

Ways to connect →

- ① SSH or Telnet (insecure)
- ② console connection

- Initially, There is No IP Address to the cisco device that means we cannot use ssh as first connection. This is where console connection comes into place.

— Console connection —

- 1 side DB9 other RJ45
- * not a ethernet cable



— New devices by cisco has

- USB to mini-USB

Levels

- ① User Level → >
- ② privilege level aka enable mode → #
going back to user level disable
- ③ Global config → conf + → (config) #

* $\text{ctrl} + \text{A}$ to move to start line.

*** if you are using commands from different level at a diff port you can just you do at the start

* iOS is not case sensitive

To exist from upper level directly to base level you can use end command.

* pipe option to search

ex. `sh run | ?`

 ↑ case sensitive after that

* + copy running-config to start
+ copy run start

* sh start

* Backup the config

Tools like → Cisco client info

* —

Copy run ?

ex. copy run flash:my-config
sh flash

• Erase

erase start

old cisco → wr erase

copy flash:my-config start

Layer 4 - Transport Layer

- Session Multiplexing supported.

Email-25

port numbers are used to determine

What traffic is for which Appⁿ is traffic
for

** * stateful firewall keep track of return traffic using port
numbers. ex. if we send traffic from 80 → 1500 port
When we get the traffic back
it will be from 1500 → 80 port that way firewall
understands return traffic.

Two protocols of L4

TCP

① Connection oriented
data can be sent bi-directional

UDP

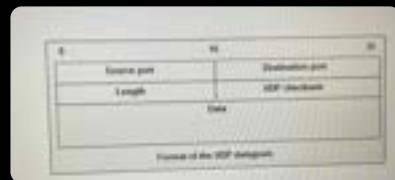
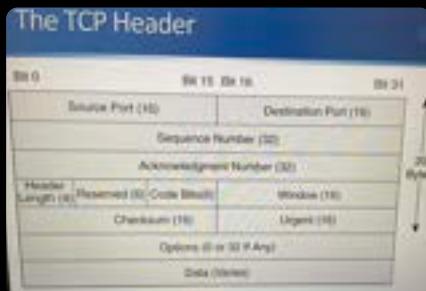
① Not

② TCP carries out sequences to ensure segments are processed in the correct order and none are missing

- ③ Reliable connection
- ④ Slower
- ⑤ Perform flow control

② does not

- ③ Not
- ④ faster
- ⑤ does not
- ⑥ Real-time - voice, video



- Applications and ports
- FTP - 21
 - SSH - 22
 - Telnet - 23
 - HTTP - 80
 - HTTPS - 443

TFTP - 69

SNMP - 161

TCP & UDP

DNS - 53

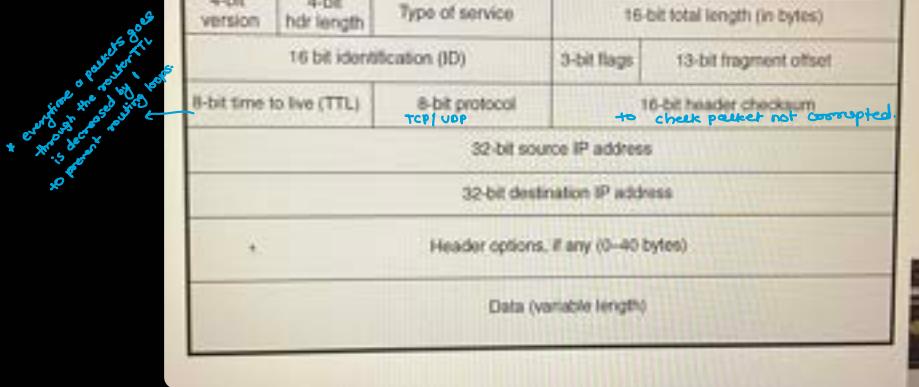
L3

Layer 3 - Network Layer.

- Responsible for routing packets to their destination for QoS
- Best known protocol → IP
- IP is connectionless protocol with no acknowledgements
- Layer 3 includes ICMP (Internet Control Message Protocol) and IPsec.
- Why smaller subnets?
→ Improves performance & security

→ IPv4/IPv6
reference

→ Used for QoS can prioritize user traffic to server or other device



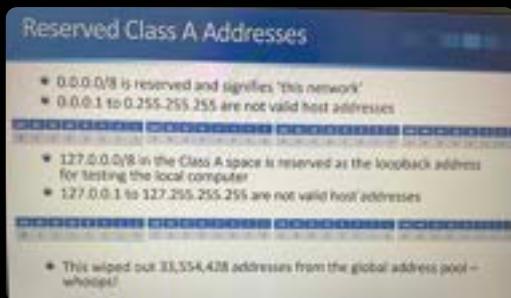
* Routers do not forward the Broadcast traffic.

Multicast → We send single copy to multiple Hosts.
ex. Radio station.

- Learn DIFF classes of IP Add.
class A - class D.

- IANA — Assigns the IP Addresses to a companies

- class A - 1.0.0.0 to 126.0.0.0 → Private — 10.0.0.0 — 10.255.255.255
- * 0.0.0.0/8 ← is Reserved IP Address



* * To test if TCP/IP is working or not we use Loopback Address
127.0.0.1

* * Not limited to that we can ping any IP in the range of 127.x.x.x
To check the TCP/IP

* Class B - /16 — Private — 172.16.0.0 — 172.31.255.255
128.0.0.0 — 191.255.0.0 /16

* Class C - Private → 192.168.0.0 — 192.168.255.255
192.0.0.0 — 223.255.255.0 /24

- * Class D -
 - reserved for multicast Address
- ** - The first four high-order bits in class D Address are always set to binary 1110
- Address are not allocated to hosts and there is no default subnet mask.
- * - valid address range from 224.0.0.0 — 239.255.255.255.
1110 ← starting range
- ** Learn How multicast works.

Class E

- Reserved for experimental & future use

Class	First Octet	Default Subnet Mask	
		Slash	Dot-Decimal
A	1 - 126	/8	255.0.0.0
B	128 - 191	/16	255.255.0.0
C	192 - 223	/24	255.255.255.0
D	224 - 239		
E	240 - 255		

* Classless Benefits

- ① More efficient use of IP Addresses
- ② Reduce in size of ISP's route table and takes up less memory

— * * — Calculating the number of Subnets

ex. We have class C with /28 that means we borrowed 4 bits from host bits

so $2^4 = \underline{16}$ available subnets

ex-2

class B with /28

$$16 + \underline{12} = 28$$

$2^{12} = 4096$ available subnets.

* * *

To calculate number of hosts

- $2^{\text{host bits}} - 2$ (since 2 IPs are reserved)

- ex. class C | 2⁸ subnet then we have ⁴ bits left for hosts.
host bits =
 $2^4 - 2 = 14$

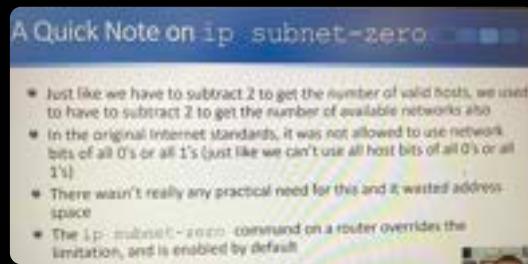
- ex. 2 class B | 2⁸ subnet then we have 4 bits left

Host bits =

$$2^4 = 16 - 2 = \underline{14}$$

*

IP - Subnet - zero



example : -

- Subnets 200.15.10.0/24
class C network | 31
 $24 - 31 = 7$

— $2^7 = 128$ subnets available which accommodates

— $2^1 = 2$ subnets each

that means the addresses will be

$\left\{ \begin{array}{l} 200.15.10.0 \text{ to } 200.15.10.1 \\ 200.15.10.2 \text{ to } 200.15.10.3 \\ \text{etc. to} \\ 200.15.10.254 \text{ to } 200.15.10.255 \end{array} \right.$

* *

/31 → then what about the network & broadcast address

→ /31 breaks the standard rules of IP Addressing.

They are supported on cisco routers for point to point links. → Which doesn't require broadcast

and network address.

$$200 \cdot 15 \cdot 10 \cdot 0 / 24 \rightarrow /30 - \underline{255 \cdot 255 \cdot 255 \cdot 252}$$

- Subnets = $2^6 \rightarrow 64$
- $\rightarrow \underline{64 \text{ available subnets}}$
- # of host in each subnet

$$\begin{array}{r} /24 + \underline{\downarrow} \\ \begin{array}{r} 11111100 \\ \hline 6 \\ 128 + 64 + 32 + 16 + 8 + 4 \\ = 252 \end{array} \end{array}$$

$$2^2 - 2 = 2 \text{ bits / subnet}$$

$200 \cdot 15 \cdot 10 \cdot 0 / 30$ — range will be

$$\begin{aligned} 200 \cdot 15 \cdot 10 \cdot 1 & - 200 \cdot 15 \cdot 10 \cdot 2 (\text{network.0} - \text{broadcast.3}) \\ \cdot 5 & - \cdot 6 (\text{network.4} - \text{broadcast.7}) \end{aligned}$$

- * * — /30 and /31 both accommodate 2 host per subnet
- * /31 support 128 subnets, /30 supports 64
- /31 useful if you need to maximize use of your add. space
- /30 more standard and commonly used.

ex. 3 — class C $200 \cdot 15 \cdot 10 \cdot 0 / 24 \rightarrow 200 \cdot 15 \cdot 10 \cdot 0 / 29$

$$200 \cdot 15 \cdot 10 \cdot 0 / 29 \rightarrow 255 \cdot 255 \cdot 255 \cdot 248$$

- Subnets = $2^5 = 32$ available subnets
- # hosts = $2^{\text{host bits}} - 2$
 - $\rightarrow 2^3 - 2$
 - $= 8 - 2 = 6$ no. of host / subnet

— VLSM — Variable length subnet mask.

$$198 \cdot 22 \cdot 45 \cdot 173 / 26$$

$$\rightarrow 255 \cdot 255 \cdot 255 \cdot 192$$

subnets available —

$$2^2 = \underline{4}$$

host each subnets

$$2^6 - 2 = 64 - 2 = \underline{\underline{62}}$$

* * # 198.22.45.173/26 → What is network address?

- We have /26 network so only first two bits from that network

198.22.45.173/26
→ $\boxed{10} \ 101101$
 $2^7 \ 2^6 \ \dots \ 2^1$

so network

198.22.45.128 → is the network Address

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

200.15.10.0/27
→ 255.255.255.224

200.15.10.0 — 31
32 — 64

$$\# \text{ of subnets} = 2^3 = \underline{\underline{8}}$$

$2^4 = 16 - 2 = 14$ host → $32 - 4 = 28$
subset will be /28

$$\text{Subnets} = 2^4 = 16 \text{ subnets}$$

200.15.10.0/28

200.15.10.0 — 200.15.10.15
· 16 — · 32
· 32 — · 48
· 64 —

$$2^4 - 2 = 16 - 2 = \underline{\underline{14}} \text{ host}$$

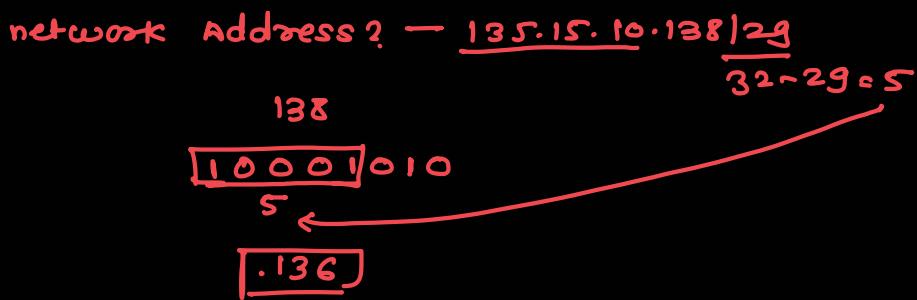
 $\underline{\underline{128}}$

— 135.15.0.0/16

12^9
→ 255.255.255.248

— # Subnets available
 $2^{13} = \underline{\underline{8192}}$

hosts per subnet
= $2^3 = 8 - 2 = 6$ / subnet



class A \rightarrow 60.0.0.0/8
 subnet mask \rightarrow 255.255.255.240
 $24+4 = \underline{\underline{128}}$

Ans \rightarrow 60.0.0.0/28

- # available subnet =
 $18 - 128 = 20$

$2^{20} = 1,048,576 \rightarrow$ Available subnets

- # host available per subnet

$2^{\text{hostbits}} - 2 = 2^4 = \underline{16}$ host including network & broadcast

60.0.0.0/28

— 60.0.0.0 — 60.0.0.15
 .16 — .32

60.15.10.75/28
 network Add — $32 - 28 = 4$

75
01001011

\rightarrow 60.15.10.64/28 \rightarrow network Address

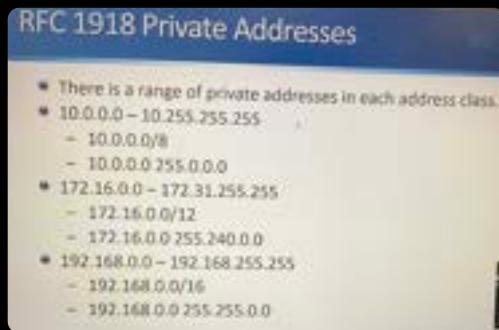
- # available subnets — $24 - 28 = \underline{\underline{4}}$

$2^4 = \underline{16}$ available subnets

host
 $2^{\text{hostbits}} - 2$

$2^4 = \underline{16}$ host / subnet including 2

— Private IP Address range
RFC - 1918 → Private IP Add.



- + — There is not a seamless migration path from IPV4 to IPV6
 - NAT was implemented as a temp. workaround to mitigate the lack of IPV4 Addresses.
- commonly
 - | 24 for end hosts
 - | 30 for point to point
 - | 32 for Loopbacks

L2 —

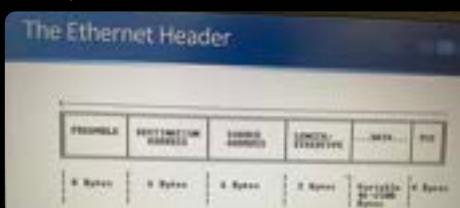
Layer - 2 - Data Link layer frames

- Ethernet is the L2 medium used on LAN.

L2 protocols —

- ① Ethernet
- ② PPP — point to point

.....



MAC Address — 48 bit hexa decimal

To get a MAC on Routers

Show interface brief

Layers - I Physical Layer

- Connections

- Coaxial - no longer used

- Twisted pair → single mode - longer distance, higher bandwidth expensive.

- Fiber cable → multi mode

- Wireless

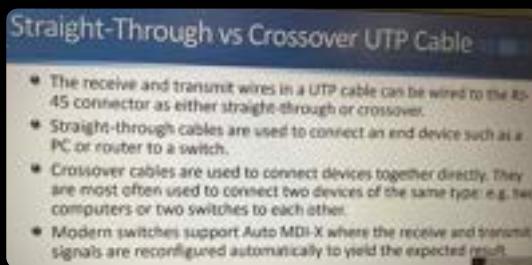
- Copper UTP (Unshielded TP) commonly used to connect desktop computer to switches.

1Gig
Cat5 →

- RJ-45 max length 100m.

10Gig
CAT 6 →

- UTP - 250Hz



PoE - Power over Ethernet

To send power over the Ethernet
ex. Telephone.

- PoE switches are used to power multiple PoE devices

Section II -

- Hubs always operate in half-duplex mode
- All host shares the same collision domain - only one device can transmit at a time.
method to detect recover from collision → CSMA/CD

Hubs are layer 1

- Not Mac aware

Whenever frame is received it is flooded out all ports apart from the one it was received on.

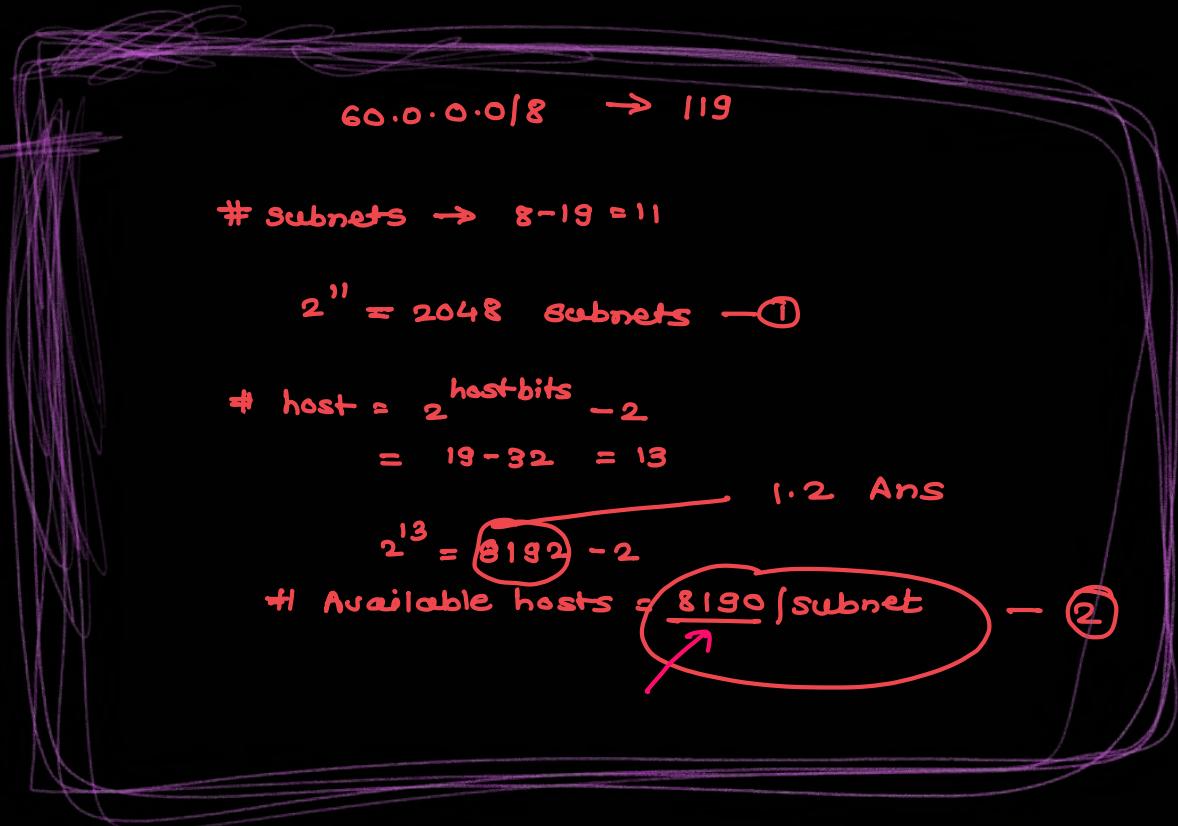
Switches - layer 2

- MAC aware

- Routers

- Two different networks are connected via routers
- Required to send traffic from one subnet to another.
- L3 device
 - also operate at L2+L1 and will typically have awareness up to Layer 7.

Students
456



Routers can route traffic bet'n networks
switch —|— Hosts

Routers supports many types of interfaces

- Ethernet
- ISDN
- ADSL
- Serial
- Console
- Auxiliary

Layer 3 switches

can be used to route traffic within the network with diff subnet. However to communicate with internet we still need routers.

— Cisco Firewall ASA — Adaptive Security Appliance

— DNS requests are sent using UDP port 53

DNS * — To set Cisco router as a DNS server



ARP — ARP Maps the destination Mac add to dest IP add

— Section 14 — Router & switch basics

— Setting IP on Router

→ In Router interface mode

R1 — Interface fe0/0

ip add 192.168.0.1 255.255.255.0
no shutdown

* — A Layer 2 switch is not IP routing aware

— It does however support a single IP address for management

** — for default VLAN1 the IP & subnet mask is configured on the switched virtual interface (SVI)

— Default gateway also needs to be configured to allow connectivity to other subnets.

• — RJ — Stands for register jack.

*** — Speed of internet is measured in bits not bytes

ex. kbps, mbps

bit - 0 or 1

bytes - 8 bits = 1 byte

• Data on harddrive is measured in bytes

Speed	Common Name	IEEE Standard	Informal Name	Maximum Length
10 Mbps	Ethernet	802.3i	10BASE-T	100 m
100 Mbps	Fast Ethernet	802.3u	100BASE-T	100 m
1 Gbps	Gigabit Ethernet	802.3ab	1000BASE-T	100 m
10 Gbps	10 Gig Ethernet	802.3an	10GBASE-T	100 m

All through the straight through cable
PC sends data from pin 142 (TX - 1,2)
receives data from pin 346 (RX - 3,6)

• Router

sends data from pin 142 (TX - 1,2)
receives data from pin 346 (RX - 3,6)

• Switch

sends data from pin 346 (Tx 3,6)
receives data from pin 142 (Rx 1,2)

* * * —

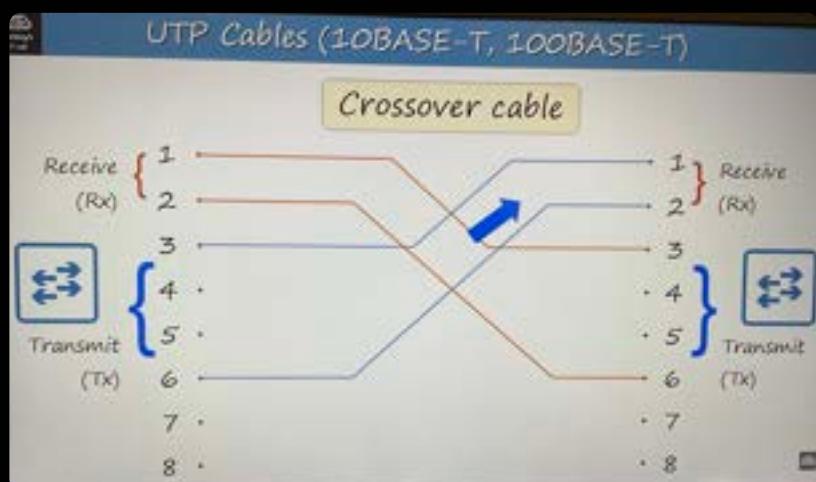
Router - to - router conn' —

— or Router - to - PC - conn' —

— cross-over cables are used to connect R to R or SW to SW or R to P

so

connection will be like this.



Device Type	Transmit (Tx) Pins	Receive (Rx) Pins
Router	1 and 2	3 and 6
Firewall	1 and 2	3 and 6
PC	1 and 2	3 and 6
Switch	3 and 6	1 and 2

.....

However, Newer devices comes with Auto-MDIx features which automatically adjust itself either straight & cross connection it will take of sending info.

... -

for 1000BaseT or 10GBaseT all 8 ports are used.

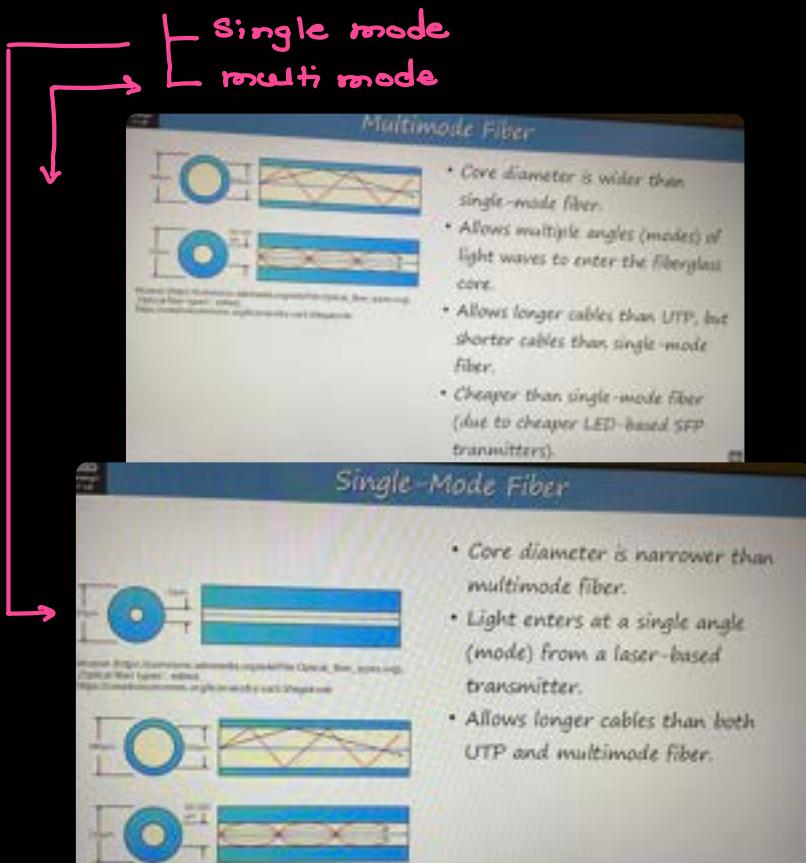
— for this 1000BaseT & 10GBaseT each pair of wire bidirectional.

old copper wire limitations

① Limited to 100m.

— New Technology wires.

connector — — SFP (small form-factor pluggable) Transceiver
Wires — fiber optic cables



- fiber optics standards

Informal Name	IEEE Standard	Speed	Cable Type	Maximum Length
1000BASE-LX	802.3z	1 Gbps	Multimode or Single-Mode	550 m (MM) 5 km (SM)
10GBASE-SR	802.3ae	10 Gbps	Multimode	400 m
10GBASE-LR	802.3ae	10 Gbps	Single-Mode	10 km
10GBASE-ER	802.3ae	10 Gbps	Single-Mode	30 km

Day - 3

Layer 7 function

- Identifying communication partners
- Synchronizing communication

L6 - Presentation Layer - Encryption of data

- Transport Layer provides Host-to-Host comm
- Application Layer provides process-to-process comm

Day 4 -

Basic Encryption & Password set

① Password set —

Go to global config mode

(config) # Service Password CCNA_Pass

R1 # Show running config
→ It startup config

*** To Save config inside a startup

- { ① Write
- ② write memory
- ③ copy running-config startup-config

*** (config) # service password-encryption

To disable → no service password-encryption

If you enable service password-encryption...

- * current passwords will be encrypted.
- * future passwords will be encrypted.
- * the enable secret will not be effected.

If you disable service password-encryption...

- * current passwords will not be decrypted.
- * future passwords will not be encrypted.
- * the enable secret will not be effected.

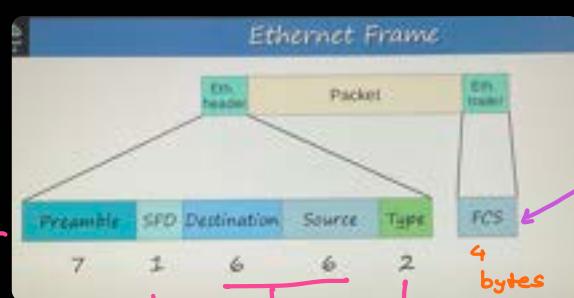
> = user exec mode

= privileged exec mode

(config) # = global config mode

(config) # run privileged-exec-level cmd
→ executes privileged level command from global config mode.

Day 5 — — Ethernet LAN switching



allows devices to synchronize their receiver clocks

frame check sequence
greater than 1500 = Type /
IPV4 or IPV6

less than 1500 means indicating length of packet
6 byte = (6x8) = 48 bit — MAC Addresses

→ start frame delimiter
 length 1 byte (8bits) - 10101011
 • Marks the end of the preamble & beginning of the payload

Total size = 26 bytes

Mac Addresses also known as Burned-in-Address (BIA)

- Mac addresses on cisco switches stay for 5 minutes if no activity for that address then removed from the tables.
- Dynamically learned frames → when switch gets new mac from PC's
- * --- Unknown unicast frames when switch doesn't know the destination mac → switch just floods the network with that frame

Day 6 -

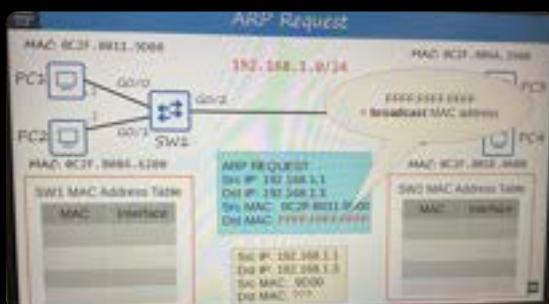
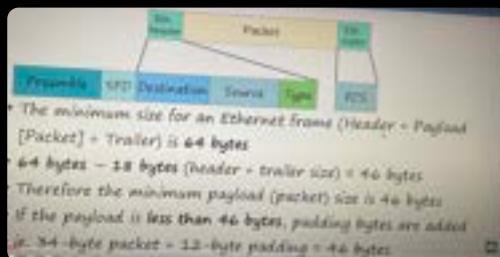
Preamble and SFD are not considered part of the Eth. header so size

$$6+6+2+4 = 18 \text{ bytes}$$

↑

minimum size for frame

64 bytes



PC1# show arp
 SW1# show mac address table
 SW1# clear mac address-table dynamic
 SW1# clear mac address-table dynamic address 02cf.ABCD.0211
clear for interface
 SW1# clear mac address-table dynamic interface Gi0/0

ARP - To get the Mac

- ① ARP request
- ② ARP reply

Ping - ICMP echo request
ICMP echo reply

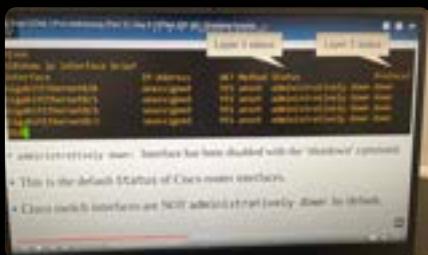
• Router Interfaces

Day 7 - IP Addressing & classes

- Broadcast Mac address will be FFF.FFF.FFF.
ex. 192.168.1.255
- DST. Mac address will be — FFF.FFF.FFF.

Cisco switches interface is not down by default like router

Day 8



...

show ip interface brief

* show interfaces g0/0

↑ This will have mac Address listed twice becz sometime we change the address virtually

* show interfaces description

— To set a description — int g0/0

description description_Here

Day 9 -

Switches interface

— Here we can see that by default switch interfaces are not in the down state

show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
Vlan 1	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	up	up
FastEthernet0/4	unassigned	YES	unset	up	up
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	down	down
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down

Switch interface is up by default to the connected interfaces

These are not administratively down like routers
Normal down means they are not connected to any device.

show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
Router interfaces have the shutdown command applied by default =will be in the administratively down/down state by default					
Switch interfaces do NOT have the 'shutdown' command applied by default =will be in the up/up state if connected to another device					
OR in the down/down state if not connected to another device					
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down

Show interfaces status

SW1 # conf t

SW1 (config) # int 0/1

speed 100 } manually setting speed & duplex

duplex ? }

duplex full }

sh int status

description # to R1

Configuring interface speed and duplex					
Port	Name	Status	Vlan	Duplex	Speed
Fa0/1	RR to R1 RR	connected	1	full	100/10/100BaseTX
Fa0/2		connected	trunk	a-full	a-100/10/100BaseTX
Fa0/3		connected	1	a-full	a-100/10/100BaseTX
Fa0/4		connected	1	a-full	a-100/10/100BaseTX
Fa0/5		notconnect	1	auto	auto 10/100BaseTX
Fa0/6		notconnect	1	auto	auto 10/100BaseTX
Fa0/7		notconnect	1	auto	auto 10/100BaseTX
Fa0/8		notconnect	1	auto	auto 10/100BaseTX
Fa0/9		notconnect	1	auto	auto 10/100BaseTX
Fa0/10		notconnect	1	auto	auto 10/100BaseTX
Fa0/11		notconnect	1	auto	auto 10/100BaseTX
Fa0/12		notconnect	1	auto	auto 10/100BaseTX

→ Manually changed

(Config) # interface range Fa0/5 - 20
description # not in use #
shutdown

- To prevent anyone from directly connecting a device to a sw.

Make sure to shutdown it.

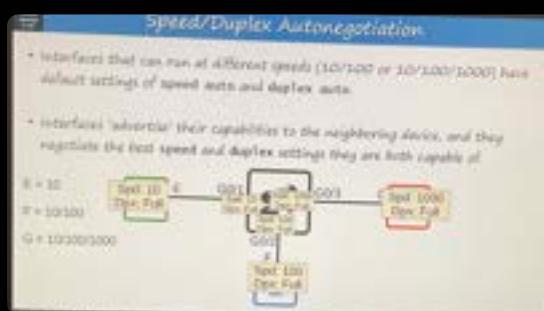
- To select particular interfaces

```
sw1(config)# int range f0/5 - 0/6, 0/9 - 0/11
```

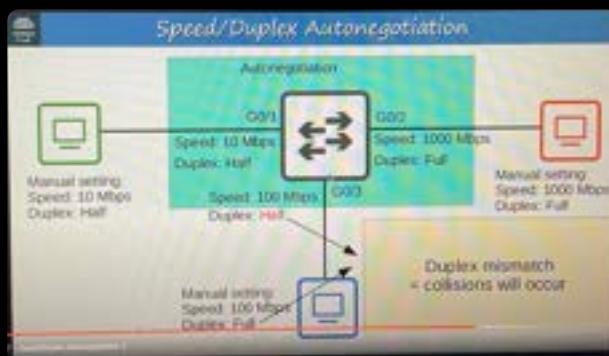
- ...
 - To deal with collisions in half-duplex situation CSMA/CD is used

CSMA/CD

- Carrier Sense Multiple Access with Collision Detection
 - Speed/Duplex autonegotiation



ex. 2 Where autonegotiation is only active on sw1



* show interfaces or show interfaces f0/1

```
Interface Errors
269 packets input, 71059 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
7290 packets output, 429875 bytes, 0 underruns
0 output errors, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

- Runts: Frames that are smaller than the minimum frame size (64 bytes)
- Giants: Frames that are larger than the maximum frame size (1518 bytes)
- CRC: Frames that failed the CRC check (in the Ethernet FCS trailer)
- Frame: Frames that have an incorrect format (due to an error)
- Input errors: Total of various counters, such as the above four
- Output errors: Frames the switch tried to send, but failed due to an error

- ...
 - Autonegotiation can only able to sense and match speed not the duplex if there is mismatch betn duplex mode collision will occur

Quiz Question 5

Switch 1 is trying to autonegotiate interface speed settings with Switch 2. However, autonegotiation is disabled on Switch 2's interface. Switch 2's interface is configured with a speed of 100 Mbps and full duplex. What speed and duplex settings will Switch 1 use, assuming it succeeds in sensing the speed?

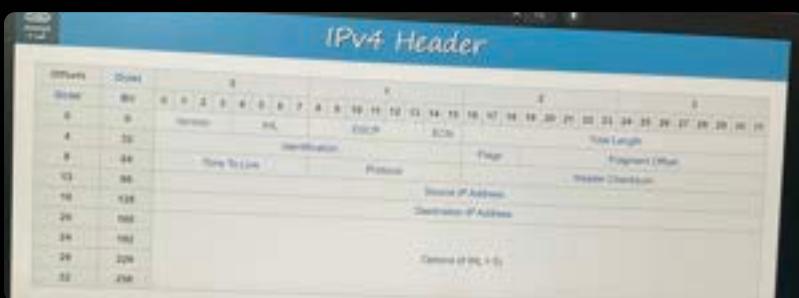
- Speed: 100 Mbps, Duplex: Full
- Speed: 100 Mbps, Duplex: Half
- Speed: 10 Mbps, Duplex: Full
- Speed: 10 Mbps, Duplex: Half

This because duplex mode cannot be sensed so to default default is

Speed	mode
10	Half
100	Half
1000	full

Day 10 -

IPv4 Header



1. Version - 4 bytes

- Used to identify version of IP used

- IPv4 (0100)
- IPv6 (0110)

2. IHL - Internet Header Length

Length - 4 bytes

- minimum value in this is 5 ($5 \times 4 = 20$ bytes)

- maximum is 15 ($15 \times 4 = 60$ bytes)

- minimum IPv4 Header Length = 20 bytes
max —————— 11 —————— = 60 bytes

3. DSCP - Differentiated Services Code Point

Length - 6 bit

Used for QoS (Quality of Service)

QoS - used to prioritize the delay sensitive data.

4. ECN - Explicit Congestion Notification
length : 2 bits

Provides end-to-end notification of network congestion without dropping packets

5. Total length - 16 bits
- Indicates the total length of the packet (L3 header + L4 seg)
- minimum value of 20 bytes
- max of 65k bytes

6. Identification - length 16 bytes
used to identify which packet the fragment belongs to
- packets are fragmented if larger than the MTU (Maximum transmission unit)
MTU is usually 1500 bytes.

7. Flags - 3 bit
control and identify fragments
Bit 0: Reserved, always set to 0
Bit 1: Don't fragment (DF) used to indicate a packet that should not be fragmented
Bit 2: More fragments (MF bit), set to 1 if there are more fragments in the packet, set to 0 for the last fragment

8. Fragment offset
- used to indicate the position of the fragment within the original, unfragmented IP packets
• Allows fragmented packets to be reassembled even if the fragments arrive out of order.

9. Time to Live - 8 bits → max = 255 bit
• A router will drop a packet with a TTL of 0
• Used to prevent infinite loops.
• Each time the packet arrives at a router, the router decreases the TTL by 1.
• Recommended TTL is 64 bytes → When TTL reaches 0 packets are dropped.

10. Protocol — 8 bits

Indicates the Protocol of L4 PDU

- value of 6 — TCP

value of 17 — UDP

value of 1 — ICMP

e.g. — OSPF

11.

- Header checksum — 16 bits

- checksum used to check for errors
in the IPv4 header.

- if both checksums doesn't match that means error has occurred.

12. Src IP — 32 bit

Dst IP — 32 bit

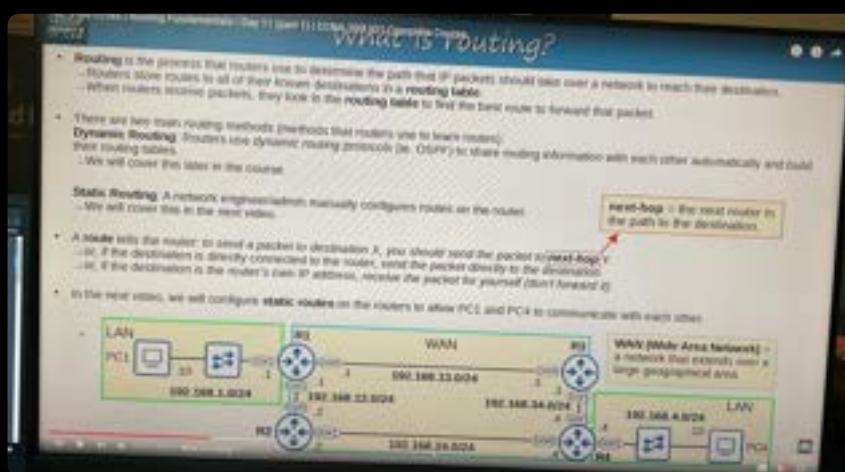
13. Options — 0-320 bits

Rarely used

If IHL > 5 that means options are present

0x → Indicates Hexadecimal

Day 11 — Routing Pt



Routing Table (show ip route)

```

Code: 0 - local; 1 - connected; 2 - static; 3 - RIP; 4 - OSPF; 5 - BGP
0 - OSPF (Ex) OSPF external type 1; 0 - OSPF (Intra-area)
0 - OSPF external type 2; 32 - OSPF NSSA external type 2
0 - OSPF external type 3; 33 - OSPF NSSA external type 3
0 - IS-IS (Ex) IS-IS external, 0 - IS-IS level-1; 12 - IS-IS level-2
0 - IS-IS (Intra-area); 13 - IS-IS level-1; 14 - IS-IS level-2
0 - OSPF (Ex) OSPF external, 0 - per-user static route
* - gateway route
+ - Mediated route; S - next hop override; o - overrides since RPF
Gateway of last resort is not set

 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.1.0/24 is directly connected, GigabitEthernet0/2
 192.168.1.1 is the interface
 192.168.1.0/24 is directly connected, GigabitEthernet0/2
 192.168.1.1 is the interface
 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.12.0/24 is directly connected, GigabitEthernet0/3
 192.168.12.1 is the interface
 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.12.0/24 is directly connected, GigabitEthernet0/3
 192.168.12.1 is the interface
 192.168.24.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.24.0/24 is directly connected, GigabitEthernet0/4
 192.168.24.1 is the interface
 192.168.24.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.24.0/24 is directly connected, GigabitEthernet0/4
 192.168.24.1 is the interface

```

The code legend in the output of show ip route lists the different protocols which routers can use to learn routes:
 - 0 - local
 - A route in the active IP address configured on the interface, with a 100 metric
 - C - connected
 - A route in the process the interface is connected to (with the actual metrics configured on the interface)

When you configure an IP address on an interface and enable it with no shutdown, it makes (new) interface will automatically be added to the routing table:
 - a connected route
 - a local route

Connected and Local routes

```

 192.168.1.0/24 is directly connected, 2 subnets, 2 masks
 192.168.1.0/24 is directly connected, GigabitEthernet0/2
 192.168.1.1 is the interface
 192.168.1.0/24 is directly connected, GigabitEthernet0/2
 192.168.1.1 is the interface
 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.12.0/24 is directly connected, GigabitEthernet0/3
 192.168.12.1 is the interface
 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.12.0/24 is directly connected, GigabitEthernet0/3
 192.168.12.1 is the interface
 192.168.24.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.24.0/24 is directly connected, GigabitEthernet0/4
 192.168.24.1 is the interface
 192.168.24.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.24.0/24 is directly connected, GigabitEthernet0/4
 192.168.24.1 is the interface

```

A connected route is a route to the network the interface is connected to:
 - R1's 0/2 is 192.168.1.0/24
 - Network Address: 192.168.1.0/24
 - It provides a route to all hosts in that network (e.g. 192.168.1.1, 192.168.1.2, etc.)
 - If R1 receives "If I want to send a packet to any host in the 192.168.1.0/24 network, I should send it via 0/2"
 - A local route is a route to specify the exact IP address of the interface:
 - 192.168.1.1 means all 32 bits are there, very specific
 - Even though R1's 0/2 is 192.168.1.0/24, the connected route is to 192.168.1.1.
 - If R1 receives "If I receive a packet destined for this IP address, the message is for me!"

Route Selection

```

 192.168.1.0/24 is directly connected, 2 subnets, 2 masks
 192.168.1.0/24 is directly connected, GigabitEthernet0/2
 192.168.1.1 is the interface
 192.168.1.0/24 is directly connected, GigabitEthernet0/2
 192.168.1.1 is the interface
 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.12.0/24 is directly connected, GigabitEthernet0/3
 192.168.12.1 is the interface
 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.12.0/24 is directly connected, GigabitEthernet0/3
 192.168.12.1 is the interface
 192.168.24.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.24.0/24 is directly connected, GigabitEthernet0/4
 192.168.24.1 is the interface
 192.168.24.0/24 is variably subnetted, 2 subnets, 2 masks
 192.168.24.0/24 is directly connected, GigabitEthernet0/4
 192.168.24.1 is the interface

```

When R1 receives a packet destined for 192.168.1.1, it will choose the route to 192.168.1.1/32. R1 will ignore the packet for class, rather than forward it out of 0/2!
 Local route = keep the packet, don't forward

Imp

- A packet destined for 192.168.1.1 is matched by both routes:
 192.168.1.1/32
 192.168.1.1/24
- Which route will R1 use for a packet destined for 192.168.1.1?
 - It will choose the most specific matching route.
- The route to 192.168.1.1/32 includes 256 different IP addresses (192.168.1.1 - 192.168.1.255)
 - The route to 192.168.1.1/24 includes only 1 IP address (192.168.1.1)
 - This route is more specific.
- Most specific matching route = the 192.168.1.1/24 with the longest prefix length!

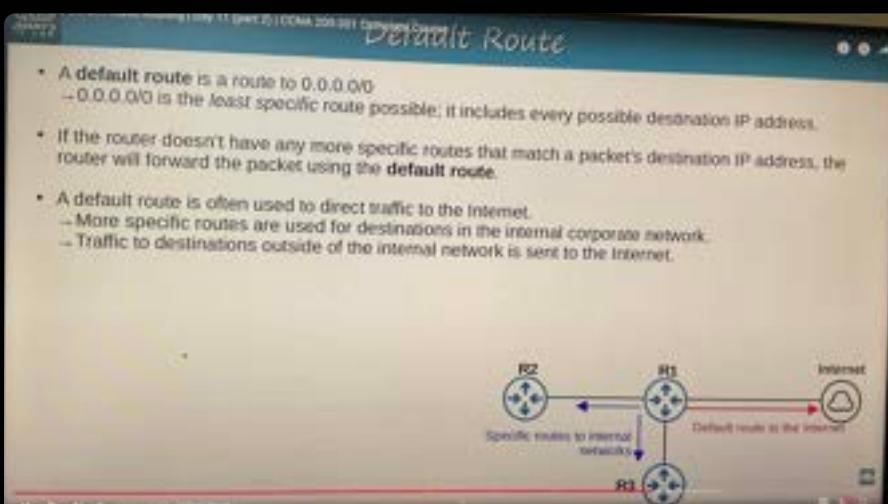
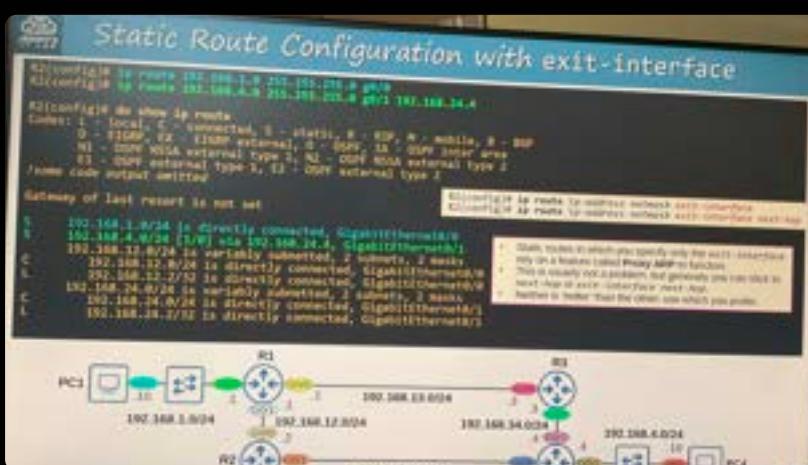
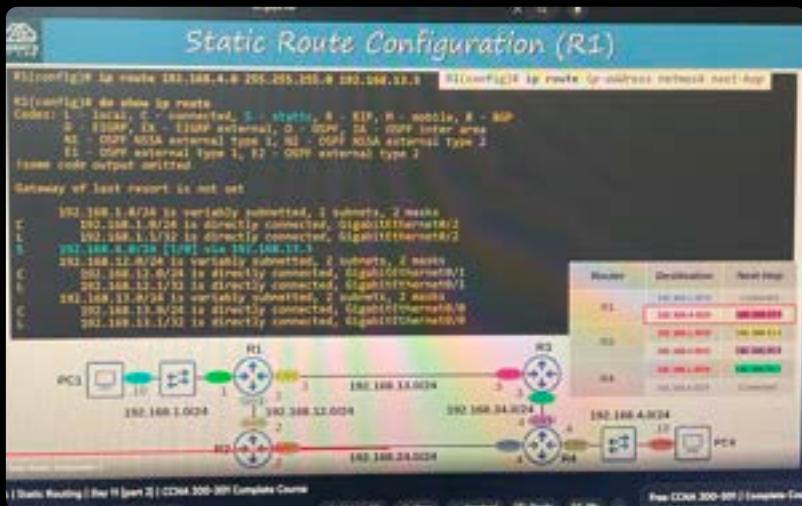
• • • When router doesn't receive a random package which is not in the routing table He will not forward to other interfaces like switches do

• • • When you configure an IP address on an int and enable the int, two routes are automatically added to the routing table

- Connected route (c)
- Local route (l) - exact IP of int /32

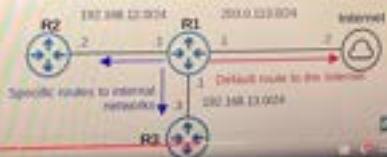
Day 11 - P2 - Creating static routes

(config)* ip route ip-address netmask next-hop



```
R1(config)# route 0.0.0.0 0.0.0.0 200.0.113.2
R1(config) do show ip route
%No route codes permitted
      ia - 25-35 inter-area, * - candidate default, U - per-user static route
%No route codes permitted
Gateway of last resort is 200.0.113.2 to network 0.0.0.0

S*  0.0.0.0/0      via 200.0.113.2
S  18.0.0.0/8 [1/0] via 200.0.113.2
S  172.16.0.0/16 [1/0] via 200.0.113.3
S  192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/24 is directly connected, GigabitEthernet0/1
L    192.168.12.1/32 is directly connected, GigabitEthernet0/1
S  192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.11.0/24 is directly connected, GigabitEthernet0/2
L    192.168.11.1/32 is directly connected, GigabitEthernet0/2
S  191.0.0.0/8 [1/0] via 200.0.113.2
C    191.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    191.0.0.1/32 is directly connected, GigabitEthernet0/2
L    191.0.0.2/32 is directly connected, GigabitEthernet0/2
```



Router	Destination	Next-Hop
R1	192.168.1.0/24	Connected
	4.0/24	? 192.168.12.2
R2	1.0/24	? 192.168.12.1
	4.0/24	? 192.168.24.4
R4	192.168.4.0/24	Connected

Day 12 - ARP

- ARP request - Broadcast
ARP reply - unicast

Day 13 -

IPv4 Address classes

easy way to remember classes

IPv4 Address Classes			
Class	First octet (binary)	First octet range (decimal)	
A	0xxxxxxx	0 - 127	0.0.0.0 - 127.255.255.255
B	10xxxxxx	128 - 191	128.0.0.0 - 191.255.255.255
C	110xxxxx	192 - 223	192.0.0.0 - 223.255.255.255
D	1110xxxx	224 - 239	224.0.0.0 - 239.255.255.255
E	1111xxxx	240 - 255	240.0.0.0 - 255.255.255.255

point to point network — connecting two points



IPv4 Address Classes					
Class	Leading bits	Size of network number bit field	Size of host bit field	Number of networks	Addresses per network
Class A	0	1	24	$128^2 = 16,777,216$	$2^{24} = 16,777,216$
Class B	10	2	16	$16,384^2 = 268,435,456$	$2^{16} = 65,536$
Class C	110	3	8	$256^2 = 65,536$	$2^8 = 256$

Day 14 - P2

When it is asked to create a subnet

ex. Divide the 192.168.255.0/24 network into five subnets of equal size

192.168.255.0/24

then we have to

$$\text{Number of subnets} = 2^x = \text{number of subnets}$$

(x = number of 'borrowed bits')

so here we need 5 subnets of 2^3 at minimum required = $2^3 = 8$

so we atleast have to borrow 3 host bits so new subnet will be /24 + 3 = /27

so to find the number of host per subnet

$$2^{\text{host-bits}} - 2 = 2^5 - 2 = \underline{82} - 2 = \underline{30}$$

so the range will be

- 5 {
- 192.168.255.0/27
 - 192.168.255.82/27 } difference of 32
 - 64
 - 96
 - 128

Ex. 10.0.0.0/8 → create 2000 subnets

$$2^{11} = 2048$$

$$8+11 = 19$$

Number of Host

- $2^{13-2} = 8192 - 2$
 $= 8190 \text{ host / subnet}$

② 10.217.182.223/11

① Network address

Network ID → 10.192.0.0/11

|
so max is 111 ←
223

that means

- ① Network Add → 10.192.0.0
- ② first usable → 10.192.0.1
- ③ Last usable → 10.223.255.254
- ④ Broadcast Add → 10.223.255.255

Num of host bits =

$$2^{21-2} = 2,097,150$$

VLSM - Variable Length subnet Mask

Variable-Length Subnet Masks

- Until now, we have practiced subnetting used FLSM (Fixed-Length Subnet Masks).
- This means that all of the subnets use the same prefix length (ie. subnetting a class C network into 4 subnets using /26).
- VLSM (Variable-Length Subnet Masks) is the process of creating subnets of different sizes, to make your use of network addresses more efficient.
- VLSM is more complicated than FLSM, but it's easy if you follow the steps correctly.

VLSM - Steps

- 1) Assign the largest subnet at the start of the address space.
- 2) Assign the second-largest subnet after it.
- 3) Repeat the process until all subnets have been assigned.

192.168.1.128/26
 $2^6 = 64$
No. of hosts
 $= 2^{6-2} = 64 - 2 = 62$
First usable IP - 192.168.1.129
Broadcast - 192.168.1.190

192.168.5.0/24

— LAN2 — 64 hosts

① 192.168.5.0/24

$2^7 = 128$ — host per subnet (-2)
that means leave the 2⁷ host bits

so network will be

192.168.5.0/25

n/w ip = 192.168.5.0/25

first usable = 192.168.5.1/25

Last usable . 126/25
Broadcast 192.168.5.127/25

LAN1 — Need 45 hosts

ip we have now is 192.168.5.128/25

so for 45 hosts →

192.168.5.128/26

because $2^6 = 64 - 2 = 62$ host more than 45

n/w IP — 192.168.5.128/26

First usable — 192.168.5.129/26

Last — . 190/26

Broadcast — . 191/26

LAN3 — start range 192.168.5.192/26

Needs 14 host

so 128 is perfect

because $2^4 - 2 = 16 - 2 = 14$

n/w ip — 192.168.5.192/28

first usable — 192.168.5.193/28

Last usable — 192.168.5.206/28

Broadcast — . 207/28

LAN4 — Needs 9 host

/28 network

192.168.5.208/28

N/w ip — 192.168.5.208/28

F usabla — .209/28

L — 1 — 192.168.5.222/28

Broadcast — 192.168.5.223/28

for point to point /30 ← best range

192.168.5.224/28 to /30

$2^2 = 4$ host

N/w ip — 192.168.5.224/30

first — .225/30

Last — .226/30

Broadcast — .227/30

Day 16 - VLAN's

Virtual LAN

- ① To separate networks
- ② Reduce Broadcast / unknown unicast floods
- ③ Increase security

• • • Without VLAN we can separate diff. deports in diff. subnets but they will still work in the same broadcast domain. Which means Broadcast messages will flood the network

• • VLAN Configuration

SW1 # show vlan brief

• • • All interfaces are in VLAN 1 by default

• • • VLAN's 1, 1002 - 1005 exist by default & cannot be deleted

To configure VLAN

```
(config)# interface range g1/0-3  
      switchport mode access  
      switchport mode vlan10
```

* A accessport is a switchport which belongs to a single VLAN, usually connects to end hosts like PCs

** switchports which carry multiple VLANs are called as "trunk ports"

```
# To change VLAN names
```

```
SW1(config)# vlan10  
(config-vlan)# name Science
```

Day 17 - VLAN - P2

Access ports - Access ports belongs to single VLAN

Trunk ports - Belongs to multiple VLAN on single interface

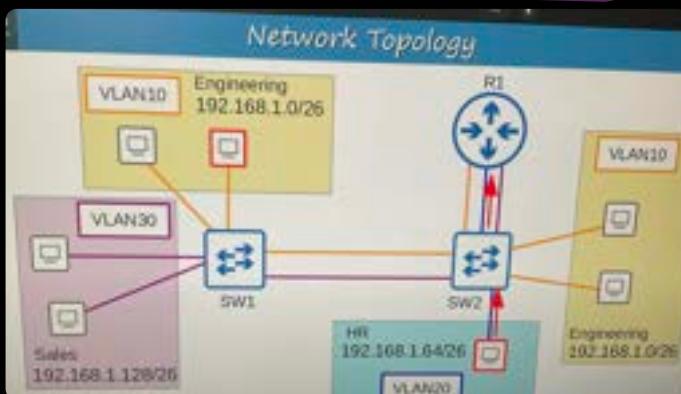
• Trunk ports

- In a small network with few VLANs, it is possible to use a separate interface for each VLAN when connecting switches to switches, and switches to routers.
- However, when the number of VLANs increases, this is not viable. It will result in wasted interfaces, and often routers won't have enough interfaces for each VLAN.
- You can use trunk ports to carry traffic from multiple VLANs over a single interface.

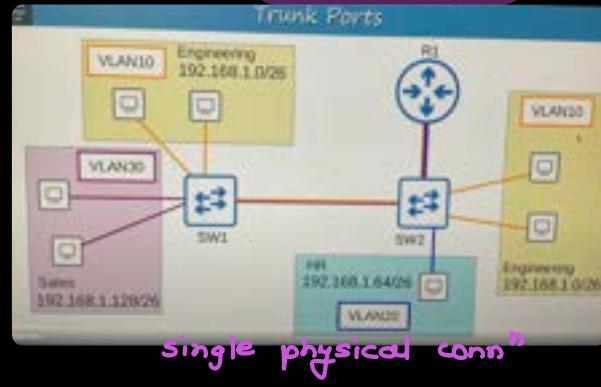
So basically rather than creating multiple separate connections for VLAN's via access port to communicate we use trunk ports to send multiple VLANs connection through single cable.

ex.

This is Access port VLAN
aka untagged ports



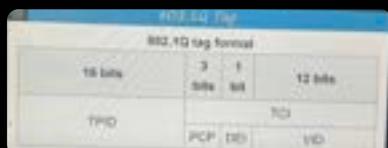
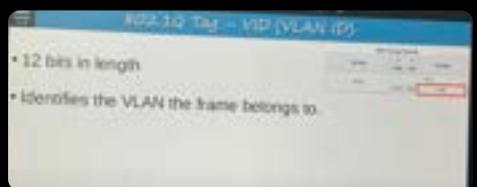
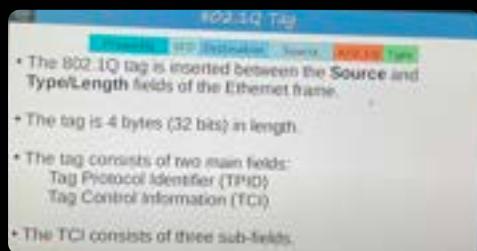
This is trunk port tagged port



- With VLAN tagging switches understands which VLAN the traffic belongs to.

Two main trunking protocols

- ① ISL (Inter-Switch Link) → not used in real world
- ② IEEE 802.1Q - aka dot1Q



The range of VLAN - 1 - 4094

Normal VLANs - 1 - 1005

Extended VLANs - 1006 - 4094

- some older sw might not support the extended VLAN range
- 802.1Q → has a feature called native VLAN
- native VLAN is VLAN 1 by default on all trunk ports, however this can be manually configured on each trunk port. → The one into which untagged traffic will be put when it's received on trunk ports. → Which makes it possible to support legacy devices or devices that don't tag their traffic.
- Sw does not add an 802.1Q tag to frames in the native VLAN
- When a switch receives an untagged frame on a trunk port, it assumes the frame belongs to the native VLAN
 - native VLANs should match each other.
 - for security reasons native VLANs are changed from default

- Configuration of Trunk ports

```
(config) # interface g0/0
          # switchport mode trunk
          if old switches we have to set encapsulation manually
          → # switchport trunk encapsulation dot1q
if not      switchport mode trunk
```

```
Sw1 # show interfaces trunk
```

- VLAN configuration to allow only certain ports for the security

```
(config-if) # switchport trunk allowed vlan 10,30
            # switchport trunk allowed vlan ? to know more
```

••• For security purpose it is best to change the native VLAN to unused VLAN

** Make sure native VLAN matches between switches

```
(config-if) # switchport trunk native vlan 1001
```

••• # show vlan brief command does not show trunk port

- use show interface trunk

- Router on a stick

When we have multiple VLAN's configured on switch and we want to use the single link between router and switch then we can divide that link into sub-interfaces ex. g0/0.10 , g0/0.20 , g0/0.30

On Router configuration →

```
int g0/0
```

```
no sh
```

```
{ int g0/0.10
```

```
encapsulation dot1Q 10
```

```
ip address 192.168.1.62
```

```
255.255.255.192
```

repeat for all

- ROAS is used to route between multiple VLANS using a single int on router and switch
- The switch int is configured as regular trunk

Router on a Stick (ROAS)

- ROAS is used to route between multiple VLANs using a single interface on the router and switch.
- The switch interface is configured as a regular trunk.
- The router interface is configured using **subinterfaces**. You configure the VLAN tag and IP address on each subinterface.
- The router will behave as if frames arriving with a certain VLAN tag have arrived on the subinterface configured with that VLAN tag.
- The router will tag frames sent out of each subinterface with the VLAN tag configured on the subinterface.

Quiz Question 2

After modifying the list of VLANs allowed on a trunk interface, you want to return it to the default state. Which command will do this?

- a) switchport trunk allowed vlan default
- b) **switchport trunk allowed vlan all**
- c) switchport trunk allowed vlan none
- d) switchport trunk allowed vlan 1,1001-1005

**

Day 18

• Native VLAN

→ Smaller frames because these are not tagged so more transfer

Two methods of config.

① encapsulation dot1q vlan-id native

② configure the IP add for the native VLAN
on the router's physical interface

• Layer 3 switches

→ Multi-layer switches are used in a situation where we have multiple VLANs and if we routers then the trunk (dot1Q) will have congestion which may lead to slower performance and that's the reason we use multilayer switches. → As switches have extra no. of ports.

• Command to reset interface to its default settings

• default interface g 0/0

•••• L3 switch Important command

ip routing

→ This command enables L3 routing on the s/w

also,

```
(config)# interface g0/1  
(c-if)# no switchport
```

→ Allows us to configure a s/w int as a routed port

SVI → Switch VLAN interfaces (L3 s/w)

- SVI are shutdown by default, so remember to use no shutdown

Inter-VLAN Routing via SVI				
Interface	IP-Address	OK?	Method	Status
FastEthernet0/0	unassigned	YES	unset	up
FastEthernet0/1	unassigned	YES	unset	up
FastEthernet0/2	unassigned	YES	unset	up
FastEthernet0/3	192.168.1.193	YES	manual	up
Vlan10	192.168.3.82	YES	manual	up
Vlan20	192.168.3.126	YES	manual	up
Vlan30	192.168.3.190	YES	manual	up
Vlan40	40.40.40.40	YES	manual	down

- 1) The VLAN must exist on the switch.
- 2) The switch must have at least one access port in the VLAN in an up/up state. AND/OR a trunk port that allows the VLAN that is in an up/up state.
- 3) The VLAN must not be shutdown (you can use the shutdown command to disable a VLAN).
- 4) The SVI must not be shutdown (SVIs are disabled by default)

Day 18's Lab is to do

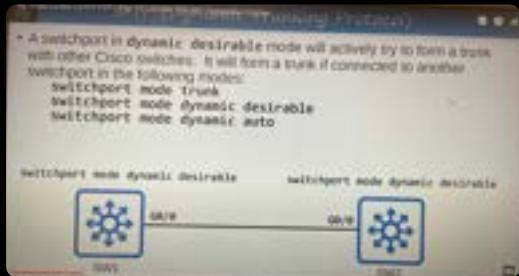
Day 19 - DTP / VTP

- DTP - Dynamic Trunking Protocol
- VTP - VLAN Trunking Protocol

Cisco DTP (Dynamic Trunking Protocol)	
• DTP is a Cisco proprietary protocol that allows Cisco switches to dynamically determine their interface status (access or trunk) without manual configuration.	
• DTP is enabled by default on all Cisco switch interfaces.	
• So far, we have been manually configuring switchports using these commands:	
switchport mode access	
OR	
switchport mode trunk	
• For security purposes, manual configuration is recommended. DTP should be disabled on all switchports.	

```
SW1 # show interfaces g0/0 switchport
```

- Dynamic desirable mode will actively try to form a trunk with other Cisco switches.



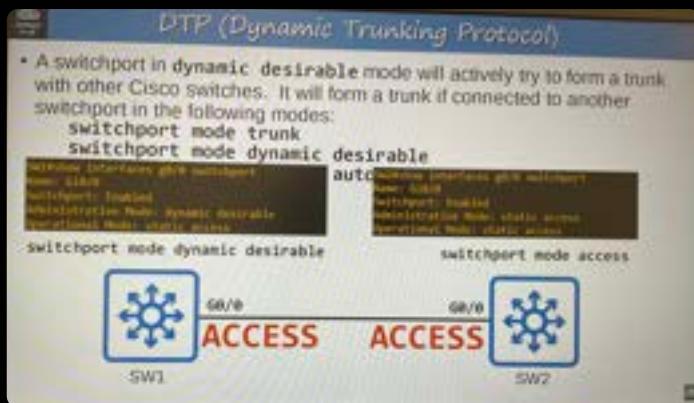
- ② In dynamic desirable switch will try to create a dynamic trunk mode automatically

③ Dynamic auto -

- Doesn't actively try to form a trunk like dynamic desirable.
- It's more passive → it communicates with other switches that if you want to form a trunk, it will form a trunk.
- Auto can form a trunk in two modes
 - Switchport mode trunk
 - Switchport mode dynamic desirable.

If two switchports in dynamic auto → They operate at access mode

ex. 3 Doesn't form trunk since one is formed manually to Access



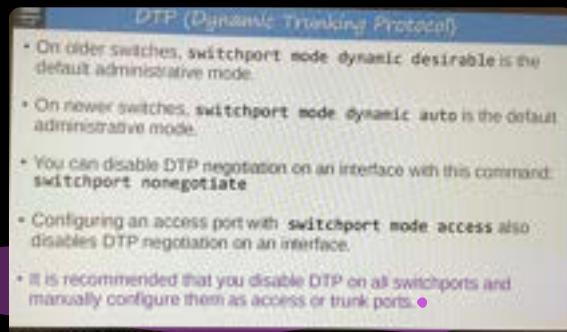
ex. If two switchports are

- { one manually trunk mode
 - { other manually access mode
- ✗ Mismatch will occur.
- error

Summarization chart

Administrative Mode	Trunk	Dynamic Desirable	Access	Dynamic Auto
Trunk	Trunk	Trunk	X	Trunk
Dynamic Desirable	Trunk	Trunk	Access	Trunk
Access	X	Access	Access	Access
Dynamic Auto	Trunk	Trunk	Access	Access

- DTP will not form a trunk with a router, pc etc
The switchport will be in access mode.



Repeat DTP Day 19
VTP
DTP/VTP Lab

default administrative mode on new switches is

- switchport mode dynamic auto

To Disable DTP negotiation

— `switchport nonegotiate`

OR

- `switchport mode access` can disable it too

• Recommendations

→ Disable DTP on all switchport

manually set them on access or trunk

Day 20 -

STP - Spanning tree protocol

- Redundancy protocol which works on L2.

STP is solution to

- Broadcast storms

• classic Spanning tree protocol is

IEEE 802.1D

STP runs on all switches by default

- 'Classic Spanning Tree Protocol' is IEEE 802.1D.
- Switches from ALL vendors run STP by default.
- STP prevents Layer 2 loops by placing redundant ports in a blocking state, essentially disabling the interface.
- These interfaces act as backups that can enter a forwarding state if an active (=currently forwarding) interface fails.
- Interfaces in a forwarding state behave normally. They send and receive all normal traffic.
- Interfaces in a blocking state only send or receive STP messages (called BPDUs = Bridge Protocol Data Units).

- By selecting which ports are **forwarding** and which ports are **blocking**, STP creates a single path to/from each point in the network. This prevents Layer 2 loops.
- There is a set process that STP uses to determine which ports should be forwarding and which should be blocking.
- STP-enabled switches send/receive Hello BPDUs out of all interfaces, the default timer is 2 seconds (the switch will send a Hello BPDU out of every interface, once every 2 seconds).
- If a switch receives a Hello BPDU on an interface, it knows that interface is connected to another switch (routers, PCs, etc. do not use STP, so they do not send Hello BPDUs).

① Election one root bridge

for election priority and Mac address is compared

by default priority on all switches = 32768

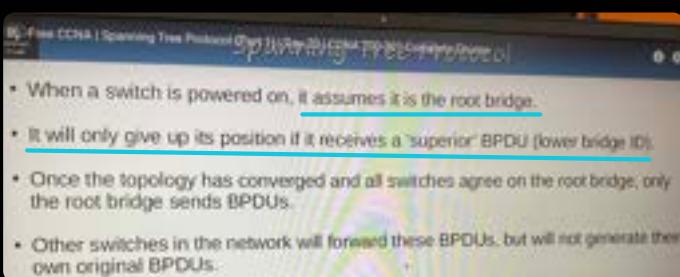
• if priority is matched the Mac address is compared.
lowest mac address wins.

In default VLAN of 1 the default bridge priority is actually 32769

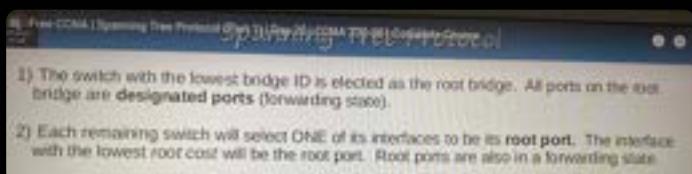
— So if there are multiple VLANs

→ VLAN 2 will have 32770

VLAN 3 will have 32771 priority



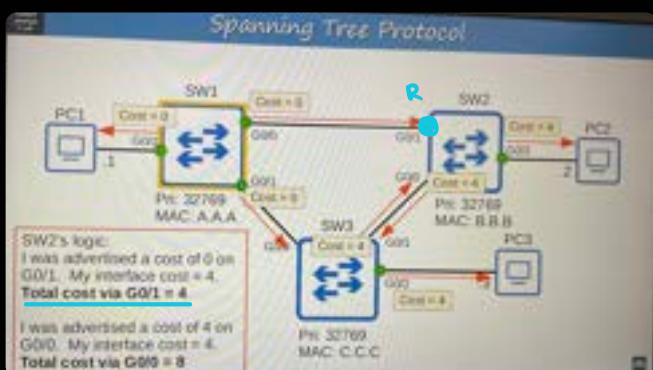
• All ports on the root bridge are under designated ports (forwarding state)



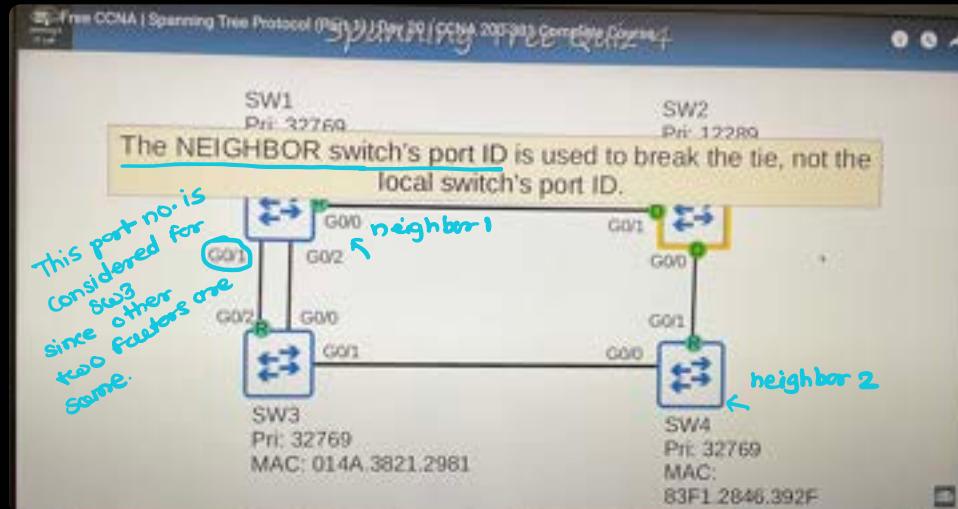
Speed	STP Cost
10 Mbps	100
100 Mbps	10
1 Gbps	4
10 Gbps	2

To find the root ports for STP.

This port will →
become root port



confusing part



R - Root ports

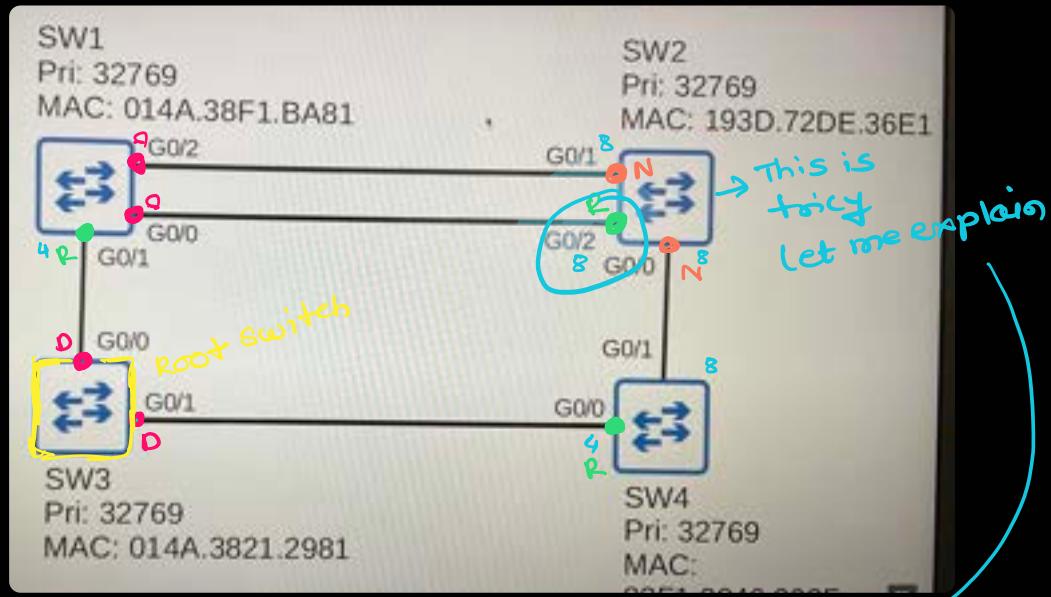
D - Designated port (forwarding state)

N - non designated (Blocking state)

Every collision Domain has a single STP designated Port.

STP root
Imp root

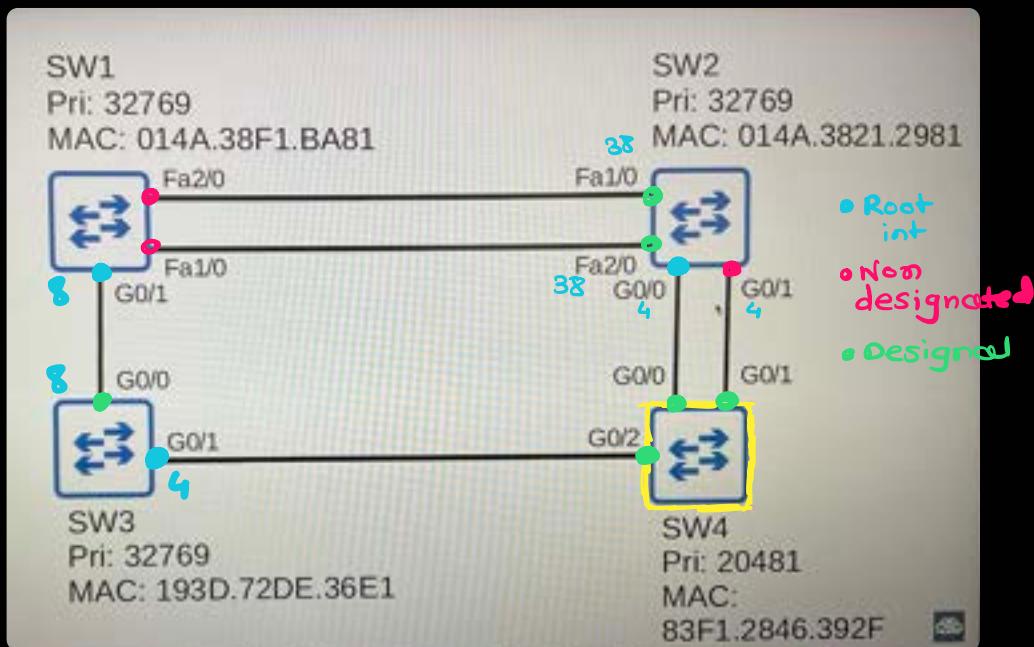
- 1) One switch is elected as the root bridge. All ports on the root bridge are designated ports (forwarding state). Root bridge selection:
1: Lowest bridge ID **if same @ lowest MAC Address**
- 2) Each remaining switch will select ONE of its interfaces to be its root port (forwarding state). Ports across from the root port are always designated ports.
Root port selection:
1: Lowest root cost
2: Lowest neighbor bridge ID
3: Lowest neighbor port ID
- 3) Each remaining collision domain will select ONE interface to be a designated port (forwarding state). The other port in the collision domain will be non-designated (blocking)
Designated port selection:
1: Interface on switch with lowest root cost
2: Interface on switch with lowest bridge ID



..... So here we already got the root for SW1
for SW2

G0/2 } are two ports of neighbours and out of that
G0/0 } the G0/0 port is smallest
then opposite to G0/0 is selected as Root interface

example 2: →



Root Switch port becomes designated ports by default

- The interface connected to root port is always designated.

SW3 # show spanning tree
also specific to vlan

show spanning tree vlan
show spanning tree detail

show spanning tree summary

Spanning tree Post states

Spanning Tree Port States		
STP Port State	Status	
Blocking	Stable	Non-designated ports remain stable in a Blocking state.
Listening	Transitional	Listening and Learning are transitional states which are passed through when an interface is activated, or when a Blocking port must transition to a Forwarding state due to a change in the network topology.
Learning	Transitional	
Forwarding	Stable	
(Disabled)		

PDU's - Are message exchanged between bridges participating in STP.

BPD's do following

- ① Root Bridge Election
 - ② Topology information
 - ③ Loop prevention
 - ④ Convergence

Non-designated ports are always blocking

- ① Listening state is 15 sec long by default

 - interface in listening state only forwards / receives BPDUs → It does not send/over normal traffic.

② same for listening state.

but in listening it learns the more addresses of regular traffic

③ forwarding state

Spanning Tree Port States				
STP Port State	Send/Receive BPDUs	Frame forwarding (regular traffic)	MAC address learning	State
Blocking	NO/YES	NO	NO	Stable
Listening	YES/YES	NO	NO	Transitional
Learning	YES/YES	NO	YES	Transitional
Forwarding	YES/YES	YES	YES	Stable
Disabled	NO/NO	NO	NO	Stable

- Spanning tree Timers

Spanning Tree Timers		
STP Timer	Purpose	Duration
Hello	How often the root bridge sends hello BPDUs only send through Designated ports	2sec
Forward delay	How long the switch will stay in the Listening and Learning states (each state is 15 seconds = total 30 seconds)	15sec
Max Age	How long an interface will wait after ceasing to receive Hello BPDUs to change the STP topology.	20sec (10* hello)

Designated ports are ports which are selected as designated path to forward traffic on that segment.

Rootport → Loop-free path to the root bridge

PVST+ supports 802.1Q

- Regular STP uses MAC Address of 0180.c200.0000

*** Portfast - Allows port to move immediately to the forwarding state bypassing Listening and Learning.

* IF used , it must be enabled only on ports connected to end hosts.
IF enabled on a port connected to another switch it could cause a Layer 2 loop.

To enable portfast →

```
(config)# int g 0/2
(config-if)* spanning-tree portfast
```

} → To globally enable
spanning-tree portfast default

* * *
portfast can also cause loops if not configured on proper end-host interface. → portfast can only be enabled on Access ports because trunk mode enabled on switch which again will cause loop, Broadcast storms.

→ To protect against such loops BPDUs Guard is used

To enable BPDUs →

interface g0/2

spanning-tree bpduguard enable

from global

- SW1(config)# Spanning-tree portfast bpduguard default
- So whenever BPDU packets are received in portfast enabled interface the port will go into shutdown mode to prevent loops.

• Spanning tree Mode.

* Spanning-tree mode ?

mst → Multiple spanning tree

pvst → pre-vlan ST

moder
cisco
default ← rapid-pvst → pre-vlan rapid ST

To manually set spanning-tree root switch

{ SW1 # spanning-tree vlan1 root primary.
—————> VLAN root secondary

Load Balancing.

Spanning Tree Quiz 9

A packet capture indicates that a switch port has an STP port ID of 0x8002. What is the STP port priority of this port?

a) 80
b) 32
c) 128
d) 224

Hexadecimal 80
= 128
port priority = 128

Spanning Tree Quiz 10

You want to make sure that a Layer 2 loop will not be caused if a user connects a switch to a switch port. Which spanning tree optional feature achieves this?

- a) PortFast
- b) Loop Guard
- c) Root Guard
- d) BPDU Guard

Day - 21 → Lab

* show spanning-tree

* To change the port cost to manually change the root port / designated port set-ups

→ int f0/1
span vlan 1 port-priority 240

cost range 1-240

* Setting up portfast

int f0/3
• spanning-tree portfast
• spanning-tree bpduguard enable

*** Rapid Spanning Tree PVST +

- PVST → only supports ISL trunking encapsulation
- PVST+ → supports DOT1Q

The problem with PVST was that it takes 50 sec (15 for listening, 15 for forwarding + 20 mg timer) to actually update that too much time to overcome that we use PVST+

- • • PVST+ works on bridge-bridge handshake mechanism, which allows ports to move directly to forwarding.

Spanning Tree Versions	
Industry standards (IEEE)	Cisco versions
Spanning Tree Protocol (802.1D)	Per-VLAN Spanning Tree Plus (PVST+)
<ul style="list-style-type: none"> The original STP All VLANs share one STP instance. Therefore, cannot load balance. 	<ul style="list-style-type: none"> Cisco's upgrade to 802.1D Each VLAN has its own STP instance. Can load balance by blocking different ports in each VLAN.
Rapid Spanning Tree Protocol (802.1w)	Rapid Per-VLAN Spanning Tree Plus (Rapid PVST+)
<ul style="list-style-type: none"> Much faster at converging/adapting to network changes than 802.1D All VLANs share one STP instance. Therefore, cannot load balance. 	<ul style="list-style-type: none"> Cisco's upgrade to 802.1w Each VLAN has its own STP instance. Can load balance by blocking different ports in each VLAN.
Multiple Spanning Tree Protocol (802.1s)	
<ul style="list-style-type: none"> Uses modified RSTP mechanics. Can group multiple VLANs into different instances (i.e. VLANs 1-5 in instance 1, VLANs 6-10 in instance 2) to perform load balancing. 	

PVST+ or RSTP cost

Speed	STP Cost	RSTP Cost
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2000
100 Gbps	X	200
1 Tbps	X	20

RSTP port states

STP Port State	Transmits BPDU's	Frame Forwarding (regular traffic)	MAC address learning	Status Transitions
Discarding	NO/YES	NO	NO	Initial
Learning	YES/YES	NO	YES	Transitional
Forwarding	YES/YES	YES	YES	Initial

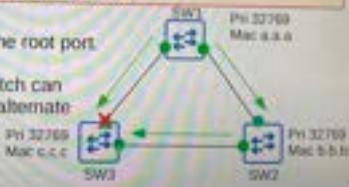
- If a port is administratively disabled (`shutdown` command) = discarding state
- If a port is enabled but blocking traffic to prevent Layer 2 loops = discarding state

Rapid Spanning Tree Port Roles	
The root port role remains unchanged in RSTP.	<ul style="list-style-type: none"> The port that is closest to the root bridge becomes the root port for the switch. The root bridge is the only switch that doesn't have a root port.
The designated port role remains unchanged in RSTP.	<ul style="list-style-type: none"> The port on a segment (collision domain) that sends the best BPDU is that segment's designated port (only one per segment).
The non-designated port role is split into two separate roles in RSTP:	
	the alternate port role
	the backup port role

- The RSTP alternate port role is a discarding port that receives a BPDU from the root port.
- This immediate move to forwarding state functions like a classic STP optional feature called UplinkFast. Because it is built into RSTP, you do not need to activate UplinkFast when using RSTP/Rapid PVST+.

- Functions as a backup to the root port.

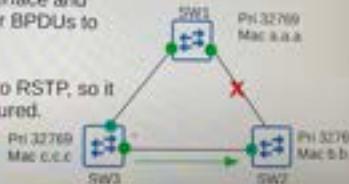
- If the root port fails, the switch can immediately move its best alternate port to forwarding.



- One more STP optional feature that was built into RSTP is BackboneFast.

- BackboneFast allows SW3 to expire the made age timers on its interface and rapidly forward the superior BPDUs to SW2.

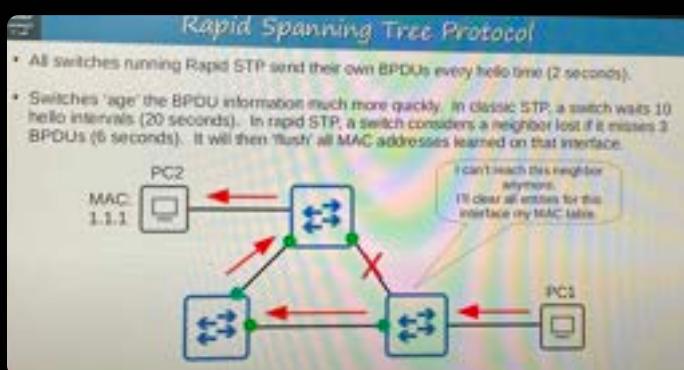
- This functionality is built into RSTP, so it does not need to be configured.



configuration →

- spanning-tree mode mst
pvst
rapid-pvst

- Rapid STP is compatible with classic STP
- Rapid STP has a protocol version no. 2
- classic STP no. 0



- RSTP has a built-in function of **Portfast**, **UplinkFast**, and **Backbonefast**.
- RSTP Every switch sends BPDUs not just the root bridge

RSTP Link types -

- ① edge → To connect host with switch
- ② point-to-point → switch to switch conn'
- ③ shared Link → switch — Hub

Manual configuration

for edge

- ① spanning-tree link type point-to-point
- ② interface f0/24
 - spanning-tree portfast

- Day 23 - Etherchannel

Oversubscription — When the bandwidth of the interfaces connected to end hosts is greater than the bandwidth of the connection to distribution switch(es).

Etherchannel — Allows us to group physical links together logically.

- shown like this



Why we use it → Etherchannels are used because of RSTP/STP there will be links which will be under alternative link means not used to prevent that happening we use etherchannels bet" switches if we want to allow traffic

- STP will treat this group as a single interface
- Etherchannel also known as Port channel or LAG (Link aggregation group)
- Etherchannel allows the load balancing based on diff types

Configuration

ASHI# show etherchannel load-balance

To see the current config-

To change the load - Balancing method

port-channel load-balancing src-dst-mac

- To configure Etherchannel configuration

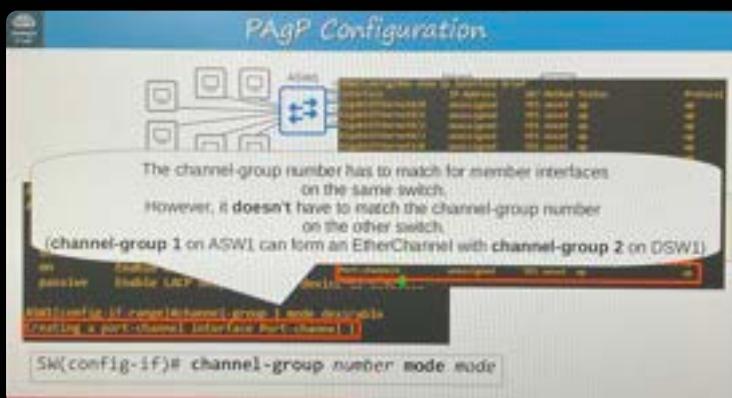
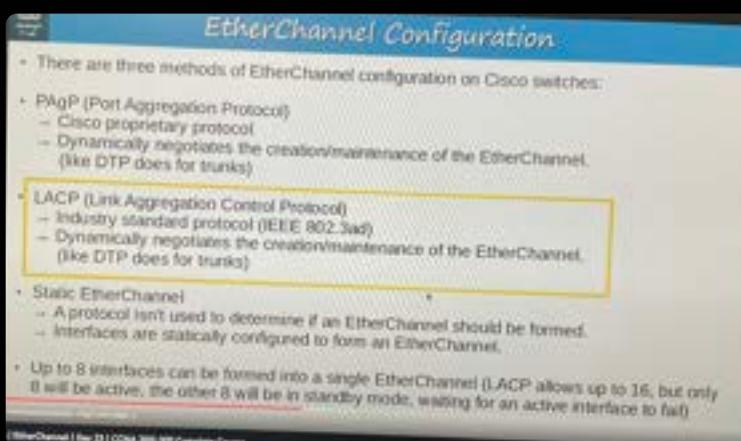
Three methods available

① PAgP (Port Aggregation Protocol)
— cisco only protocol

② LACP - Link Aggregation control protocol

↳ Industry standards (IEEE 802.3ad)

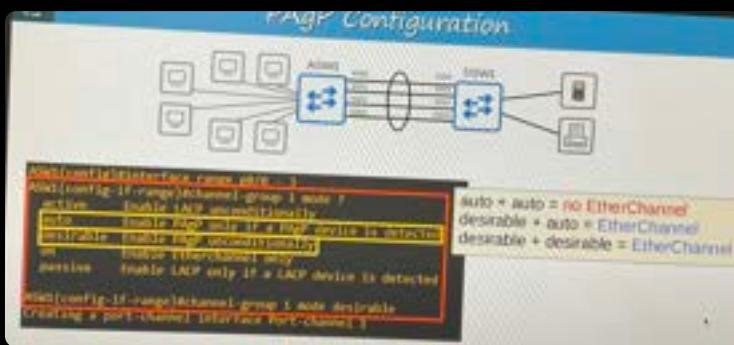
③ static Etherchannel
→ Avoid to statically .



for LACP if both ends are configured like this
Passive + Passive = no Etherchannel
active + active = Etherchannel

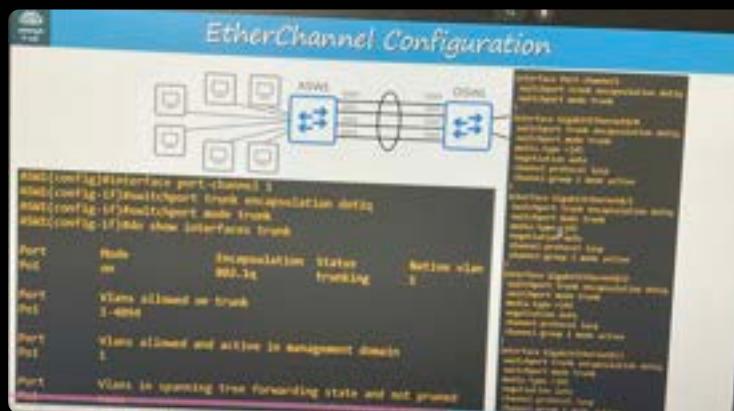
active + passive = Etherchannel.

and for PAgP →

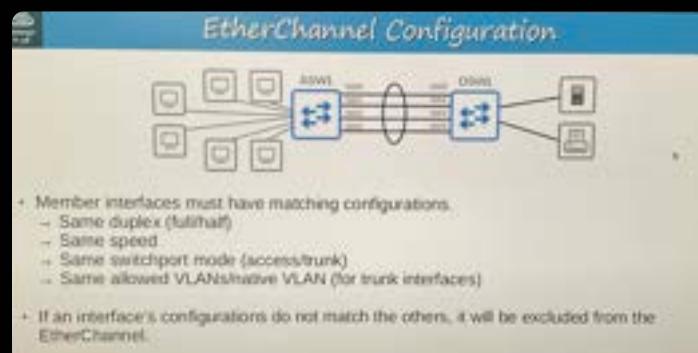


channel-protocol lACP } not much used commands
channel-protocol pagp }

- then those logical links can be configured as a trunk



To be a Etherchannel Link member interfaces must have →



show etherchannel summary

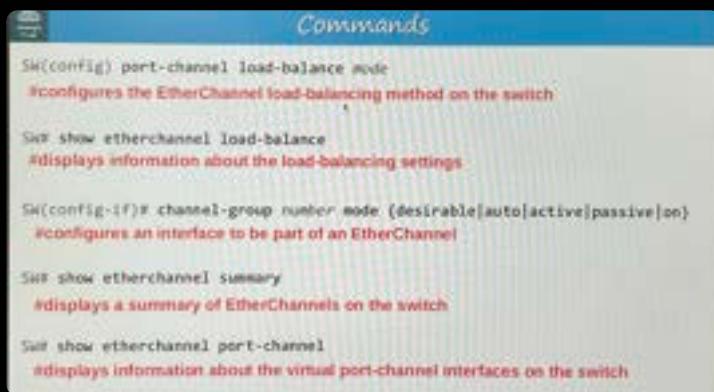
show etherchannel port-channel

L3 Etherchannel Configuration.

```
(config) # int range g0/0 - 3  
      # no switchport → To make it L3  
      # channel-group 1 mode active
```

for IP

```
# int po1  
# ip address 10.0.0.1 255.255.255.252
```



LAB →

Configuring etherchannels demo

```
* int range g0/1 - 2  
* channel-group 1 mode active LCAP  
* int po1  
* switchport mode trunk
```

if switch also supports ISL then we have to

```
* switchport trunk encapsulation dot1q  
  then  
* switchport mode trunk  
* do sh eth sum
```

L3 switches things to remember

① To enable routing on L3 switch
we have to run

+ no switchport first

then enable routing with
(config) # ip routing

To see the default load-balance

* do sh etherchannel load-balance

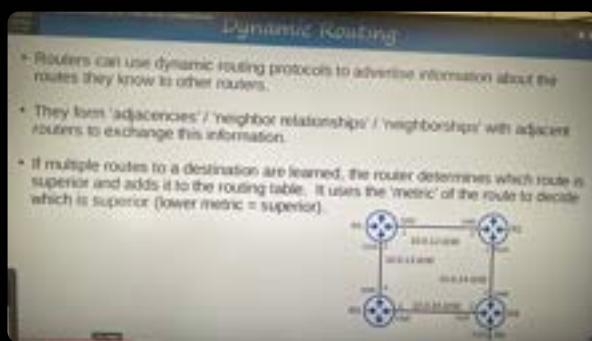
To configure load-balance

(config) # port-channel load-balance src-dst ip

Dynamic Routing

Network route - route of complete network

Host route - exact ip of Host /32



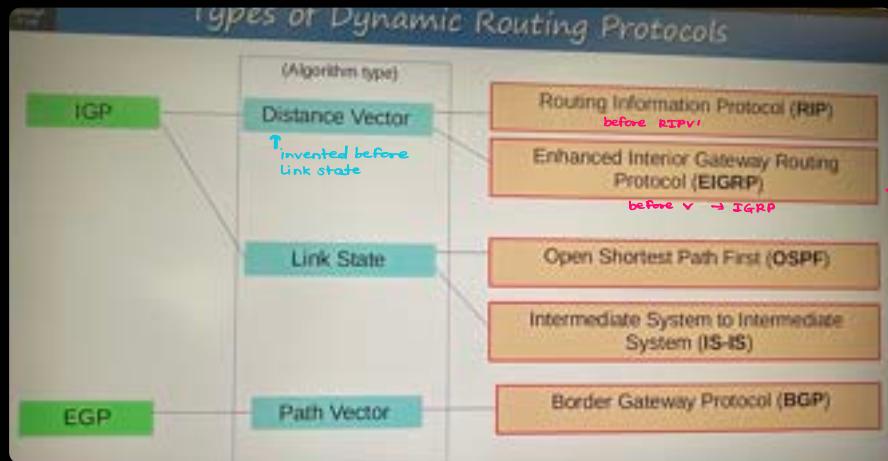
Different types of dynamic routing

① IGP - Interior Gateway protocol

used to share routes within a single autonomous sys (AS), which is a single org.

Two IGP types

- ① Distance vector → RIP, EIGRP
- ② Link state → OSPF, IS-IS



② EGP – Exterior Gateway protocol

Used to share routes betn different AS

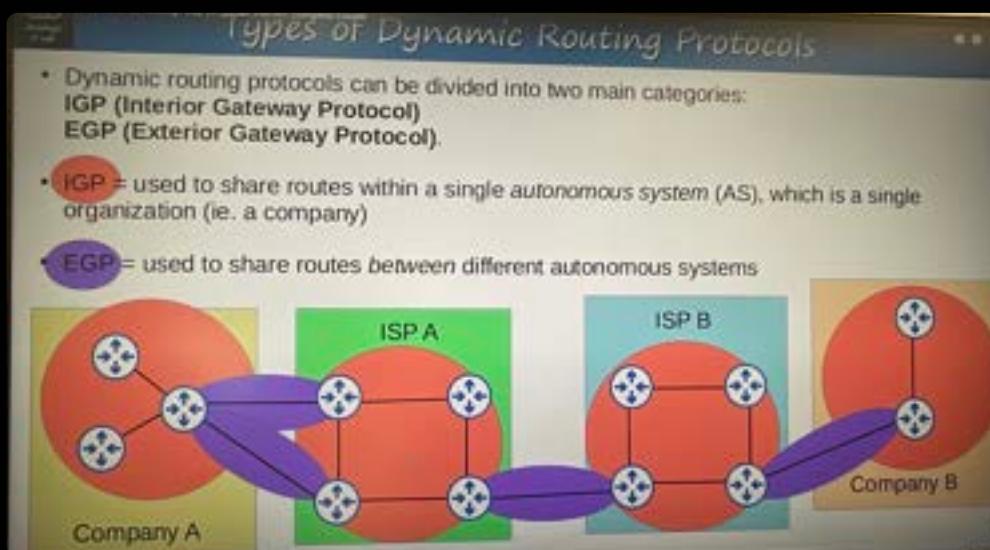
Only one → Path vector → ex. BGP (Border Gateway protocol)

EGP used to share route information betn routers.

EGP type → (only one)

① Path vector

example → BGP



Distance Vector protocol

Distance Vector Routing Protocols

- Distance vector protocols were invented before link state protocols.
- Early examples are **RIPv1** and Cisco's proprietary protocol **IGRP** (which was updated to **EIGRP**)
- Distance vector protocols operate by sending the following to their directly connected neighbors:
 - their known destination networks
 - their metric to reach their known destination networks
- This method of sharing route information is often called 'routing by rumor'
- This is because the router doesn't know about the network beyond its neighbors. It only knows the information that its neighbors tell it.
- Called 'distance vector' because the routers only learn the 'distance' (metric) and 'vector' (direction, the next-hop router) of each route.

Link state routing

Link State Routing Protocols

- When using a link state routing protocol, every router creates a 'connectivity map' of the network.
- To allow this, each router advertises information about its interfaces (connected networks) to its neighbors. These advertisements are passed along to other routers, until all routers in the network develop the same map of the network.
- Each router independently uses this map to calculate the best routes to each destination.
- Link state protocols use more resources (CPU) on the router, because more information is shared.
- However, link state protocols tend to be faster in reacting to changes in the network than distance vector protocols.

Routing protocol Metrics

- It's same like root cost from spanning-tree protocol where link state calculate costs and select best route with the lowest cost.

situation — if two routers have the same route cost aka metrics both will be added to the route table and traffic will LB.

↓

IMP

Dynamic Routing Protocol Metrics	
Network IP Prefix	
Codes: L - local, C - connected, S - static, R - OSPF, N - neighbor, E - EGP	
D - EIGRP, EX - EIGRP external, O - OSPF inter-area	
NL - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2	
E1 - OSPF external type 1, E2 - OSPF external type 2	
I - IS-IS, SE - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2	
LA - IS-IS inter-area, * - candidate default, # - per-user static route	
Metric: 0 - 16777215, Cost: 0 - 16777215, Priority: 0 - 16777215	
ECMP (Equal Cost Multi-Path)	
Gateway of last resort is not set	
192.0.0.0/0 is variably subnetted, 6 subnets, 2 routes 192.0.12.0/16 is directly connected, GigabitEthernet0/0 192.0.12.1/32 is directly connected, GigabitEthernet0/0 192.0.13.0/16 is directly connected, GigabitEthernet0/0 192.0.13.1/32 is directly connected, GigabitEthernet0/0 192.0.24.0/16 [118/2] via 192.0.12.2, 00:00:09, GigabitEthernet0/0 192.0.24.0/16 [118/2] via 192.0.13.2, 00:00:09, GigabitEthernet0/0 192.168.4.0/24 [119/1] via 192.0.13.2, 00:00:09, GigabitEthernet0/0 192.168.4.0/24 [119/1] via 192.0.12.2, 00:00:09, GigabitEthernet0/0	

AD
Administrative
distance
route metrics is 3 here

← Preemptive approach

IGP	Metric	Explanation
RIP	• only cares about hop count • doesn't matter the link speed	Each router in the path counts as one hop. The total metric is the total number of hops to the destination. Links of all speeds are equal.
EIGRP	Metric based on bandwidth & delay (try default)	Complex formula that can take into account many values. By default, the bandwidth of the slowest link in the route and the total delay of all links in the route are used.
OSPF	Cost	The cost of each link is calculated based on bandwidth. The total metric is the total cost of each link in the route.
IS-IS	Cost	The total metric is the total cost of each link in the route. The cost of each link is not automatically calculated by default. All links have a cost of 10 by default.

Administrative Distance

* * →

Administrative Distance	
• In most cases a company will only use a single IGP – usually OSPF or EIGRP.	
• However, in some rare cases they might use two. For example, if two companies connect their networks to share information, two different routing protocols might be in use.	
• Metric is used to compare routes learned via the same routing protocol.	
• Different routing protocols use totally different metrics, so they cannot be compared.	
• For example, an OSPF route to 192.168.4.0/24 might have a metric of 30, while an EIGRP route to the same destination might have a metric of 33280. Which route is better? Which route should the router put in the route table?	
• The administrative distance (AD) is used to determine which routing protocol is preferred.	
• A lower AD is preferred, and indicates that the routing protocol is considered more ‘trustworthy’ (more likely to select good routes).	

* * *

Administrative Distance			
Route protocol/type	AD	Route protocol/type	AD
Directly connected	0	IS-IS	115
Static	1	RIP	120
External BGP (eBGP)	20	EIGRP (external)	170
EIGRP	90	Internal BGP (iBGP)	200
IGRP	100	Unusable route	255
OSPF	110		

* * * Metrics are used to learn the route over the same protocol

* * * But AD (Administrative distance) is used to find the distance bet" two different routing protocols

Administrative Distance

- The following routes to the destination network 10.1.1.0/24 are learned:
 - next hop 192.168.1.1, learned via RIP, metric 5
 - next hop 192.168.2.1, learned via RIP, metric 3
 - next hop 192.168.3.1, learned via OSPF, metric 10

Which route to 10.1.1.0/24 will be added to the route table?

- Metric is used to compare routes learned from the same routing protocol.
- However, before comparing metrics, AD is used to select the best route.
- The OSPF route will always take precedence over the RIP routes, because it has a lower AD.

Floating static route aka Backup static route

- We can manually change the AD cost for static route to change the selection preference that is called as floating static route.

To set it manually →

```
# Conf t
*(config)* ip route 10.0.2.0 255.255.255.0 203.0.113.1 100
#          best      Mask        next hop AD
```

Distance Vector

RIP – Routing information Protocol

- Routing Information Protocol (industry standard)
- Distance vector IGP (uses routing-by-rumor logic to learn/share routes)
- Uses hop count as its metric. One router = one hop (bandwidth is irrelevant)
- The maximum hop count is 15 (anything more than that is considered unreachable)
- Has three versions:
 - RIPv1 and RIPv2, used for IPv4
 - RIPvng (RIP Next Generation), used for IPv6
- Uses two message types:
 - Request: To ask RIP-enabled neighbor routers to send their routing table
 - Response: To send the local router's routing table to neighboring routers
- By default, RIP-enabled routers will share their routing table every 30 seconds

RIPv1 and RIPv2

- RIPv1:
 - only advertises *classful* addresses (Class A, Class B, Class C)
 - doesn't support VLSM, CIDR
 - doesn't include subnet mask information in advertisements (Response messages)
 - 10.1.1.0/24 will become 10.0.0.0 (Class A address, so assumed to be /8)
 - 172.16.192.0/18 will become 172.16.0.0 (Class B address, so assumed to be /16)
 - 192.168.1.4/30 will become 192.168.1.0 (Class C address, so assumed to be /24)
 - messages are broadcast to 255.255.255.255
- RIPv2:
 - supports VLSM, CIDR
 - includes subnet mask information in advertisements
 - messages are **multicast** to 224.0.0.9

Broadcast messages are delivered to all devices on the local network.
Multicast messages are delivered only to devices that have joined that specific multicast group.

To configure RIP

```
• R1(config)# router rip
(config-router)# version 2
    * no auto-summary
    * network 10.0.0.0
    # network 172.16.0.0
```

* default-information originate

- Command is used to send routing information with neighbours in RIP & OSPF

R1 # Shows ip protocols

```
show ip protocols

R1#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 28 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip          RIP V2
  Default version control: send version 2, receive version 2
    Interface      Send   Recv   Triggered RIP  Key-chain
      GigabitEthernet0/0  2      2
      GigabitEthernet1/0  2      2
  Automatic network summarization is not in effect
  Maximum path: 4 }→ Amount of ECMP load balancing
  Routing for Networks:  Path's allowed
    10.0.0.0
    172.16.0.0
  Passive Interface(s): → To prevent RIP to send
    GigabitEthernet2/0   msg's every 60 sec on
  Routing Information Sources:   that int
    Gateway        Distance   Last Update
    10.0.12.2       120        00:00:21
    10.0.13.2       120        00:00:06
Distance: (default is 120)
```

R1(config-router)#maximum-paths ?
<1-32> Number of paths
R1(config-router)#maximum-paths 8

R1(config-router)#distance ?
<1-255> Administrative distance
R1(config-router)#distance 85

• EIGRP – Enhanced Interior Routing protocol

```
EIGRP
```

- Enhanced Interior Gateway Routing Protocol
- Was Cisco proprietary, but Cisco has now published it openly so other vendors can implement it on their equipment.
- Considered an 'advanced' / 'hybrid' distance vector routing protocol.
- Much faster than RIP in reacting to changes in the network.
- Does not have the 15 'hop-count' limit of RIP.
- Sends messages using multicast address 224.0.0.10.
- Is the only IGP that can perform unequal-cost load-balancing (by default it performs ECMP load-balancing over 4 paths like RIP)

We can have RIP & EIGRP running at the same time .