1-10

Section 4-

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

Connection to device

Lapto port (need serial to USB conv.)

— New devices by Cisco has
• USB to mini-USB

Levels

① User Level → >
② priviledge level aka enable mode → #
going back to user level disable

③ Global config → conf t → (config) #

* ctrl + 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 sensetive
** To exist from upper level directly to base level you can use end command.

* pipe option to search
ex. sh run | i
↑ case sensetive after that

* Copy running-config to start
  + copy run start

+ sh start

* Backup the config

Tools like → cisco client infra

* — Copy run ?

ex. copy run flash:my-config
sh flash

. • Erase

erase start
. Old cisco → use 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 Appl^n is traffic for

** • stateful firewall keep track of return traffic using port numbers. ex. if we send traffic from 80 (src) → 1500 (dst) 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	UDP
① Connection oriented data can be sent bi-direc^n	① Not

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

③ Reliable connection
④ Slower
⑤ Perform flow control

② doesnot

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

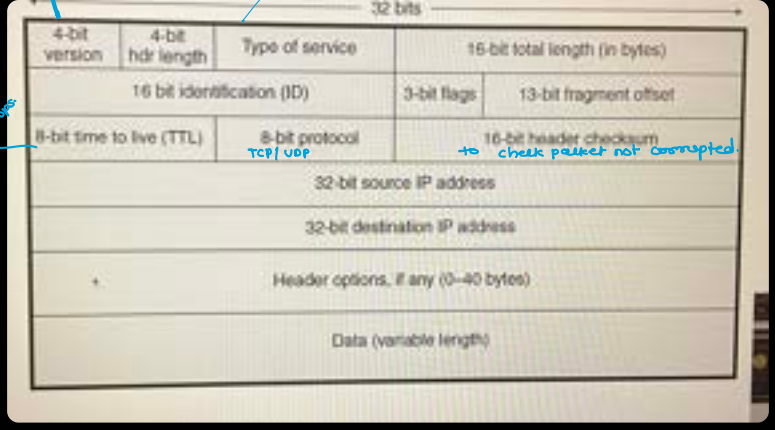
— IP is connectionless protocol with no acknoledgements

- Layer 3 includes ICMP (Internet control message protocol) and IPsec.

— Why smaller subnets ?
→ Improves performance & Security

→ IPV4/IPV6 difference

→ used for QoS can put packets in order that packets go first before service



* Routers do not forward the Broadcast traffic.

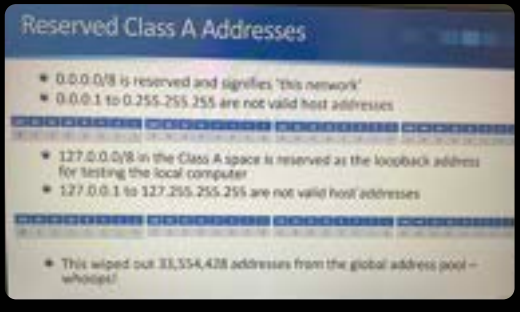
Multicast → We send single copy to multiple Hosts.
ex. Radio station.

- Learn diff classes of IP Add.
  class A- classD.

- 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 & feature use

Class	First Octet	Default Subnet Mask	
		Slash	Dotted 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 effecient 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 $2^4 = 16$ available subnets

ex.2
class B with /28
16+12 = 28

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

*** To calculate number of host

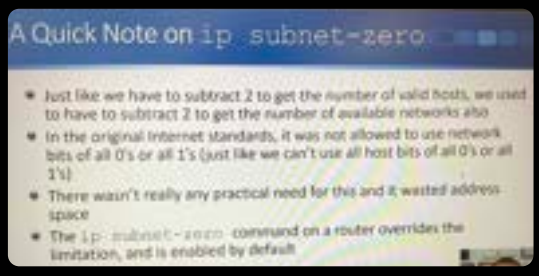
- $2^{hostbits} - 2$ (since 2 IPs are reserved)

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

* IP - subnet - zero



example :-

- Subnets 200.15.10.0/24
  Class C network /31
  24-31 = 7

— $2^7 = 128$ subnets available which accomodates
— $2^1 = 2$ subnets each
that means the Addresses will be
- 200.15.10.0 to 200.15.10.1
- 200.15.10.2 to 200.15.10.3
- etc. to
- 200.15.10.254 to 200.15.10.255

** /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.

— 200.15.10.0/24 → /30 — 255.255.255.252

/24 + 11111100
6
128+64+32+16+8+4
= 252

Subnets = 2^6 → 64
→ 64 available subnets
# of host in each subnet

$2^2 - 2 = 2$ bits/subnet

200.15.10.0/30 — range will be

200.15.10.1 — 200.15.10.2 (network.0 — broadcost.3)
.5 — .6 (network.4 — broadcost.7)

** — /30 and /31 both accomodate 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 200.15.10.0/24 → 200.15.10.0/29

200.15.10.0/29
↳ 255.255.255.248

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

—— VLSM - Variable length subnet mask.

— 198.22.45.173/26
L
255.255.255.192

Subnets available —

$2^2 = 4$

host each subnets
$2^6 - 2 = 64 - 2 = 62$

*** 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

→ 1 0 | 1 0 1 1 0 1

2^7 2^6 .... 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

# of subnets = $2^3 = 8$

$2^4 = 16 - 2 = 14$ host → 32 - 4 = 28

Subnet will be /28

Subnets = $2^4 = 16$ subnets

200.15.10.0/28

200.15.10.0 — 200.15.10.15

.16 — .32

.32 — .48

64 —

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

/28

— 135.15.0.0/16

/29

└ 255.255.255.248

Subnets available

— $2^{13} = 8192$

hosts per subnet

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

network Address? — 135.15.10.138/29

32-29 = 5

138

10001 010

5

.136

— Class A → 60.0.0.0/8

Subnet mask → 255.255.255.240

24+4 = /28

Ans → 60.0.0.0/28

- # available subnets =

/8 − /28 = 20

2^{20} = 1,048,576 → Available subnets

- # host available per subnet

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

60.0.0.0/28

— 60.0.0.0 — 60.0.0.15

.16 — .32

— 60.15.10.75/28

32-28 = 4

network Add —

75

0100 1011

→ 60.15.10.64/28 → network Address

— # available subnets — 24 − 28 = 4

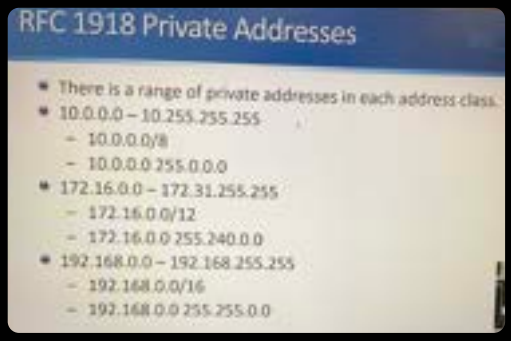
2^4 = 16 available subnets

host

$2^{hostbits} - 2$

2^4 = 16 host/subnet including 2

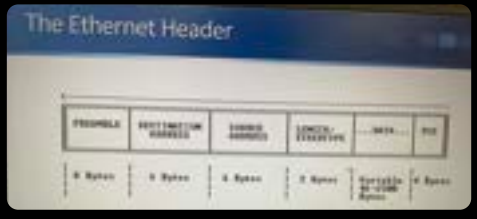
— Private Ip Address range
RFC – 1918 → Private IP Add.



— 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

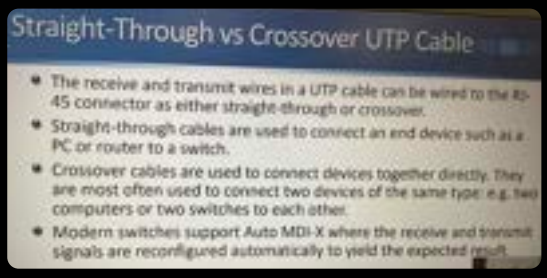
L1 — Layer – 1
physical layer

— Connections
  — Coaxial – no longer used
  — Twisted pair
  — fiber cable → single mode – longer distance, higher bandwidth expensive.
                → 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 11 –

L7 – 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 @L2&L1 and will typically have awarness up to Layer 7.

Students 456

60.0.0.0/8 → 119

subnets → 8-19 = 11

2^{11} = 2048 subnets —①

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

= 19 - 32 = 13

1.2 Ans

2^{13} = 8192 - 2

Available hosts = 8190 ∫subnet — ②

Routers can route traffic betn networks

switch ——|| —— Hosts

Routers supports many types of interfaces
- Ethernet
- ISDN
- ADSL
- Serial
- Console
- Auxillary

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 request 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 fa 0/0
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 VLAN 1 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

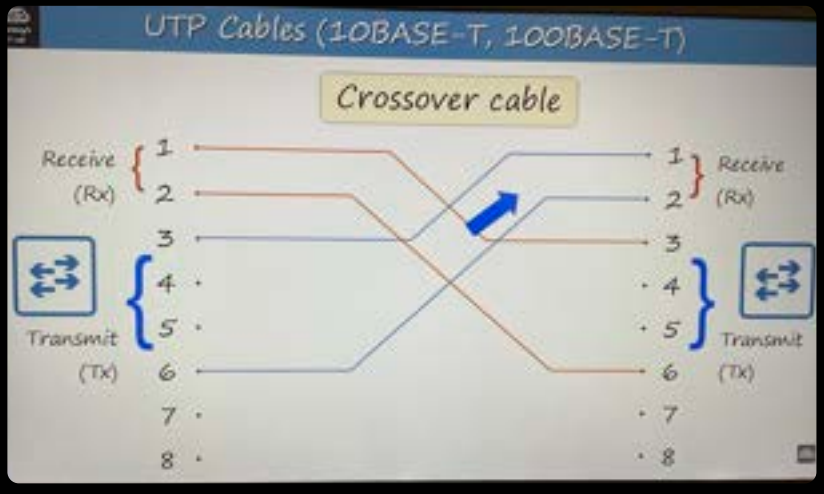
PC sends data from pin 1 & 2 (TX – 1,2)
receives data from pin 3 & 6 (RX – 3,6)

- Router
  sends data from pin 1 & 2 (TX – 1,2)
  receives data from pin 3 & 6 (RX – 3,6)

- Switch
  sends data from pin 3 & 6 (TX 3,6)
  receives data from pin 1 & 2 (RX 1,2)

Router – to-router connⁿ —
or Router – to – PC – connⁿ –

— cross-over cables are used to connect R to R or SW to SW or R to P
so
connection will be like this.



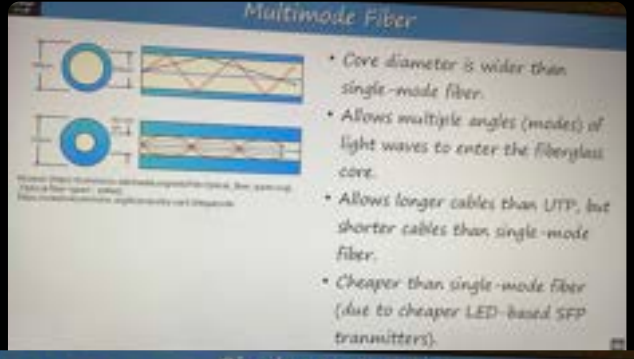
Device Type	Transmit (Tx) Pins	Receive (Rx) Pins
Router	1 and 2	3 and 6
Firewall	1 and 2	3 and 6
PC	1 and 2	3 and 6
Switch	3 and 6	1 and 2

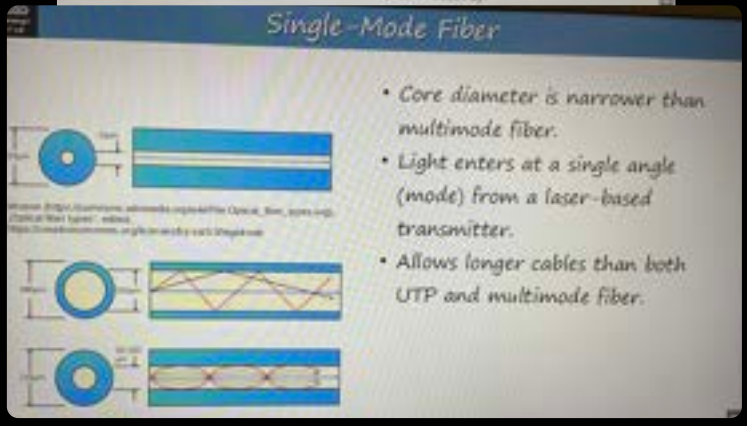
• • • • • However, Newer devices comes with Auto-MDIX features Which automatically adjust itself either straight & cross connection it will take of sending info.

• • • for 1000BaseT or 10GBaseT all 8 ports are used.
— for this 1000BaseT & 10GBaseT each pair of wire bidirectional.

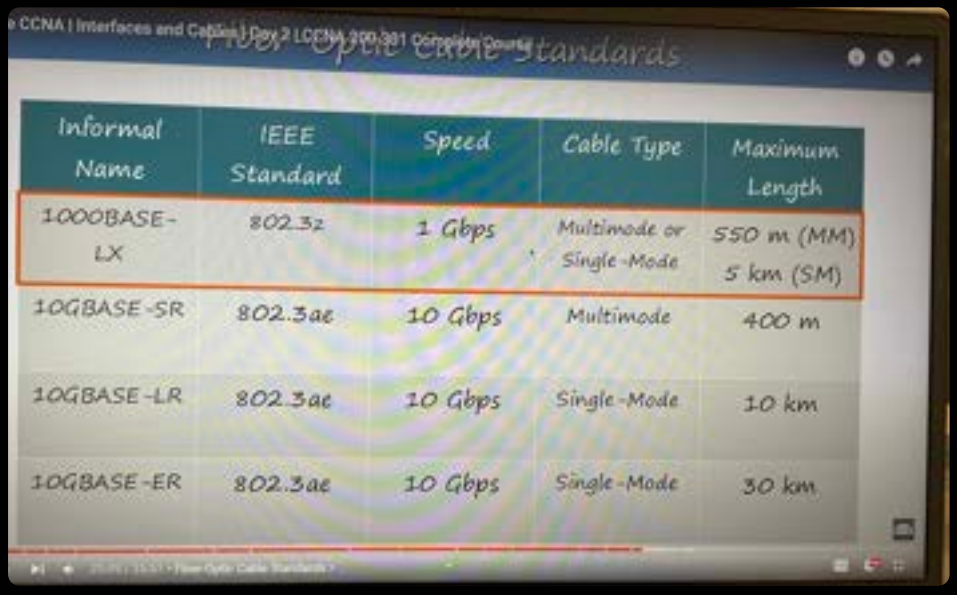
Old copper wire limitations
① Limited to 100m.

— New Technology wires.
connector — — SFP (small form-factor pluggable) Transreciever
Wires — fiber optic cables
- Single mode
- multi mode





- fiber optics standards



Day-3

Layer 7 function
- Identifying communication partners
- Synchronizing communication

L6 - Presentation layer - Encryption of data

... — Transport layer provides Host-to-Host comm^n

- Application layer provides process-to-process comm^n

Day 4 - Basic Encryption 4 Password set

① Password set —
Go to global config mode

(config) # service password CCNA-Pass

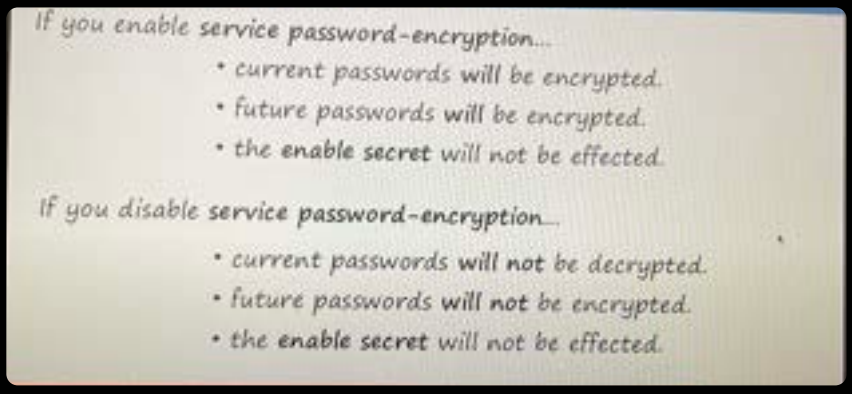
R1 # Show running config
→ startup config

\# # # To Save config inside a startup

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

\# # # (config) # service password-encryption

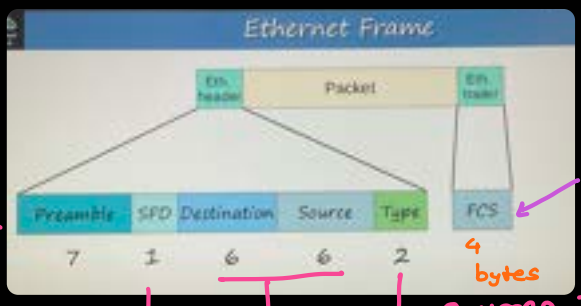
To disable → no service password-encryption



> = 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



frame check sequence

greater than 1500 = Type IPV4 or IPV6

less than 1500 means indicating length of packet

allows devices to synchronize their receiver clocks

Source
type

6 byte = (6x8) = 48 bit — MAC Addresses

↳ start frame Delimiter
length 1 byte (8bits) – 10101011
• Marks the end of the preamble & begging of the preamble

Total size = 26 bytes

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

— Mac addresses on cisco switches stays for 5 minutes if no activity for that addresses 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 n/w with that frame

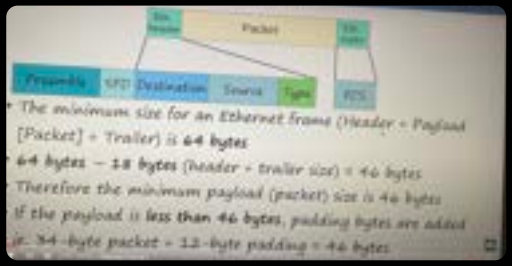
Day 6 —

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

6+6+2+4 = 18 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 0 2cf. ABCD .0211

clear for interface

SW1 # clear mac address-table dynamic interface Gi 0/0

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

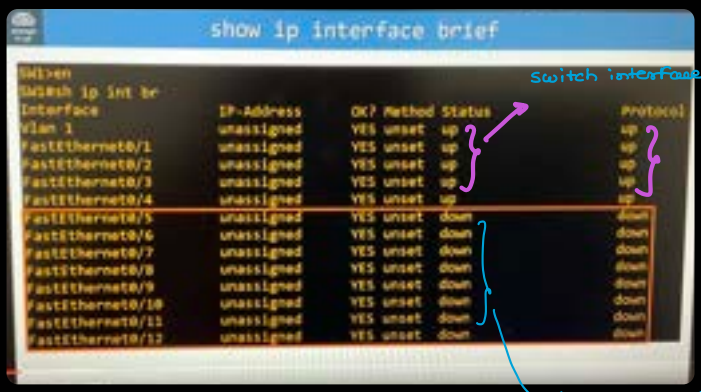
... # show ip interface brief

* 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 g 0/0
description description_Here

Day 9 – Switches interface

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



show interfaces status

SW1 # conf t

SW1 (config) # int 0/1

speed 100

duplex ?

duplex full

manually setting speed & duplex

description #to R1

sh int status

(config) # interface range f0/5 - 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

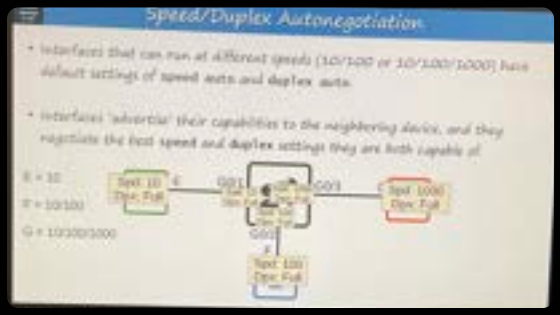
sw1(config)# int range f0/5 - 0/6, 0/9 - 0/11

• • • — To deal with collusions in half-duplex situation CSMA/CD is used

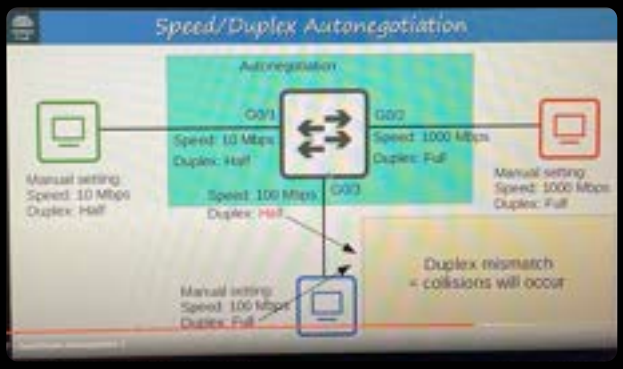
CSMA/CD

— Carrier Sense multiple Access with collision Detection

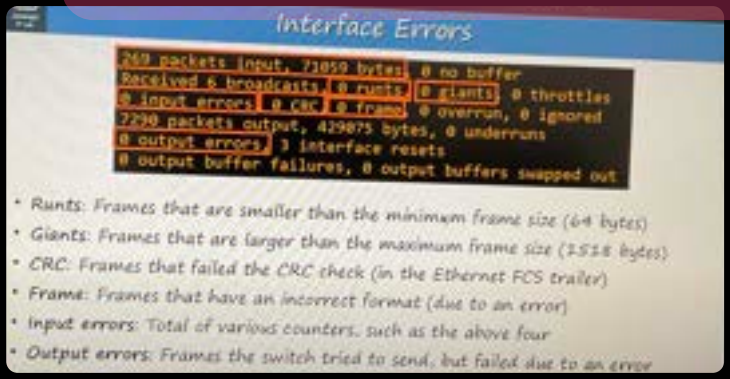
— Speed/Duplex autonegotiation



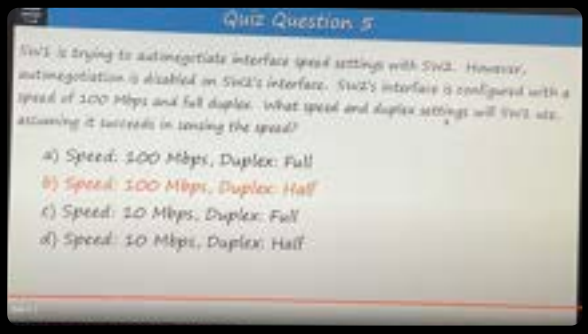
ex. 2 Where autonegotiation is only active on sw1



show interfaces or show interfaces f0/1



• • • • Autonegotiation can only able to sense and match Speed not the duplex if there is mismatch betn duplex mode Collusion will occure



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 (5×4 = 20 bytes)
   - maximum is (15×4 = 60 bytes)
   - minimum IPV4 Header length = 20 bytes
     max ——|—— = 60 bytes

3. DSCP - Differentiated services code point
   Length - 6 bit
   Used for QoS (Quality of service)

QoS - used to prioritize the delay sensetive 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 packets (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 Longer 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 packet
   - Allows fragmented packets to be reassembled even if the fragments arrive out of order.

9. Time to Live - 8 bits → so 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 decreses 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
89 — OSPF

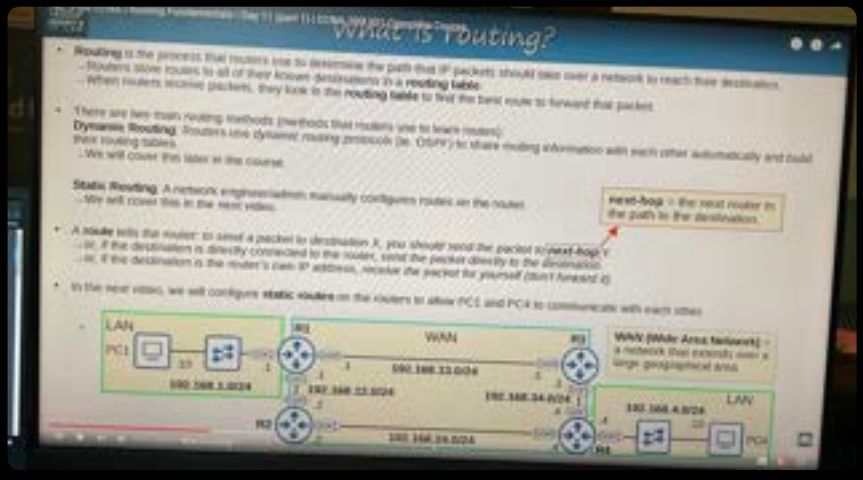
11.
- Header checksum — 16 bits
- checksum used to check for errors in the IPV4 header.
- if both checksums doesn't match that means error has occured.

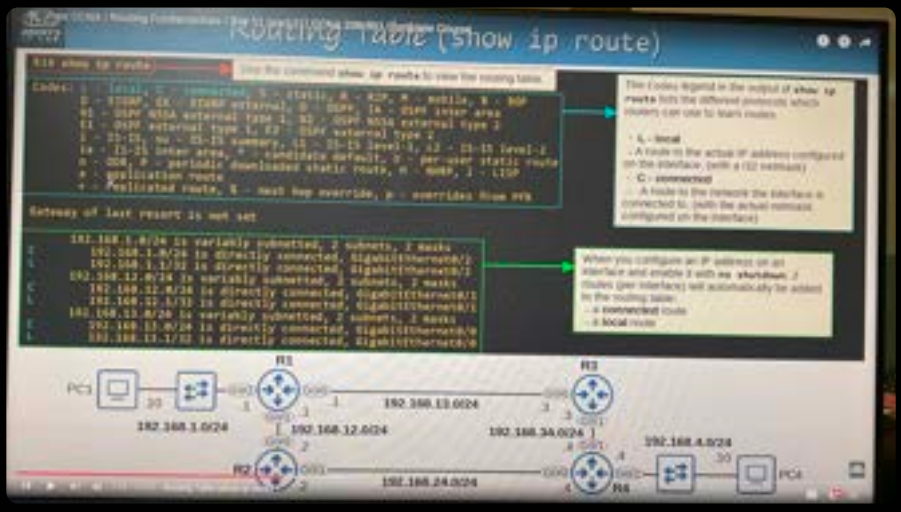
12. Src IP - 32 bit
Dst IP — 32 bit

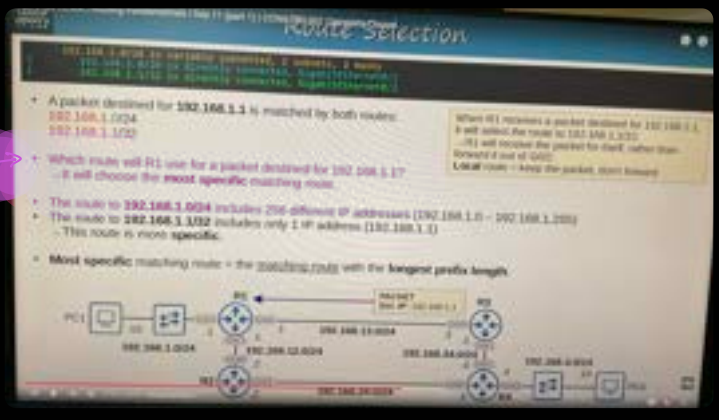
13. Options — 0 - 320 bits
Rarely used
if IHL > 5 that means options are present

0x → Indicates Hexadecimal

Day 11 - Routing P1







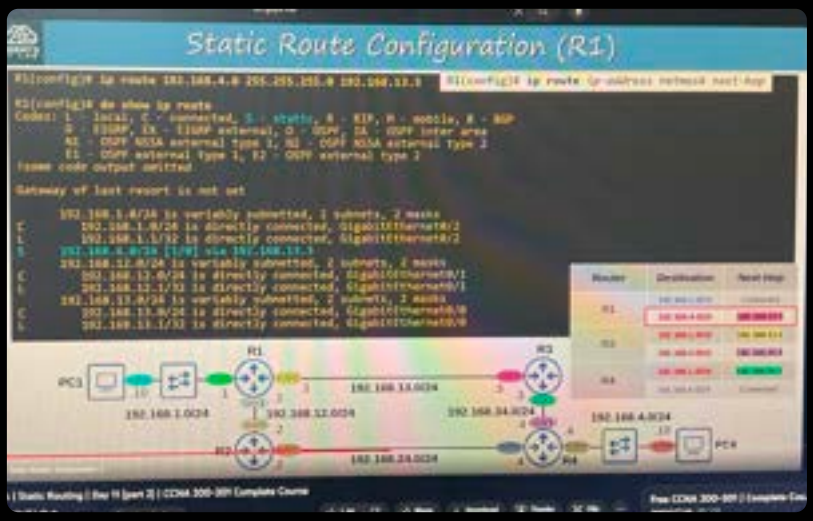
Imp

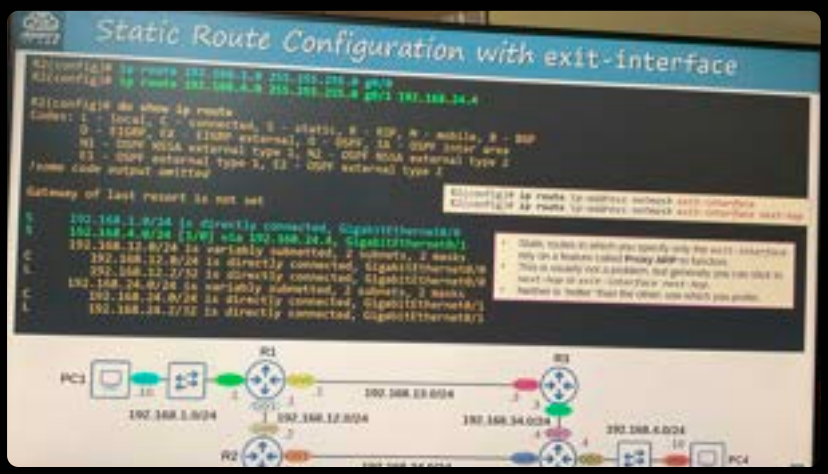
• • • When router doesn't receives a random package which is not in the routing table He will not forword to other interfaces likes switches do

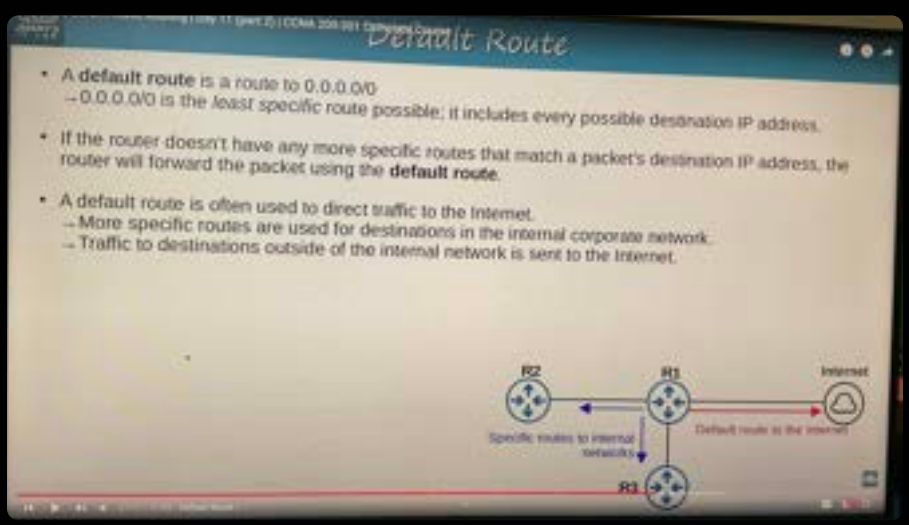
• • • When you configure an IP address on an int and enable the int, two routes are automatically added to the routing table
- Connected route (C)
- Local route (L) — exact IP of int /32

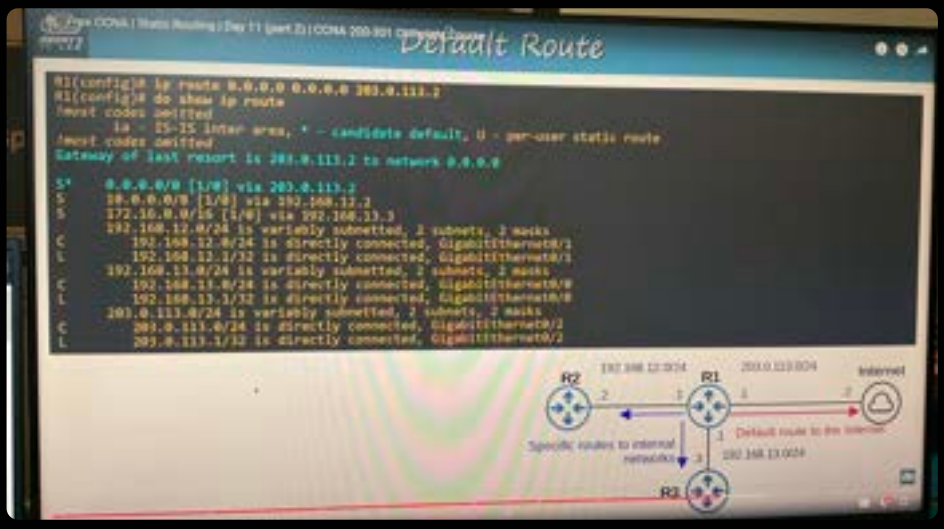
Day 11 - P2 - Creating static routes

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









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
	20/24	? 192.168.24.4
R4	1?0/24	? 192.168.24.2
	192.168.4.0/24	Connected

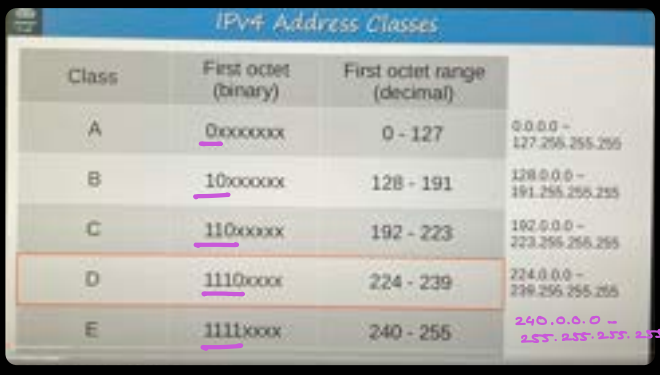
Day 12 - ARP

- ARP request — Broadcast
  ARP reply - unicast

Day 13 –

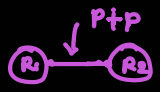
IPV4 Address classes

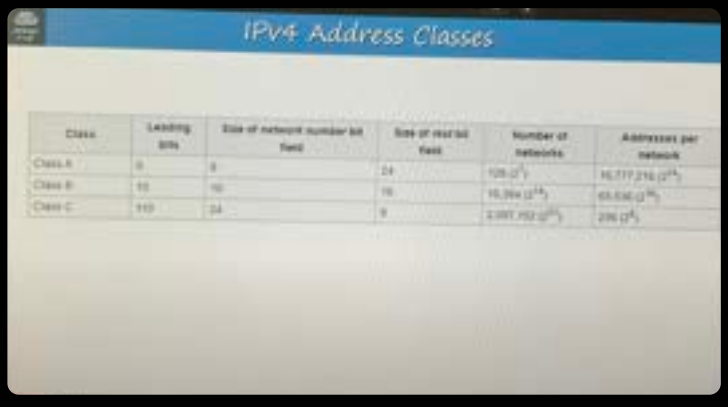
easy way to remember classes



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 ex. 



IPV4 Address Classes

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 do

Number of subnets = 2^x = number of subnets

(x = number of 'borrowed bits')

so here we need 5 subnets of 2^3 at minimum required = $2^3 = 6$

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

$2^{\text{host-bits}} - 2 = 2^5 - 2 = 32 - 2 = 30$

So the range will be

- 192.168.255.0/27
- 192.168.255.32/27 } difference of 32
  - .64
  - .96
  - .128

5

Ex. 10.0.0.0/8 → Create 2000 subnets

$2^{11} = 2048$

$8 + 11 = /19$

Number of Host

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

② 10.217.182.223/11

① Network address

Network ID — 10.192.0.0/11

So max is 1 1 1 ← 223

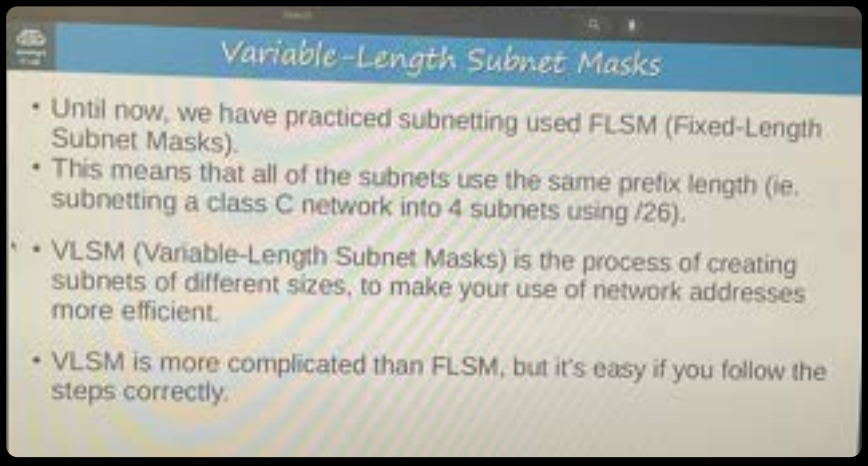
that means

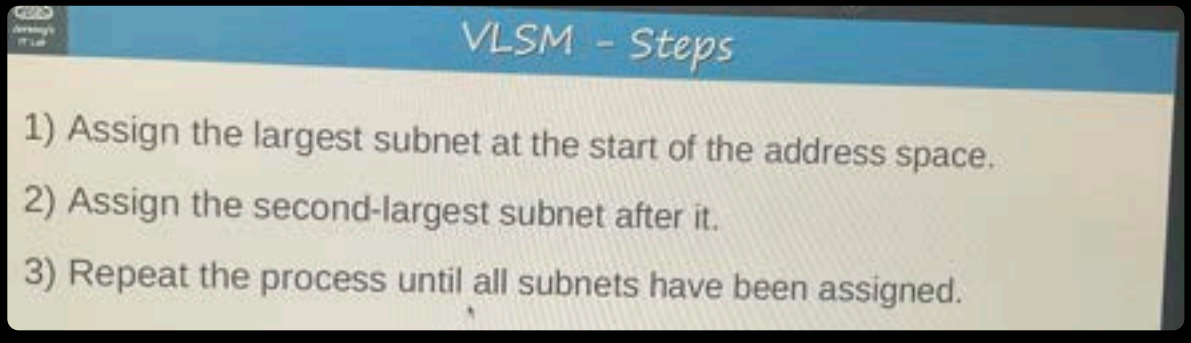
① Network Add — 10.192.0.0
② first usable — 10.192.0.1
③ Last usable — 10.223.255.254
④ Broadcast Add — 10.223.255.255

Num of host bits =

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

VLSM - Variable Length Subnet Mask





192.168.1.128/26

26 = 64

No. of host
= 26 - 2 = 64 - 2 = 62

N/w first — .128
Last usable — .129
Broadcast — .190
.191

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 2^7 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 26 = 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 /28 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 usable — .209/28
L ⊣⊢ — 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 seperate networks
② Reduce Broadcast / unknown unicast floods
③ Increase security

••• Without VLAN we can seperate diff depots 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 accesspost is a switchpost which belongs to a singlevlan, usually connects to end hosts like PCs

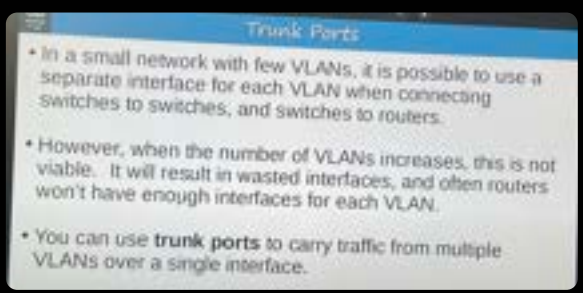
** switchports which carry multiple vlans are called as "trunk ports"

```
# 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

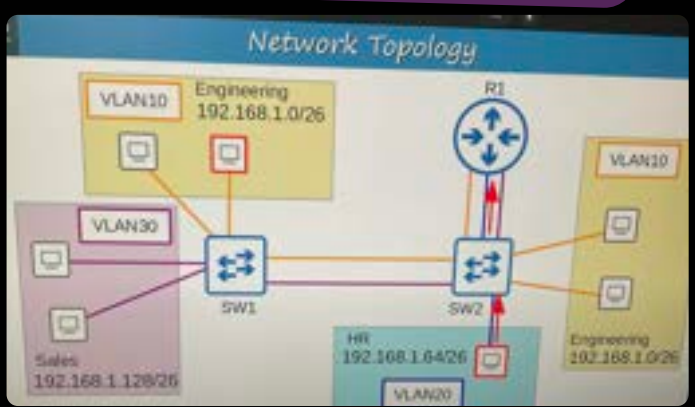
- Trunk ports



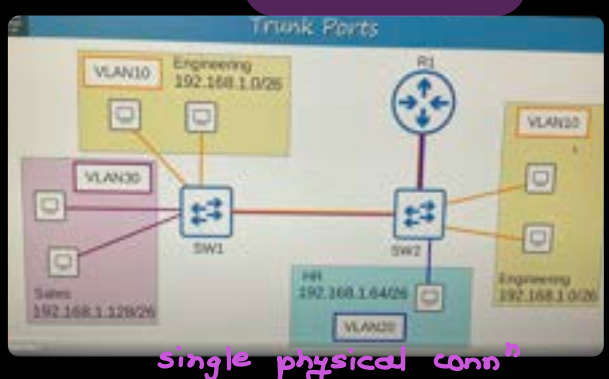
So basically rather than creating multiple seperate connections for VLAN's via access port to communicate we use trunk ports to send multiple VLANS connection through single cable.

ex.

This is Access port VLAN
aka untagged ports



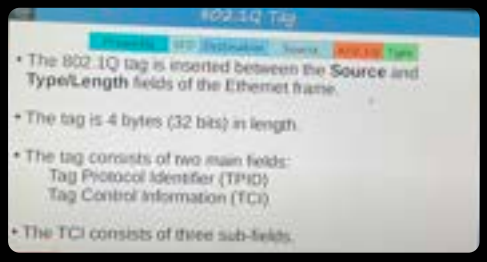
This is trunk port
tagged port

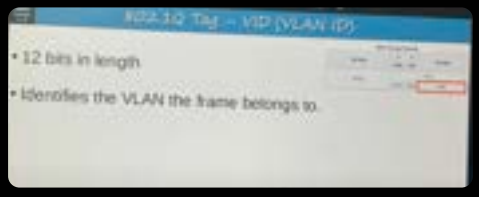


single physical conn"

- 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 port. → 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

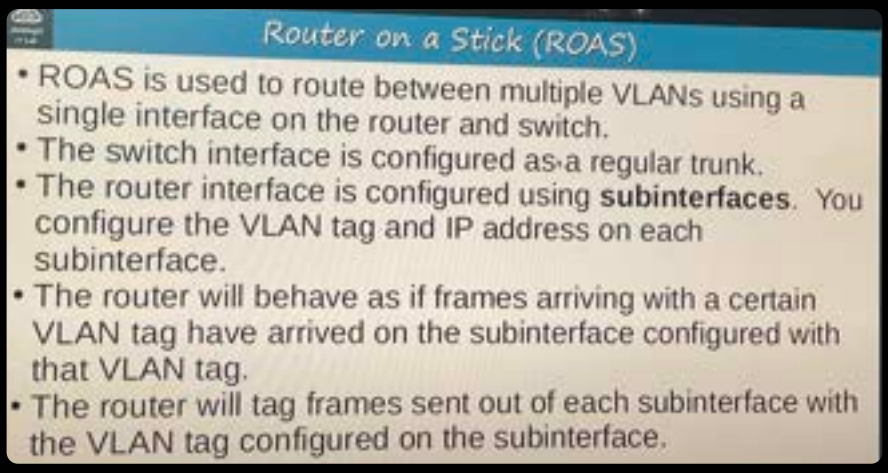
••• # show vlan brief command does not show trunk port
- use show interface trunk

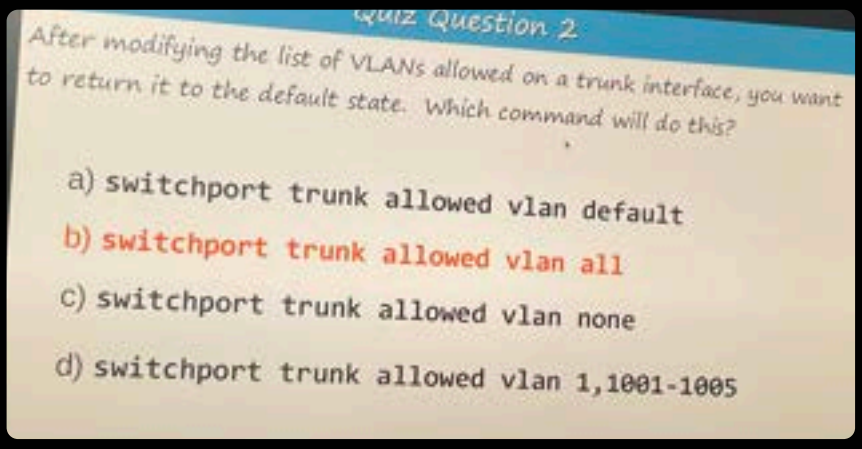
- Router on a stick

When we have multiple vlan's configured on switch and we want to use the single link bet^n 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
repeat for all
int g0/0.10
encapsulation dot1Q 10
ip address 192.168.1.62 255.255.255.192

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





#4 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 there the trunk (dot1Q) will have conjestion 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

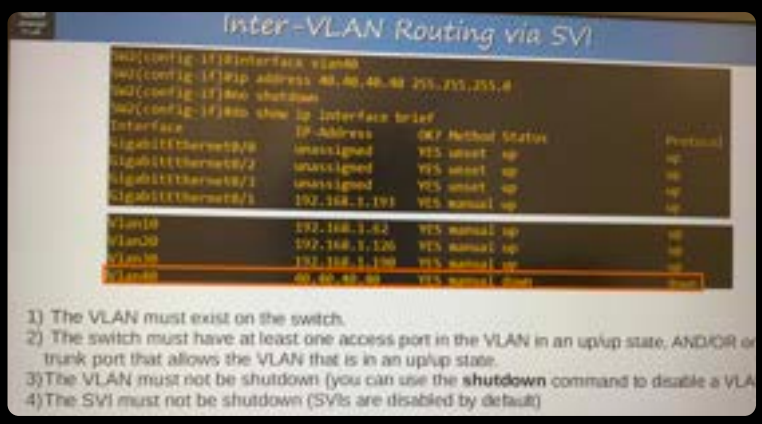
also,

```
(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)

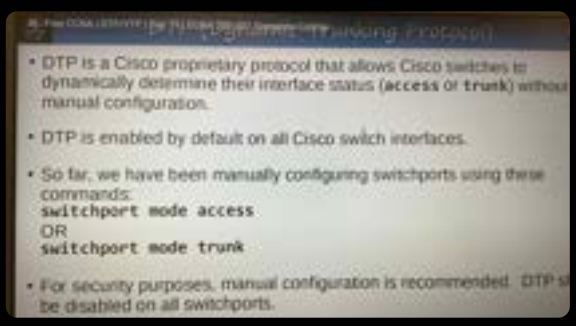
- SVI are shutdown by default, so remember to use no shutdown



Day 18's Lab is to do

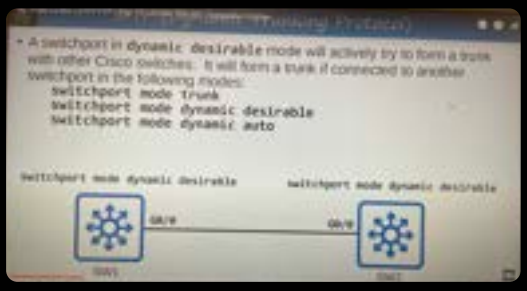
Day 19 – DTP/VTP

- DTP – Dynamic trunking protocol
  VTP – VLAN Trunking protocol




```
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.

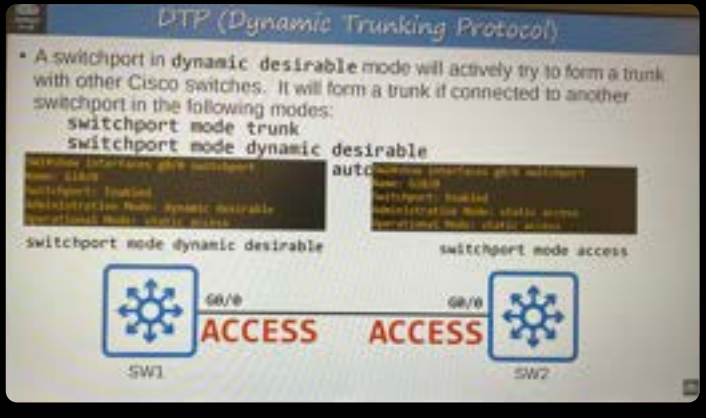
– Its more passive → it communicates with other switches that if you want to form a trunk, i will form a trunk.

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

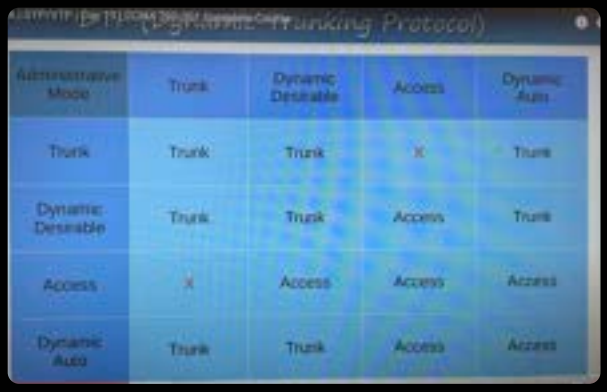


ex. if two switchports are

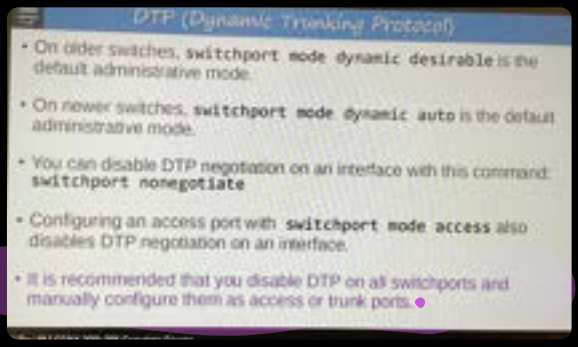
{ one manually trunk mode
{ other manually access mode

✕ Missmatch will occure.
error

Summerization chart



- 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 nonegotiation
OR
- Switchport mode access can disable it too

- Recommendation
  → Disable DTP on all switchport manually set them on access or trunk

Day 20 -

STP - Spanning tree protocol

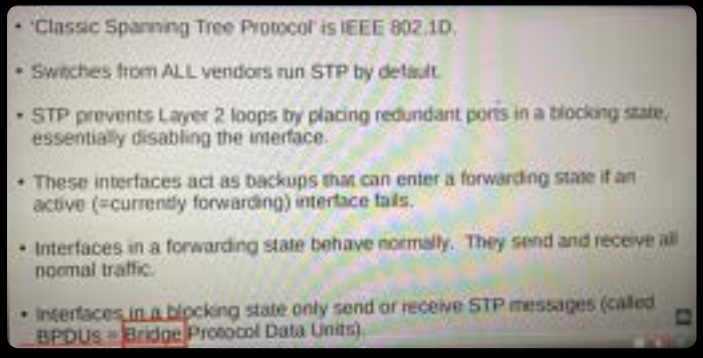
- Redudancy protocol which works on L2.

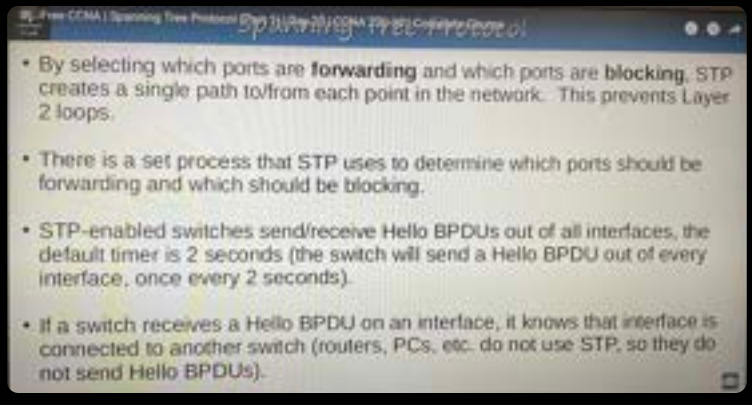
STP is solution to
- Broadcast storms

••• classic Spanning tree protocol is

IEEE 802.1D
STP runs on all switches by default

-





① Election one root bridge

for election priority and Mac address is compared

By default priority on all switches = 32768

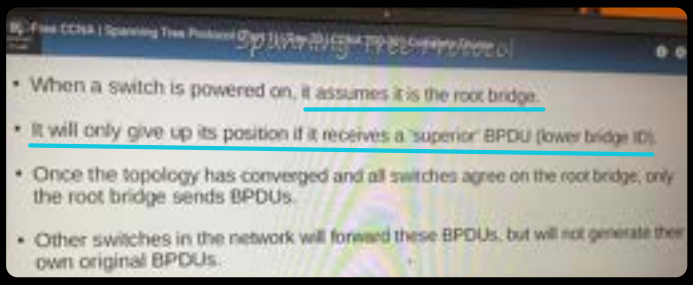
•• if priority is matched the MAC address is compared.
lowest mac address wins.

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

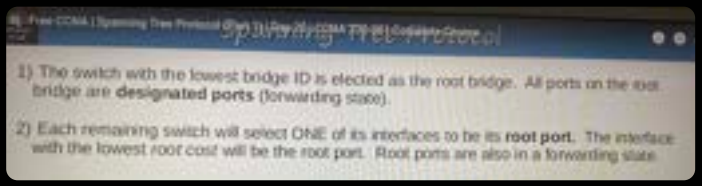
— So if there are multiple VLANS

→ VLAN 2 will have 32770

VLAN 3 will have 32771 priority

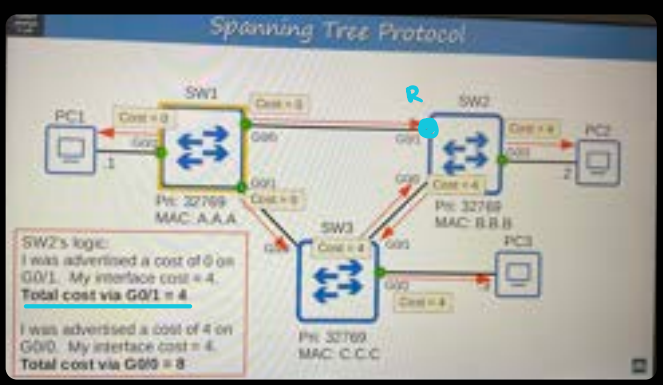


• All ports on the root bridge are under designated ports (forwarding state)

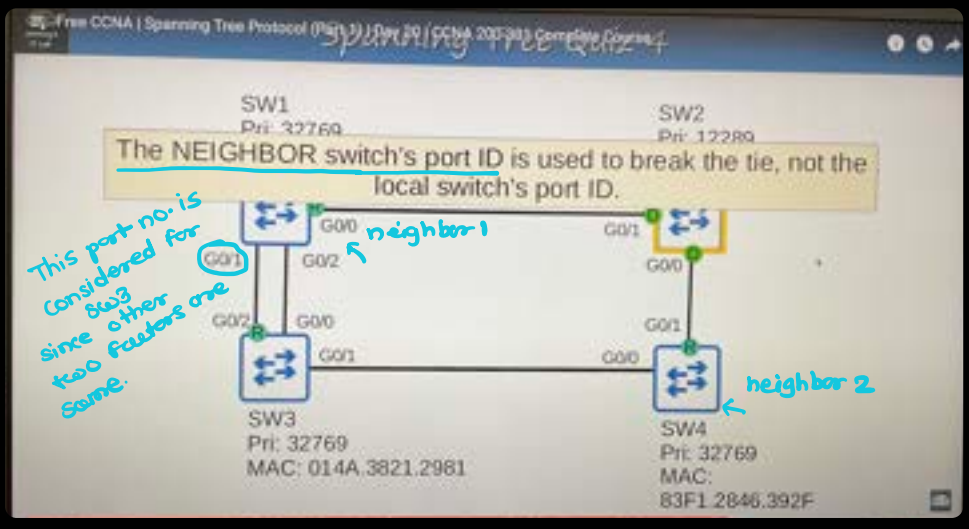


To find the root ports for STP.

This port will become root port →



Confusing part



R- Root ports
D- Designated port (forwarding state)
N- non designated (Blocking state)

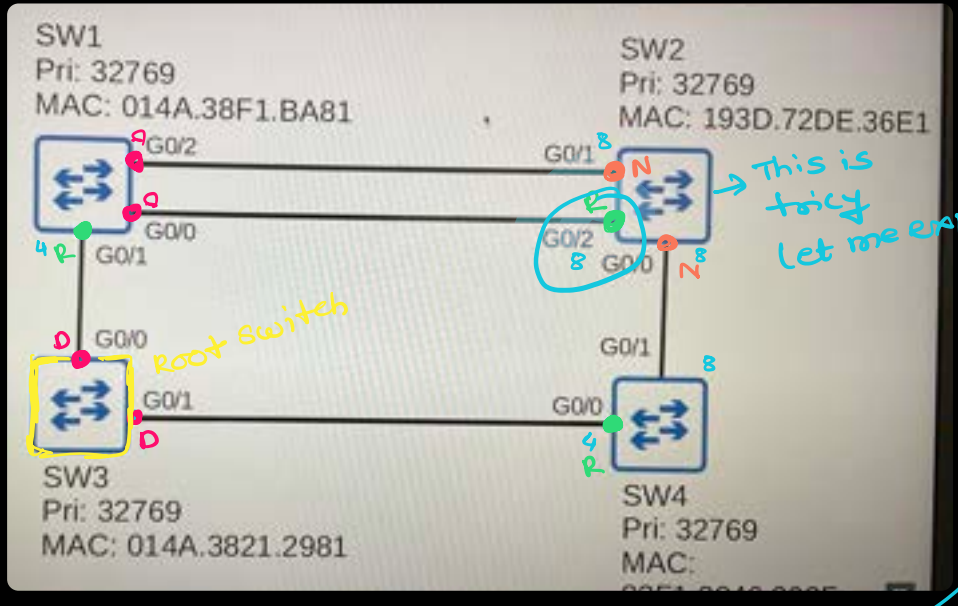
** Every collusion Domain has a single STP designated Port.

Imp for STP 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 ② lowest MAC Address

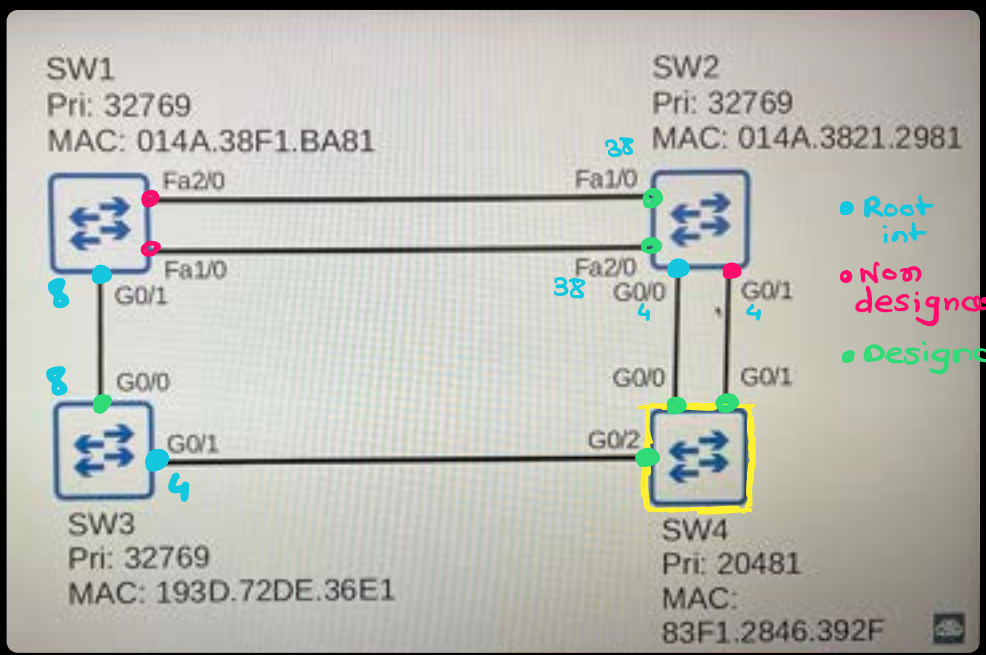
2) Each remaining switch will select ONE of its interfaces to be its **root port** (forwarding state). Ports across from the root port are always **designated** ports.
Root port selection:
1: Lowest root cost
2: Lowest neighbor bridge ID
3: Lowest neighbor port ID

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

Example 2: →



Root switch port becomes designated ports by default

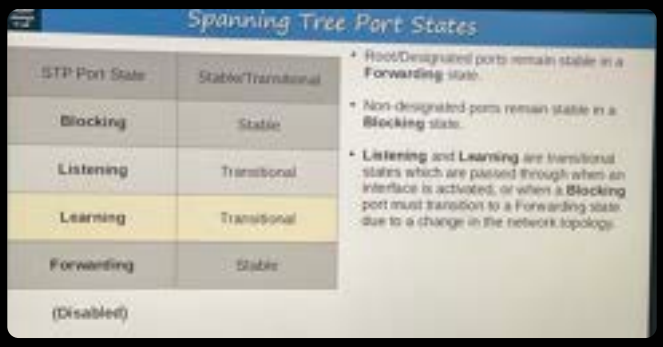
- The interface connected to root port is alway designated.

SW3 # show spanning tree
also specific to vlan

show spanning tree vlan1
show spanning tree detail

show spanning tree summary

Spanning tree Port states



15sec
15sec

BPDU's – Are message exchanged between bridges participating in STP.

BPD's DO following

① Root Bridge Election
② Topology information
③ Loop prevention
⑤ Convergence

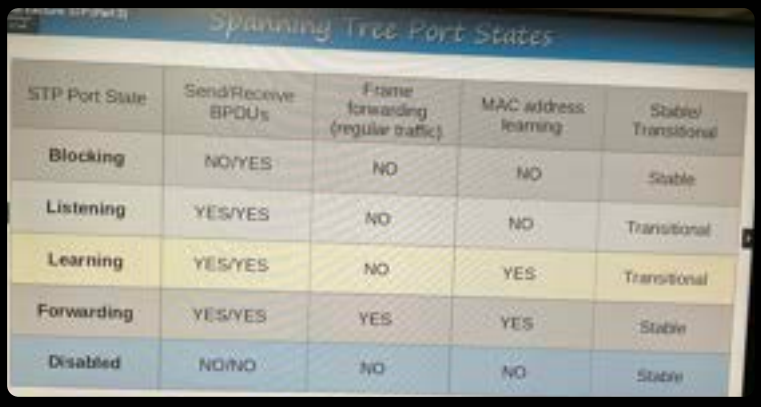
Non-designated ports are always blocking

① Listening state is 15 sec long by default
• interface in listening state only forwards / receives BPDUs → It does not send/or normal traffic.

② Same for Listening state.

but in Listening it learns the mac addresses of regular traffic

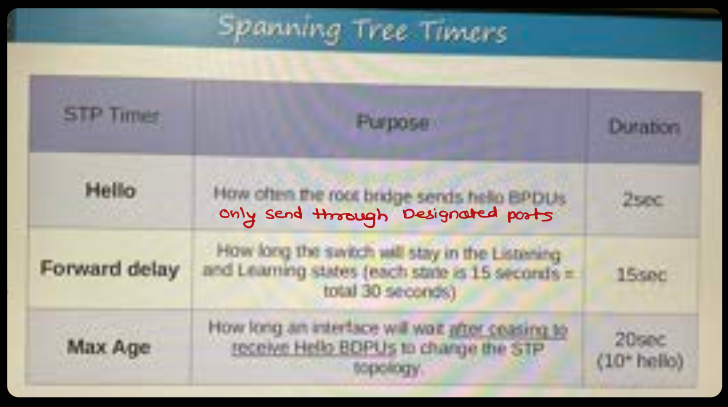
③ forwarding state



Spanning Tree Port States

STP Port State	Send/Receive BPDUs	Frame forwarding (regular traffic)	MAC address learning	Stable/ Transitional
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 BDPUs 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 BPDU Guard is used

To enable BPDU →

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 → Per-Vlan ST

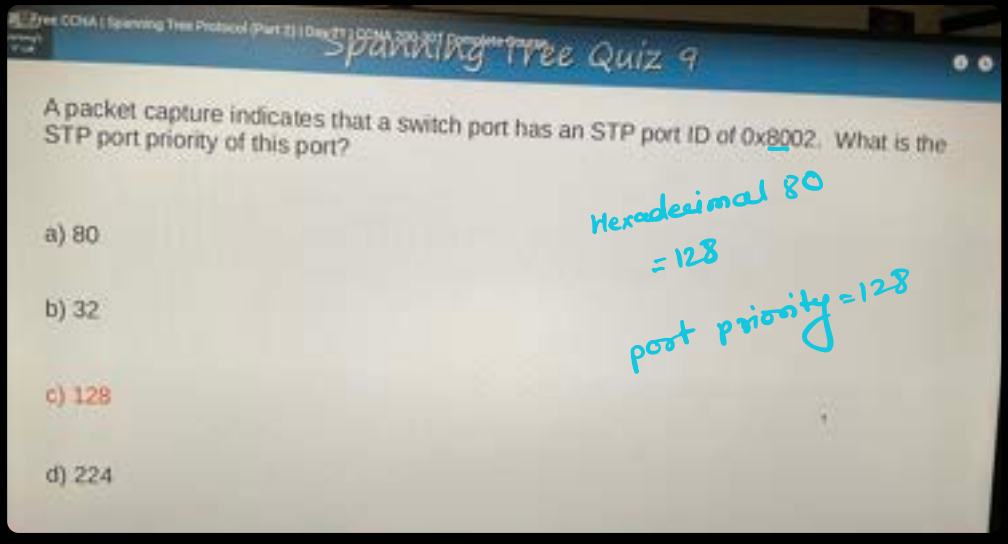
rapid-pvst → Per-Vlan rapid ST ← moder cisco default

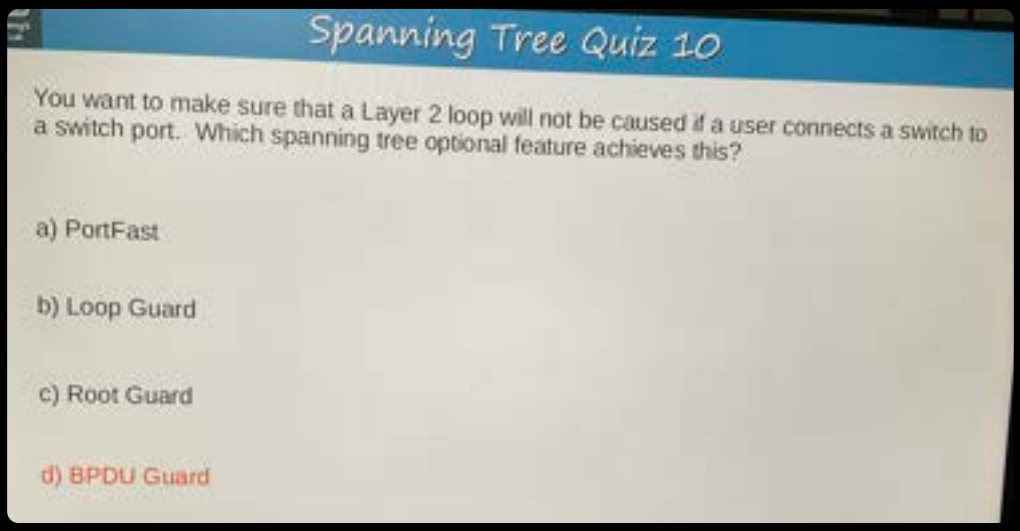
To manually set spanning-tree root switch

SW1 # spanning-tree vlan1 root primary.

vlan1 root secondary

Load Balancing.





Day - 21 → Lab

show spanning-tree

* TO change the port cost to manually change the root port / designated port setups

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

cost range 1-240

* Setting up portfast

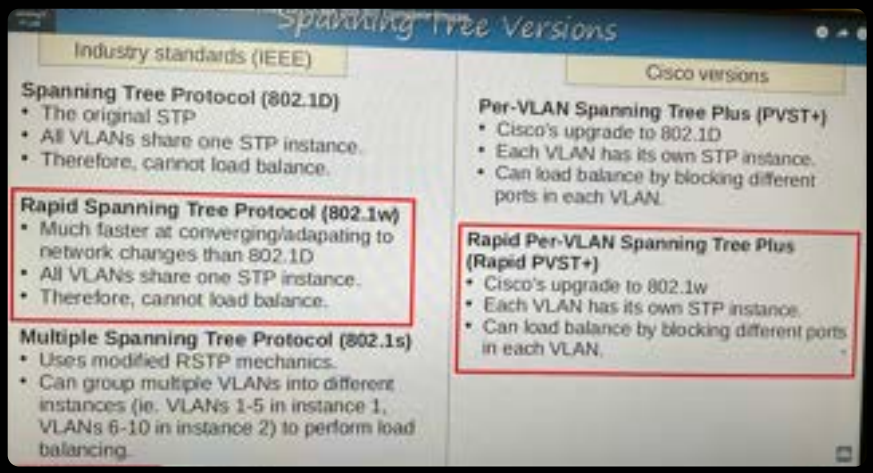
int f0/3
- spanning-tree portfast
- spanning-tree bpduguard enable

... Rapid Per-Vlan spanning tree PVST+

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

The problem with pvst was that it takes 50 sec (15 for listening, 15 forwarding + 20 msg 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.



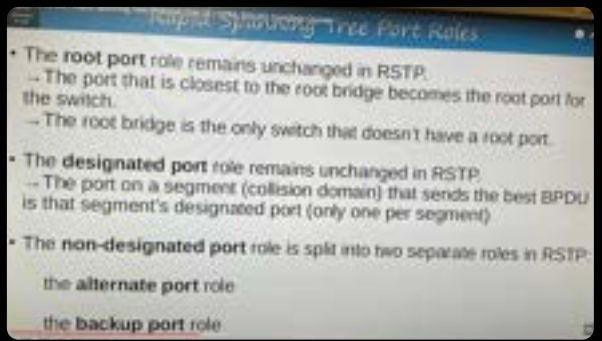
PVST+ or RSTP cost

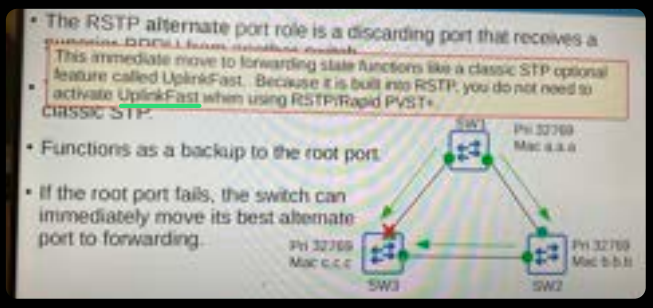
Speed	STP Cost	RSTP Cost
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2000
100 Gbps	X	200
1 Tbps	X	20

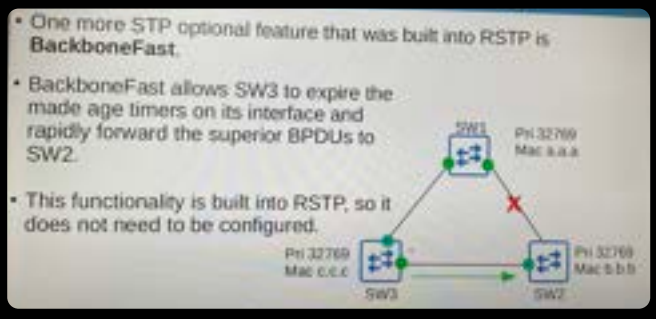
RSTP port states

STP Port State	Sends/Receive BPDUs	Frame forwarding (regular traffic)	MAC address learning	Stable/ Transitional
Discarding	NO/YES	NO	NO	Stable
Learning	YES/YES	NO	YES	Transitional
Forwarding	YES/YES	YES	YES	Stable

- if a port is administratively disabled (**shut down** command) = discarding state
- if a port is enabled but blocking traffic to prevent Layer 2 loops = discarding state





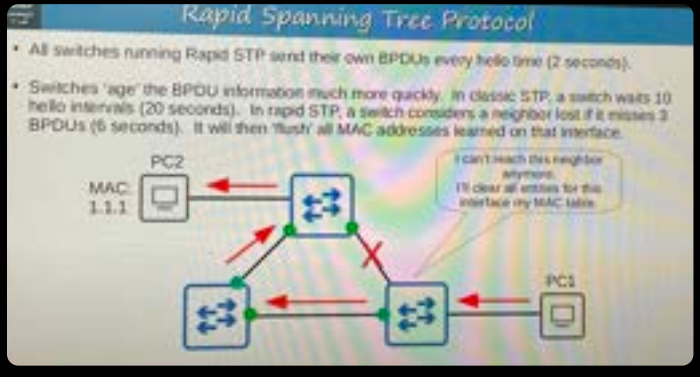


Configuration →

- 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
  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^n
③ shared Link → switch — Hub

Manual configuration

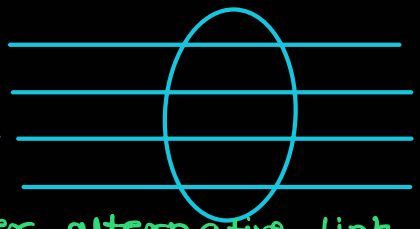
for edge ① spanning-tree Link type point-to-point
② interface f0/24
– spanning-tree portfast

– Day 23 - Etherchannel

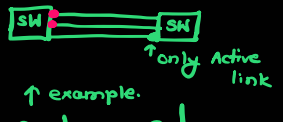
Oversubscription — When the bandwith of the interfaces connected to end hosts is greater than the bandwidth of the connection to distribution switch(es).

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 under alternative link means not used to prevent that happening we use etherchannels bet^n switches if we want to allow traffic



↑ example.

- STP will treat this group as a single interface

- Etherchannel also know as Port channel or LAG
LAG(Link aggregation group)

- Etherchannel allows the load Balancing based on diff types

Configuration

ASW1# 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

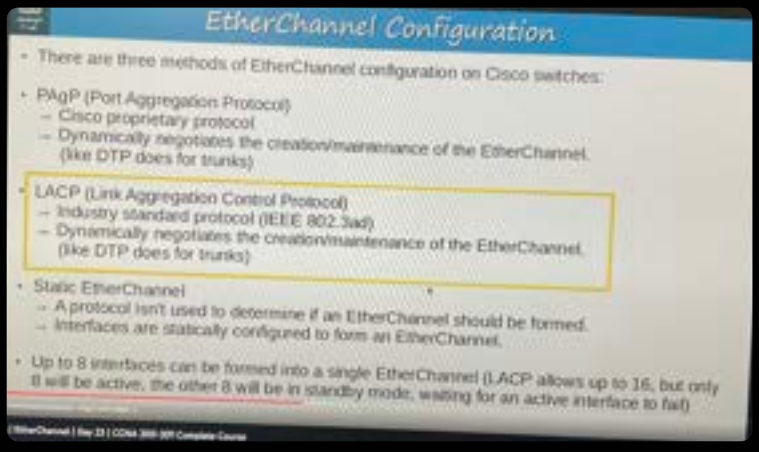
Three methods available

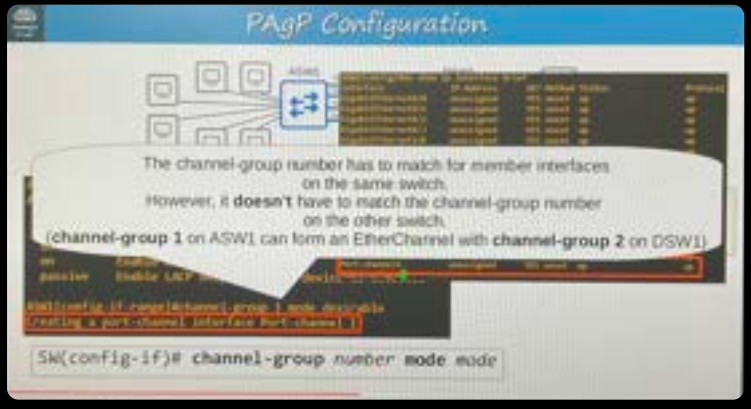
① PAgP (Port Aggregation Protocol)
   – Cisco only protocol

② LACP- Link Aggregation Control Protocol

   ↳ Industry standards (IEEE 802.3ad)

③ static Etherchannel
   → Avoid to statically.

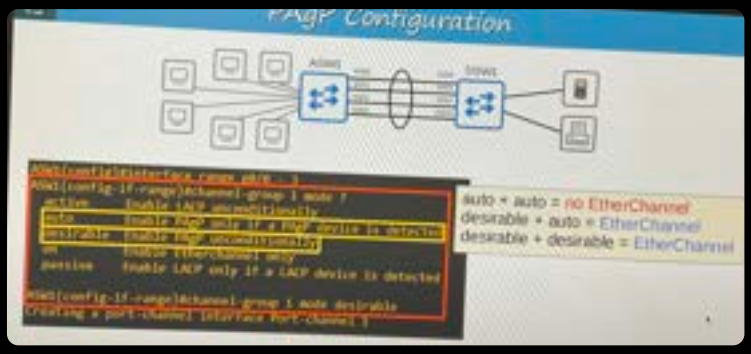




for LACP if both ends are configured like this
Passive + Passive = no Etherchannel
active + active = Etherchannel

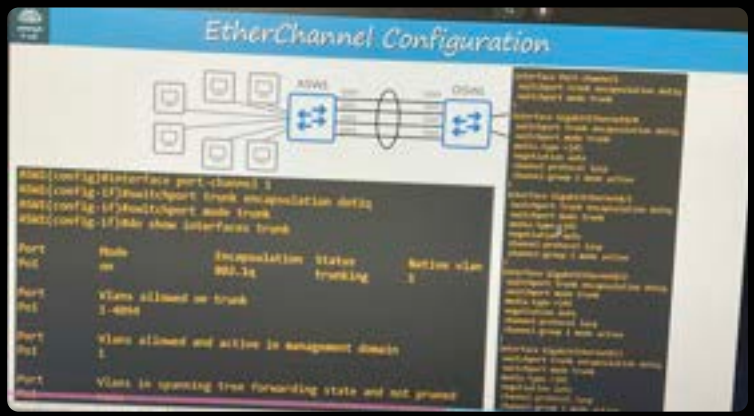
active + passive = Etherchannel.

and for PAgp ⟶

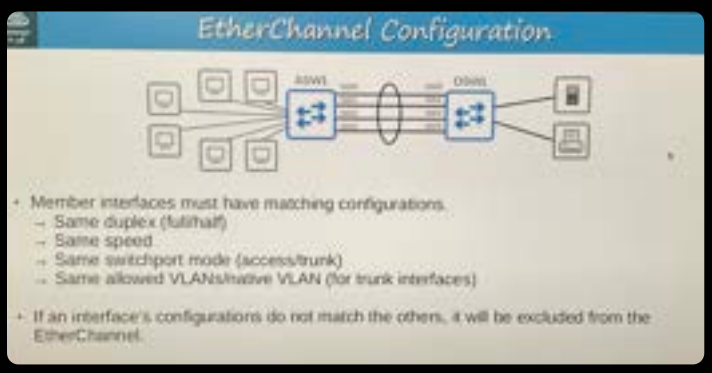


channel-protocol lacp } not much used commands
pagp

- then thoes logical links can be configured as a trunk



To be a Etherchannel Link member infaces must have ⟶



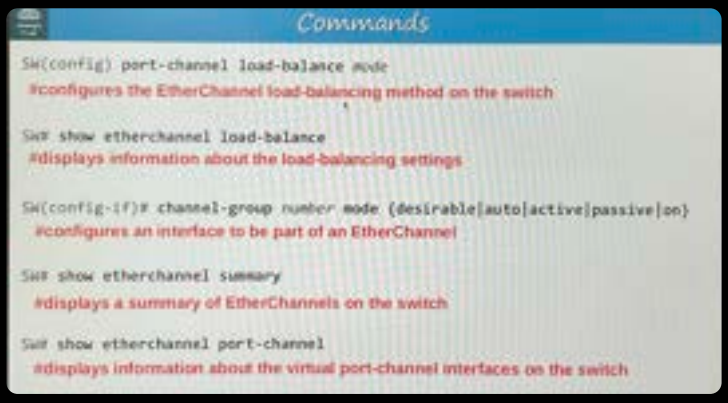
show etherchannel summary
show etherchannel port-channel

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 g 0/1 - 2
channel-group 1 mode active LCAP
int po1
switchport mode trunk

if switch also supports ISL then we have to

switchport trunk encapsulation dot
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

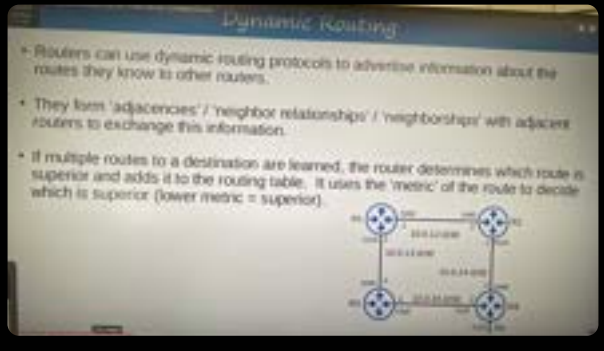
do sh etherchannel load-balance

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

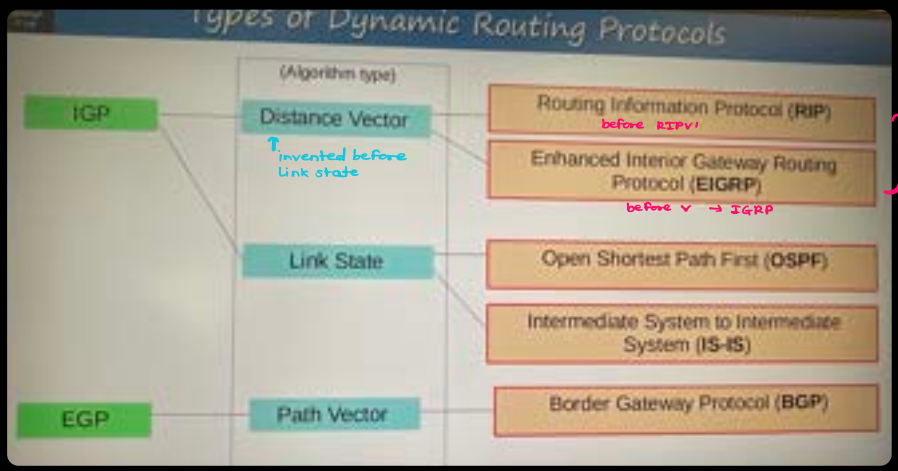


Different types of Dynamic routing

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



routing by rumor

② EGP – Exterior Gateway protocol

Used to share routes b/w different AS

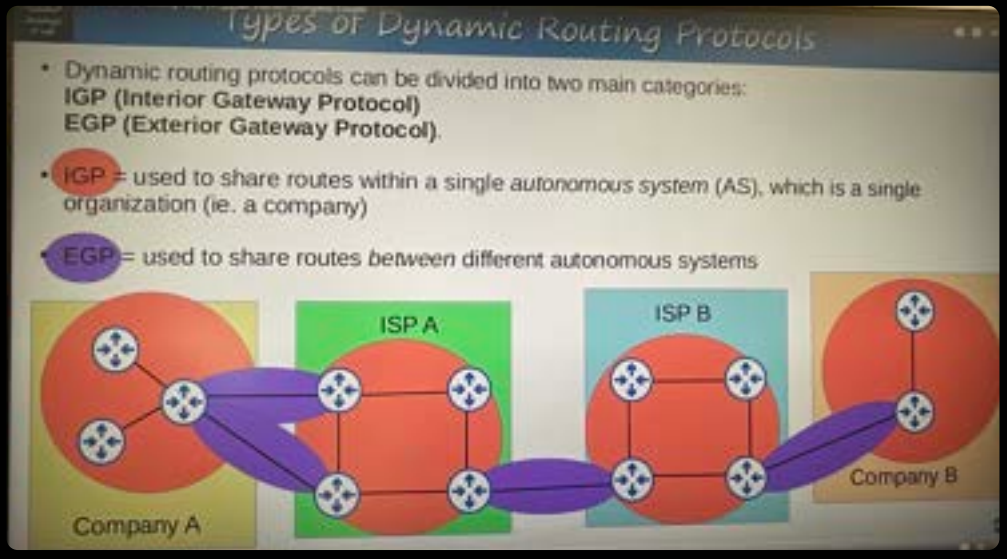
Only one → Path vector → ex. BGP (Boarder Gateway protocol)

EGP used to share route information b/w routers.

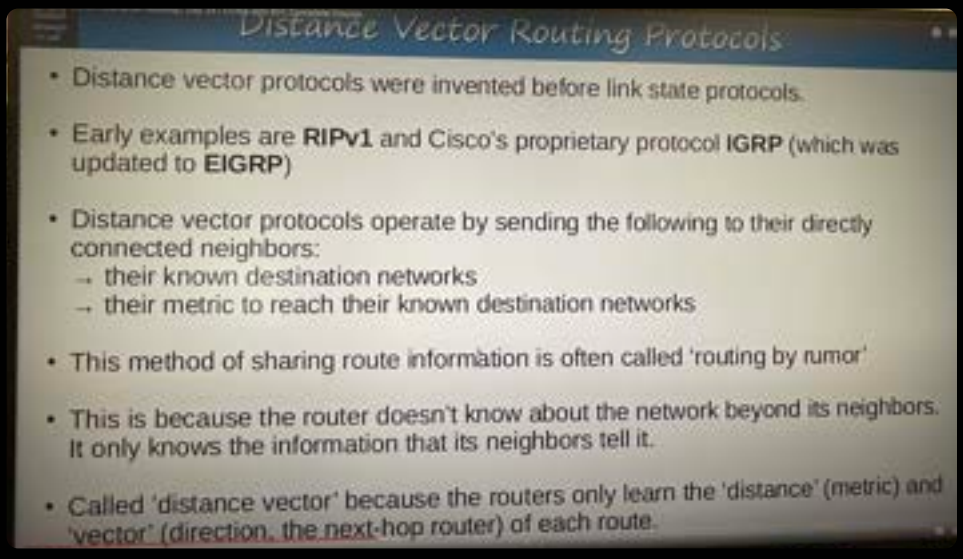
EGP type → (only one)

① Path vector

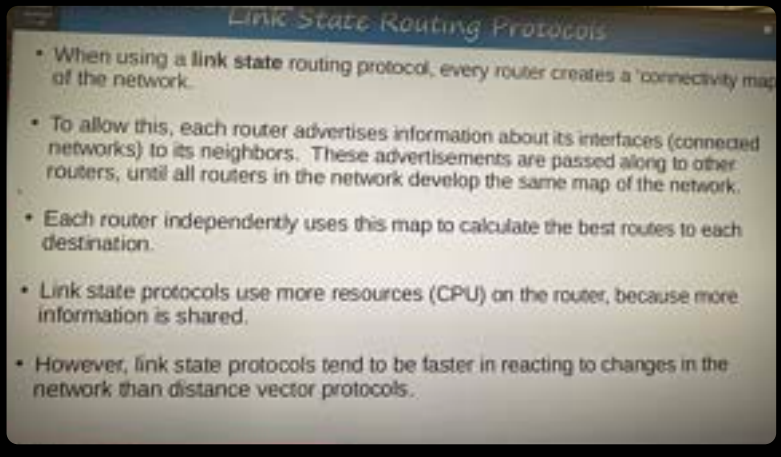
example → BGP



Distance Vector protocol



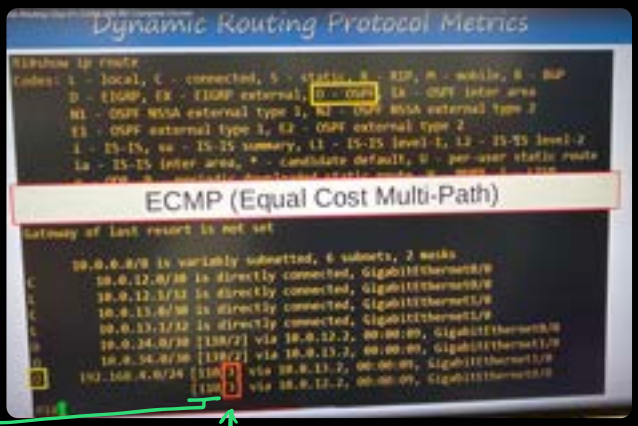
- Link state Routing



- 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.

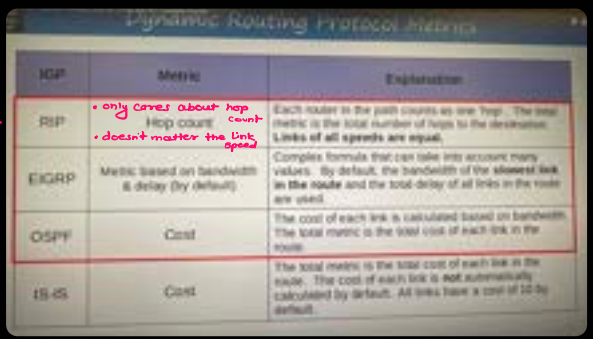
situation — if two routers have the same route cost aka metrics both will be added to the route table and traffic will LB.



Jmp →

AD Administrative distance

route metrics is 3 here

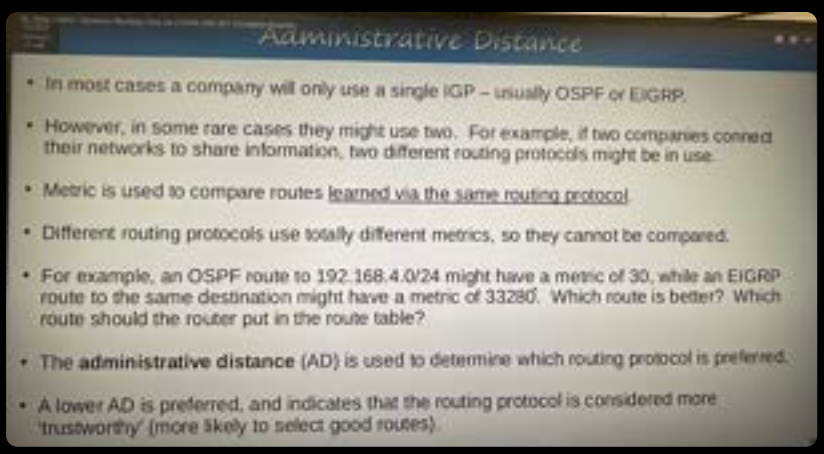


Premetive approach ←

• only cares about hop count

• doesn't master the link speed

Administrative Distance



* * →

# # #

Administrative Distance

Route protocol/type	AD
Directly connected	0
Static	1
External BGP (eBGP)	20
EIGRP	90
IGRP	100
OSPF	110

Route protocol/type	AD
IS-IS	115
RIP	120
EIGRP (external)	170
Internal BGP (iBGP)	200
Unusable route	255

Metrics are used to learn the route over the same protocol

But AD (Administrative distance) is used to find the distance bet^n 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

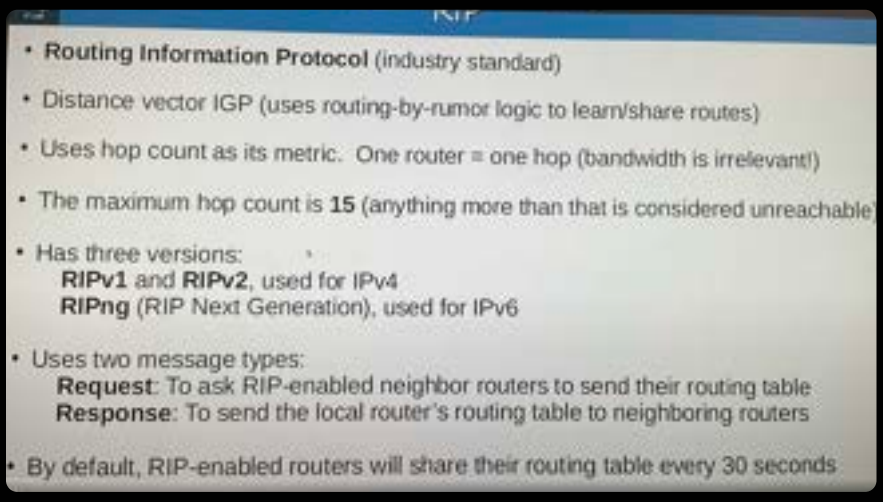
- We can manually change the AD cost for static route to change the selection preferance that is called as floating static route.

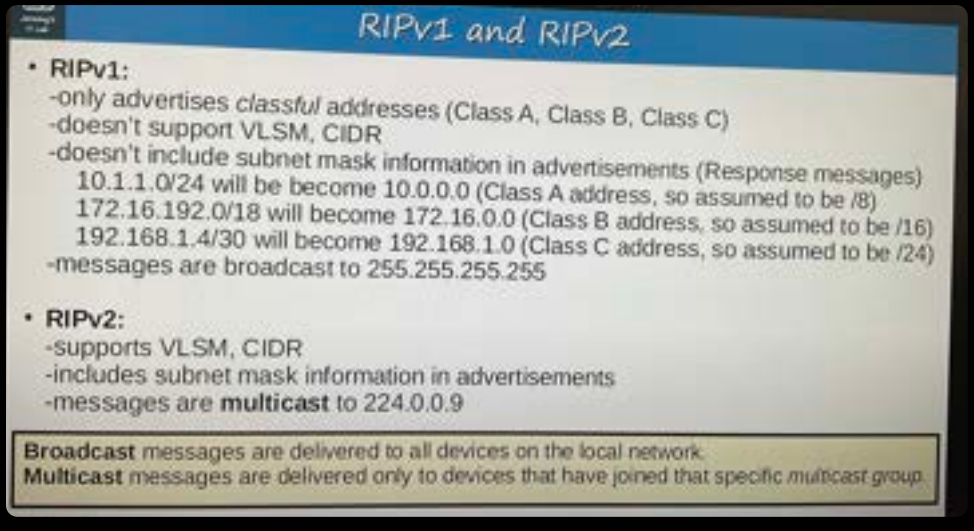
To set it manually →

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

Distance vector

RIP – Routing information Protocol





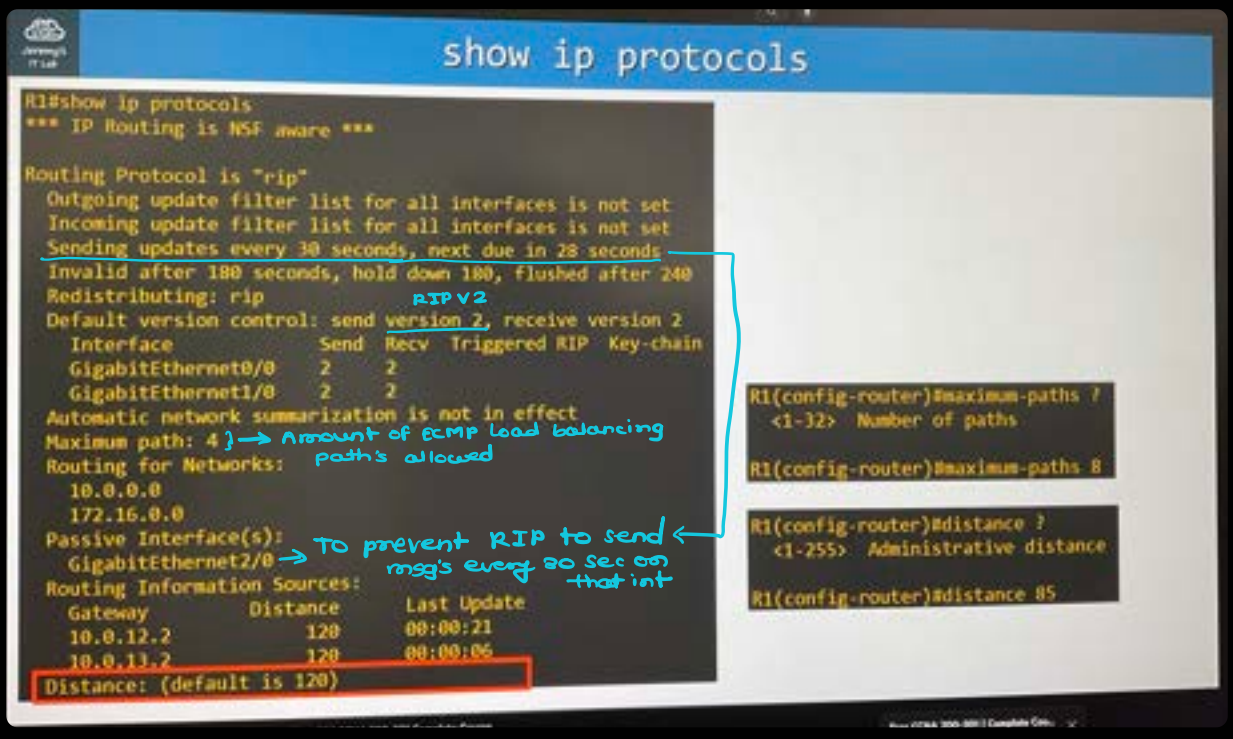
To configure RIP

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

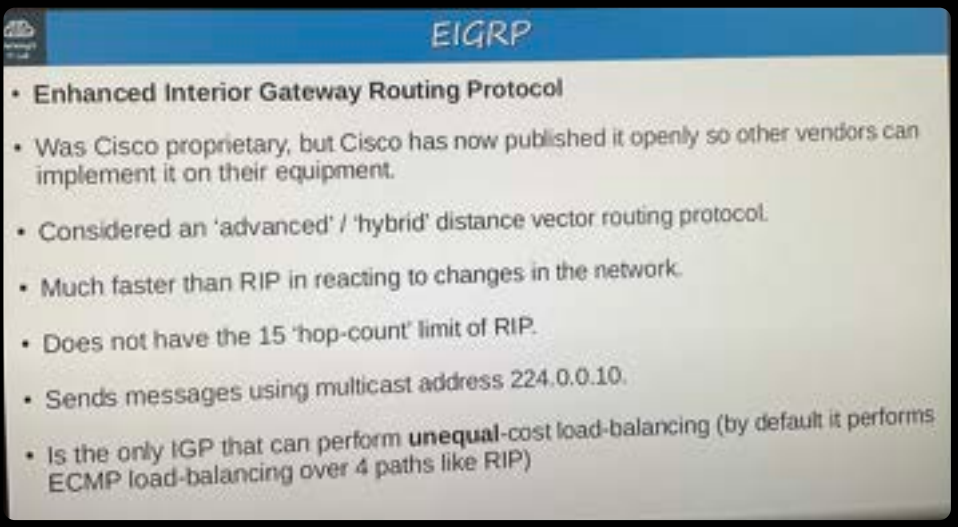
default information originate

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

R1 # show ip protocols



- EIGRP — Enhanced Interior Routing protocol



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