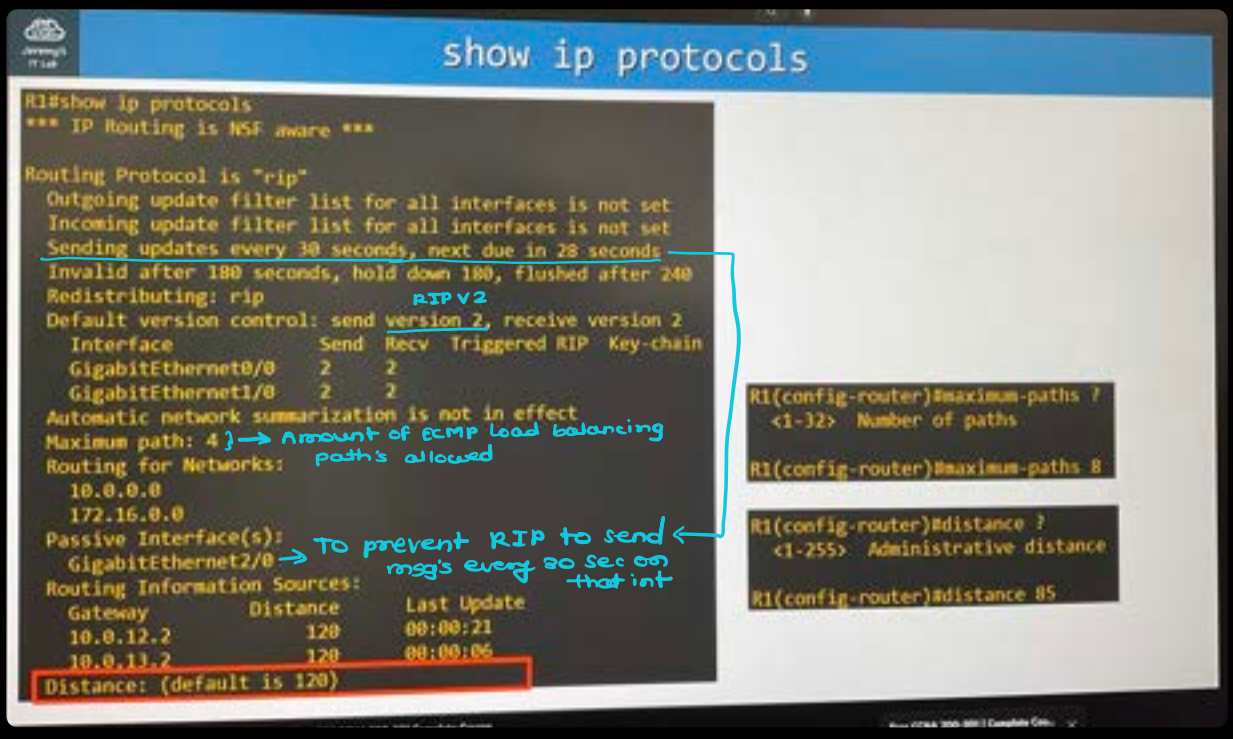
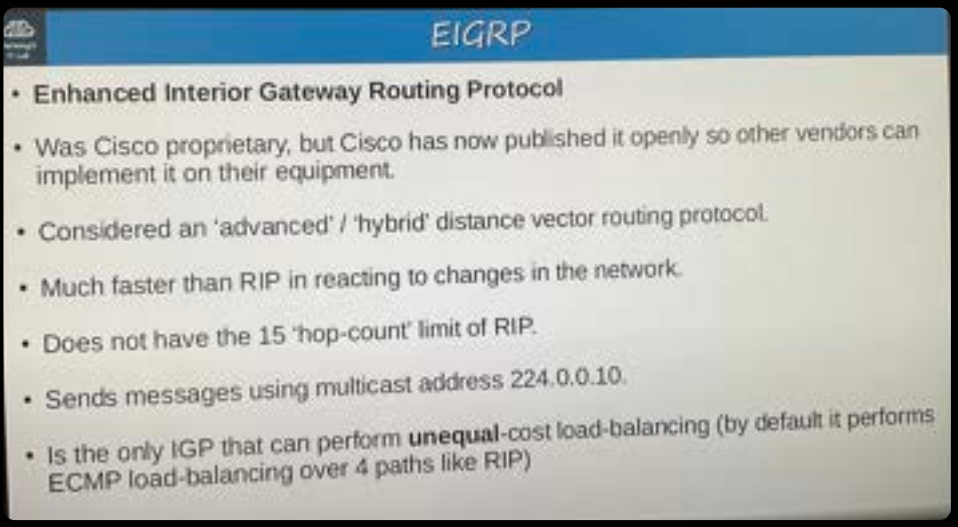
default information originate

- 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.

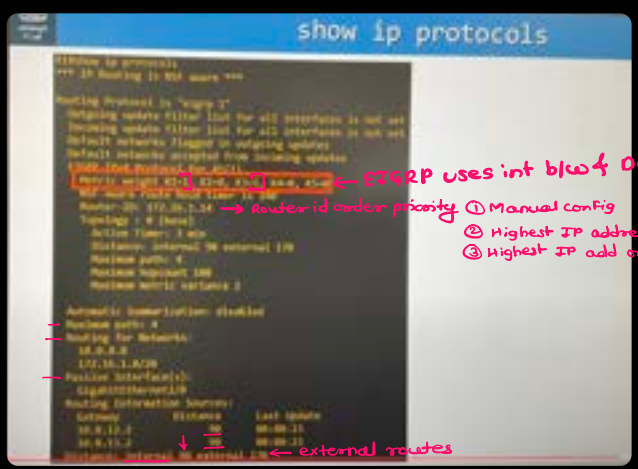
Configuration of EIGRP

R1(config)# router eigrp 1 — As Number & they should match among routers
no auto-summary → used to advertise classful networks
passive-interface g2/0
network 10.0.0.0
network 172.16.1.0.0 0.0.0.15
Wildcard Mask not regular Mask

Wildcard Mask is basically inverted Mask

- So All 1's from regular Mask are 0's in Wildcard Mask

show ip protocols



- EIGRP is shown by D in routing table

R1's G1/0 interface has an IP address of 172.20.20.17 and its G2/0 interface has an IP address of 172.26.20.12. Which of the following **network** commands will activate EIGRP on both interfaces?

a) R1(config-router)# network 128.0.0.0 127.255.255.255 ← Ans

b) R1(config-router)# network 172.16.0.0 0.0.255.255

c) R1(config-router)# network 172.20.0.0 0.0.127.255

d) R1(config-router)# network 172.20.0.0 0.3.255.255

R1 G1/0 IP address:

172	.	20	.	20	.	17
10101100	.	00010100	.	00010100	.	00010001

R1 G2/0 IP address:

172	.	26	.	20	.	12
10101100	.	00011010	.	00010100	.	00001100

EIGRP **network** command:

10000000	.	00000000	.	00000000	.	00000000
128	.	0	.	0	.	0
01111111	.	11111111	.	11111111	.	11111111
127	.	255	.	255	.	255

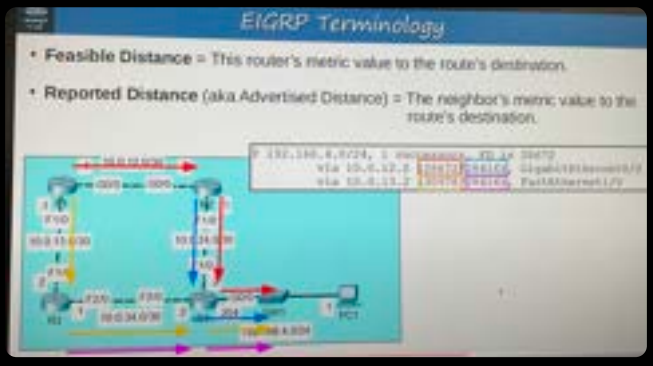
Configuring loopback addresses

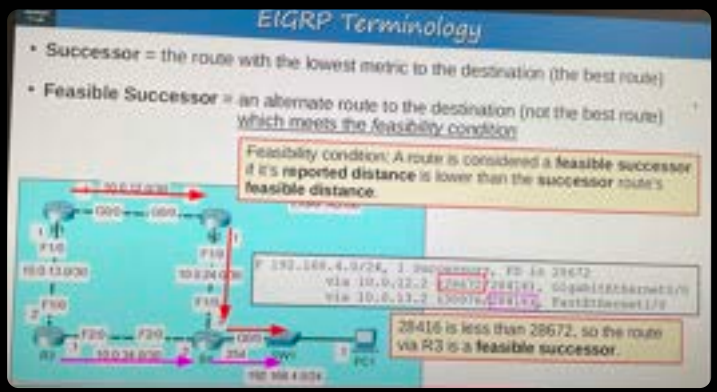
① (config) # interface loopback 1
ip address 1.1.1.1 255.255.255.255

To configure EIGRP

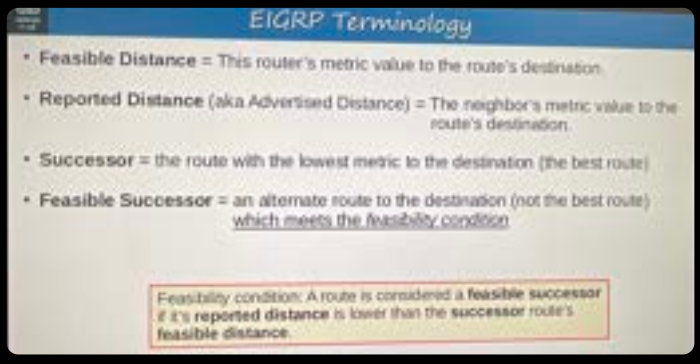
(config) # router eigrp 100
(AS num)

network ip Wildcard subnet
no-auto summary

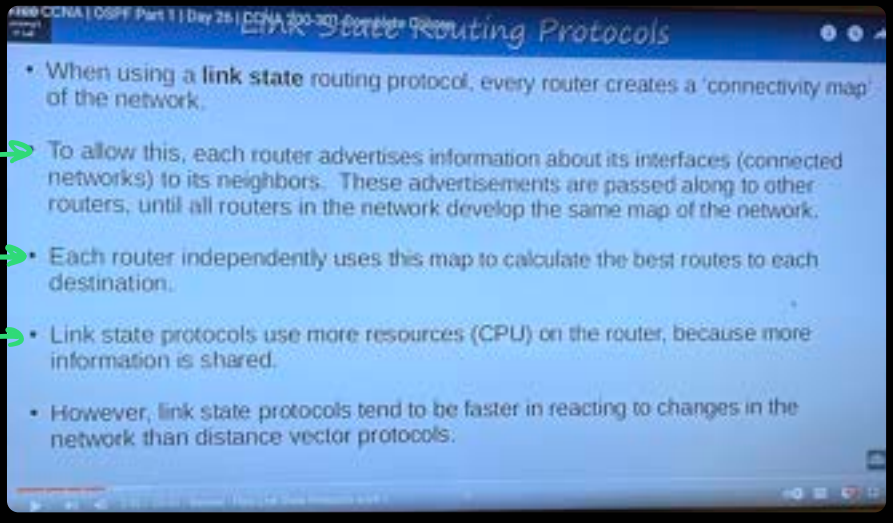




EIGRP can perform unequal cost load balancing



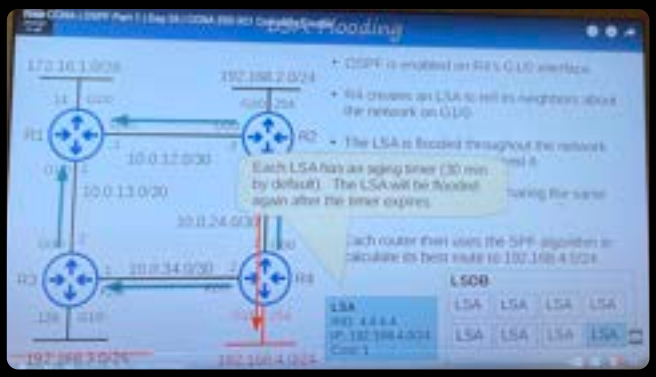
OSPF — Link state routing



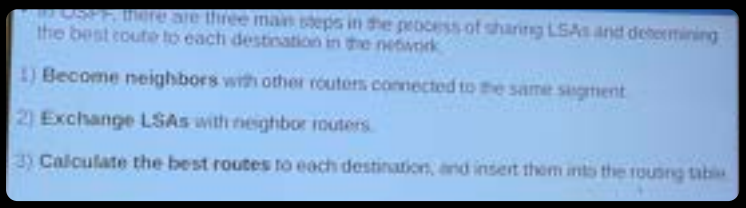
→ OSPF is also known as Dijkstra's Algo.

Three types
① OSPF
② OSPF v2 — IPV4
③ OSPFv3 — IPV6

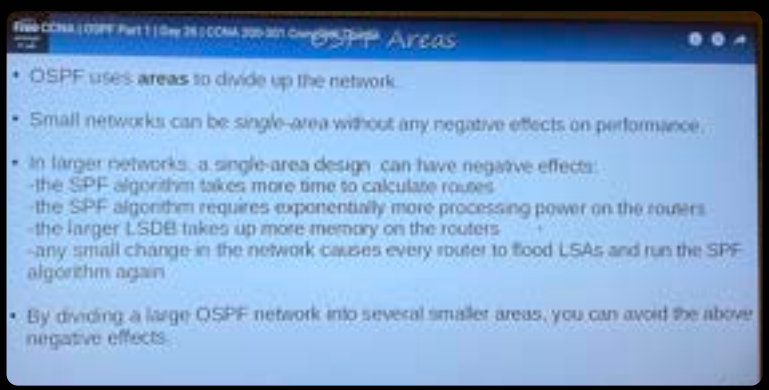
- Routers store information about the network in LSA (Link State Ads) which are organized in structure called LSDB (Link State Database)
- Routers will flood LSA's until all routers in the OSPF are develop the same map of the network.



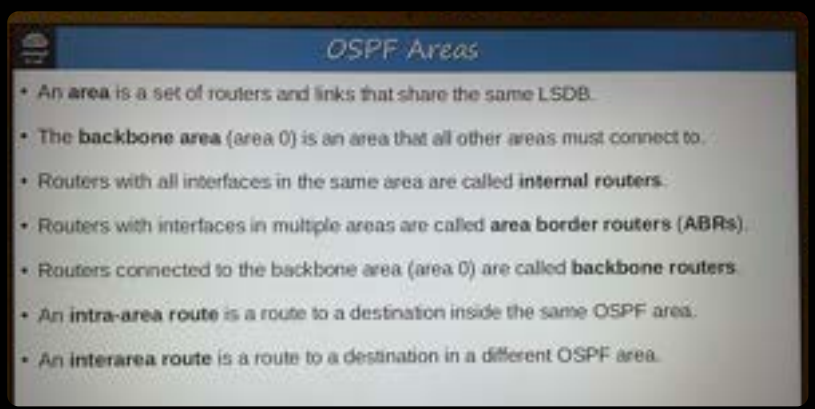
OSPF steps

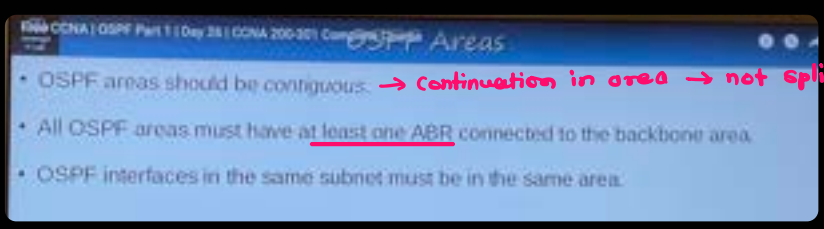


- OSPF uses area to devide bigger network



OSPF areas





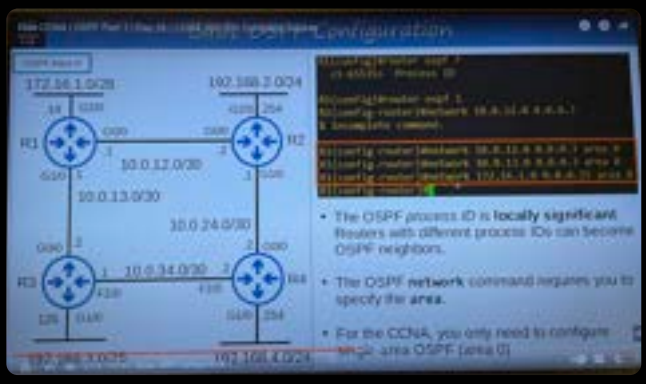
→ continuation in area → not split betⁿ networks

• Configuration of OSPF

R1(config) # router ospf 1

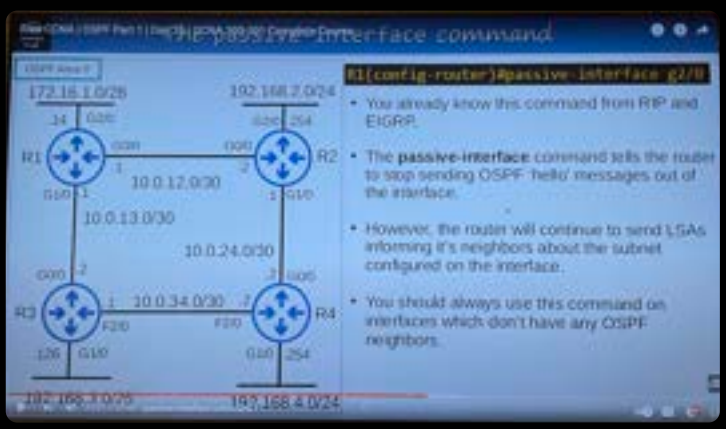
network ip wildcard area 0

Example →



passive-interface g2/0

↳ To set the links in passive mode to prevent sending LSA



To advertice in OSPF

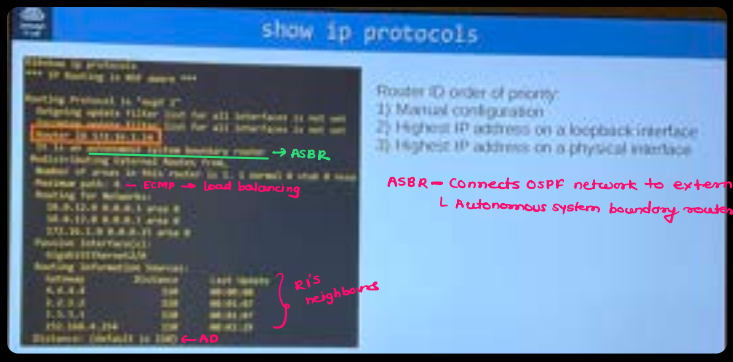
* To configure a default route →

route 0.0.0.0 0.0.0.0 203.0.113.2

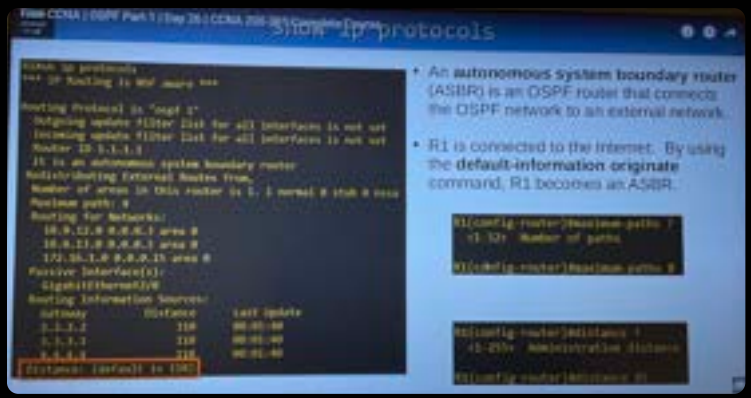
internet IP over cloud

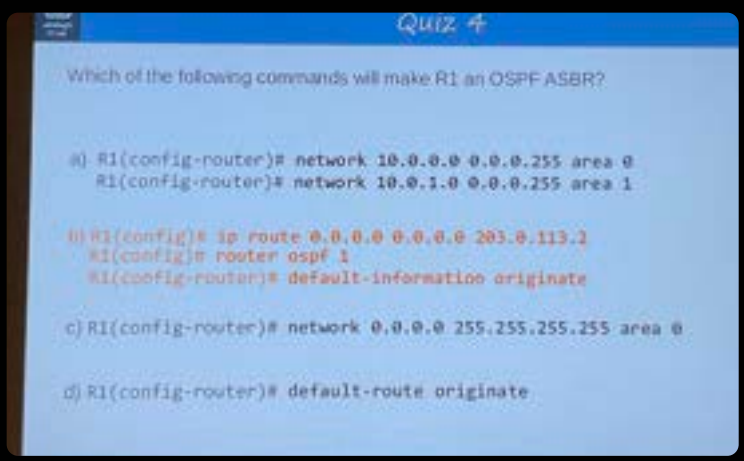
* To advertise the default route in OSPF same as RIP

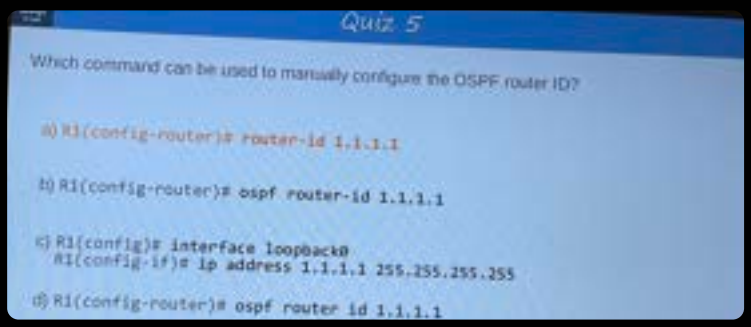
default-information originate



ASBR – Connects OSPF network to external network
└ Autonomous system boundary router





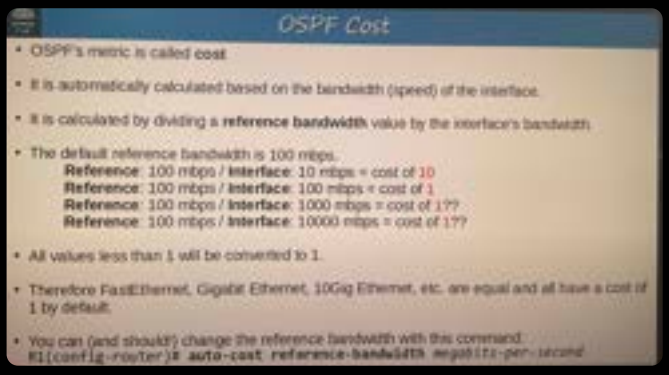


Show ip ospf database
show ip ospf neighbour

—— Day 27- Ospf p2

- Ospf metrics called as cost
- Its automatically calculated based on the bandwidth (speed) of interface.
-

$$\text{ospf cost} = \frac{\text{reference bandwidth value}}{\text{interfaces' bandwidth}}$$



To see the cost of interface

R3 # show ip ospf interface F 2/0

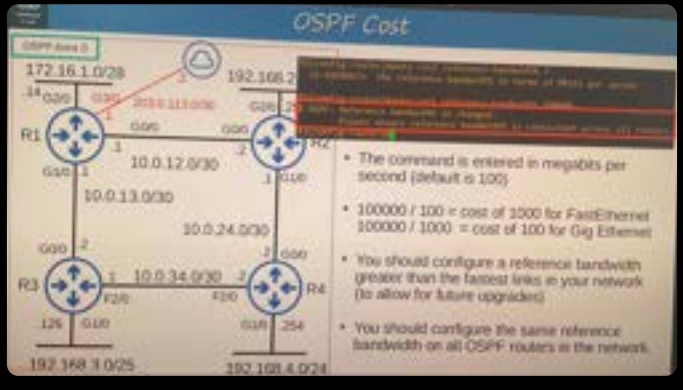
To change the ospf cost

auto-cost reference-bandwidth 100000

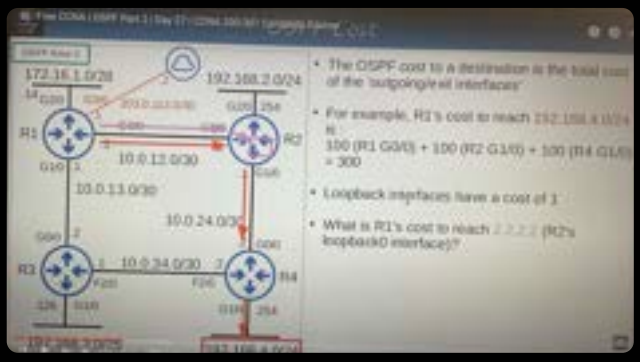
so for fastEthernet

100000/100 = cost of 1000 for FastEthernet

100000/1000 = cost of 100 for Gig Ethernet

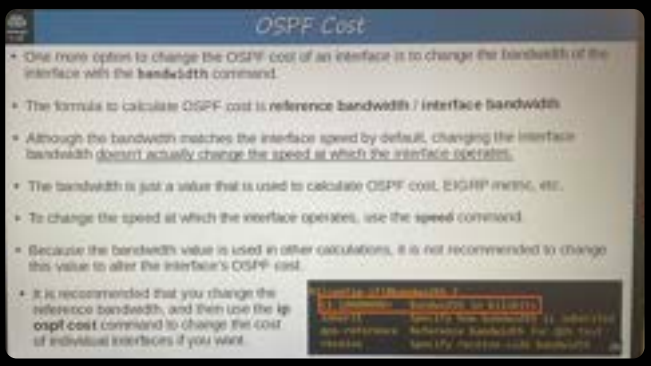


- Reference bandwidth has to be same on all ospf configured routers on net



TO manually configure ospf cost

R1(config-if)# ip ospf cost 2

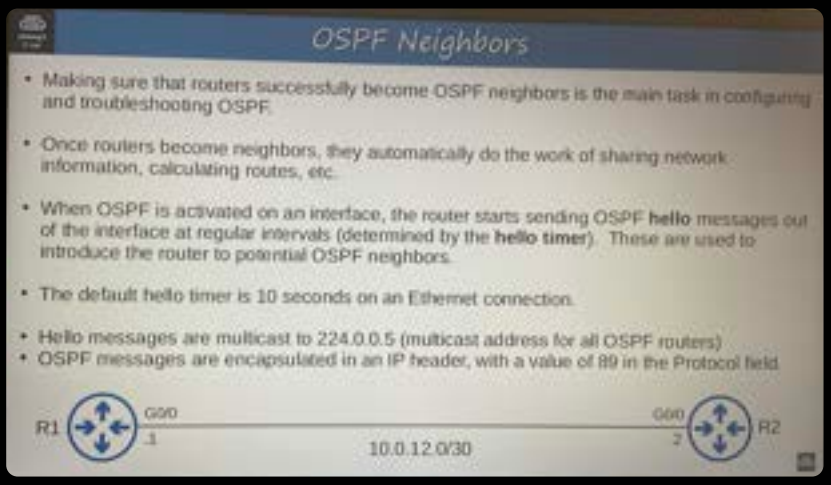


Ospf neighbours

Default hello message timer is 10 seconds on an Ethernet conn^{n}

Hello messages are multicast to 224.0.0.5 Multicast add. of OSPF

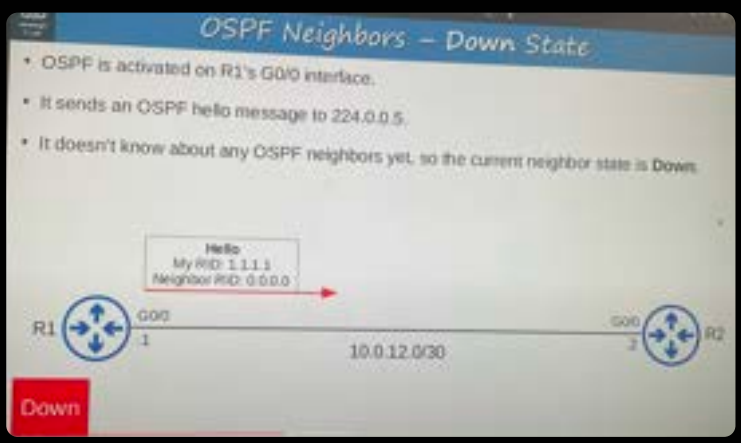
OSPF Multicast – 224.0.0.5
RIP Multicast – 224.0.0.9
EIGRP Multicast – 224.0.0.10



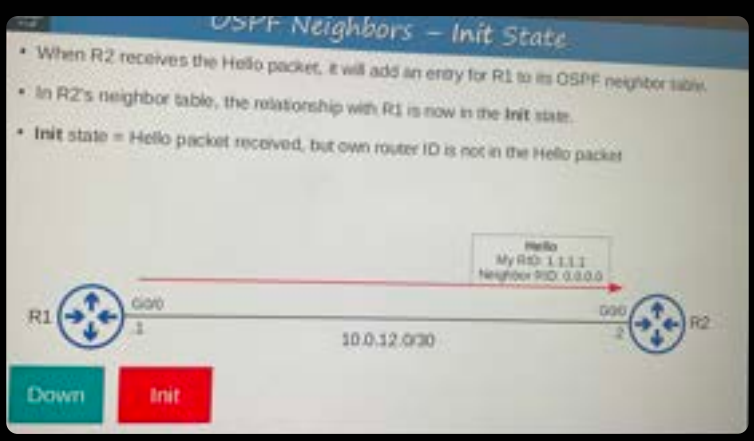
Ospf neighbour steps

Once ospf is activated on one interface

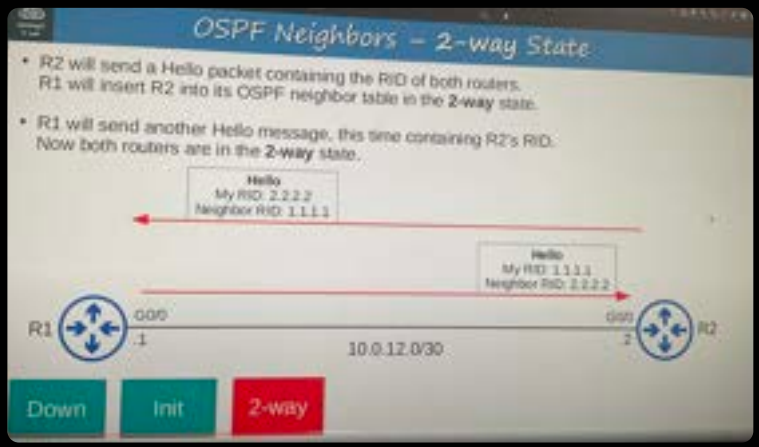
① ospf hello message is sent
current state- down



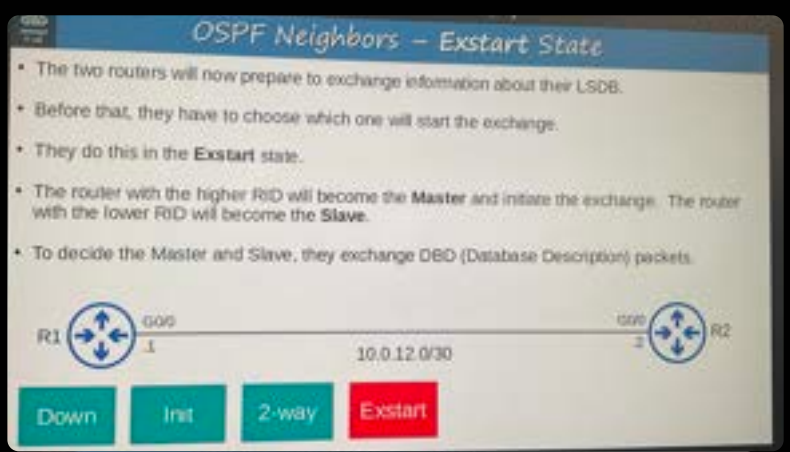
②

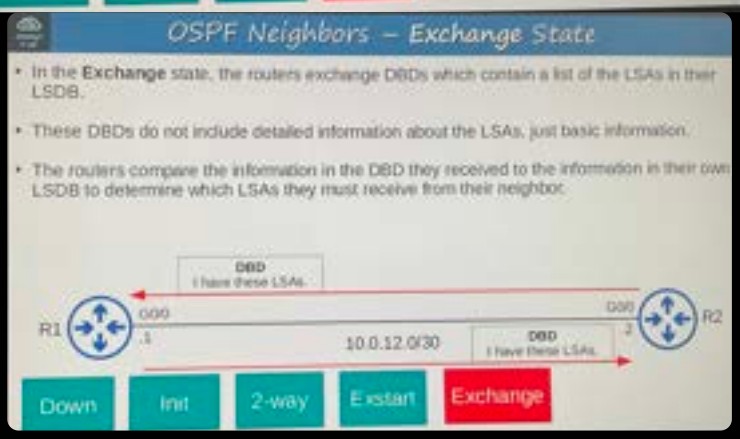


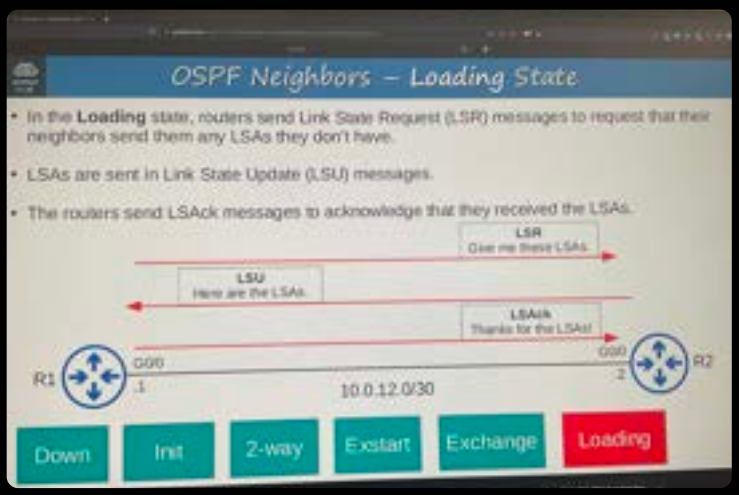
③ 2-way state

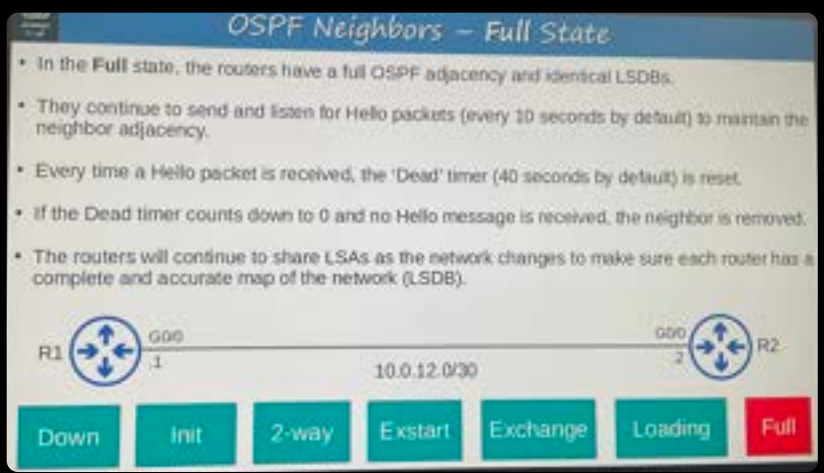

OSPF Neighbors – 2-way State
• R2 will send a Hello packet containing the RID of both routers. R1 will insert R2 into its OSPF neighbor table in the 2-way state.
• R1 will send another Hello message, this time containing R2's RID. Now both routers are in the 2-way state.
Hello
My RID: 2.2.2.2
Neighbor RID: 1.1.1.1
Hello
My RID: 1.1.1.1
Neighbor RID: 2.2.2.2
R1
Gi0/0
.1
10.0.12.0/30
Gi0/0
.2
R2
Down
Init
2-way

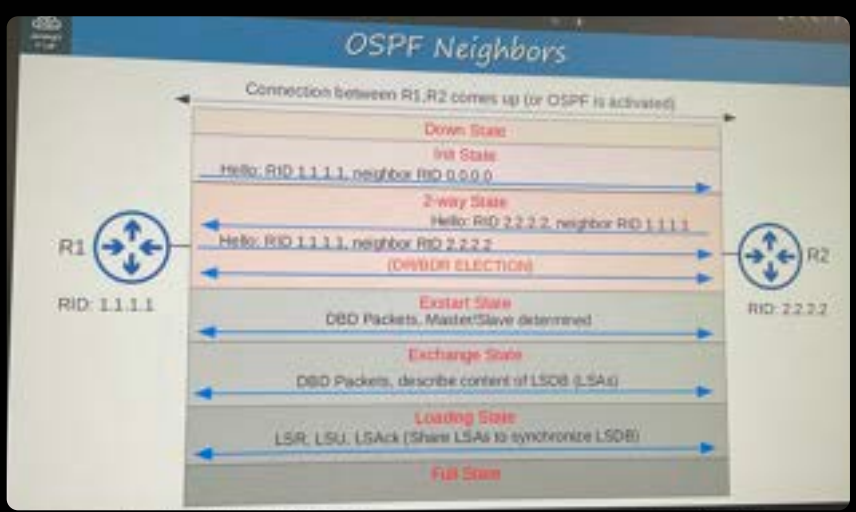

OSPF Neighbors – 2-way State
• The 2-way state means the router has received a Hello packet with its own RID in it.
• If both routers reach the 2-way state, it means that all of the conditions have been met for them to become OSPF neighbors. They are now ready to share LSAs to build a common LSDB.
• In some network types, a DR (Designated Router) and BDR (Backup Designated Router) will be elected at this point.
(I will talk about OSPF network types and DR/BDR elections in Day 28)
R1
Gi0/0
.1
10.0.12.0/30
Gi0/0
.2
R2
Down
Init
2-way


OSPF Neighbors – Exstart State
• The two routers will now prepare to exchange information about their LSDB.
• Before that, they have to choose which one will start the exchange.
• They do this in the Exstart state.
• The router with the higher RID will become the Master and initiate the exchange. The router with the lower RID will become the Slave.
• To decide the Master and Slave, they exchange DBD (Database Description) packets.
R1
Gi0/0
.1
10.0.12.0/30
Gi0/0
.2
R2
Down
Init
2-way
Exstart


OSPF Neighbors – Exchange State
• In the Exchange state, the routers exchange DBDs which contain a list of the LSAs in their LSDB.
• These DBDs do not include detailed information about the LSAs, just basic information.
• The routers compare the information in the DBD they received to the information in their own LSDB to determine which LSAs they must receive from their neighbor.
DBD
I have these LSAs
R1
Gi0/0
.1
10.0.12.0/30
Gi0/0
.2
R2
DBD
I have these LSAs
Down
Init
2-way
Exstart
Exchange

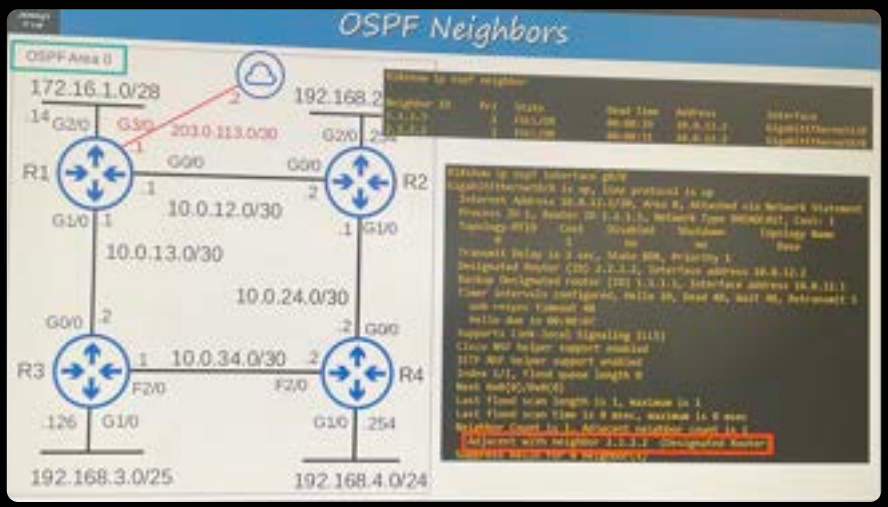

OSPF Neighbors – Loading State
In the Loading state, routers send Link State Request (LSR) messages to request that their neighbors send them any LSAs they don't have.
LSAs are sent in Link State Update (LSU) messages.
The routers send LSAck messages to acknowledge that they received the LSAs.
LSR
Give me these LSAs
LSU
Here are the LSAs
LSAck
Thanks for the LSAs!
R1
G0/0
.1
10.0.12.0/30
G0/0
.2
R2
Down
Init
2-way
Exstart
Exchange
Loading


OSPF Neighbors – Full State
In the Full state, the routers have a full OSPF adjacency and identical LSDBs.
They continue to send and listen for Hello packets (every 10 seconds by default) to maintain the neighbor adjacency.
Every time a Hello packet is received, the 'Dead' timer (40 seconds by default) is reset.
If the Dead timer counts down to 0 and no Hello message is received, the neighbor is removed.
The routers will continue to share LSAs as the network changes to make sure each router has a complete and accurate map of the network (LSDB).
R1
G0/0
.1
10.0.12.0/30
G0/0
.2
R2
Down
Init
2-way
Exstart
Exchange
Loading
Full

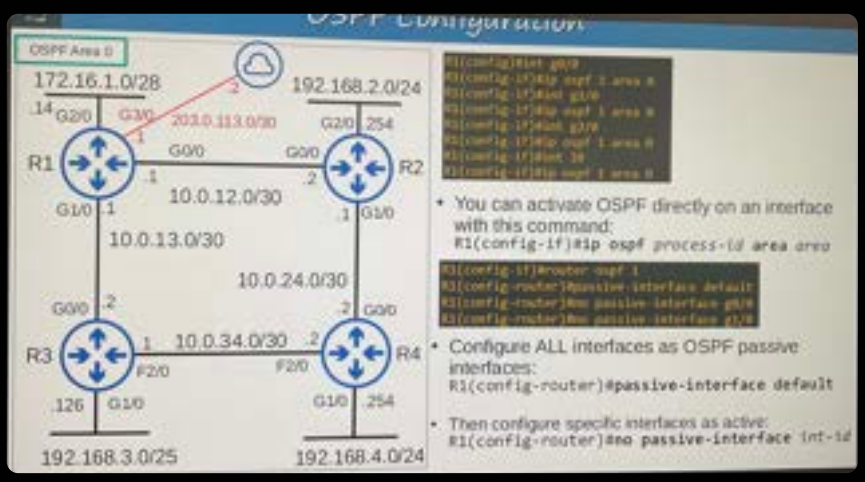

OSPF Neighbors
Connection between R1,R2 comes up (or OSPF is activated)
Down State
Init State
Hello: RID 1.1.1.1, neighbor RID 0.0.0.0
2-way State
Hello: RID 2.2.2.2, neighbor RID 1.1.1.1
Hello: RID 1.1.1.1, neighbor RID 2.2.2.2
(DR/BDR ELECTION)
R1
RID: 1.1.1.1
R2
RID: 2.2.2.2
Exstart State
DBD Packets, Master/Slave determined
Exchange State
DBD Packets, describe content of LSDB (LSAs)
Loading State
LSR, LSU, LSAck (Share LSAs to synchronize LSDB)
Full State

OSPF

Type	Name	Purpose
1	**Hello**	Neighbor discovery and maintenance.
2	**Database Description (DBD)**	Summary of the LSDB of the router. Used to check if the LSDB of each router is the same.
3	**Link-State Request (LSR)**	Requests specific LSAs from the neighbor.
4	**Link-State Update (LSU)**	Sends specific LSAs to the neighbor.
5	**Link-State Acknowledgement (LSAck)**	Used to acknowledge that the router received a message.

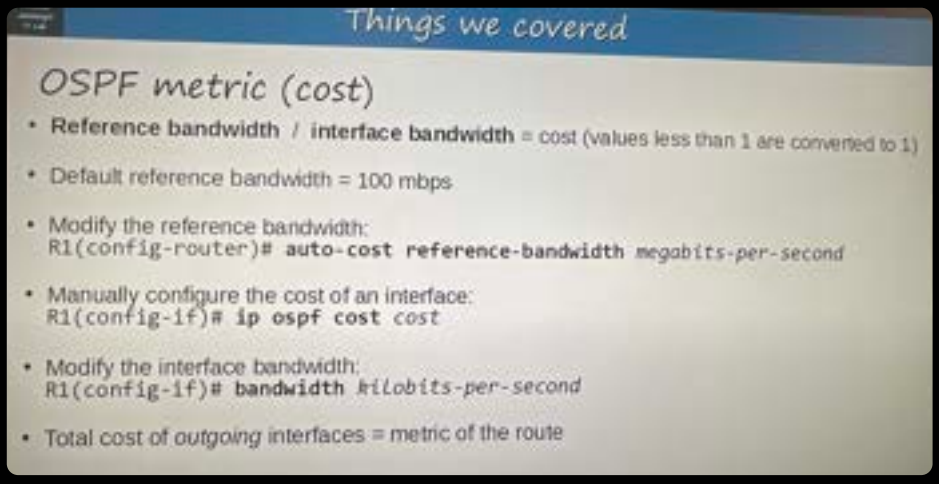


Another method to configure OSPF.

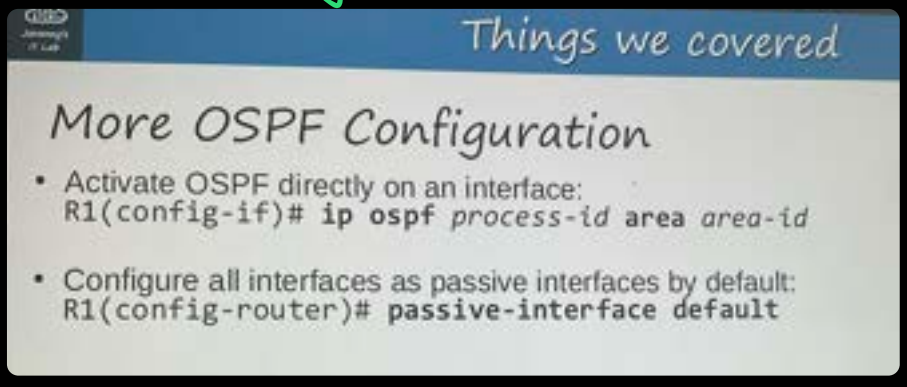


Every Awesome cisco engineer will need

ice.coe — Daily



— Alternative way:



ospf neighbour states

① Down	D	Darling
② init	I	I
③ 2-way	T	Taste
④ Exstart	E2	some
⑤ Exchange	L	extremely
⑥ Loading	f	large
⑦ Full		fries

- Default Hello/Dead timers on ospf are

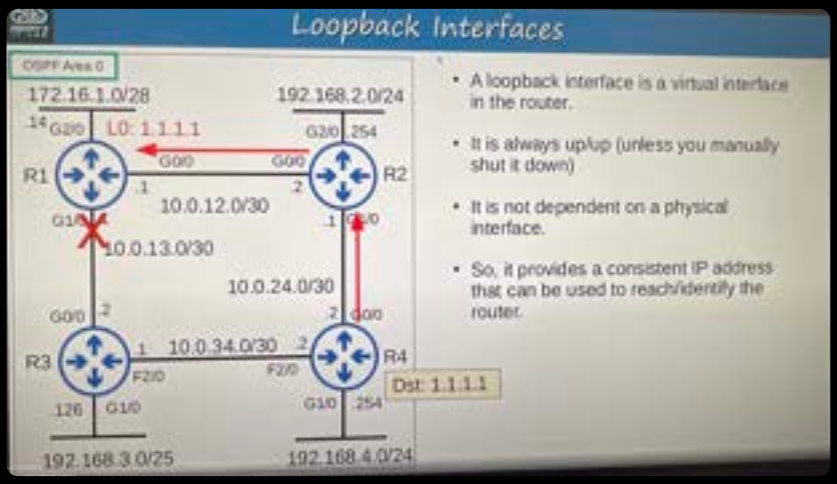
  - Hello — 10 sec
  - Dead timer — 40 sec
  - wait timer — 40 sec

* show ospf neighbours

** All routers should have same reference b/w configured on all routers under that area.

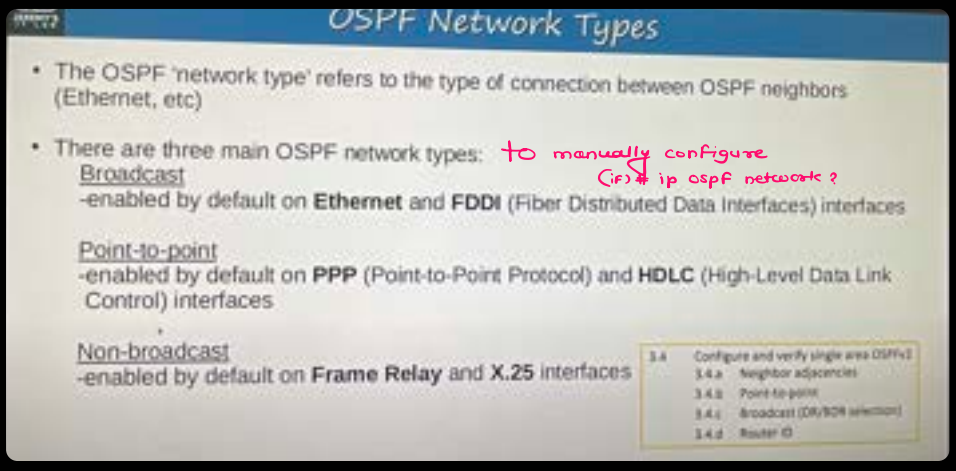
show ip protocols → To see currently running protocols

Day 28 – ospf p3



Ospf network types

Ospf network types are designed to give the best routing results in different topologies.

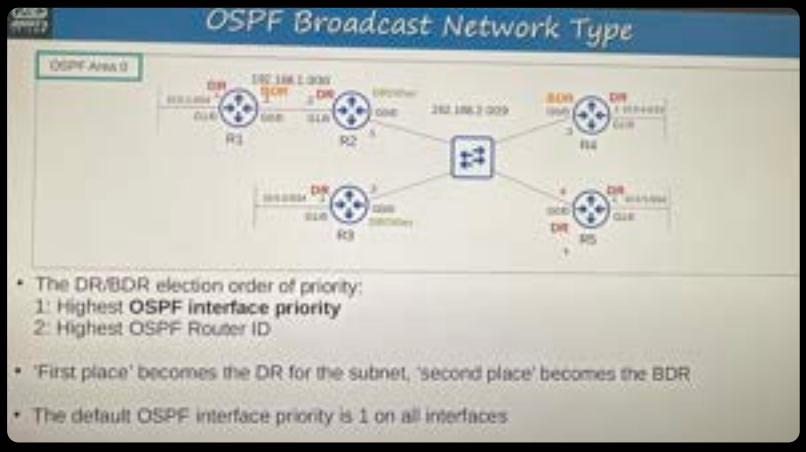


- Election of DR | BDR

① Highest OSPF interface priority
② Highest OSPF Router ID

To change ospf priority
R2(config-if)# ip ospf priority ?
range (0-255)

① Broadcast network type



if you set the OSPF interface priority to 0, the router cannot be the DR/BDR for the subnet.

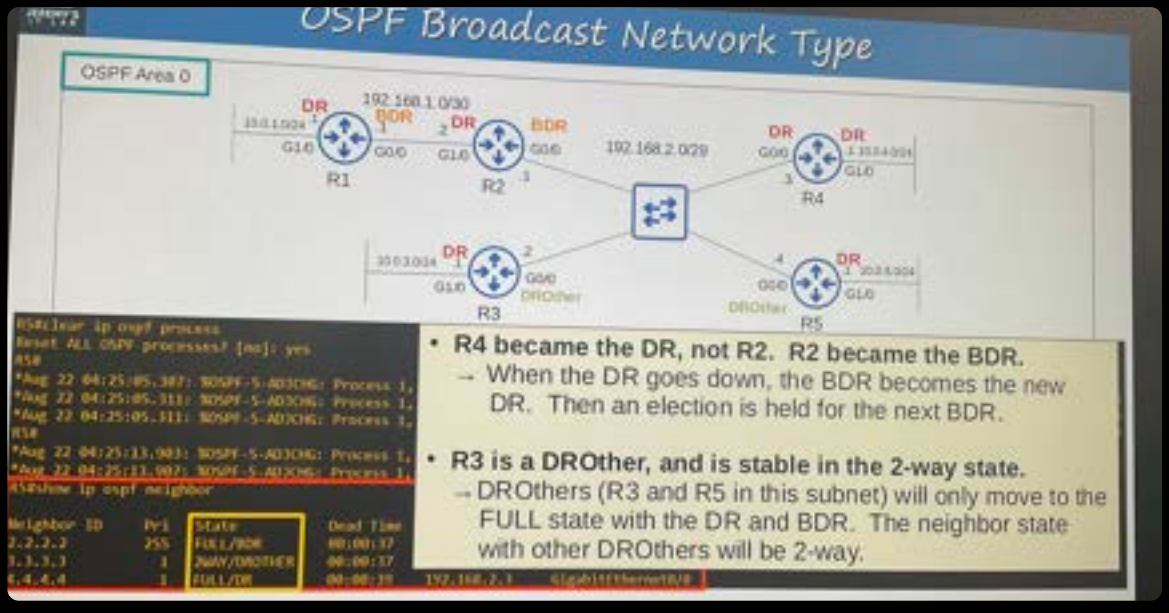
Ospf election for DR/BDR are non-preemptive. Once the DR/BDR are selected they will keep their role until OSPF is reset, the int fails/shut etc.

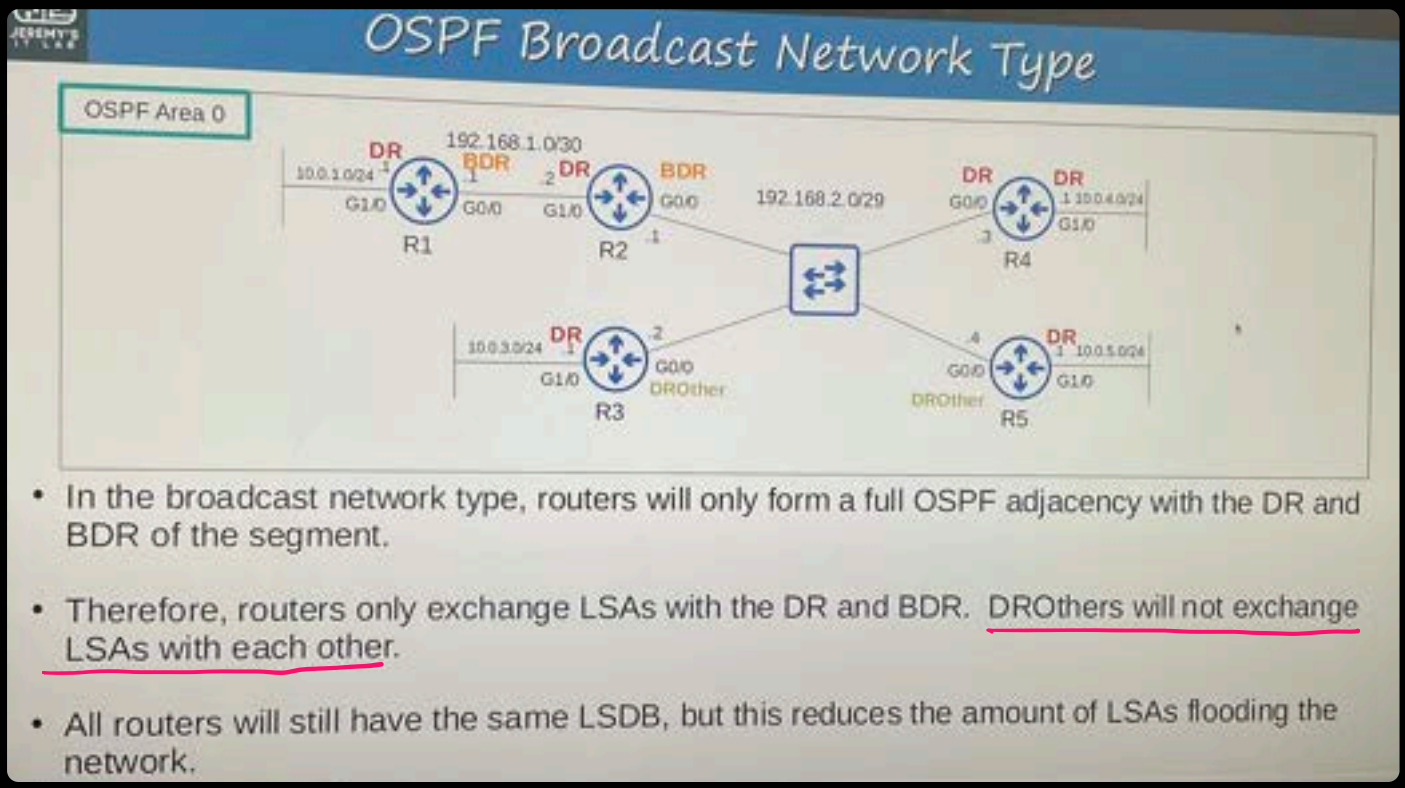
for DR/BDR election

① Even if we change the priority for interface manually still then ospf is non-preemptive so it needs to be resetted/shutdown or fail

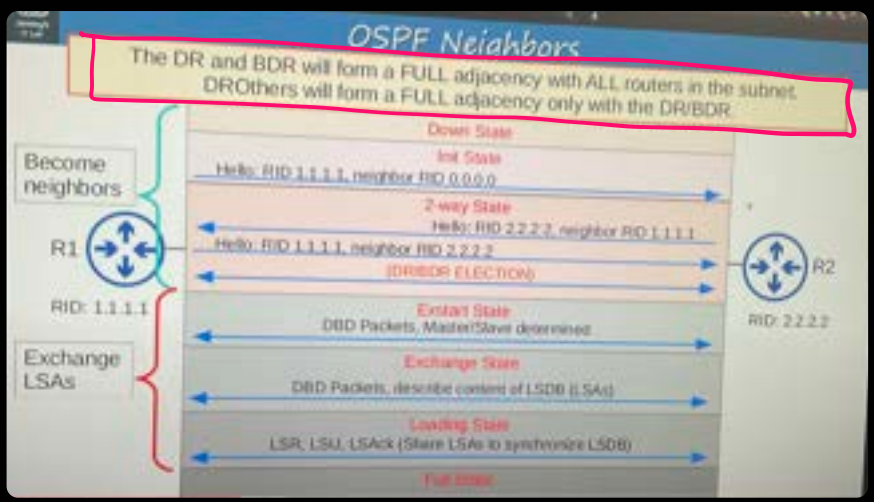
② once reset still the BDR will become the new DR and election will be held for the BDR position.

③ DROthers will only move to the full state with the DR and BDR The neighbour state with other DROther will be 2-way

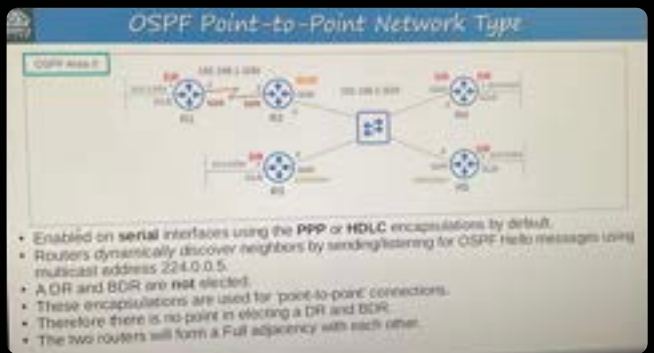


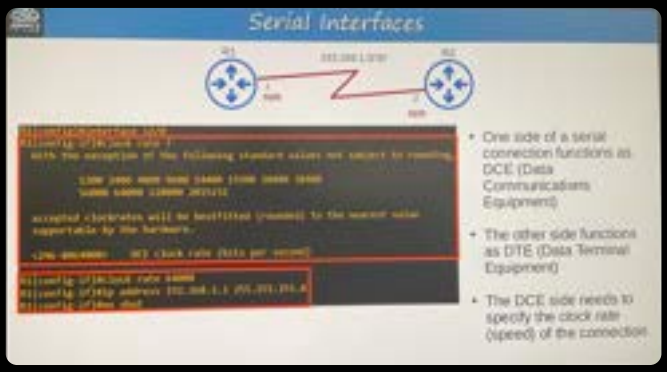


Messages to the DR/BDR are multicast using 224.0.0.6



② Point-to-point Connection.





Ethernet uses speed command to config speed

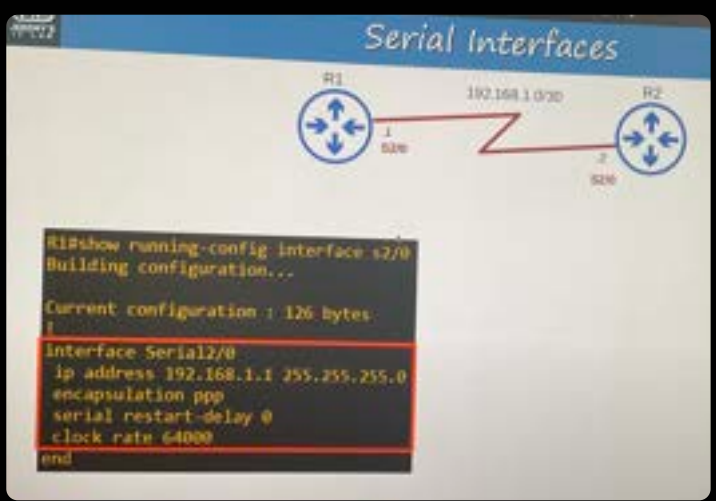
- serial is old & we have to set DCE & DTE on both routers
- Serial Headers doesn't have mac addresses

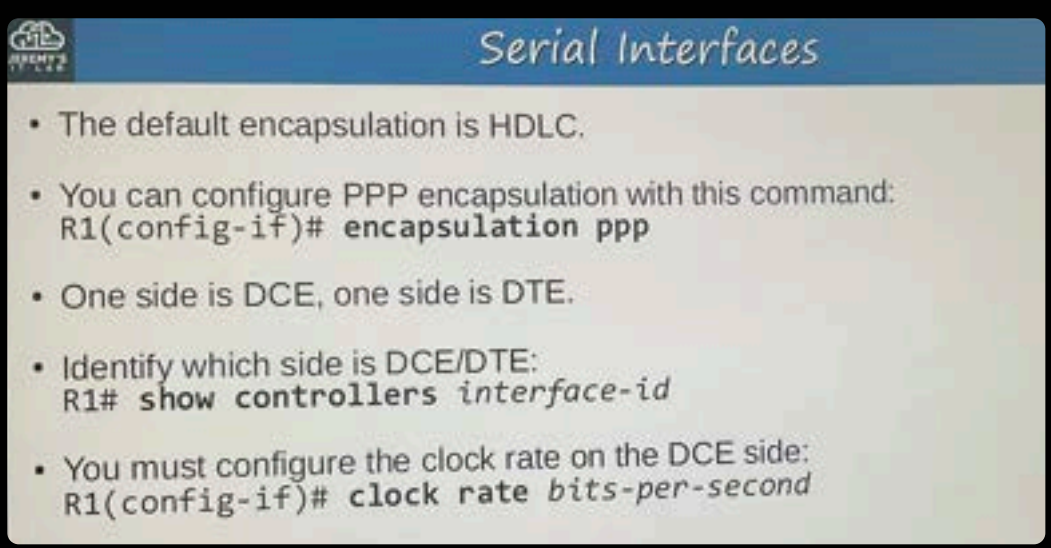
There are two encapsulations on the routers

① HDLC → default

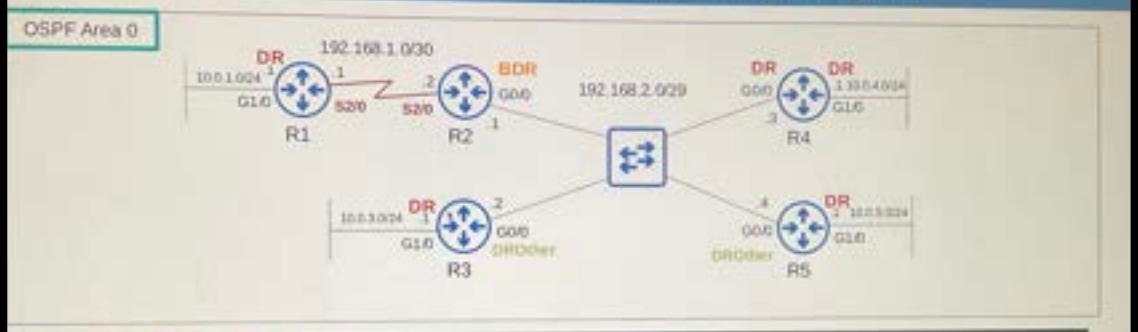
② ppp - point-to-point

Both routers should have same encapsulation





OSPF Point-to-Point Network Type



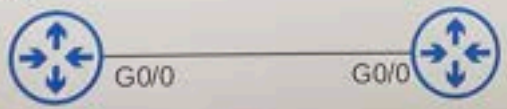

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:31    192.168.1.1     Serial2/0
3.3.3.3           1   2WAY/DROTHER    00:00:39    192.168.2.2     GigabitEthernet0/0
4.4.4.4           1   FULL/DR         00:00:38    192.168.2.3     GigabitEthernet0/0
5.5.5.5           1   FULL/BDR        00:00:31    192.168.2.4     GigabitEthernet0/0
```

↳ Here routers are connected via serial ppp that's why its —

Configure the OSPF Network Type

```
R1(config-if)#ip ospf network ?
  broadcast              Specify OSPF broadcast multi-access network
  non-broadcast          Specify OSPF NBMA network
  point-to-multipoint    Specify OSPF point-to-multipoint network
  point-to-point         Specify OSPF point-to-point network
```

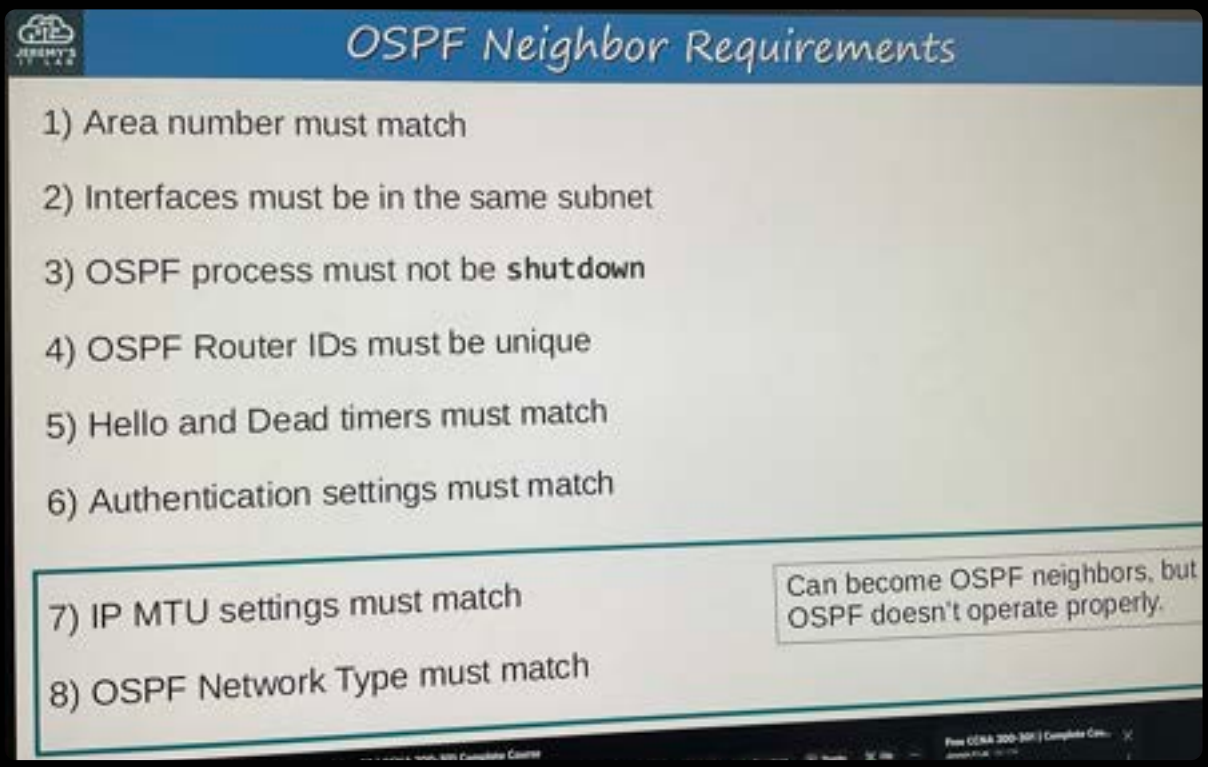
- You can configure the OSPF network type on an interface with `ip ospf network type`
- For example, if two routers are directly connected with an Ethernet link, there is no need for a DR/BDR. You can configure the point-to-point network type in this case.
- NOTE: Not all network types work on all link types (for example, a serial link cannot use the broadcast network type)



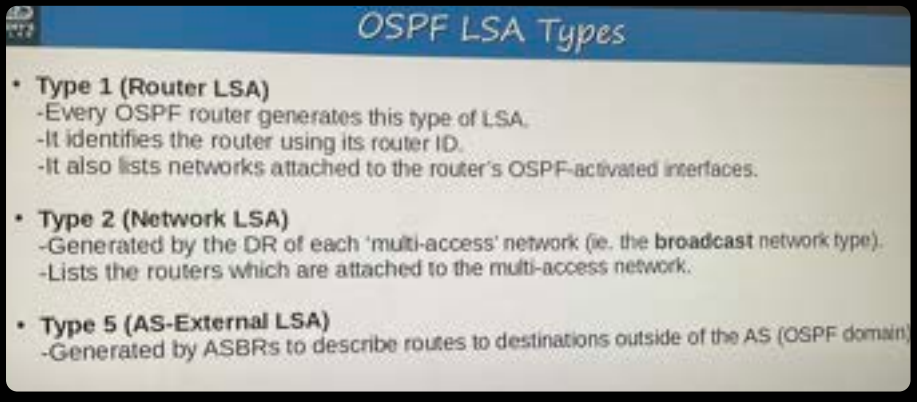
Configure the OSPF Network Type

Broadcast	Point-to-point
Default on **Ethernet**, **FDDI** interfaces	Default on **HDLC**, **PPP** (serial) interfaces
DR/DBR elected	No DR/BDR
Neighbors dynamically discovered	Neighbors dynamically discovered
Default timers: Hello 10, Dead 40	Default timers: Hello 10, Dead 40

(**Non-broadcast** network type default timers = Hello 30, Dead 120)



Ospf lsa types



show ip ospf database

— Day 29 — First Hop Redundancy Protocols

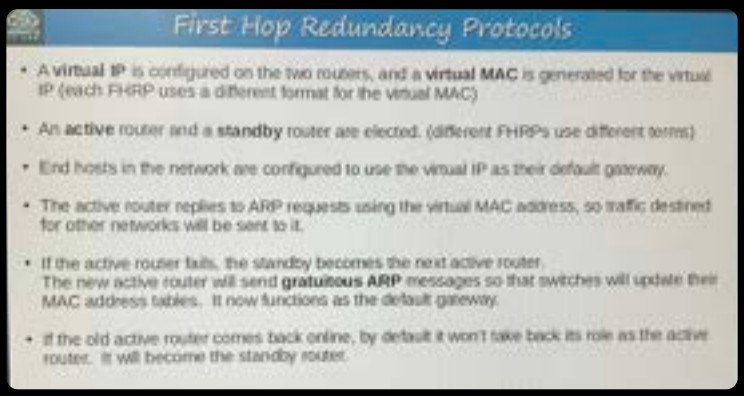
The purpose of FHRP's

— ① HSRP — (Hot standby Router protocol)
② VRRP — (virtual Router Redundancy Protocol)
③ GLBP — (Gateway load balancing protocol)

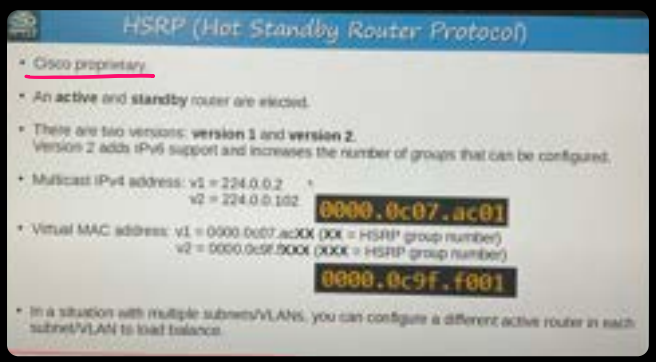
FHRP is designed to protect the default gateway used on a subnetwork by allowing two or more routers to provide backup for that address; in the event of failure of an active router, the backup router will take over the address, usually within a few seconds

How HSRP do it?

HSRP creates a VIP (virtual IP)
VMAC (Virtual MAC)



HSRP — (Hot standby Router protocol)



② Virtual router redundancy protocol (VRRP)
– open standard

VRRP (Virtual Router Redundancy Protocol)

- Open standard
- A **master** and **backup** router are elected.
- Multicast IPv4 address: 224.0.0.18
- Virtual MAC address: 0000.5e00.01**XX** (**XX** = VRRP group number)

0000.5e00.01c8 (0xc8 = 200)

- In a situation with multiple subnets/VLANs, you can configure a different master router in each subnet/VLAN to load balance.

③ GLBP –
Cisco proprietary

GLBP (Gateway Load Balancing Protocol)

- Cisco proprietary
- Load balances among multiple routers within a single subnet
- An **AVG (Active Virtual Gateway)** is elected.
- Up to four **AVFs (Active Virtual Forwarders)** are assigned by the AVG (the AVG itself can be an AVF, too)
- Each AVF acts as the default gateway for a portion of the hosts in the subnet.
- Multicast IPv4 address: 224.0.0.102
- Virtual MAC address: 0007.b400.**XXYY** (**XX** = GLBP group number, **YY** = AVF number)

0007.b400.0101

Comparing FHRPs

FHRP	Terminology	Multicast IP	Virtual MAC	Cisco proprietary?
HSRP	Active/Standby	v1: 224.0.0.2 v2: 224.0.0.102	v1: 0000.0c07.acXX v2: 0000.0c9f.fXXX	Yes
VRRP	Master/Backup	224.0.0.18	0000.5e00.01XX	No
GLBP	AVG / AVF	224.0.0.102	0007.b400.XXYY	Yes

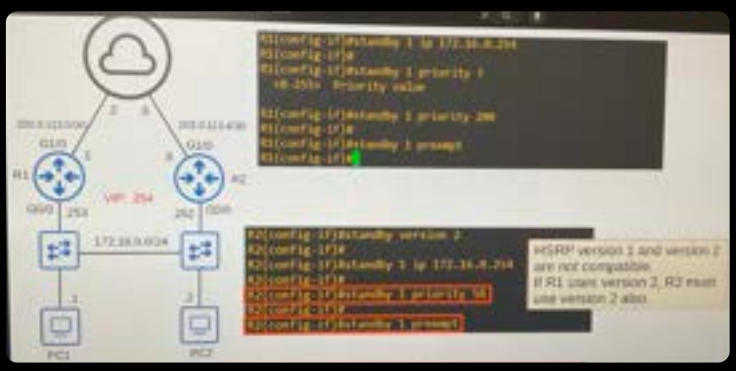
Configuring HSRP if both routers have the same ip then router with the highest ip will be selected.

① interface g 0/0
 # standby
  if range (0-255) then that V1

To change to V2
 R1 (config-if) # standby version 2
  range will be (0-4095)

group numbers should match with routers

standby 1 preempt cmd will overtake the Active router status if this router has
① highest priority if same then highest IP

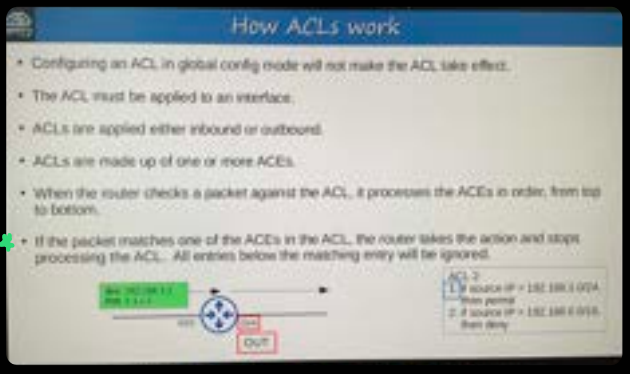


R2 # show standby

Day 30 - 33 skipped for now

Day 34 - ACL

- ACL's are configured in global config mode but they must be applied in interface



* A maximum of one ACL can be applied to a single interface per direction.

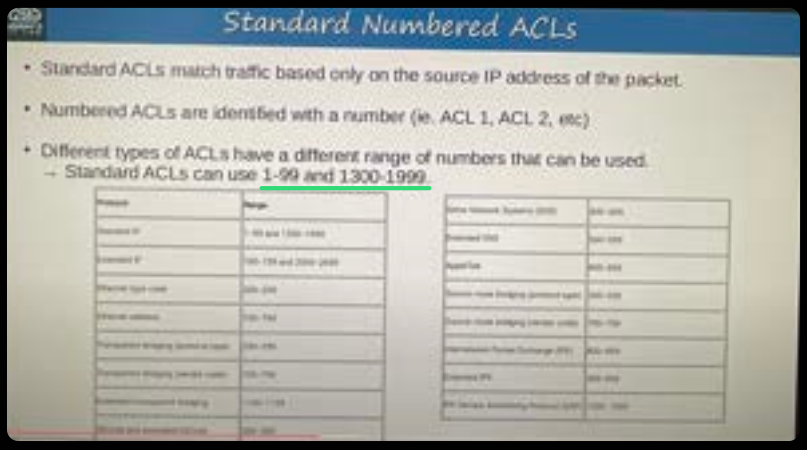
inbound : Maximum one ACL
Outbound : Maximum one ACL

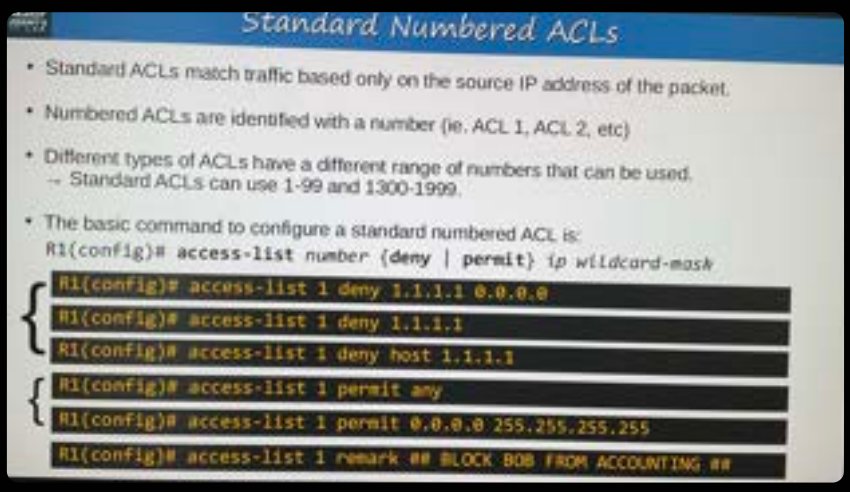
→ implicit deny
ACL have a implicit deny policy like AWS → that means the Ip doesn't match any of the records it will be denied.

— ACL Types
— ① standard ACL
↳ ① standard numbered ACL
② standard named ACL

② Exteded ACL : Match based on Source/Destination Ip, source/Destination port etc.
— ① Extended Numbered ACL's
② Extended Named ACL's

① standard Numbered ACL





(config) # do show access-lists

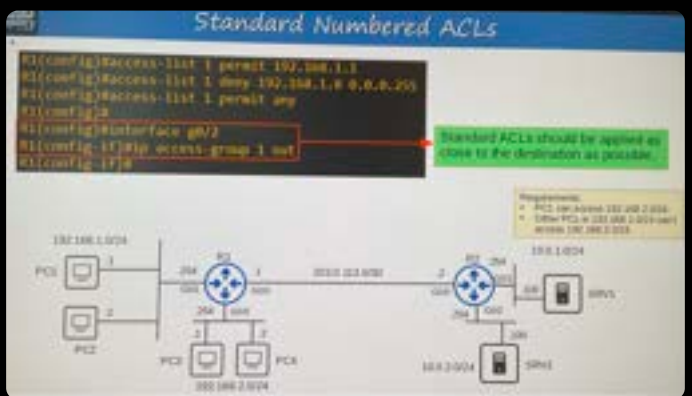
ACL works based on the order so it is important to focus on entries

Once we create the ACL we have to apply this to interface

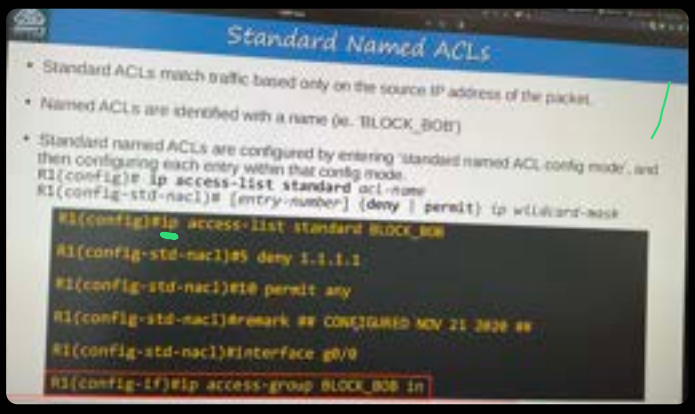
** To do that →

*** R1(config-if) # ip access-group number {in | out}

ex. -if) # ip access-group 1 out



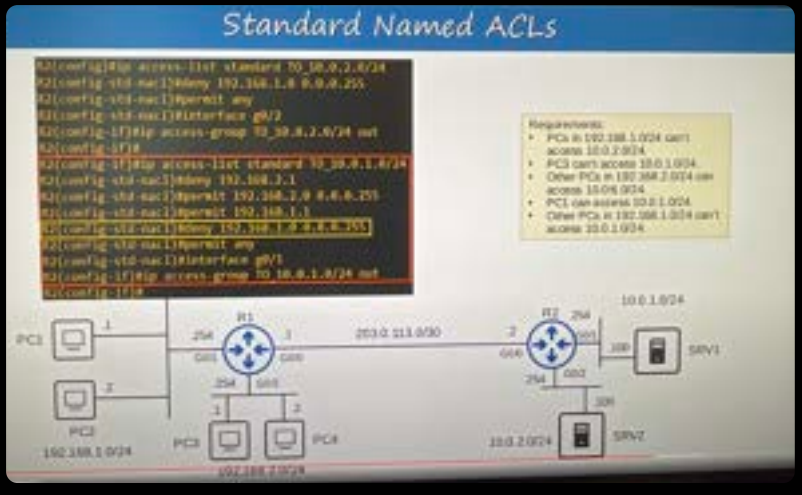
① standard Named ACL



show running-config | section access-list

① ip access-list standard Block-Bob
deny 192.168.1.0 0.0.0.255
✓ permin any
int g0/2
ip access-group Block-bob out

Ans



Standard named
ip access-list standard TO-10.0.2.0/24
deny 192.168.1.0
permit any

② # ip access-list standard TO_10.0.1.0/24
deny 192.168.2.1
permit 192.168.2.0 0.0.0.255
permit 192.168.1.1
deny 192.168.1.0 0.0.0.255
permit any

int g 0/1
ip access-group TO_10.0.1.0/24 out

ACL's are processed from the first entry in the list to the last entry

- Standard ACL's are placed as close to the destination as possible
- Extended close to the source

→ ACL are performed from Top to bottom

Access-list 1 permit 172.16.1.1
Access-list 1 permit 172.16.2.1
access-list deny any

int g 0/0
Access-group 1 out

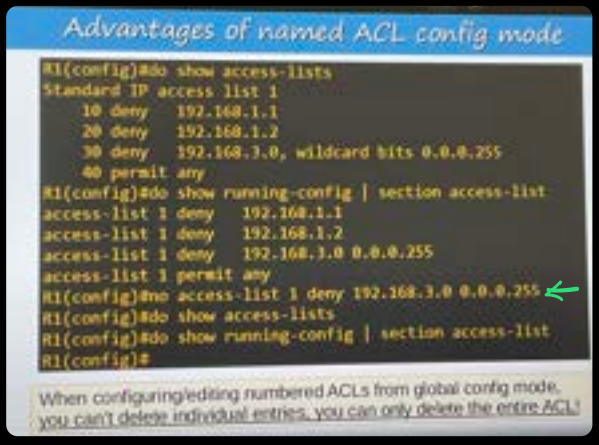
access-list 2 deny 172.16.2.0 0.0.0.255
int g0/1
access-group 2 out

Extended ACL — Day 35

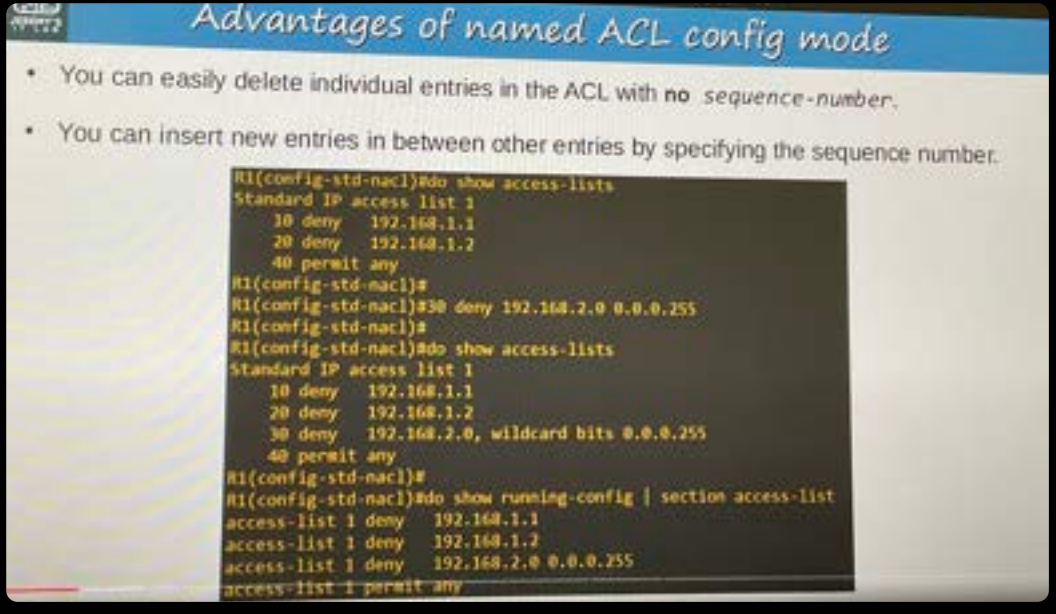
for standard ACL We can set the ACL's named & numbered with same cmnd

ip access-list standard ?
named
number — 1-99 1300-1999

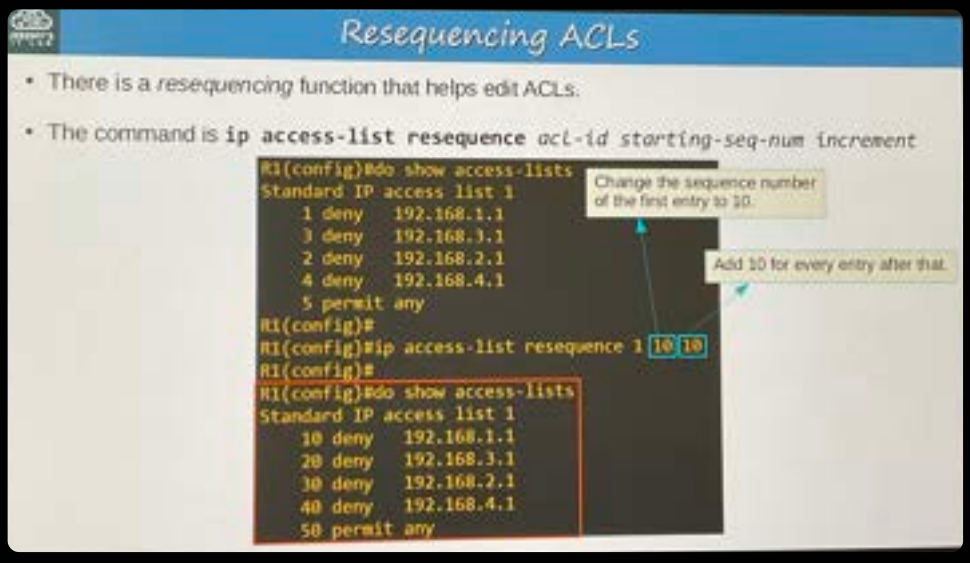
To edit the entry



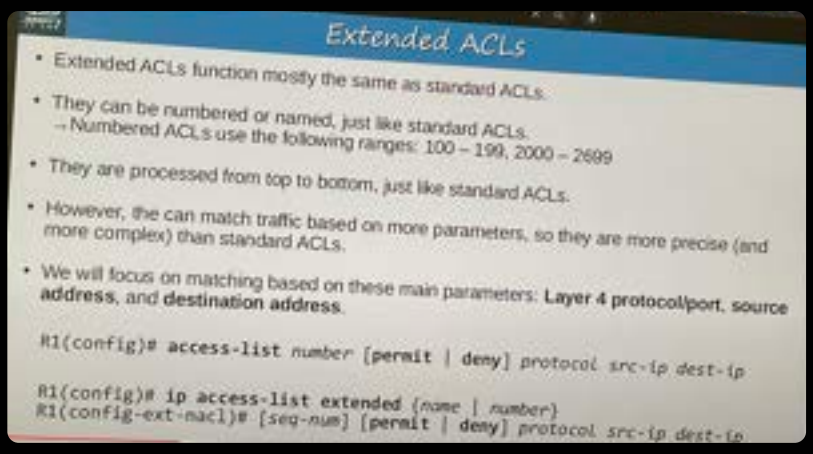
This will delete the complete ACL
To only delete specific entry you can use
no sequence-number
→ no 10



Resequencing ACL's



Extended Acl



Extended ACL has a granular control and complex

different IP protocol numbers

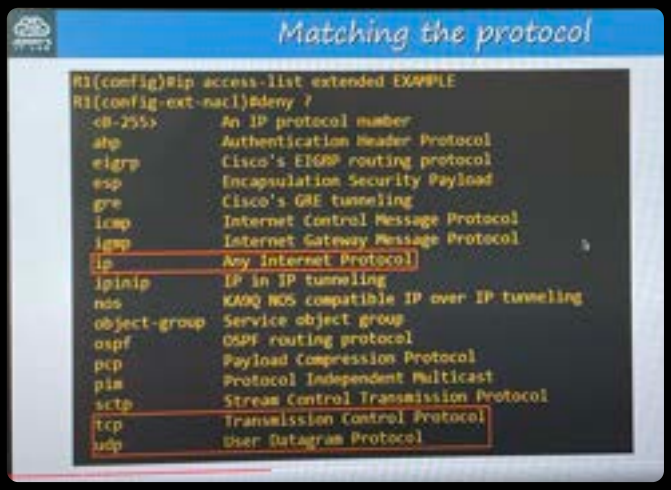
1 : ICMP

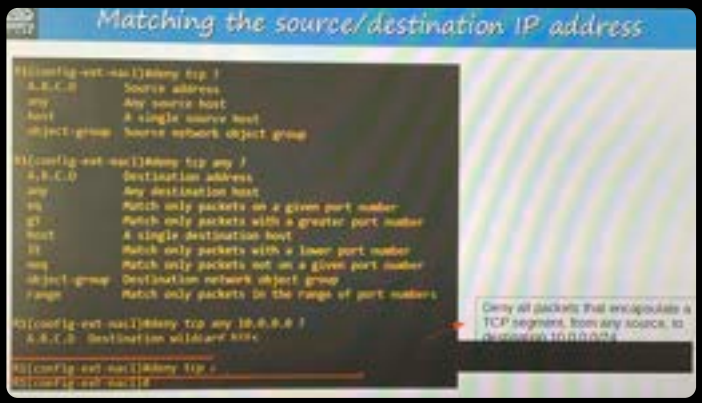
6: TCP

17: UDP

88: EIGRP

89: OSPF

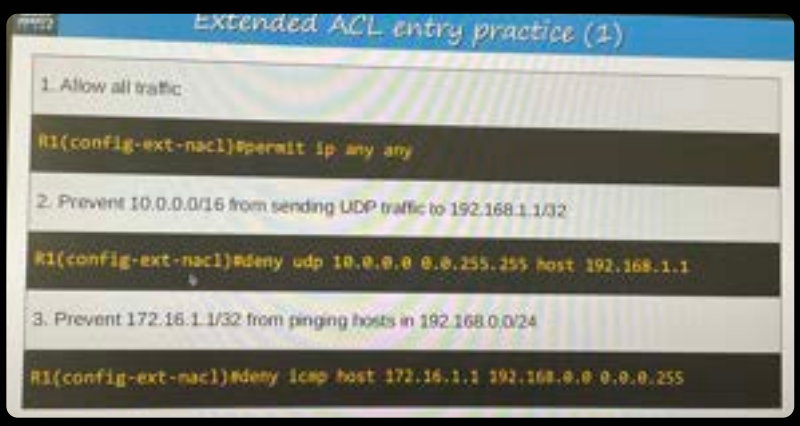




ip access-list extended Example

deny udp 10.0.0.0 0.0.255.255 host 192.168.1.1

deny icmp host 172.16.1.1 192.168.0.0 0.0.0.255



Matching the TCP/UDP port numbers

- When matching TCP/UDP, you can optionally specify the source and/or destination port numbers to match.

```
R1(config-ext-nacl)#deny tcp src-ip  eq   src-port-num   dest-ip  eq   dst-port-num
                                     gt                           gt
                                     lt                           lt
                                     neq                          neq
                                     range                        range
```

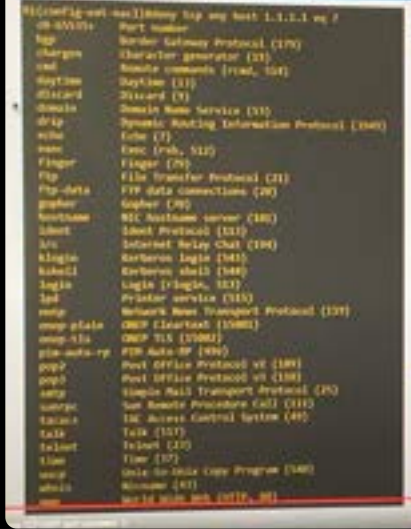
- `eq 80` = equal to port 80
- `gt 80` = greater than 80 (81 and greater)
- `lt 80` = less than 80 (79 and less)
- `neq 80` = NOT 80
- `range 80 100` = from port 80 to port 100

TCP
- FTP data (20)
- FTP control (21)
- SSH (22)
- Telnet (23)
- SMTP (25)
- HTTP (80)
- POP3 (110)
- HTTPS (443)

UDP
- DHCP server (67)
- DHCP client (68)
- TFTP (69)
- SNMP agent (161)
- SNMP manager (162)
- Syslog (514)

TCP & UDP
- DNS (53)

Matching the TCP/UDP port numbers



```
R1(config-std-nacl)#deny tcp any host 1.1.1.1 eq 80
```

→ Deny all packets destined for IP address 1.1.1.1/32, TCP port 80.

After the destination IP address and/or destination port numbers, there are many more options you can use to match (not necessary for the CCNA).
Some examples:

- `ack`: match the TCP ACK flag
- `fin`: match the TCP FIN flag
- `syn`: match the TCP SYN flag
- `ttl`: match packets with a specific TTL value
- `dscp`: match packets with a specific DSCP value

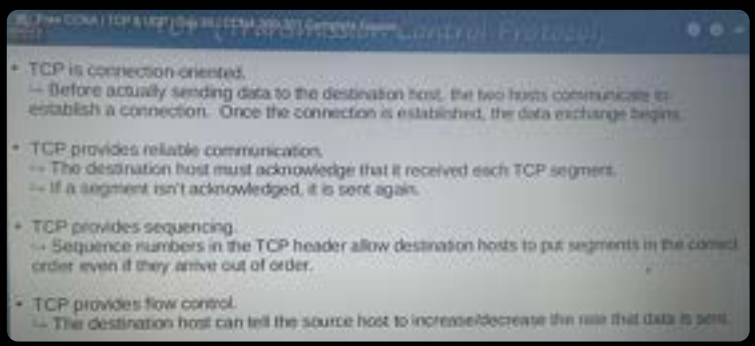
If you specify the protocol, source IP, source port, destination IP, destination port, etc. a packet must match ALL of those values to match the ACL entry. Even if it matches all except one of the parameters, the packet won't match that entry of the ACL.

① permit tcp 10.0.0.16 0.0.255.255 eq 443 2.2.2.2 255.255.255.255 eq 443

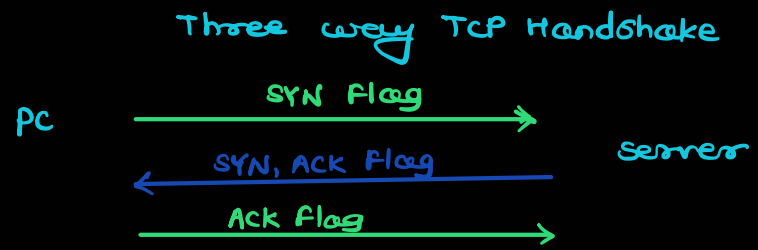
② deny udp any 1

Day 30 - TCP/UDP

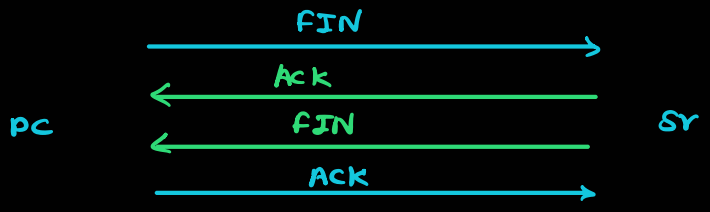
- Layer 4 provides various services to Appln
  - reliable data transfer
  - error recovery
  - data sequencing
  - flow control

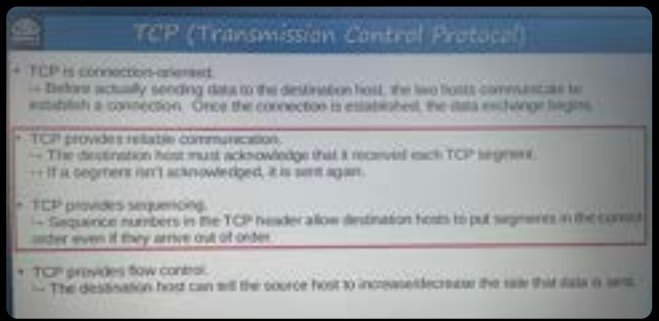


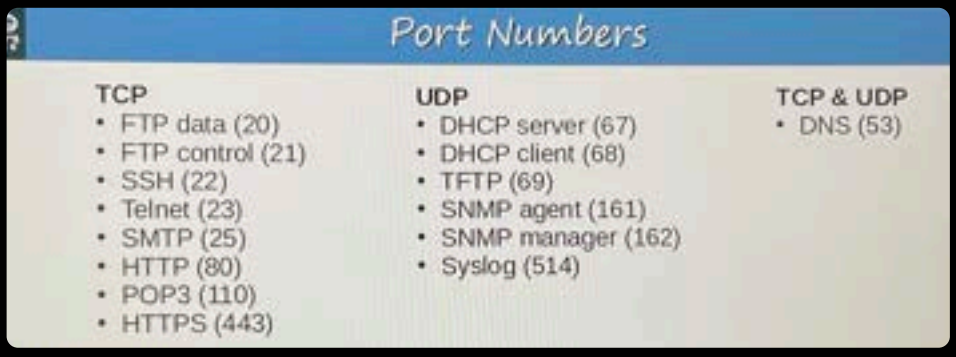
TCP three way handshake →

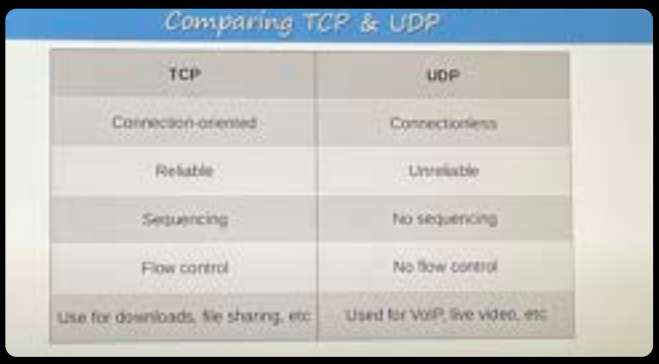


four way Handshake to terminate session









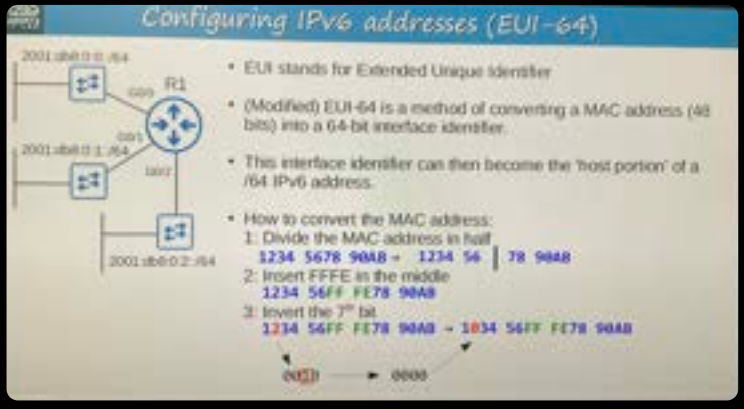
Day 31 – IPv6

To enable IPv6 on the router use command

`(config) # IPv6 unicast-routing`

Day 32 - EUI

Extended Unique identifiers



Convert following Mac address to EUI identified.

① 782B CBAC 0867

782BCBFF FE0867

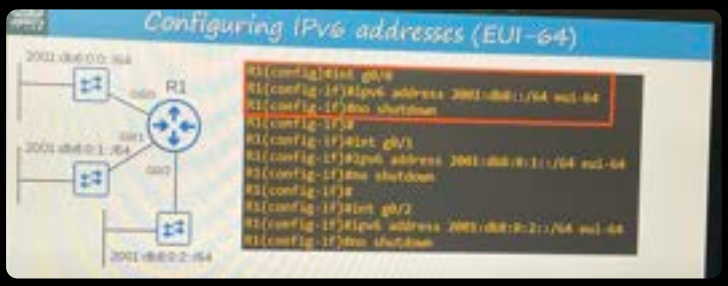
7th bit

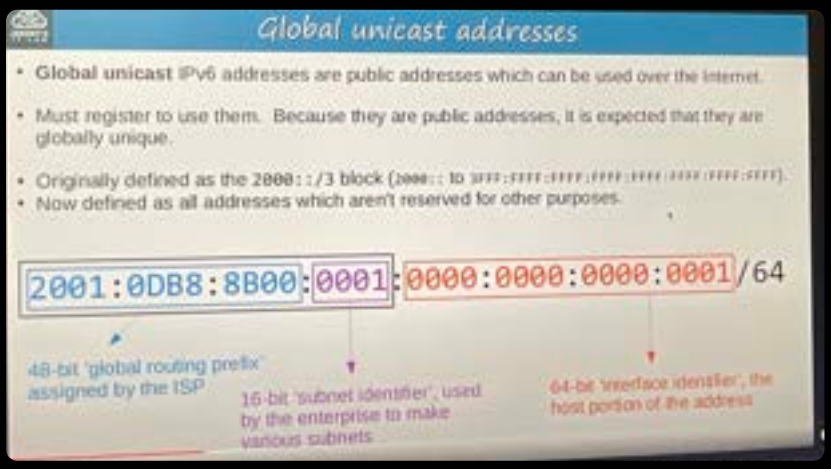
1000

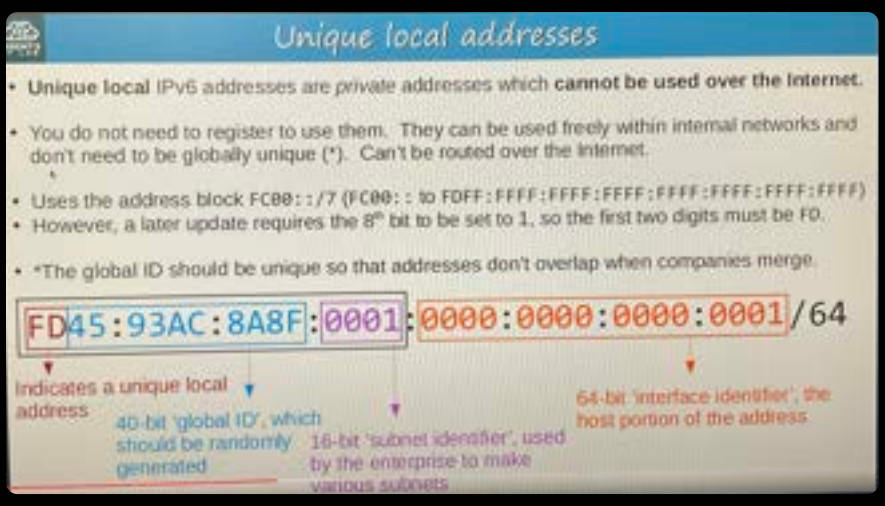
↓

1010

→ 7A2B CBFF FE0867







Multicast addresses

- **Unicast** addresses are one-to-one.
  → One source to one destination.
- **Broadcast** addresses are one-to-all.
  → One source to all destinations (within the subnet).
- **Multicast** addresses are one-to-many.
  → One source to multiple destinations (that have joined the specific multicast group).
- IPv6 uses range `FF00::/8` for multicast. (`FF00::` to `FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF`)
- **IPv6 doesn't use broadcast** (there is no 'broadcast address' in IPv6!)

Multicast addresses

Purpose	IPv6 Address	IPv4 Address
All nodes/hosts (functions like broadcast)	FF02::1	224.0.0.1
All routers	FF02::2	224.0.0.2
All OSPF routers	FF02::5	224.0.0.5
All OSPF DRs/BDRs	FF02::6	224.0.0.6
All RIP routers	FF02::9	224.0.0.9
All EIGRP routers	FF02::A	224.0.0.10

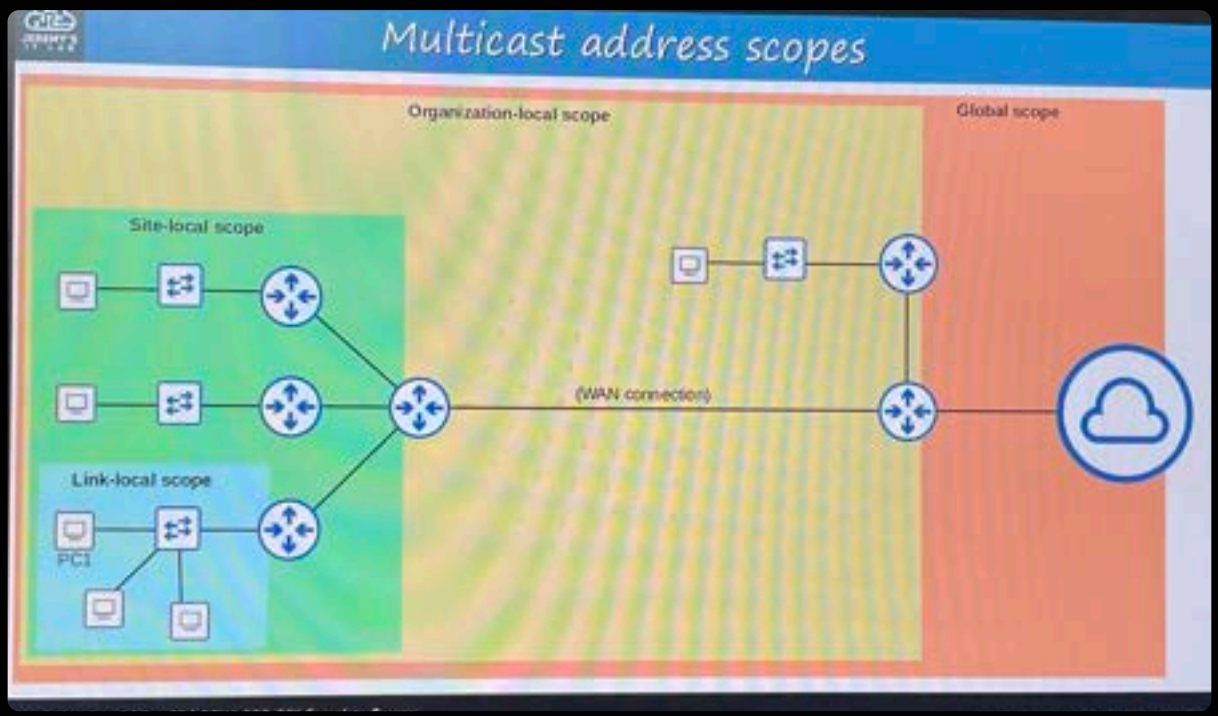
Link local addresses

- **Link-local** IPv6 addresses are automatically generated on IPv6-enabled interfaces.
- Use command `R1(config-if)# ipv6 enable` on an interface to enable IPv6 on an interface.
- Uses the address block `FE80::/10` (`FE80::` to `FEBF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF`)
- However, the standard states that the 54 bits after `FE80/10` should be all 0, so you won't see link local addresses beginning with `FE9`, `FEA`, or `FEB`. Only `FE8`.
- The interface ID is generated using EUI-64 rules.
- *Link-local* means that these addresses are used for communication within a single link (subnet). Routers **will not** route packets with a link-local destination IPv6 address.
- Common uses of link-local addresses:
  → routing protocol peerings (OSPFv3 uses link-local addresses for neighbor adjacencies)
  → next-hop addresses for static routes
  → *Neighbor Discovery Protocol* (NDP, IPv6's replacement for ARP) uses link-local addresses to function

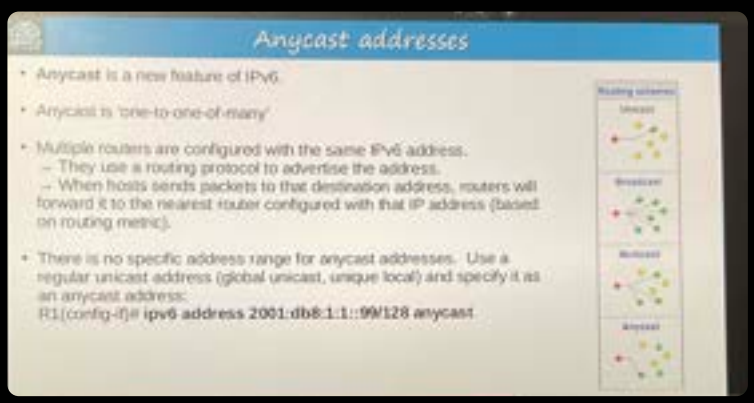
DO 32 again

Multicast address scopes

- IPv6 defines multiple multicast 'scopes' which indicate how far the packet should be forwarded.
- The addresses in the previous slide all use the 'link-local' scope (FF02), which stays in the local subnet.
- IPv6 multicast scopes:
  - ↳ **Interface-local** (FF01): The packet doesn't leave the local device. Can be used to send traffic to a service within the local device.
  - ↳ **Link-local** (FF02): The packet remains in the local subnet. Routers will not route the packet between subnets.
  - ↳ **Site-local** (FF05): The packet can be forwarded by routers. Should be limited to a single physical location (not forwarded over a WAN)
  - ↳ **Organization-local** (FF08): Wider in scope than site-local (an entire company/organization).
  - ↳ **Global** (FF0E): No boundaries. Possible to be routed over the Internet.



Anycast Addoess –



Other IPv6 Addresses

- :: = The *unspecified* IPv6 address
  - Can be used when a device doesn't yet know its IPv6 address.
  - IPv6 default routes are configured to `::/0`
  - IPv4 equivalent: `0.0.0.0`
- ::1 = The loopback address
  - Used to test the protocol stack on the local device.
  - Messages sent to this address are processed within the local device, but not sent to other devices.
  - IPv4 equivalent: `127.0.0.0/8` address range

R1's G0/1 interface has a MAC address of `0D2A.4FA3.0081`.
What will G0/1's IPv6 address be after issuing the following command?
R1(config-if)# **ipv6 address 2001:db8:0:1::/64 eui-64**

a) 2001:db8:0:1:082A:4FFF:FFA3:81

b) 2001:db8:0:1:C2A:4FFF:FEA3:81

c) 2001:db8:0:1:0F2A:4FFF:FFA3:81

d) 2001:db8:0:1:F2A:4FFF:FEA3:81

Quiz 2

Which portion of the IPv6 address below is the 'global ID'?
FD89:3B12:3794:0020:0000:0000:2347:0001/64

a) FD89:3B12:3794:0020:0000:0000:2347:0001/64

b) FD89:3B12:3794:0020:0000:0000:2347:0001/64

c) FD89:3B12:3794:0020:0000:0000:2347:0001/64

d) FD89:3B12:3794:0020:0000:0000:2347:0001/64

Quiz 4

What kind of IPv6 address is automatically configured on an interface when the following command is used? (select the best answer)
`R1(config-if)# ipv6 enable`

a) Unique local

b) Node-local

c) Link-local

d) EUI-64

Day 32 - 37 → skipped FN

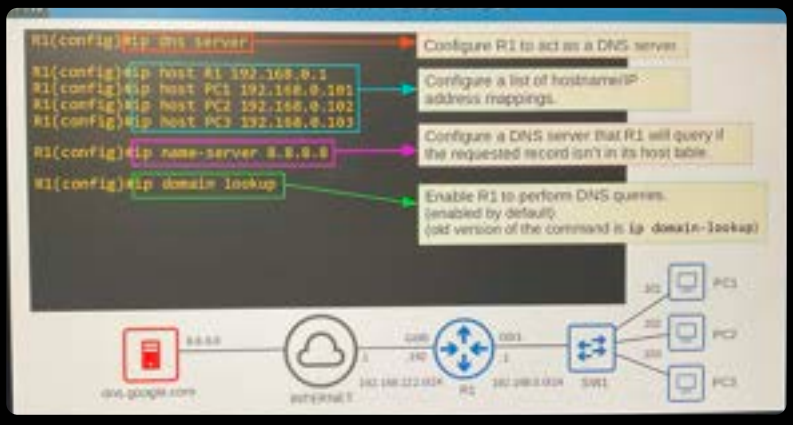
Day 38 - DNS

① ipconfig/displaydns
② ipconfig/flushdns

Configuring router as a DNS server

```
(config) #   ip dns server
   →←    #   ip host R1  192.168.0.1
   →←        ip host PC1 192.168.0.101
```

```
#   ip name-server 8.8.8.8
#   ip domain lookup
```



To see the configured hosts

```
R1 # show hosts
```

** • DNS uses port 53 and both protocols TCP/UDP
** if message is greater than 512 bytes DNS uses TCP

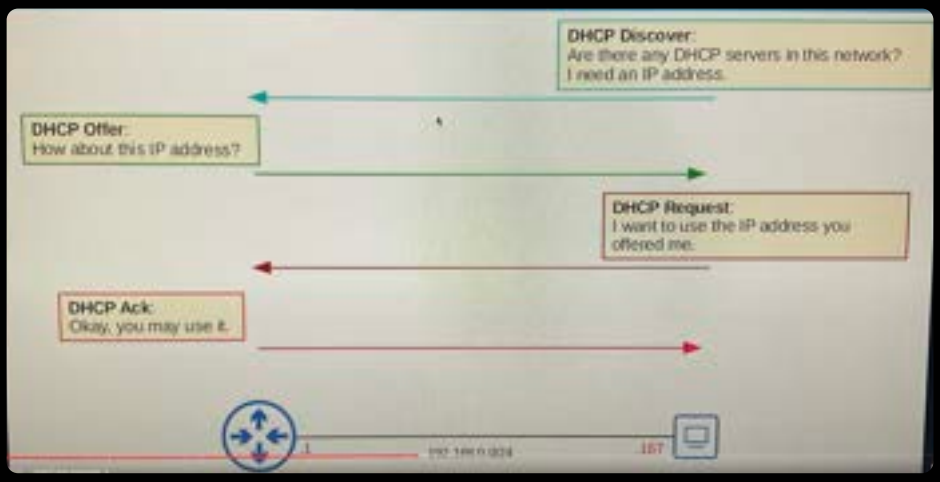
DHCP is used to assign DNS servers to Hosts

- Day 39 - DHCP

- Dynamic Host configuration Protocol

DHCP server → UDP 67
DHCP client → UDP 68

— DORA —

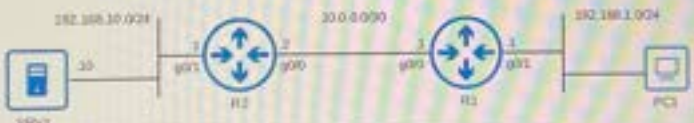


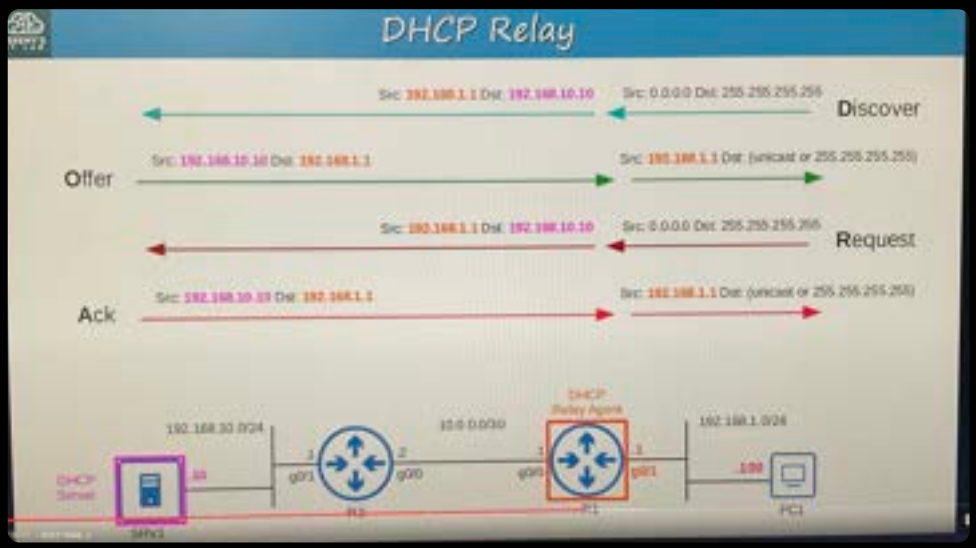
DHCP D-O-R-A

Discover	Client → Server	Broadcast
Offer	Server → Client	Broadcast or Unicast
Request	Client → Server	Broadcast
Ack	Server → Client	Broadcast or Unicast

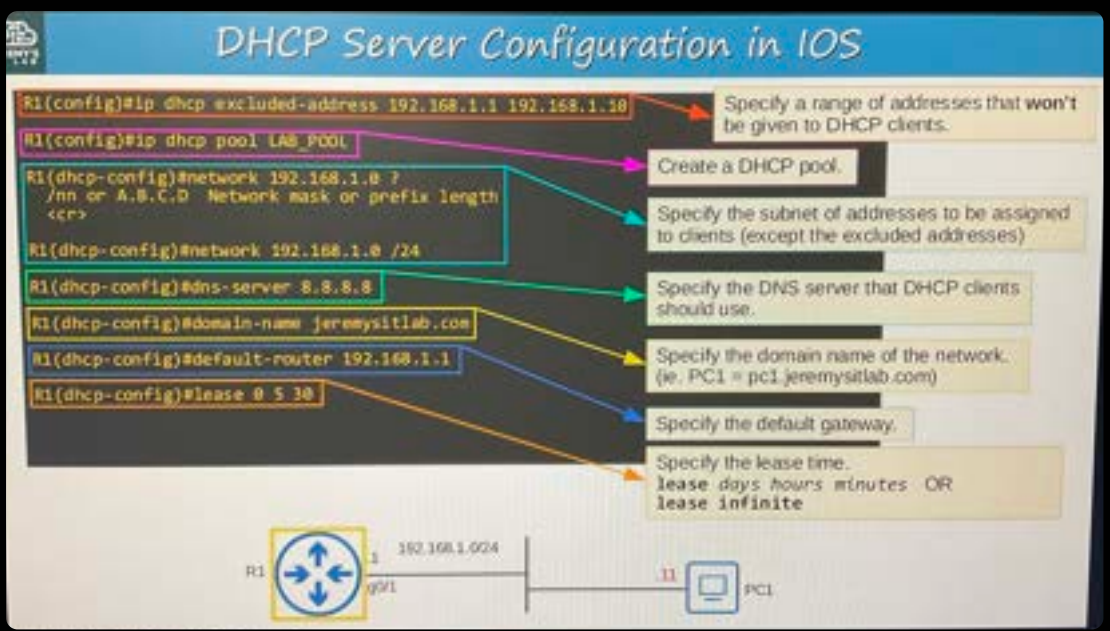
DHCP Relay

- Some network engineers might choose to configure each router to act as the DHCP server for its connected LANs.
- However, large enterprises often choose to use a centralized DHCP server.
- If the server is centralized, it won't receive the DHCP clients' broadcast DHCP messages. (broadcast messages don't leave the local subnet)
- To fix this, you can configure a router to act as a **DHCP relay agent**.
- The router will forward the clients' broadcast DHCP messages to the remote DHCP server as unicast messages.





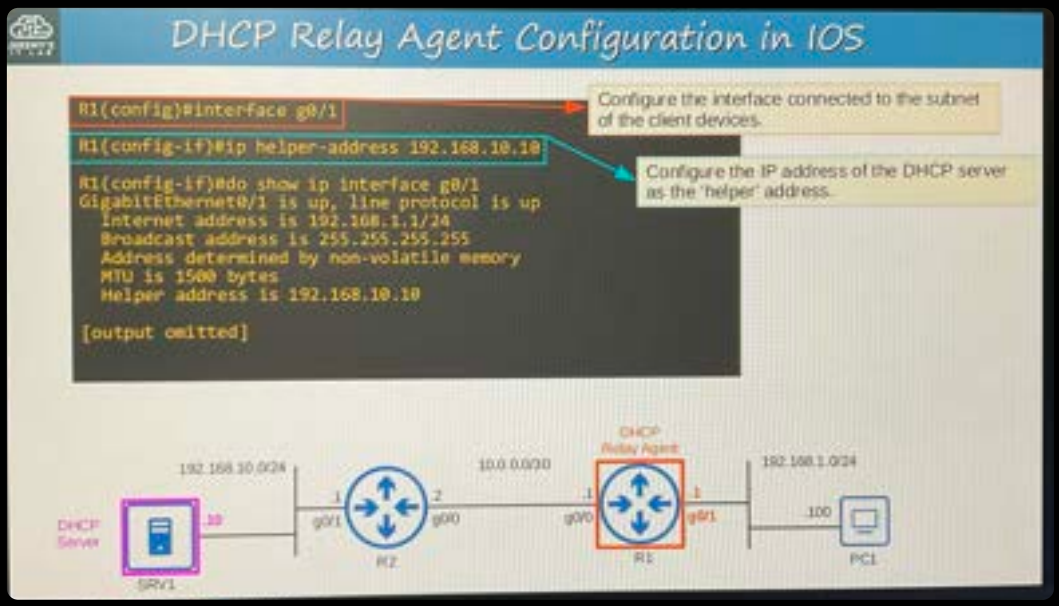
DHCP configuration in IOS



show ip dhcp binding

+ DHCP Relay agent configuration

- We also have to make it client first

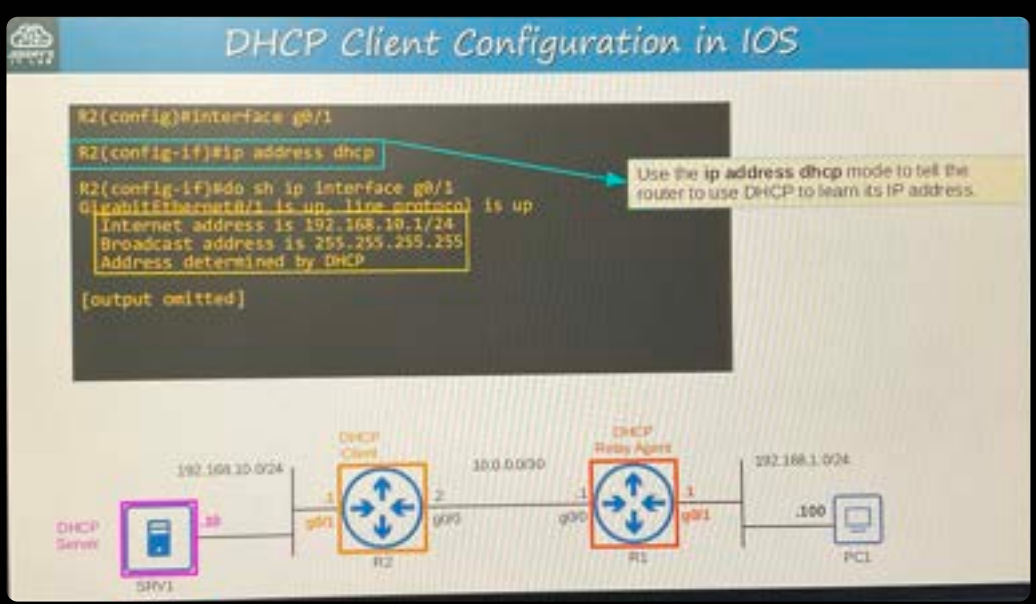


+ DHCP client

To configure cisco devices interfaces with DHCP.

→ However, it is rare that we do this way

We usually, set them manually



Day 40 → SNMP

Simple network Management protocol

Two types

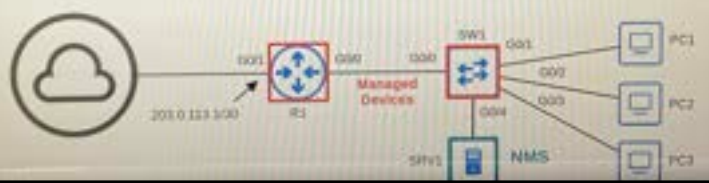
1. Managed devices
2. Network management station (NMS)

Simple Network Management Protocol

- SNMP is an industry-standard framework and protocol that was originally released in 1988.
  RFC 1065 – Structure and identification of management information for TCP/IP-based internets
  RFC 1066 – Management information base for network management of TCP/IP-based internets
  RFC 1067 – A simple network management protocol
  SNMPv1
- Don't let the 'Simple' in the name fool you!
- SNMP can be used to monitor the status of devices, make configuration changes, etc.
- There are two main types of devices in SNMP:
  1) Managed Devices
  → These are the devices being managed using SNMP.
  → For example, network devices like routers and switches.
  2) Network Management Station (NMS)
  → The device/devices managing the managed devices.
  → This is the SNMP 'server'.

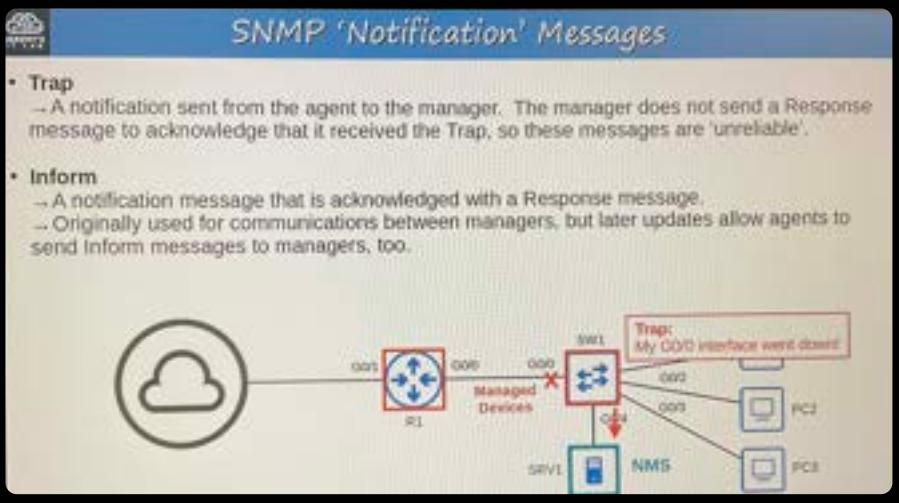
SNMP Operations

- There are three main operations used in SNMP.
  1) Managed devices can notify the NMS of events.
  2) The NMS can ask the managed devices for information about their current status.
  3) The NMS can tell the managed devices to change aspects of their configuration.



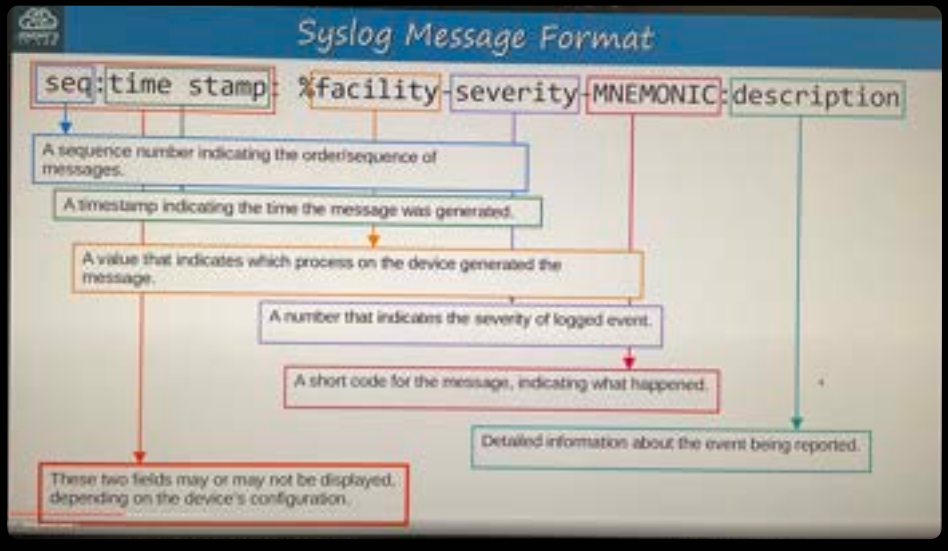
SNMP Messages

Message Class	Description	Messages
Read	Messages sent by the **NMS** to read information from the **managed devices**. (ie. What's your current CPU usage %?)	*Get* *GetNext* *GetBulk*
Write	Messages sent by the **NMS** to change information on the **managed devices**. (ie. change an IP address)	*Set*
Notification	Messages sent by the **managed devices** to alert the **NMS** of a particular event. (ie. interface going down)	*Trap* *Inform*
Response	Messages sent in response to a previous message/request.	*Response*



— SNMP Agent = UDP 161
— SNMP Manager = UDP 162

Day 41 — Syslog



Syslog Severity Levels

Level	Keyword	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition (**Notification**)
6	Informational	Informational messages
7	Debugging	Debug-level messages

EACEWNID

Every Awesome Cisco Engineer will Need Ice cream Daily

example →

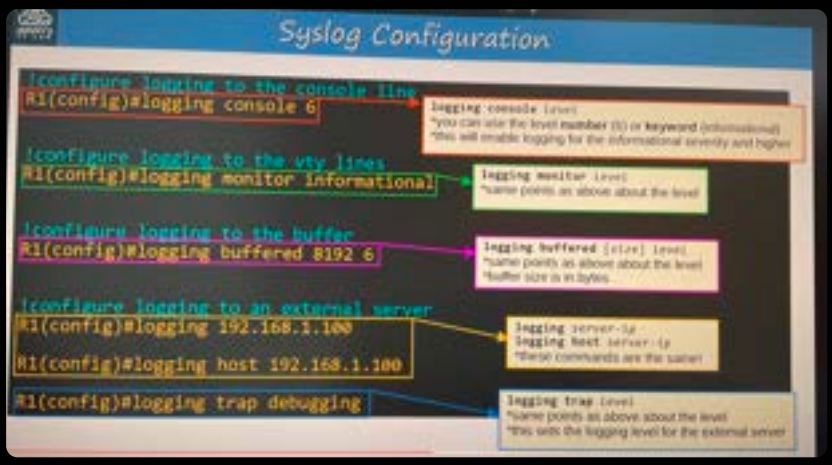
Syslog Message Examples

seq:time stamp: %facility-severity-MNEMONIC:description

```
*Feb 11 03:02:55.304: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up

*Feb 11 05:04:39.606: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on GigabitEthernet0/0 from
LOADING to FULL, Loading Done

000043: *Feb 11 05:06:43.331: %SYS-5-CONFIG_I: Configured from console by jeremy on console
```

###

Syslog servers will listen for messages on UDP port 514



Every Awesome Cisco Engineer will Need Ice cream Daily

terminal monitor

- Even if **logging monitor** *Level* is enabled, by default Syslog messages will not be displayed when connected via Telnet or SSH.
- For the messages to be displayed, you must use the following command:

```
R1#terminal monitor
```

- This command must be used **every time you connect to the device via Telnet or SSH**.

logging synchronous

- By default, logging messages displayed in the CLI while you are in the middle of typing a command will result in something like this:

```
R1(config)#exit
R1#show ip in
*Feb 11 09:38:41.607: %SYS-5-CONFIG_I: Configured from console by jeremy on
consoleterface brief
```

- To prevent this, you should use the **logging synchronous** on the appropriate *line*.
(I will talk more about 'line' configuration in the Telnet/SSH video!)

```
R1(config)#line console 0
R1(config-line)#logging synchronous
```

- This will cause a new line to be printed if your typing is interrupted by a message.

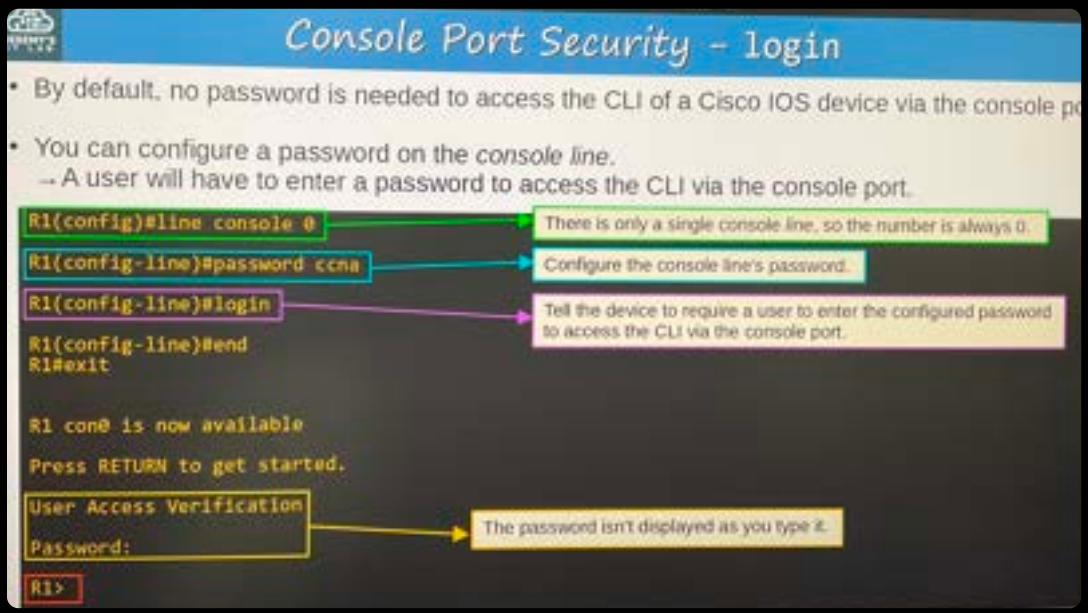
```
R1(config)#exit
R1#show ip int
*Feb 11 09:41:00.554: %SYS-5-CONFIG_I: Configured from console by jeremy on console
R1#show ip int
```

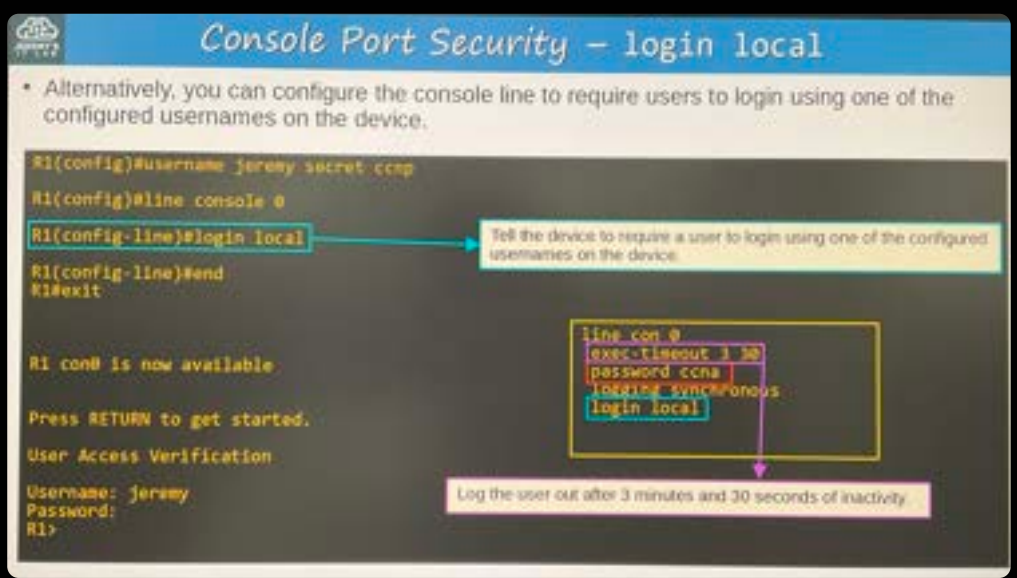
service timestamps / service sequence-numbers

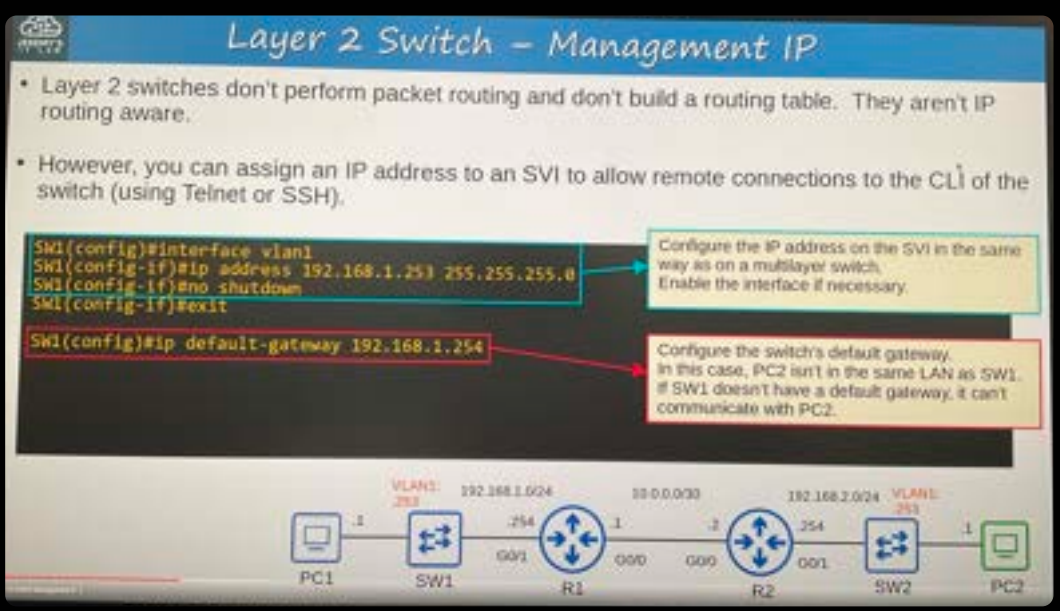
```
R1(config)#service timestamps log ?
  datetime  Timestamp with date and time
  uptime    Timestamp with system uptime
  <cr>

R1(config)#service timestamps log datetime
R1(config)#
R1(config)#service sequence-numbers
R1(config)#exit
R1#
000039: *Feb 11 10:32:46: %SYS-5-CONFIG_I: Configured from console by
jeremy on console
```

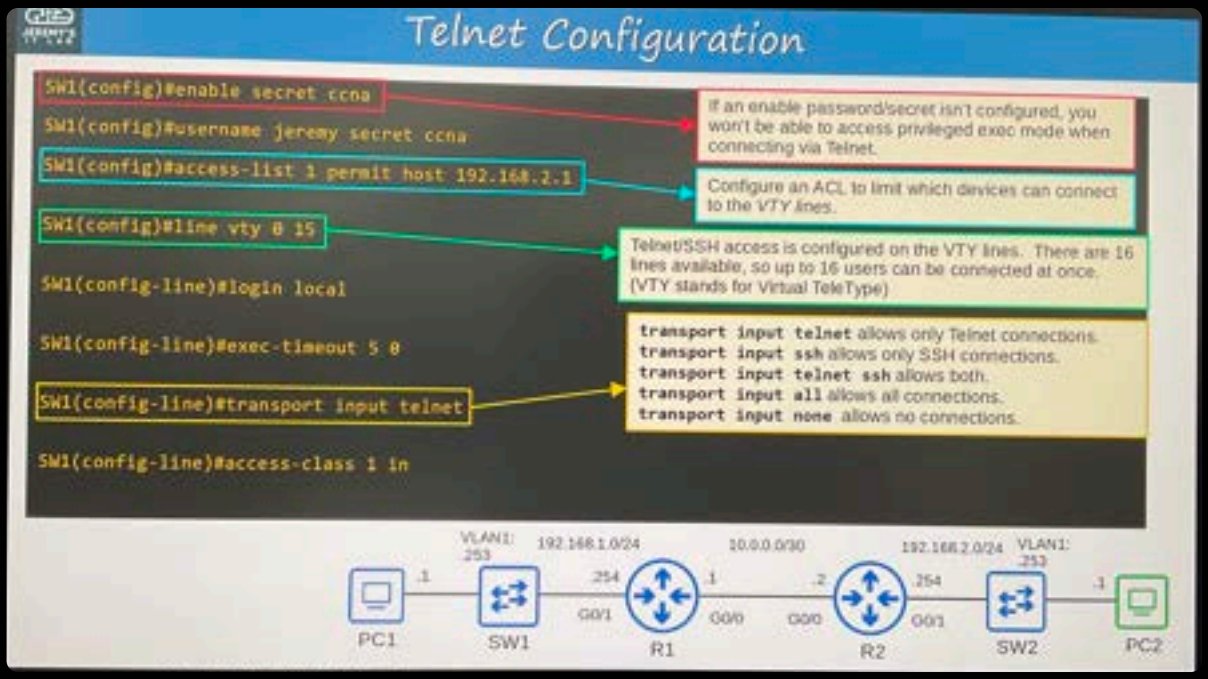
datetime = timestamps will display the date/time when the event occurred.
uptime = timestamps will display how long the device had been running when the event occurred.

Day 42 - SSH, Telnet









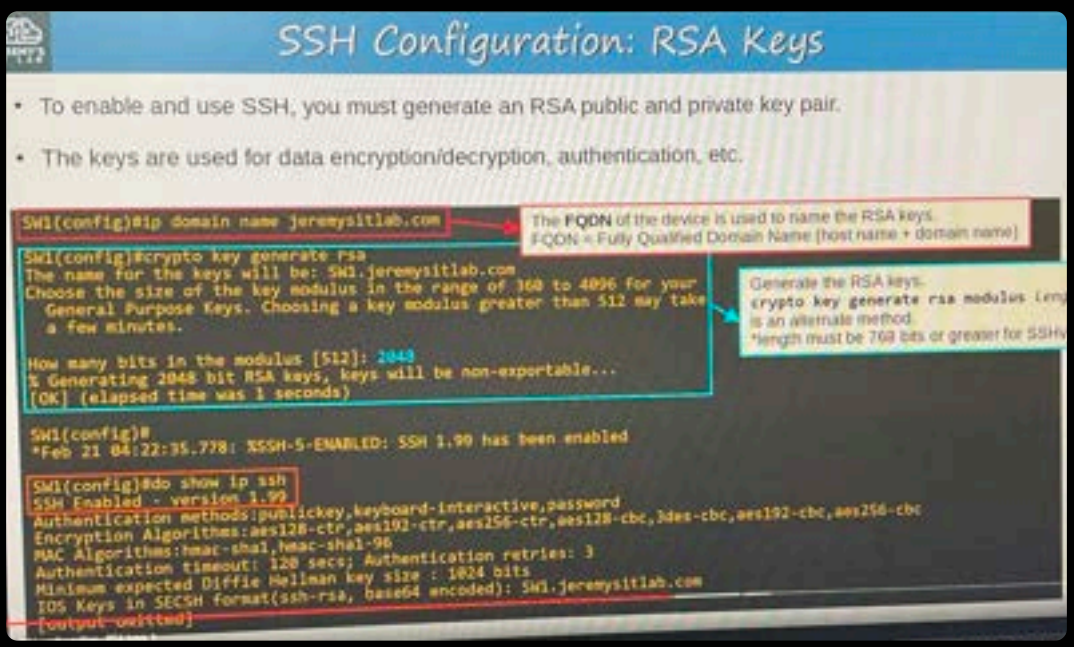
SSH – Secure shell

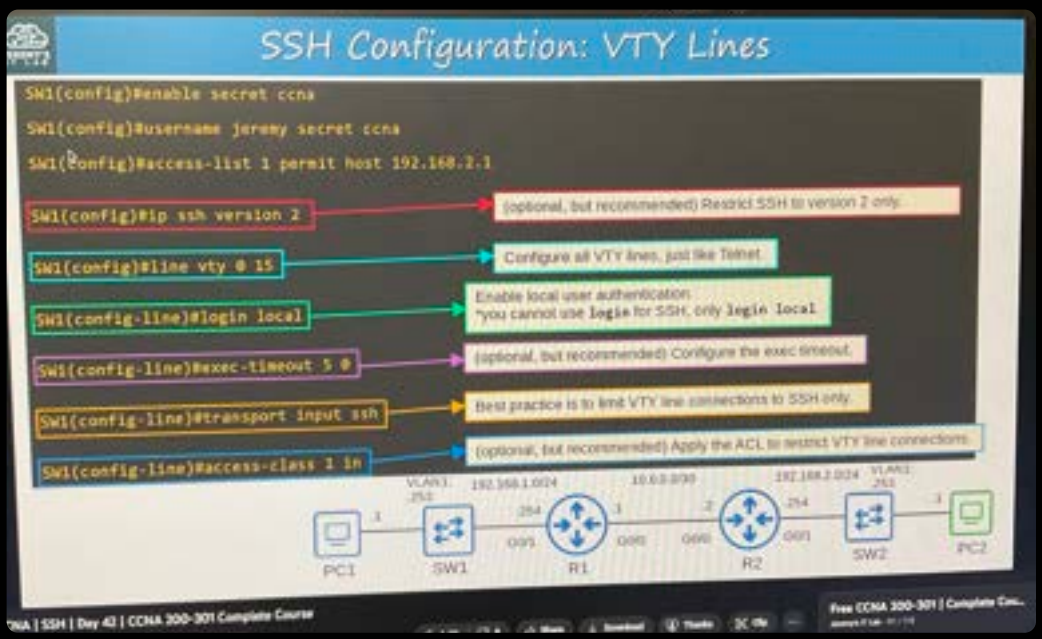
- if device supports version 1 and version 2 it is said to run 'version 1.99'

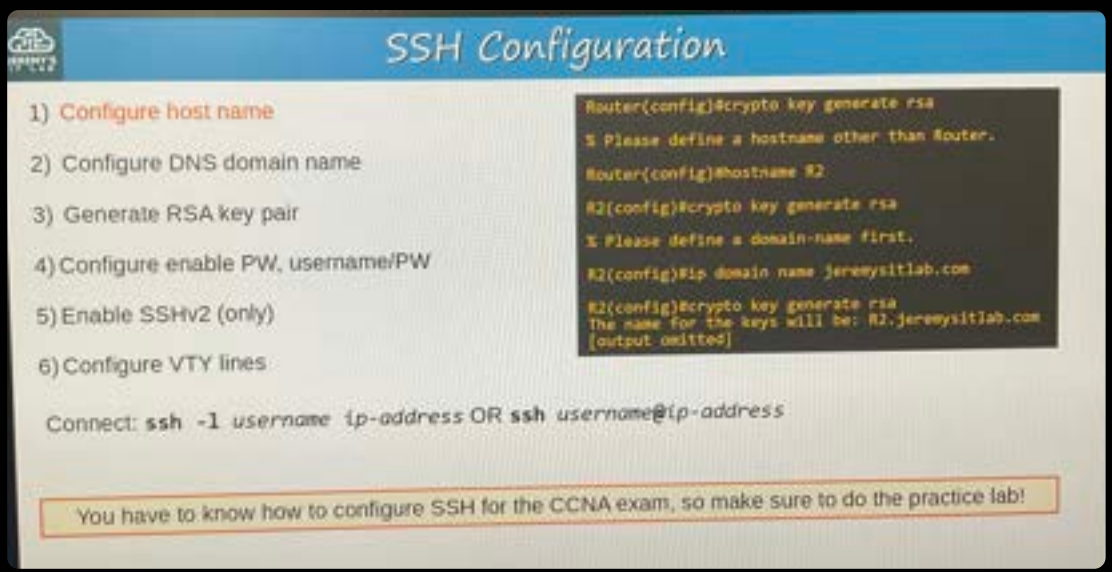
ios images that supports ssh will have k9 in their name

`sw1 # show version`

`sw1 # show ip ssh`







You want to allow only 192.168.1.1 to connect to R1 via SSH. Which of the following configurations fulfills that requirement?

a)
```
R1(config)#access-list 199 permit tcp host 192.168.1.1 any eq 23
R1(config)#line vty 0 15
R1(config-line)#access-class 199 in
```

b)
```
R1(config)#access-list 199 permit tcp host 192.168.1.1 any eq 22
R1(config)#line vty 0 15
R1(config-line)#access-class 199 in
```

c)
```
R1(config)#access-list 199 permit tcp host 192.168.1.1 any eq 22
R1(config)#line con 0
R1(config-line)#access-group 199 in
```

d)
```
R1(config)#access-list 199 permit tcp host 192.168.1.1 any eq 22
R1(config)#line vty 0 15
R1(config-line)#access-group 199 in
```

e)
```
R1(config)#access-list 199 permit udp host 192.168.1.1 any eq 22
R1(config)#line vty 0 15
R1(config-line)#access-class 199 in
```

Quiz 5

A network admin using PC1 is remotely configuring SW1 by connecting to the CLI of SW1 via SSH. What is the role of SW1 in this situation?

a) SSH peer

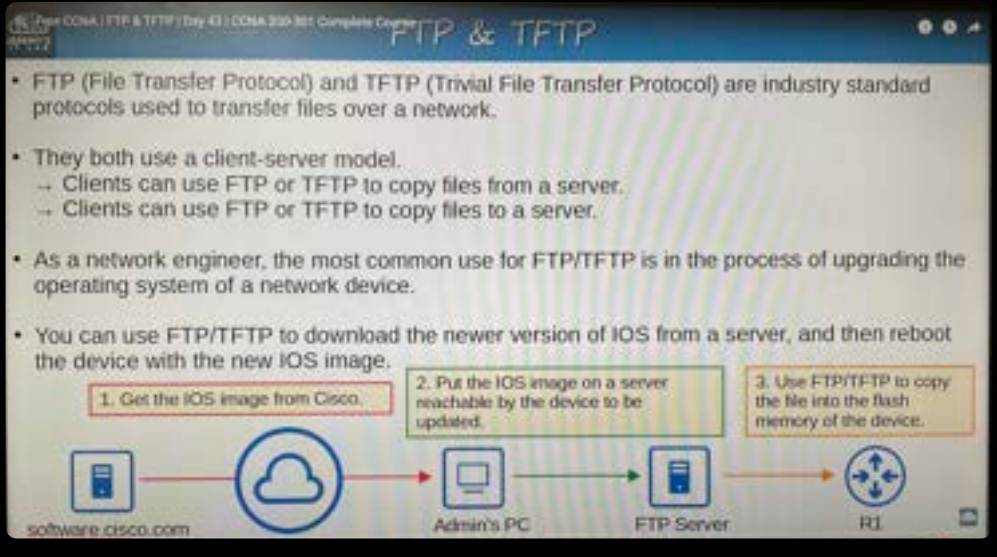
b) SSH server

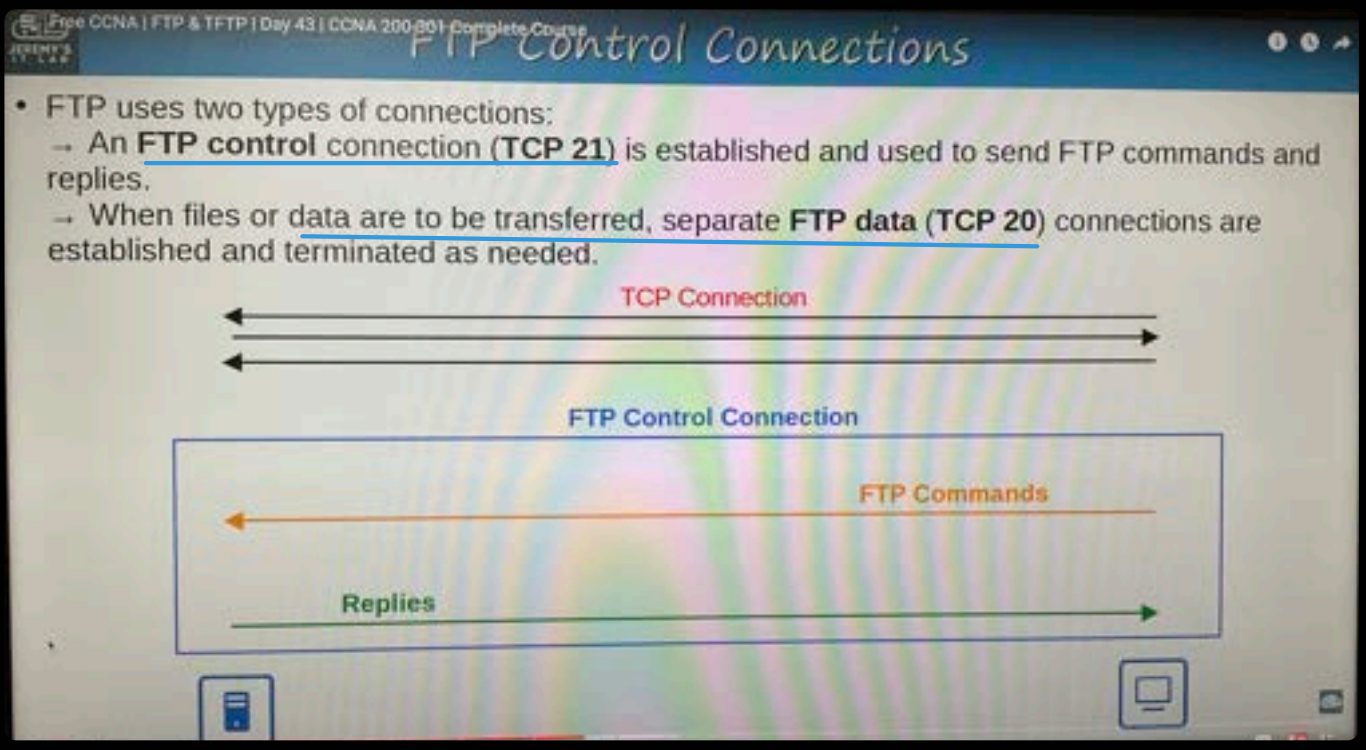
c) SSH client

d) None of the above

Day 43 – FTP / TFTP

① File transfer protocol — UDP port 69
② Trivial File transfer protocol — TCP port 20 & 21





① Active mode

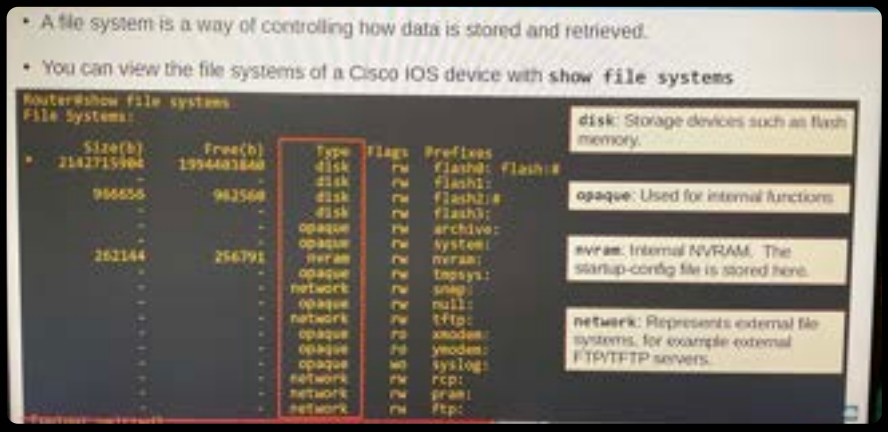
In FTP Active mode server initiates the connection

② Possive mode - client initiates the connection this is usually done when client is behind the firewall and any incoming connections are blocked.

FTP	TFTP
-Uses TCP (20 for data, 21 for control) for connection-based communication	-Uses UDP (69) for connectionless communication (although a basic form of 'connection' is used within the protocol itself)
-Clients can use FTP commands to perform various actions, not just copy files	-Clients can only copy files to or from the server
-Username/PW authentication	-No authentication
-More complex	-Simpler

Cisco device file systems

— Router # show file systems



Upgrading ios —

show version
⟶ if k9 in version that means SSH enabled

show flash

R1 # copy tftp: flash:

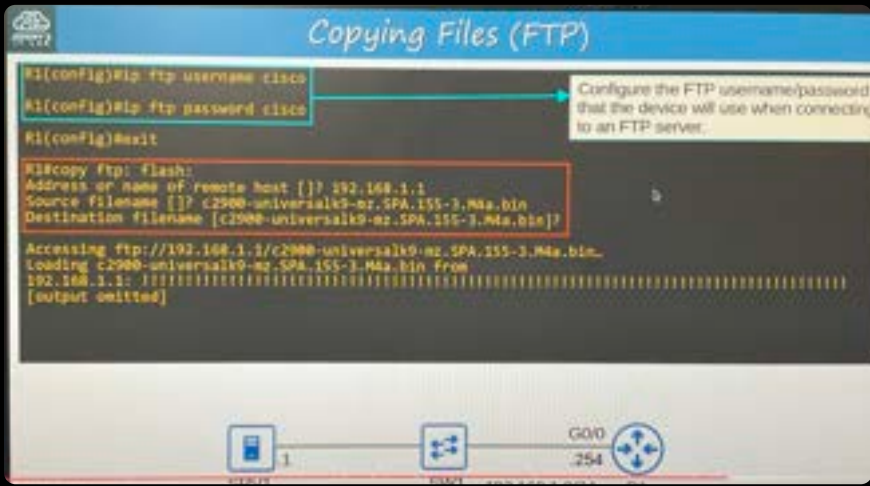
To upgrade —

R1(config) # boot system flash : filename.bin

wr
Reload
show version

To delete → delete flash: filename

R1 (config) # ip ftp username cisco



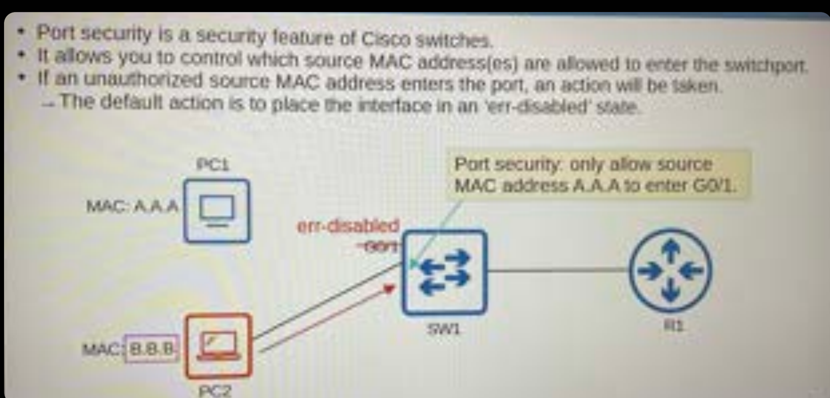

```
R1# show file systems
R1# show version
R1# show flash
R1# copy source destination
R1(config)# boot system filepath
R1(config)# ip ftp username username
R1(config)# ip ftp password password
```

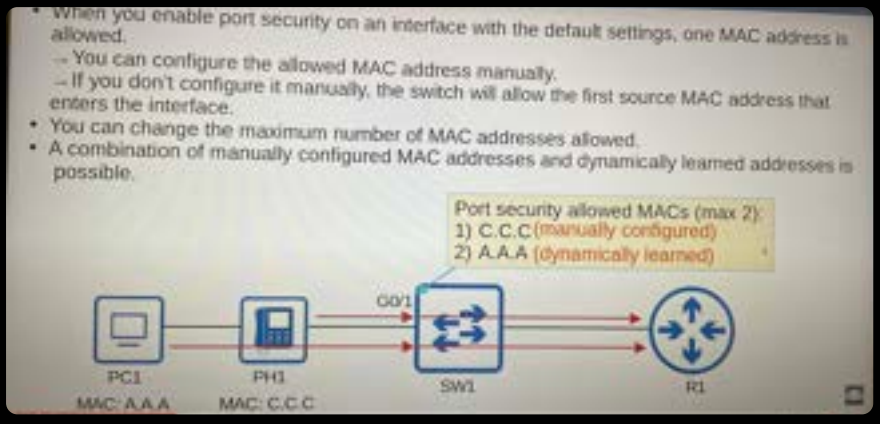
→ Skip 44-47

Day 48 —

Security fundamentals

Day 49 - Port Security





- Post security isn't a perfect solution because we can spoof Mac addresses

Config –

show post-security interface g0/1

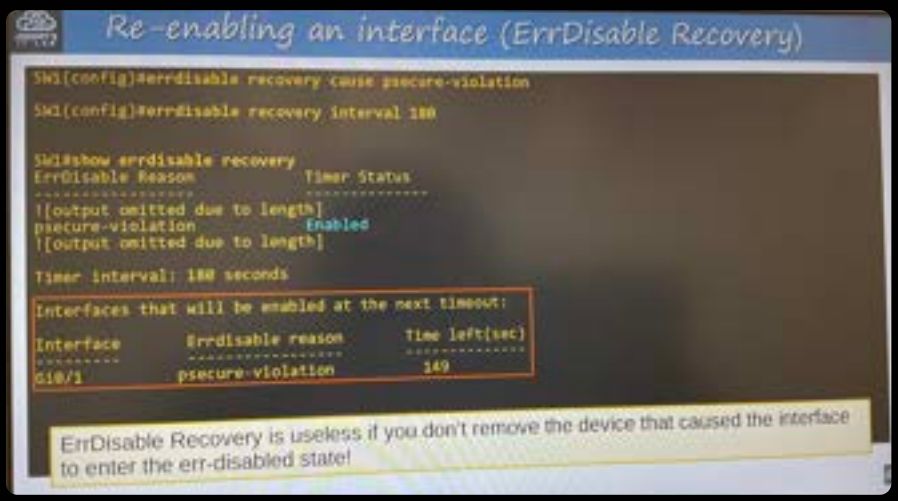
show interfaces status

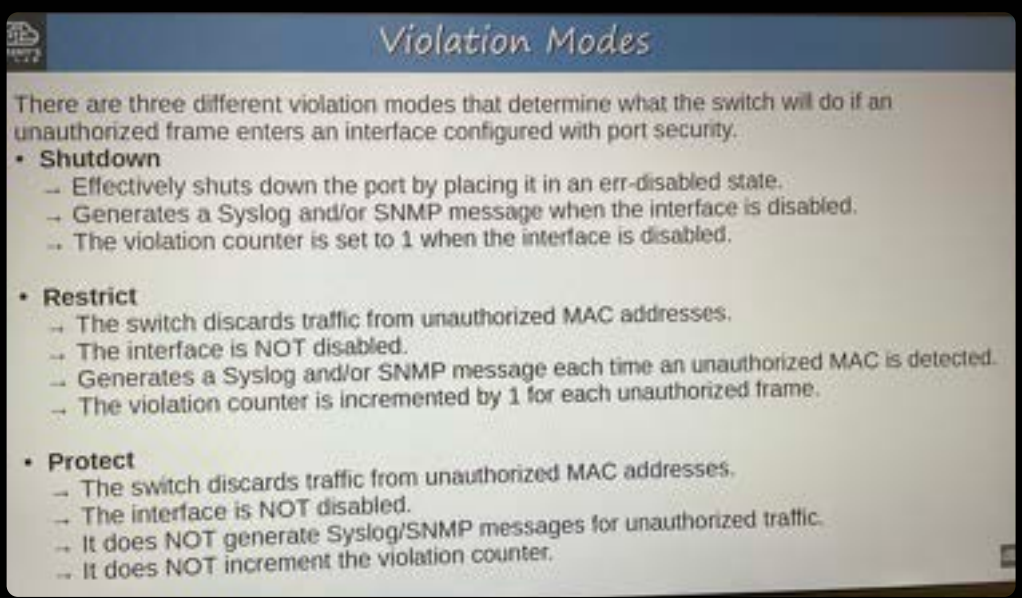
TO re-enable device which is err-disconnecting

interface g0/1
shutdown
no shutdown

TO automatically re-enable after certain time

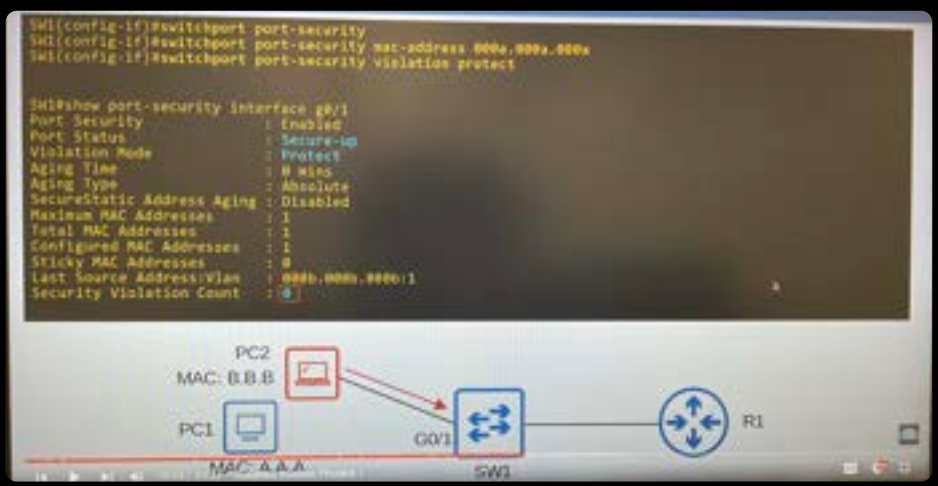
errdisable recovery cause psecure-violation
errdisable recovery interval 180
show errdisable recovery





Configuring different violation modes

→



Secure MAC address aging

```
SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000a.000a.000a:1
Security Violation Count   : 0
```

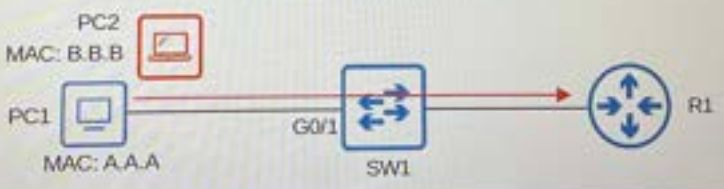
- By default secure MAC addresses will not 'age out' (`Aging Time : 0 mins`)
  - → Can be configured with **`switchport port-security aging time`** *minutes*
- The default aging type is **Absolute**
  - → **Absolute**: After the secure MAC address is learned, the aging timer starts and the MAC is removed after the timer expires, even if the switch continues receiving frames from that source MAC address.
  - → **Inactivity**: After the secure MAC address is learned, the aging timer starts but is reset every time a frame from that source MAC address is received on the interface.
  - → Aging type is configured with **`switchport port-security aging type {absolute | inactivity}`**
- Secure Static MAC aging (addresses configured with **`switchport port-security mac-address`** *x.x.x*) is disabled by default.
  - → Can be enabled with **`switchport port-security aging static`**

Secure MAC address aging

```
SW1(config-if)#switchport port-security aging time 30
SW1(config-if)#switchport port-security aging type inactivity
SW1(config-if)#switchport port-security aging static


SW1#show port-security interface g0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 30 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Enabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000a.000a.000a:1
Security Violation Count   : 0

SW1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------------
     Gi0/1            1             1                0          Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

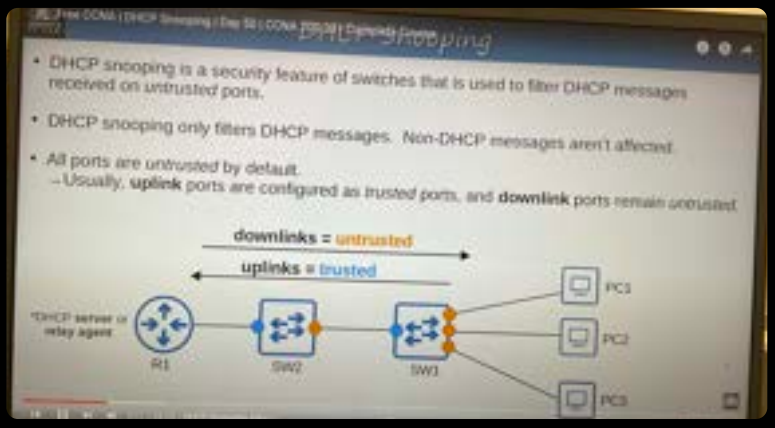
Sticky Secure MAC Addresses

```
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address sticky
SW1(config-if)#do show running-config interface g0/1
!
interface GigabitEthernet0/1
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000a.000a.000a
 switchport port-security
 negotiation auto
```

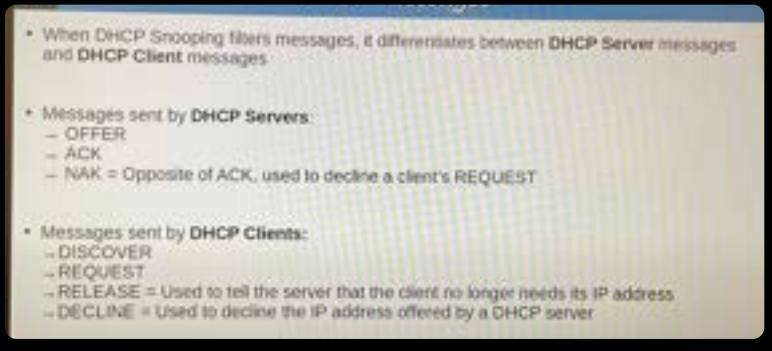


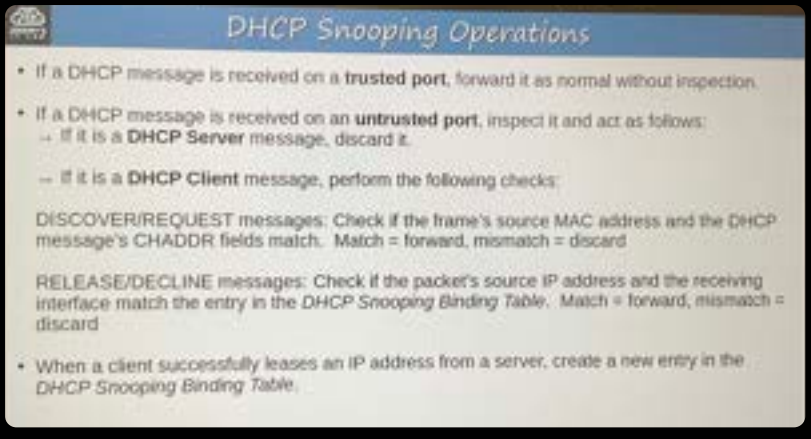
Day 50 —
DHCP Snooping

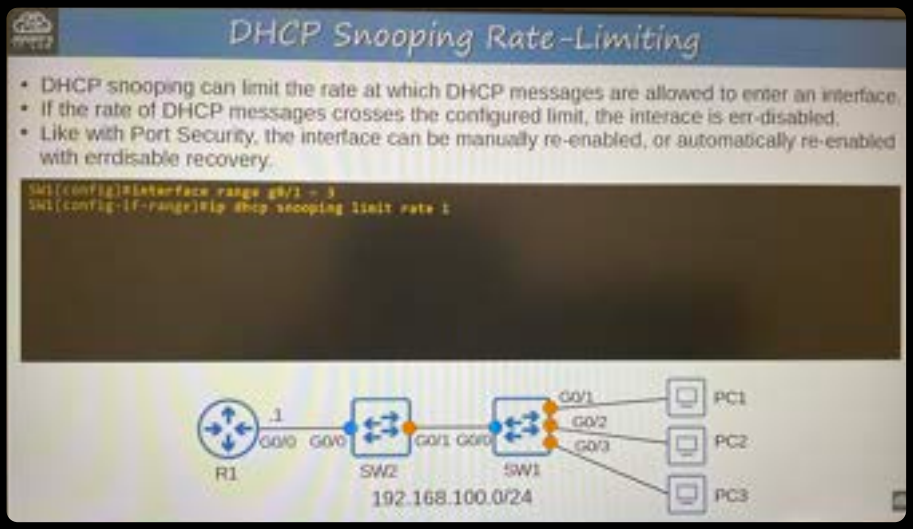
It is a security feature of switches that is used to filter DHCP messages received on untrusted ports.



DHCP Snooping protect against a attacks like
① DHCP starvation
② DHCP Poisoining



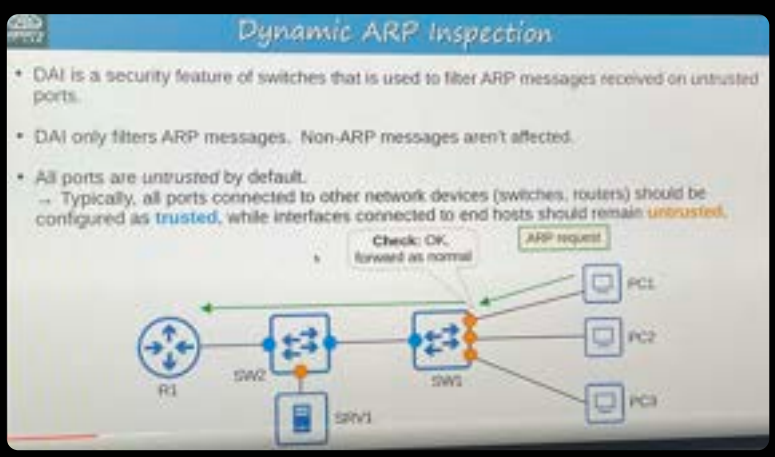


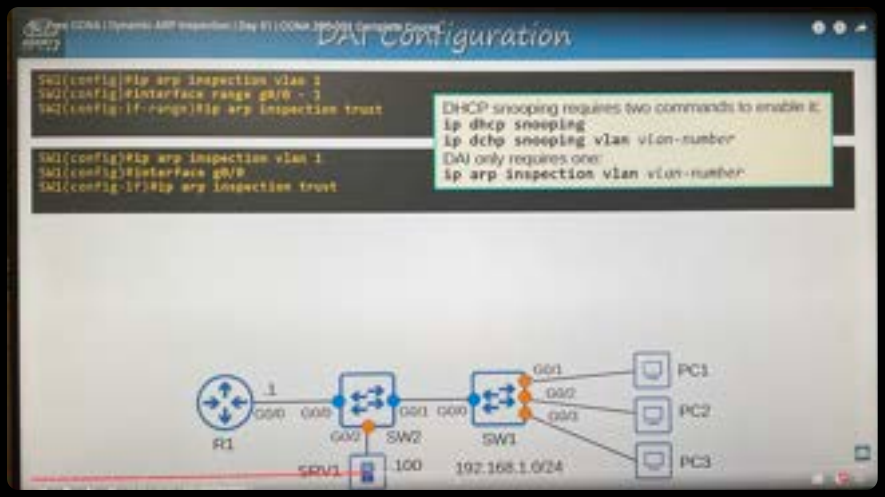


Day 51

Dynamic ARP Inspection

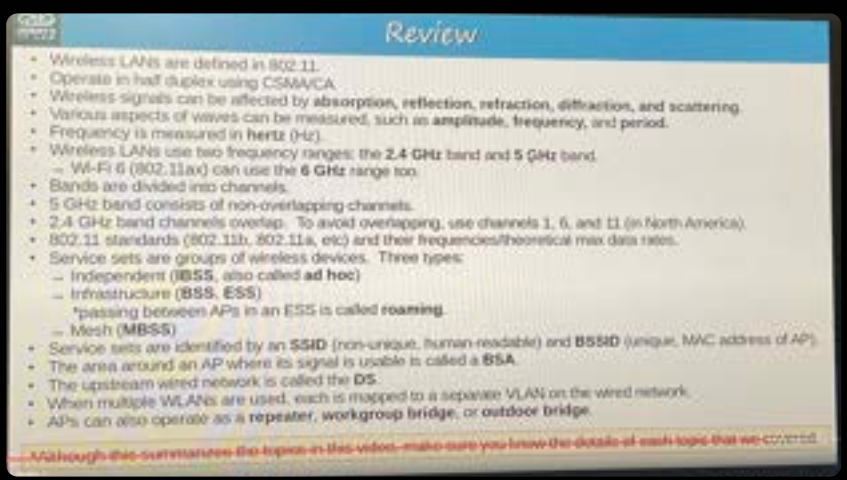
DAI –



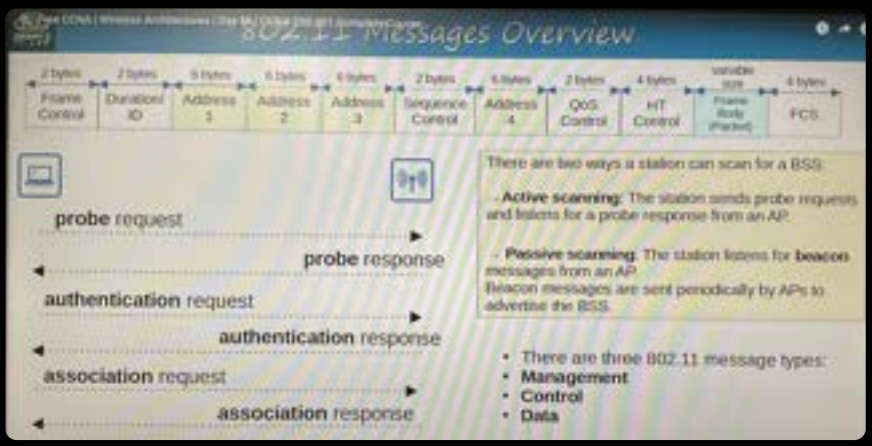


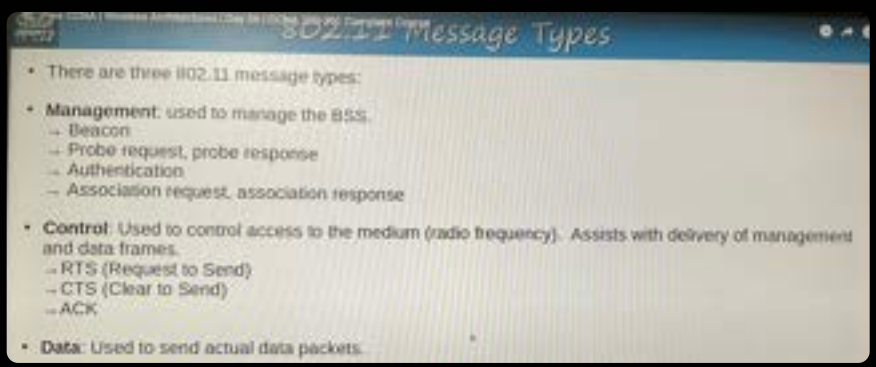
Day 55- Wireless lans

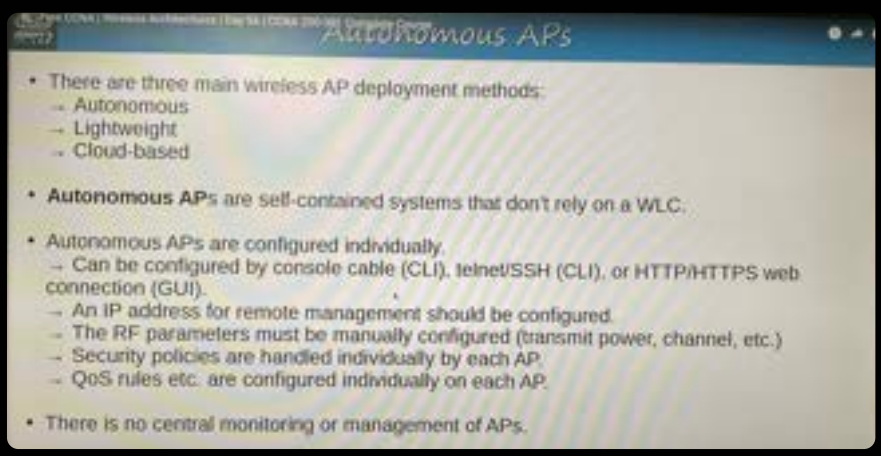
- 802.11 Lans are called WiFi

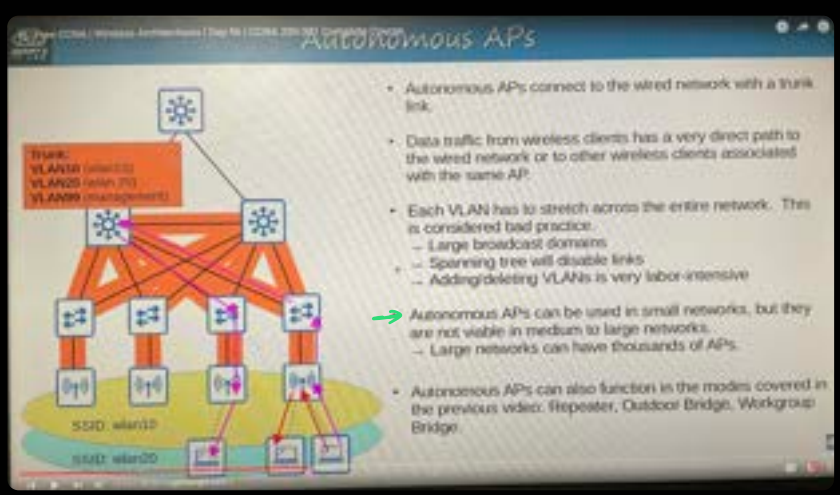


Day 56 — WLAN - 2


802.11 Messages Overview
2 bytes
2 bytes
6 bytes
6 bytes
6 bytes
2 bytes
6 bytes
2 bytes
4 bytes
variable size
4 bytes
Frame Control
Duration/ ID
Address 1
Address 2
Address 3
Sequence Control
Address 4
QoS Control
HT Control
Frame Body (Packet)
FCS
probe request
probe response
authentication request
authentication response
association request
association response
There are two ways a station can scan for a BSS:
- Active scanning: The station sends probe requests and listens for a probe response from an AP.
- Passive scanning: The station listens for beacon messages from an AP.
Beacon messages are sent periodically by APs to advertise the BSS.
There are three 802.11 message types:
Management
Control
Data


802.11 Message Types
There are three 802.11 message types:
Management: used to manage the BSS.
→ Beacon
→ Probe request, probe response
→ Authentication
→ Association request, association response
Control: Used to control access to the medium (radio frequency). Assists with delivery of management and data frames.
→ RTS (Request to Send)
→ CTS (Clear to Send)
→ ACK
Data: Used to send actual data packets.

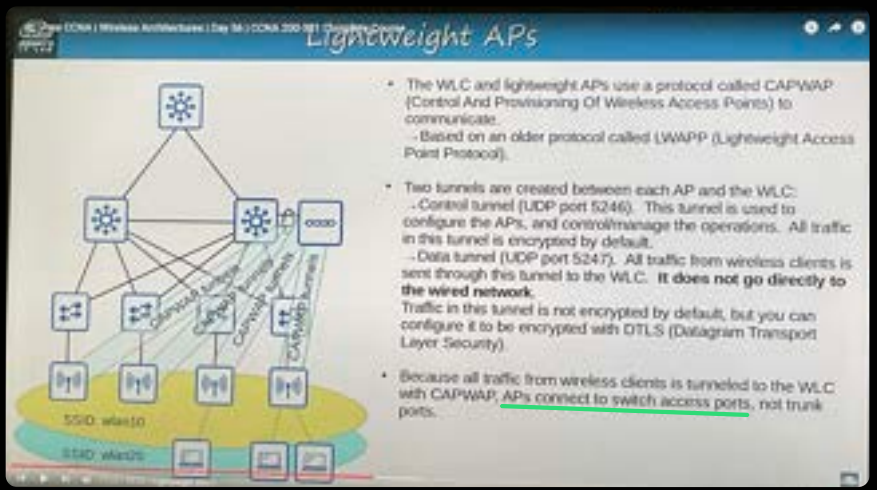

Autonomous APs
There are three main wireless AP deployment methods:
→ Autonomous
→ Lightweight
→ Cloud-based
Autonomous APs are self-contained systems that don't rely on a WLC.
Autonomous APs are configured individually.
→ Can be configured by console cable (CLI), telnet/SSH (CLI), or HTTP/HTTPS web connection (GUI).
→ An IP address for remote management should be configured.
→ The RF parameters must be manually configured (transmit power, channel, etc.)
→ Security policies are handled individually by each AP.
→ QoS rules etc. are configured individually on each AP.
There is no central monitoring or management of APs.

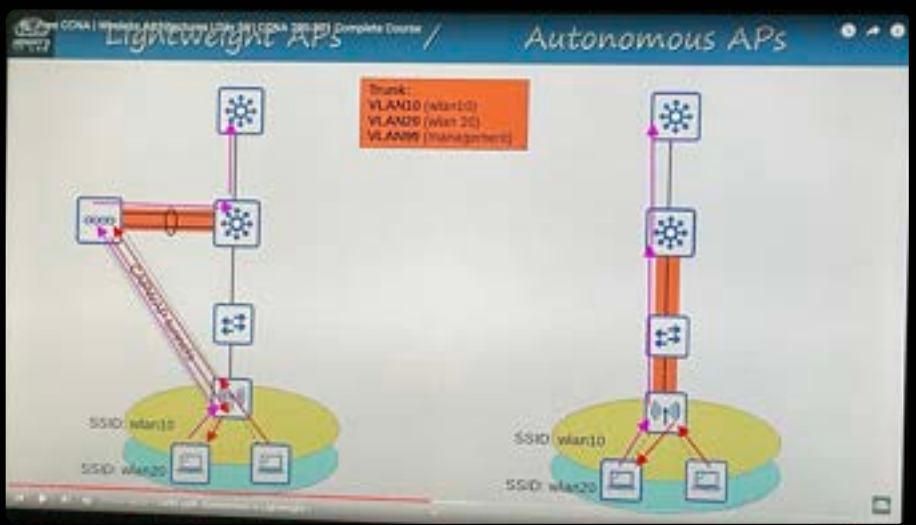

Autonomous APs
Trunk:
VLAN10
VLAN20
VLAN99 (management)
SSID: wlan10
SSID: wlan20
Autonomous APs connect to the wired network with a trunk link.
Data traffic from wireless clients has a very direct path to the wired network or to other wireless clients associated with the same AP.
Each VLAN has to stretch across the entire network. This is considered bad practice.
→ Large broadcast domains
→ Spanning tree will disable links
→ Adding/deleting VLANs is very labor-intensive
Autonomous APs can be used in small networks, but they are not viable in medium to large networks.
→ Large networks can have thousands of APs.
Autonomous APs can also function in the modes covered in the previous video: Repeater, Outdoor Bridge, Workgroup Bridge.

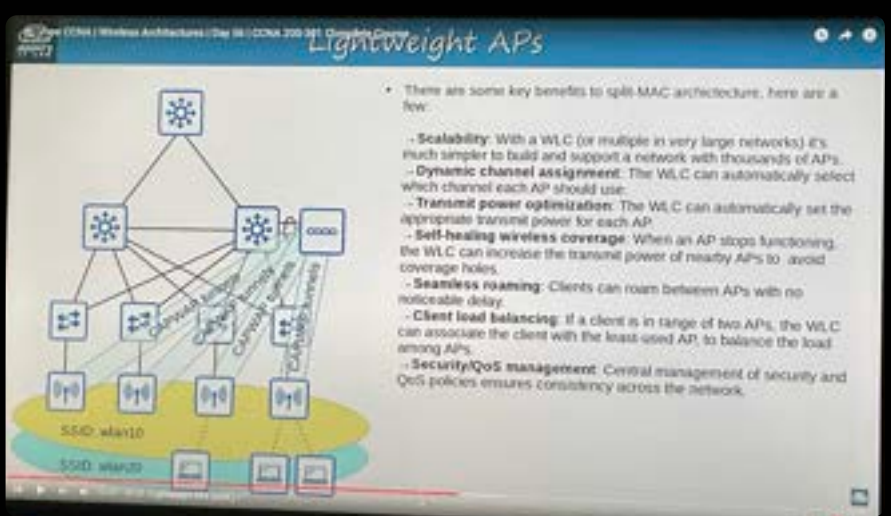
2. Lightweight APs

— control tunnel uses UDP port 5246

— Data tunnel uses UDP port 5247







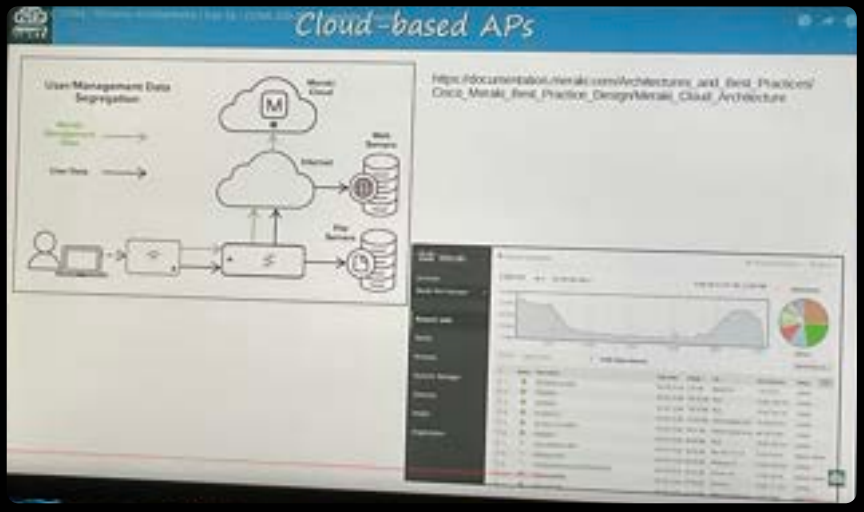
Lightweight APs

- Lightweight APs can be configured to operate in various modes:
  - **Local**: This is the default mode where the AP offers a BSS (more multiple BSSs) for clients to associate with.
  - **FlexConnect**: Like a lightweight AP in Local mode, it offers one or more BSSs for clients to associate with. However, FlexConnect allows the AP to locally switch traffic between the wired and wireless networks if the tunnels to the WLC go down.
  - **Sniffer**: The AP does not offer a BSS for clients. It is dedicated to capturing 802.11 frames and sending them to a device running software such as Wireshark.
  - **Monitor**: The AP does not offer a BSS for clients. It is dedicated to receiving 802.11 frames to detect rogue devices. If a client is found to be a rogue device, it can send de-authentication messages to disassociate them from their AP.
  - **Rogue Detector**: The AP does not even use its radio. It listens to traffic on the wired network only, but it receives a list of suspected rogue clients and AP MAC addresses from the WLC. By listening to ARP messages on the wired network and correlating it with the information it receives from the WLC, it can detect rogue devices.
  - **SE-Connect (Spectrum Expert Connect)**: The AP does not offer a BSS for clients. It is dedicated to RF spectrum analysis on all channels. It can send information to software such as Cisco Spectrum Expert on a PC to collect and analyze the data.
  - **Bridge/Mesh**: Like the autonomous AP's *Outdoor Bridge*, the lightweight AP can be a dedicated bridge between sites, for example over long distances. A mesh can be made between the access points.
  - **Flex plus Bridge**: Adds FlexConnect functionality to the Bridge/Mesh mode. Allows wireless access points to locally forward traffic even if connectivity to the WLC is lost.

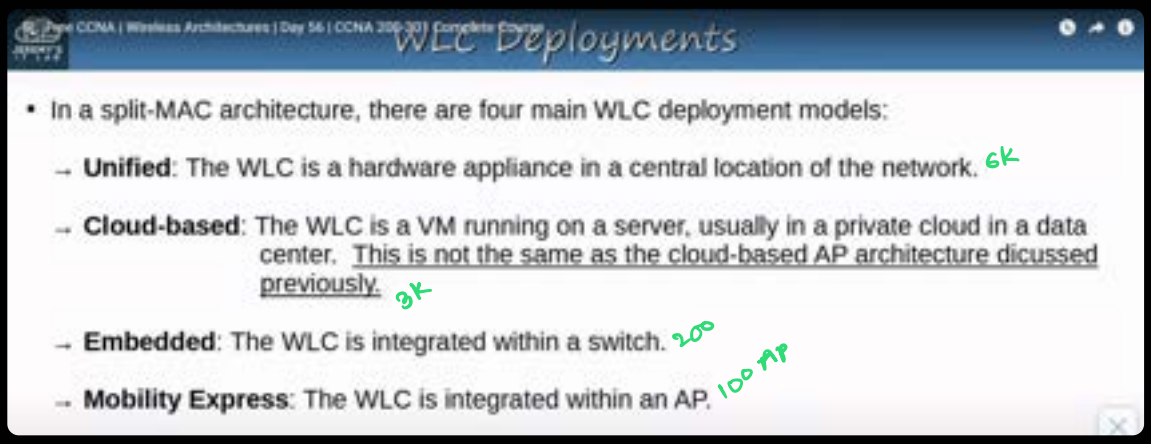
— 3. cloud based AP

Cloud-based APs

- **Cloud-Based AP** architecture is in between autonomous AP and split-MAC architecture.
  - Autonomous APs that are centrally managed in the cloud.
- Cisco Meraki is a popular cloud-based Wi-Fi solution.
- The Meraki dashboard can be used to configure APs, monitor the network, generate performance reports, etc.
  - Meraki also tells each AP which channel to use, what transmit power, etc.
- However, data traffic is not sent to the cloud. It is sent directly to the wired network like when using autonomous APs.



- WLC deployments



- Day 57 - WLAN security

- WLC only supports LAG it does not support PAgP or LACP.
so thats why command will be

(channel-if-range) # interface range F0/1 - 2
channel-group 1 mode on → LAG

Layer 2 Header - frame

PSDST

Preamble	SFD	Dest	Src	Type	FCS
7	1	6	6	2	4

→ lets the device know to start the frame sending
SFD → A unique pattern that marks the end of preamble

OSI model PDU