Practical

① To set static ip address

```
# int g0/0
if # ip add 192.168.1.1 255.255.255.0
```

② VLAN Setup

2.1 Access mode → for single VLAN

```
# int g0/0
      OR
# int range g 0/0 - 3
# switchpost mode aeess
# switchpost access vlan 10
```

Supporting commands

```
(config) # do show vlan brief
```

2.2 trunk – for multiple vlan

```
# int g0/0
c-if # switchpost mode trunk
# switchpost trunk encapsulation dot1q
```

Supporting commands

```
SW1 # show interface trunk
# show vlan brief
c-if # switchpost trunk allowed vlan 2
```

* Also it is recommended to change the default vlan on the link for Security purposes

```
c-if # switchpost trunk native vlan 1001      → on both side.
```

3. Router on a Stick
(ROAS)

- To create single link for multiple vlan from switch to Router

```
# int g 0|0.10
(config-subif) # encapsulation  dot1Q  10  native
               # ip address  —  —
```

4. Inter-Vlan routing on L3 Switches

- Inter-vlan means routing Vlan can communicate the traffic between each other with the help of switch rather than sending that traffic to router to forward.

for SVI
ip routing → To enable routing

4. DTP — Dynamic trunking protocol

To set trunking automatically
- for security purposes, manual config is recommended.

DTP should be disabled on all switchports.

(config-if) # switchport mode dynamic
— desirable — actively try to form trunk
auto

- check chart

desirable	—	desirable = trunk
desirable	—	Auto = trunk
desirable	—	trunk = trunk
desirable	—	access = Access

— for dynamic auto
— not actively trying to form a trunk
trunk with
switch mode mode trunk
desirable

5. VTP (Vlan trunking protocol)

6. STP

default bridge priority = 32768
default Mac address is used as the breaker

In default Vlan of 1, the default bridge priority is actually 32769 (32768+1)

Spanning tree Protocol cost

Speed	STP Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

1 • All ports on the root bridge are designated ports

— Root bridge selection
1. lowest bridge ID

2. • Each remaining switch will select one of its interfaces to be its root port.
— Ports across from the root ports are always designated ports.
Root ports selection —
1. lowest root cost
2. lowest neighbor bridge ID.
3. lowest neighbor port ID.

3. Each remaining collision domain will select ONE interface to be a designated port. The other port will be non-designated (blocking)

Designated Port selection :-
1. Interface on switch with lowest root cost
2. Interface on switch with lowest bridge ID

6.1 Configuring STP

SW1(config)# spanning-tree mode pvst
spanning tree vlan 1 root priority
do show spanning-tree

spanning tree vlan 2 root secoundary

spanning-tree vlan 1 cost ?

spanning-tree vlan 1 port-priority 32

7. Ether channel – To allow all links from two switches to transfer traffic.
– groups multiple interfaces together to act as a single int.

other names
① Port channel
② LAG(Link Aggregation Group)

SW1 # show etherchannel load-balance

(config)# port-channel load-balance ?

3 methods
- ① PAgP – Port Aggregation Protocol

#② LACP – Link aggregation control protocol

③ static etherchannel

upto 8 interfaces can be formed into single EC.

interface range g0/0-3

channel-group 1 mode ?

- passive + passive = no Etherc
- Active + passive = Etherchannel
- Active + Active = Etherchannel

do show ip interface brief

do show etherchannel summary
(config)# interface po1

show etherchannel port-channel

Commands

```
SW(config) port-channel load-balance mode
 #configures the EtherChannel load-balancing method on the switch

SW# show etherchannel load-balance
 #displays information about the load-balancing settings

SW(config-if)# channel-group number mode {desirable|auto|active|passive|on}
 #configures an interface to be part of an EtherChannel

SW# show etherchannel summary
 #displays a summary of EtherChannels on the switch

SW# show etherchannel port-channel
 #displays information about the virtual port-channel interfaces on the switch
```

8. Dynamic routing

- Dynamic routing
  - EGP – Exterior Gateway P
    - Distance vector
      - RIP
      - EIGRP
    - Link state
      - OSPF
      - IS-IS
  - IGP – Interior gateway P
    - Path vector
      - BGP.

8.1 Distance vector

Metrics are used to find best route

if same metrics both will be added.

ECMP – Equal cost Multi-path → load balancing

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

- Metrics are used to compare routes learned via same routing protocol
- Administrative distance is used to determine which route to prefer if two routing protocols are used.

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

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

If the administrative distance is 255, the router does not believe the source of that route and does not install the route in the routing table.

8.2 RIP configurations

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

* No need to Enter network mask.

R1 (config-router) # passive-interface g2/0
→ To stop sending RIP advertisements

skipped routing.

- FHRP (first hop redudancy protocol)

Gratitous ARP – Reply sent without receiving arp request

FHRP are non-preemptive – The current Active router wont give up its role even if the former active router returns.

FHRP

Multicast IPV4 – v1 – 224.0.0.2
v2 – 224.0.0.102

Virtual MAC address – v1 – 0000.0c07.ac xx
v2 – 0000.0c9F.F xxx

2. VRRP

Multicast – 224.0.0.18
Virtual Mac – 0000.5e00.01xx

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

Configuring HSRP

```
# interface g 0/0
(c-if) # standby version ?
       # standby version 2      → Both routers should be using same version.

       # standby 1 ip 172.16.0.254

       # standby 1 priority 200      → default is 100
         (group number)

(c-if) # standby 1 preempt → To take active router role

       # show standby
```

9. Configuring IPV6 Add

```
# ipv6 unicast-routing → Allows router to perform IPV6 routing
# int g 0/0
# ipv6 address 2001:db8:0:0::1/64
# no shutdown

# show ipv6 interface brief
```

IPV6 – EUI-64

↳ Extended Unique identifier

Method of converting a Mac address (48 bits) into 64-bit interface identifiers

- Divide in half
- Add FFFE in middle
- Inver the 7th bit

- Configuring IPV6 addresses

```
# int g0/0
# ipv6 address 2001:db8::/64   eui-64"
# no shutdown
```

→ Where we use interface Mac address to set Ip Address.

We do this to autoconfigure IPV6 Addresses using SLAAC.

- Global Unicast –

2000::/3 block to 3FFF:FFFF:FFFF .....

- Unique local address –
  - private addresses cannot be used over the internet
  - no registration needed to use them
  - Not globally unique

– Uses address block –

FD00::/7 to FDFF:FFFF:...

- Link local – automatically generated on IPV6-enabled interface

ipv6 enable → on int to enable IPV6 on interface

- Uses FE80::/10

begins with FE8

IPV6 uses FF00::/8 for multicast
IPV6 doesn't support broadcast

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

Loopback — ::1

Unspecified addresses — ::/0

SLACC — Stateless Address Auto-configuration.

Using NDP we can auto-configure Address

so without NDP (Network discovery protocol) we have to:-

use # ipv6 address prefix/prefix length eui-64 command

but With SLACC

ipv6 address autoconfig → Will automatically get the prefix

Config →

```
# int g0/0
# ipv6 address autoconfig
```

DAD (Duplicate address detection)

→ To check the duplicate address on the local link

g. IPV6 static routing —

IPV6 routing is disabled by default & must be enabled with

`IPV6 unicast-routing`

- If IPV6 routing is disabled, the router will still send & receive IPV6 traffic.

ipv6 route dst/pre-length { next hop | exit int [next-hop] } [ad]

Acl's skip for now

10. CDP & LLDP

- CDP Multicast Address - 0100.0ccc.cccc
- CDP Messages are sent once every 60 sec.
- Holdtime is 180 seconds.

```
# show cdp
# show cdp traffic
# show cdp interface
# show cdp neighbors
# show cdp neighbors detail
# show cdp entry R2
```

CDP config

- CDP enabled by default
- To enable/disable CDP globally - # no cdp run
- To enable/disable CDP on specific interface - R1(config-if) no cdp enable

- configuring cdp timer # cdp timer 60 → default every 60 sec

- Holdtime config R1(config) # cdp holdtime 180 → default

- Enable/disable CDPv2 - [no] cdp advertise-v2

LLDP -

Disable by default

- When device receives LLDP messages it processes and discard the msgs does not forward.

- Every 30 second
- Holdtime - 120 sec

- initilization of LLDP is - 2 seconds

- To enable - (config) # lldp run
- on specific int (tx) - lldp transmit
  (rx) - lldp receive

lldp timer 30
lldp holdtime 120
lldp reinit seconds

show same as cdp

NTP

show clock
show clock detail
show logging

Manual time config

R2# clock set

- Hardware clock and software clock are two different clocks
- Hardware calender is a default time source

clock update-calender → to sync the calender to the clocks time
clock recal - calender → to sync the clock to calender

- Timezone config

- clock timezone JST 9

- NTP
— The distance of an NTP server from the original reference clock is called stratum

NTP uses UDP - 123

- Reference clocks are stratum 0.
- NTP servers directly connected to reference clocks are stratum 1.

- stratum 15 is the maximum. Anything above that is considered unreliable.
- Devices are also peer with devices at the same stratum to provide more accurate time.

NTP configuration

ntp server 216.239.35.0 prefer

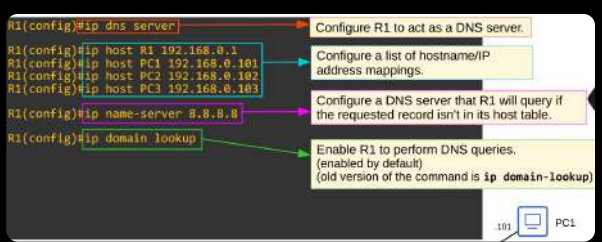
show ntp association
show ntp status
show clock details

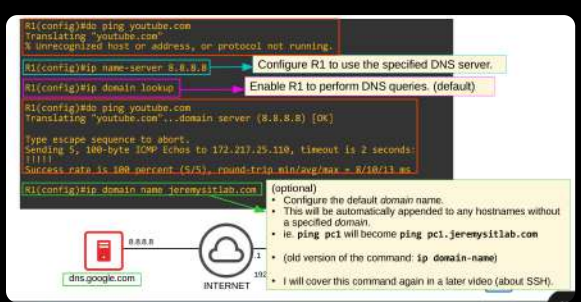
default stratum of ntp master is 8

11. DNS server

Router as DNS

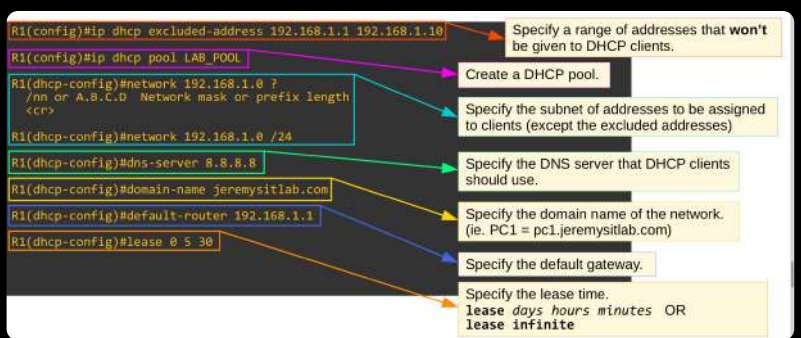
(config) # ip dns server
ip host R1 192.168.0.1





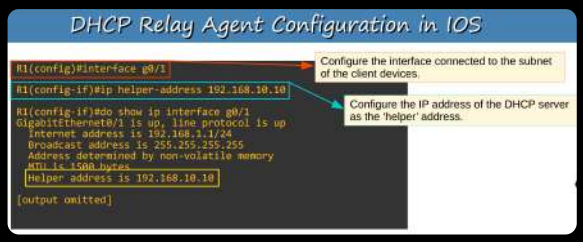
DHCP server config

R1 (config) # ip dhcp excluded-address 192.168.1.1 192.168.1.10
↳ To exclude ip address from dhcp



To see dhcp bindings

R1 # show ip dhcp binding

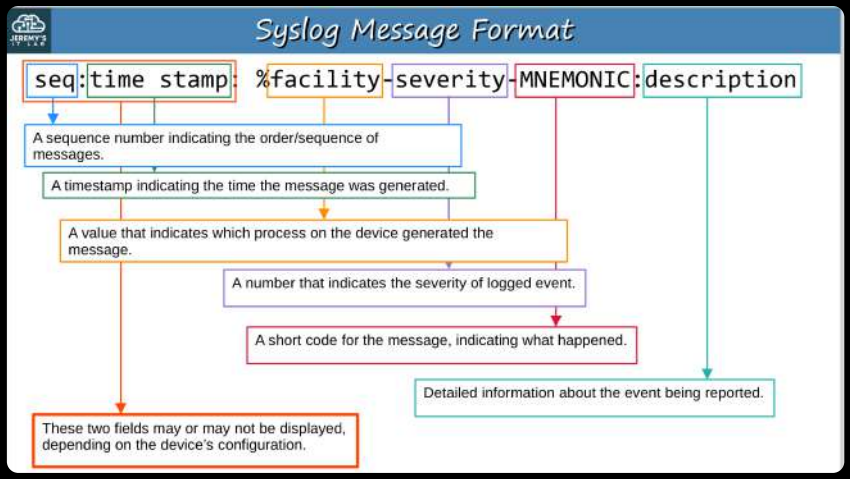


12. SNMP Configuration

(config) # snmp-server contact sam@sam.com
snmp-server location sam

13. Syslog.

Syslog message format

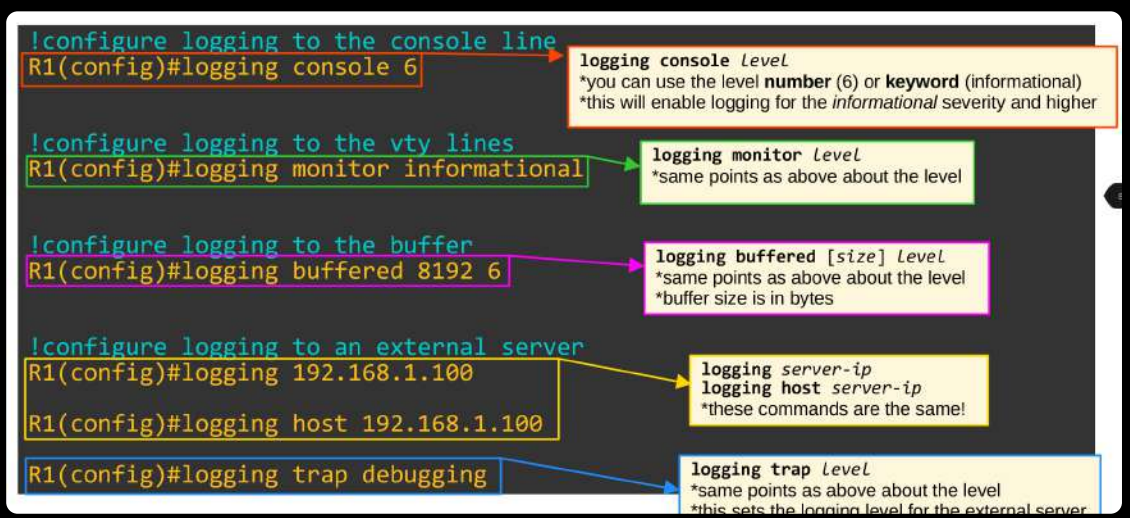


Syslog logging location

① console port
② VTY lines
③ Buffer
④ External server

– Syslog configuration

R1 (config) # logging console 6 → 6 and above syslogs

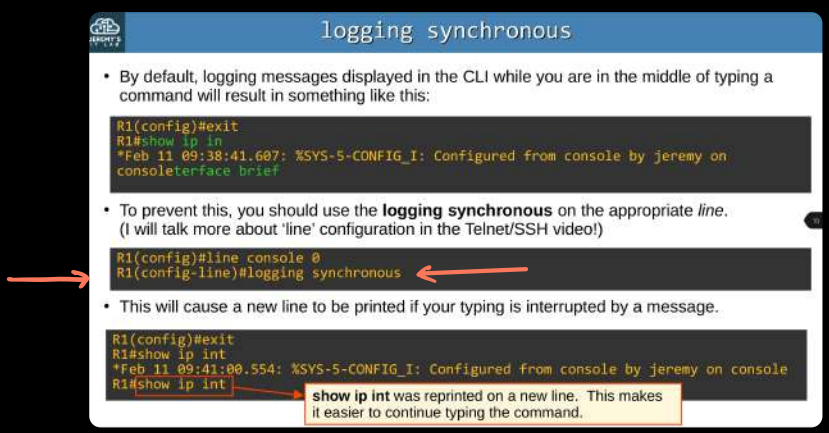


Important for Telnet and SSH.

① Even if logging monitor level is enabled, by default syslog messages will not be displayed when connected via Telnet or SSH.

for that

R1 # terminal logging → Must be used everytime we connect.



```
R1(config)# logging console severity
R1(config)# logging monitor severity
R1(config)# logging buffered [size] severity
R1(config)# logging server-ip
R1(config)# logging host server-ip
R1(config)# logging trap severity
R1# terminal monitor
R1(config-line)# logging synchronous
R1(config)# service timestamps log [datetime | uptime]
R1(config)# service sequence-numbers
```

FTP

show file systems
show version
show flash
→ # copy source destination

→ # boot system filepath
ip ftp username username
ip ftp password password.

QoS.

- VOIP phones configuration

SW1(config) # interface gigabitethernet 0/0
(Co-IF) # switchport mode access
switchport access vlan 10
switchport voice vlan 11

show interfaces g 0/0 switchport

Even though we are using multiple vlans it is not considered as trunk port.

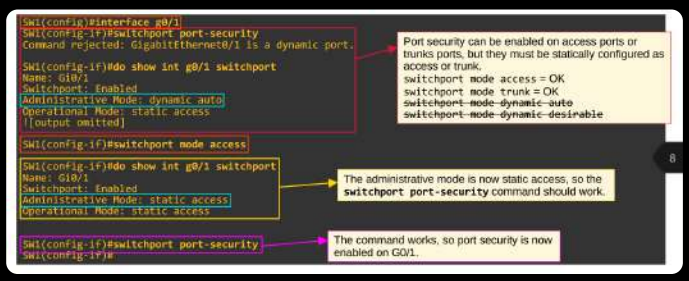
Port Security -

To allow only the defined or first Mac address to use the configured port.
- If no MAC address configured manually then first mac address will be Taken.
- Can change max no. of mac allowed on single port.

13. Port Security config.

(config) # interface g0/1
(if) # switchport post-security
do show int g0/1 switch port

(config-if) switchport mode access



show post-security interface 0/1

When attacker connects to that port it goes into err-disabled mode
To re-enable just shutdown, no shutdown will do it.

* err-disable recovery
# show errdisable recovery

* if err-disable recovery has been enabled it will recover every 5 min by default

We can change the cause for violation with
errdisable recovery cause psecure-violation

errdisable recovery interval 180 → default 300sec

```
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
```

14. DHCP snooping

(config) # ip dhcp snooping

ip dhcp snooping vlan 1
no ip dhcp snooping information option
interface g0/0
(-if) # ip dhcp snooping trust

show ip dhcp snooping binding

ip dhcp snooping limit rate 1 → To limit the dhcp msg

option 82 - DHCP relay agent

↑

(config) # no ip dhcp snooping information option

errdisable recovery cause dhcp-rate-limit

15. Dynamic ARP Inspection (DAI)

Same like DHCP snoop downlinks are untrusted and request are filtered & checked.

— Verifies senders Mac with CHAddr & senders IP field of ARP message received.

show ip dhcp snooping binding

DAI Config

(c) # ip arp inspection vlan 1
interface range g0/0-1
(config-if-range) # ip arp inspection trust

show ip arp inspection interfaces

ip arp inspection validate ?

dst-mac
ip
src-mac

} has to match else invalid

15. VRF config

(config) # ip vrf customer1
ip vrf customer2
do show ip vrf

(config-vrf) # interface g0/0
(-if) # ip vrf forwarding customer1
ip address 192.168.1.1 255.255.255.252

same for other interface & customer2

To see ip routes of vrf
show ip route vrf customer1

ping vrf customer1 192.168.1.2