

* default-information originate

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

R1 # Shows ip protocols

```
show ip protocols

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

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 28 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip          RIP v2
  Default version control: send version 2, receive version 2
    Interface      Send   Recv   Triggered RIP  Key-chain
      GigabitEthernet0/0  2      2
      GigabitEthernet1/0  2      2
  Automatic network summarization is not in effect
  Maximum path: 4 }→ Amount of ECMP load balancing
  Routing for Networks:  Path's allowed
    10.0.0.0
    172.16.0.0
  Passive Interface(s): → To prevent RIP to send
    GigabitEthernet2/0   msg's every 60 sec on
  Routing Information Sources:   that int
    Gateway        Distance   Last Update
    10.0.12.2       120       00:00:21
    10.0.13.2       120       00:00:06
Distance: (default is 120)
```

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

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

• EIGRP – Enhanced Interior Routing protocol

```
EIGRP
```

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

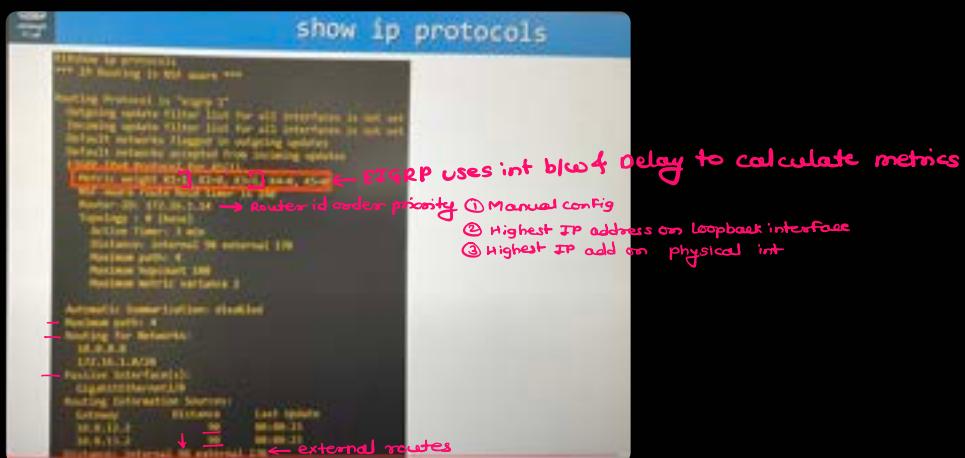
We can have RIP & EIGRP running at the same time .

Configuration of EIGRP

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 172.25.20.12. 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

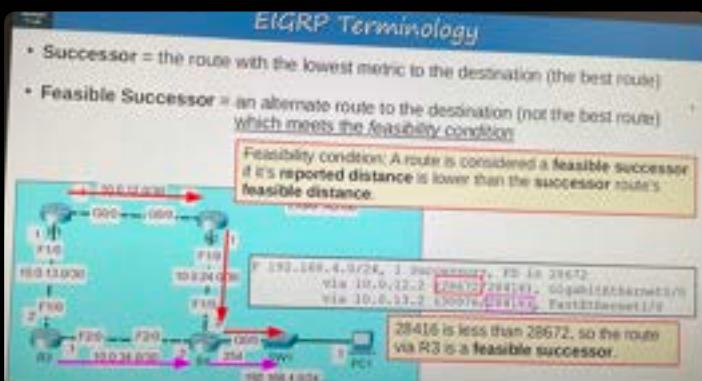
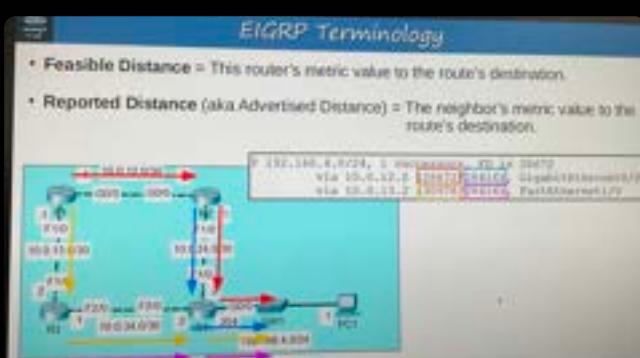
```

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

EIGRP Terminology

- Feasible Distance = This router's metric value to the route's destination.
- Reported Distance (aka Advertised Distance) = The neighbor's metric value to the route's destination.
- Successor = the route with the lowest metric to the destination (the best route)
- Feasible Successor = an alternate route to the destination (not the best route) which meets the feasibility condition

Feasibility condition: A route is considered a feasible successor if its reported distance is lower than the successor route's feasible distance.

OSPF — Link state routing

CCNA | OSPF Part 1 | Day 26 | CCNA 200-301 Complete Course

Link State Routing Protocols

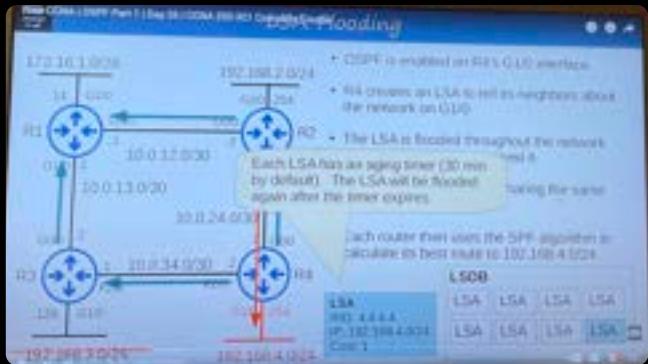
- When using a **link state** routing protocol, every router creates a 'connectivity map' of the network.
- To allow this, each router advertises information about its interfaces (connected networks) to its neighbors. These advertisements are passed along to other routers, until all routers in the network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

→ OSPF is also known as Dijkstra's Algo.

Three types

- ① OSPF
- ② OSPF v2 - IPv4
- ③ OSPFv3 - IPv6

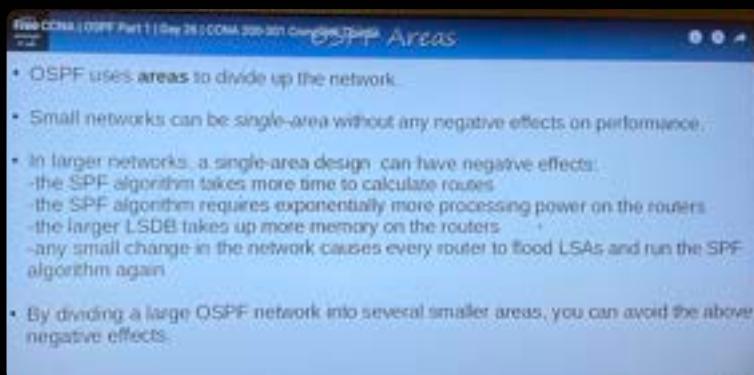
- Routers store information about the network in LSA (Link State Ads) which are organized in structure called LSDB (Link State Database)
- Routers will flood LSA's until all routers in the OSPF are develop the same map of the network.



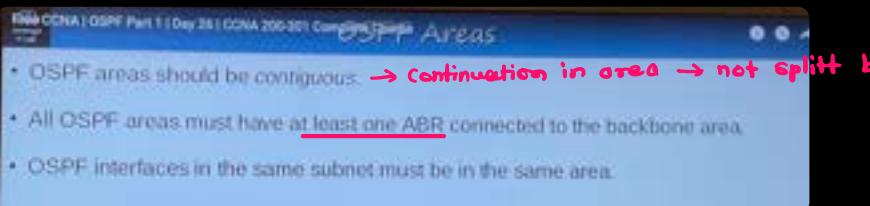
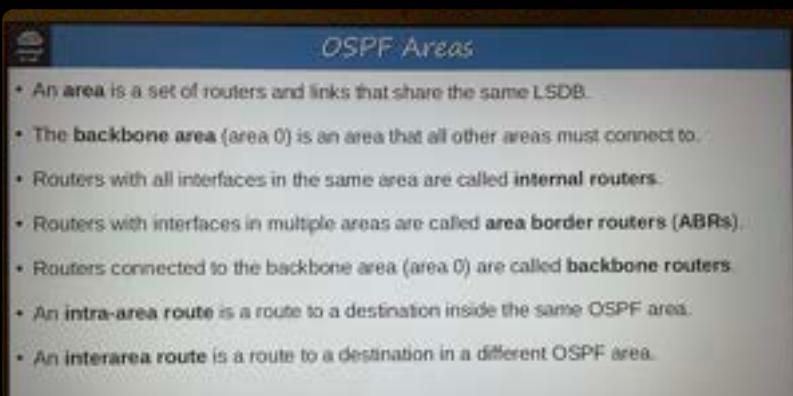
OSPF steps

- In OSPF, there are three main steps in the process of sharing LSAs and determining the best route to each destination in the network:
 - 1) Become neighbors with other routers connected to the same segment.
 - 2) Exchange LSAs with neighbor routers.
 - 3) Calculate the best routes to each destination, and insert them into the routing table.

• OSPF uses area to divide bigger network



OSPF areas

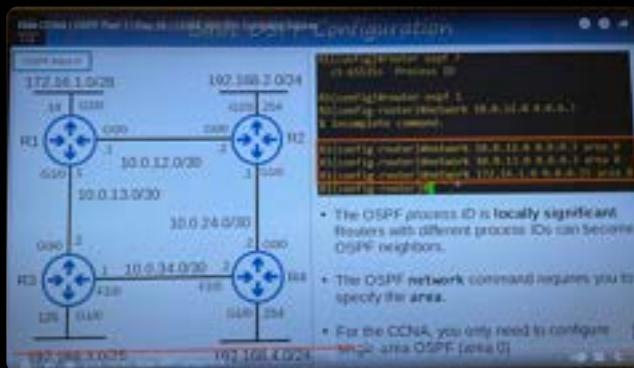


• Configuration of OSPF

R1(config) # router ospf 1

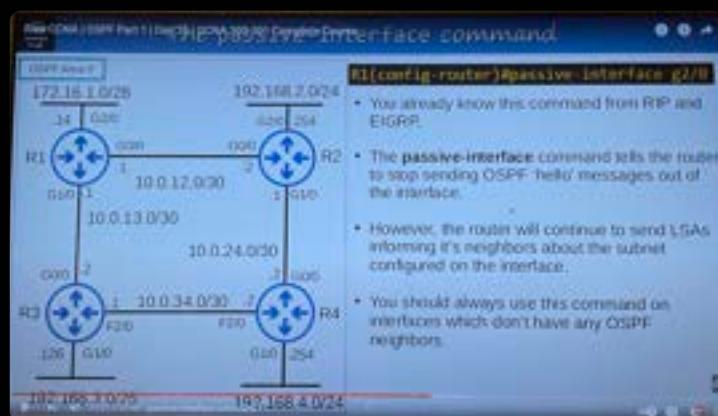
network ip wildcard area 0

Example →



passive-interface g2/0

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



To advertise in OSPF

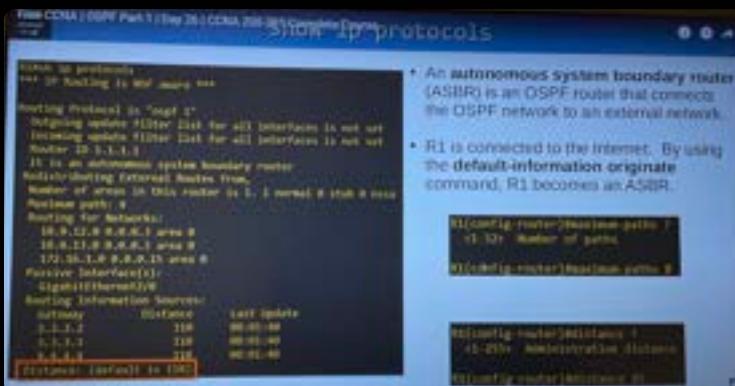
* To configure a default route →

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
L Autonomous system boundary router



QUIZ 4

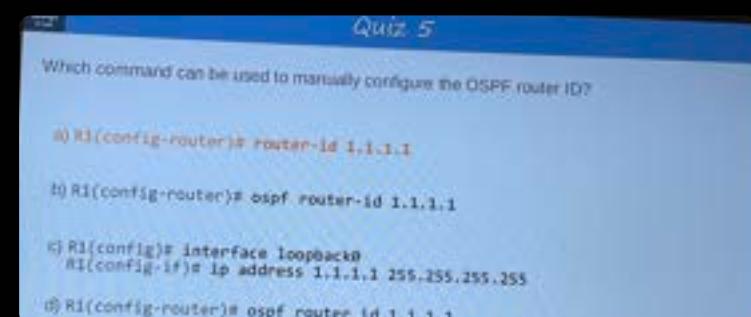
Which of the following commands will make R1 an OSPF ASBR?

- ```
a) R1(config-router)# network 10.0.0.0 0.0.0.255 area 0
 R1(config-router)# network 10.0.1.0 0.0.0.255 area 1

b) R1(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.1
 R1(config)# router ospf 1
 R1(config-router)# default-information originate

c) R1(config-router)# network 0.0.0.0 255.255.255.255 area 0

d) R1(config-router)# default-route originate
```

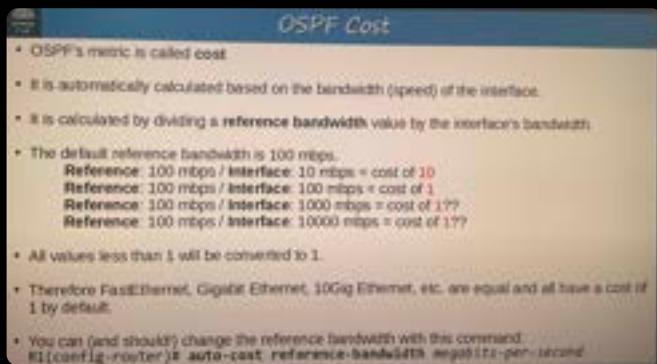


```
Show ip ospf database
show ip ospf neighbour
```

## — Day 27 - OSPF p2

- OSPF metrics called as cost
- It's 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

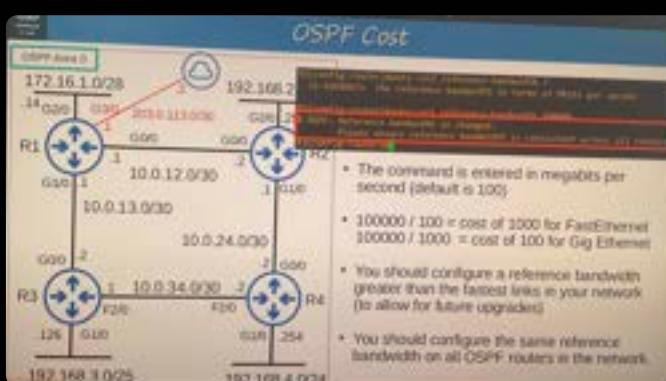
R3 # show ip ospf interface F 2/0

To change the ospf cost

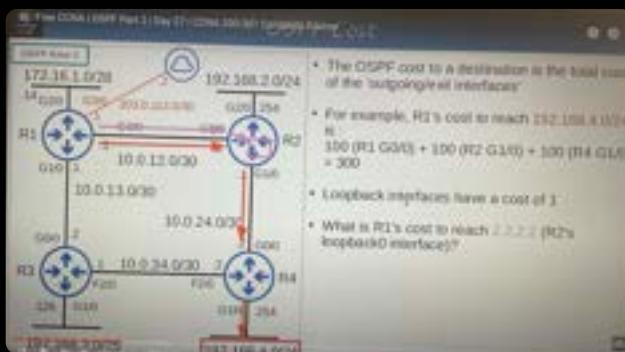
# auto-cost reference-bandwidth 100000  
so far fast Ethernet

$$100000 / 100 = \text{cost of 1000 for FastEthernet}$$

$$100000 / 1000 = \text{cost of 100 for GigEthernet}$$

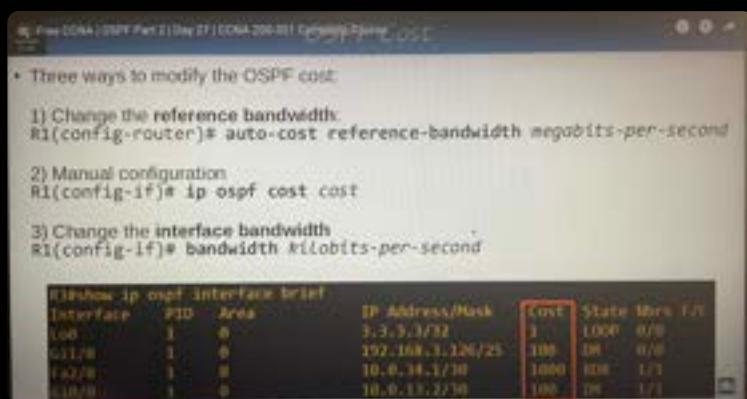
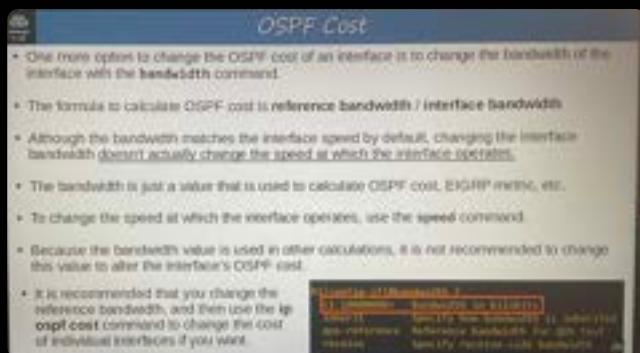


- Reference bandwidth has to be same on all ospf configured routers on net



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'

Hello messages are multicast to 224.0.0.5 Multicast add. of OSPF

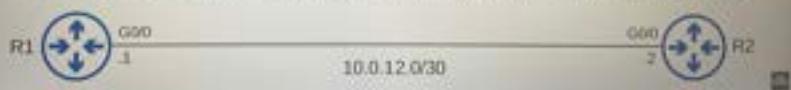
OSPF Multicast - 224.0.0.5

RIP Multicast - 224.0.0.9

EIGRP Multicast - 224.0.0.10

## OSPF Neighbors

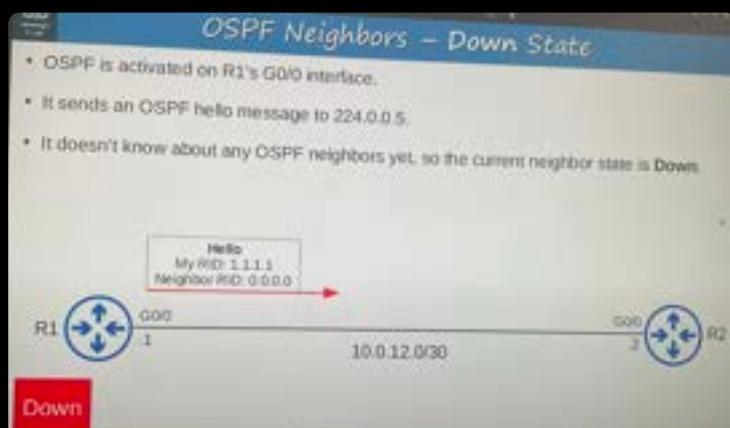
- Making sure that routers successfully become OSPF neighbors is the main task in configuring and troubleshooting OSPF.
- Once routers become neighbors, they automatically do the work of sharing network information, calculating routes, etc.
- When OSPF is activated on an interface, the router starts sending OSPF hello messages out of the interface at regular intervals (determined by the hello timer). These are used to introduce the router to potential OSPF neighbors.
- The default hello timer is 10 seconds on an Ethernet connection.
- Hello messages are multicast to 224.0.0.5 (multicast address for all OSPF routers).
- OSPF messages are encapsulated in an IP header, with a value of 89 in the Protocol field.



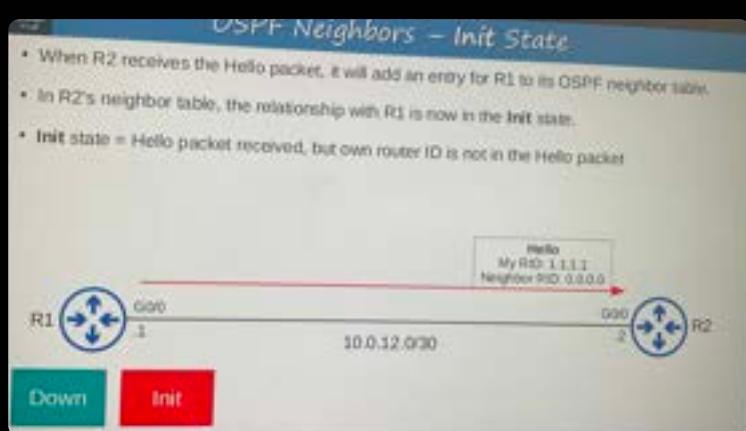
### Ospf neighbour steps

Once ospf is activated on one interface

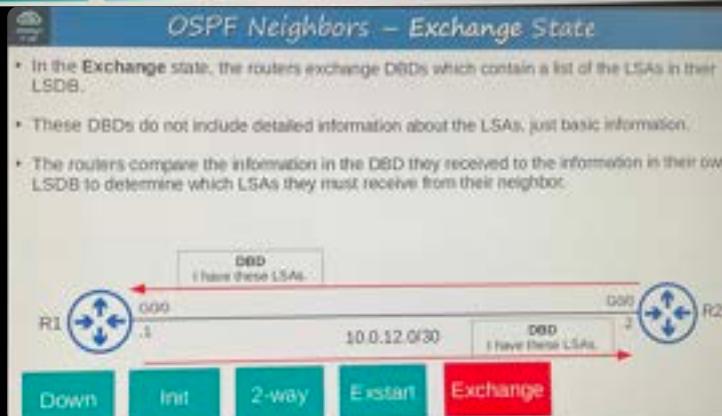
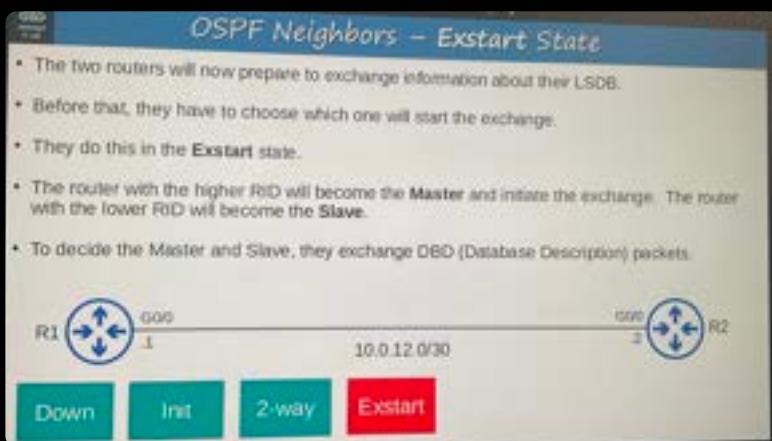
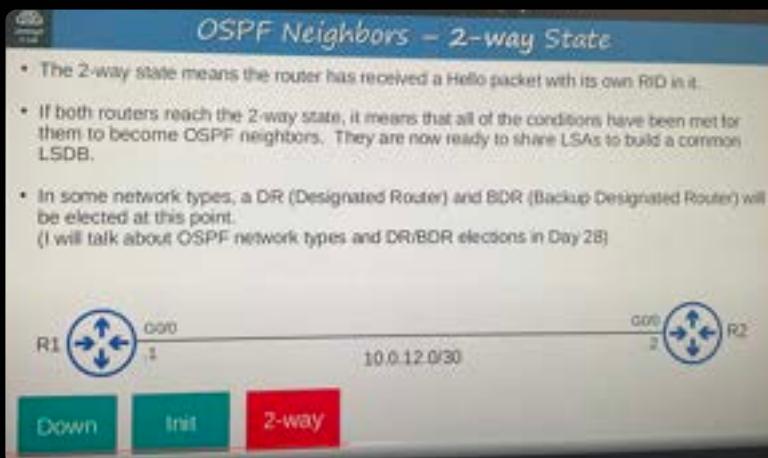
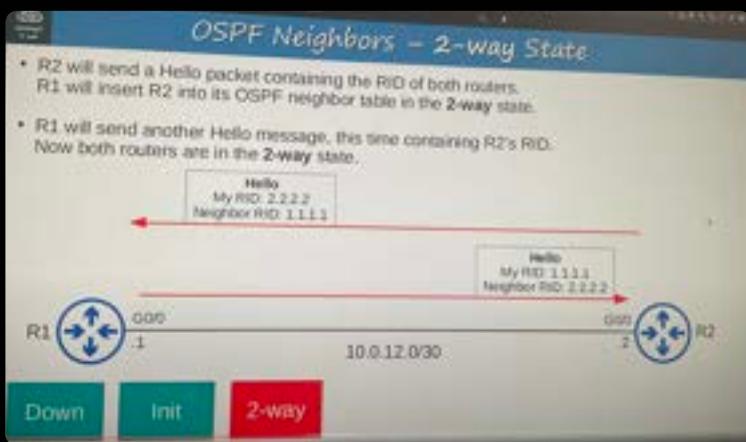
- ① OSPF hello message is sent  
current state - down

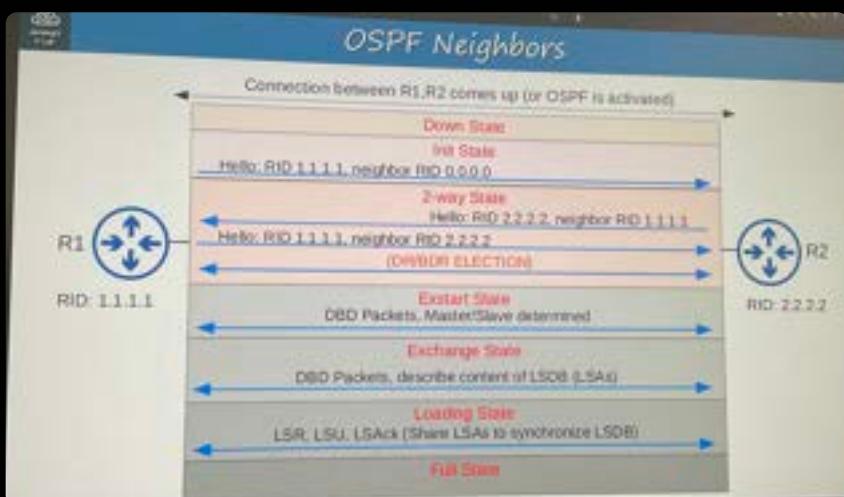
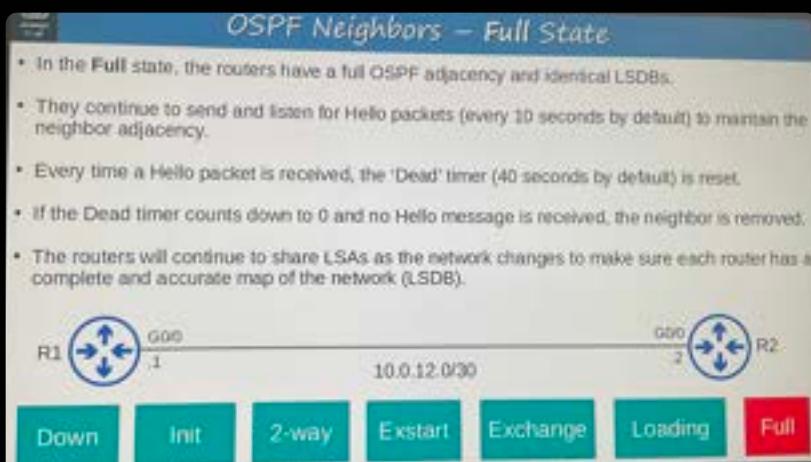
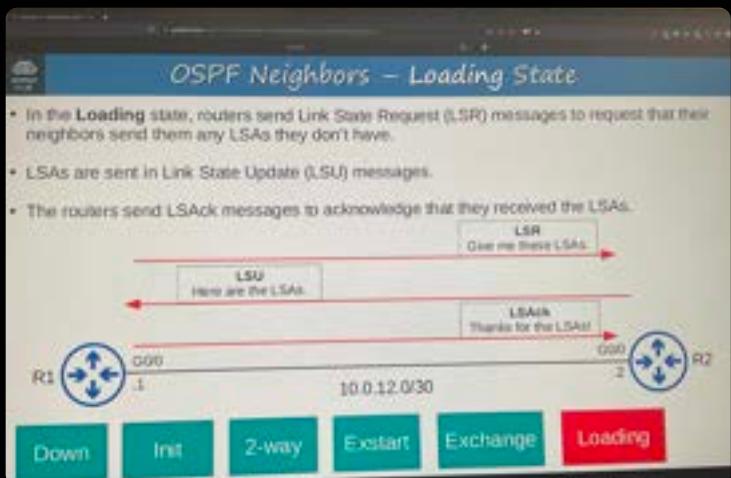


②

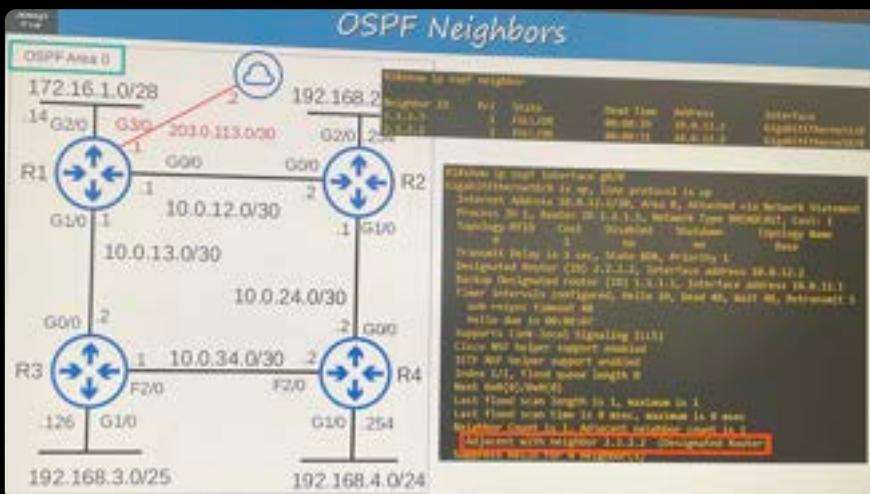


## ② 2-way state

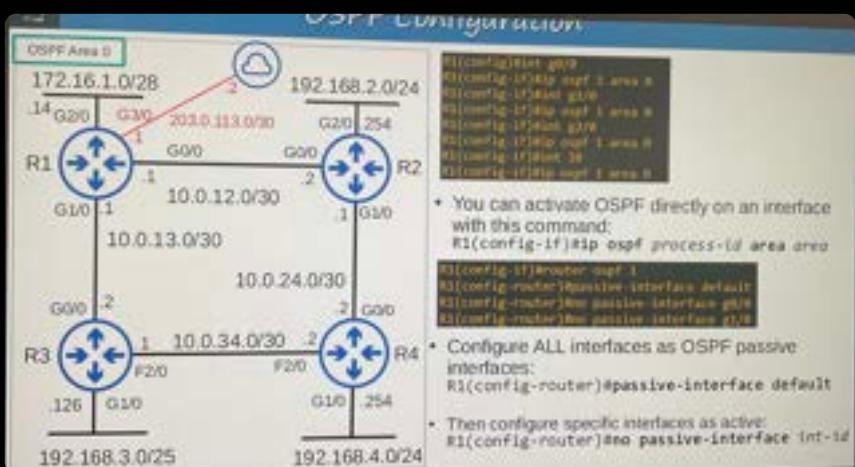




| Type | Name                               | Purpose                                                                                     |
|------|------------------------------------|---------------------------------------------------------------------------------------------|
| 1    | Hello                              | Neighbor discovery and maintenance.                                                         |
| 2    | Database Description (DBD)         | Summary of the LSDB of the router.<br>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.



## Things we covered

### OSPF metric (cost)

- Reference bandwidth / interface bandwidth = cost (values less than 1 are converted to 1)
- Default reference bandwidth = 100 mbps.
- Modify the reference bandwidth:  
R1(config-router)# auto-cost reference-bandwidth megabits-per-second
- Manually configure the cost of an interface:  
R1(config-if)# ip ospf cost cost
- Modify the interface bandwidth:  
R1(config-if)# bandwidth kilobits-per-second
- Total cost of outgoing interfaces = metric of the route

— Alternative way:

## Things we covered

### More OSPF Configuration

- Activate OSPF directly on an interface:  
R1(config-if)# ip ospf process-id area area-id
- Configure all interfaces as passive interfaces by default:  
R1(config-router)# passive-interface default

### OSPF neighbour states

- ① down
- ② init
- ③ 2-way
- ④ Exstart
- ⑤ Exchange
- ⑥ Loading
- ⑦ Full

- D
- I
- T
- E2
- L
- F

bordering  
Taste  
some  
extremely  
large  
fries

- default Hello/Dead timers on OSPF area

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

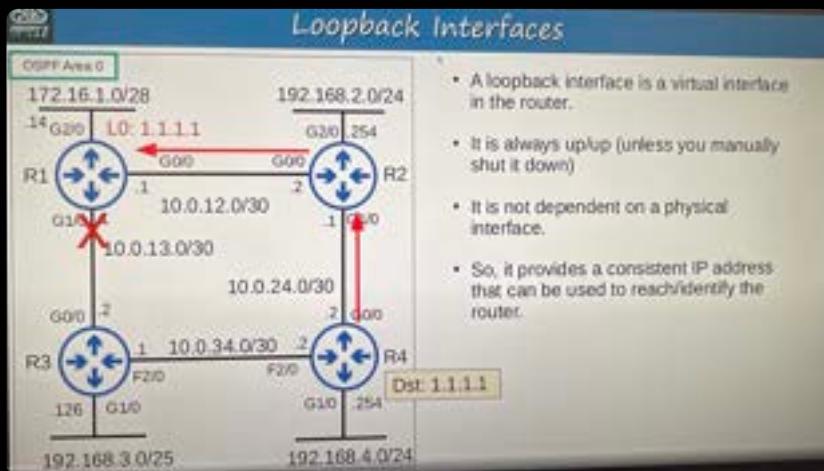
\* show ospf neighbours

\* All routers should have same reference bw configured on all routers under that area.

Every Cisco engine with core daily

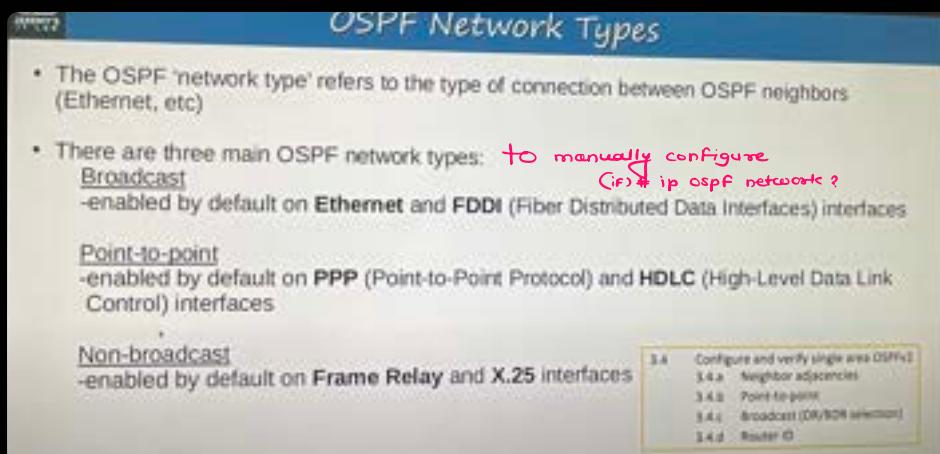
# show ip protocols → To see currently running protocols

## Day 28 - ospf p3



## OSPF network types

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

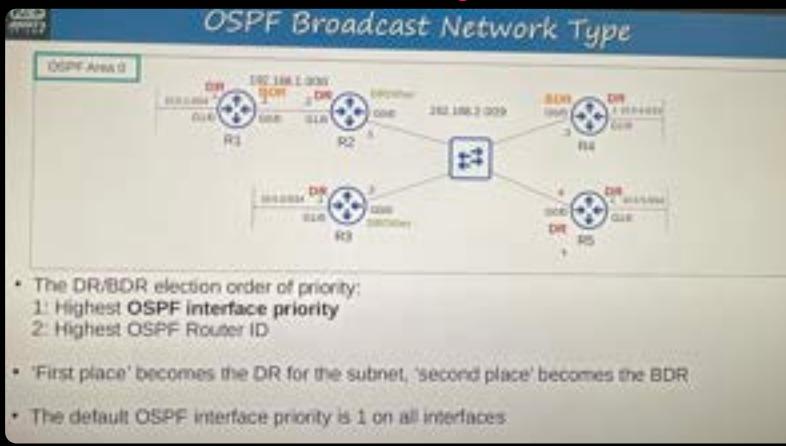


### • Election of DR/BDR

- 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

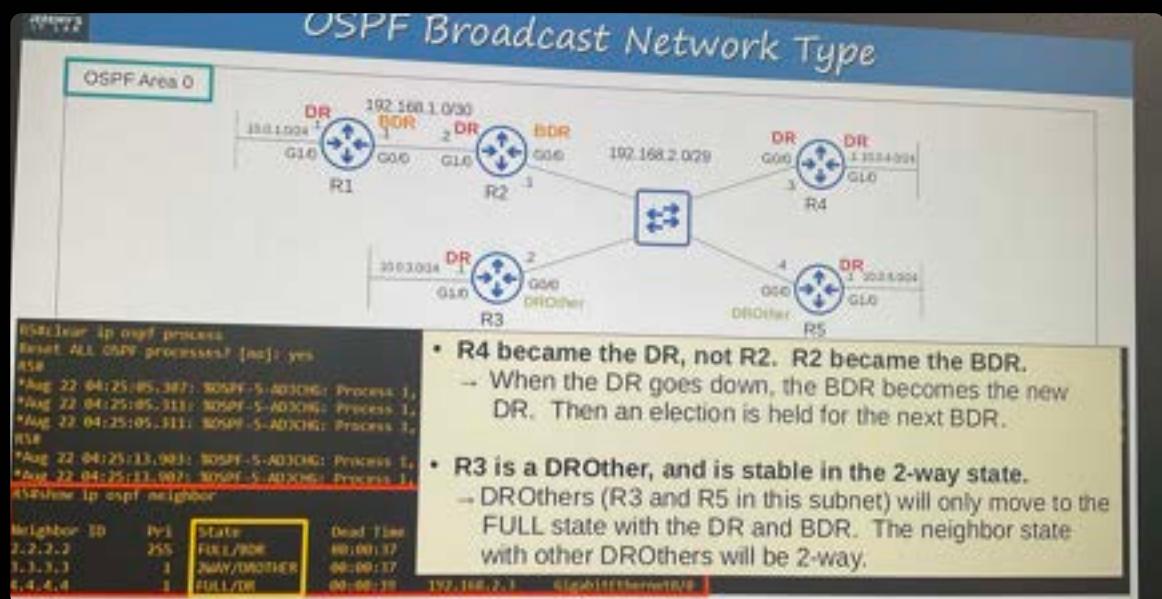


\*\*\* if you set the OSPF interface priority to 0, the router cannot be the DR/BDR for the subnet.

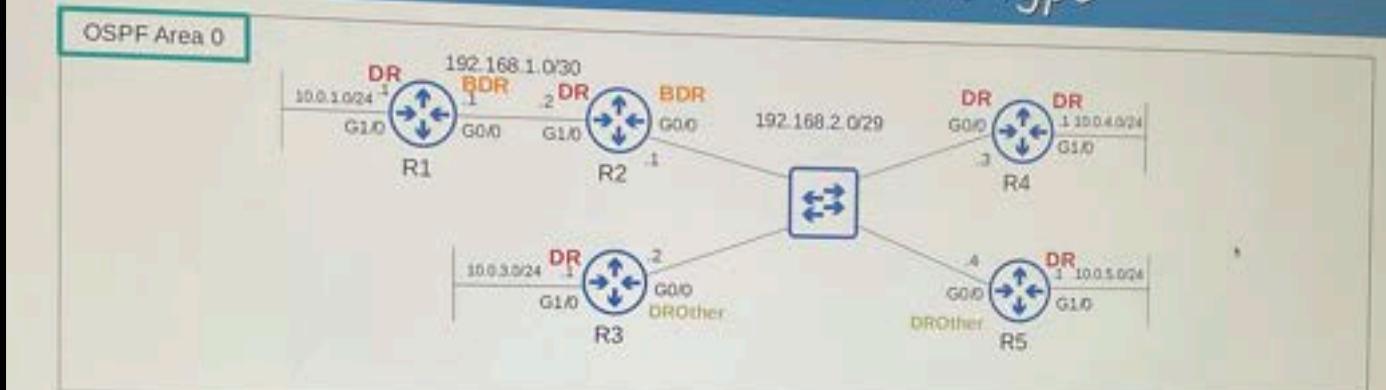
\*\*\* OSPF election for DR/BDR are non-preemptive. Once the DR/BDR are selected they will keep their role until OSPF is reset, the int fails/shut etc.

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 reset/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

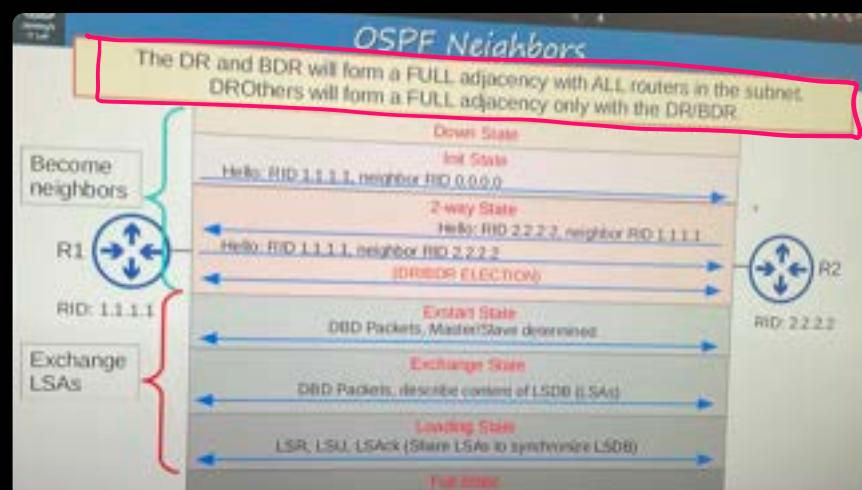


# OSPF Broadcast Network Type

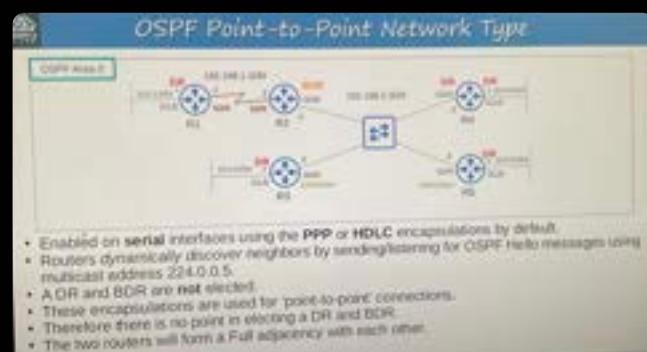


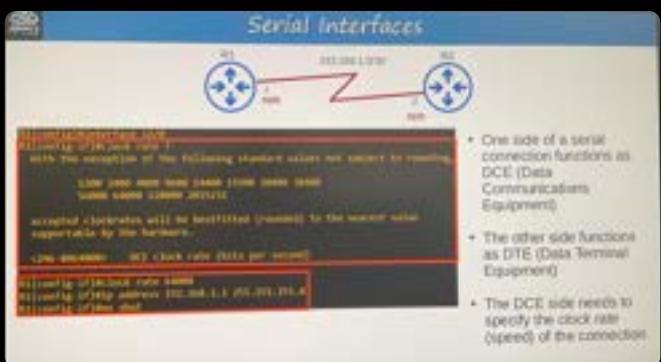
- In the broadcast network type, routers will only form a full OSPF adjacency with the DR and BDR of the segment.
- Therefore, routers only exchange LSAs with the DR and BDR. DROthers will not exchange LSAs with each other.
- All routers will still have the same LSDB, but this reduces the amount of LSAs flooding the network.

Messages to the DR/BDR are multicast using 224.0.0.6



② Point - to - point connection .





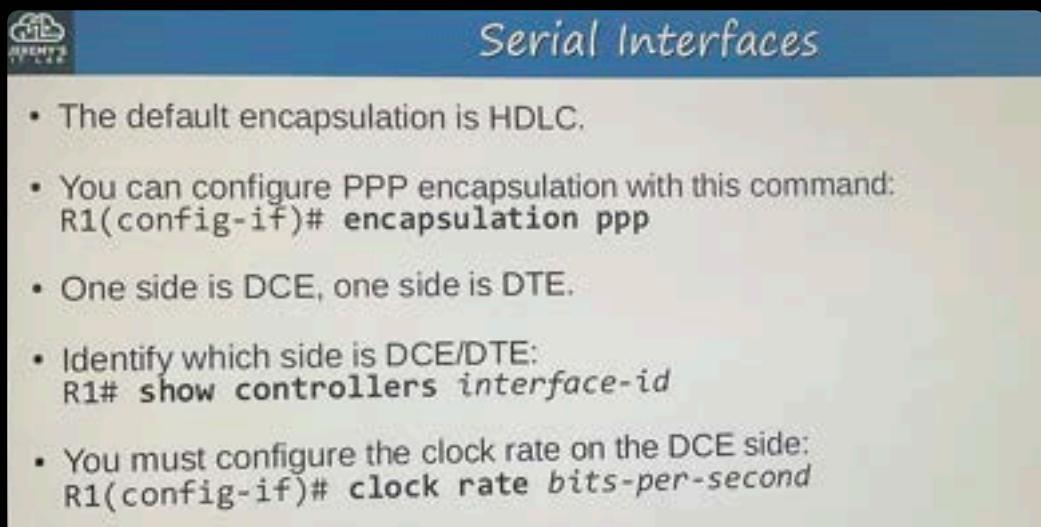
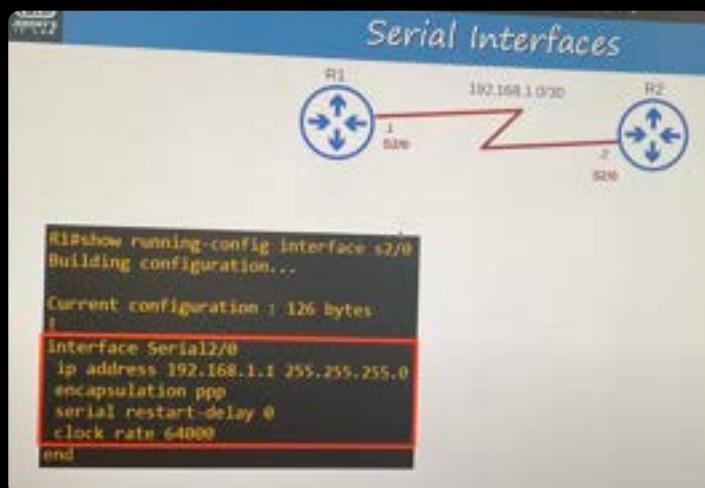
Ethernet uses speed command to config speed

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

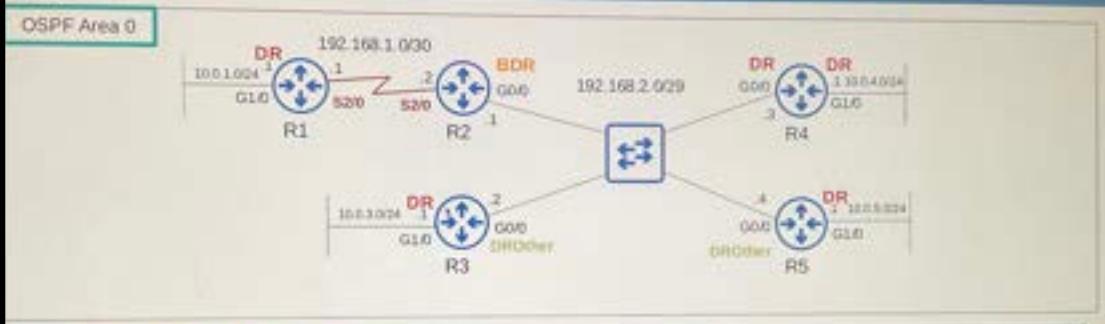
There are two encapsulations on the routers

- 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 Neighbor Requirements

- 1) Area number must match
  - 2) Interfaces must be in the same subnet
  - 3) OSPF process must not be **shutdown**
  - 4) OSPF Router IDs must be unique
  - 5) Hello and Dead timers must match
  - 6) Authentication settings must match
- 
- 7) IP MTU settings must match
  - 8) OSPF Network Type must match

Can become OSPF neighbors, but  
OSPF doesn't operate properly.

## Ospf LSA types

### OSPF LSA Types

- **Type 1 (Router LSA)**
  - Every OSPF router generates this type of LSA.
  - It identifies the router using its router ID.
  - It also lists networks attached to the router's OSPF-activated interfaces.
- **Type 2 (Network LSA)**
  - Generated by the DR of each 'multi-access' network (ie. the broadcast network type).
  - Lists the routers which are attached to the multi-access network.
- **Type 5 (AS-External LSA)**
  - Generated by ASBRs to describe routes to destinations outside of the AS (OSPF domain)

# 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 subnet 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)

**First Hop Redundancy Protocols**

- \* A virtual IP is configured on the two routers, and a virtual MAC is generated for the virtual IP (each FHRP uses a different format for the virtual MAC)
- \* An active router and a standby router are elected. (different FHRPs use different terms)
- \* End hosts in the network are configured to use the virtual IP as their default gateway.
- \* The active router replies to ARP requests using the virtual MAC address, so traffic destined for other networks will be sent to it.
- \* If the active router fails, the standby becomes the next active router. The new active router will send gratuitous ARP messages so that switches will update their MAC address tables. It now functions as the default gateway.
- \* If the old active router comes back online, by default it won't take back its role as the active router. It will become the standby router.

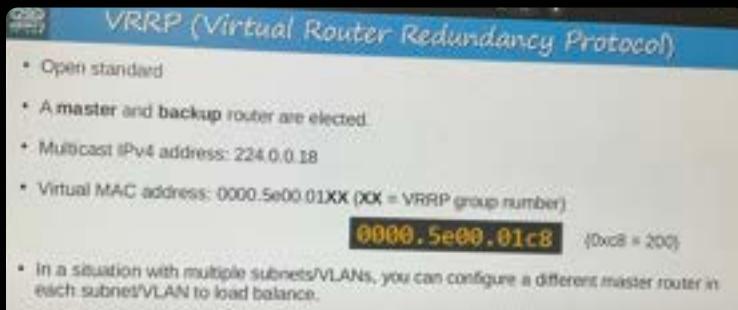
### HSRP - (Hot standby Router protocol)

**HSRP (Hot Standby Router Protocol)**

- \* Cisco proprietary.
- \* An active and standby router are elected.
- \* There are two versions: version 1 and version 2. Version 2 adds IPv6 support and increases the number of groups that can be configured.
- \* Multicast IPv4 address: v1 = 224.0.0.2      v2 = 224.0.0.102  
**0000.0c07.ac01**
- \* Virtual MAC address: v1 = 0000.0007.ac0X (0X = HSRP group number)  
v2 = 0000.0001.0004 (0004 = HSRP group number)  
**0000.0c9F.F001**
- \* In a situation with multiple subnets/VLANs, you can configure a different active router in each subnet/VLAN to load balance.

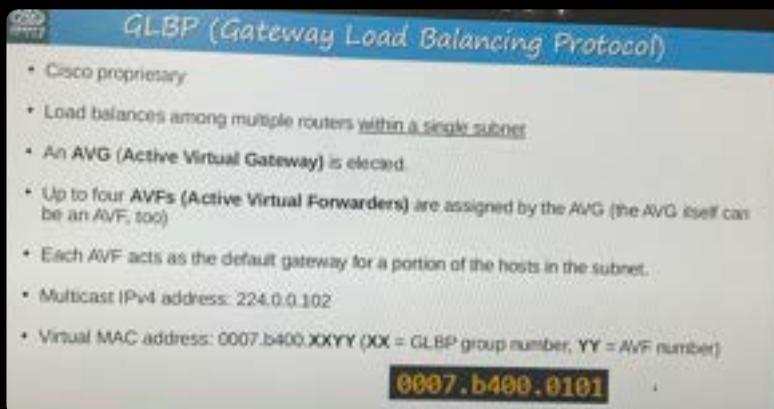
## ② Virtual router redundancy protocol (VRRP)

- open standard



## ③ GLBP -

Cisco proprietary



| Comparing FHRPs |                |                                  |                                                |                    |
|-----------------|----------------|----------------------------------|------------------------------------------------|--------------------|
| FHRP            | Terminology    | Multicast IP                     | Virtual MAC                                    | Cisco proprietary? |
| HSRP            | Active/Standby | v1: 224.0.0.2<br>v2: 224.0.0.102 | v1:<br>0000.0c07.acXX<br>v2:<br>0000.0c9f.DXXX | 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 g0/0

\* standby

if range (0-255) then that vi

To change to v2

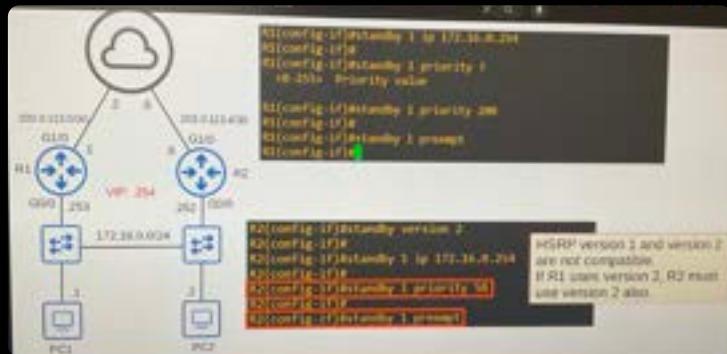
R1 (config-if) # standby version 2

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

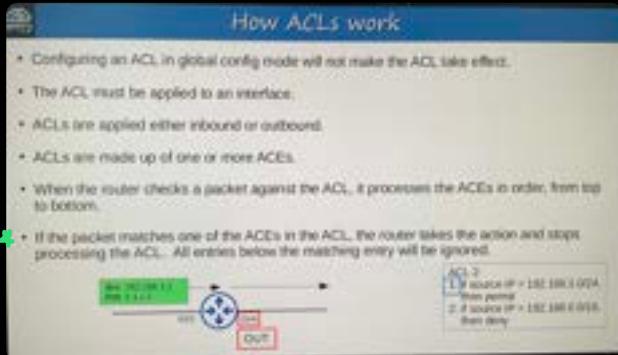


R2# show standby

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 has 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 Extended 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

Standard Numbered ACLs

- Standard ACLs match traffic based only on the source IP address of the packet.
- Numbered ACLs are identified with a number (ie. ACL 1, ACL 2, etc)
- Different types of ACLs have a different range of numbers that can be used.
  - Standard ACLs can use 1-99 and 1300-1999

| Range   | Description                                  |
|---------|----------------------------------------------|
| 1-99    | Standard IP                                  |
| 100-199 | Extended IP                                  |
| 200-269 | Standard TCP/UDP                             |
| 270-399 | Extended TCP/UDP                             |
| 400-499 | IP Precedence                                |
| 500-599 | Priority Queueing (Priority-based)           |
| 600-699 | Priority Queueing (Service-based)            |
| 700-799 | Intermedium Priority Queuing (IP Precedence) |
| 800-899 | DiffServ                                     |
| 900-999 | Per Device Accounting (Protocol-based)       |

Standard Numbered ACLs

- Standard ACLs match traffic based only on the source IP address of the packet.
- Numbered ACLs are identified with a number (ie. ACL 1, ACL 2, etc)
- Different types of ACLs have a different range of numbers that can be used.
  - Standard ACLs can use 1-99 and 1300-1999.
- The basic command to configure a standard numbered ACL is:  
R1(config)# access-list number {deny | permit} ip wildcard-mask

```
R1(config)# access-list 1 deny 1.1.1.1 0.0.0.0
R1(config)# access-list 1 deny 1.1.1.1
R1(config)# access-list 1 deny host 1.1.1.1
R1(config)# access-list 1 permit any
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)# access-list 1 remark # BLOCK BOB FROM ACCOUNTING #
```

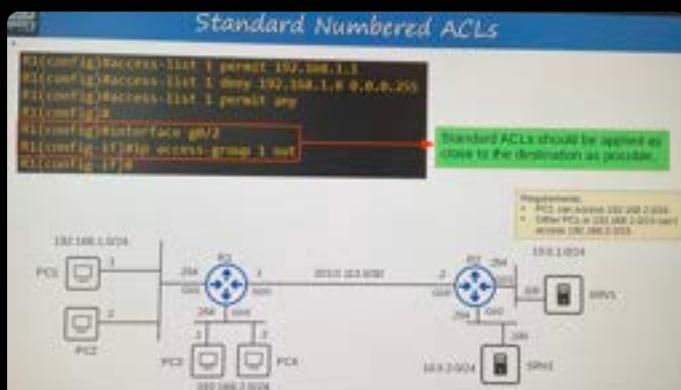
(config) # do show access-lists

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

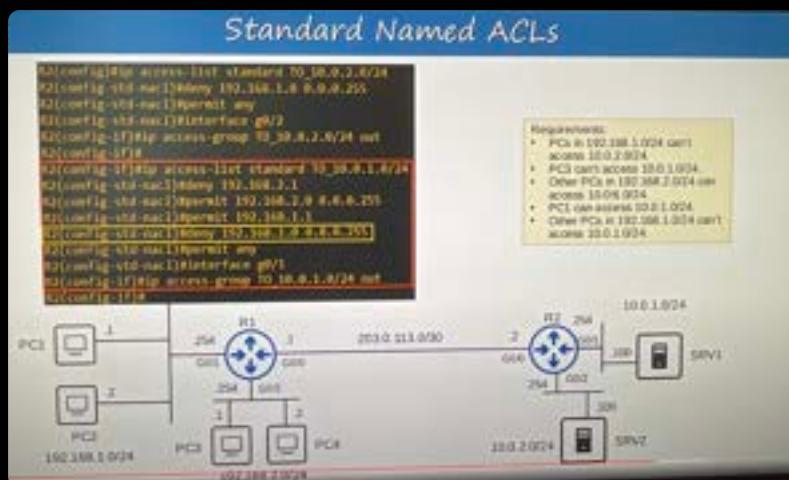
Standard Named ACLs

- Standard ACLs match traffic based only on the source IP address of the packet.
- Named ACLs are identified with a name (e.g. BLOCK\_BOB)
- Standard named ACLs are configured by entering "standard named ACL config mode", and then configuring each entry within that config mode.  
R1(config)# ip access-list standard BLOCK\_BOB  
R1(config-std-nacl)#5 deny 1.1.1.1  
R1(config-std-nacl)#10 permit any  
R1(config-std-nacl) #remark as CONFIGURED NOV 21 2020 as  
R1(config-std-nacl) #interface g0/0  
R1(config-if)#ip access-group BLOCK\_BOB in

\* show running-config | section access-list

① ip access-list standard Block-Bob  
✓  
    deny 192.168.1.0 0.0.0.255  
    perm 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 g0/1
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

\_\_\_\_\_ X \_\_\_\_\_ X \_\_\_\_\_

Access-list 1 permit 172.16.1.1

Access-list 1 permit 172.16.2.1

Access-list deny any

```
int g0/0
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 command

ip access-list standard ?  
named  
number — 1-99 100-199

To edit the entry

Advantages of named ACL config mode

```
R1(config)#do show access-lists
Standard IP access list 1
 10 deny 192.168.1.1
 20 deny 192.168.1.2
 30 deny 192.168.3.0, wildcard bits 0.0.0.255
 40 permit any
R1(config)#do show running-config | section access-list
access-list 1 deny 192.168.1.1
access-list 1 deny 192.168.1.2
access-list 1 deny 192.168.3.0 0.0.0.255
access-list 1 permit any
R1(config)#no access-list 1 deny 192.168.3.0 0.0.0.255 ←
R1(config)#do show access-lists
R1(config)#do show running-config | section access-list
R1(config)#
When configuring/editing numbered ACLs from global config mode,
you can't delete individual entries, you can only delete the entire-ACL!
```

This will delete the complete ACL

To only delete specific entry you can use  
no sequence-number  
→ no 10

Advantages of named ACL config mode

- \* You can easily delete individual entries in the ACL with no sequence-number.
- \* You can insert new entries in between other entries by specifying the sequence number.

```
R1(config-std-nacl)#do show access-lists
Standard IP access list 1
 10 deny 192.168.1.1
 20 deny 192.168.1.2
 40 permit any
R1(config-std-nacl)#
R1(config-std-nacl)830 deny 192.168.2.0 0.0.0.255
R1(config-std-nacl)#
R1(config-std-nacl)#do show access-lists
Standard IP access list 1
 10 deny 192.168.1.1
 20 deny 192.168.1.2
 30 deny 192.168.2.0, wildcard bits 0.0.0.255
 40 permit any
R1(config-std-nacl)#
R1(config-std-nacl)#do show running-config | section access-list
access-list 1 deny 192.168.1.1
access-list 1 deny 192.168.1.2
access-list 1 deny 192.168.2.0 0.0.0.255
access-list 1 permit any
```

## Resequencing ACLs

Resequencing ACLs

- There is a resequencing function that helps edit ACLs.
- The command is `ip access-list resequence acl-id starting-seq-num increment`

```
R1(config)# do show access-lists
Standard IP access list 1
 1 deny 192.168.1.1
 3 deny 192.168.3.1
 2 deny 192.168.2.1
 4 deny 192.168.4.1
 5 permit any
R1(config)#
R1(config)# ip access-list resequence 1 10 10
R1(config)#
R1(config)# do show access-lists
Standard IP access list 1
 10 deny 192.168.1.1
 20 deny 192.168.3.1
 30 deny 192.168.2.1
 40 deny 192.168.4.1
 50 permit any
```

Change the sequence number of the first entry to 10.  
Add 10 for every entry after that.

## Extended ACL

Extended ACLs

- Extended ACLs function mostly the same as standard ACLs.
- They can be numbered or named, just like standard ACLs.  
→ Numbered ACLs use the following ranges: 100 – 199, 2000 – 2699
- They are processed from top to bottom, just like standard ACLs.
- However, they can match traffic based on more parameters, so they are more precise (and more complex) than standard ACLs.
- We will focus on matching based on these main parameters: Layer 4 protocol/port, source address, and destination address.

```
R1(config)# access-list number {permit | deny} protocol src-ip dest-ip
R1(config)# ip access-list extended {name | number}
R1(config-ext-nacl)# [seq-num] {permit | deny} protocol src-ip dest-ip
```

Extended ACL has a granular control and complex

different IP protocol numbers

1: ICMP

6: TCP

17: UDP

88: EIGRP

89: OSPF

R3(config)#ip access-list extended EXAMPLE  
R3(config-ext-nacl)#deny ?  
cbr-255> An IP protocol number  
ahp Authentication Header Protocol  
eigrp Cisco's EIGRP routing protocol  
esp Encapsulation Security Payload  
gre Cisco's GRE tunneling  
icmp Internet Control Message Protocol  
igmp Internet Gateway Message Protocol  
ip Any Internet Protocol  
ipinip IP in IP tunneling  
nds KAME NOS compatible IP over IP tunneling  
object-group Service object group  
ospf OSPF routing protocol  
pvp Payload Compression Protocol  
pim Protocol Independent Multicast  
sctp Stream Control Transmission Protocol  
tcp Transmission Control Protocol  
udp User Datagram Protocol

```
#config-ext-mac]#mkey ip 1
A,B,C,D Source address
any Any source host
host A single source host
object-group Source endpoint object group

#config-ext-mac]#mkey ip any 1
A,B,C,D Destination address
any Any destination host
lt Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
gt Match only packets not on a given port number
object-group Destination network object group
range Match only packets in the range of port numbers

#config-ext-mac]#mkey ip any 18.0.0.1
A,B,C,D Destination port will always be 18

#config-ext-mac]#mkey ip 1
#config-ext-mac]#
```

## 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

| Extended ACL entry practice (1)                                   |                                                                     |
|-------------------------------------------------------------------|---------------------------------------------------------------------|
| 1. Allow all traffic                                              | R1(config-ext-nacl)#permit ip any any                               |
| 2. Prevent 10.0.0.0/16 from sending UDP traffic to 192.168.1.1/32 | R1(config-ext-nacl)#deny udp 10.0.0.0 0.0.255.255 host 192.168.1.1  |
| 3. Prevent 172.16.1.1/32 from pinging hosts in 192.168.0.0/24     | R1(config-ext-nacl)#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)#d deny tcp src-ip eq src-port-num dest-ip eq dst-port-num
gt
lt
neq
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              | UDP                |
|------------------|--------------------|
| FTP data (20)    | DHCP server (67)   |
| FTP control (21) | DHCP client (68)   |
| SSH (22)         | TFTP (69)          |
| Telnet (23)      | SNMP agent (161)   |
| SMTPT (25)       | SNMP manager (162) |
| HTTP (80)        | Syslog (514)       |
| POP3 (110)       | TCP & UDP          |
| HTTPS (443)      | DNS (53)           |

**Matching the TCP/UDP port numbers**

```
R1(config-ext-nacl)#d 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 !

## Day 30 - TCP / UDP

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

AZURE DATA STUDIO (SQL SERVER) - Complete Issues (TCP/IP Protocol)

- TCP is connection-oriented.
  - Before actually sending data to the destination host, the two hosts communicate to establish a connection. Once the connection is established, the data exchange begins.
- TCP provides reliable communication.
  - The destination host must acknowledge that it received each TCP segment.
  - If a segment isn't acknowledged, it is sent again.
- TCP provides sequencing.
  - Sequence numbers in the TCP header allow destination hosts to put segments in the correct order even if they arrive out of order.
- TCP provides flow control.
  - The destination host can tell the source host to increase/decrease the rate that data is sent.

TCP three way handshake →



four way Handshake to terminate session



AZURE DATA STUDIO (SQL SERVER) - Complete Issues (TCP/IP Protocol)

- TCP is connection-oriented.
  - Before actually sending data to the destination host, the two hosts communicate to establish a connection. Once the connection is established, the data exchange begins.
- TCP provides reliable communication.
  - The destination host must acknowledge that it received each TCP segment.
  - If a segment isn't acknowledged, it is sent again.
- TCP provides sequencing.
  - Sequence numbers in the TCP header allow destination hosts to put segments in the correct order even if they arrive out of order.
- TCP provides flow control.
  - The destination host can tell the source host to increase/decrease the rate that data is sent.

## Port Numbers

### 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)

### Comparing TCP & UDP

| TCP                                    | UDP                             |
|----------------------------------------|---------------------------------|
| Connection-oriented                    | Connectionless                  |
| Reliable                               | Unreliable                      |
| Sequencing                             | No sequencing                   |
| Flow control                           | No flow control                 |
| Used for downloads, file sharing, etc. | Used for VoIP, live video, etc. |

## Day 31 - IPv6

To enable IPv6 on the router use command

(config) # IPv6 unicast-routing

## Day 32 - EUI

Extended Unique Identifier

### Configuring IPv6 addresses (EUI-64)



- EUI stands for Extended Unique Identifier
- (Modified) EUI-64 is a method of converting a MAC address (48 bits) into a 64-bit interface identifier.
- This interface identifier can then become the 'host portion' of a /64 IPv6 address.
- How to convert the MAC address:
  1. Divide the MAC address in half  
`1234 5678 90AB - 1234 56 | 78 90AB`
  2. Insert FFFE in the middle  
`1234 56FF FE78 90AB`
  3. Invert the 7th bit  
`1234 56FF FE78 90AB - 1234 56FF FE78 90AB`

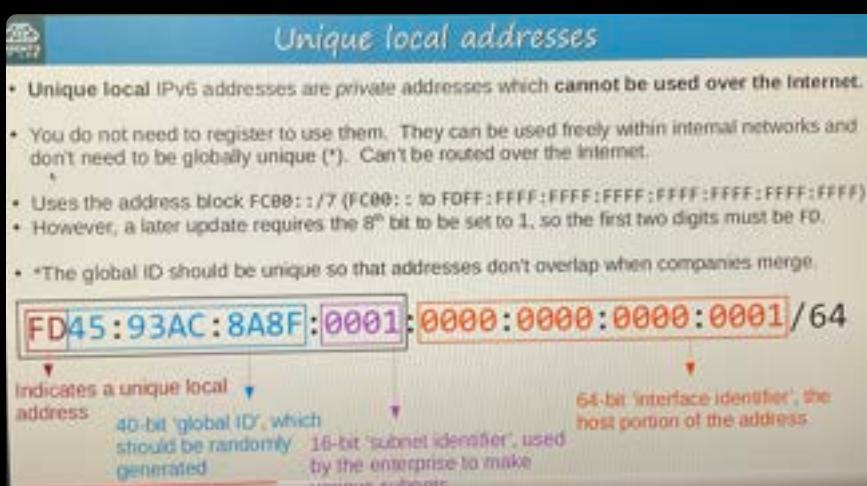
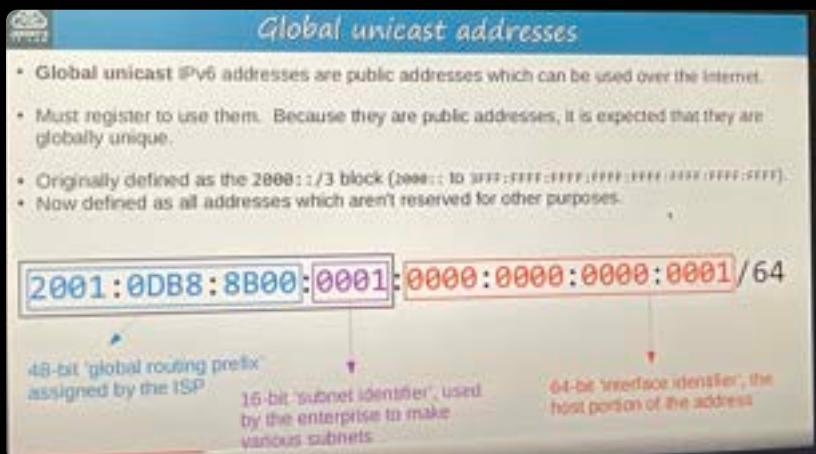
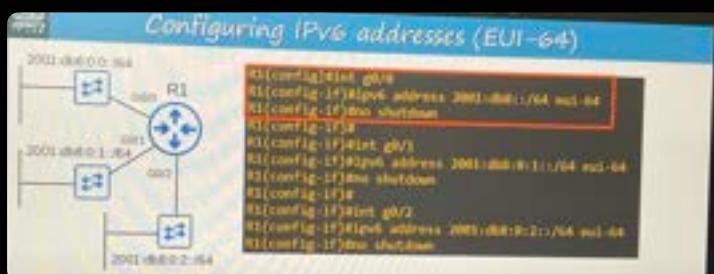
Convert following Mac address to EUI identified.

① 782B CBAC 0867

7~~8~~2BCBFF FE0867  
7th bit

1000  
↓  
1  
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.

## Multicast address scopes



## Anycast Addresses ~

### Anycast addresses

- Anycast is a new feature of IPv6.
- Anycast is 'one-to-one-of-many'.
- Multiple routers are configured with the same IPv6 address.
  - They use a routing protocol to advertise the address.
  - When hosts send packets to that destination address, routers will forward it to the nearest router configured with that IP address (based on routing metric).
- There is no specific address range for anycast addresses. Use a regular unicast address (global unicast, unique local) and specify it as an anycast address:  
R1(config-if)# ipv6 address 2001:db8:1:1::99/128 anycast



## 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 002A.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:B1
- b) 2001:db8:0:1:C2A:4FFF:FEA3:B1
- c) 2001:db8:0:1:0F2A:4FFF:FFA3:B1
- d) 2001:db8:0:1:F2A:4FFF:FEA3:B1

## 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

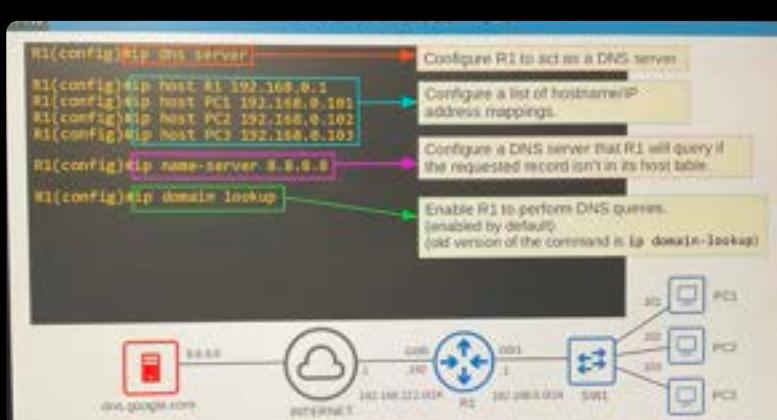
Day 38 - DNS

- ① ifconfig / displaydns
- ② ifconfig / 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

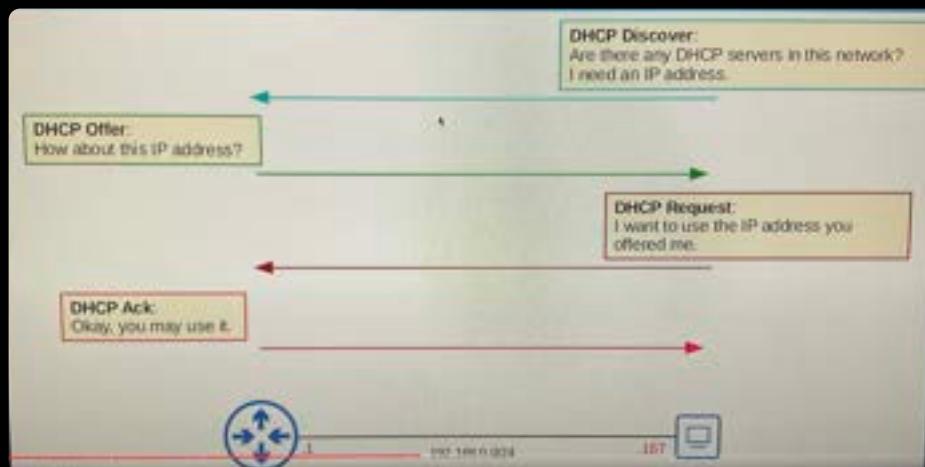
## • Day 39 - DHCP

### • Dynamic Host Configuration Protocol

DHCP Server → UDP 67

DHCP Client → UDP 68

### — DORA —

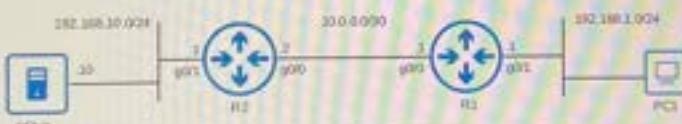


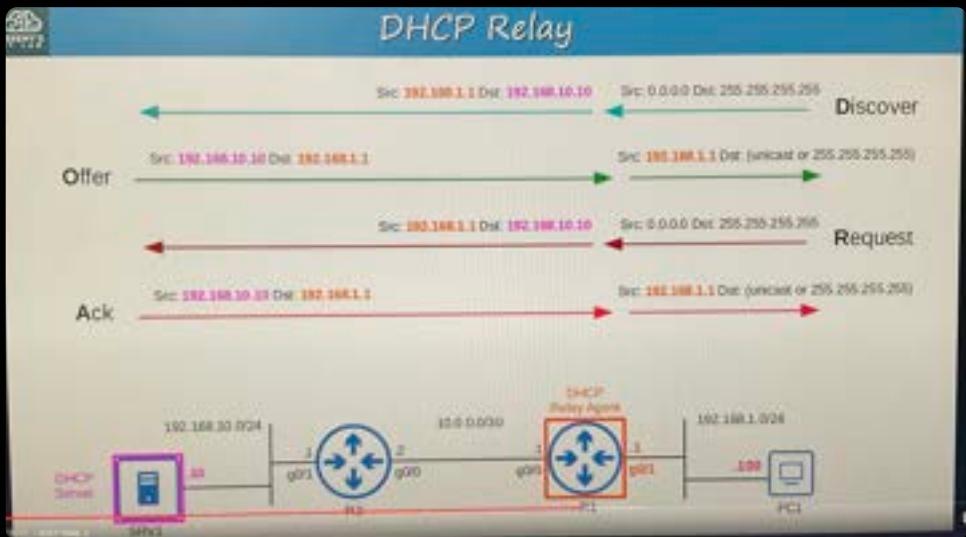
### DHCP D-O-R-A

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

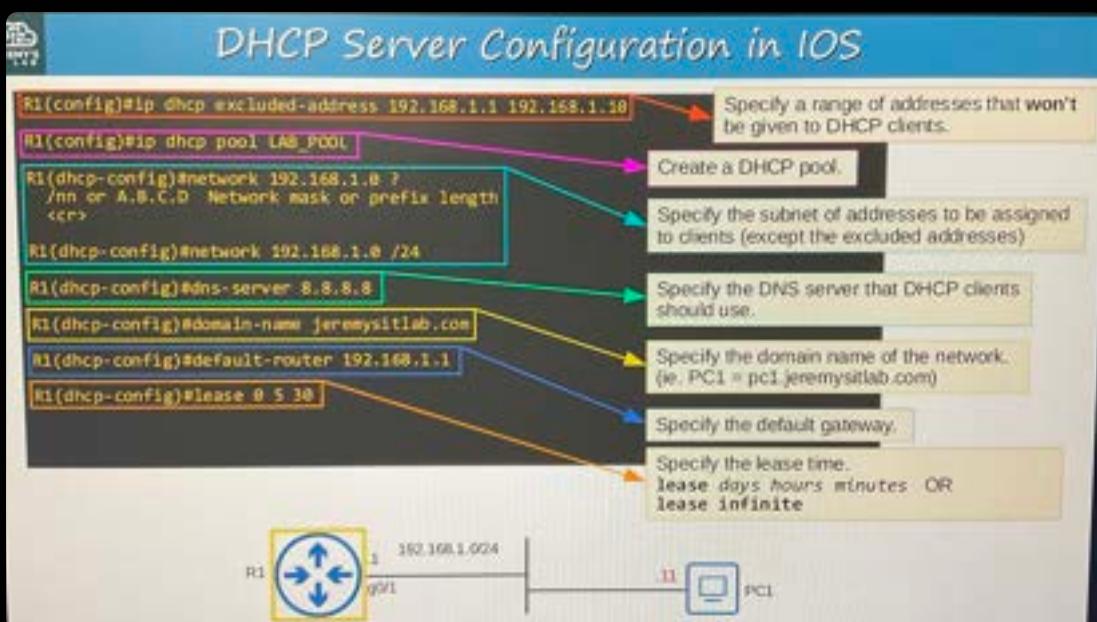
### DHCP Relay

- 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 Relay Agent Configuration in IOS

```
R1(config)#interface g0/1
R1(config-if)#ip helper-address 192.168.10.10
R1(config-if)#do show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is 192.168.10.10
[output omitted]
```

Configure the interface connected to the subnet of the client devices.  
Configure the IP address of the DHCP server as the 'helper' address.

```
graph LR; SRV1[DHCP Server SRV1] --- R2((R2)); R2 --- R1((DHCP Relay Agent R1)); R1 --- PC1[PC1];
```

## \* DHCP client

To configure cisco devices interfaced with DHCP

→ However, it is rare that we do this way

We usually set them manually

DHCP Client Configuration in IOS

```
R2(config)#interface g0/1
R2(config-if)#ip address dhcp
R2(config-if)#do sh ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.10.1/24
Broadcast address is 255.255.255.255
Address determined by DHCP
[output omitted]
```

Use the ip address dhcp mode to tell the router to use DHCP to learn its IP address.

```
graph LR; SRV1[DHCP Server SRV1] --- R2((DHCP Client R2)); R2 --- R1((DHCP Relay Agent R1)); R1 --- PC1[PC1];
```

# Day 40 → SNMP

## Simple network Management protocol

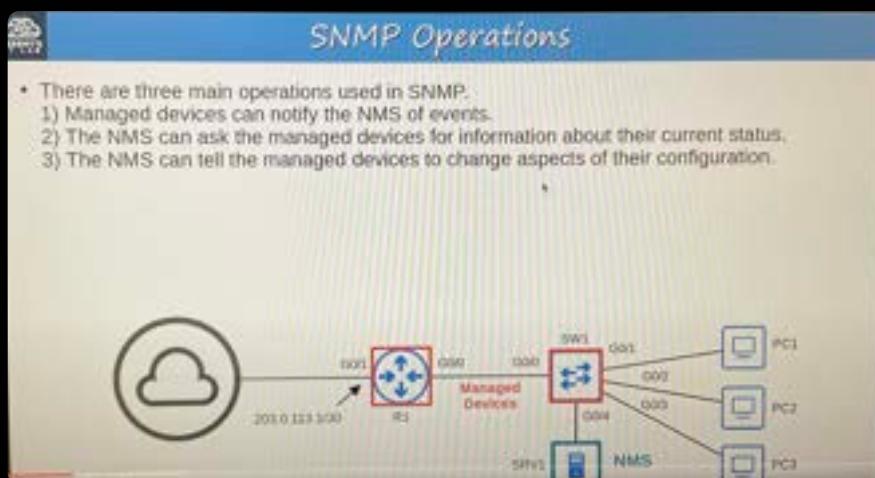
Two types

① Managed devices

② Network management station (NMS)

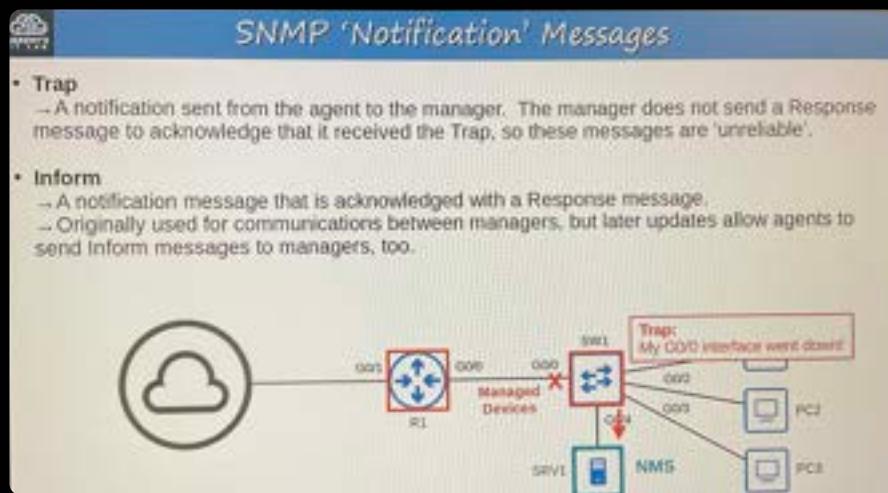
### Simple Network Management Protocol

- 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
- 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:
  - Managed Devices
    - These are the devices being managed using SNMP.
    - For example, network devices like routers and switches.
  - Network Management Station (NMS)
    - The device/devices managing the managed devices.
    - This is the SNMP 'server'.



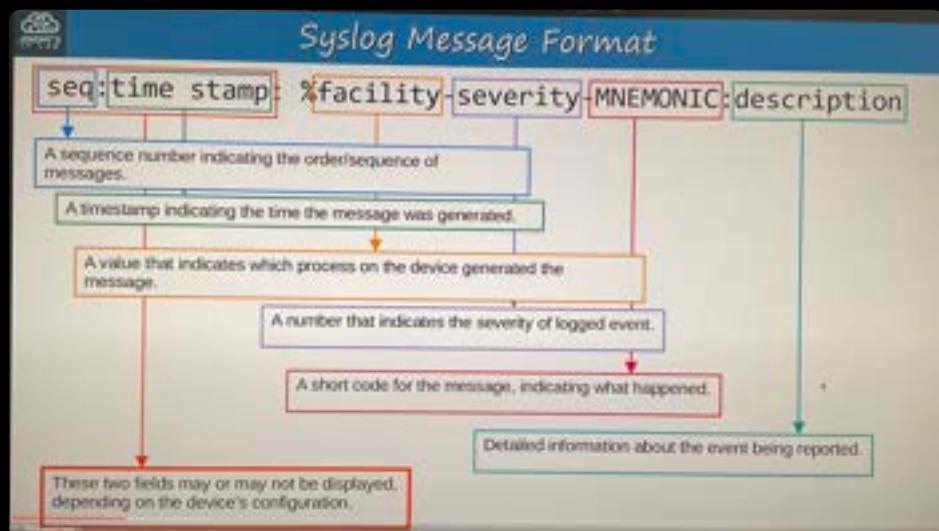
### SNMP Messages

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



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

## Day 41 — Syslog



| 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                            |

## EACENNIOD

Every Awesome Cisco Engineer will Needs  
Ice cream Daily

example →

| Syslog Message Examples |                       |                                                                                     |                                              |
|-------------------------|-----------------------|-------------------------------------------------------------------------------------|----------------------------------------------|
| seq:                    | time stamp:           | %facility-severity-MNEMONIC:                                                        | description                                  |
| "Feb 11 03:02:55.384:   | %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

Syslog Configuration

```
R1(config)#logging console 6 Logging console level
 *you can use the level number (6) or keyword informational
 *this will enable logging for the informational severity and higher

R1(config)#logging monitor informational Logging monitor level
 *same points as above about the level

R1(config)#logging buffered 8192 6 Logging buffered [size] level
 *same points as above about the level
 *buffer size is in bytes

R1(config)#logging 192.168.1.100 Logging server-ip
R1(config)#logging host 192.168.1.100 Logging Host server-ip
 *these commands are for easier

R1(config)#logging trap debugging Logging trap level
 *same points as above about the level
 *this sets the logging level for the external server
```

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 int
*Feb 11 09:38:41.607: %SYS-5-CONFIG_I: Configured from console by jeremy on
consoleinterface 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 datetime when the event occurred.  
**uptime** = timestamps will display how long the device had been running when the event occurred.

## Day 42 - SSH, Telnet

### Console Port Security - login

- By default, no password is needed to access the CLI of a Cisco IOS device via the console port.
- You can configure a password on the console line.
  - A user will have to enter a password to access the CLI via the console port.

```
R1(config)#line console 0
R1(config-line)#password ccna
R1(config-line)#login
R1(config-line)#end
R1#exit

R1 con0 is now available
Press RETURN to get started.

User Access Verification
Password:
```

There is only a single console line, so the number is always 0.

Configure the console line's password.

Tell the device to require a user to enter the configured password to access the CLI via the console port.

The password isn't displayed as you type it.

### Console Port Security - login local

- Alternatively, you can configure the console line to require users to login using one of the configured usernames on the device.

```
R1(config)#username jeremy secret ccomp
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#end
R1#exit

R1 con0 is now available
Press RETURN to get started.

User Access Verification
Username: jeremy
Password:
```

Tell the device to require a user to login using one of the configured usernames on the device.

```
line con 0
exec-timeout 3 30
password ccna
logging synchronous
login local
```

Log the user out after 3 minutes and 30 seconds of inactivity

### Layer 2 Switch - Management IP

- Layer 2 switches don't perform packet routing and don't build a routing table. They aren't IP routing aware.
- However, you can assign an IP address to an SVI to allow remote connections to the CLI of the switch (using Telnet or SSH).

```
SW1(config)#interface v1
SW1(config-if)#ip address 192.168.1.251 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit

SW1(config)#ip default-gateway 192.168.1.254
```

Configure the IP address on the SVI in the same way as on a multilayer switch. Enable the interface if necessary.

Configure the switch's default gateway. In this case, PC2 isn't in the same LAN as SW1. If SW1 doesn't have a default gateway, it can't communicate with PC2.

```
graph LR; PC1 --- SW1[VLAN: 203]; SW1 --- R1(()); R1 --- R2(()); R2 --- SW2[VLAN: 202]; SW2 --- PC2
```

## Telnet Configuration

```

SW1(config)#enable secret ccna
SW1(config)#username jeremy secret ccna
SW1(config)#access-list 1 permit host 192.168.1.1
SW1(config)#line vty 0 15
SW1(config-line)#login local
SW1(config-line)#exec-timeout 5 0
SW1(config-line)#transport input telnet
SW1(config-line)#access-class 1 in

```

If an enable password/secret isn't configured, you won't be able to access privileged exec mode when connecting via Telnet.

Configure an ACL to limit which devices can connect to the VTY lines.

Telnet/SSH access is configured on the VTY lines. There are 16 lines available, so up to 16 users can be connected at once. (VTY stands for Virtual Teletype)

`transport input telnet` allows only Telnet connections.  
`transport input ssh` allows only SSH connections.  
`transport input telnet ssh` allows both.  
`transport input all` allows all connections.  
`transport input none` allows no connections.



## 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 kg in their name  
**sw1 # show version**

**sw1 # show ip ssh**

### SSH Configuration: RSA Keys

- To enable and use SSH, you must generate an RSA public and private key pair.
- The keys are used for data encryption/decryption, authentication, etc.

```

SW1(config)#ip domain name jeremysitlab.com
The FQDN of the device is used to name the RSA keys.
FQDN = Fully Qualified Domain Name (host name + domain name)

SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.jeremysitlab.com
Choose the size of the key modulus in the range of 368 to 4096. For your
General Purpose Keys, choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

SW1(config)#
*Feb 21 04:22:35.778: %SSH-5-ENABLED: SSH 1.99 has been enabled

SW1(config)#do show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr,des128-cbc,des192-cbc,des256-cbc
MAC Algorithms: hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSSH format(ssh-rsa, base64 encoded): SW1.jeremysitlab.com
[output-truncated]

```

The FQDN of the device is used to name the RSA keys.  
FQDN = Fully Qualified Domain Name (host name + domain name)

Generate the RSA keys.  
`crypto key generate rsa modulus length` is an alternate method.  
Length must be 768 bits or greater for SSHv2.

## SSH Configuration: VTY Lines

```

SW1(config)#enable secret ccons
SW1(config)#username jeremy secret ccons
SW1(config)#access-list 1 permit host 192.168.2.1
SW1(config)#ip ssh version 2
SW1(config)#line vty 0 15
SW1(config-line)#login local
SW1(config-line)#exec-timeout 5 0
SW1(config-line)#transport input ssh
SW1(config-line)#access-class 1 in

```

(optional, but recommended) Restrict SSH to version 2 only.

Configure all VTY lines, just like Telnet.

Enable local user authentication. "you cannot use login for SSH, only login local"

(optional, but recommended) Configure the exec timeout.

Best practice is to limit VTY line connections to SSH only.

(optional, but recommended) Apply the ACL to restrict VTY line connections.

## SSH Configuration

- 1) Configure host name
- 2) Configure DNS domain name
- 3) Generate RSA key pair
- 4) Configure enable PW, username/PW
- 5) Enable SSHv2 (only)
- 6) Configure VTY lines

```

Router(config)#crypto key generate rsa
% Please define a hostname other than Router.
#router(config)#hostname R2
#2(config)#crypto key generate rsa
% Please define a domain-name first.
#2(config)#ip domain name jermysitlab.com
#2(config)#crypto key generate rsa
The name for the keys will be: R2.jermysitlab.com
[output omitted]

```

Connect: ssh -l username ip-address OR ssh username@ip-address

You have to know how to configure SSH for the CCNA exam, so make sure to do the practice lab!

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

FTP & TFTP

- FTP (File Transfer Protocol) and TFTP (Trivial File Transfer Protocol) are industry standard protocols used to transfer files over a network.
- They both use a client-server model.
  - Clients can use FTP or TFTP to copy files from a server.
  - Clients can use FTP or TFTP to copy files to a server.
- As a network engineer, the most common use for FTP/TFTP is in the process of upgrading the operating system of a network device.
- You can use FTP/TFTP to download the newer version of IOS from a server, and then reboot the device with the new IOS image.

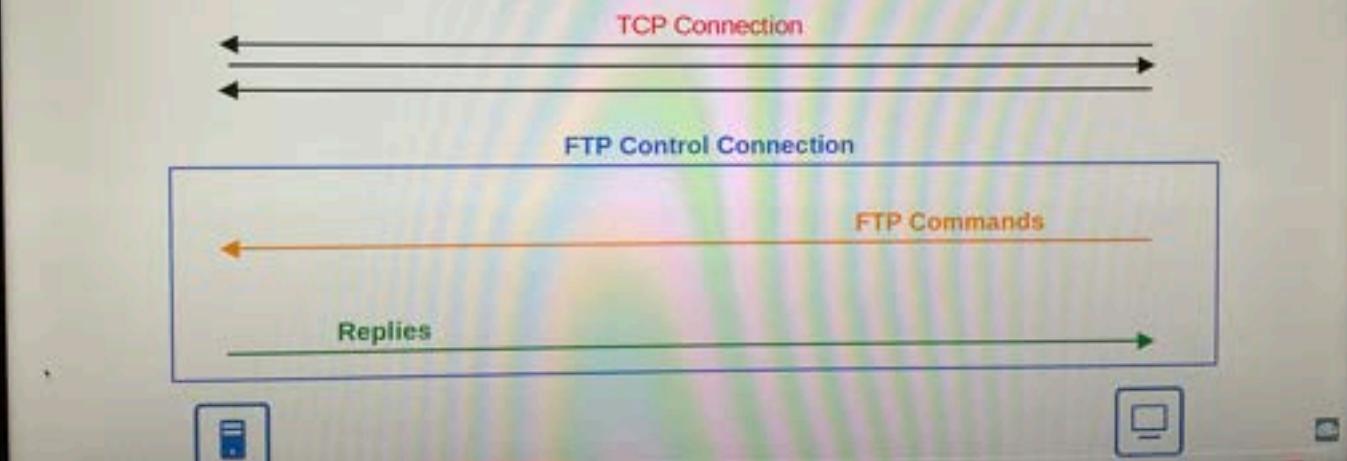
1. Get the IOS image from Cisco.

2. Put the IOS image on a server reachable by the device to be updated.

3. Use FTP/TFTP to copy the file into the flash memory of the device.

```
graph LR; A[software.cisco.com] --> B((Cloud)); B --> C[Admin's PC]; C --> D[FTP Server]; D --> E((R1))
```

- FTP uses two types of connections:
  - An **FTP control connection (TCP 21)** is established and used to send FTP commands and replies.
  - When files or data are to be transferred, separate **FTP data (TCP 20)** connections are established and terminated as needed.



## ① Active mode

In FTP **Active mode** server initiates the connection

- ② **Passive 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

- A file system is a way of controlling how data is stored and retrieved.
- You can view the file systems of a Cisco IOS device with `show file systems`

| Router# show file systems |            |         |       |                  |                                                                                   |
|---------------------------|------------|---------|-------|------------------|-----------------------------------------------------------------------------------|
| File Systems:             |            |         |       |                  |                                                                                   |
| Size(b)                   | Free(b)    | Type    | Flags | Prefixes         |                                                                                   |
| 2142715904                | 1994403840 | disk    | rw    | flash0: flash1:  | disk: Storage devices such as flash memory.                                       |
|                           |            | disk    | rw    | flash2: flash3:  |                                                                                   |
|                           |            | disk    | rw    | flash4: archive: | opaque: Used for internal functions                                               |
|                           |            | disk    | rw    | system: nvram:   |                                                                                   |
|                           |            | opaque  | rw    | nvram: biosys:   | nvram: Internal NVRAM. The startup-config file is stored here.                    |
|                           |            | opaque  | rw    | snmp: null:      |                                                                                   |
|                           |            | opaque  | rw    | tftp: xmodem:    |                                                                                   |
|                           |            | network | rw    | syslog: rcp:     | network: Represents external file systems, for example external FTP/TFTP servers. |
|                           |            | opaque  | rw    | prnt: ftp:       |                                                                                   |
|                           |            | network | rw    |                  |                                                                                   |
|                           |            | network | rw    |                  |                                                                                   |
|                           |            | network | rw    |                  |                                                                                   |

Upgrading ios —

# show version

→ if kg in version that means SSH enabled

# show Flash

R1 # copy tftp: flash:

To upgrade —

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

# wiz  
# Reload  
# show version

To delete → delete flash:filename

R1(config)\*# ip ftp username cisco

**Copying Files (FTP)**

```
R1(config)*#ip ftp username cisco
R1(config)*#ip ftp password cisco
R1(config)*#exit
R1#copy ftp: flash:
Address or name of remote host []? 192.168.1.1
Source filename []? c2900-universalk9-mz.SPA.155-3.M4a.bin
Destination filename [c2900-universalk9-mz.SPA.155-3.M4a.bbe]?
Accessing ftp://192.168.1.1/c2900-universalk9-mz.SPA.155-3.M4a.bin...
Loading c2900-universalk9-mz.SPA.155-3.M4a.bin from
192.168.1.1: [/]
[output omitted]
```



```
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
```

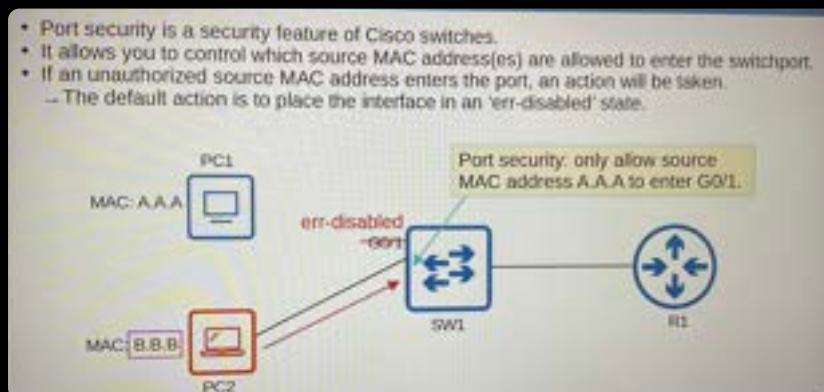
→ Skip 44 - 47

Day 48 —

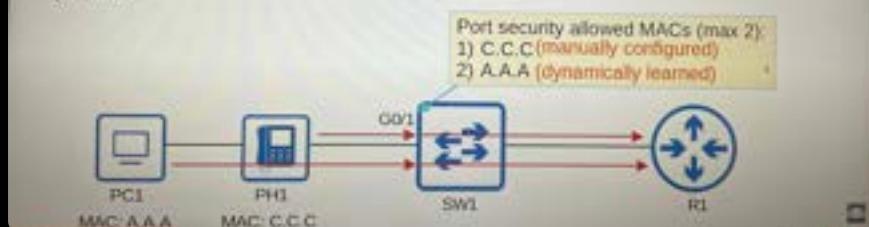
## Security fundamentals

## Day 49 - Port security

- Port security is a security feature of Cisco switches.
- It allows you to control which source MAC address(es) are allowed to enter the switchport.
- If an unauthorized source MAC address enters the port, an action will be taken.
  - The default action is to place the interface in an 'err-disabled' state.

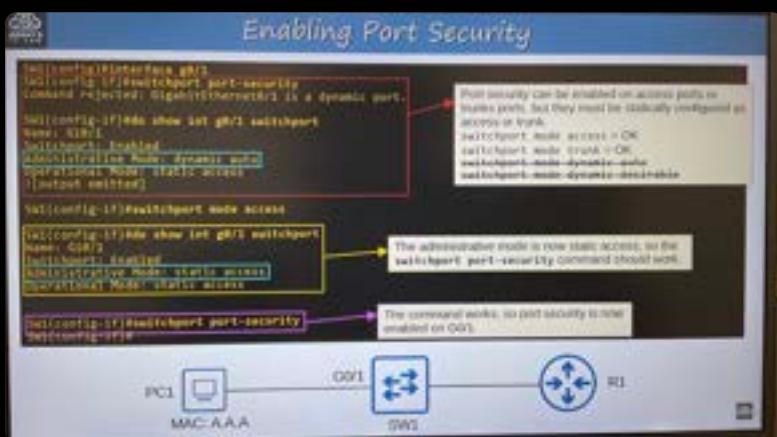


- When you enable port security on an interface with the default settings, one MAC address is allowed.
  - You can configure the allowed MAC address manually.
  - If you don't configure it manually, the switch will allow the first source MAC address that enters the interface.
- You can change the maximum number of MAC addresses allowed.
- A combination of manually configured MAC addresses and dynamically learned addresses is possible.



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

### Config -



# show port-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
```

**Re-enabling an interface (ErrDisable Recovery)**

```
SW1(config)#errdisable recovery cause psecure-violation
SW1(config)#errdisable recovery interval 180

SW1#show errdisable recovery
ErrDisable Reason Timer Status
-----+-----+
! [output omitted due to length]
psecure-violation enabled
! [output omitted due to length]

Timer Interval: 180 seconds

Interfaces that will be enabled at the next timeout:
Interface Errdisable reason Time left(sec)
-----+-----+
G10/1 psecure-violation 149

ErrDisable Recovery is useless if you don't remove the device that caused the interface
to enter the err-disabled state!
```

**Violation Modes**

There are three different violation modes that determine what the switch will do if an unauthorized frame enters an interface configured with port security.

- **Shutdown**
  - Effectively shuts down the port by placing it in an err-disabled state.
  - Generates a Syslog and/or SNMP message when the interface is disabled.
  - The violation counter is set to 1 when the interface is disabled.
- **Restrict**
  - The switch discards traffic from unauthorized MAC addresses.
  - The interface is NOT disabled.
  - Generates a Syslog and/or SNMP message each time an unauthorized MAC is detected.
  - The violation counter is incremented by 1 for each unauthorized frame.
- **Protect**
  - The switch discards traffic from unauthorized MAC addresses.
  - The interface is NOT disabled.
  - It does NOT generate Syslog/SNMP messages for unauthorized traffic.
  - It does NOT increment the violation counter.

## 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

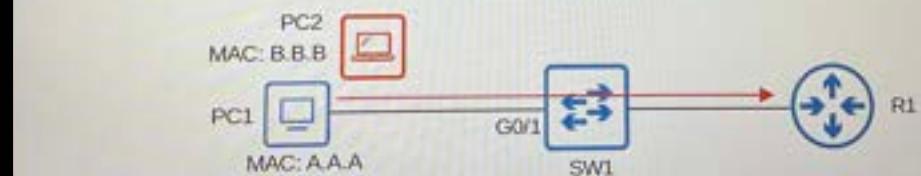
SW1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
 (Count) (Count) (Count)

 G0/1 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
```

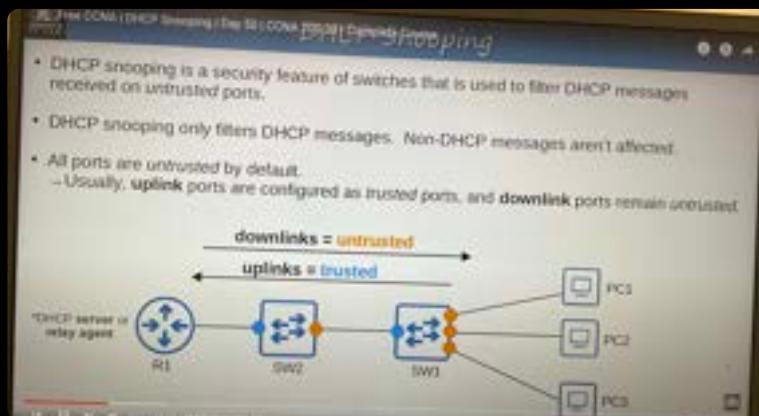
**Sticky Secure MAC Addresses**

```
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
```



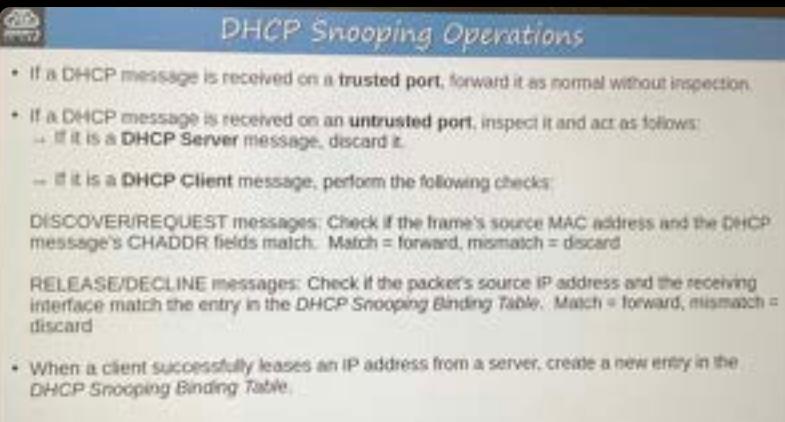
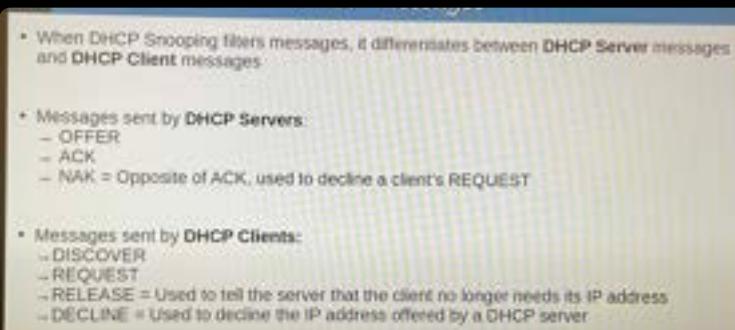
## Day 50 – DHCP Snooping

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



DHCP Snooping protects against attacks like

- ① DHCP starvation
- ② DHCP Poisoning



### DHCP Snooping

```

Switch# config t
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 3
Switch(config)# ip dhcp snooping information option
Switch(config)# interface g0/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# show ip dhcp snooping binding
MacAddress Lease(sec) Type VLAN Interface
0C:29:2F:28:79:00 98384 dhcp-snooping 3 GigabitEthernet0/1
0E:29:2F:28:91:00 98384 dhcp-snooping 3 GigabitEthernet0/2
0C:29:2F:28:87:00 98384 dhcp-snooping 3 GigabitEthernet0/3
Total number of bindings: 3

```

### DHCP Snooping Rate-Limiting

- DHCP snooping can limit the rate at which DHCP messages are allowed to enter an interface.
- If the rate of DHCP messages crosses the configured limit, the interface is err-disabled.
- Like with Port Security, the interface can be manually re-enabled, or automatically re-enabled with errdisable recovery.

```

Switch(config)# interface range g0/1 - 3
Switch(config)# f-range 1-3 dhcp-snooping limit-rate 1

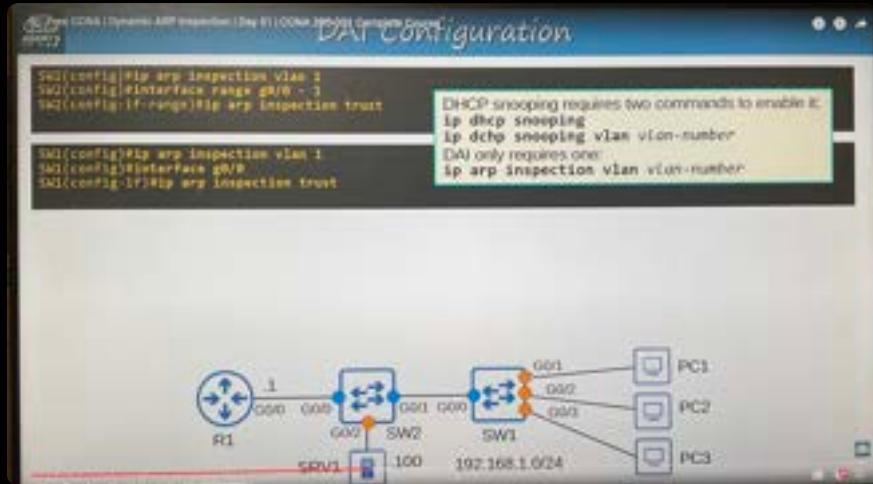
```

## Day 51 Dynamic ARP Inspection

DAI -

### Dynamic ARP Inspection

- DAI is a security feature of switches that is used to filter ARP messages received on untrusted ports.
- DAI only filters ARP messages. Non-ARP messages aren't affected.
- All ports are untrusted by default.
  - Typically, all ports connected to other network devices (switches, routers) should be configured as **trusted**, while interfaces connected to end hosts should remain **untrusted**.



## Day 55- Wireless Lans

- 802.11 Lans are called WiFi

**Review**

- Wireless LANs are defined in 802.11.
- Operate in half duplex using CSMA/CA.
- Wireless signals can be affected by absorption, reflection, refraction, diffraction, and scattering.
- Various aspects of waves can be measured, such as amplitude, frequency, and period.
- Frequency is measured in hertz (Hz).
- Wireless LANs use two frequency ranges: the 2.4 GHz band and 5 GHz band.
  - Wi-Fi 6 (802.11ax) can use the 6 GHz range too.
- Bands are divided into channels.
- 5 GHz band consists of non-overlapping channels.
- 2.4 GHz band channels overlap. To avoid overlapping, use channels 1, 6, and 11 (in North America).
- 802.11 standards (802.11b, 802.11a, etc) and their frequencies/theoretical max data rates.
- Service sets are groups of wireless devices. Three types:
  - Independent (IBSS, also called ad hoc)
  - Infrastructure (BSS, ESS)
    - "passing between APs in an ESS is called roaming."
  - Mesh (MBSS)
- Service sets are identified by an SSID (non-unique, human-readable) and BSSID (unique, MAC address of AP).
- The area around an AP where its signal is usable is called a BSA.
- The upstream wired network is called the DS.
- When multiple WLANs are used, each is mapped to a separate VLAN on the wired network.
- APs can also operate as a repeater, workgroup bridge, or outdoor bridge.

Although this summarizes the topics in this video—make sure you know the details of each topic that we covered!

| 802.11 Standards |                 |                             |                |           |
|------------------|-----------------|-----------------------------|----------------|-----------|
| Standard         | Frequencies     | Max Data Rate (theoretical) | Alternate Name |           |
| 802.11           | 2.4 GHz         | 2 Mbps                      |                |           |
| 802.11b          | 2.4 GHz         | 11 Mbps                     |                |           |
| 802.11a          | 5 GHz           | 54 Mbps                     |                |           |
| 802.11g          | 2.4 GHz         | 54 Mbps                     |                |           |
| 802.11n          | 2.4 / 5 GHz     | 600 Mbps                    | 'Wi-Fi 4'      |           |
| 802.11ac         | 5 GHz           | 6.93 Gbps                   | 'Wi-Fi 5'      |           |
| 802.11ax         | 2.4 / 5 / 6 GHz | 4*802.11ac                  |                | 'Wi-Fi 6' |

# Day 56 — WLAN - 2

**802.11 Messages Overview**

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.

probe request → probe response

authentication request → authentication response

association request → association response

• 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**

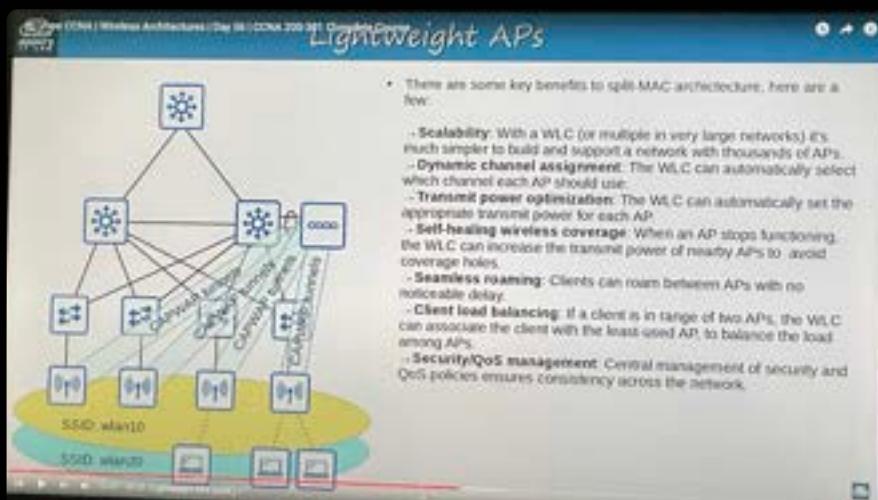
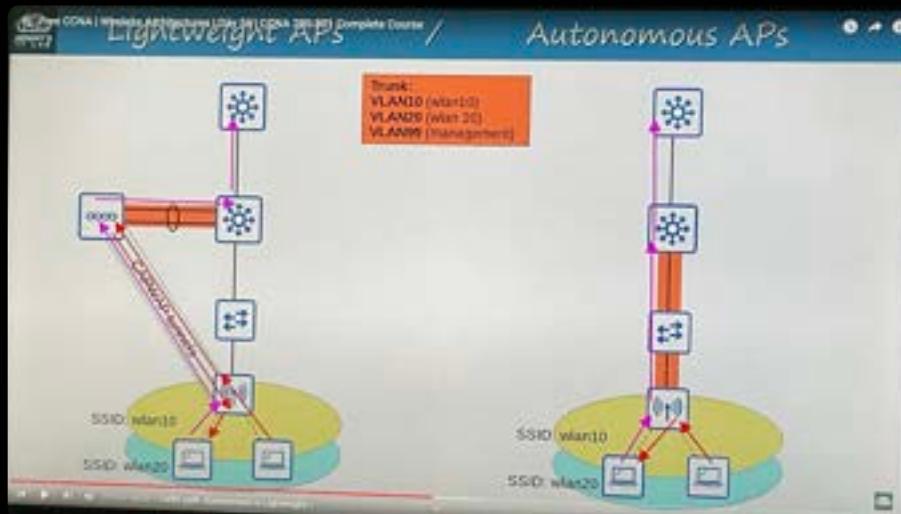
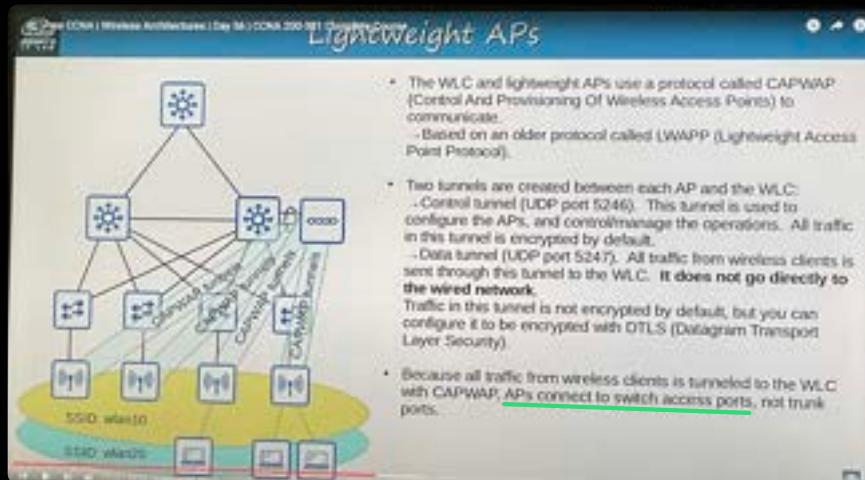
- There are three main wireless AP deployment methods:
  - Autonomous
  - Lightweight
  - Cloud-based
- **Autonomous APs** are self-contained systems that don't rely on a WLC.
- Autonomous APs are configured individually.
  - Can be configured by console cable (CLI), telnet/SSH (CLI), or HTTP/HTTPS web 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**

- 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**



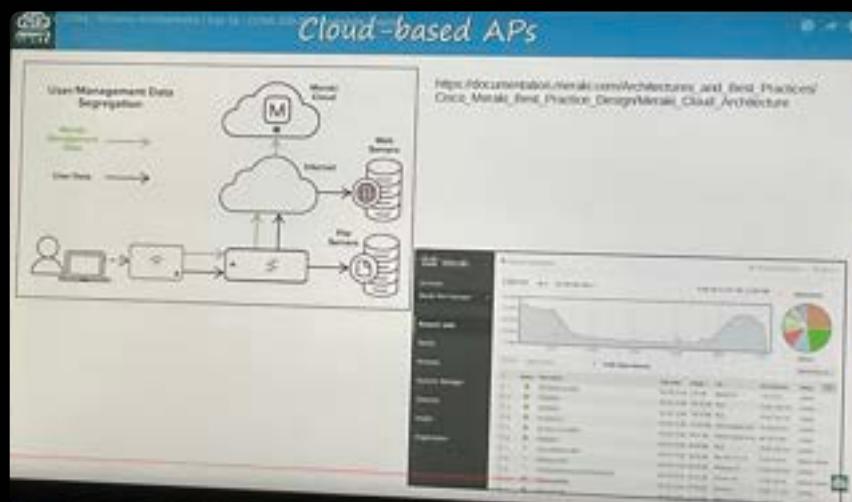
- Lightweight APs can be configured to operate in various modes:

- 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

The slide is titled "WLC Deployments". It lists four deployment models:

- In a split-MAC architecture, there are four main WLC deployment models:
  - **Unified:** The WLC is a hardware appliance in a central location of the network. *6K*
  - **Cloud-based:** The WLC is a VM running on a server, usually in a private cloud in a data center. This is not the same as the cloud-based AP architecture discussed previously. *9K*
  - **Embedded:** The WLC is integrated within a switch. *200*
  - **Mobility Express:** The WLC is integrated within an AP. *100 AP*

- Day 57 - WLAN security

- WLC only supports LAG it does not support PAgP or LACP.

so that's 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   |

|*6th Head*| *payload* |*6th trailer*|

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

## OSI model POU

