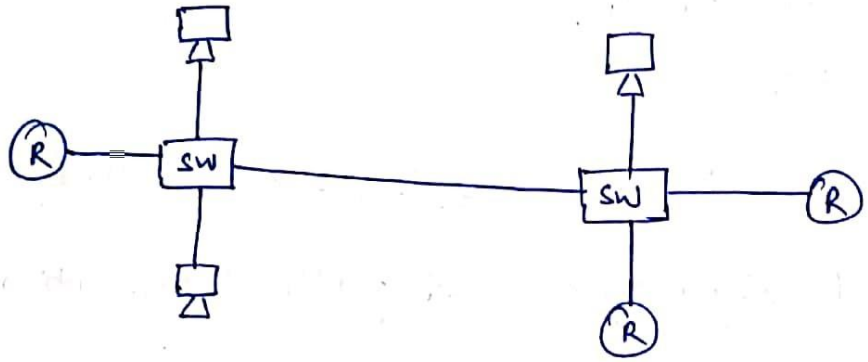


↳ Cisco consider it as Broadcast n/w not point to point n/w.

↳ Broadcast n/w [Multi-access n/w]

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

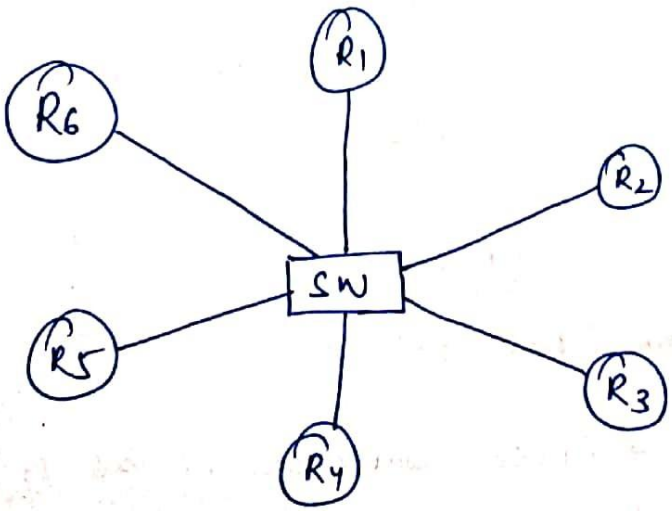
ex



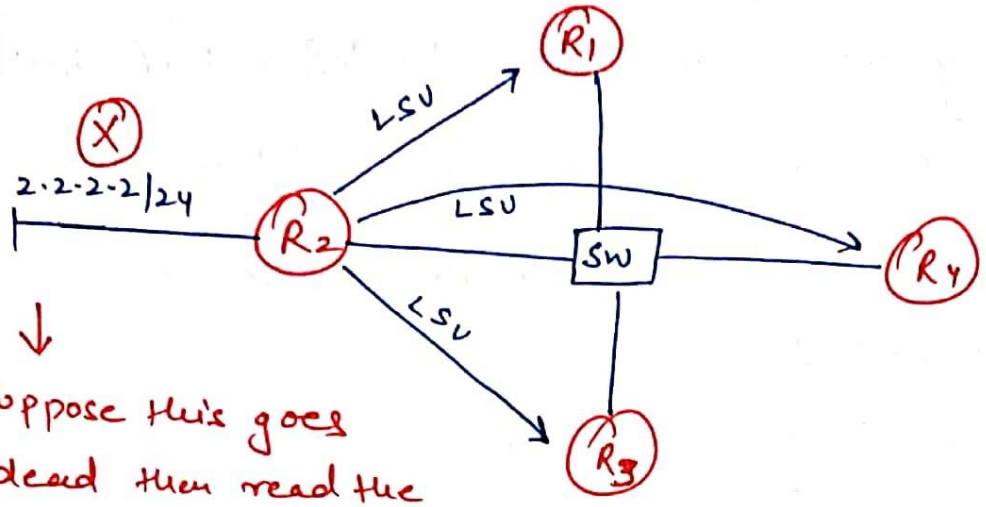
→ Challenges in Broadcast n/w [Multi-access n/w]

1. Multiple adjency (neighbors)
2. flooding of LSA (data)

Total no. of neighbor = $\frac{n(n-1)}{2} = \frac{6(6-1)}{2} = \frac{6\times5}{2} = \frac{30}{2} = 15$



(11)



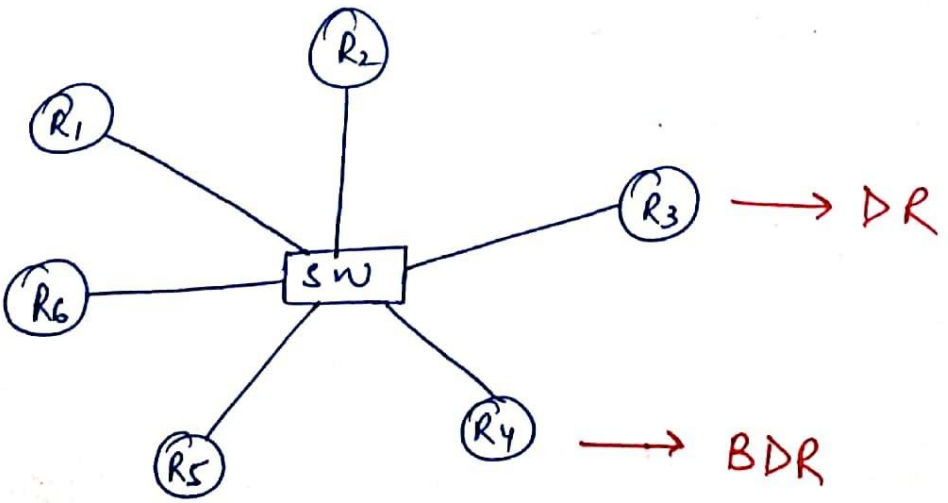
↓ Suppose this goes dead then read the point below

* 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

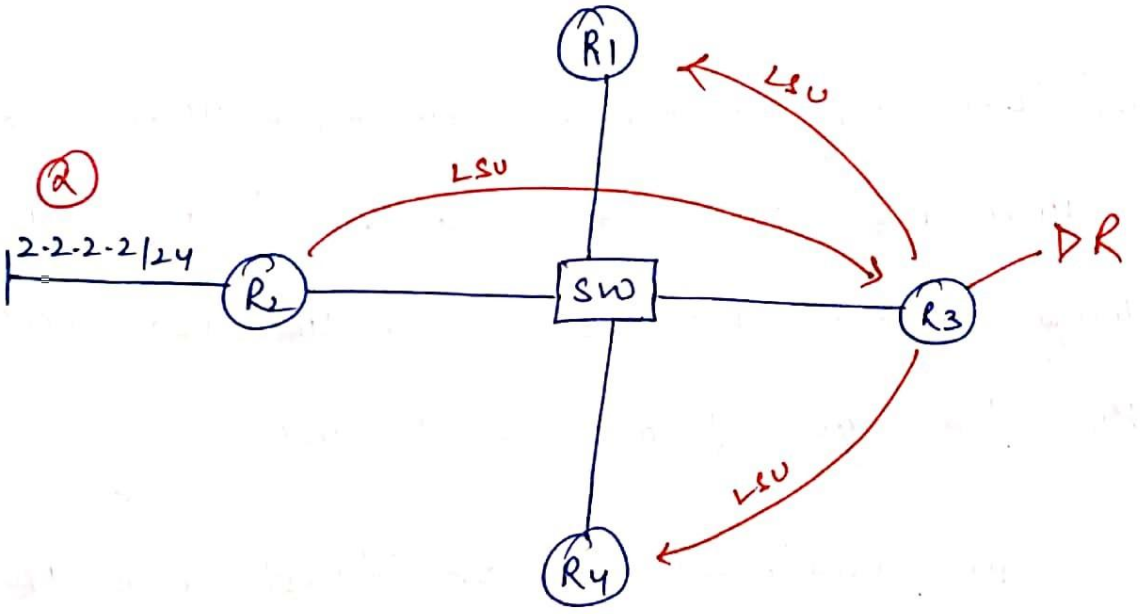
→ DR (Designated Router)

→ BDR (Backup Designated Router)



* So here every routers 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-1 is controlled.

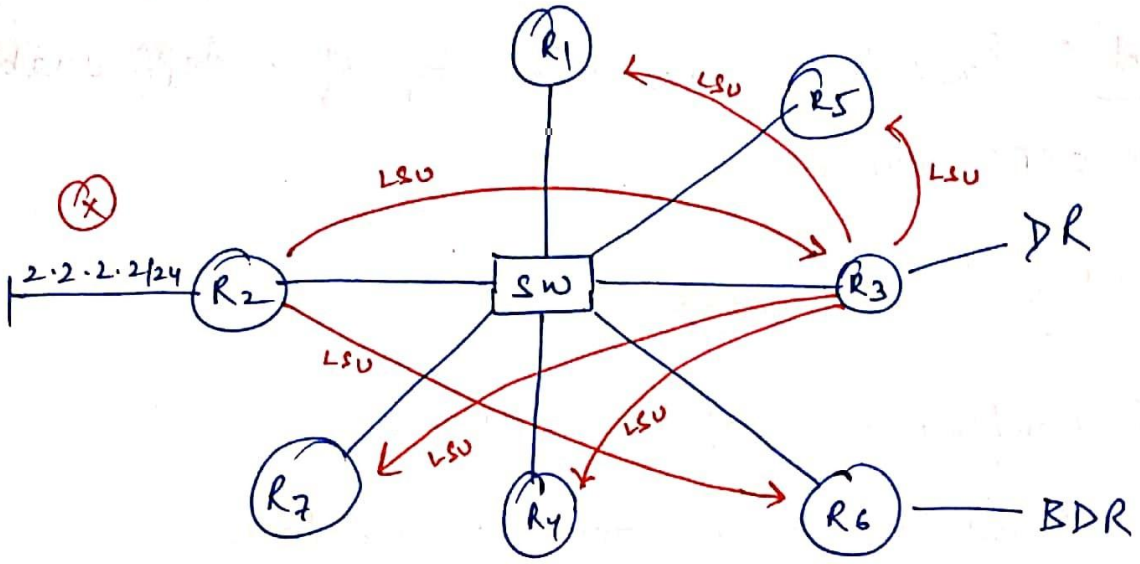
Now assume 2nd challenge scenario



* 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 this'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~~ 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 set router priority 0 then router becomes 'DR other.'

this happens in the case we do not want any routers to become DR or BDR.

↳ **Router id** :- Provides unique identity of a ospf enabled routers in ospf domain.

↳ **Router-id election Process** :-

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

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

↳ **WildCard Mask** :- Opposite of Subnet Mask.

Class C → 255.255.255.0 - S/M

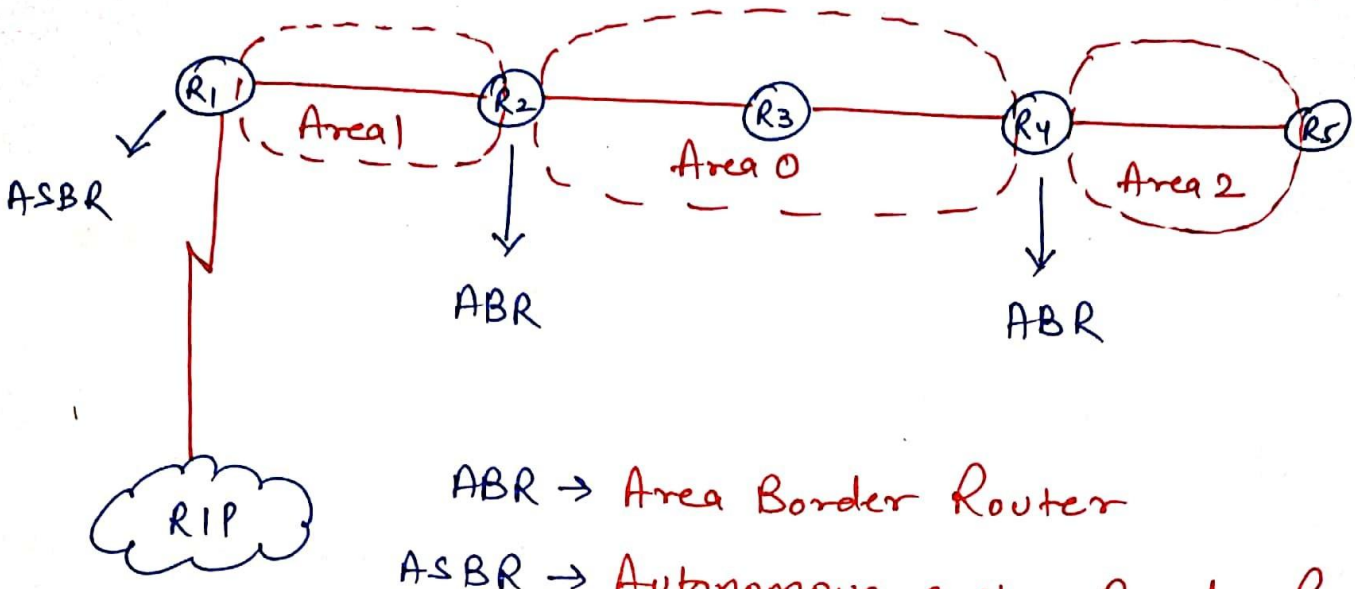
WildCard Mask → 0.0.0.255

Class C → 255.255.255.192

wildcard Mask → 0.0.0.63

↳ In W.M 0 → Matching bit

1 → don't care bit.



ABR → Area Border Router

ASBR → Autonomous system Border Router

* Area 0 is called Backbone Area.
* ASBR is routes 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 routes as it is in complete Backbone area.

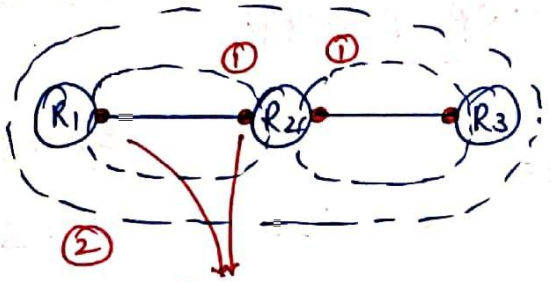
↳ Neighbour Requirements for EIGRP & OSPF

	OSPF	EIGRP
→ 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 watch	→ 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 router should be neighbours.

* Same subnet must be a member of same area.

Case1

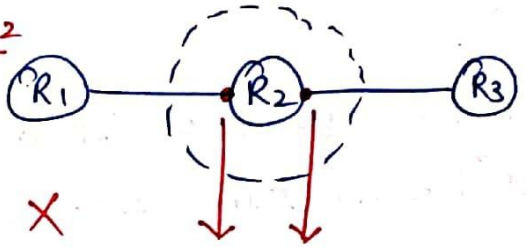


① ✓

② X

Both interface are same subnet

Case2



Both are diff subnet So choice of Area is wrong.

↳ Syntax

Router(config)# router_ospf_P.ID (Process Id)

network_own n/w id_wildcard Mask_Area_Area-id

ex Area 2

#

#

Exit.

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

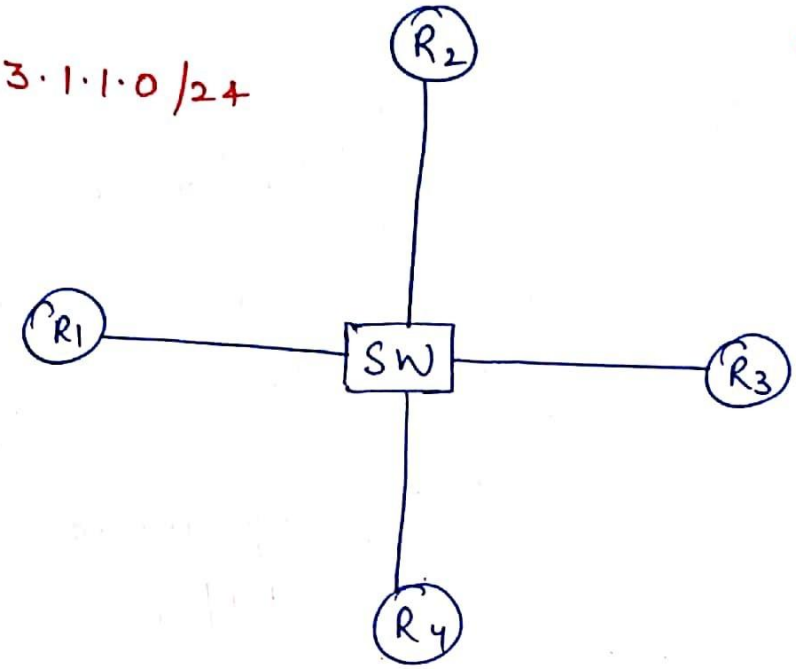
→ Locally Known

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

19/12/2019

Class practical

N/w → 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 the router waits for 40 sec to elect DR & BDR as might be other routers may go live in n/w.

* But if routers gets assigned as DR bieng a lowest ip also then after highest ip go live the already assigned router will stay DR unh'll its dead.

* 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 ↓] Privelege mode.

then enter Yes/No

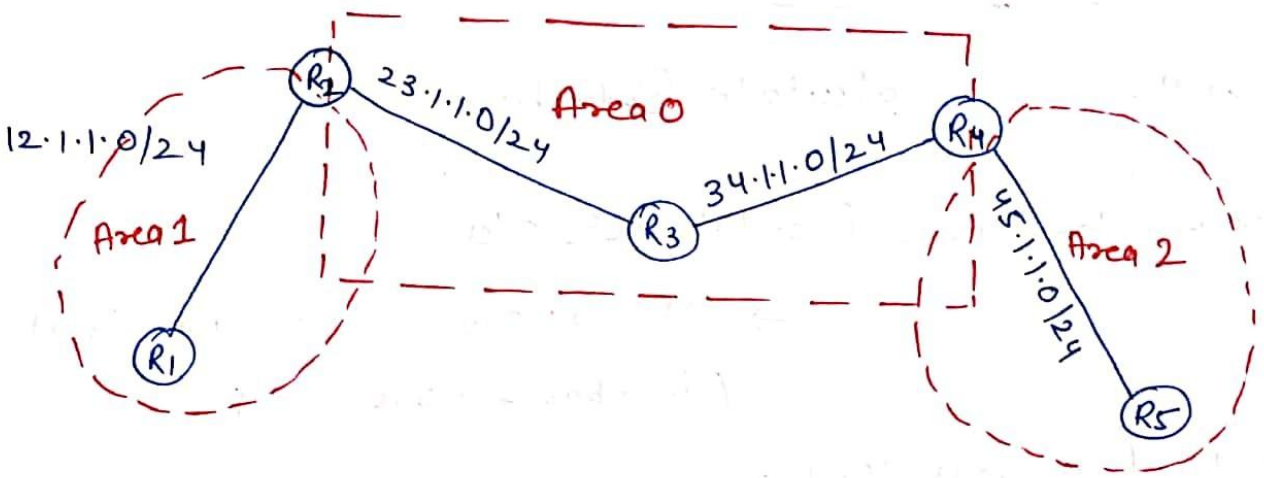
* Manual router id is preferred so we set it up manually above & after reload router id will change to 4.4.4.4

↳ 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 scenario.

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 110/20 or 110/30 for diff routes.
(110 → AD, 20/30 → Metric)

Metric (Cost) = reference B.W / Interface B.W

Reference B.W = 100 mbps by default

↳ 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

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

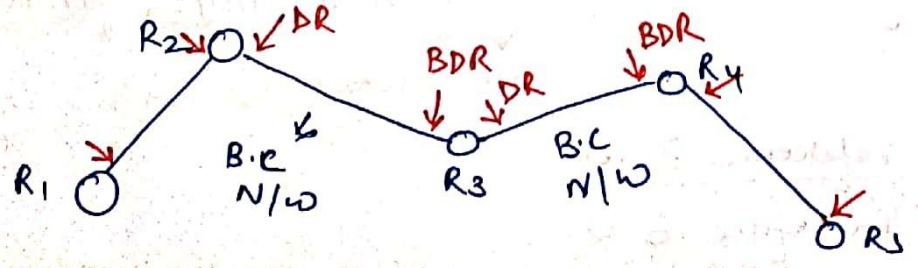
↳ OSPF Maintains 3 types of Tables :-

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 is B.C n/w so it will have its own DR & BDR)

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 adjencies 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

↳ ospf has to get through 7 states in order to become neighbors. :-

① Down: no ospf neighbors detected at this moment.

② Init: Hello packet recieved.

③ Two-way: Own router ID found in recieved Hello packet.

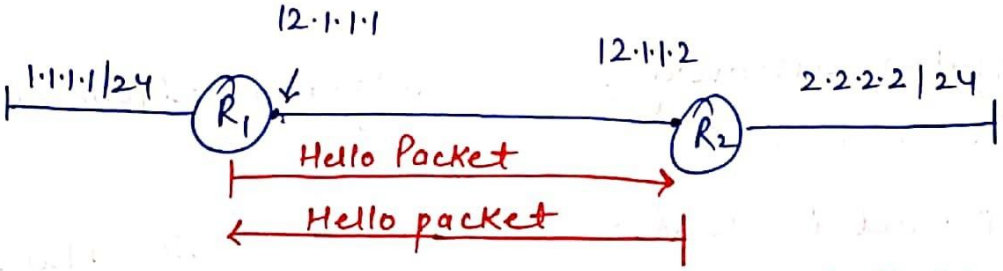
④ Exstart: Master & slave roles determined.

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 adjency.

ex

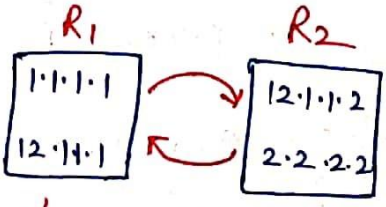


① hello timer = 10 sec
Dead timer = 40 sec

* if suppose R_1 does not send Hello packet the R_2 will hold last sent hello packet for 40 sec & if still not new hello packet recieved then R_2 will consider R_1 dead & neighborship will be lost.

② DBD (Summary of LSR or LSDB)

DBD



③ LSR

LSR

New entry Request

(4) LSU → update regarding request will be sent
LSU ←

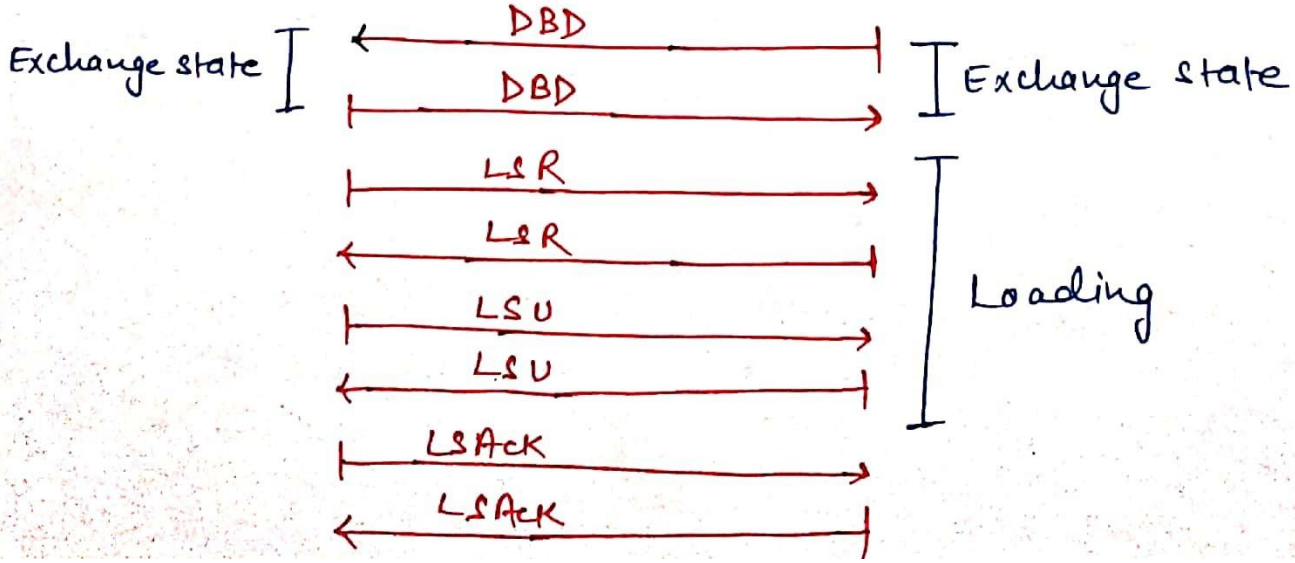
(5) LAck → Ack for updates.
LAck ←

LSA → Link state Advertisement
↳ status of a particular link (Interface)

LSDB → Link state database
↳ Database of LSAs.

LSA timer = 30 minutes = 1800 sec
LSA Deadtimer = 60 minutes = 3600 sec

↳ Routers with lower ip
Master & slave election | ex start state
Here R2
Router with higher id



* Neighbor is just 2 way state & 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)

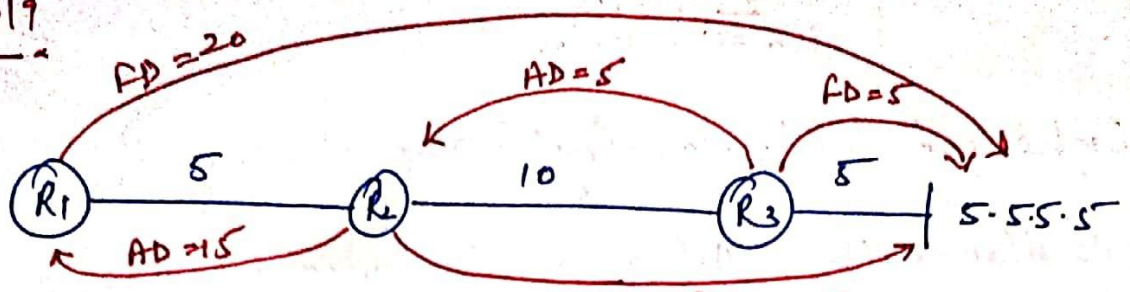
* EIGRP is also called Advance distance Routing protocol and also hybrid routing Protocol
* EIGRP works on protocol no. 88
* EIGRP uses Dual algo. for best path calculation.
* Multicast address — 224.0.0.10
* Metric - Bandwidth, load, Delay, Reliability & MTU.
* Supports both equal & unequal cost load balancing.
* By default, EIGRP supports 100 hops but we can extend it to up to 255.
* Classless Routing Protocol.

We will not find B.W, load, delay, etc. 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 FD = 5 for 5.5.5.5 n/w

& AD = 5 will be advertised to R_2

So for R_2 FD = 5 + 10 = 15

& AD = 15 will be advertised to R_1

So for R_1 FD = 20

Advertised Distance :- How far the dest^n 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 < Feasible distance of Successor.

↳ EIGRP maintains 3 Tables :-

① Neighbor Table → for neighbors entry

② Topology Table → for Best path and Backup path entery

③ Global Routing Table → only for Best path entery.

23/12/2019

↳ Syntax

Router (Config) # router _ eigrp _ As.no

no - auto_summary

Network _ own n/w address

_____

Exit

As no. (Autonomous System no.)

↳ 16 bit identity (1-65,535)

↳ Globally Known

↳ Group of Routers 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

23/12/2019

↳ :

↳ 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 → Bandwidth.

ex Metric = (i) $\frac{10^7}{105} = 10^2 = 100$

BW checked By command

(ii) Cumulative delay $= \frac{300}{10} = 30$

3 interfaces with 100 delay in each = 300

So $[100 + 30] = 130 \times 256$

$= 33280$

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

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

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

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

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 Dest"
- Direction (Exit Interface)

* This type of routing is totally dependent on neighboring router updates only & does not Know about topology beyond neighbor

* In Contrast in the link state routing protocol router is aware of the topology like how it looks. (Map).

24/12/2019

↳ 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

→ (a) Standard ACL
→ (b) Extended ACL

② Named ACL

→ (a) Standard ACL
→ (b) 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)

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

↳ to allow any n/w except

cmd# int _ fo/o

ip _ access-group _ 1 _ out/in

↳ Based on incoming / Outgoing interface.

exit

cmd# show _ access-lists

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

cmd# no _ access-list _1

↳ to delete access list

• 24/12/2019

cmd# access-list _1_ deny _ 192.168.1.0 _ 0.0.0.255

↓ we use wildcard mask to block any subnet.

access-list _1_ permit _any

int_f0/0

ip_access-group_1_out

↳ 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

* By default implicit deny statement 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
Source Dest"

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
eq_80
↓
to indicate the http protocol

cmd # access-list_100_permit_udp_host_192.168.1.3_host_192.168.3.3
eq 53
↓
To ~~block~~ allow dns service.

↳ NAT (Network Address Translation)

* Main function of NAT is to enable private IP 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

↓

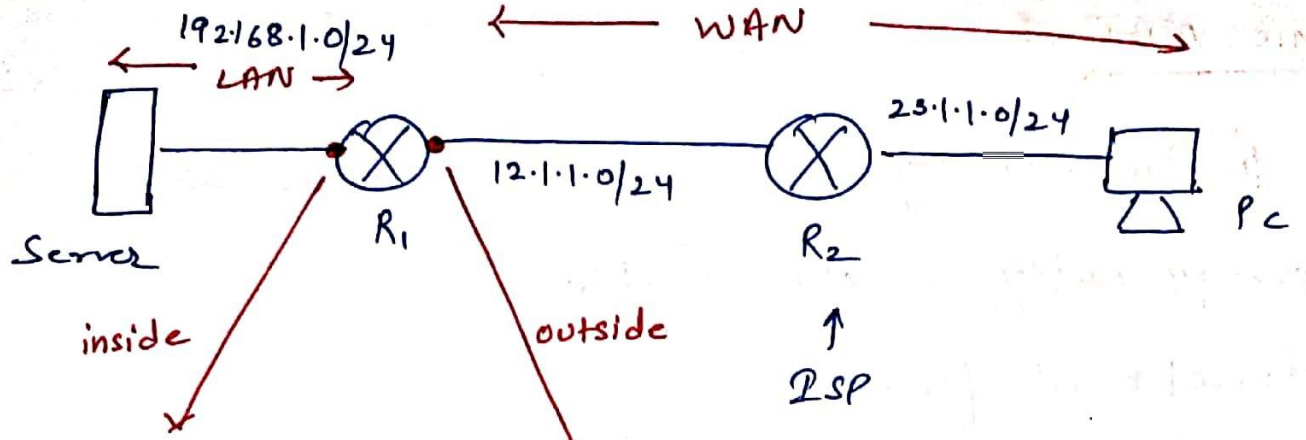
Permanent Entry in NAT Table

↓

Bidirectional flow.

① 31/12/2019

LECTURE-23



Int_f0/0
ip_nat_inside
ex

Int_Se0/0/0
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.

↳ Dynamic NAT :-

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

* 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 ① internal/private network.

② We need to define ip nat pool to define public ip range

③ Define NAT rule and integrate ACL and ip pool.

Commands :-

① {
Int_ Fo/0
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 netmask 255.255.255.(?
} (3) pool

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

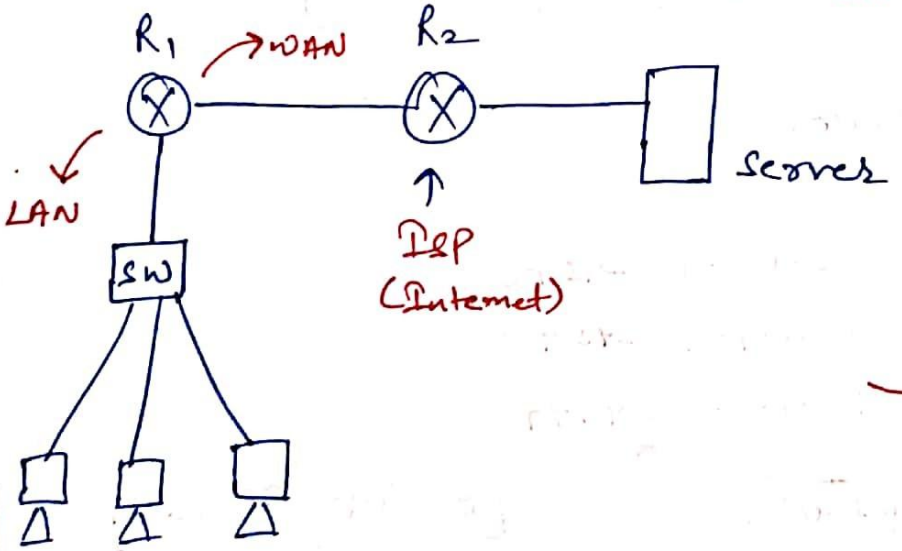
show ip nat translation

↳ to check NAT Table

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

clear ip nat translation

↳ to clear NAT Table



↗ for above Configuration

31/12/2019

④ ↳ NAT - PAT (Port Address Translation).

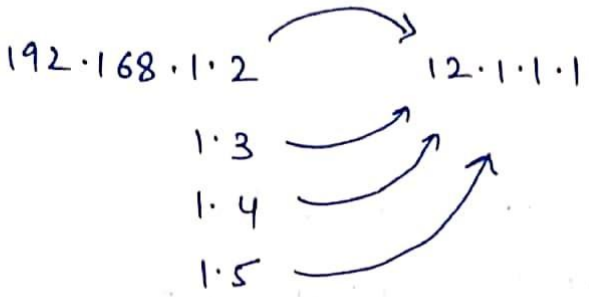
① Used for end Users

② Unidirectional flow

③ Temporary entery in NAT Table.

④ One to many NAT

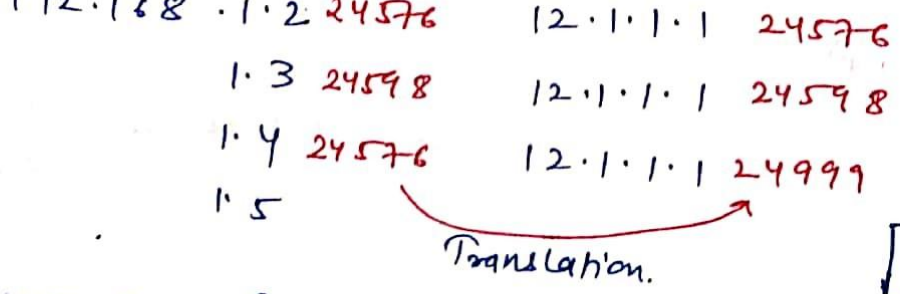
Ex



* if we bind this single public ip with each private ip then the traffic which 12.1.1.1 will bring would not be ~~difficult~~ to decide that which ip it is for so we possible

Here NAT-PAT in Rescue.

Ex



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

int_ fo/o

ip_nat_inside

ex

int_ se/o/o/o

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

(underscore)

ip_nat_inside_source_list_1_pool_null_admin_overload

(underscore)

with overload Cmd Dynamic NAT behaviour converts into NAT-PAT

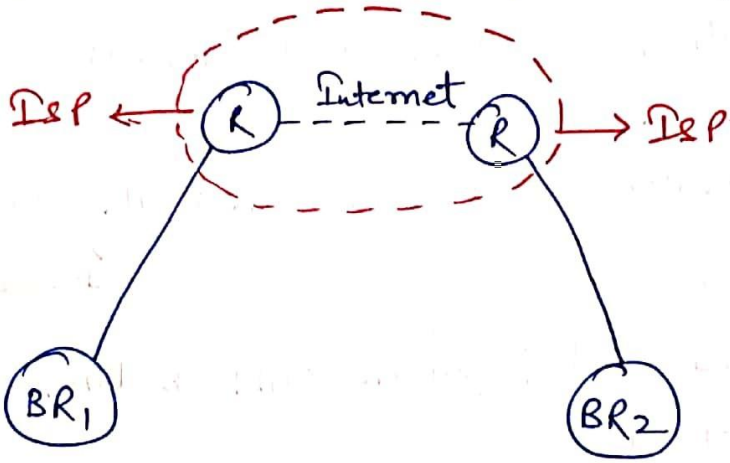
↳ GRE TUNNEL

① L-3 Protocol

② Works on protocol no. 47

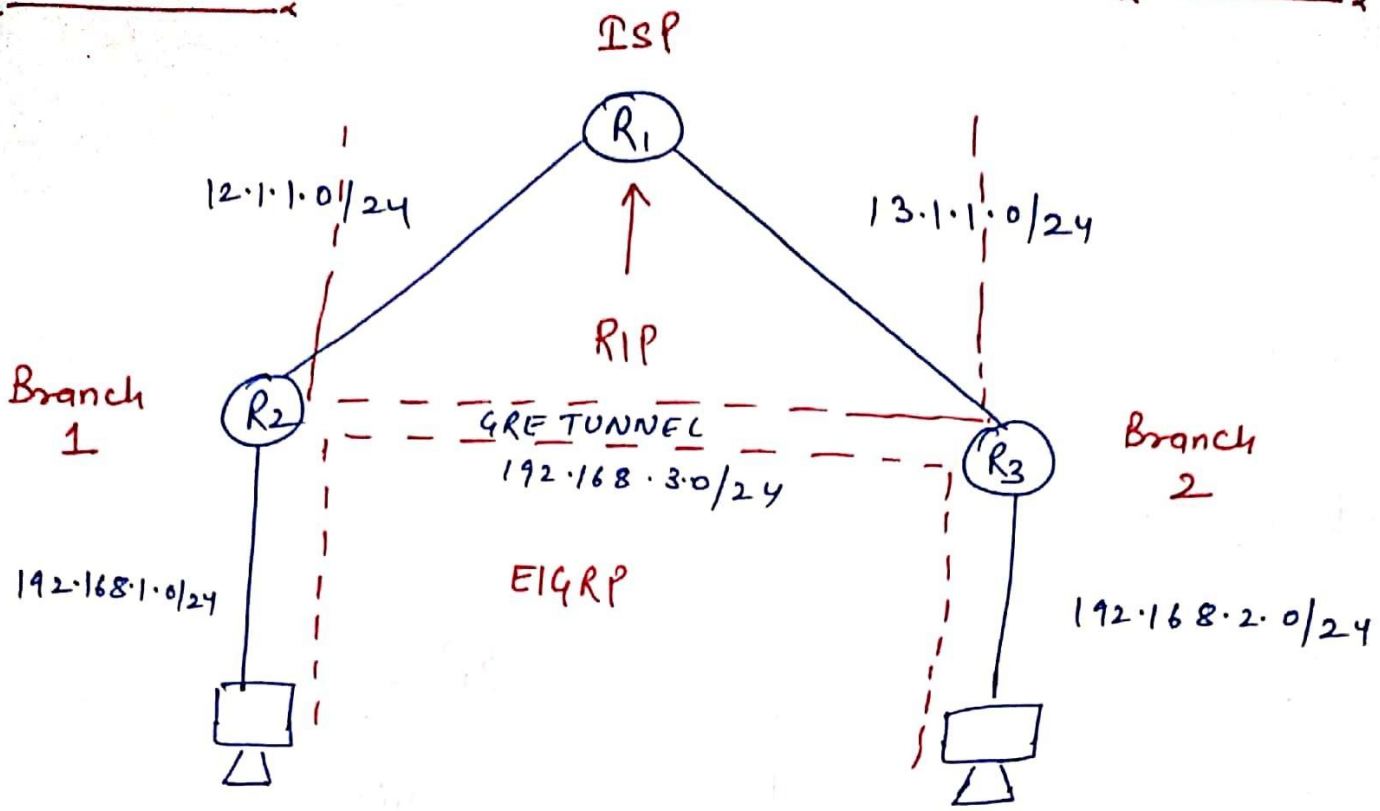
③ GRE adds 24 bytes of extra overhead to the original packet.

VPN :- logical channel over public N/W [Not Security] → (IPsec + VPN)



* Earlier Physical link was used b/w Branches which was costly & required high maintanence 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

R2 # interface _ tunnel _ 0

ip _ address _ 192.168.3.1 _ 255.255.255.0

tunnel _ source _ Serial 0/0/0 → In clt we use int no. → In real device use ip only for source also

tunnel _ Destination _ 13.1.1.2

exit.

R3 # Same as R2 & just change ip, source & destination as per network.

Inner Packet → 4 bytes → 20 bytes.

S.IP	G	S.IP
192.168.1.2	R	12.1.1.1
D.IP	E	D.IP
192.168.2.2		13.1.1.2

Outer packet

↳ IPv6 —:

IPv4	IPv6
(1) 32 bit	(1) 128 bit
(2) written in Decimal format	(2) written in hexadecimal format
(3) 4 Octet (8 bit each)	(3) 8 groups (each 16 bit)
(4) Octet are separated with dot (.)	(4) Groups are separated with colon (:)
(5) Five classes A, B, C, D, E	(5) No classes
(6) Has N/w bits & host bits according classes	(6) It has mostly fixed N/w bits (64 bits) & Host bits (64 bits)
(7) It uses subnet mask	(7) It does not use subnet mask. It uses prefix

01/01/2020

↳ 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
(4 hex per group; 16 bit)

1 hex = 4 bit

4 hex = 16 bit (1 Group)

8 Group × 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 dual stack.

④ 01/01/2020

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) 01/01/2020

↳ Some of the Prefixes are reserved -:

(1) 2000::/3 - Global Unicast

(2) FD: Unique local → if ip starts with then 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_fo/o
no_shut
IPv6_add_2001::2/64
exit

show_ipv6_int_brief

* for ip use IPv6 everywhere for IPv6

↳ EUI 64 (Extended Unique identifier)

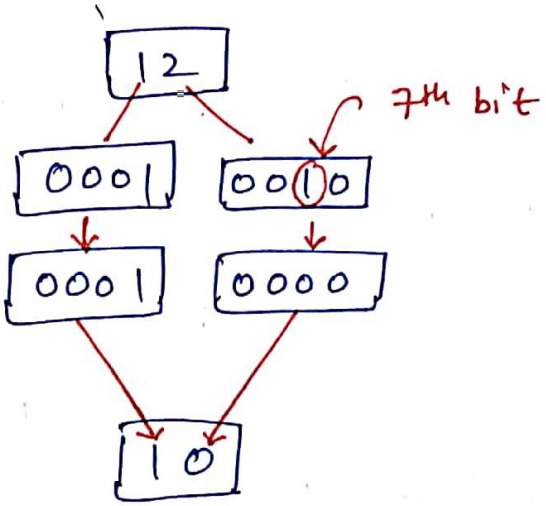
*It is used to configure id as it can be used to make the routers generate its own interface id. instead of typing 128 bit Complete ip ourselves. [it generates interface id of fix length 64 bit]

* 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

MAC ID | 1234 | 5678 | abcd |

Interface Id | 1234 | 56ff | ff78 | abcd |

Now we invert the 7th 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 7th bit of the interface Id.

```
cmd # int_fo1o
    # no_shut
    # ipv6_add_2000::/64_cui 64
    # exit
```

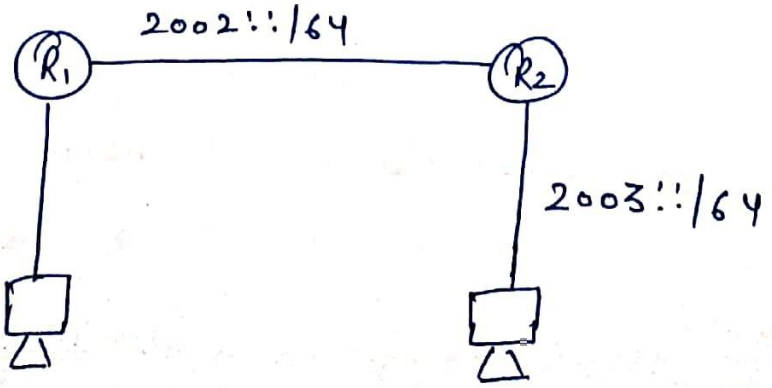
* Each device that has ipV6 enabled will automatically generate a link local address. These addresses are unicast can't be routed and are only used with Subnet, which is why they are called link-local.

* 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 adjancies and also as the next hop for routes.

* Multicast address - EIGRP uses ff02::A & OSPF uses ff02::5 & ff02::6.

ex for Default/static Routing.



* Routing command are exactly same just use ipv6 inplace 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 n/w with Network commands in ipv4 by in ipv6 we enable network on the interface itself

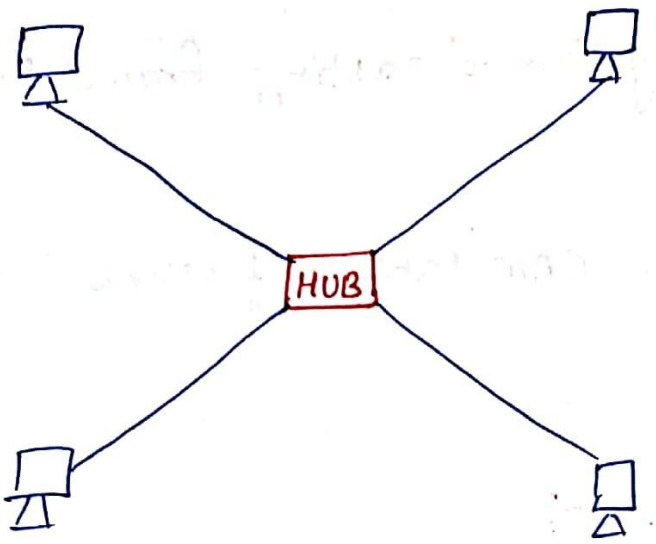
* Also we need to give router id manually in ipv6.

```
R1# ipv6 _ unicast-routing
  # ipv6 _ router _ ospf _ 1
  # router-id _ 2.2..2.2
  # int _ fo/0
  # ipv6 _ ospf _ 1 _ area _ 0
```

→ Same for other interfaces & other routers.

↳ SWITCHING :-

ex



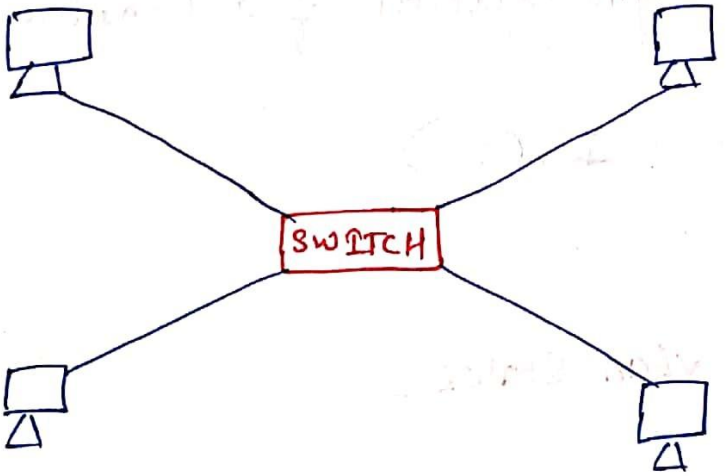
(1) Single collision domain

(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 Address Memory).
* CAM table maintains the database of MAC address, port id, vlan id etc.
* So basically it is a smarter device as compared to HUB.

show_mac-address-table

↳ to show mac address table

* After resolving ARP by broadcasting frame switch show 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 administrator 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

(5) 02/01/2020

↳ VLAN Ranges :-

① Standard vlan Range :-

Range from 1 — 1005

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_ fo/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.

cmd # int_range _ fa0/12, fa 0/15, fa 0/18

switchport_access_vlan_21

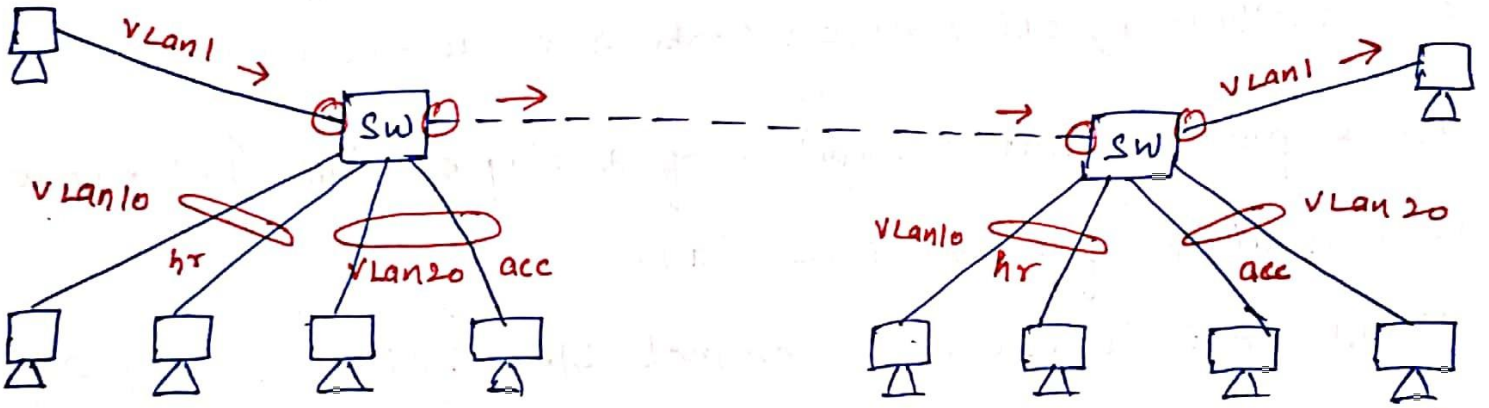
exit

↳ if we write 21 in place of 10 then it will see that no vlan 21 exist so it will create one.

① LECTURE-26

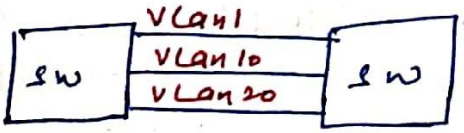
03/01/2020

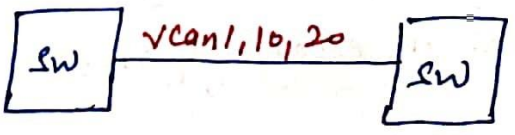
* Different vlan should have different network, we can give same but then it would not be differentiated while communicating b/w different vlan.
* By default we can communicate ~~between~~ in intra vlan (same vlan) only.
* We would be needing routing or L3 switch to communicate b/w different vlan.



* vlan1 will ping vlan1 on other switch as Broadcast domain is same & freame will travel through link.

But in case of other vlans ping will not work as the Broadcast domain will be different. So now 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~~ create for vlan group.

03/01/2020

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 (sw to sw) & b/w switch & router.

↳ Vlan Frame-Tagging -:

*when vlans span multiple switches, a mechanism is required to identify which vlan a frame belong 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.

(3) 03/1/2020

↳ 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 disregared ISL-tagged frames as being oversized & drop the frame.

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

(2) IEEE 802.1Q or refferred to as dot1Q is an industry-standared frame-tagging protocol.

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

* 802.1Q embeds a 4byte 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.

↳ Configuring interface as a trunk :-

```
# int_ fo/6
# switchport_ trunk_ encapsulation_ dot1Q
# Switchport_ mode_ trunk
```

Switch – 2960, 2950 } L2 Switch

SW – 3750, 3550, 3560, 3850, 6500, 6800, 4 } L3 Switch

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

```
# show_ int_ f 0/6 _ 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).

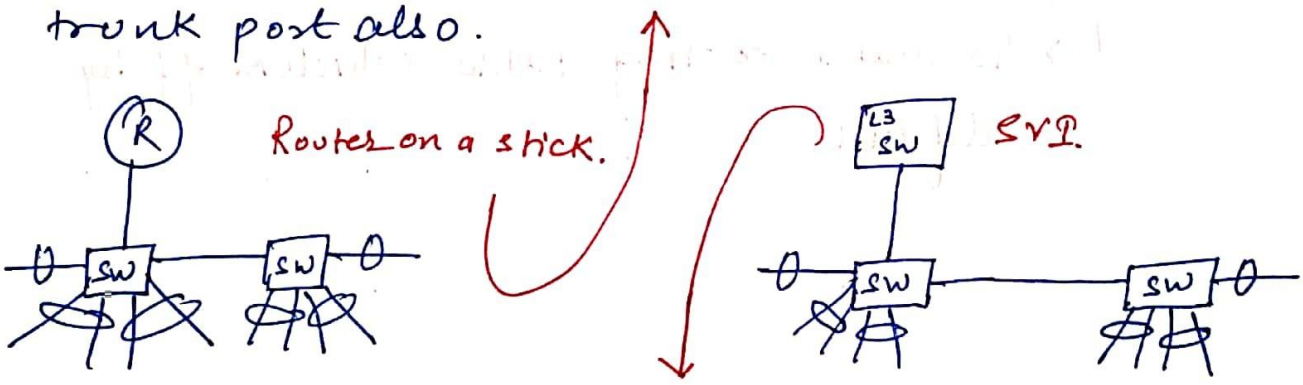
```
Router # int_ fo/0
Cmd
    # no_ shut
    # ex.
    # int_ f 0/0.1   (for vlan 1) sub interface.
    # encapsulation_ dot1Q
    # ip_ add_ 192.168.1.3 _ 255.255.255.0
    # ex.
```

int_fo/0.10 (for vlan 10) Subinterface
encapsulation_dot1Q_10
ip_add_192.168.10.10_255.255.255.0
ex

(* IP add given to router interface will be a gateway)

int_fo/0.20 (for vlan 20) sub interface.
encapsulation_dot1Q_20
ip_add_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
ex
vlan_20
ex

[vlan1 created by default]

int_fo/1
switchport_trunk_encapsulation_dot1Q
switchport_mode_trunk
ex
int_vlan1
no_shut

{shut by default for security purpose}

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 vlan 20).

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 ⟷ Manual trunk

  Manual trunk ⟷ Dynamic Desirable

  Manual trunk ⟷ Dynamic auto

  Dynamic desirable ⟷ Dynamic Desirable

  Dynamic desirable ⟷ 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 manually configure trunk ports to avoid DTP.

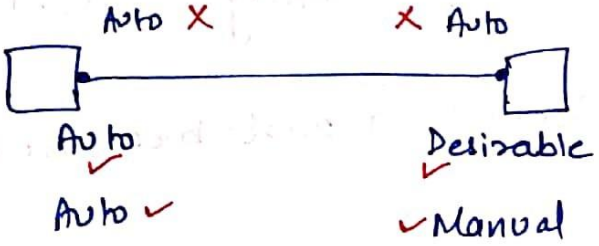
→ negotiation error. DTP is also vulnerable to vlan spoofing attacks.

* Switchport mode trunk → Send & Recive 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

ext

* Switch ↔ end device (Access port)

Switch ↔ Switch (trunk port).

int _ f _ 0/2 → Interface connecting to switch.

switchport _ trunk _ encapsulation _ Dot 1Q

Switchport _ mode _ trunk

switchport _ nonegotiate → to turn off DTP packets

ex.

08/11/2020

↳ 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 →

(i) Allowed to create and delete vlan.

(ii) VTP Server, distributes vlan database from one switch to another switch in a domain

2. VTP transparent :-

(i) Allowed to create & delete vlan

(ii) it maintains its own local database → [Avoid flooding of data from one sw to other sw]

(iii) Acts as a transparent switch, when it recieves vlan database from vtp server and forward to the other switch in a domain.

(3) VTP client :-

(1) Not allowed to create & delete vlan.

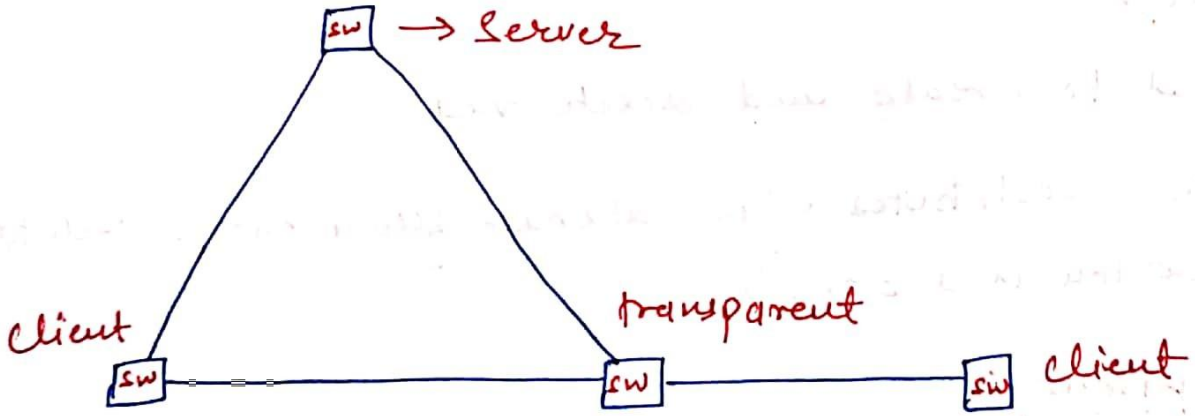
(2) It forwards its vlan database to other switch in a domain.

↳ VTP versions :-

(1) VTP version 1 } Only supports standard vlan range
2 } (1-1005)

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 (Prefered).

change your domain name.

↳ Port Security :-

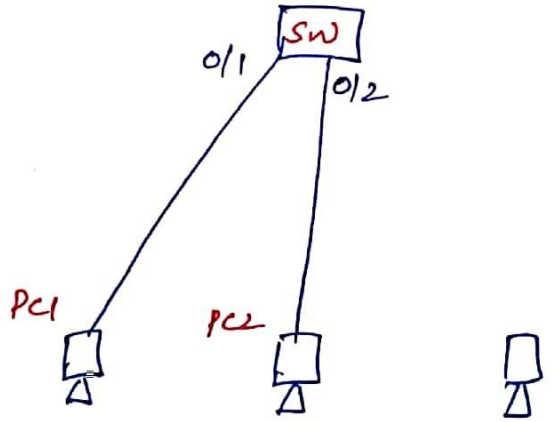
① L-2 Security feature.

② Used to allow limited no. of MAC-address on a interface (MAC-Binding).

③ By default disabled on cisco switches.

④ Protect Switched nw from MAC flooding attack.

* Port security is always enabled on the port to which end device is connected.



(two mac-add are allowed in table)

int _ f_0/2

Switch(port) _ port-Security_maximum_2

Switch(port) _ port-Security_mac-address_sticky (Automatic)

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

Cmd# show_port-Security

show_port-Security_int_ fo/2

* Error Disabled state.

07/01/2020

LECTURE-28

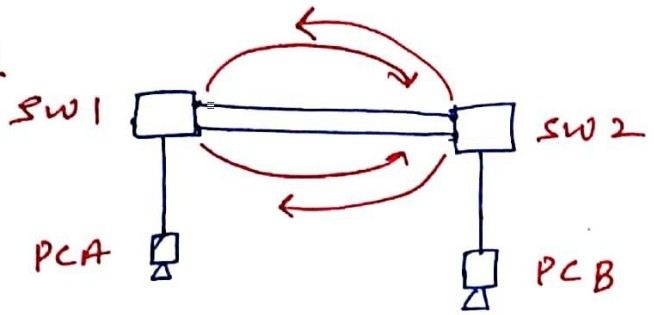
↳ SPANNING TREE PROTOCOL (STP).

① L-2 Protocol

② By Default, enabled on Cisco switches.

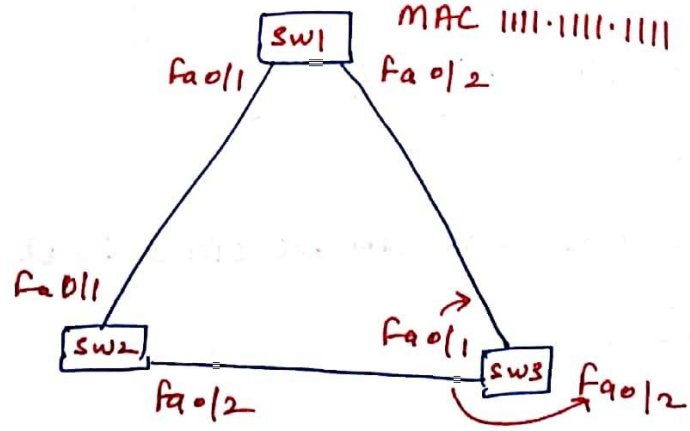
③ used to prevent (avoid) loop in switched n/w.

ex1



* 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



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 recieve best BPDU (Bridge protocol Data Unit).

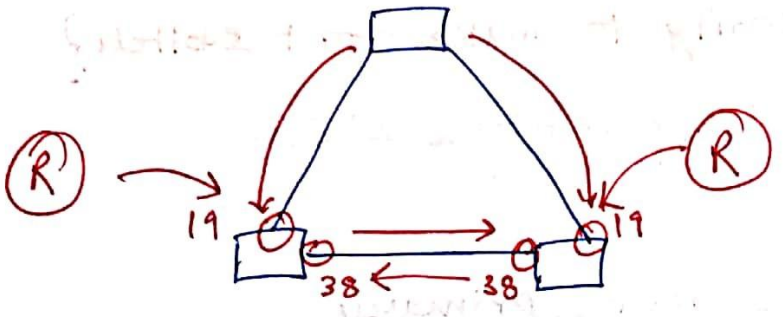
* Root port is decided by Bw(link) & Cost.

eth	100
Fast eth	19
Gig	4
10 Gig	2

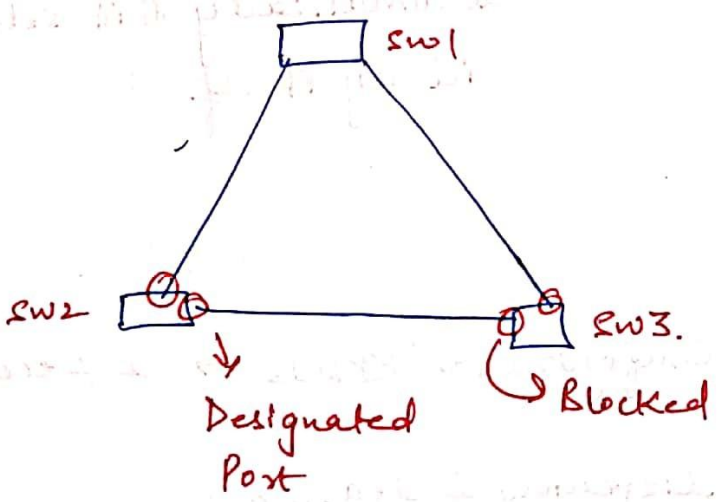
07/01/2020

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

(Root port is on non-root bridge) ~~root ex~~.



Step 3 : Designated Port :-



* SW2 has designated port as it has best BPDU & Rec 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 forwarding state. → 15 seconds.

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.

07/1/2020

↳ STP States and Port Activity

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

↳ Port Fast

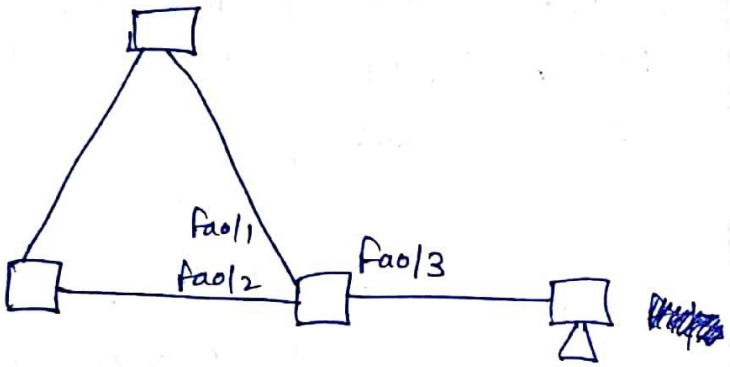
* Port fast is enabled on access port (Port Connecting to end device)
* Improves convergence time and directly put your interface into forwarding state.

int_f_0/3

switchport_mode_access

spanning-tree_Portfast (should be on access port with end devices).

ex



↳ BPDU Guard :-

int_f_0/3

switchport_mode_access

spanning-tree_bpduguard_enable

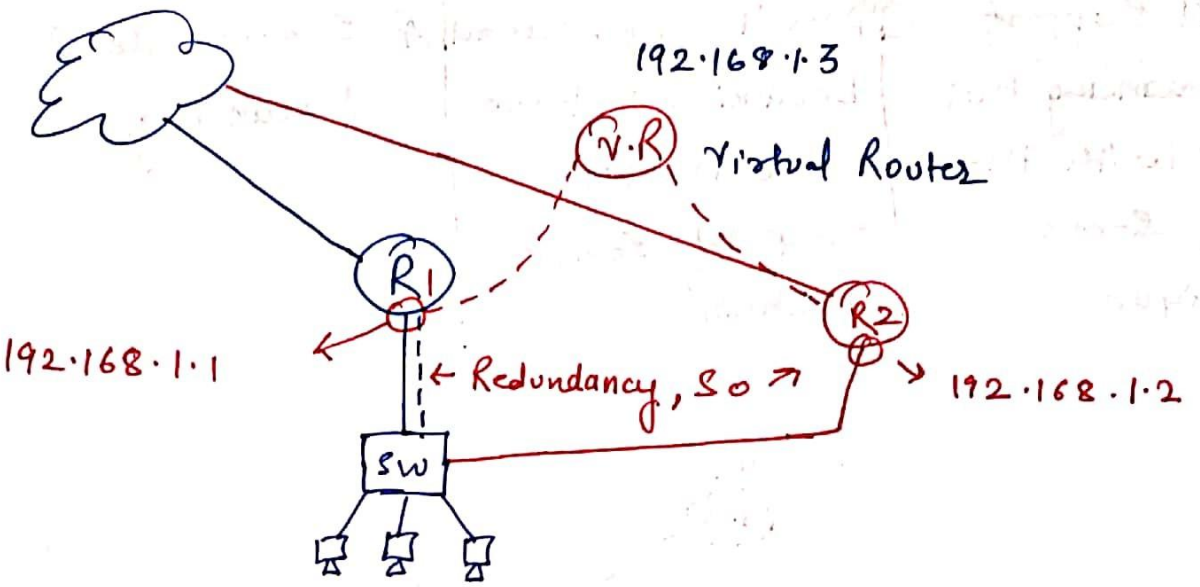
ex.

*

 08/01/2020

LECTURE -29

fHRP (First hop redundancy Protocol)



* R_1 → Active Router.

  R_2 → standby Router

  R_3 → It is created with the help of R_1 & R_2

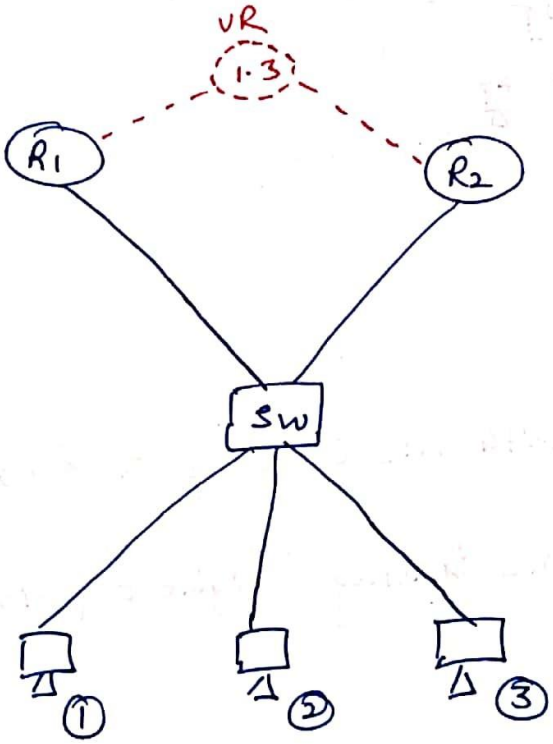
* Active Router is the one having highest priority

*

↳ To create virtual Routers we have 3 protocols :-

HSRP	VRRP	GLBP
① Hot standby Routing Protocol	① Virtual Router redundancy Protocol	① Gateway load Balancing Protocol.
② Cisco proprietary Protocol.	② open standard	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.



(R1) # Give ip
standby _ 1 _ ip _ 192.168.1.3

(R2) # Same

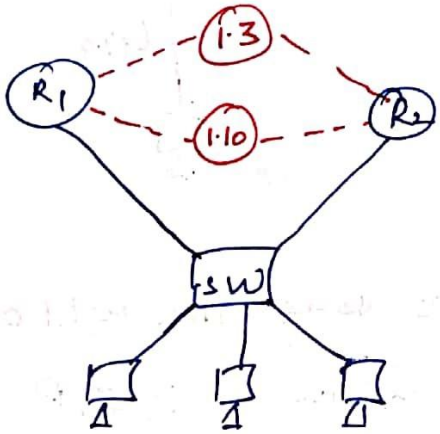
↓ Group no. should be same in both routers

* if R1 becomes dead then R2 will be active & to make R1 active we need to increase priority with preempt command.

(R1) # standby – 1 – priority – 180
standby – 1 – preempt
} to make R1 active from standby

* Priority then highest ip will be compared for active routers but normally routers configured first will be active.

ex



(R1) & R2 Same as Before

then (R1) # standby – 2 – ip – 192.168.1.6
standby – 2 – priority – 60
standby – 2 – preempt

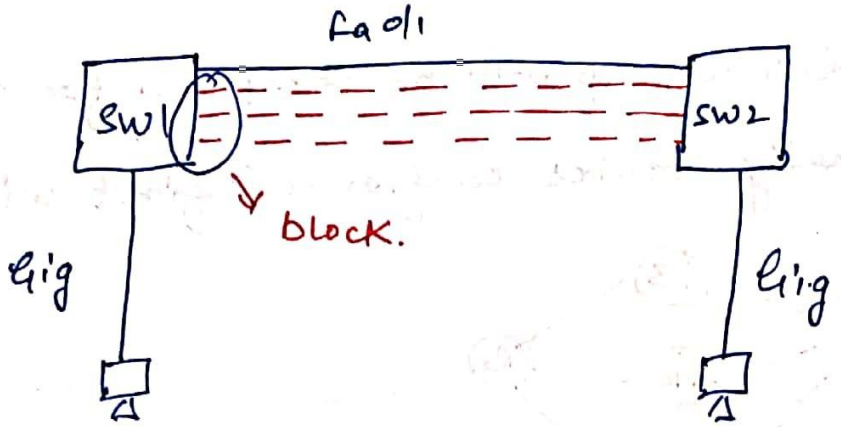
(R2) # standby – 2 – ip – 192.168.1.6
#

Cmd # show – standby

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

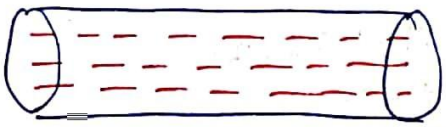
08/01/2020

↳ Etherchannel (link aggregation.



Since Gig > Fa so traffic congestion will occur.

* So we can add multiple links but STP will block all the redundant port then 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 there 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).

SW1 # Int_range_fa_0/1-6
channel-Protocol_pagp
channel-group_1_mode_desirable
ex
int_port-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.

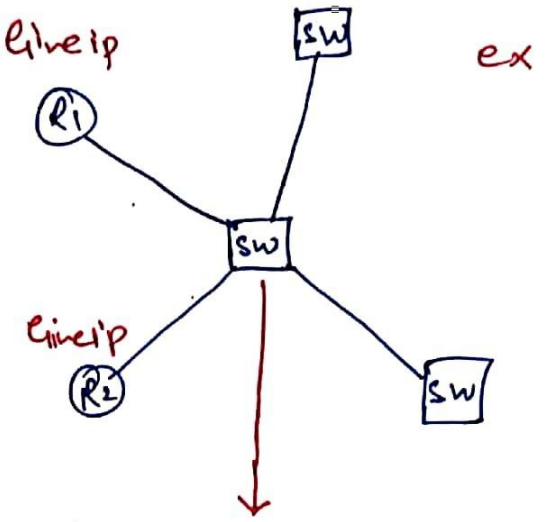
} For both Switches

↳ 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 neighbors. 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 transit through it to reach other autonomous system. Ex ISP (As a transmit 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.

(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 naighborship.
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

09/1/2020

cmd# show_ip_bgp_summary

↳ Bgp neighbor table.

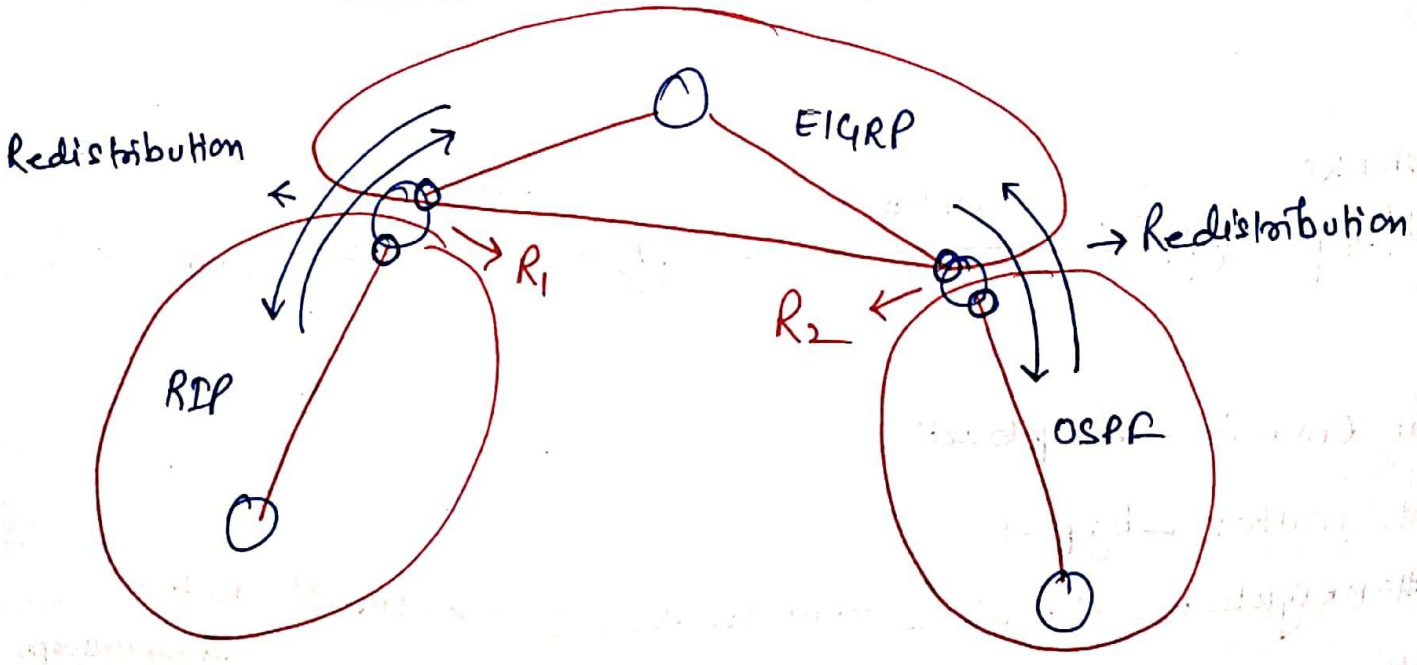
cmd# show_ip_bgp

↳ Bgp table

cmd# show_ip_route_bgp

↳ for Bgp routing table.

↳ REDISTRIBUTION :-



(R1) # After enabling Rip & Eigrp proceed for redistribution
router_rip
redistribute_eigrp_1_metric_2
ex

↳ Rip metric

(R2) # router_eigrp_1
redistribute_rip_metric_1_1_1_1_1

↳ eigrp metric.

(R2) # router_ospf_1

redistribute_eigrp_1_?Subnet

↳ we use Subnet instead of metric because

ex

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.