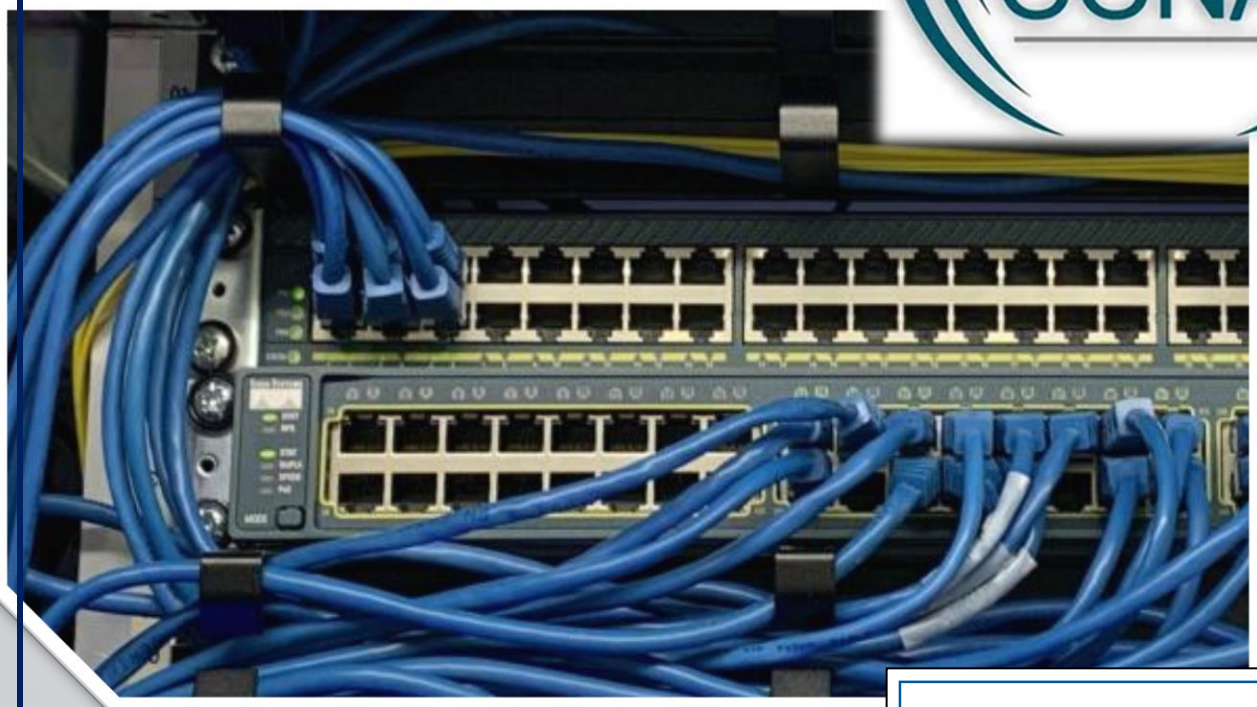
CCNA 200-301

CISCO CERTIFIED NETWORK ASSOCIATE

CISCO CERTIFIED CCNA



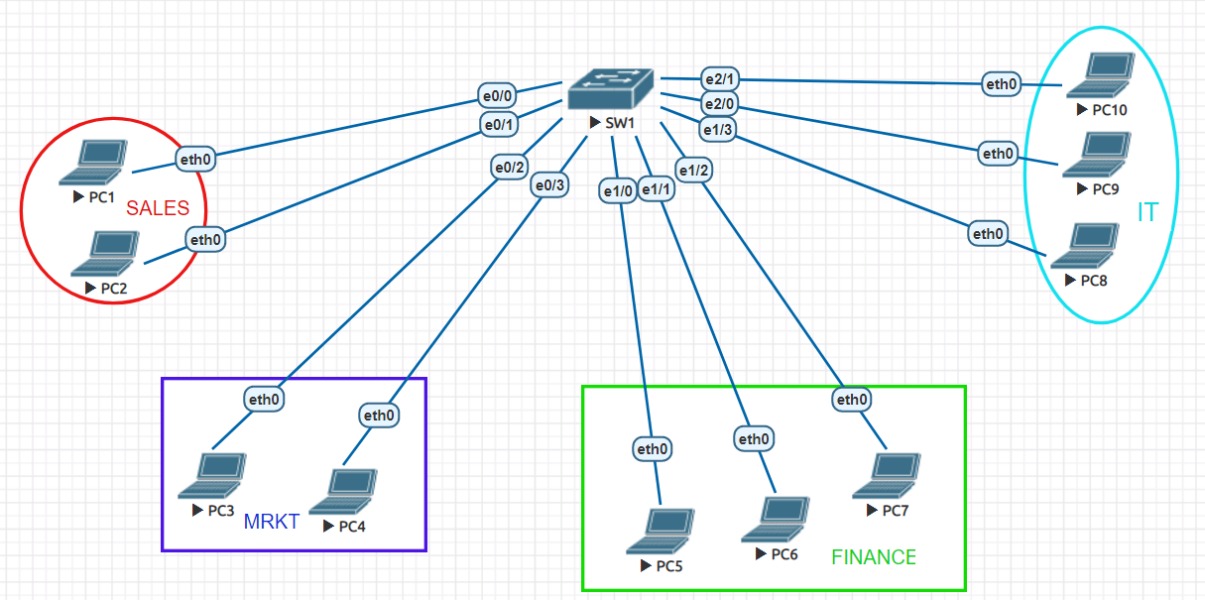
Contents

https://www.linkedin.com/in/gitesh-d-aa95a8227/

VLAN

VLAN stands for virtual local area network. VLAN is a technology we use for the purpose of Broadcast isolation or segregation of LAN .

Generally what happen in company there is so many department , for that each and every department require pc and to connect that pc we require Switch .If we buy different switch for each department the cost of IT infra will going to increase ,to save that cost company implement vlan on their switch.so here we go.



Task-1.1 Create VLAN

VLAN 10 sales

VLAN 20 mrkt

VLAN 30 finance

VLAN 40 IT

Task-1.2 IP Range

VLAN 10 - 192.168.10.0/27	For sales department require IP is 30
VLAN 20 - 192.168.20.0/26	For marketing department require IP is 42
VLAN 30 - 192.168.30.0/27	For finance department require IP is 25
VLAN 40 - 192.168.40.0/28	For IT department require IP is 14

Task-1.3 Assign VLAN to the respected port as per diagram & assign IP to the pc

https://www.linkedin.com/in/gitesh-d-aa95a8227/

SOLUTION

So, start first with the switch

Switch> enable

Switch#configure terminal

Step 1:- Now we have to create VLAN

Switch(config)#vlan 10
Switch(config)#name sales
Switch(config)#exit

Switch(config)#vlan 20
Switch(config)#name mrkt
Switch(config)#exit

Switch(config)#Vlan 30
Switch(config)#name finance
Switch(config)#exit

Switch(config)#vlan 40
Switch(config)#name IT
Switch(config)#exit

Step 2 :- Assignment of VLAN

Now open interface and assign VLAN

Switch(config)#interface ethernet 0/0
Switch(config)#Switchport mode access
Switch(config)#Switchport access vlan 10
Switch(config)#Exit

Switch(config)#interface ethernet 0/1
Switch(config)#switchport mode access
Switch(config)#switchport access vlan 10
Switch(config)#exit

Switch(config)#interface ethernet 0/2
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 20
Switch(config)# exit

Switch(config)#interface ethernet 0/3
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 20
Switch(config)# exit

Switch(config)#interface ethernet 1/0
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 30
Switch(config)# exit

Switch(config)#interface ethernet 1/1
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 30
Switch(config)# exit

Switch(config)#interface ethernet 1/2
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 30
Switch(config)# exit

Switch(config)#interface ethernet 1/3
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 40
Switch(config)# exit

Switch(config)#interface ethernet 2/0
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 40
Switch(config)# exit

Switch(config)#interface ethernet 2/1
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 40
Switch(config)# exit

Note- Assign IP to the respected VLAN Pc's

VERIFICATION

Switch# show vlan

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et2/2, Et2/3
10   sales                            active    Et0/0, Et0/1
20   mrkt                             active    Et0/2, Et0/3
30   finance                          active    Et1/0, Et1/1, Et1/2
40   IT                               active    Et1/3, Et2/0, Et2/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```


https://www.linkedin.com/in/gitesh-d-aa95a8227/

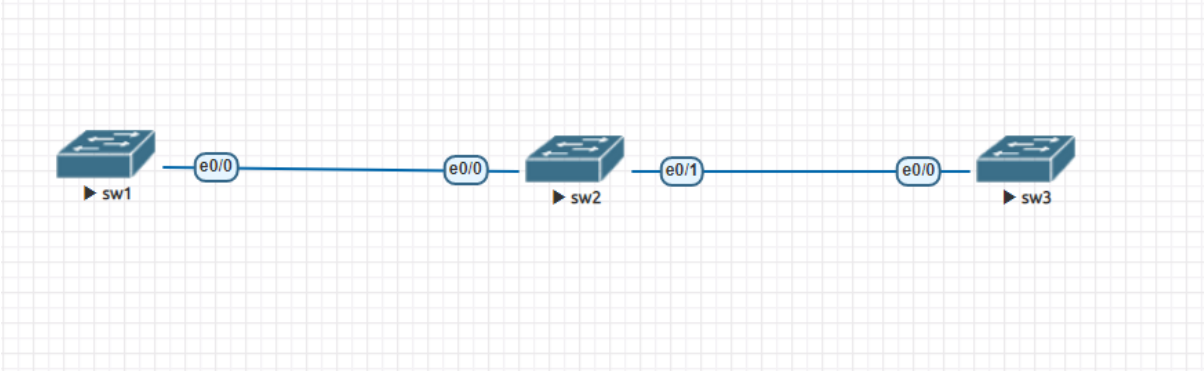
Switch# Show running-config

```
!
interface Ethernet0/0
 switchport access vlan 10
 switchport mode access
!
interface Ethernet0/1
 switchport access vlan 10
!
interface Ethernet0/2
 switchport access vlan 20
 switchport mode access
!
interface Ethernet0/3
 switchport access vlan 20
 switchport mode access
!
interface Ethernet1/0
 switchport access vlan 30
 switchport mode access
!
interface Ethernet1/1
 switchport access vlan 30
 switchport mode access
!
interface Ethernet1/2
 switchport access vlan 30
 switchport mode access
!
interface Ethernet1/3
 switchport access vlan 40
 switchport mode access
!
interface Ethernet2/0
 switchport access vlan 40
 switchport mode access
!
interface Ethernet2/1
 switchport access vlan 40
 switchport mode access
```

VTP

VTP stands for VLAN Trunking Protocol. why we use VTP? This is the important question we generally face. So, in the company there were almost 30-40 switches more or less. As engineer we need to configure each and every switch and if each switch has minimum 10 VLAN on it. It means 40 Switches x 10 VLAN per switch = 400 times you need create vlan.to reduce this task and to make all switches manageable we configure VTP.

So here we go,



Task 2.1- Create VLAN on sw1

Task 2.2- Make interface trunk on sw1 eth0/0 and sw2 eth0/0 & eth0/1 , sw3 eth0/0

Task 2.3- Configure VTP mode, vtp domain, vtp password on all switches.

SOLUTION

Task 2.1

sw1(config)#vlan 10
sw1(config-vlan)#name sales
sw1(config-vlan)#exit

sw1(config)#vlan 20
sw1(config-vlan)#name mrkt
sw1(config-vlan)#exit

sw1(config)#vlan 30
sw1(config-vlan)#name IT
sw1(config-vlan)#exit

sw1(config)#vlan 40
sw1(config-vlan)#name DC
sw1(config-vlan)#exit

Task 2.2

On switch 1

sw1(config)#interface ethernet0/0
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
sw1(config-if)#exit

On switch 2

sw2(config)#interface ethernet0/0
sw2(config-if)#switchport trunk encapsulation dot1q
sw2(config-if)#switchport mode trunk
sw2(config-if)#exit

sw2(config)#interface ethernet0/1
sw2(config-if)#switchport trunk encapsulation dot1q
sw2(config-if)#switchport mode trunk
sw2(config-if)#exit

On switch 3

sw3(config)#interface ethernet0/0
sw3(config-if)#switchport trunk encapsulation dot1q
sw3(config-if)#switchport mode trunk
sw3(config-if)#exit

Task 2.3

sw1(config)#vtp mode server
Device mode already VTP Server for VLANS.
sw1(config)#vtp domain ccn.com
Changing VTP domain name from NULL to ccn.com
sw1(config)#vtp password ccn@123
Setting device VTP password to ccn@123

sw2(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
sw2(config)#vtp domain ccn.com
Domain name already set to ccn.com.
sw2(config)#vtp password ccn@123
Setting device VTP password to ccn@123

sw3(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
sw3(config)#vtp domain ccn.com
Domain name already set to ccn.com.
sw3(config)#vtp password ccn@123
Setting device VTP password to ccn@123

VERIFICATION

Verification of #show vlan command

Sw1

```
sw1#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/1, Et0/2, Et0/3
10   sales                             active
20   mrkt                              active
30   IT                                active
40   DC                                active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Sw2

```
sw2#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/2, Et0/3
10   sales                             active
20   mrkt                              active
30   IT                                active
40   DC                                active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Sw3

```
sw3#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/1, Et0/2, Et0/3
10   sales                             active
20   mrkt                              active
30   IT                                active
40   DC                                active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Verification of #show vtp status command

Sw1

```
sw1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : ccn.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.1000
Configuration last modified by 0.0.0.0 at 6-1-22 11:38:59
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
Configuration Revision          : 4
MD5 digest                      : 0x4C 0xBB 0xB6 0x01 0x5F 0x0E 0x8D 0xE8
                                  0xC5 0xFC 0xD8 0x72 0x9B 0xB2 0xB5 0x46
```

Sw2

```
sw2#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : ccn.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.2000
Configuration last modified by 0.0.0.0 at 6-1-22 11:38:59

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
Configuration Revision          : 4
MD5 digest                      : 0x4C 0xBB 0xB6 0x01 0x5F 0x0E 0x8D 0xE8
                                  0xC5 0xFC 0xD8 0x72 0x9B 0xB2 0xB5 0x46
```

Sw3

```
sw3#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : ccn.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.4000
Configuration last modified by 0.0.0.0 at 6-1-22 11:38:59

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
Configuration Revision          : 4
MD5 digest                      : 0x4C 0xBB 0xB6 0x01 0x5F 0x0E 0x8D 0xE8
                                  0xC5 0xFC 0xD8 0x72 0x9B 0xB2 0xB5 0x46
```

Note – After VLAN data forwarding to each and every switch via vtp configuration we can assign VLAN to switchports with the help of Step 2 :- Assignment of VLAN

EtherChannel

EtherChannel is a technology use to Bundle/Aggregate the Link/Node/Port, with the use of some protocols such as LACP or PAgP.
Why we use EtherChannel?
When we face lack of bandwidth with links then at that time we configure EtherChannel to bundle the link and get combined speed. Like each interface is ethernet means 10MBPS of each then, if we bundle 3 link at a time then the combine speed will be 300 MBPS

EtherChannel uses PAgP or LACP as a Negotiation Protocol

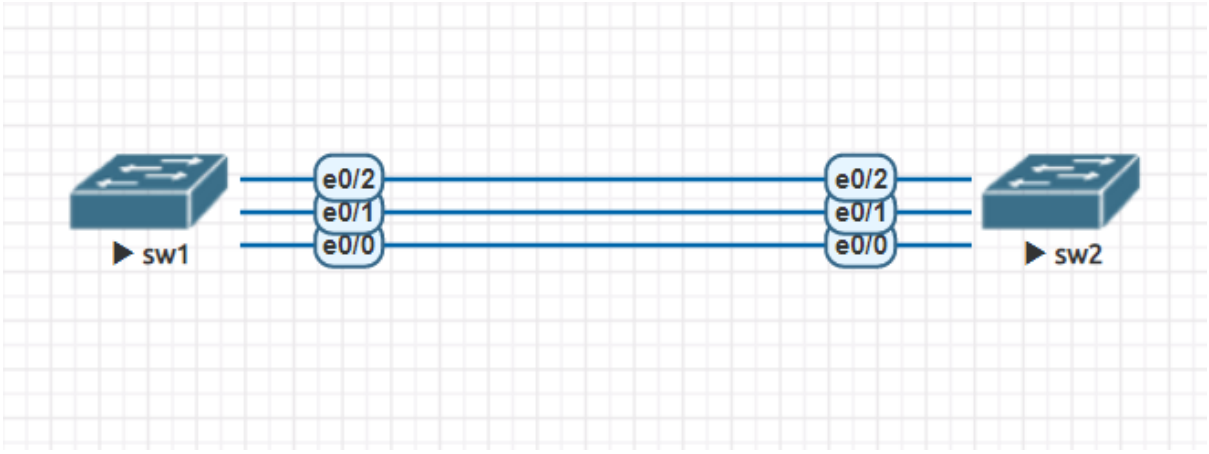
LINK AGGREGATION CONTROL PROTOCOL (LACP)

- LACP was made by IEEE and define with code of 802.3ad
- LACP is a Open Source and support all vendors in the market
- LACP adds up LACPDU to establish a etherchannel
- LACP has two modes
  1. Active – enable LACP unconditionally
  2. passive – enable LACP when LACP device is detected

PORT AGGREGATION CONTROL PROTOCOL (PAgP)

- PAgP was made by cisco.
- PAgP is a Cisco Proprietary Protocol. Hence, it only supports cisco devices
- PAgP has two modes
  1. Desirable – enable PAgP unconditionally
  2. Auto – enable PAgP when PAgP device is detected

So here we go,



Task 3
Task 3.1 - Configure sw1 interface ethernet 0/0, 0/1, 0/2 for EtherChannel
Task 3.2 - Configure sw2 interface ethernet 0/0, 0/1, 0/2 for EtherChannel
Task 3.3 – Configure sw1 to sw2 link as a trunk

Solution,

Task 3.1

Sw1

sw1(config)#interface range ethernet 0/0-2
sw1(config)#channel-protocol lacp
sw1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
sw1(config-if-range)#exit

Task 3.2

sw2

sw2(config)#interface range ethernet 0/0-2
sw1(config)#channel-protocol lacp
sw2(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
sw2(config-if-range)#exit

Task 3.3

Sw1

sw1(config)#interface range ethernet 0/0-2
sw1(config-if-range)#switchport trunk encapsulation dot1q
sw1(config-if-range)#switchport mode trunk
sw1(config-if-range)#exit

OR

sw1(config)#interface port-channel 1
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
sw1(config-if)#exit

sw2

sw2(config)#interface range ethernet 0/0-2

sw2(config-if-range)#switchport trunk encapsulation dot1q

sw2(config-if-range)#switchport mode trunk

sw2(config-if-range)#exit

VERIFICATION

Sw1

```
sw1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et0/0(P)    Et0/1(P)    Et0/2(P)
```

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
```

sw2

```
sw2#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et0/0(P)    Et0/1(P)    Et0/2(P)
```

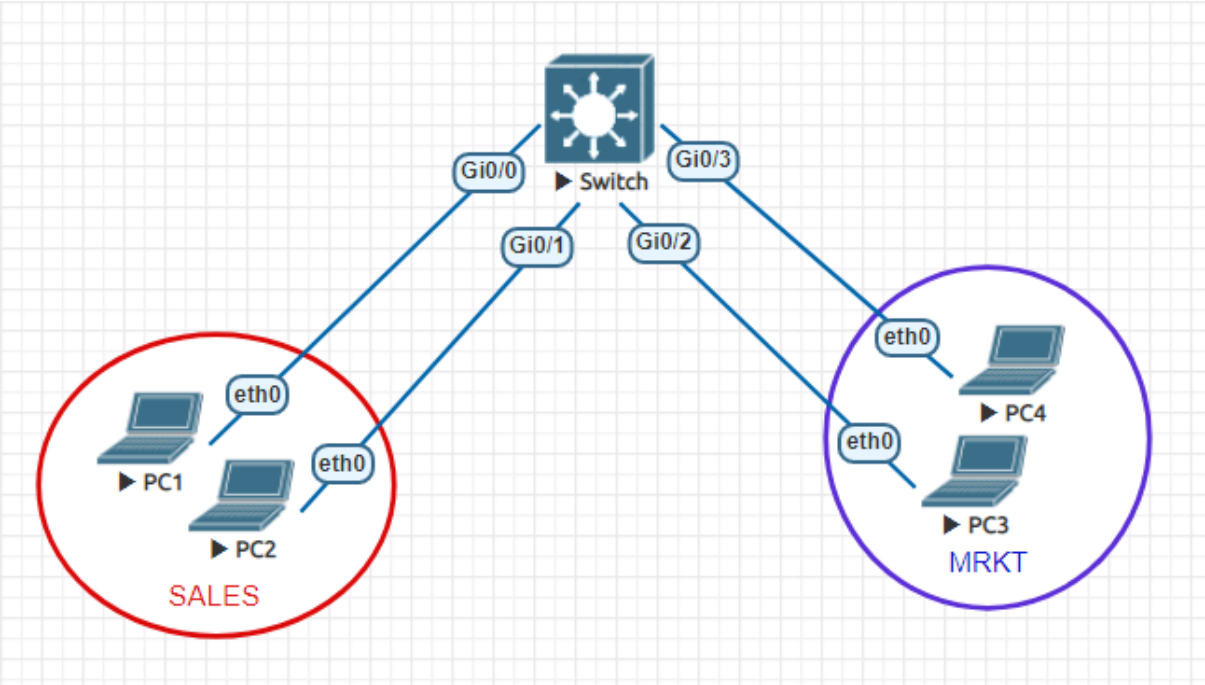
```
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
```


https://www.linkedin.com/in/gitesh-d-aa95a8227/

INTER VLAN ROUTING (IVR)

- Inter VLAN routing is method we use for the purpose of inter VLAN communication.
- Inter VLAN Routing is a new method to route between Multiple VLAN's.
- Inter VAN Routing require one device which is L3 Switch.

So here we go,



TASK

Task 4.1 Configure switch with VLAN 10 – SALES & VLAN 20 – MRKT

Task 4.2 Implement VLAN on the respected interface as per Diagram

Task 4.3 Create Default Gateway for the VLAN 10 & VLAN 20 PC's

Task 4.4 Assign IP to the PC

SOLUTION

Task 4.1 On switch,first we need to create vlan

Switch(config)#vlan 10
Switch(config-vlan)#name SALES
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name MRKT
Switch(config-vlan)#exit

Task 4.2 We need to apply vlan on interface

Switch(config)#interface range gigabitethernet0/0-1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range gigabitethernet0/2-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit

Task 4.3 Now, we need to configure interface vlan as a gateway for the PC's

Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config-if)#interface vlan 20
Switch(config-if)#ip address 192.168.20.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Note - Now IP given on interface VLAN, will become a gateway for the PC to communicate over the VLAN.

VERIFICATION

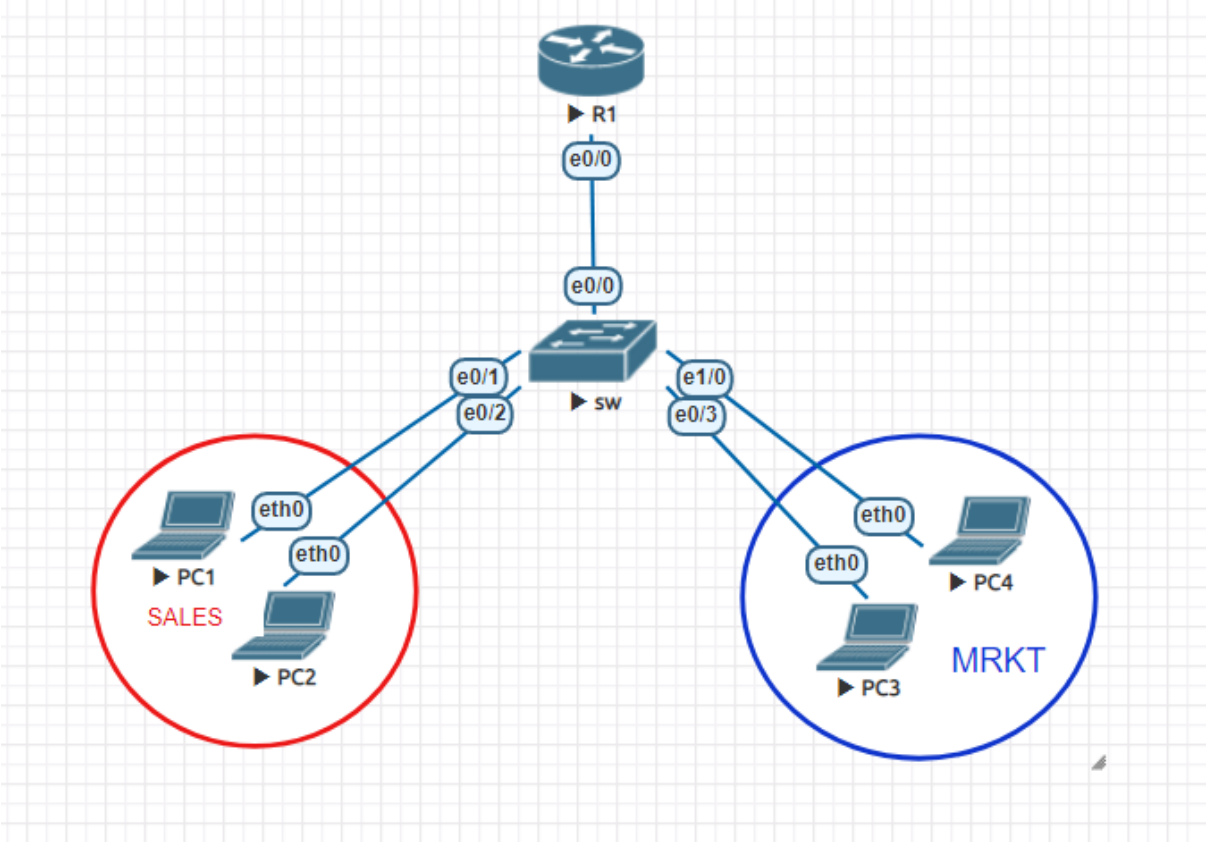
```
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
GigabitEthernet0/3     unassigned      YES unset  up                    up
GigabitEthernet1/0     unassigned      YES unset  up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  up                    up
GigabitEthernet1/3     unassigned      YES unset  up                    up
Vlan10                 192.168.10.254  YES manual up                    up
Vlan20                 192.168.20.254  YES manual up                    up
```

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0, Gi1/1, Gi1/2, Gi1/3
10   SALES                            active    Gi0/0, Gi0/1
20   MRKT                             active    Gi0/2, Gi0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

ROUTER ON STICK (ROAS)

- ❖ Router On Stick is also method to establish communication between two or more VLAN.
- ❖ Router On Stick configuration is old Method
- ❖ It requires 2 devices that is Router and L2 Switch

so here we go,



TASK

Task 5.1 Configure VLAN 10 – SALES & VLAN 20 – MRKT

TASK 5.2 Implement VLAN on respected interface

Task 5.3 Make interface Trunk which is connected to Router

Task 5.4 Create a gateway on Router

Task 5.5 Assign IP's to the PC of respected VLAN

SOLUTION

Task 5.1 First we need to Create VLAN

SW(config)#vlan 10
SW(config-vlan)#name SALES
SW(config-vlan)#exit

SW(config)#vlan 20
SW(config-vlan)#name MRKT
SW(config-vlan)#exit

Task 5.2 We need to Assign VLAN

SW(config)#interface range ethernet 0/1-2
SW(config-if-range)#switchport mode access
SW(config-if-range)#switchport access vlan 10
SW(config-if-range)#exit

SW(config)#interface range ethernet 0/3 , ethernet 1/0
SW(config-if-range)#switchport mode access
SW(config-if-range)#switchport access vlan 20
SW(config-if-range)#exit

Task 5.3 Now we have to create trunk

SW(config)#interface ethernet 0/0
SW(config-if)#switchport trunk encapsulation dot1q
SW(config-if)#switchport mode trunk
SW(config-if)#exit

Task 5.4 Now, configure router

R1(config)#interface ethernet0/0
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface ethernet0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.254 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#exit

R1(config)#interface ethernet0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.254 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#exit

VERIFICATION

On Router

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES unset  up                    up
Ethernet0/0.10             192.168.10.254  YES manual up                    up
Ethernet0/0.20             192.168.20.254  YES manual up                    up
Ethernet0/1                unassigned      YES unset  administratively down down
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
```

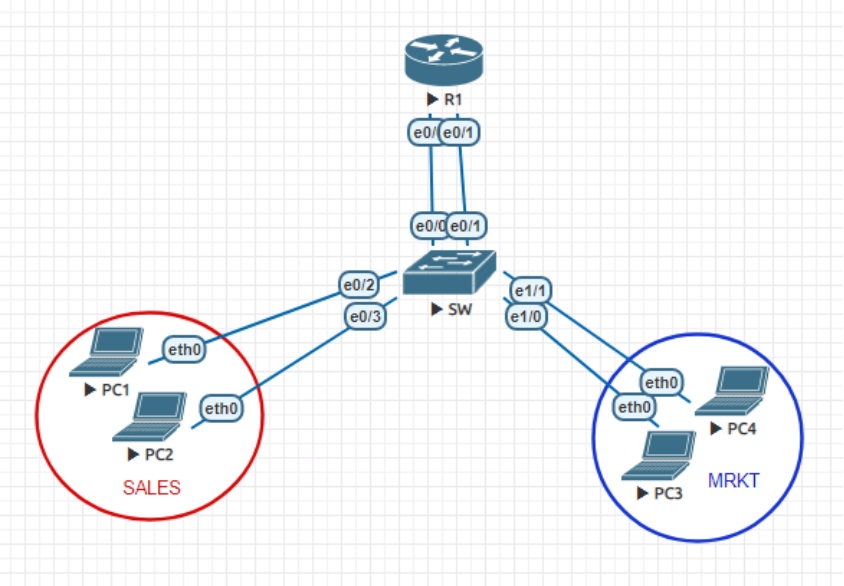
```
R1#show running-config | section interface Ethernet0/0
interface Ethernet0/0
 no ip address
interface Ethernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.254 255.255.255.0
interface Ethernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.254 255.255.255.0
```

On Switch

```
SW#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/1, Et1/2, Et1/3
10   SALES                            active    Et0/1, Et0/2
20   MRKT                             active    Et0/3, Et1/0
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
SW#  show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,10,20
```

METHOD 2



Creation of VLAN

SW(config)#vlan 10
SW(config-vlan)#name SALES
SW(config-vlan)#exit
SW(config)#vlan 20
SW(config-vlan)#name MRKT
SW(config-vlan)#exit

VLAN Assignment

SW(config)#interface range ethernet 0/2-3
SW(config-if-range)#switchport mode access
SW(config-if-range)#switchport access vlan 10
SW(config-if-range)#exit
SW(config)#interface range ethernet 1/0-1
SW(config-if-range)#switchport mode access
SW(config-if-range)#switchport access vlan 20
SW(config-if-range)#exit

Configure switch interface which is connected to the router

SW(config)#interface ethernet 0/0
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 10
SW(config-if)#exit
SW(config)#interface ethernet 0/1

SW(config-if)#switchport mode access

SW(config-if)#switchport access vlan 20

SW(config-if)#exit

Now, configure router

R1(config)#interface ethernet 0/0

R1(config-if)#ip address 192.168.10.254 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface ethernet 0/1

R1(config-if)#ip address 192.168.20.254 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

NOTE:-In this method we are not configuring only one interface for multiple VLAN rather we are configuring multiple interfaces for multiple VLAN .that's why here we are not configuring trunk interface.

VERIFICATION

On Switch

```
SW#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/2, Et1/3
10   sales                            active    Et0/0, Et0/2, Et0/3
20   MRKT                             active    Et0/1, Et1/0, Et1/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

On Router

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.10.254  YES manual up                    up
Ethernet0/1                192.168.20.254  YES manual up                    up
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
```

```
R1#show running-config | section interface Ethernet
interface Ethernet0/0
 ip address 192.168.10.254 255.255.255.0
interface Ethernet0/1
 ip address 192.168.20.254 255.255.255.0
interface Ethernet0/2
 no ip address
 shutdown
interface Ethernet0/3
 no ip address
 shutdown
```

SPANNING TREE PROTOCOL (STP)

Spanning tree is a loop prevention mechanism, generally used to stop broadcast storm in a Switch based network topology.it uses election method to select a ROOT BRIDGE in a switch network to have control over a switch network. if switch will able to choose a root bridge, then all the traffic passes through that root bridge where, it uses

STEP-1 SELECTION OF ROOT BRIDGE

1.lowest priority

- Default priority of every cisco switch is 32,768
- Then it adds up a VLAN ID so default VLAN is 1, hence ultimate value become a 32,769 (32,768+1)
- So, the default priority of every switch is same hence it tie up this criteria ,then the next criteria is

2.lowest MAC address

The first question is how to calculate lowest mac address

Here it is, MAC address is Hexadecimal value consist of numbers and alphabets

0 1 2 3 4 5 6 7 8 9 A B C D E F

HERE 0 IS LOWEST, THEN MOVE IT FORWARD TO F IS HIGHEST

NOTE:- IF LOWEST PRORITY HIT THEN ROOT BRIDGE SELECTED ON THE BASIS OF LOWEST PRIORITY, IF THAT CRITERIA TIE UP THEN MOVE FORWARD TO LOWEST MAC ADDRESS.

STEP-2 SELECTION OF ROOT PORT

Root port get selected on the basis of port cost which is already assigned on interfaces

Default Port Cost of interface

INTERFACE TYPE	PORT COST
ETHERNET (10MBPS)	100
FAST ETHERNET (100 MBPS)	19
1 GIGABIT ETHERNET (1 GBPS)	4
10 GIGABIT ETHERNET (10 GBPS)	2

Root port defines the nearest path to reach the destination

So, the rule is

Root port ⇔ designated port [RP=DP]

Designated port ⇔ root port or block port [DP=RP / DP=BP]

Root bridge has each port as designated port, and ports on other switches can be root port or block port

https://www.linkedin.com/in/gitesh-d-aa95a8227/

STEP -3 SELECTION OF BLOCK PORT

In the process of selection of block port switch uses a lowest priority and lowest MAC address criteria again, the same criteria applied here as it is. If the lowest priority is equal, then it move toward the lowest mac address.

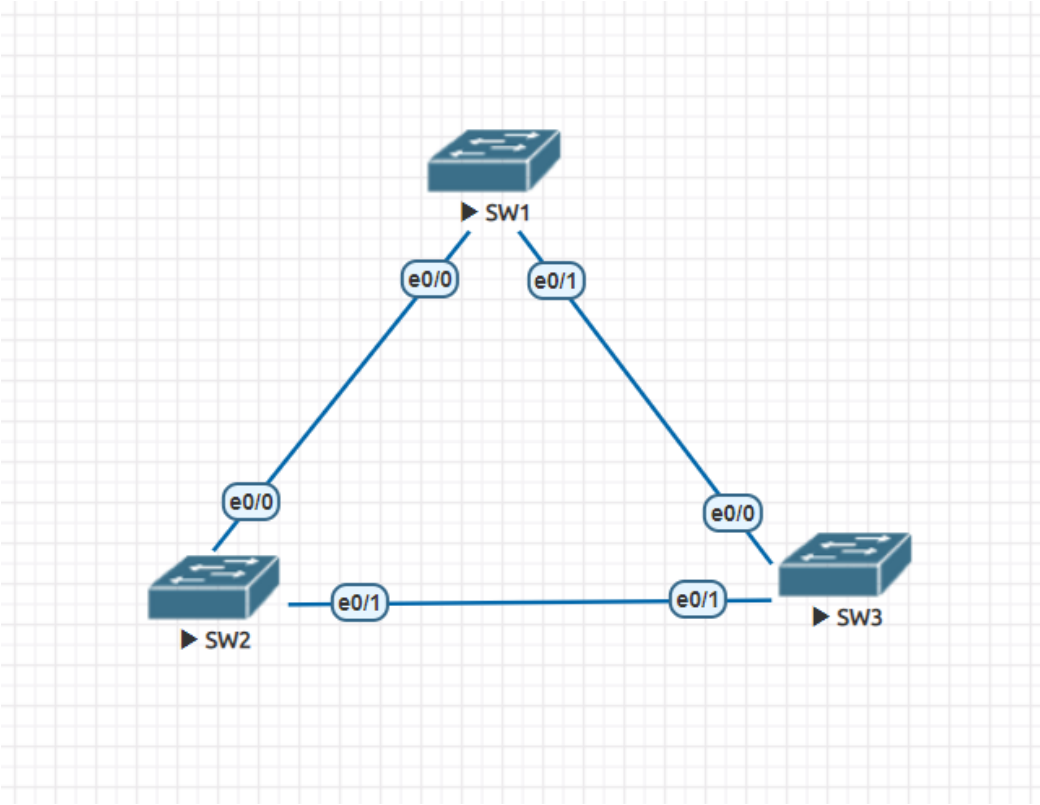
TASK 6

Task 6.1 Verify the root bridge

Task 6.2 Change the root bridge

Task 6.3 Change the port cost

So, let's start



In this picture

Sw-1 Will become a root bridge

```
SW-1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     aabb.cc00.1000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     aabb.cc00.1000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
```

Now see switch 1 has all port ad designated port

Now, we are going to change root bridge

We going to plan switch 2 must be root bridge and if switch 2 fails in network switch 3 will become a root bridge

```
SW-2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     aabb.cc00.1000
             Cost        100
             Port        1 (Ethernet0/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     aabb.cc00.2000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Et0/0               Root FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
```

In this switch 2 configuration we can clearly see eth 0/0 selected as root port cause the cost to reach the root bridge is only 100. if switch chooses other route it will take 200 cost, to reach the destination. (from switch 2 >switch 3 > switch 1= 200 cost)

Same goes with switch 3

```
SW-3#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     aabb.cc00.1000
              Cost        100
              Port        1 (Ethernet0/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     aabb.cc00.3000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Et0/0               Root FWD 100       128.1    Shr
Et0/1               Altn BLK 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
```

In this switch eth0/0 will become a root bridge as the cost is 100, whereas if switch chooses a different path to reach the destination it will take more cost than usual (from switch 3 > switch 2 > switch 1= 200 cost)

Now what if we dedicatedly want to change the root bridge role from switch 1 to switch 2

So, we play with switch priority first because we won't change the mac address of the switches.

SW-2(config)#spanning-tree vlan 1 root primary

We make switch 2 as root bridge by giving above command

```
SW-2(config)#do show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    24577
              Address     aabb.cc00.2000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     aabb.cc00.2000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
```

As a result of that command switch 2 act as a root switch

Now,

SW-3(config)#spanning-tree vlan 1 root secondary

By giving this above command we make switch 3 as a secondary root switch means if switch 2 fails as a root bridge. Then, switch 3 will become a root bridge.

Now how to change path cost

```
SW-3(config)#do show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    24577
              Address     aabb.cc00.2000
              Cost        100
              Port        2 (Ethernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28673  (priority 28672 sys-id-ext 1)
              Address     aabb.cc00.3000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Root FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
```

See, switch 3 has root port as eth 0/1 after changing the path cost. we make other port as a root port

SW-3(config)#interface ethernet 0/0

SW-3(config-if)#spanning-tree cost 10

SW-3(config-if)#exit

By applying such command on switch 3 ethernet 0/0, switch 1 – ethernet 0/0 & 0/1, switch 2 ethernet 0/0 we create root port on switch 3 from 0/1 to 0/0

```
SW-3(config)#do show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    24577
              Address     aabb.cc00.2000
              Cost        20
              Port        1 (Ethernet0/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28673  (priority 28672 sys-id-ext 1)
              Address     aabb.cc00.3000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Root FWD 10        128.1    Shr
Et0/1               Altn BLK 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
```

ROUTING

Router is a device which we use for the purpose of routing. Now, there is a question what is routing. routing means to route a data packet between networks .in layman language routing means to show the path to the data packet.

here we go to the routing

routing has generally major two type

1. static routing
2. dynamic routing

STATIC ROUTING – In this method we as a network engineer, have to define each and every route to the destination on every router till the destination.

DYNAMIC ROUTING – In this method we as a network engineer, have to only advertise the network which is directly connected to router. Dynamic Routing has different types of protocol, some of them are RIPv1 , RIPv2 , EIGRP , OSPF , ETC

STATIC ROUTING

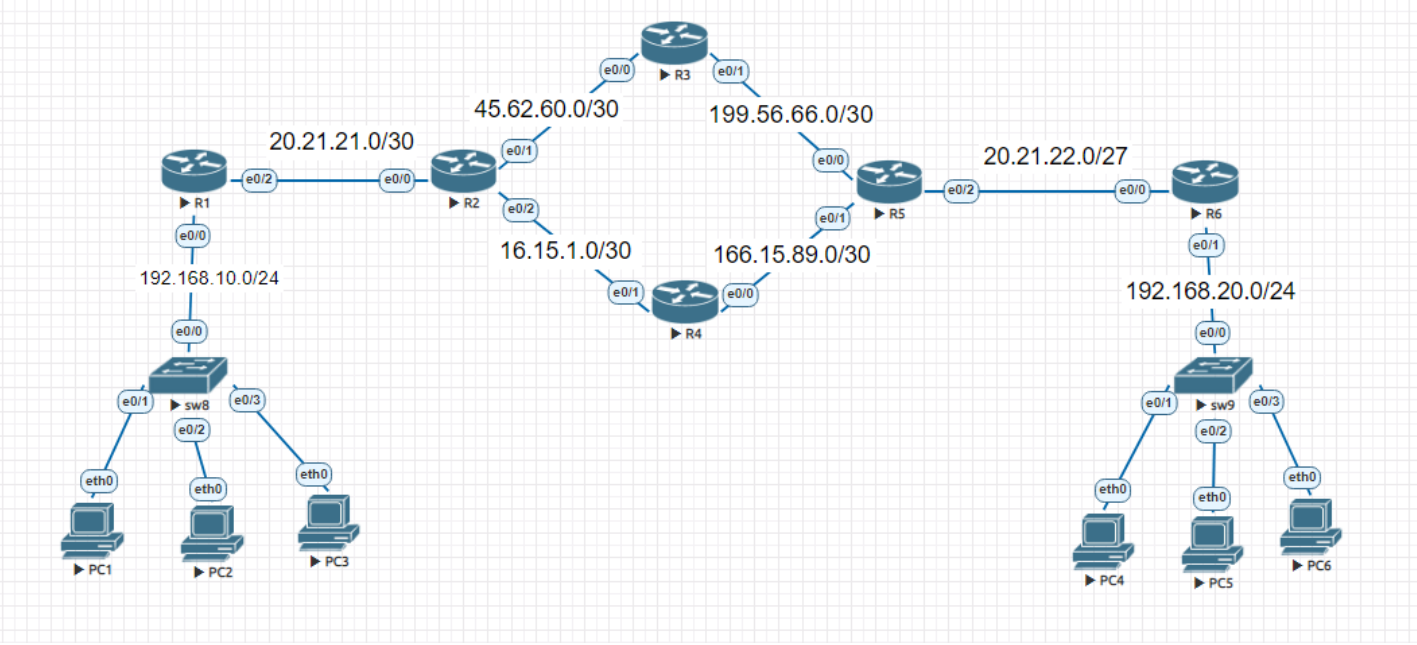
LET'S START WITH THE STATIC ROUTING FIRST

TASK-7

Task 7.1 provide hostname accordingly

Task 7.2 Assign IP address to interface

Task 7.3 Do static routing, PC-1,2,3 should communicate withPC-4,5,6



IN THE ABOVE LAB CONFIGURE THE GIVEN TASK

R1

Router(config)#hostname R1
R1(config)#interface ethernet 0/0
R1(config-if)#ip address 192.168.10.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface ethernet 0/2
R1(config-if)#ip address 20.21.21.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit

R2

Router(config)#hostname R2
R2(config)#interface ethernet 0/0
R2(config-if)#ip address 20.21.21.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface ethernet 0/1
R2(config-if)#ip address 45.62.60.1 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface ethernet 0/2
R2(config-if)#ip address 16.15.1.1 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit

R3

Router(config)#hostname R3
R3(config)#interface ethernet 0/0
R3(config-if)#ip address 45.62.60.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface ethernet 0/1
R3(config-if)#ip address 199.56.66.1 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit

R4

Router(config)#hostname R4
R4(config)#interface ethernet 0/1
R4(config-if)#ip address 16.15.1.2 255.255.255.252
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface ethernet 0/0
R4(config-if)#ip address 166.15.89.1 255.255.255.252
R4(config-if)#no shutdown
R4(config-if)#exit

R5

Router(config)#hostname R5
R5(config)#interface ethernet 0/0
R5(config-if)#ip address 199.56.66.2 255.255.255.252
R5(config-if)#no shutdown
R5(config-if)#exit
R5(config)#interface ethernet 0/1
R5(config-if)#ip address 166.15.89.2 255.255.255.252
R5(config-if)#no shutdown
R5(config-if)#exit
R5(config)#interface ethernet 0/2
R5(config-if)#ip address 20.21.22.1 255.255.255.224
R5(config-if)#no shutdown
R5(config-if)#exit

R6

Router(config)#hostname R6
R6(config)#interface ethernet 0/0
R6(config-if)#ip address 20.21.22.2 255.255.255.224
R6(config-if)#no shutdown
R6(config-if)#exit
R6(config)#interface ethernet 0/1
R6(config-if)#ip address 192.168.20.254 255.255.255.0
R6(config-if)#no shutdown
R6(config-if)#exit

Now, we have done with initial configuration part that is IP'S to the interface and hostname to router.

Well further we have to do is static routing. Let's start with it.

In static routing we have to define path to reach the destination.

Command for static routing

IP ROUTE <….Dest Network Address……> <……Dest Subnet Mask….> <Next hop ip address>

```
R1(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        20.21.21.0/30 is directly connected, Ethernet0/2
L        20.21.21.1/32 is directly connected, Ethernet0/2
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Ethernet0/0
L        192.168.10.254/32 is directly connected, Ethernet0/0
```

Before starting with routing there is no route to the destination of 192.168.20.0 network. so, we have to provide path for that network.

Start with R1,

R1(config)#ip route 192.168.20.0 255.255.255.0 20.21.21.2

Destination network address- 192.168.20.0

Destination subnet mask – 255.255.255.0

Next hop ip address – 20.21.21.2

After static routing command, there is an additional route start with "S"

```
      20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        20.21.21.0/30 is directly connected, Ethernet0/2
L        20.21.21.1/32 is directly connected, Ethernet0/2
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Ethernet0/0
L        192.168.10.254/32 is directly connected, Ethernet0/0
S     192.168.20.0/24 [1/0] via 20.21.21.2
```

Same thing we have to do with other routers, each router require path to reach the destination.

R2

R2(config)#ip route 192.168.20.0 255.255.255.0 45.62.60.2

R3

R3(config)#ip route 192.168.20.0 255.255.255.0 199.56.66.2

R5

R5(config)#ip route 192.168.20.0 255.255.255.0 20.21.22.2

We don't need to configure R6 cause R6 already has route which is directly connected to it. Represented with "C" in routing table.

```
      20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        20.21.22.0/27 is directly connected, Ethernet0/0
L        20.21.22.2/32 is directly connected, Ethernet0/0
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Ethernet0/1
L        192.168.20.254/32 is directly connected, Ethernet0/1
```

When data came in the network of 192.168.20.0/24 then the PC gives back echo-reply to the source device. Because we were trying to ping that network PC.

So, in this case source device is 192.168.10.1 in the network of 192.168.10.0/24, and to give back a reply we don't have return route to the 192.168.10.0/24 network. Now we need to provide path to the destination network of 192.168.10.0/24.

R6

R6(config)#ip route 192.168.10.0 255.255.255.0 20.21.22.1

R5

R5(config)#ip route 192.168.10.0 255.255.255.0 166.15.89.1

R4

R4(config)#ip route 192.168.10.0 255.255.255.0 16.15.1.1

R2

R2(config)#ip route 192.168.10.0 255.255.255.0 20.21.21.1

Now we don't need to provide path to the R1 for 192.168.10.0 network because that network is directly connected to R1.

Now provide IP to pc and verify it by doing ping

```
VPCS> ip 192.168.10.1/24 192.168.10.254
Checking for duplicate address...
PC1 : 192.168.10.1 255.255.255.0 gateway 192.168.10.254

VPCS> ping 192.168.20.1

84 bytes from 192.168.20.1 icmp_seq=1 ttl=59 time=4.758 ms
84 bytes from 192.168.20.1 icmp_seq=2 ttl=59 time=3.515 ms
84 bytes from 192.168.20.1 icmp_seq=3 ttl=59 time=3.374 ms
84 bytes from 192.168.20.1 icmp_seq=4 ttl=59 time=2.740 ms
84 bytes from 192.168.20.1 icmp_seq=5 ttl=59 time=3.145 ms
```

Done with the static routing.

DEFAULT ROUTING

we have done static routing here. now there is a concept called default routing which is a part of static routing. Default routing basically forwarding data to some given IP and then that data can be forwarded by the device which is holding a given IP with the help of their routing table. when we do default routing on edge router we only create one default entry rest of the work is done by other router. we use default routing entry when we connect router to internet. And on internet there is a lot of networks which we can't define so there we use default entry to push all the data packets to particular IP which is belongs to ISP and then ISP do the main routing stuff.

Considering the static routing lab, where R1 is companies edge router which is connected with multiple networks.

R1

R1(config)#ip route 0.0.0.0 0.0.0.0 20.21.21.2

Destination network address- 0.0.0.0 (UNKNOWN)

Destination subnet mask – 0.0.0.0 (UNKNOWN)

Next hop ip address – 20.21.21.2

Here we are telling the router that we don't know the path to reach the destination but we are forwarding that data on IP 20.21.21.2. So,20.21.21.2 can forward the data with their own routing table. Rest configuration is same.

ROUTING INFORMATION PROTOCOL (RIP)

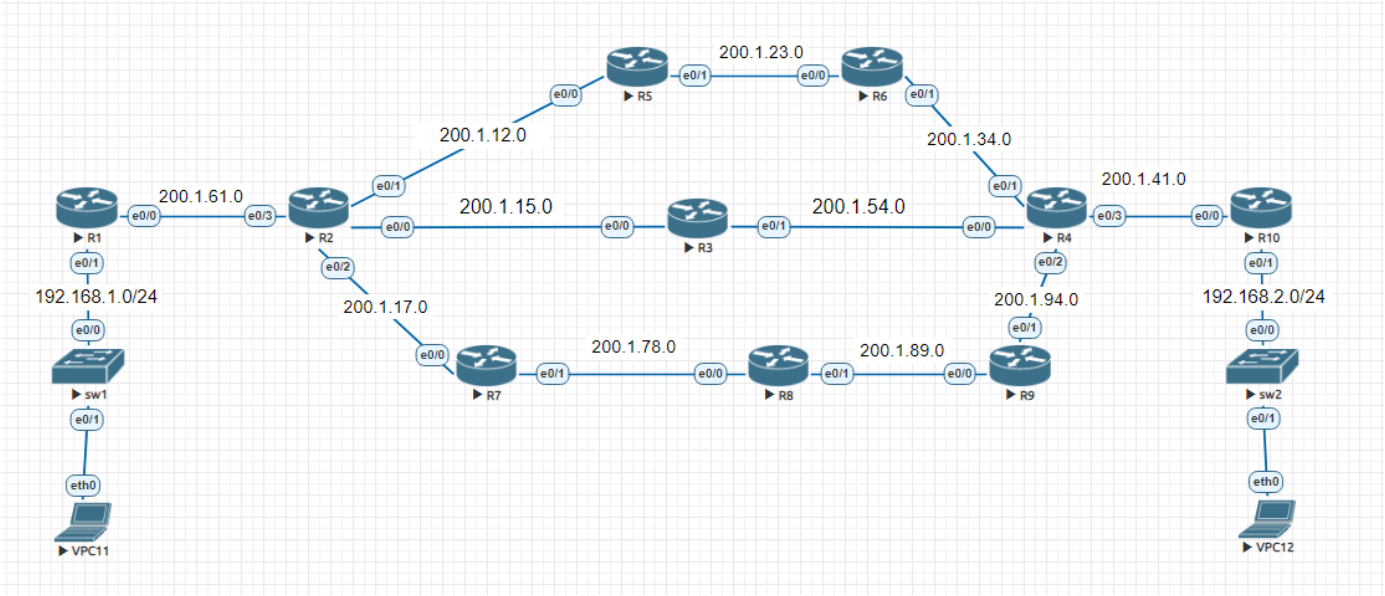
- Rip is a dynamic routing protocol
- Rip uses Bellman Ford Algorithm
- Rip supports max 15 hop count
- Rip has AD value of 120
- Rip has a periodic update timer of 30 sec
- Rip has flush timer of 240 sec out of which 180 sec is a hold down timer & 60 sec is path update timer.
- Rip has two version- version 1(RIPv1) & version 2(RIPv2)
- Ripv1 uses broadcast address to send messages, ripv1 do not support authentication
- Ripv2 has multicast address – 224.0.0.9, ripv2 support authentication.

TASK 8

Task 8.1 Assign hostname to the devices

Task 8.2 IP address to interfaces & pc's

Task 8.3 Configure Routing



FROM THE ABOVE GIVEN LAB ASSIGN IP ADDRESS ACCORDINGLING

R1-R2	200.1.61.0/24	R2-R7	200.1.17.0/24
R2-R3	200.1.15.0/24	R7-R8	200.1.78.0/24
R3-R4	200.1.54.0/24	R8-R9	200.1.89.0/24
R4-R10	200.1.41.0/24	R9-R4	200.1.94.0/24
R2-R5	200.1.12.0/24	R1 LAN	192.168.1.0/24
R5 -R6	200.1.23.0/24	R10 LAN	192.168.2.0/24
R6-R4	200.1.34.0/24	--	--

After Assigning Ip on The Interfaces, Let's Move Further to The Routing

R1

R1(config)#router rip

R1(config-router)#network 192.168.1.0

R1(config-router)#network 200.1.61.0

R1(config-router)#exit

Here, we only have to advertise the directly connected network on router.

R2

R2(config)#router rip

R2(config-router)#network 200.1.12.0

R2(config-router)#network 200.1.15.0

R2(config-router)#network 200.1.17.0

R2(config-router)#network 200.1.61.0

R2(config-router)#exit

Now, we go through R7 to verify how rip works

R7

R7(config)#router rip

R7(config-router)#network 200.1.17.0

R7(config-router)#network 200.1.78.0

R7(config-router)#exit

R8

R8(config)#router rip

R8(config-router)#network 200.1.78.0

R8(config-router)#network 200.1.89.0

R8(config-router)#exit

R9

R9(config)#router rip

R9(config-router)#network 200.1.89.0

R9(config-router)#network 200.1.94.0

R9(config-router)#exit

R4

R4(config)#router rip

R4(config-router)#network 200.1.34.0

R4(config-router)#network 200.1.54.0

R4(config-router)#network 200.1.94.0

R4(config-router)#network 200.1.41.0

R4(config-router)#exit

R10

R10(config)#router rip

R10(config-router)#network 200.1.41.0

R10(config-router)#network 192.168.2.0

R10(config-router)#exit

Lets try to do ping from pc1 – pc2

```
pc1> ping 192.168.2.1

84 bytes from 192.168.2.1 icmp_seq=1 ttl=58 time=5.210 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=58 time=3.513 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=58 time=3.774 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=58 time=3.974 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=58 time=3.007 ms
```

Now try to do tracing

```
pc1> trace 192.168.2.1
trace to 192.168.2.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.254   1.737 ms  2.019 ms  3.228 ms
 2   200.1.61.2   1.596 ms  1.690 ms  2.507 ms
 3   200.1.17.2   2.792 ms  4.085 ms  2.148 ms
 4   200.1.78.2   1.657 ms  1.949 ms  3.443 ms
 5   200.1.89.2   3.711 ms  2.698 ms  1.550 ms
 6   200.1.94.2   1.866 ms  1.955 ms  4.700 ms
 7   200.1.41.2   4.191 ms  2.329 ms  1.805 ms
 8   *192.168.2.1   3.163 ms (ICMP type:3, code:3, Destination port unreachable)
```

See in the above trace, router chooses a route of R1--R2--R7--R8--R9--R4--R10

Lets go to the R2 to check the route

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

R     192.168.1.0/24 [120/1] via 200.1.61.1, 00:00:18, Ethernet0/3
R     192.168.2.0/24 [120/5] via 200.1.17.2, 00:00:07, Ethernet0/2
      200.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
```

Router R2 chooses 200.1.17.2 path to reach the destination of 192.168.2.0 network

NOW CONFIGURE ROUTE OF R1—R2—R5—R6—R4—R10

R1—R2—R4—R10 were already configured. So, we have to configure the rest

R5

R5(config)#router rip

R5(config-router)#network 200.1.12.0

R5(config-router)#network 200.1.23.0

R5(config-router)#exit

R6

R6(config)#router rip

R6(config-router)#network 200.1.23.0

R6(config-router)#network 200.1.34.0

R6(config-router)#exit

NOW GO TO R2

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

R     192.168.1.0/24 [120/1] via 200.1.61.1, 00:00:23, Ethernet0/3
R     192.168.2.0/24 [120/4] via 200.1.12.2, 00:00:14, Ethernet0/1
      200.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
```

Now see R2 chooses 200.1.12.2 path to reach the destination of 192.168.2.0 network

pc1 tracing path to reach 192.168.2.1

```
pc1> trace 192.168.2.1
trace to 192.168.2.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.254   0.765 ms  1.730 ms  0.953 ms
 2   200.1.61.2   1.966 ms  1.198 ms  1.947 ms
 3   200.1.12.2   3.509 ms  3.366 ms  2.216 ms
 4   200.1.23.2   2.434 ms  2.088 ms  1.855 ms
 5   200.1.34.2   4.099 ms  4.993 ms  2.753 ms
 6   200.1.41.2   2.610 ms  1.971 ms  3.238 ms
 7   *192.168.2.1   9.625 ms (ICMP type:3, code:3, Destination port unreachable)
```

Now configure the path of R1—R2—R3—R4—R10

R3

R3(config)#router rip

R3(config-router)#network 200.1.15.0

R3(config-router)#network 200.1.54.0

R3(config-router)#exit

router R2 for routes update

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

R     192.168.1.0/24 [120/1] via 200.1.61.1, 00:00:23, Ethernet0/3
R     192.168.2.0/24 [120/3] via 200.1.15.2, 00:00:17, Ethernet0/0
      200.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
```

Now let's look at pc1 tracing

```
pc1> trace 192.168.2.1
trace to 192.168.2.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.254   0.731 ms  0.963 ms  0.646 ms
 2   200.1.61.2   2.170 ms  2.511 ms  1.038 ms
 3   200.1.15.2   3.672 ms  1.400 ms  2.135 ms
 4   200.1.54.2   1.572 ms  2.741 ms  3.123 ms
 5   200.1.41.2   6.363 ms  1.894 ms  1.711 ms
 6   *192.168.2.1   7.881 ms (ICMP type:3, code:3, Destination port unreachable)
```

So, here we are with the conclusion of RIP chooses lowest hop count path to reach the destination.

ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL(EIGRP)

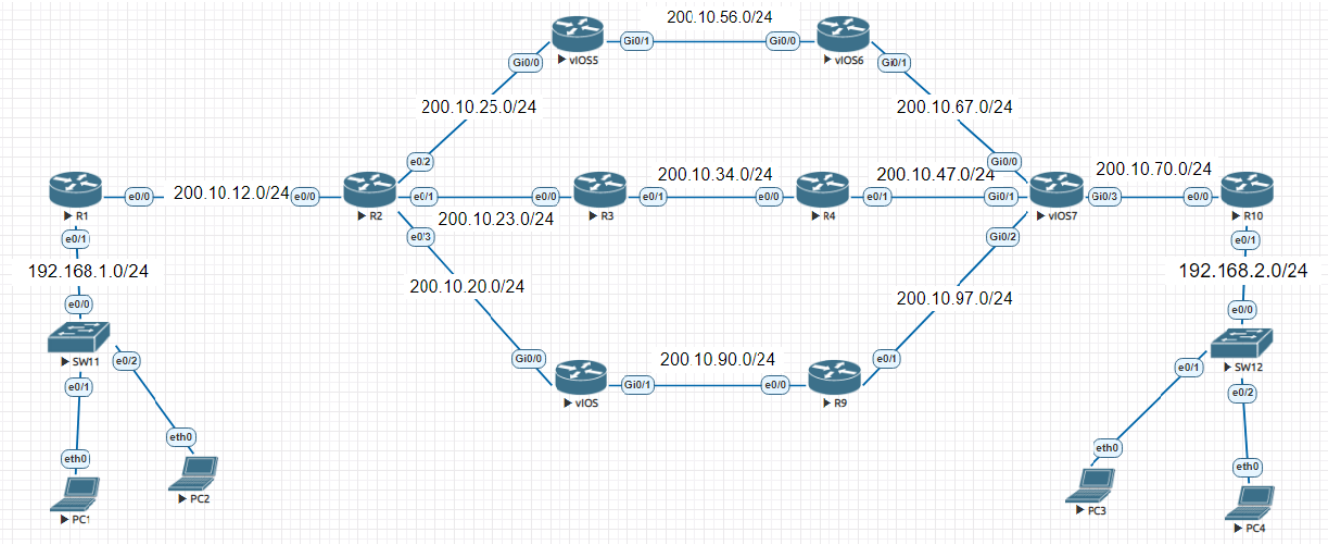
- Eigrp is a Dynamic routing protocol. Under this it is a Hybrid Protocol.
- Eigrp uses DUAL ALGORITHEM (Diffusing Update Algorithm)
- Eigrp support classless IP addressing, also support Authentication.
- Eigrp has AD value of 90
- Eigrp has hello timer of 5 sec and hold down timer is 15 sec. Eigrp do incremental update.
- Eigrp has Multicast address 224.0.0.10
- Eigrp has default hop count is 100. We can increase the limit till 255 hops.
- Eigrp uses Metric : Bandwidth + Delay (+MTU+Reliability+load)
- Eigrp make three table :- 1.Neighbor table 2.Topology table 3.Routing table

TASK 9

Task 9.1 Assign ip to the interfaces

Task 9.2 Assign hostname on devices

Task 9.3 Configure EIGRP routing



Assign ip and hostname to the devices

Now lets move to the Routing part

Firstly we choose middle part to route data (R1—R2—R3—R4—vIOS7—R10)

R1

R1(config)#router eigrp 100

R1(config-router)#network 192.168.1.0 0.0.0.255

R1(config-router)#network 200.10.12.0 0.0.0.255

R1(config-router)#exit

R2

R2(config)#router eigrp 100
R2(config-router)#network 200.10.12.0 0.0.0.255
R2(config-router)#network 200.10.25.0 0.0.0.255
R2(config-router)#network 200.10.23.0 0.0.0.255
R2(config-router)#network 200.10.20.0 0.0.0.255
R2(config-router)#exit

R3

R3(config)#router eigrp 100
R3(config-router)#network 200.10.23.0 0.0.0.255
R3(config-router)#network 200.10.34.0 0.0.0.255
R3(config-router)#exit

R4

R4(config)#router eigrp 100
R4(config-router)#network 200.10.34.0 0.0.0.255
R4(config-router)#network 200.10.47.0 0.0.0.255
R4(config-router)#exit

vIOS7

vISO7(config)#router eigrp 100
vISO7(config-router)#network 200.10.47.0 0.0.0.255
vISO7(config-router)#network 200.10.67.0 0.0.0.255
vISO7(config-router)#network 200.10.97.0 0.0.0.255
vISO7(config-router)#network 200.10.70.0 0.0.0.255
vISO7(config-router)#exit

R10

R10(config)#router eigrp 100
R10(config-router)#network 200.10.70.2 0.0.0.255
R10(config-router)#network 192.168.2.0 0.0.0.0.255
R10(config-router)#network 192.168.2.0 0.0.0.255
R10(config-router)#exit

Now lets ping from PC1 – PC3

```
PC1> ping 192.168.2.1

84 bytes from 192.168.2.1 icmp_seq=1 ttl=58 time=33.137 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=58 time=6.274 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=58 time=16.597 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=58 time=14.116 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=58 time=12.713 ms
```

Now trace for path

```
PC1> trace 192.168.2.1
trace to 192.168.2.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.254   2.678 ms  5.613 ms  0.790 ms
 2   200.10.12.2   4.754 ms  2.201 ms  1.600 ms
 3   200.10.23.2   2.589 ms  1.996 ms  2.432 ms
 4   200.10.34.2   3.744 ms  5.336 ms  2.788 ms
 5   200.10.47.2   10.887 ms  8.903 ms  8.951 ms
 6   200.10.70.2   5.661 ms  3.093 ms  8.780 ms
 7   *192.168.2.1   8.572 ms (ICMP type:3, code:3, Destination
 port unreachable)
```

Now we have to configure new path R1—R2—vIOS—R9—vIOS7—R10

vIOS

vIOS(config)#router eigrp 100

vIOS(config-router)#network 200.10.90.0 0.0.0.255

vIOS(config-router)#network 200.10.20.0 0.0.0.255

vIOS(config-router)#exit

R9

R9(config)#router eigrp 100

R9(config-router)#network 200.10.90.0 0.0.0.255

R9(config-router)#network 200.10.97.0 0.0.0.255

R9(config-router)#exit

Now eigrp chooses route of R1—R2—vIOS—R9—vIOS7—R10

trace from PC1 to PC3

```
PC1> trace 192.168.2.1
trace to 192.168.2.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.254   1.053 ms  0.569 ms  0.585 ms
 2   200.10.12.2   0.993 ms  0.797 ms  0.862 ms
 3   200.10.20.2   15.397 ms  6.707 ms  4.480 ms
 4   200.10.90.2   5.058 ms  8.661 ms  5.224 ms
 5   200.10.97.2   32.548 ms  12.786 ms  12.535 ms
 6   200.10.70.2   14.830 ms  15.371 ms  12.013 ms
 7   *192.168.2.1   13.717 ms (ICMP type:3, code:3, Destination port unreachable)
```

Now configure upper route

vIOS5

vISO5(config)#router eigrp 100

vISO5(config-router)#network 200.10.25.0 0.0.0.255

vISO5(config-router)#network 200.10.56.0 0.0.0.255

vISO5(config-router)#exit

vIOS6

vIOS6(config)#router eigrp 100

vIOS6(config-router)#network 200.10.56.0 0.0.0.255

vIOS6(config-router)#network 200.10.67.0 0.0.0.255

vIOS6(config-router)#exit

Now router R2 chooses a upper path

```
R2(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

D     192.168.1.0/24 [90/307200] via 200.10.12.1, 00:00:09, Ethernet0/0
D     192.168.2.0/24 [90/307968] via 200.10.25.2, 00:00:14, Ethernet0/2
      200.10.12.0/24 is variably subnetted, 2 subnets, 2 masks
```

Now let's trace from PC1 to PC3

```
PC1> trace 192.168.2.1
trace to 192.168.2.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.254   0.823 ms  0.648 ms  0.686 ms
 2   200.10.12.2   0.976 ms  1.823 ms  1.363 ms
 3   200.10.25.2   19.500 ms  4.837 ms  10.388 ms
 4   200.10.56.2   15.936 ms  8.064 ms  13.643 ms
 5   200.10.67.2   20.538 ms  18.308 ms  22.251 ms
 6   200.10.70.2   20.940 ms  17.046 ms  13.785 ms
 7   *192.168.2.1   20.780 ms (ICMP type:3, code:3, Destination port unreachable)
```

OPEN SHORTEST PATH FIRST (OSPF)

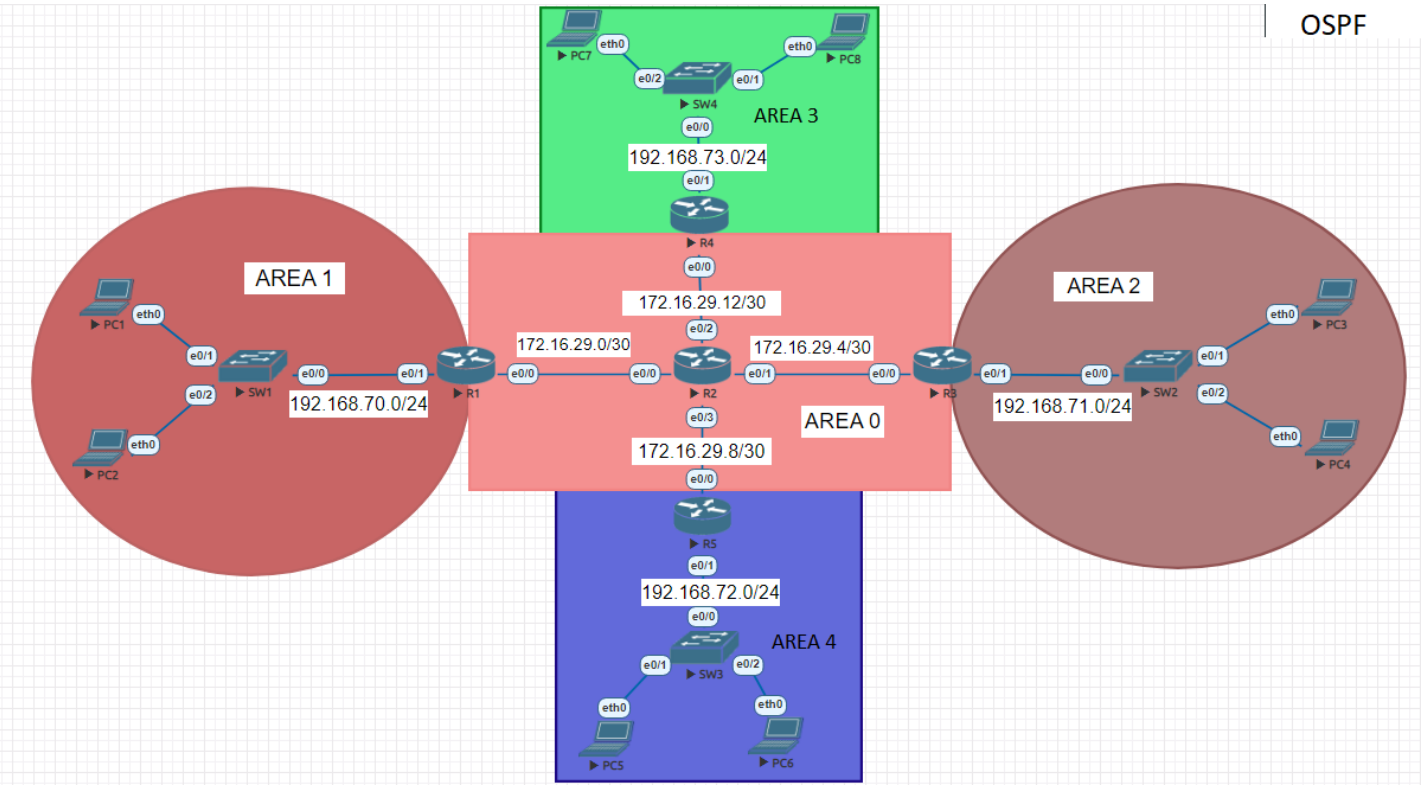
- OSPF is dynamic routing protocol, under this ospf is a link state protocol.
- OSPF uses DIJKSTRA ALGORITHM or SPF (SHORTEST PATH FIRST) ALGORITHEM
- OSPF has AD value of 110
- OSPF uses multicast address 224.0.0.5 and 224.0.0.6
- OSPF supports classless routing and also supports authentication
- OSPF creates 3 Routing Table
    1. Neighbor table
    2. Database table
    3. Routing table
- OSPF do trigger update (incremental update + every 30 min whole routing table update)
- OSPF uses lowest bandwidth as a cost to reach the destination

TASK 10

Task 10.1 Assign IP to the interfaces

Task 10.2 Assign hostname on devices

Task 10.3 Configure OSPF routing



WE HAVE ALREADY GIVEN AN IP ADDRESS AND HOSTNAME TO THE DEVICES

R1

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                172.16.29.1     YES manual up                    up
Ethernet0/1                192.168.70.254  YES manual up                    up
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
```

R2

```
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                172.16.29.2     YES manual up                    up
Ethernet0/1                172.16.29.6     YES manual up                    up
Ethernet0/2                172.16.29.14    YES manual up                    up
Ethernet0/3                172.16.29.10    YES manual up                    up
```

R3

```
R3#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                172.16.29.5     YES manual up                    up
Ethernet0/1                192.168.71.254  YES manual up                    up
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
```

R4

```
R4#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                172.16.29.13    YES manual up                    up
Ethernet0/1                192.168.73.254  YES manual up                    up
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
```

R5

```
R5#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                172.16.29.9     YES manual up                    up
Ethernet0/1                192.168.72.254  YES manual up                    up
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
```

We done with the verification of ip and hostname on the devices

Let’s move to the OSPF configuration

R1

R1(config)#router ospf 100

R1(config-router)#network 192.168.70.0 0.0.0.255 area 1

R1(config-router)#network 172.16.29.0 0.0.0.3 area 0

R1(config-router)#exit

R2

R2(config)#router ospf 100

R2(config-router)#network 172.16.29.0 0.0.0.3 area 0

R2(config-router)#network 172.16.29.4 0.0.0.3 area 0

R2(config-router)#network 172.16.29.8 0.0.0.3 area 0

R2(config-router)#network 172.16.29.12 0.0.0.3 area 0

R2(config-router)#exit

R3

R3(config)#router ospf 100

R3(config-router)#network 172.16.29.4 0.0.0.3 area 0

R3(config-router)#network 192.168.71.0 0.0.0.255 area 2

R3(config-router)#exit

R4

R4(config)#router ospf 100

R4(config-router)#network 172.16.29.12 0.0.0.3 area 0

R4(config-router)# network 192.168.73.0 0.0.0.255 area 3

R4(config-router)#exit

R5

R5(config)#router ospf 100

R5(config-router)#network 172.16.29.8 0.0.0.3 area 0

R5(config-router)#network 192.168.72.0 0.0.0.255 area 4

R5(config-router)#exit

For VERIFICATION,

#show ip route

R1

```
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.16.29.0/30 is directly connected, Ethernet0/0
L        172.16.29.1/32 is directly connected, Ethernet0/0
O        172.16.29.4/30 [110/20] via 172.16.29.2, 00:11:15, Ethernet0/0
O        172.16.29.8/30 [110/20] via 172.16.29.2, 00:11:15, Ethernet0/0
O        172.16.29.12/30 [110/20] via 172.16.29.2, 00:11:03, Ethernet0/0
      192.168.70.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.70.0/24 is directly connected, Ethernet0/1
L        192.168.70.254/32 is directly connected, Ethernet0/1
O IA  192.168.71.0/24 [110/30] via 172.16.29.2, 00:09:58, Ethernet0/0
O IA  192.168.72.0/24 [110/30] via 172.16.29.2, 00:06:45, Ethernet0/0
```

R2

```
      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.16.29.0/30 is directly connected, Ethernet0/0
L        172.16.29.2/32 is directly connected, Ethernet0/0
C        172.16.29.4/30 is directly connected, Ethernet0/1
L        172.16.29.6/32 is directly connected, Ethernet0/1
C        172.16.29.8/30 is directly connected, Ethernet0/3
L        172.16.29.10/32 is directly connected, Ethernet0/3
C        172.16.29.12/30 is directly connected, Ethernet0/2
L        172.16.29.14/32 is directly connected, Ethernet0/2
O IA  192.168.70.0/24 [110/20] via 172.16.29.1, 00:16:53, Ethernet0/0
O IA  192.168.71.0/24 [110/20] via 172.16.29.5, 00:15:26, Ethernet0/1
O IA  192.168.72.0/24 [110/20] via 172.16.29.9, 00:12:13, Ethernet0/3
```

R3

```
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O        172.16.29.0/30 [110/20] via 172.16.29.6, 00:17:55, Ethernet0/0
C        172.16.29.4/30 is directly connected, Ethernet0/0
L        172.16.29.5/32 is directly connected, Ethernet0/0
O        172.16.29.8/30 [110/20] via 172.16.29.6, 00:17:55, Ethernet0/0
O        172.16.29.12/30 [110/20] via 172.16.29.6, 00:17:55, Ethernet0/0
O IA  192.168.70.0/24 [110/30] via 172.16.29.6, 00:17:55, Ethernet0/0
      192.168.71.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.71.0/24 is directly connected, Ethernet0/1
L        192.168.71.254/32 is directly connected, Ethernet0/1
O IA  192.168.72.0/24 [110/30] via 172.16.29.6, 00:14:31, Ethernet0/0
```

R4

```
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O        172.16.29.0/30 [110/20] via 172.16.29.14, 00:16:57, Ethernet0/0
O        172.16.29.4/30 [110/20] via 172.16.29.14, 00:16:57, Ethernet0/0
O        172.16.29.8/30 [110/20] via 172.16.29.14, 00:16:57, Ethernet0/0
C        172.16.29.12/30 is directly connected, Ethernet0/0
L        172.16.29.13/32 is directly connected, Ethernet0/0
O IA  192.168.70.0/24 [110/30] via 172.16.29.14, 00:16:57, Ethernet0/0
O IA  192.168.71.0/24 [110/30] via 172.16.29.14, 00:16:57, Ethernet0/0
O IA  192.168.72.0/24 [110/30] via 172.16.29.14, 00:15:39, Ethernet0/0
      192.168.73.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.73.0/24 is directly connected, Ethernet0/1
L        192.168.73.254/32 is directly connected, Ethernet0/1
```

R5

```
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O        172.16.29.0/30 [110/20] via 172.16.29.10, 00:16:37, Ethernet0/0
O        172.16.29.4/30 [110/20] via 172.16.29.10, 00:16:37, Ethernet0/0
C        172.16.29.8/30 is directly connected, Ethernet0/0
L        172.16.29.9/32 is directly connected, Ethernet0/0
O        172.16.29.12/30 [110/20] via 172.16.29.10, 00:16:37, Ethernet0/0
O IA  192.168.70.0/24 [110/30] via 172.16.29.10, 00:16:37, Ethernet0/0
O IA  192.168.71.0/24 [110/30] via 172.16.29.10, 00:16:37, Ethernet0/0
      192.168.72.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.72.0/24 is directly connected, Ethernet0/1
L        192.168.72.254/32 is directly connected, Ethernet0/1
```

We have verify the routing, now let's try to ping form PC1 to PC4

```
PC1> ping  192.168.71.2

84 bytes from 192.168.71.2 icmp_seq=1 ttl=61 time=5.260 ms
84 bytes from 192.168.71.2 icmp_seq=2 ttl=61 time=1.640 ms
84 bytes from 192.168.71.2 icmp_seq=3 ttl=61 time=2.058 ms
84 bytes from 192.168.71.2 icmp_seq=4 ttl=61 time=2.167 ms
84 bytes from 192.168.71.2 icmp_seq=5 ttl=61 time=2.199 ms
```

From PC1 to PC7

```
PC1> ping  192.168.73.1

84 bytes from 192.168.73.1 icmp_seq=1 ttl=61 time=4.014 ms
84 bytes from 192.168.73.1 icmp_seq=2 ttl=61 time=2.274 ms
84 bytes from 192.168.73.1 icmp_seq=3 ttl=61 time=3.176 ms
84 bytes from 192.168.73.1 icmp_seq=4 ttl=61 time=2.759 ms
84 bytes from 192.168.73.1 icmp_seq=5 ttl=61 time=2.184 ms
```

From PC1 to PC6

```
PC1> ping 192.168.72.2

84 bytes from 192.168.72.2 icmp_seq=1 ttl=61 time=4.491 ms
84 bytes from 192.168.72.2 icmp_seq=2 ttl=61 time=2.397 ms
84 bytes from 192.168.72.2 icmp_seq=3 ttl=61 time=2.732 ms
84 bytes from 192.168.72.2 icmp_seq=4 ttl=61 time=2.613 ms
84 bytes from 192.168.72.2 icmp_seq=5 ttl=61 time=3.566 ms
```

So, here we done with OSPF.

Till the time we have done routing with each single protocol like only lab with RIP/ EIGRP / OSPF individually. What if we want to do routing between multiple protocol like routing between RIP, EIGRP, OSPF at a same time, that's what we called "REDISTRIBUTION".

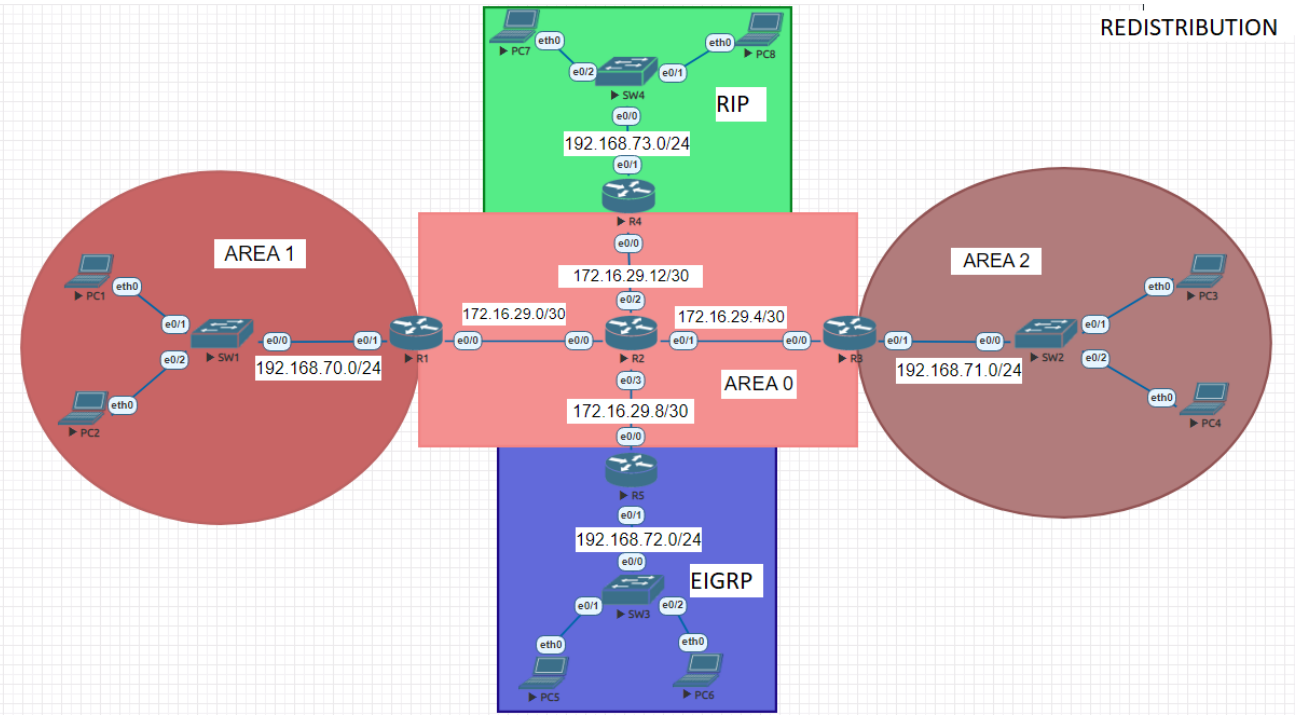
CONSIDER THIS LAB FOR REDISTRIBUTION

WE HAVE MADE SLIGHT CHANGES IN THE OSPF LAB FOR MAKE IT FIT FOR THE PURPOSE OF REDISTRIBUTION

TASK 10

Task 10.4 R4 ROUTER NOW PROCESS TWO PROTOCOL OF OSPF & RIPv2

Task 10.5 R5 ROUTER NOW PROCESS TWO PROTOCOL OF OSPF 100 & EIGRP 90



REST CONFIGURATION IS SAME.EXCEPT R4 and R5

R4

Interface ethernet 0/0 consist network of 172.16.29.12/30 will be advertise in OSPF and Interface ethernet 0/1 consist network of 192.168.73.0/24 will be advertise in RIP .

R4(config)#router ospf 100

R4(config-router)#network 172.16.29.13 0.0.0.3 area 0

R4(config-router)#exit

R4(config)#router rip

R4(config-router)#version 2

R4(config-router)#network 192.168.73.0

R4(config-router)#exit

See there is no route on R2 router for 192.168.73.0/24 network cause R2 is in ospf and 192.168.73.0/24 is in RIP

```
      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.16.29.0/30 is directly connected, Ethernet0/0
L        172.16.29.2/32 is directly connected, Ethernet0/0
C        172.16.29.4/30 is directly connected, Ethernet0/1
L        172.16.29.6/32 is directly connected, Ethernet0/1
C        172.16.29.8/30 is directly connected, Ethernet0/3
L        172.16.29.10/32 is directly connected, Ethernet0/3
C        172.16.29.12/30 is directly connected, Ethernet0/2
L        172.16.29.14/32 is directly connected, Ethernet0/2
O IA  192.168.70.0/24 [110/20] via 172.16.29.1, 01:08:29, Ethernet0/0
O IA  192.168.71.0/24 [110/20] via 172.16.29.5, 01:07:02, Ethernet0/1
```

Let's do it

R4(config)#router ospf 100

R4(config-router)#redistribute rip subnets

R4(config-router)#exit

R4(config)#router rip

R4(config-router)#redistribute ospf 100 metric 1

R4(config-router)#exit

Now see R2 will have 192.168.73.0/24 network in his routing table

```
      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.16.29.0/30 is directly connected, Ethernet0/0
L        172.16.29.2/32 is directly connected, Ethernet0/0
C        172.16.29.4/30 is directly connected, Ethernet0/1
L        172.16.29.6/32 is directly connected, Ethernet0/1
C        172.16.29.8/30 is directly connected, Ethernet0/3
L        172.16.29.10/32 is directly connected, Ethernet0/3
C        172.16.29.12/30 is directly connected, Ethernet0/2
L        172.16.29.14/32 is directly connected, Ethernet0/2
O IA  192.168.70.0/24 [110/20] via 172.16.29.1, 01:17:35, Ethernet0/0
O IA  192.168.71.0/24 [110/20] via 172.16.29.5, 01:16:08, Ethernet0/1
O E2  192.168.73.0/24 [110/20] via 172.16.29.13, 00:04:25, Ethernet0/2
```

R5

Interface ethernet 0/0 consist network of 172.16.29.8/30 will be advertise in OSPF and

Interface ethernet 0/1 consist network of 192.168.72.0/24 will be advertise in EIGRP .

R5(config)#router ospf 100

R5(config-router)#network 172.16.29.8 0.0.0.3 area 0

R5(config-router)#exit

R5(config)#router eigrp 90

R5(config-router)#network 192.168.72.0 0.0.0.255

R5(config-router)#exit

See there is no route on R2 router for 192.168.72.0/24 network cause R2 is in ospf and 192.168.72.0/24 is in EIGRP

```
      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.16.29.0/30 is directly connected, Ethernet0/0
L        172.16.29.2/32 is directly connected, Ethernet0/0
C        172.16.29.4/30 is directly connected, Ethernet0/1
L        172.16.29.6/32 is directly connected, Ethernet0/1
C        172.16.29.8/30 is directly connected, Ethernet0/3
L        172.16.29.10/32 is directly connected, Ethernet0/3
C        172.16.29.12/30 is directly connected, Ethernet0/2
L        172.16.29.14/32 is directly connected, Ethernet0/2
O IA  192.168.70.0/24 [110/20] via 172.16.29.1, 01:29:20, Ethernet0/0
O IA  192.168.71.0/24 [110/20] via 172.16.29.5, 01:27:53, Ethernet0/1
O E2  192.168.73.0/24 [110/20] via 172.16.29.13, 00:16:10, Ethernet0/2
```

Now we have to advertise EIGRP network in OSPF and vice versa

R5(config)#router eigrp 90

R5(config-router)#redistribute ospf 100 metric 10000 1000 255 255 1500

R5(config-router)#exit

Here 10000 is a bandwidth of interface,1000 is a delay of the ethernet interface,255 is a reliability,255 is a load, 1500 is MTU

R5(config)#router ospf 100

R5(config-router)#redistribute eigrp 90 subnets

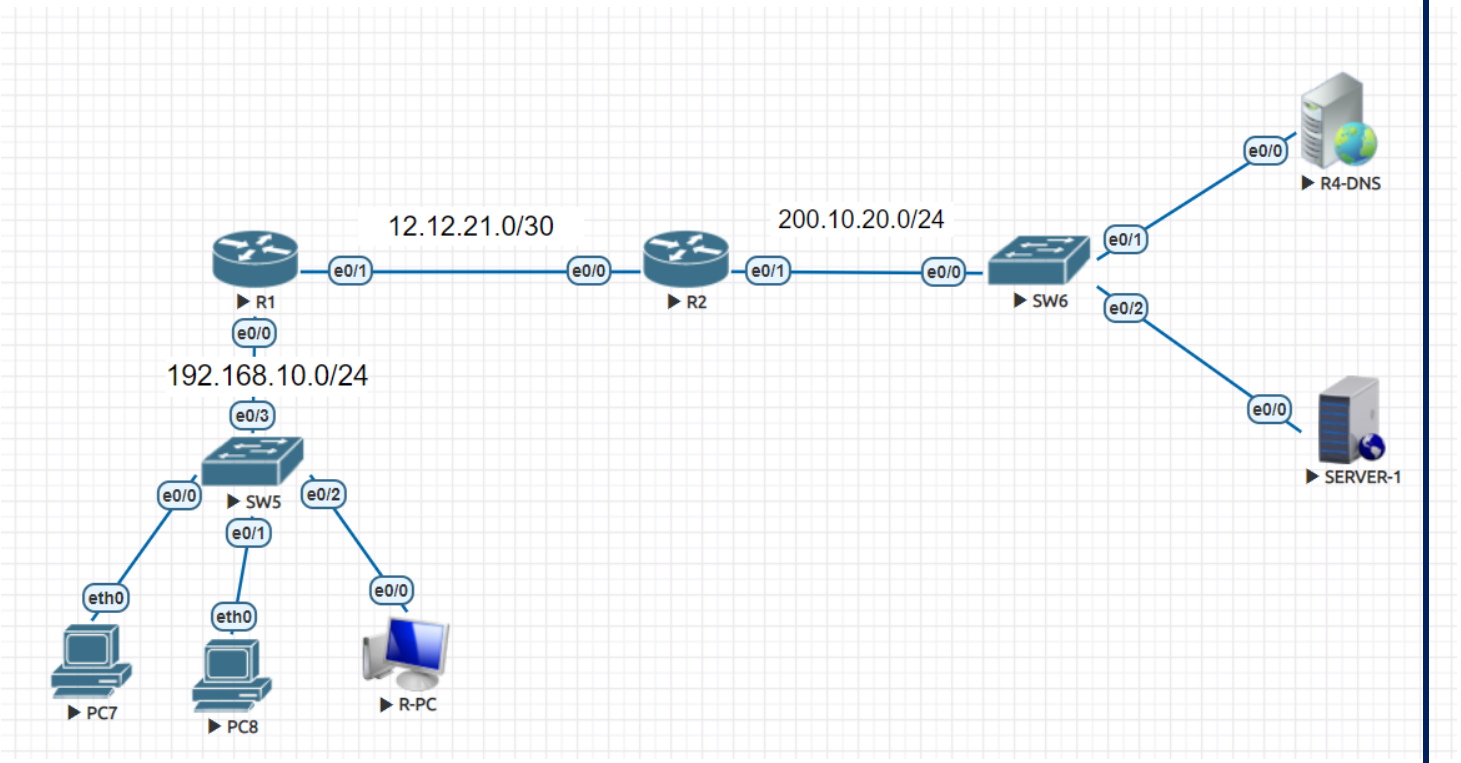
R5(config-router)#exit

Now we can see 192.168.72.0/24 network in R2's routing table

```
      172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.16.29.0/30 is directly connected, Ethernet0/0
L        172.16.29.2/32 is directly connected, Ethernet0/0
C        172.16.29.4/30 is directly connected, Ethernet0/1
L        172.16.29.6/32 is directly connected, Ethernet0/1
C        172.16.29.8/30 is directly connected, Ethernet0/3
L        172.16.29.10/32 is directly connected, Ethernet0/3
C        172.16.29.12/30 is directly connected, Ethernet0/2
L        172.16.29.14/32 is directly connected, Ethernet0/2
O IA  192.168.70.0/24 [110/20] via 172.16.29.1, 01:35:56, Ethernet0/0
O IA  192.168.71.0/24 [110/20] via 172.16.29.5, 01:34:29, Ethernet0/1
O E2  192.168.72.0/24 [110/20] via 172.16.29.9, 00:00:12, Ethernet0/3
O E2  192.168.73.0/24 [110/20] via 172.16.29.13, 00:22:46, Ethernet0/2
```

We have done with the REDISTRIBUTION task.

DHCP and DNS



IN THIS ABOVE LAB we are going to configure DHCP, DNS first

So what is DHCP (dynamic host configuration protocol), it is the protocol we generally used to assign IP address automatically.

And what is DNS (domain name system/server), it is the service we uses to resolve domain name to IP address .like if we put www.google.com in our web browser ,it redirect us to that website but in actual scenario we are heading towards the ip address of that perticullar web site instead .cause devices wont understand domain name rather they recognize ip address which is associated with that domain name just like

Example :- www.google.com = 142.250.183.4

TASK 11

Task 11.1 Configure R1 LAN network with the IP range of 192.168.10.0/24

Task 11.2 Assign ip to the pc through DHCP

Task 11.3 Then, do routing on all devices

Task 11.4 Configure R4-DNS as a DNS server

Task 11.5 Try to ping www.ccn.com which is SERVER-1

IP's of the devices

R1	Eth0/0 – 192.168.10.254/24	Eth0/1 – 12.12.21.1/30
R2	Eth0/0 – 12.12.21.2/30	Eth0/1 – 200.10.20.30/24
R4-DNS	ETH 0/0 – 200.10.20.10/24	
SERVER-1	ETH 0/0 – 200.10.20.20/24	

Let's do it

R1(config)#ip dhcp pool CCN-LAN

R1(dhcp-config)#network 192.168.10.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.10.254

R1(dhcp-config)#dns-server 200.10.20.10

R1(dhcp-config)#lease 0 12

R1(dhcp-config)#exit

- To configure DHCP we need 4 basic things that is IP, subnet mask, default gateway and DNS
- From network command we provide IP and subnet mask
- From default-router command we have provide a default gateway
- From DNS-SERVER command we provided a DNS server IP
- And by giving lease command we provided a lease period for that assigning IP

R1(config)#ip dhcp excluded-address 192.168.10.254

(If we want to remove any IP from that DHCP POOL, just to avoid duplicate IP's)

VERIFICATION

```
R1#show ip dhcp pool

Pool CCN-LAN :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.10.2         192.168.10.1     - 192.168.10.254    1
```

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.1        0100.5079.6668.07       Feb 15 2023 02:48 PM    Automatic
```

Then, how to ip to the VPC and R-PC

VPC

```
VPCS> ip dhcp
DDORA IP 192.168.10.1/24 GW 192.168.10.254
```

R-PC, this is actually a router considering and acting as a PC

R-PC(config)#interface ethernet 0/0

R-PC(config-if)#ip address dhcp

R-PC(config-if)#no shutdown

R-PC(config-if)#exit

To verify that give command

```
R-PC#show ip interface  brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.10.2    YES DHCP   up                    up
Ethernet0/1                unassigned      YES unset  administratively down down
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
```

3 so now do routing on all devices here we running eigrp on router you can do any routing

R1

R1(config)#router eigrp 100

R1(config-router)#network 192.168.10.0 0.0.0.255

R1(config-router)#network 12.12.21.0 0.0.0.3

R1(config-router)#exit

R2

R2(config)#router eigrp 100

R2(config-router)#network 12.12.21.0 0.0.0.3

R2(config-router)#network 200.10.20.0 0.0.0.255

R2(config-router)#exit

R-PC

R-PC(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.254

R-DNS

R4-DNS(config)#ip route 0.0.0.0 0.0.0.0 200.10.20.30

SERVER-1 (www.ccn.com)

www.ccn.com(config)#ip route 0.0.0.0 0.0.0.0 200.10.20.3

4 now start the dns server on R4-DNS

R4-DNS(config)#ip dns server

R4-DNS(config)#ip host www.ccn.com 200.10.20.20

First command is to start DNS server port number udp-53

And second command is to bind domain name with ip address

5 now ping the www.ccn.com consist ip 200.10.20.20

```
VPCS> ping www.ccn.com
www.ccn.com resolved to 200.10.20.20

84 bytes from 200.10.20.20 icmp_seq=1 ttl=253 time=7.019 ms
84 bytes from 200.10.20.20 icmp_seq=2 ttl=253 time=3.204 ms
84 bytes from 200.10.20.20 icmp_seq=3 ttl=253 time=4.116 ms
84 bytes from 200.10.20.20 icmp_seq=4 ttl=253 time=1.287 ms
84 bytes from 200.10.20.20 icmp_seq=5 ttl=253 time=4.267 ms
```

NETWORK TIME PROTOCOL (NTP)

- NTP is a network time uses UDP port -123
- Basically, NTP uses on all LAN as well as WAN devices just to sync time of their devices with NTP server, if time of those won't match then internet won't be able to work on that device.
- With the help of NTP we generate logs of the devices to solve the issues which generally occur in Enterprise environment. if time is mismatching then the troubleshoot will be more difficult.

We are going to consider lab which we used for the DHCP & DNS configuration

R2 (NTP Master)

R2(config)#interface loopback 1
R2(config-if)#ip address 10.10.10.1 255.255.255.255
R2(config-if)#no shutdown
R2(config-if)#exit

R2(config)#ntp master 1
R2(config)#ntp source loopback 1

Here we specify the NTP master stratum number 1 which mean it is most trusted NTP server in a network and we specify the source interface from where NTP broadcast will happen

R1(NTP Client)

R1(config)#ntp server 10.10.10.1

Here we specify the NTP servers ip address which is R2's loopback 1 interface ip address

Now the NTP authentication is totally optional

R1

R1(config)#ntp authentication-key 1 md5 ccn
R1(config)#ntp authenticate

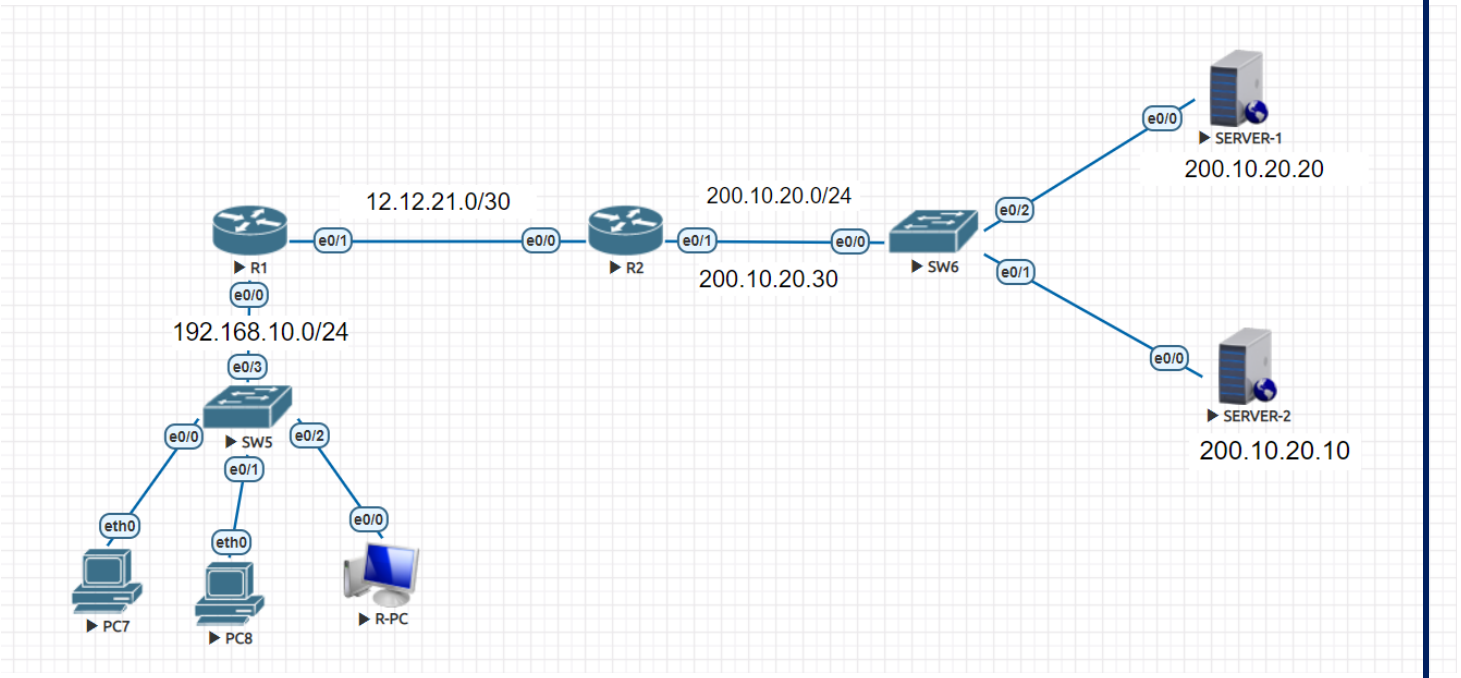
R2

R2(config)#ntp authentication-key 1 md5 ccn
R2(config)#ntp authenticate

VERIFICATION

R1#show ntp status OR R1#show ntp association

TELNET, SSH, HTTP, HTTPS



TELNET

Telnet is a remote access service works under TCP and uses port number 23 .generally telnet sends data in clear text format.

SSH

SSH is also a remote access service works under tcp and uses port number 22 . Genrally , ssh send data in encrypted format over the networks .it encrypts data through rsa algorithem , and consist key size of 2048 bit which is market standard.

Now configure the TELNET, SSH, HTTP, HTTPS on devices

Task 12

Task 12.1 Assign IP according to networks represents in diagram

Task 12.2 Configure SERVER 1 for TELENT service

Task 12.3 Configure SERVER 2 for SSH service

Task 12.4 Configure SERVER 1 for HTTP service

Task 12.5 Configure SERVER 2 for HTTPS service

R1	ETH 0/0 192.168.10.254/24		ETH 0/1 12.12.21.1/30
R1- INTERNAL NETWORK PC	PC7 192.168.10.1/24	PC8 192.168.10.2/24	R-PC 192.168.10.3/24
R2	ETH 0/0 12.12.21.2/24		ETH 0/1 200.10.20.30/24
SERVER 1	ETH 0/0 200.10.20.20/24		
SERVER 2	ETH 0/0 200.10.20.10		

NOW WE ARE CONFIGURING THE SERVER 1 FOR TELNET

ON SERVER 1

SERVER-1(config)#line vty 0 4

SERVER-1(config-line)#transport input telnet

SERVER-1(config-line)#login local

SERVER-1(config-line)#exit

Local username & password creation

SERVER-1(config)#username ccn privilege 15 password ccn

Here, line vty means virtual teletype which means a connection over a networks or connection which is virtual. console access is direct access but telnet access is virtual access on device. transport input telnet means the data travels over a network should only connect to a telnet service activated on a device .and, login local means at the time of login device should ask username & password which is verified from local user database which is created on device.

How to take access?

For that we need a router(R-PC) in eve-ng setup

Router# telnet <destination_ip_address> <desired_service_port>

```
R-PC#telnet 200.10.20.20 23
Trying 200.10.20.20 ... Open


User Access Verification

Username: ccn
Password:
SERVER-1#
```

SSH

SSH on server 2

SERVER-2(config)#line vty 0 4

SERVER-2(config-line)#transport input ssh

SERVER-2(config-line)#login local

SERVER-2(config-line)#exit

SERVER-2(config)#crypto key generate rsa modulus 2048 label mypubkey

Username & password

SERVER-2(config)#username ccn privilege 15 password ccn

Here line vty means virtual teletype which means a connection over a networks or connection which is virtual .then , 0 4 means at a time 5 line connection can be activate .transport input ssh means the data travels over a network should only connect to a ssh service activated on a device .and , login local means at the time of login device should ask username & password which is verified from local user database which is created on device. Crypto key command is to start the encryption process of the data through rsa algorithem with standard key 0f 2048 bit.

How to take access?

Router# ssh -l <username> <destination_ip_address>

```
R-PC#ssh -l ccn 200.10.20.10
Password:

SERVER-2#
SERVER-2#
SERVER-2#
```

HTTP

HTTP on server 1

SERVER-1(config)#ip http server

By applying above command, we are enabling TCP port 80 which we generally use to take GUI access.

VERIFICATION

Router# telnet <destination_ip_address> <desired_port>

With the command we get a output of [.....open] means http is enable on device

```
R-PC#telnet 200.10.20.20 80
Trying 200.10.20.20, 80 ... Open
```

HTTPS

https on server 2

SERVER-2(config)#ip http secure-server

By applying this command we are enabling tcp port 443 on device which we genrally use to take secure GUI access

To additional security we enable authentication

SERVER-2(config)#ip http authentication local

By applying this command we are enabling authentication on devices through local user database.

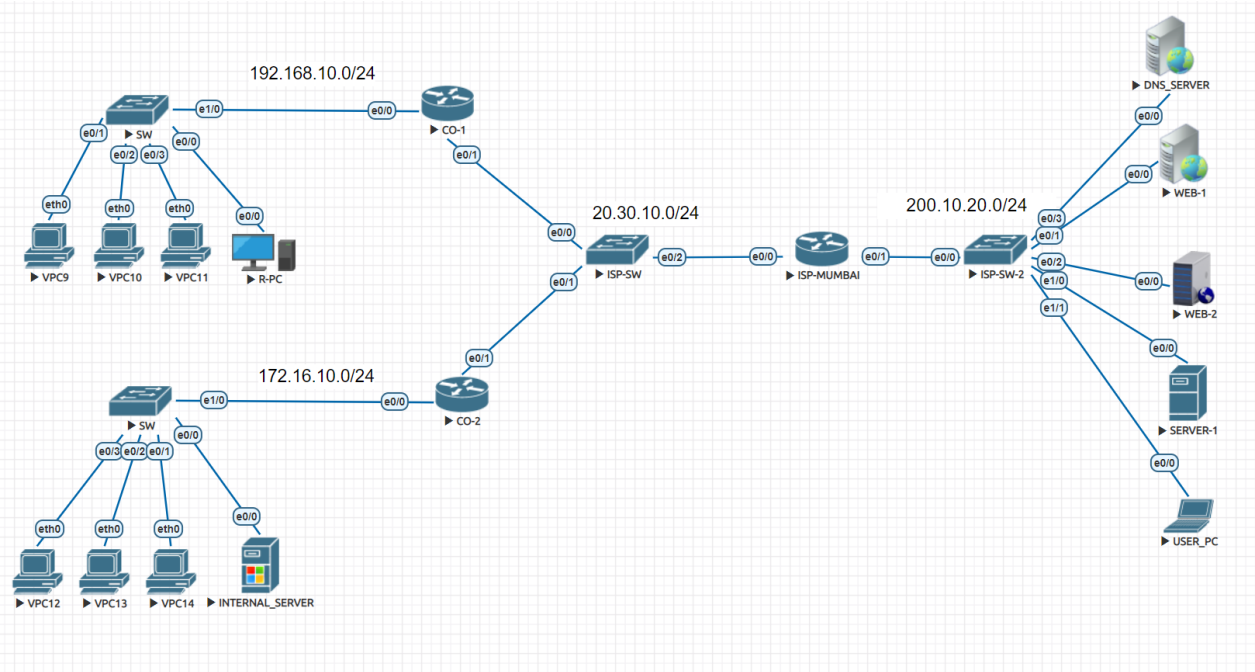
VERIFICATION

Router# telnet <destination_ip_address> <desired_port>

With the command we get a output of [.....open] means https is enable on device

```
R-PC#telnet 200.10.20.10 443
Trying 200.10.20.10, 443 ... Open
```

ACCESS-CONTROL LIST (ACL)



TASK - 13

Task 13.1 Provide IP to the devices.

SECTION	DEVICE NAME	IP ON INTERFACE
COMPANY - 1	CO-1	ETH0/0= 192.168.10.254/24 ETH0/1= 20.30.10.10/24
	VPC9	192.168.10.1/24
	VPC10	192.168.10.2/24
	VPC11	192.168.10.3/24
	R-PC	192.168.10.100/24
COMPANY - 2	CO-2	ETH0/0= 172.16.10.254/24 ETH 0/1 = 20.30.10.20/24
	VPC12	172.16.10.1/24
	VPC13	172.16.10.2/24
	VPC14	172.16.10.3/24
	INTERNAL_SERVER	172.16.10.100/24
ISP	ISP-MUMBAI	ETH0/0 = 20.30.10.30/24 ETH0/1= 200.10.20.10/24
OTHERS	DNS_SERVER	200.10.20.20/24
	WEB-1	200.10.20.30/24
	WEB-2	200.10.20.40/24
	SERVER-1	200.10.20.50/24
	USER_PC	200.10.20.60/24

Task 13.2 Do Routing on devices (Any kind of Routing)

Task 13.3 Create a ACL for company - 1

1. R-PC should TELNET WEB-1 and WEB-2
2. R-PC should SSH WEB-1 and WEB-2
3. R-PC should HTTP WEB-1 and WEB-2
4. R-PC should HTTPS WEB-1 and WEB-2
5. Network of 192.168.10.0/24 should PING DNS_SERVER & SERVER-1
6. R-PC should PING/TELNET/SSH/HTTP/HTTPS to SERVER-1 (www.ccn.com)

Task 13.4 Create A ACL For Company – 2

1. USER_PC should TELNET INTERNAL_SERVER
2. USER_PC should SSH INTERNAL_SERVER
3. USER_PC should HTTP INTERNAL_SERVER
4. USER_PC should HTTPS INTERNAL_SERVER
5. USER_PC should PING a Network of 172.16.10.0/24

SOLUTION

COMPANY 1 ACL

1) R-PC SHOULD TELNET WEB-1 AND WEB-2

ip access-list extended in-out
1 permit tcp host 192.168.10.100 host 200.10.20.30 eq telnet
2 permit tcp host 192.168.10.100 host 200.10.20.40 eq telnet
ip access-list extended out-in
1 permit tcp host 200.10.20.30 host 192.168.10.100 ack
2 permit tcp host 200.10.20.40 host 192.168.10.100 ack

2) R-PC SHOULD SSH WEB-1 AND WEB-2

ip access-list extended in-out
3 permit tcp host 192.168.10.100 host 200.10.20.30 eq 22
4 permit tcp host 192.168.10.100 host 200.10.20.40 eq 22

In first entry we are provided permission of ack to the TCP given IP, so again we don't need to do it

3) R-PC SHOULD HTTP WEB-1 AND WEB-2

ip access-list extended in-out
5 permit tcp host 192.168.10.100 host 200.10.20.30 eq 80
6 permit tcp host 192.168.10.100 host 200.10.20.40 eq 80

4) R-PC SHOULD HTTPS WEB-1 AND WEB-2

ip access-list extended in-out

7 permit tcp host 192.168.10.100 host 200.10.20.30 eq 443

8 permit tcp host 192.168.10.100 host 200.10.20.40 eq 443

5) NETWORK OF 192.168.10.0/24 SHOULD PING DNS_SERVER & SERVER-1

ip access-list extended in-out

9 permit icmp 192.168.10.0 0.0.0.255 host 200.10.20.20 echo

10 permit icmp 192.168.10.0 0.0.0.255 host 200.10.20.50 echo

ip access-list extended out-in

3 permit icmp host 200.10.20.20 192.168.10.0 0.0.0.255 echo-reply

4 permit icmp host 200.10.20.50 192.168.10.0 0.0.0.255 echo-reply

6) R-PC SHOULD PING/TELNET/SSH/HTTP/HTTPS TO SERVER-1 (www.ccn.com)

ip access-list extended in-out

11 permit tcp host 192.168.10.100 host 200.10.20.50 eq www

12 permit tcp host 192.168.10.100 host 200.10.20.50 eq 443

13 permit tcp host 192.168.10.100 host 200.10.20.50 eq 22

14 permit tcp host 192.168.10.100 host 200.10.20.50 eq telnet

15 permit icmp host 192.168.10.100 host 200.10.20.50 echo

ip access-list extended out-in

5 permit tcp host 200.10.20.50 host 192.168.10.100 ack

6 permit icmp host 200.10.20.50 host 192.168.10.100 echo-reply

COMPANY 2 ACL

1) USER_PC SHOULD TELNET INTERNAL_SERVER

ip access-list extended out-in

permit tcp host 200.10.20.60 host 172.16.10.100 eq 23

2) USER_PC SHOULD SSH INTERNAL_SERVER

ip access-list extended out-in

permit tcp host 200.10.20.60 host 172.16.10.100 eq 22

3) USER_PC SHOULD HTTP INTERNAL_SERVER

ip access-list extended out-in

permit tcp host 200.10.20.60 host 172.16.10.100 eq 80

4) USER_PC SHOULD HTTPS INTERNAL_SERVER

ip access-list extended out-in

permit tcp host 200.10.20.60 host 172.16.10.100 eq 443

5) USER_PC SHOULD PING NETWORK OF 172.16.10.0/24

ip access-list extended out-in

permit icmp host 200.10.20.60 172.16.10.0 0.0.0.255 echo

WE HAVE TO PERMIT ROUTING PROTOCOL BECAUSE THAT PROTOCOL SENDING HELLO MESSGAES AND BLOCKED BY ACL

ip access-list extended out-in

permit eigrp any any

VERIFICATION

COMPANY-1

```
CO-1#show ip access-lists
Extended IP access list in-out
    10 permit tcp host 192.168.10.100 host 200.10.20.30 eq telnet
    20 permit tcp host 192.168.10.100 host 200.10.20.40 eq telnet
    30 permit tcp host 192.168.10.100 host 200.10.20.30 eq 22
    40 permit tcp host 192.168.10.100 host 200.10.20.40 eq 22
    50 permit tcp host 192.168.10.100 host 200.10.20.30 eq www
    60 permit tcp host 192.168.10.100 host 200.10.20.40 eq www
    70 permit tcp host 192.168.10.100 host 200.10.20.30 eq 443
    80 permit tcp host 192.168.10.100 host 200.10.20.40 eq 443
    90 permit icmp 192.168.10.0 0.0.0.255 host 200.10.20.20 echo
    100 permit icmp 192.168.10.0 0.0.0.255 host 200.10.20.50 echo
Extended IP access list out-in
    10 permit tcp host 200.10.20.30 host 192.168.10.100 ack
    20 permit tcp host 200.10.20.40 host 192.168.10.100 ack
    30 permit icmp host 200.10.20.20 192.168.10.0 0.0.0.255 echo-reply
    40 permit icmp host 200.10.20.50 192.168.10.0 0.0.0.255 echo-reply
    50 permit eigrp any any (964 matches)
```

COMPANY-2

```
CO-2#show ip access-lists
Extended IP access list in-out
    10 permit tcp host 172.16.10.100 host 200.10.20.60 ack
    20 permit icmp host 172.16.10.100 host 200.10.20.60 echo-reply (10 matches)
Extended IP access list out-in
    10 permit tcp host 200.10.20.60 host 172.16.10.100 eq telnet
    20 permit tcp host 200.10.20.60 host 172.16.10.100 eq 22
    30 permit tcp host 200.10.20.60 host 172.16.10.100 eq www
    40 permit tcp host 200.10.20.60 host 172.16.10.100 eq 443
    50 permit icmp host 200.10.20.60 172.16.10.0 0.0.0.255 echo (10 matches)
    60 permit eigrp any any (396 matches)
```

STANDARD ACL

- Basically, We Do Make Standard Access-Control List For Permit/Deny Source Traffic Only Unlike Extended ACL Where We Permit/Deny Source To Destination Traffic With The Control Of Protocol & Services As Well
- Standard ACL permit source traffic and allow all kinds of traffic on that give ip or a network/subnet

Let's make Standard ACL

CREATION

Router(config)#ip access-list standard lan-wan

Router(config)#permit host 192.168.10.1 ……..(permit single ip with all source traffic)

OR

Router(config)#permit 192.168.10.0 0.0.0.255…permit whole network with all source traffic)

Router(config)#deny any

IMPLEMENTATION

Router(config)#interface ethernet 0/0
Router(config)#ip access-group lan-wan in
Router(config)#exit

VERIFICATION

Router# show ip access-list ……..(show all acl)

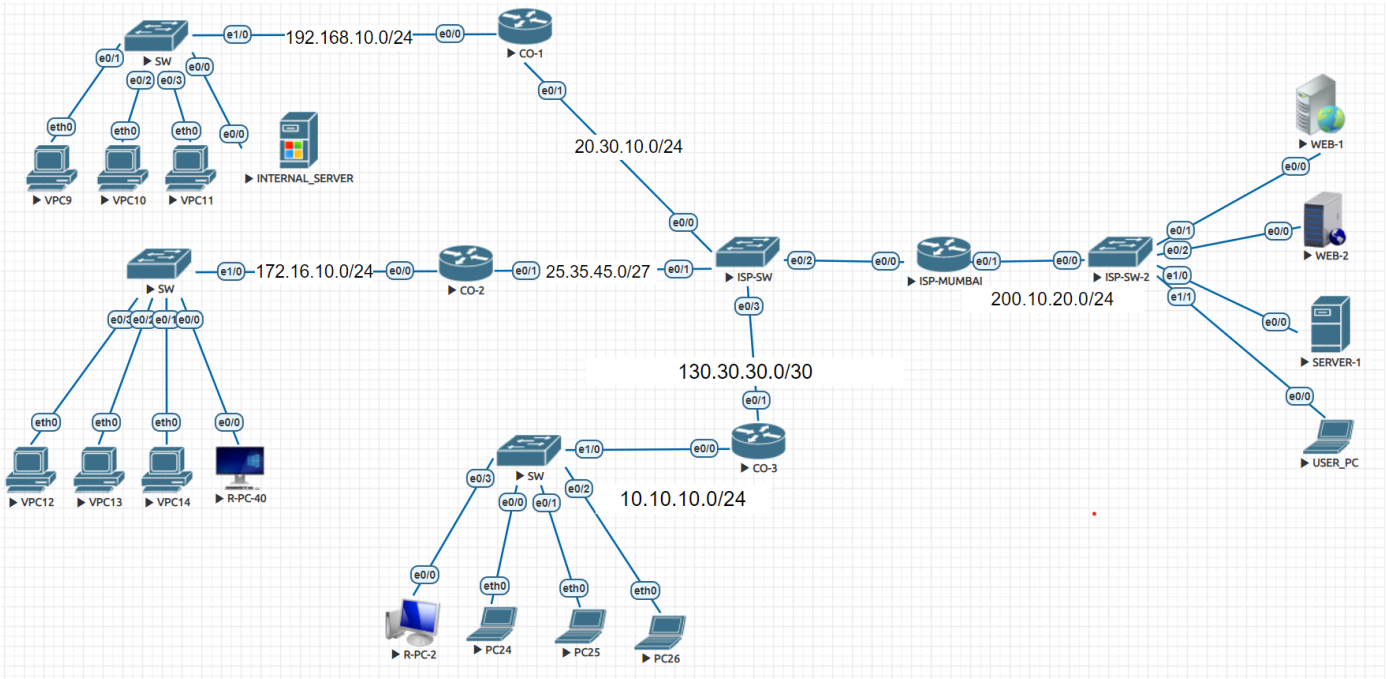
OR

Router#show ip access-list lan-wan ……(show only lan-wan acl)

Allowing all kinds of source traffic will make it more vulnerable that's why we use extended ACL, otherwise we use Standard ACL for NAT/PAT configuration or VPN configuration.

NETWORK ADDRESS TRANSALATION (NAT) &

PORT ADDRESS TRANSLATION (PAT)



- We use a NAT technology to translate private IP to public IP. Then, there are many things in a NAT that is Static NAT, Dynamic NAT, PAT (Port Address Translation)
- Static NAT – in Static NAT translate private IP to public IP, it is one to one translate and we do manual entry for that. with Static NAT bidirectional connection can be made.
- Dynamic NAT- dynamic NAT also translate private IP to public IP but in different way. Here
  we create pool of public IP then random private IP can be translate to public IP out of this pool. It creates unidirectional connection.
- PAT – PAT also translate private IP to public IP but adds up port number. Many private IP translate into one public IP with the effect of port number. pat provide unidirectional connection.

TASKS – 14

IP

CO-1	ETH 0/0=192.168.10.254/24	ETH 0/1=20.30.10.1/24
CO-1 PC	VPC9	192.168.10.1
	VPC10	192.168.10.2
	VPC11	192.168.10.3

	INTERNAL_SERVER	192.168.10.100
CO-2	ETH0/0 = 172.16.10.254/24	ETH0/1 = 25.35.45.1/27
CO-2 PC	VPC12	172.16.10.1
	VPC13	172.16.10.2
	VPC14	172.16.10.3
	R-PC-40	172.16.10.100
CO-3	ETH0/0=10.10.10.254/24	ETH0/1=130.30.30.1/30
CO-3 PC	R-PC-2	10.10.10.100
	PC24	10.10.10.1
	PC25	10.10.10.2
	PC26	10.10.10.3
ISP-MUMBAI		
ETH0/0.111		20.30.10.2/24
ETH0/0.219		25.35.45.2/27
ETH0/0.389		130.30.30.2/30
ETH0/1		200.10.20.1/24
ISP-SW		
ETH0/0		VLAN 111 = CO-1_ISP
ETH0/1		VLAN 219 = CO-2_ISP
ETH0/3		VLAN 389 = CO-3_ISP
ETH0/2		TRUNK
OTHERS		
WEB-1		200.10.20.10/24
WEB-2		200.10.20.20/24
SERVER-1		200.10.20.30/24
USER_PC		200.10.20.40/24

ROUTING EIGRP 199

Task 14.1 CO-1

VPC-9, VPC-10 , VPC-11 , INTERNAL SERVER Should Assign Static Mapped With The Ip Of 20.30.10.10 ,20.30.10.20 , 20.30.10.30 , 20.30.10.40

Do telnet on IP 20.30.10.40 it redirects to the INTERNAL SERVER

Task 14.2 – CO-2

VPC-12 , VPC-13 , VPC-14 , R-PC-40 Should Dynamically Mapped With The Given Pool Of IP 25.35.45.3 – 25.35.45.7

Task 14.3 -CO-3

A Whole Network of Company 3 Should Mapped With The Ip Of ETH 0/1 (CO-3)

LET'S DO IT

TASK – 14.1

1.Do Static NAT entry on router

CO-1(config)#ip nat inside source static 192.168.10.1 20.30.10.10

CO-1(config)#ip nat inside source static 192.168.10.2 20.30.10.20

CO-1(config)#ip nat inside source static 192.168.10.3 20.30.10.30

CO-1(config)#ip nat inside source static 192.168.10.100 20.30.10.40

2.then activate NAT on interface

CO-1(config)#interface ethernet 0/0

CO-1(config-if)#ip nat inside

CO-1(config-if)#exit

CO-1(config)#interface ethernet 0/1

CO-1(config-if)#ip nat outside

CO-1(config-if)#exit

VERIFCATION

ON ROUTER

```
CO-1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 20.30.10.10        192.168.10.1       ---                ---
--- 20.30.10.20        192.168.10.2       ---                ---
--- 20.30.10.30        192.168.10.3       ---                ---
--- 20.30.10.40        192.168.10.100     ---                ---
```

Debug on web-1 A ping via vpc-9

WEB-1#debug ip packet

```
*Mar  3 10:44:53.526: IP: s=20.30.10.10 (Ethernet0/0), d=200.10.20.10 (Ethernet0/0), len 84, rcvd 3
*Mar  3 10:44:53.526: IP: s=20.30.10.10 (Ethernet0/0), d=200.10.20.10, len 84, stop process pak for for
s packet
*Mar  3 10:44:53.526: IP: s=200.10.20.10 (local), d=20.30.10.10 (Ethernet0/0), len 84, sending
*Mar  3 10:44:53.526: IP: s=200.10.20.10 (local), d=20.30.10.10 (Ethernet0/0)
WEB-1#, len 84, sending full packet
```

To stop Debugging

WEB-1#undebug all

Telnet

```
USER_PC#telnet 20.30.10.40 23
Trying 20.30.10.40 ...
% Connection refused by remote host

USER_PC#telnet 20.30.10.40 23
Trying 20.30.10.40 ... Open


User Access Verification

Username: ccn
Password:
INTERNAL_SERVER#
INTERNAL_SERVER#
```

TASK – 14.2

To Combine all Private IP we create Standard ACL

CO-2(config)#ip access-list standard DYN_NAT-LIST

CO-2(config-std-nacl)#permit 172.16.10.0 0.0.0.255

CO-2(config-std-nacl)#exit

To create NAT POOL

CO-2(config)# ip nat pool CCN-DYN_NAT 25.35.45.3 25.35.45.7 netmask 255.255.255.224

To match up Private IP ‘s list (ACL) with NAT POOL (pool)

CO-2(config)#ip nat inside source list DYN_NAT-LIST pool CCN-DYN_NAT

To Implement NAT

CO-2(config)#interface ethernet 0/0

CO-2(config-if)#ip nat inside

CO-2(config-if)#exit

CO-2(config)#interface ethernet 0/1

CO-2(config-if)#ip nat outside

CO-2(config-if)#exit

VERIFICATION

Did ping from vpc-12 to web-1

```
CO-2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 25.35.45.3:14043  172.16.10.1:14043  200.10.20.10:14043 200.10.20.10:14043
icmp 25.35.45.3:14299  172.16.10.1:14299  200.10.20.10:14299 200.10.20.10:14299
icmp 25.35.45.3:14555  172.16.10.1:14555  200.10.20.10:14555 200.10.20.10:14555
icmp 25.35.45.3:14811  172.16.10.1:14811  200.10.20.10:14811 200.10.20.10:14811
```

TASK – 14.3

To combine all Private IP we create Standard ACL

CO-3(config)#ip access-list standard PAT-LIST

CO-3(config-std-nacl)#permit 10.10.10.0 0.0.0.255

CO-3(config-std-nacl)#exit

To combine ACL with Interface for PAT

CO-3(config)# ip nat inside source list PAT-LIST interface ethernet 0/1 overload

To Implement NAT/PAT

CO-3(config)#interface ethernet 0/0

CO-3(config-if)#ip nat inside

CO-3(config-if)#exit

CO-3(config)#interface ethernet 0/1

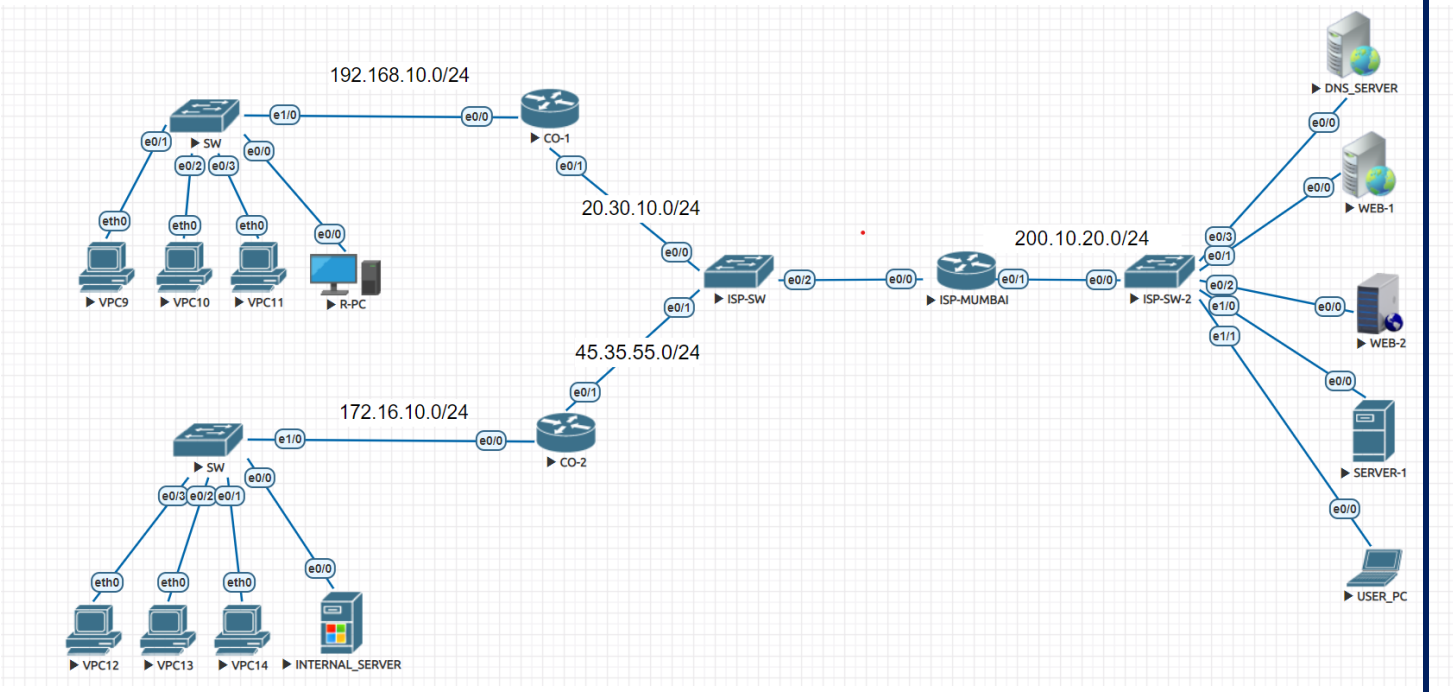
CO-3(config-if)#ip nat outside

CO-3(config-if)#exit

VERIFICATION

```
CO-3#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 130.30.30.1:2013  10.10.10.1:2013    200.10.20.1:2013   200.10.20.1:2013
icmp 130.30.30.1:2269  10.10.10.1:2269    200.10.20.1:2269   200.10.20.1:2269
icmp 130.30.30.1:2525  10.10.10.1:2525    200.10.20.1:2525   200.10.20.1:2525
icmp 130.30.30.1:2781  10.10.10.1:2781    200.10.20.1:2781   200.10.20.1:2781
icmp 130.30.30.1:3037  10.10.10.1:3037    200.10.20.1:3037   200.10.20.1:3037
icmp 130.30.30.1:3805  10.10.10.1:3805    200.10.20.10:3805  200.10.20.10:3805
icmp 130.30.30.1:4061  10.10.10.1:4061    200.10.20.10:4061  200.10.20.10:4061
icmp 130.30.30.1:4317  10.10.10.1:4317    200.10.20.10:4317  200.10.20.10:4317
icmp 130.30.30.1:4573  10.10.10.1:4573    200.10.20.10:4573  200.10.20.10:4573
icmp 130.30.30.1:4829  10.10.10.1:4829    200.10.20.10:4829  200.10.20.10:4829
```

ACL AND NAT



CO-1	ETH0/0 = 192.168.10.254/24	ETH0/1 = 20.30.10.10/24
	VPC-9	192.168.10.1/24
	VPC-10	192.168.10.2/24
	VPC-11	192.168.10.3/24
	R-PC	192.168.10.100/24
CO-2	ETH0/0= 172.16.10.254/24	ETH0/1 = 45.35.55.65/24
	VPC-12	172.16.10.1/24
	VPC-13 =	172.16.10.2/24
	VPC-14	172.16.10.3/24
	INTERNAL_SERVER	172.16.10.100/24
ISP-SW		
ETH0/0	VLAN 99 => ISP_CO-1	

ETH0/1		VLAN 199 => ISP_CO-2
ETH 0/2		TRUNK
ISP-MUMBAI	ETH0/0	NO SHUT / NO IP ADDRESS
	ETH0/0.99 =	20.30.10.20/24
	ETH0/0.199	45.35.55.75/24
	ETH0/1	200.10.20.1/24
OTHERS		
DNS_SERVER		200.10.20.10/24
WEB-1		200.10.20.20
WEB-2		200.10.20.30
SERVER-1		200.10.20.40
USER_PC		200.10.20.50

ROUITNG

- CO-1 > EIGRP 199 on both side
- CO-2 > OSPF 100 AREA 1 both side
- ISP_MUMBAI > EIGRP 199 / OSPF 100 AREA 1 for CO-1 & CO-2's other side RIP
- DNS_SERVER / WEB-1 / WEB-2 / SERVER-1 / USER_PC / R-PC / INTERNAL_SERVER = DEFAULT ROUTING

TASK – 15

CO-1

Task – 15.1 ACL TASK

1.A whole network can PING WEB-1 AND WEB-2

2.R-PC can TELNET & SSH WEB-1 & WEB-2

3.R-PC can do HTTP & HTTPS TO SERVER-1

Task – 15.2 STATIC NAT TASK

VPC-9, VPC-10 , VPC-11 , R-PC should assign static mapped IP OF 20.30.10.1 , 20.30.10.2 , 20.30.10.3 , 20.30.10.100 respectively

CO-2

Task – 15.3 ACL TASK

1.USER_PC can PING a whole network

2.USER_PC can TELNET, SSH, HTTP , HTTPS to INTERNAL SERVER

Task – 15.4 STATIC NAT TASK

VPC-12, VPC-13, VPC-14 , INTERNAL SERVER should assign static ip of 45.35.55.10 , 45.35.55.20 , 45.35.55.30 , 45.35.55.100

LET's DO THE TASK

CO-1

First we are going to do NAT Task

Task - 15.2

CO-1(config)#ip nat inside source static 192.168.10.1 20.30.10.1
CO-1(config)#ip nat inside source static 192.168.10.2 20.30.10.2
CO-1(config)#ip nat inside source static 192.168.10.3 20.30.10.3
CO-1(config)#ip nat inside source static 192.168.10.100 20.30.10.100

Implementation of NAT

CO-1(config)#interface ethernet 0/0
CO-1(config-if)#ip nat inside
CO-1(config-if)#exit
CO-1(config)#interface ethernet 0/1
CO-1(config-if)#ip nat outside
CO-1(config-if)#exit

ACL

Task 15.1 = 1)

CO-1(config)#ip access-list extended in-out
CO-1(config-ext-nacl)#1 permit icmp 192.168.10.0 0.0.0.255 host 200.10.20.20 echo

CO-1(config-ext-nacl)#ip access-list extended out-in
CO-1(config-ext-nacl)#1 permit icmp host 200.10.20.20 host 20.30.10.1 echo-reply
CO-1(config-ext-nacl)#2 permit icmp host 200.10.20.20 host 20.30.10.2 echo-reply
CO-1(config-ext-nacl)#3 permit icmp host 200.10.20.20 host 20.30.10.3 echo-reply
CO-1(config-ext-nacl)#4 permit icmp host 200.10.20.20 host 20.30.10.100 echo-reply

Task 15.1 = 2)

CO-1(config-ext-nacl)#ip access-list extended in-out

CO-1(config-ext-nacl)#2 permit tcp host 192.168.10.100 host 200.10.20.20 eq 23

CO-1(config-ext-nacl)#3 permit tcp host 192.168.10.100 host 200.10.20.20 eq 22

CO-1(config-ext-nacl)#2 permit tcp host 192.168.10.100 host 200.10.20.30 eq 23

CO-1(config-ext-nacl)#3 permit tcp host 192.168.10.100 host 200.10.20.30 eq 22

CO-1(config-ext-nacl)#ip access-list extended out-in

CO-1(config-ext-nacl)#5 permit tcp host 200.10.20.20 host 20.30.10.100 ack

CO-1(config-ext-nacl)#6 permit tcp host 200.10.20.30 host 20.30.10.100 ack

Task 15.1 = 3)

CO-1(config-ext-nacl)#ip access-list extended in-out

CO-1(config-ext-nacl)#4 permit tcp host 192.168.10.100 host 200.10.20.40 eq 80

CO-1(config-ext-nacl)#5 permit tcp host 192.168.10.100 host 200.10.20.40 eq 443

CO-1(config-ext-nacl)#ip access-list extended out-in

CO-1(config-ext-nacl)#7 permit tcp host 200.10.20.40 host 20.30.10.100 ack

Permit routing Eigrp on out-in

CO-1(config-ext-nacl)#ip access-list extended out-in

CO-1(config-ext-nacl)#8 permit eigrp any any

Implementation of ACL

CO-1(config-ext-nacl)#interface ethernet 0/0

CO-1(config-if)#ip access-group in-out in

CO-1(config-if)#exit

CO-1(config)#interface ethernet 0/1

CO-1(config-if)#ip access-group out-in in

CO-1(config-if)#exit

VERIFICATION

CO-1(config)#Show ip access-list

```
CO-1(config)#do show ip access-lists
Extended IP access list in-out
    1 permit icmp 192.168.10.0 0.0.0.255 host 200.10.20.20 echo
    2 permit tcp host 192.168.10.100 host 200.10.20.20 eq telnet (37 matches)
    3 permit tcp host 192.168.10.100 host 200.10.20.20 eq 22
    4 permit tcp host 192.168.10.100 host 200.10.20.40 eq www (7 matches)
    5 permit tcp host 192.168.10.100 host 200.10.20.40 eq 443 (8 matches)
Extended IP access list out-in
    1 permit icmp host 200.10.20.20 host 20.30.10.1 echo-reply
    2 permit icmp host 200.10.20.20 host 20.30.10.2 echo-reply
    3 permit icmp host 200.10.20.20 host 20.30.10.3 echo-reply
    4 permit icmp host 200.10.20.20 host 20.30.10.100 echo-reply
    5 permit tcp host 200.10.20.20 host 20.30.10.100 ack (28 matches)
    6 permit tcp host 200.10.20.30 host 20.30.10.100 ack
    7 permit tcp host 200.10.20.40 host 20.30.10.100 ack (12 matches)
    8 permit eigrp any any (66 matches)
```

CO – 2

First we are going to do NAT Task

Task -15.4

NAT

CO-2(config)#ip nat inside source static 172.16.10.1 45.35.55.10

CO-2(config)#ip nat inside source static 172.16.10.2 45.35.55.20

CO-2(config)#ip nat inside source static 172.16.10.3 45.35.55.30

CO-2(config)#ip nat inside source static 172.16.10.100 45.35.55.100

Implementation of NAT

CO-2(config)#interface ethernet 0/0

CO-2(config-if)#ip nat inside

CO-2(config-if)#exit

CO-2(config)#interface ethernet 0/1

CO-2(config-if)#ip nat outside

CO-2(config-if)#exit

ACL

Task 15.3 = 1)

CO-2(config)#ip access-list extended wan-lan

CO-2(config-ext-nacl)#1 permit icmp host 200.10.20.50 45.35.55.0 0.0.0.255 echo

CO-2(config)#ip access-list extended lan-wan

CO-2(config-ext-nacl)#1 permit icmp 172.16.10.0 0.0.0.255 host 200.10.20.50 echo-reply

Task 15.3 = 2)

CO-2(config)#ip access-list extended wan-lan

CO-2(config-ext-nacl)#2 permit tcp host 200.10.20.50 host 45.35.55.100 eq 22 23 80 44

CO-2(config)#ip access-list extended lan-wan

CO-2(config-ext-nacl)#2 permit tcp host 172.16.10.100 host 200.10.20.50 ack

Implementation of ACL

CO-2(config)#interface ethernet 0/0

CO-2(config-if)#ip access-group lan-wan in

CO-2(config-if)#exit

CO-2(config)#interface ethernet 0/1

CO-2(config-if)#ip access-group wan-lan in

CO-2(config-if)#exit

Permit routing ospf

CO-2(config)#ip access-list extended wan-lan

CO-2(config-ext-nacl)#3 permit ospf any any

VERIFICATION

CO-2#Show ip access-list

```
CO-2#show ip access-lists
Extended IP access list lan-wan
    1 permit icmp 172.16.10.0 0.0.0.255 host 200.10.20.50 echo-reply
    2 permit tcp host 172.16.10.100 host 200.10.20.50 ack
Extended IP access list wan-lan
    1 permit icmp host 200.10.20.50 45.35.55.0 0.0.0.255 echo
    2 permit tcp host 200.10.20.50 host 45.35.55.100 eq 22 telnet www 443
    3 permit ospf any any (21 matches)
```

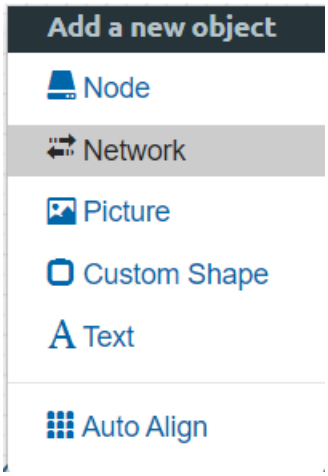
ISP-MUMBAI

```
ISP-MUMBAI#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES NVRAM  up                    up
Ethernet0/0.99             20.30.10.20     YES NVRAM  up                    up
Ethernet0/0.199            45.35.55.75     YES NVRAM  up                    up
Ethernet0/1                200.10.20.1     YES NVRAM  up                    up
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
```

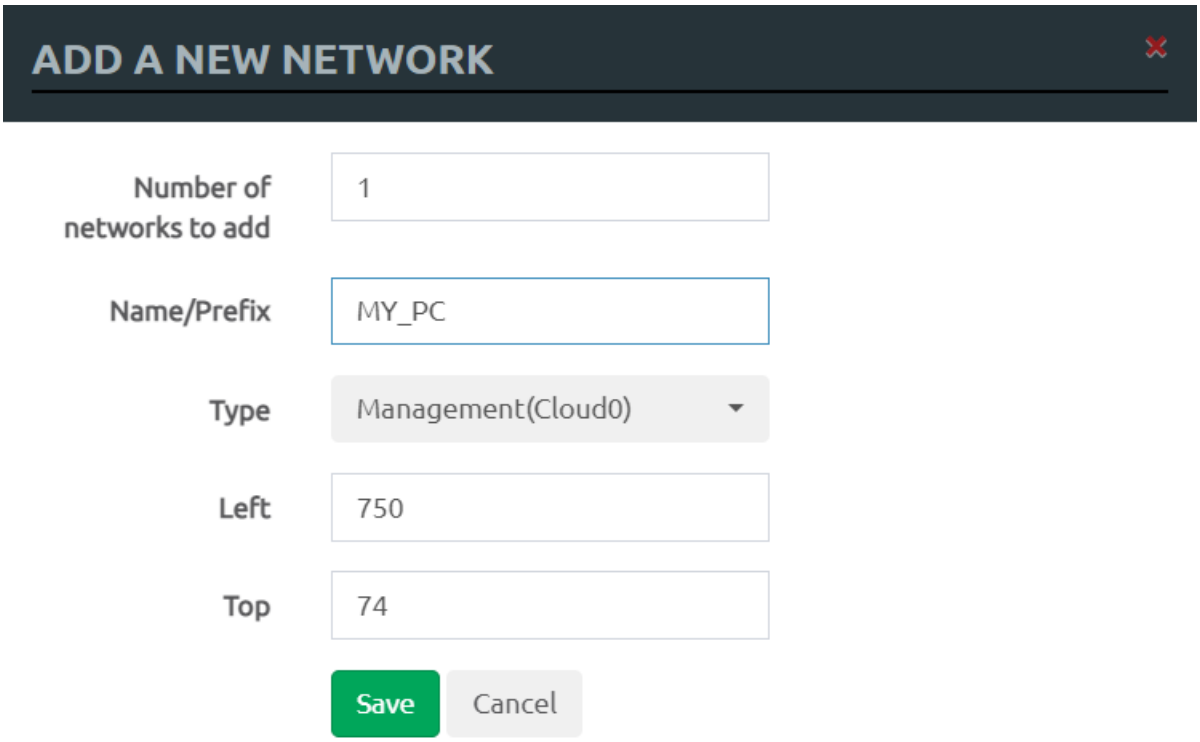
```
router eigrp 199
 network 20.30.10.0 0.0.0.255
 redistribute rip metric 10000 1000 255 1 1500
 redistribute ospf 100 metric 10000 1000 255 1 1500
!
router ospf 100
 redistribute eigrp 199 subnets
 redistribute rip subnets
 network 45.35.55.0 0.0.0.255 area 1
!
router rip
 redistribute eigrp 199 metric 1
 redistribute ospf 100 metric 1
 network 200.10.20.0
!
```

HOW TO ADD YOUR LAPTOP/PC TO EVE-NG LAB SETUP

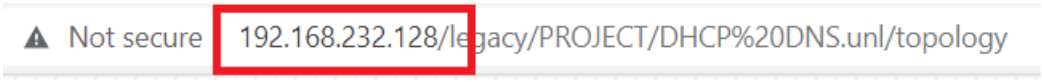
1.DO RIGHT CLICK SELECT ADD A NEW OBJECT >“NETWORK”.



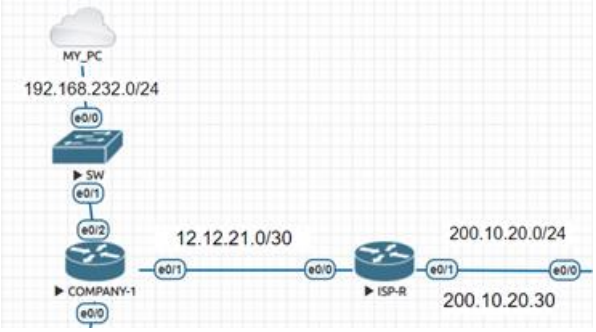
Then, NAME/PREFIX - MY_PC >TYPE – Management(cloud0)



2.Here IP of the network is 192.168.232.0/24, here we put IP of that eve-ng network .so your IP might be change according to your eve-ng network IP



3.Assign one IP of that network to router interface ethernet 0/2=192.168.232.100 255.255.255.0



COMPANY-1(config)#interface ethernet 0/2

COMPANY-1(config-if)#ip address 192.168.232.100 255.255.255.0

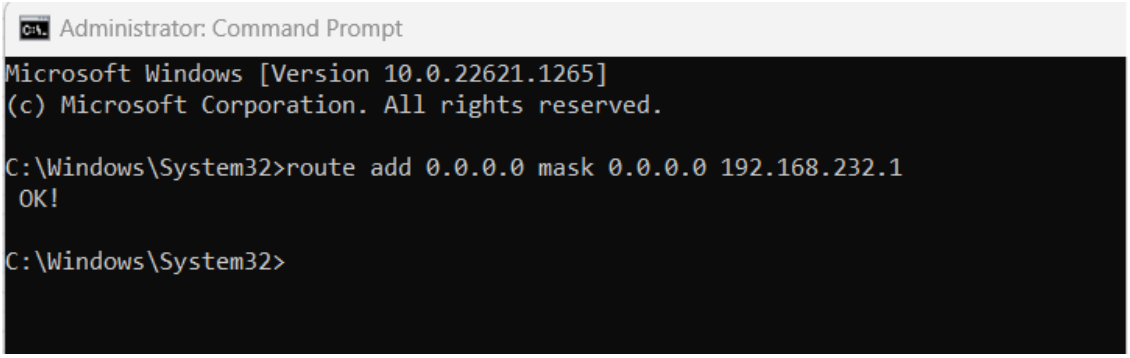
COMPANY-1(config-if)#no shutdown

COMPANY-1(config-if)#exit

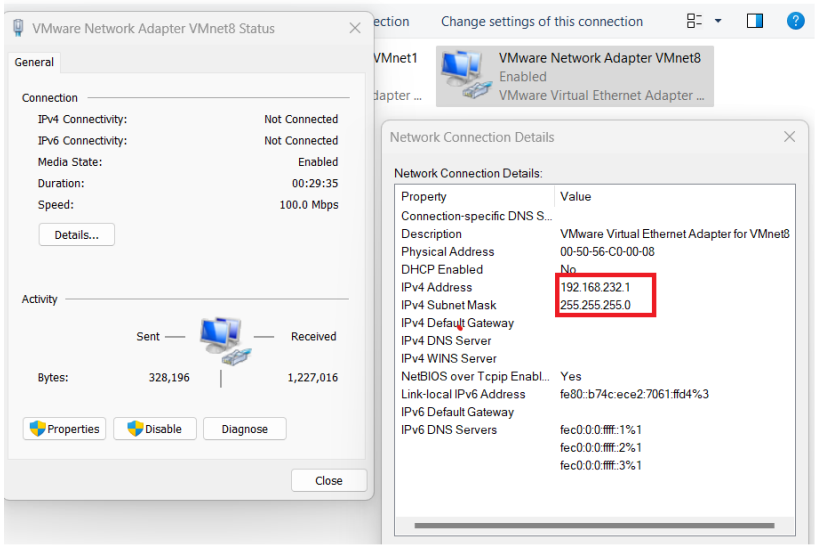
4.Advertise that route via routing of any means here we using Router EIGRP

```
router eigrp 100
 network 12.12.21.0 0.0.0.3
 network 192.168.10.0
 network 192.168.232.0
!
```

5.Then, go to your real PC/LAPTOP open **command prompt – run as administrator** and add a manual route to the eve-ng network



The IP of 192.168.232.1 is the ip of your VMnet8 adapters



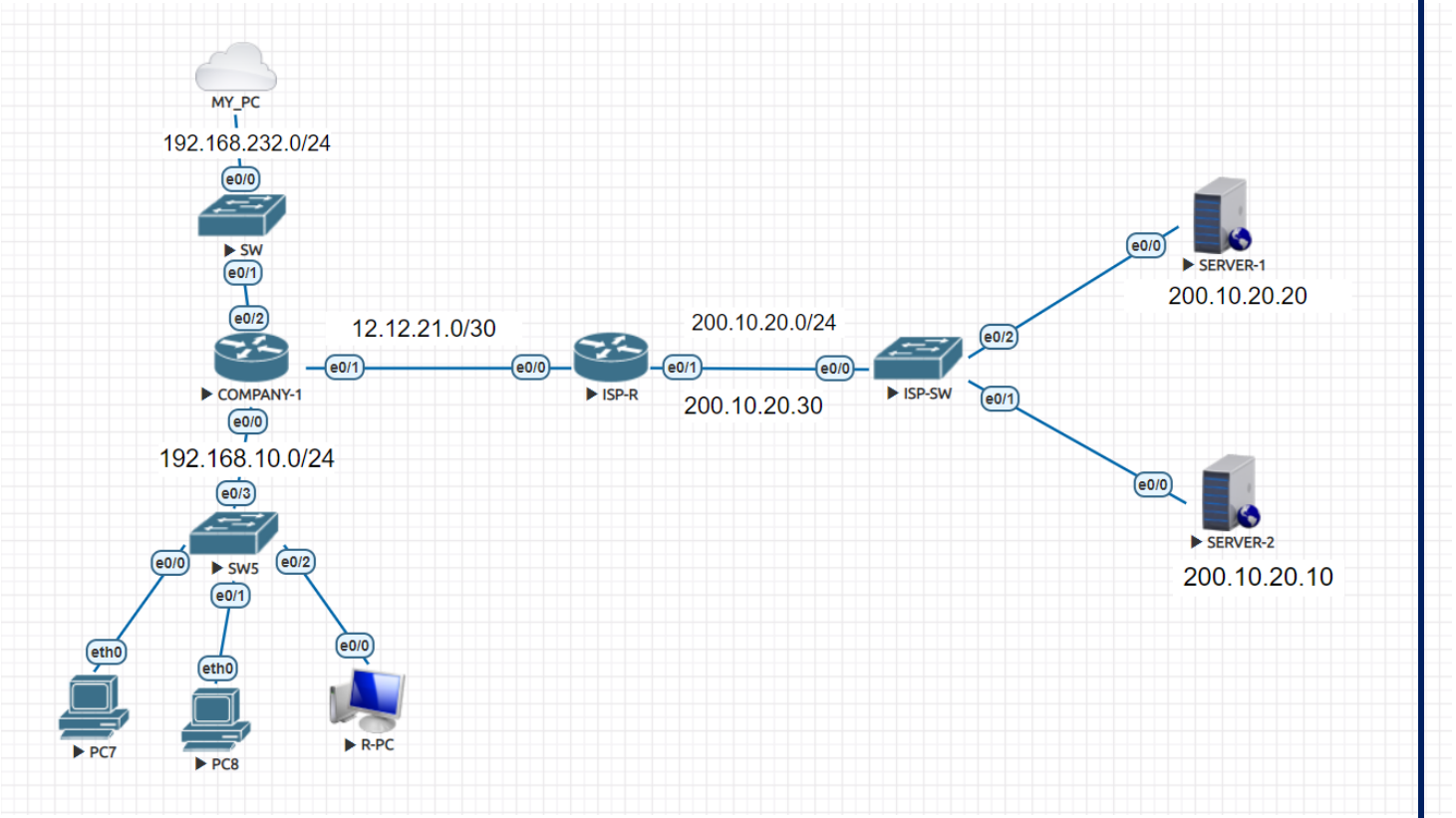
6. Then try to ping IP 192.168.232.100(router's IP)

```
C:\Windows\System32>ping 192.168.232.100

Pinging 192.168.232.100 with 32 bytes of data:
Reply from 192.168.232.100: bytes=32 time=2ms TTL=255
Reply from 192.168.232.100: bytes=32 time=1ms TTL=255
Reply from 192.168.232.100: bytes=32 time=1ms TTL=255
Reply from 192.168.232.100: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.232.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

If it is pinging it means your real PC/LAPTOP got connected with eve-ng LAB setup

SYSLOG

- Syslog means system logs. we generally use this log to identify the problem or trouble shoot the issue, to monitor the network, to identify the problematic area
- Syslog has basically THREE METHODS
  1. CONSOLE- all the logs generated by the device will show it on screen/terminal like putty, Secure-CRT
  2. BUFFER- All the logs generated by the device will stored it in buffer/memory of the device
  3. TRAP- All the logs generated by the device will trap and send it given specific IP



CONSOLE

COMPANY-1(config)#logging on …..(to start the logging on devices)

COMPANY-1(config)#logging console informational

BUFFER

COMPANY-1(config)#logging on

COMPANY-1(config)#logging buffered 4096 …… (allocate memory size)

COMPANY-1(config)#logging buffered informational (logs message till informational level)

Verification

COMPANY-1# show logging

TRAP

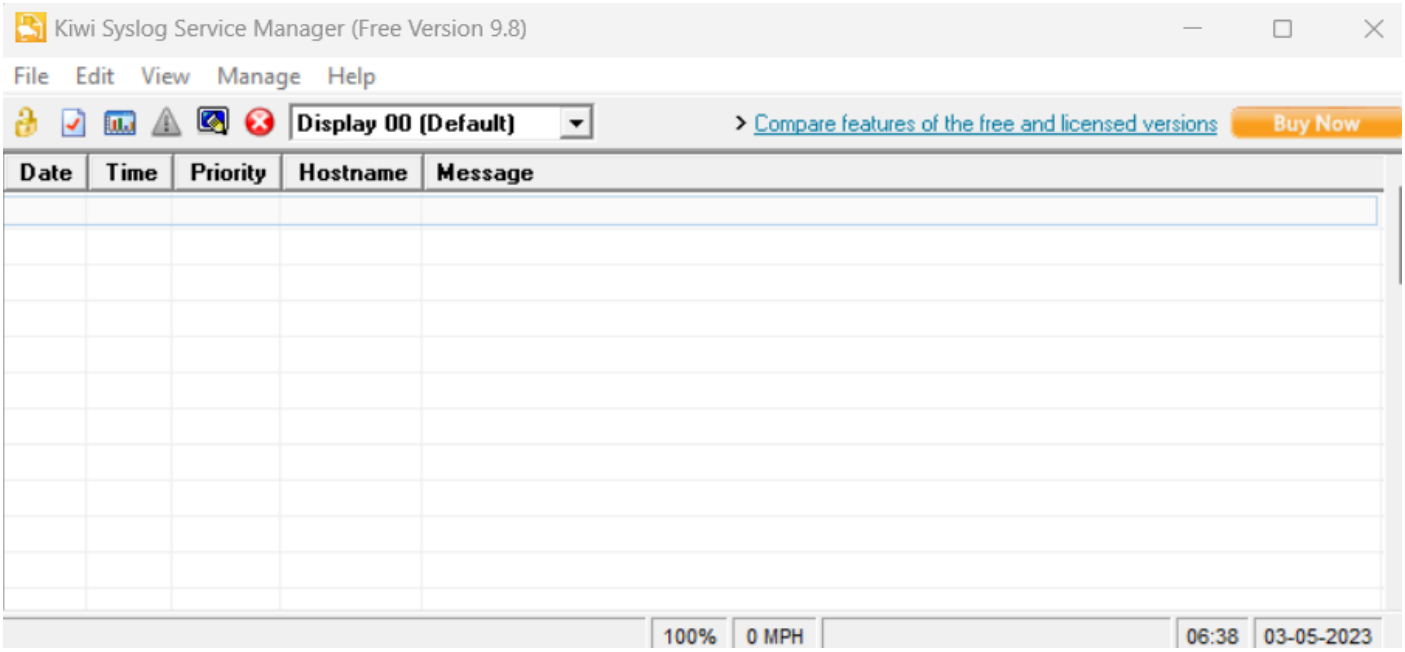
COMPANY-1(config)#logging on

COMPANY-1(config)#logging trap informational

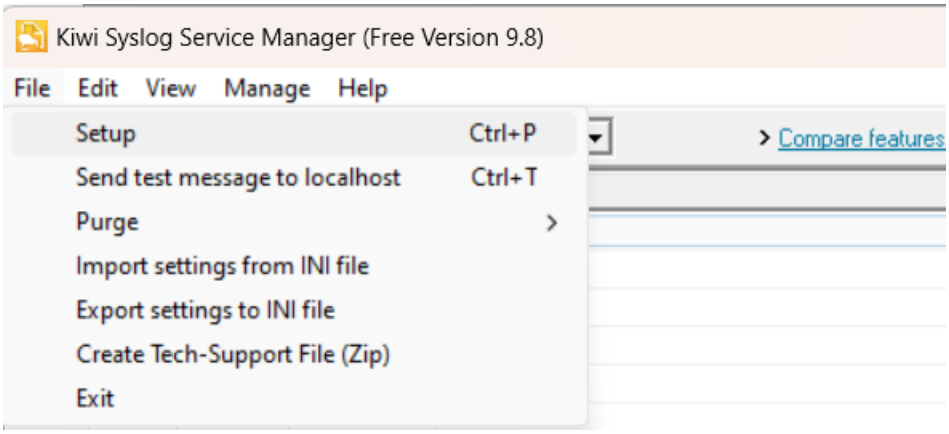
COMPANY-1(config)#logging host 192.168.232.1 ……(logs are trapped and send it to this ip)

For trapped messages we need some tools to view it so here we use the ‘kiwi syslog server’

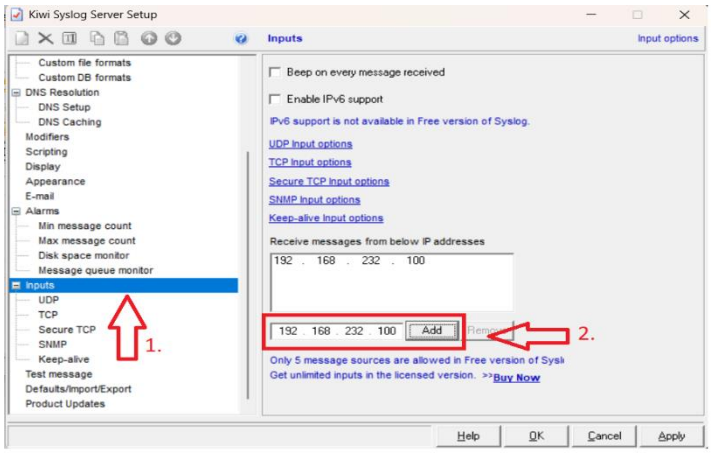
1.This is the kiwi syslog server look



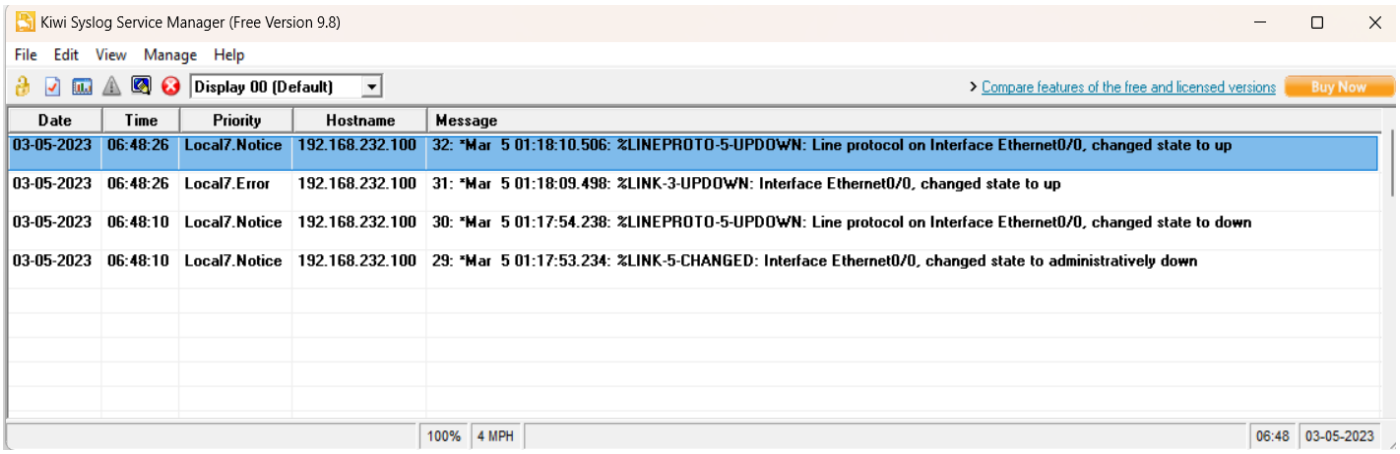
2.how to setup this application. Go to File > Setup



3.then , go to 1.Input > 2.Add IP address of the log generating device > Add > Apply > OK



4.finally you get message over here like this if event occur. here we done manual interface shutdown just to check messages are trapped or not. so, we get the messages.



CDP

- CDP stands for Cisco Discovery Protocol uses to find neighboring cisco devices only.
- Default, CDP timer is 60 sec, whereas CDP hold down timer is 180 sec.
- CDP is default running on cisco devices.

Commands

To run CDP on Global mode

COMPANY-1(config)#cdp run

To set CDP timer

COMPANY-1(config)#cdp timer …. <5-254>……

To set CDP Holdtime

COMPANY-1(config)#cdp holdtime ……<10-255>……..

To enable CDP on interface

COMPANY-1(config)#interface ethernet 0/1
COMPANY-1(config-if)#cdp enable
COMPANY-1(config-if)#exit
COMPANY-1(config)#interface ethernet 0/0
COMPANY-1(config-if)#cdp enable
COMPANY-1(config-if)#exit

VERIFICATION

COMPANY-1#show cdp neighbors

COMPANY-1#show cdp neighbors detail

```
COMPANY-1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch           Eth 0/2           158             R S I  Linux Uni Eth 0/1
Switch           Eth 0/0           140             R S I  Linux Uni Eth 0/3
R2               Eth 0/1           174              R B   Linux Uni Eth 0/0

Total cdp entries displayed : 3
```


https://www.linkedin.com/in/gitesh-d-aa95a8227/

LLDP

LLDP is a Link Layer Discovery Protocol we use this to find out neighbor devices in a network. it is a Layer 2 protocol of OSI model. LLDP timer is 30 sec. whereas, LLDP holdtime is 120 sec.

Commands

To start LLDP Globally

COMPANY-1(config)#lldp run

To LLDP on interface (first start it Globally)

COMPANY-1(config-if)#interface ethernet 0/0
COMPANY-1(config-if)#lldp transmit
COMPANY-1(config-if)#lldp receive
COMPANY-1(config-if)#exit
COMPANY-1(config)#interface ethernet 0/1
COMPANY-1(config-if)#lldp transmit
COMPANY-1(config-if)#lldp receive
COMPANY-1(config-if)#exit

VERIFICATION

COMPANY-1#show lldp neighbors

COMPANY-1#show lldp neighbors detail

```
COMPANY-1#show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
R2                  Et0/1          120        R               Et0/0

Total entries displayed: 1
```


https://www.linkedin.com/in/gitesh-d-aa95a8227/

PASSWORD ASSIGNMENT

How to assign password on router and switches?

the commands are same no changes

ROUTER/SWITCH

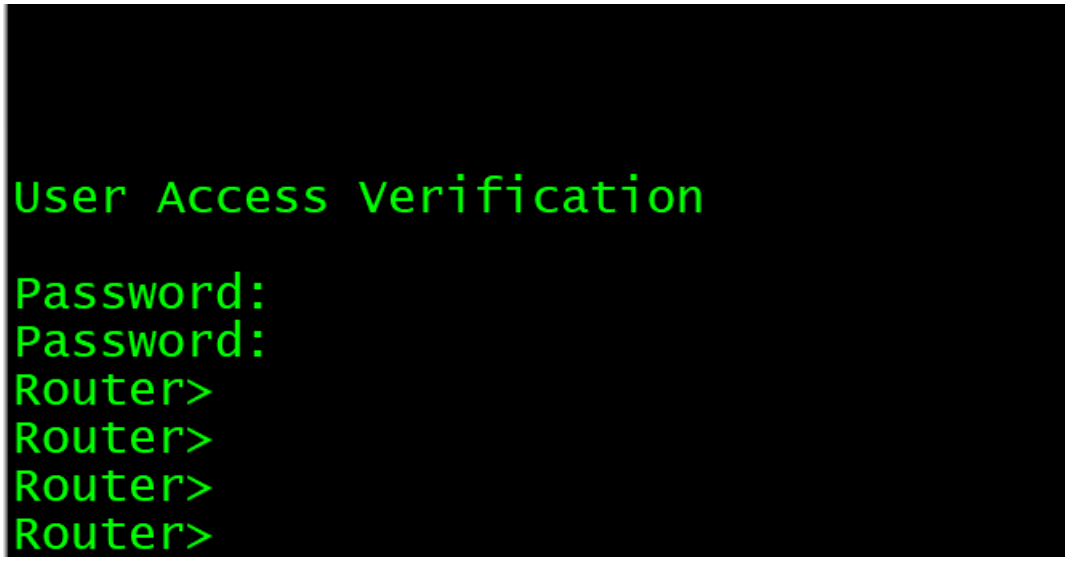
To Give Password to CONSOLE PORT

Router(config)#line con 0

Router(config-line)#password ccn

Router(config-line)#login

Router(config-line)#exit



NOTE:-By Applying This Command Device Will Only Ask For The Password

If Company Wants To Ask For Username And Password To There Employee Then We Can Set Accordingly

Router(config)#line con 0

Router(config-line)#login local ……(by this it will ask for username & password at the time of console login)

Router(config-line)#exit

For that we have to create username and password

Router(config)#username ccn privilege 1 password ccn …..(make entry in clear text format)

OR

Router(config)#username ccn privilege 1 secret ccn123 …..(make entry in clear encrypted format)

```
User Access Verification

Username: ccn
Password:
Router>
Router>
```

Applying password at PRIVILAGE MODE

Router(config)#enable password ccn1234

This will enable password at privilege mode with clear text format

```
Router(config)#do show running-config | section enable
enable password ccn1234
```

VERIFICATION

```
User Access Verification

Username: ccn
Password:
Router>enable
Password:
Password:
Password:
Router#
```

For that we have to encrypt this password

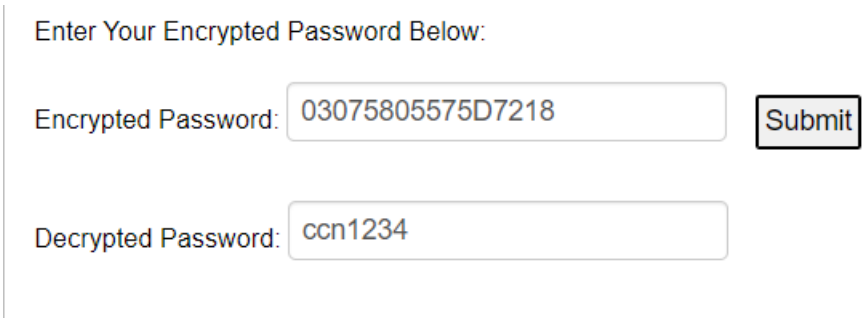
Router(config)#service password-encryption

```
Router(config)#do show running-config | section enable
enable password 7 03075805575D7218
```

We can crack this password

https://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/358-cisco-type7-password-crack.html

to decrypt this password go to above link and put this value on Encrypted Password section " 03075805575D7218 " and press submit button.



Now, because of this weakness we most probably assign password in encrypted format

Router(config)#enable secret ccn123

```
Router(config)#do show running-config | section enable
enable secret 5 $1$36UY$lD4YFKJc.LsdkzzrZSKzy/
```

This password is now encrypted in md5 hash value. Now, this value is not reversible.

PASSWORD RECOVERY

if we fail to remember the password then the only condition is to recover the password this situation is not that often in company. we need to know what to do in such condition.

ROUTER PASSWORD RECOVERY

1.First Check Router Register Value

Router#show version

In this command we can see the register value

Configuration register is 0x2102

- 0x2102 is a default value by reading this value router read the startup-config
- 0x2142 is another value by reading this value router skip the startup-config

So we have to change this value but we can't get inside the router CLI .so what else we can do is

Go to routers rommon mode (read only memory monitor mode).

1.Restart the router

2.When router is decompressing the iso image press button

CTRL + C

OR

CTRL + PAUSE/BREAK

3.And enter in rommon mode

Now change the register value

rommon 1 > confreg 0x2142

rommon 2 > boot

after booting the router go to privilege type **#show version**

Configuration register is 0x2142

It will show you 0x2142

Now, bring startup-config to running-config

Router#copy startup-config running-config

4.It is the time to change the password or remove the password

5.After changing the password change the register value as well

Router(config)#config-register 0x2102

Now, to verify

Router#show version

It will show you output like this

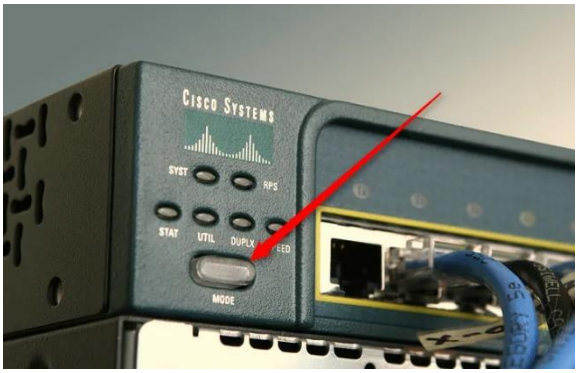
Configuration register is 0x2142 (will be 0x2102 at next reload)

After all this save the configuration

Router# write memory

SWITCH PASSWORD RECOVERY

Because of password we can't enter in switch so we have to recover the password by entering in switch mode. by clicking mode button on cisco switch while decompressing the image. We will enter in switch mode.



switch: flash_init …..(to initiate flash)

switch:dir flash: ……(to check the flash content)

switch store all the configuration in config.text file so if we change the file extension then the file will not be in readable format

switch: rename flash:config.text config:config.aaa

switch:reset …..(to start the switch)

after booting the switch,

check out the flash of switch

switch#dir flash:

now you can see the **config.aaa** file > change it back to **config.text**

switch#rename flash:config.aaa flash:config.text

now,get back your startup-config

switch#copy startup-config running-config

change all the password and then save the configuration

IOS UPGRADATION

IOS stands for INTERNETWORK OPERATING SYSTEM which is a Basic OS for all cisco Router and Switches.

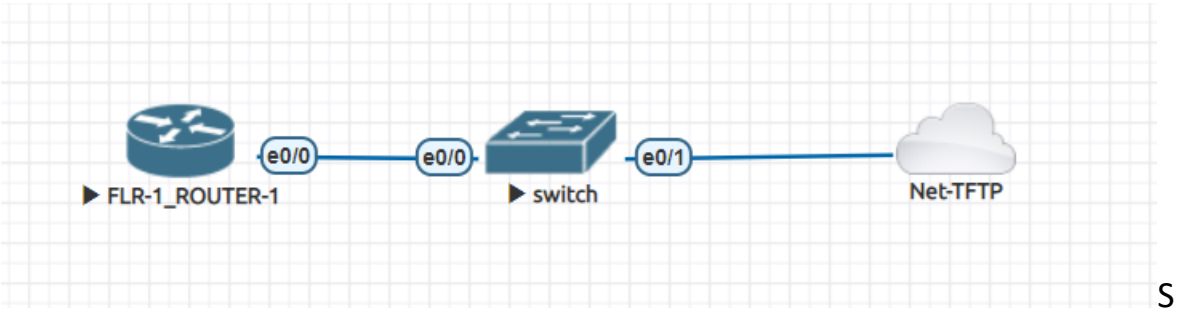
Certainly, Cisco launches a New updates in their operating system like current version of cisco IOS is 15.1.1 after some fixes cisco launches a new update which will be like 15.1.2. so here we have to upgrade the old OS with new one.

How to do it?

Let's see,

On ROUTER,

Here is the reference diagram,



S

In the above reference lab "FLR-1_ROUTER-1"is the main router. then, that Net-TFTP is our real pc connected in a network

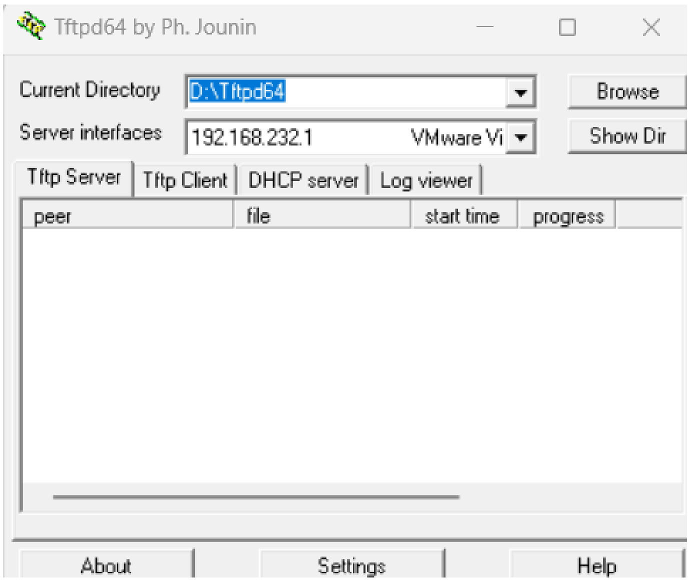
Before going for upgradation we took backup of the configuration file and current IOS version just to take care from future uncertainty.

1.Take Configuration backup of Device

```
FLR-1_ROUTER-1#copy running-config tftp:
Address or name of remote host []? 192.168.232.1
Destination filename [flr-1_router-1-confg]?
!!
1121 bytes copied in 0.055 secs (20382 bytes/sec)
```

we are using tftpd64 tool to create our pc as a TFTP se

NOTE:- All the upcoming task like IOS upgradation , configuration file and IOS file backup .all are done on real devices or we can do it cisco packet tracer if you don't have devices to co



Here is the first look of the tftpd64 tool

2.Take IOS back up on device

FLR-1_ROUTER-1#copy flash: tftp:

Then, provide remote address of the host means address of TFTP server => now provide source file which will be going copy from routers flash to

```
FLR-1_ROUTER-1#copy flash: tftp
Source filename []? c2800nm-advipservicesk9-mz.151-4.M1.bin
Address or name of remote host []? 192.168.10.1
Destination filename [c2800nm-advipservicesk9-mz.151-4.M1.bin]?
```

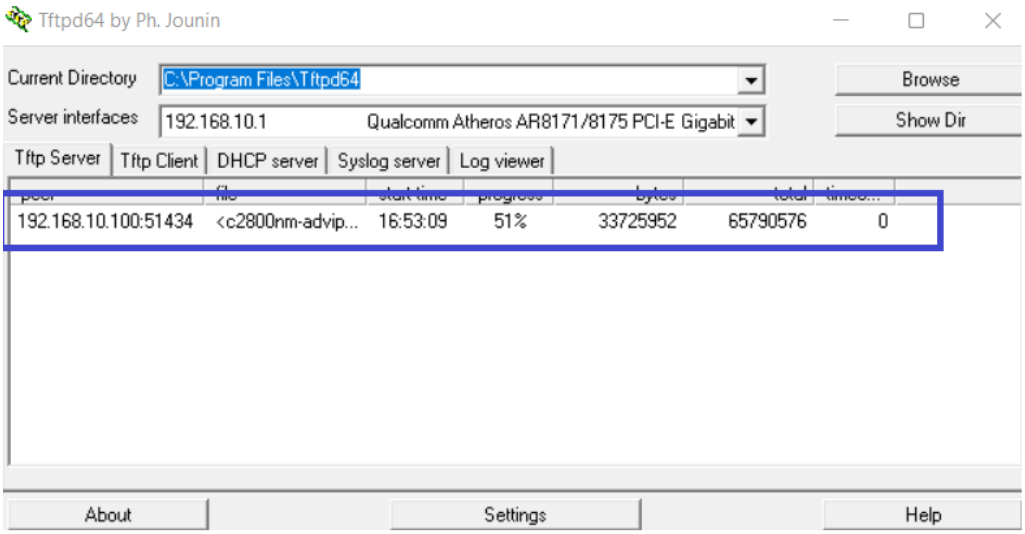
Here we can take backup of IOS file

Now, how to load IOS in device (it only support actual device)

FLR-1_ROUTER-1#copy tftp: flash:

```
FLR-1_ROUTER-1#copy tftp: flash:
Address or name of remote host []? 192.168.10.1
Source filename []? c2800nm-advipservicesk9-mz.151-4.M1.bin
Destination filename [c2800nm-advipservicesk9-mz.151-4.M1.bin]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing tftp://192.168.10.1/c2800nm-advipservicesk9-mz.151-4.M1.bin...
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
 ...erased
Erase of flash: complete
Loading c2800nm-advipservicesk9-mz.151-4.M1.bin from 192.168.10.1 (via FastEthernet0/0): !!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 65790576 bytes]

Verifying checksum... cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccc OK (0xAAA5)
65790576 bytes copied in 1854.112 secs (35484 bytes/sec)
```

While copying of this data, tftpd64 looks like



Provide them remote address of tftp server and file name of the IOS which we want to load

Then it will start copying the file. It will take some time to copy data.

Similarly, we can do reversal of configuration file.

Provide them remote address of the tftp server. And source file name.

WHAT IF WE DO HAVE TWO OPERATING SYSTEM ON DEVICE. then,

```
FLR-1_ROUTER-1(config)#boot system flash c2800nm-advipservicesk9-mz.151-4.M1.b$
```

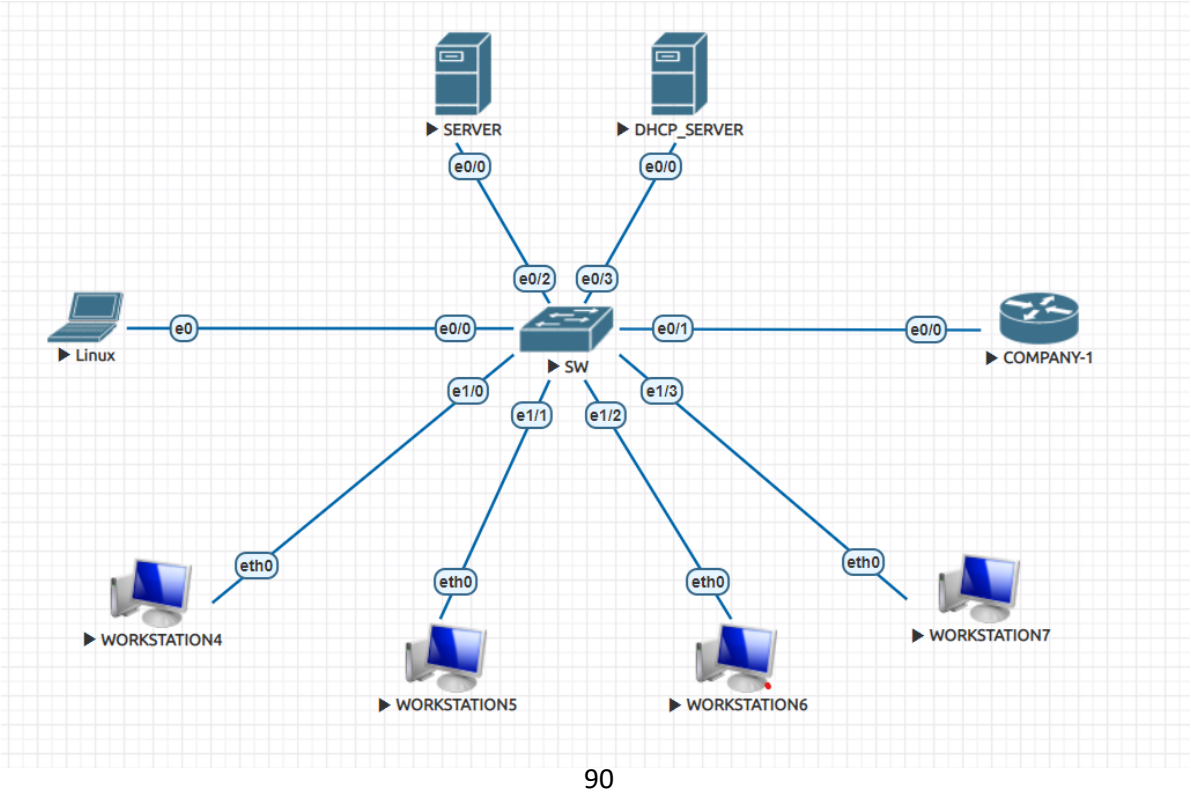
By applying the above command, we can specify the OS which will be loading at the time of booting.

L2 SECURITY

- L2 security means overall switch security. when it comes to LAN network we have to secure the network switches and when it comes to internet we have to secure routers by doing proper configuration.
- So, in LAN network there is possibility that a rouge employee can attack a company's IT Infra with some malicious intention. Just like to steal company's data, to create jitter in a network, to redirect company's employees to malicious site just to gather information.
- in such situation how can we secure our organization, so here is the solution – L2 security

In This Scenario We Have to Consider Potential Threats And Make Our Lan Network More Secure Against The Attacks

ATTACKS	SECURITY
DHCP starvation attack	SWITCHPORT SECUIRTY
MAC spoofing	
MAC flooding	
CDP flooding	
Rouge DHCP server / DHCP spoofing	DHCP SNOOPING
IP spoofing	IP SOURCE GUARD
ARP poisoning	DYNAMIC ARP INSPECTION (DAI)
STP attacks	BPDU GUARD / BPDU FILTER / ROOT GUARD

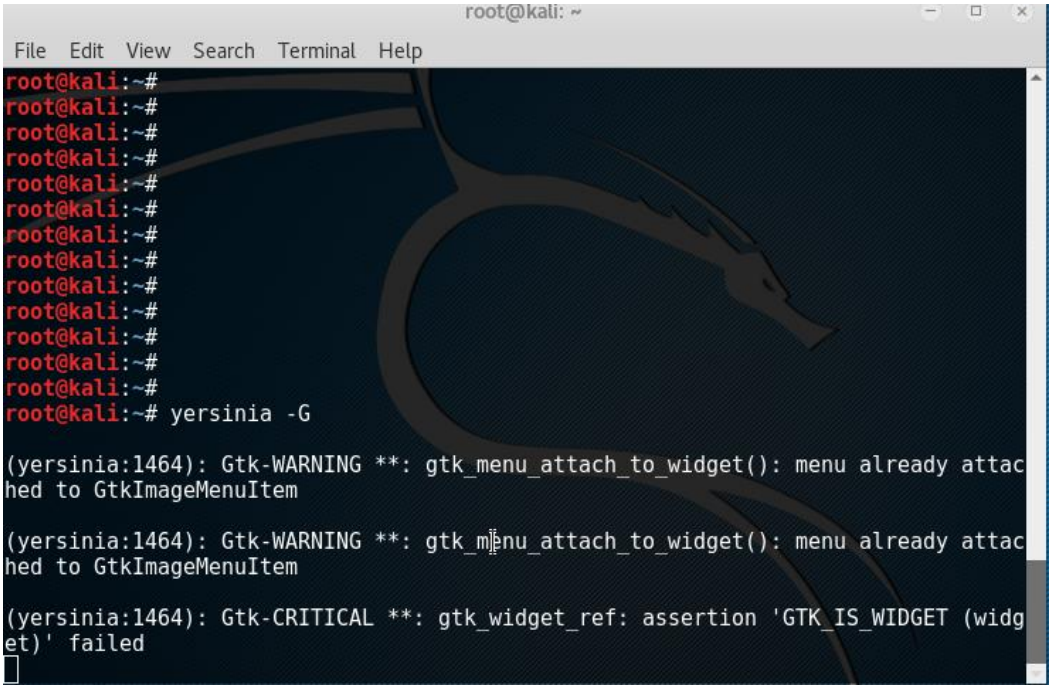


1.DHCP STRAVATION ATTACK

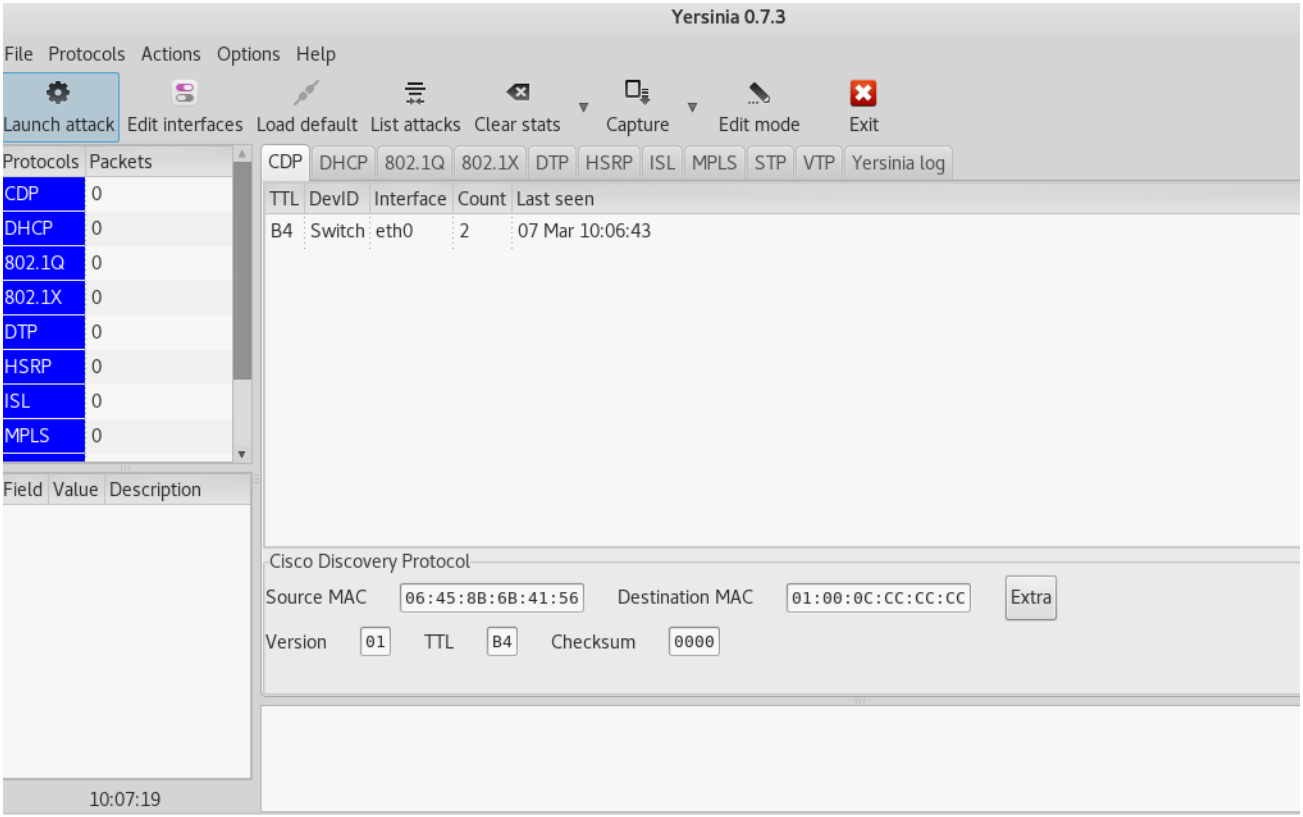
In this attack linux PC fetch all the IP of DHCP pool and left it with 0 IP's to assign to genuine user.

How to perform this attack

Go to linux =>Terminal => yersinia -G



Tool like this will open



This tool can perform different types of attacks

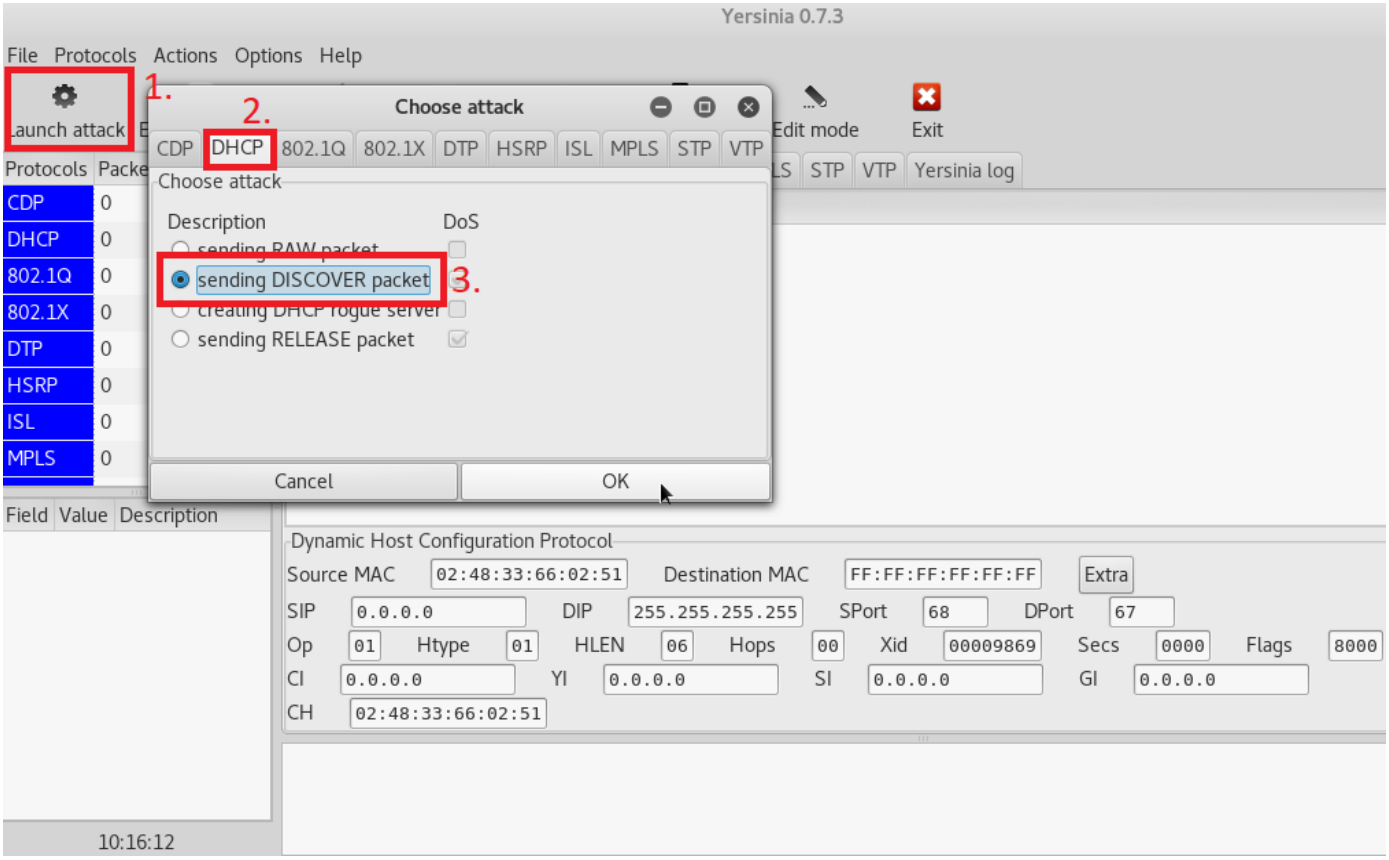
First, we are going do DHCP starvation attack

Before this attack DHCP server allotted only two IP's

```
DHCP_SERVER#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.1        0050.0000.0900          Mar 08 2023 04:59 PM    Automatic
192.168.10.2        0100.5079.6668.04       Mar 08 2023 05:11 PM    Automatic
```

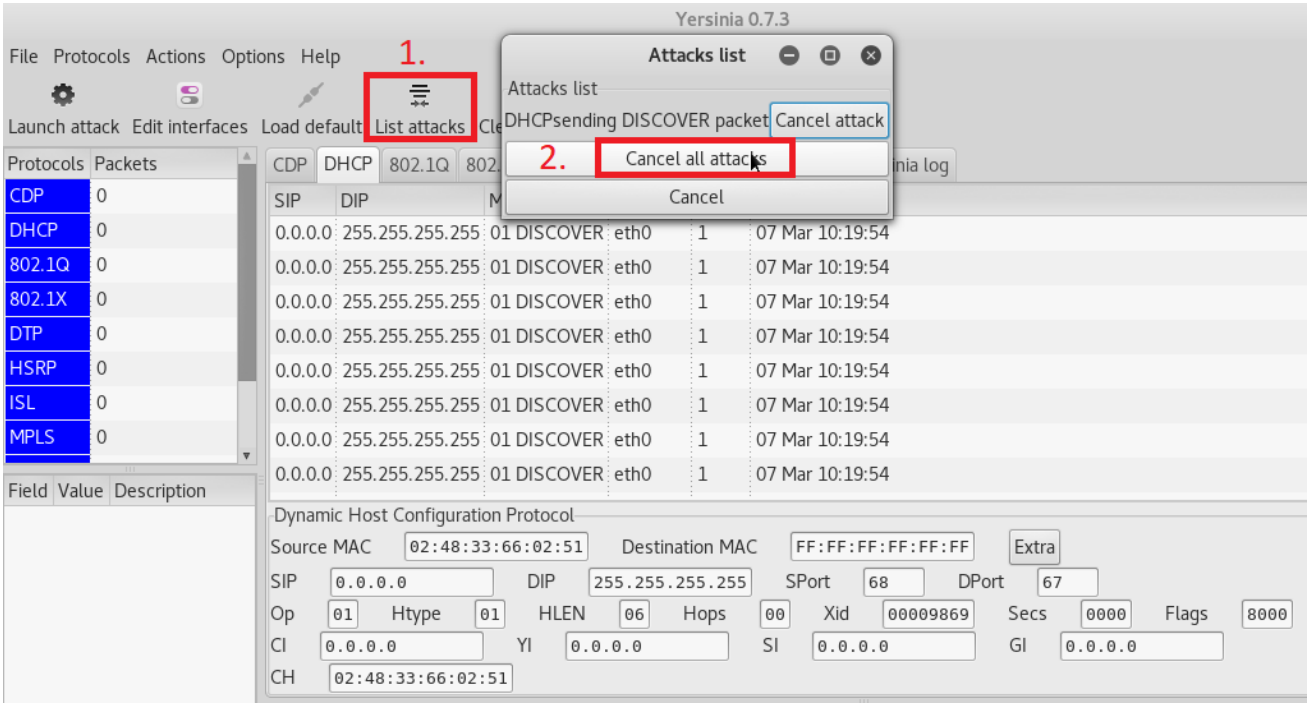
Let's perform attack

1.launch attack => 2. DHCP tab => 3. Sending DISCOVER packet => OK



How to stop attack

1.list attack => 2. Cancel all attacks



Effect of this attack is pool of DHCP server will get empty

```
DHCP_SERVER# show ip dhcp pool

Pool CCN-LAN :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 251
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 0.0.0.0              192.168.10.1     - 192.168.10.254    251
```

See leased addresses is 251 means all IP's of this pool is allotted.

Effect on switch

```
Switch#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 13635
Static  Address Count  : 0
Total Mac Addresses    : 13635

Total Mac Address Space Available: 212588024
```

See dynamic address count is 13,635 it means switch reads multiple MAC addresses. we also can see it with command

#show mac address-table

2.MAC SPOOFING

Mac spoofing means to mask someone's mac address and put it on our interface.

How to perform this attack

Select a target = workstation4 is our target => command - show ip => observe MAC – 00:50:79:66:68:04

```
WRKST4> show ip

NAME          : WRKST4[1]
IP/MASK       : 192.168.10.2/24
GATEWAY       : 192.168.10.254
DNS           : 8.8.8.8
DHCP SERVER   : 192.168.10.253
DHCP LEASE    : 82504, 86400/43200/75600
DOMAIN NAME   : ccn.com
MAC           : 00:50:79:66:68:04
LPORT         : 20000
RHOST:PORT    : 127.0.0.1:30000
MTU           : 1500
```

Observe this mac of workstation because we are spoofing this mac and putting it on linux pc

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.1  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::250:ff:fe00:900  prefixlen 64  scopeid 0x20<link>
        ether 00:50:00:00:09:00  txqueuelen 1000  (Ethernet)
        RX packets 3472  bytes 306366 (299.1 KiB)
        RX errors 0  dropped 23  overruns 0  frame 0
        TX packets 576290  bytes 164810004 (157.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Default mac address of this linux pc 00:50:00:00:09:00

Now we have to change linux mac address with workstation4 mac address

With the use of macchanger tool command => macchanger -m 00:50:79:66:68:04 eth0

```
root@kali:~# macchanger -m 00:50:79:66:68:04 eth0
Current MAC:   00:50:00:00:09:00 (NEXO COMMUNICATIONS, INC.)
Permanent MAC: 00:50:00:00:09:00 (NEXO COMMUNICATIONS, INC.)
New MAC:       00:50:79:66:68:04 (PRIVATE)
```

New spoofed mac address of linux pc

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.1  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::250:ff:fe00:900  prefixlen 64  scopeid 0x20<link>
        ether 00:50:79:66:68:04  txqueuelen 1000  (Ethernet)
        RX packets 3472  bytes 306366 (299.1 KiB)
        RX errors 0  dropped 23  overruns 0  frame 0
        TX packets 585498  bytes 165307468 (157.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

This is how we can spoof the mac address

How to change back it to normal

Same macchanger tool with command of > macchanger -p eth0

```
root@kali:~# macchanger -p eth0
Current MAC:   00:50:79:66:68:04 (PRIVATE)
Permanent MAC: 00:50:00:00:09:00 (NEXO COMMUNICATIONS, INC.)
New MAC:       00:50:00:00:09:00 (NEXO COMMUNICATIONS, INC.)
```

Check it on interface properties

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.1  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::250:ff:fe00:900  prefixlen 64  scopeid 0x20<link>
        ether 00:50:00:00:09:00  txqueuelen 1000  (Ethernet)
        RX packets 3472  bytes 306366 (299.1 KiB)
        RX errors 0  dropped 23  overruns 0  frame 0
        TX packets 576290  bytes 164810004 (157.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3.MAC FLOODING

In mac flooding attack we flood the mac address table of the switch.

Before this attack switch mac table

```
Switch#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 3
Static  Address Count  : 0
Total Mac Addresses    : 3

Total Mac Address Space Available: 212588024
```

Now perform an attack with the command of **~#macof -i eth0**

```
root@kali:~# macof -i eth0
```

To stop this attack press **CTRL+C**

After attack switch MAC Address table get flooded

```
Switch#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 13030
Static  Address Count  : 0
Total Mac Addresses    : 13030

Total Mac Address Space Available: 212588024
```

4.CDP FLOODING

In the CDP Flooding Attack, we flood the CDP table of the switch with fake entries

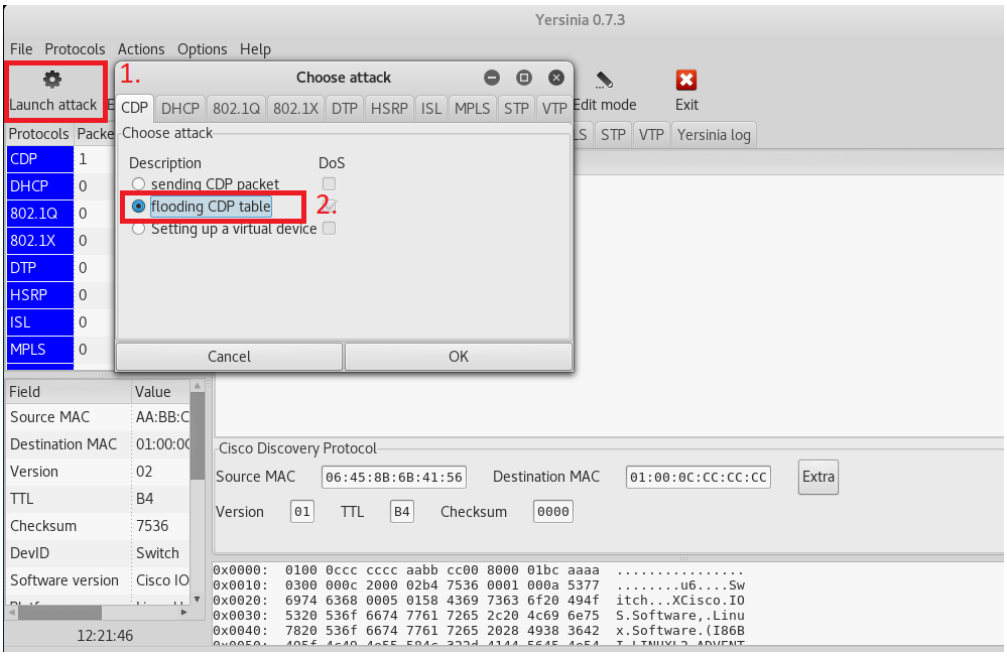
Before starting the attack

```
Switch#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SERVER           Eth 0/2           156              R B   Linux Uni Eth 0/0
DHCP_SERVER      Eth 0/3           156              R B   Linux Uni Eth 0/0
COMPANY-1        Eth 0/1           166              R B   Linux Uni Eth 0/0

Total cdp entries displayed : 3
```

Check it out, at last CDP entries is 3

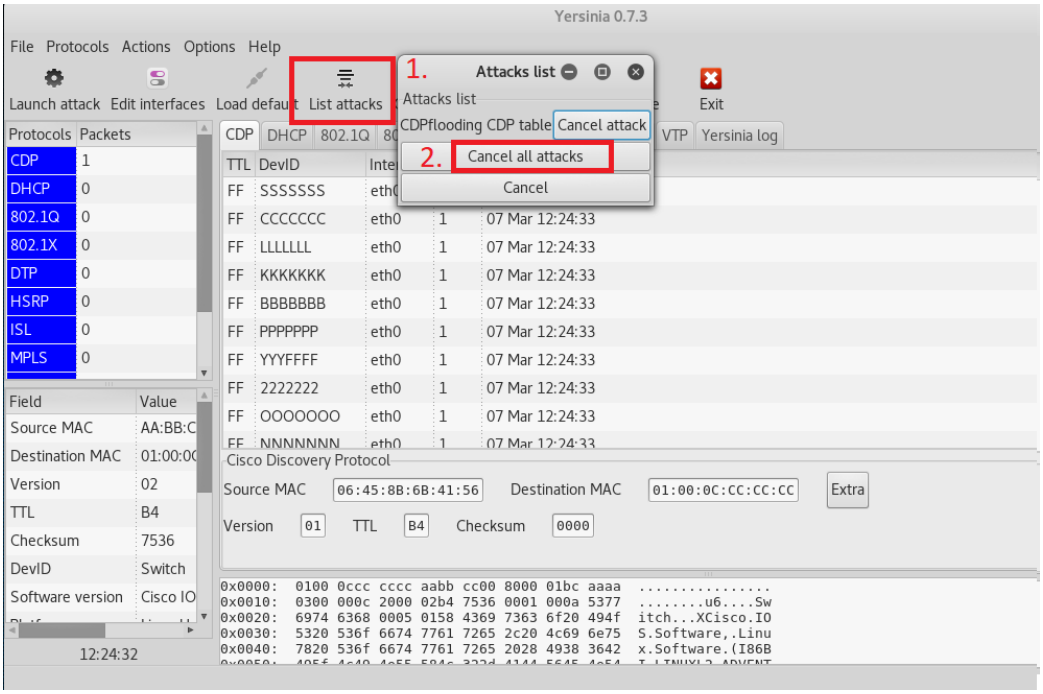
Now, perform CDP flooding attacks

Go to terminal => yersinia -G > Move to CDP tab => flooding CDP table > OK



To stop attack

List attacks => cancel all attacks



After this attack check CDP table, you will see it flooded.

Now, how can we secure switches from such type of attacks cause all of this attacks are mac based attacks.

Here we use **SWITCHPORT SECURITY**

Switch(config)#interface eth 0/0

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security mac-address 00:50:00:00:09:00 ….(manual mac)

OR

Switch(config-if)#switchport port-security mac-address sticky(sticky means any mac address)

Switch(config-if)#switchport port-security maximum 1 …..(max mac accepted is 1)

Switch(config-if)#switchport port-security violation protect ..(take action if max limit violate)

Switch(config-if)#switchport port-security ……(to activate this above parameter)

For violation we do have 3 options. we can use anyone of them as per policy.

- Protect—This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses when over the allowed MAC address limit. When configured with this mode, no notification action is taken when traffic is dropped.
- Restrict—This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses and make interface status as error-disable. when over the allowed MAC address limit. When configured with this mode, a syslog message is logged, a Simple Network Management Protocol (SNMP) trap is sent, and a violation counter is incremented when traffic is dropped.
- Shutdown—This mode is the default violation mode; when in this mode, the switch will automatically force the switchport into an error disabled (*err-disable*) state when a violation occurs. While in this state, the switchport forwards no traffic. The switchport can be brought out of this error disabled state by issuing the *errdisable recovery cause* CLI command or by disabling and reenabling the switchport.

Basically, we activate switchport security on all the Access Ports interfaces except the trunk interface.

5.ROUGE DHCP SERVER / DHCP SPPOFING

In this attack we create a fake/rouge DHCP server to redirect users from its original network. This attack is a part of MITM (man in the middle) attack.

Let's perform this attack

First, we have to do DHCP starvation attack and fetch all the IP's. so that genuine user won't get IP from original DHCP server. now the real task is to generate Rouge DHCP in a network and PC's in a network get Rouge DHCP networks IP.

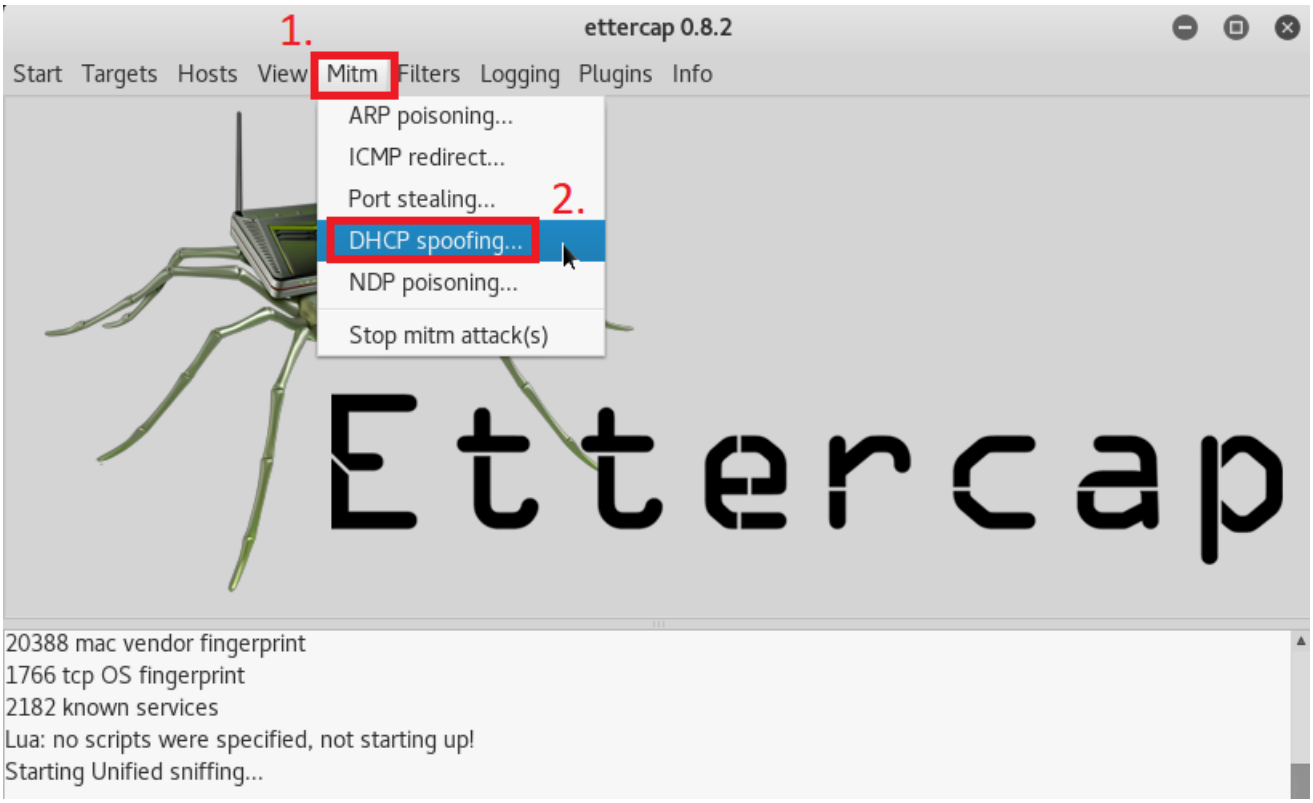
Go to Linux - terminal => ettercap -G

```
root@kali:~# ettercap -G
```

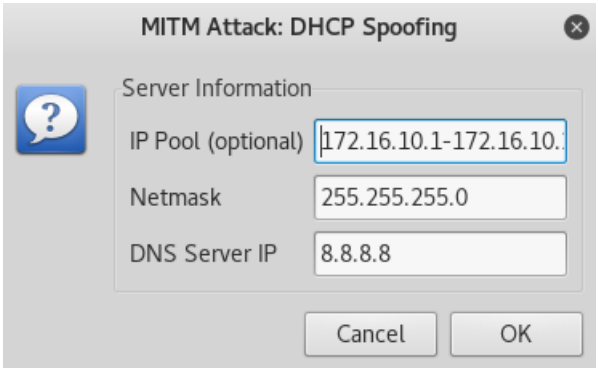
Now tool like this will open

After opening to click on Sniff => unified sniffing => Network interface – eth0

Then, go to MITM > DHCP Spoofing



Now set the parameter and then click OK



Will create a Rouge DHCP server

Our existing network is 192.168.10.0/24 but, Rogue DHCP Pool IP is 172.16.10.0/24

After, Rogue DHCP server creation pc will take IP of that network

```
WRKST4> ip dhcp
DORA IP 172.16.10.1/24 GW 192.168.10.1

WRKST4> show ip

NAME         : WRKST4[1]
IP/MASK      : 172.16.10.1/24
GATEWAY      : 192.168.10.1
DNS          : 8.8.8.8
DHCP SERVER  : 192.168.10.1
DHCP LEASE   : 1793, 1800/900/1575
MAC          : 00:50:79:66:68:04
LPORT        : 20000
RHOST:PORT   : 127.0.0.1:30000
MTU          : 1500
```

Now we have to secure this network from such attack with DHCP snooping security

DHCP SNOOPING SECURITY

In this security we are untrusting all the interfaces of switch except one which is directly connected to DHCP Server. So, we have to make that interface trust by applying command.

Switch(config)#ip dhcp snooping vlan 1 …..(to set snooping parameter)

Switch(config)#ip dhcp snooping ……..(to activate DHCP snooping)

Now we are trusting only one port which is connected to Actual DHCP server

Switch(config)#interface ethernet 0/3

Switch(config-if)#ip dhcp snooping trust

Switch(config-if)#exit

When we activate DHCP Snooping it will add on additional information to the packet- that information is VLAN ID and interface details. Now this additional information won't understand by actual DHCP server for that we have to put command to reply it back

DHCP_SERVER(config)#ip dhcp relay information trust-all

By this command router will understand the additional information

VERIFICATION

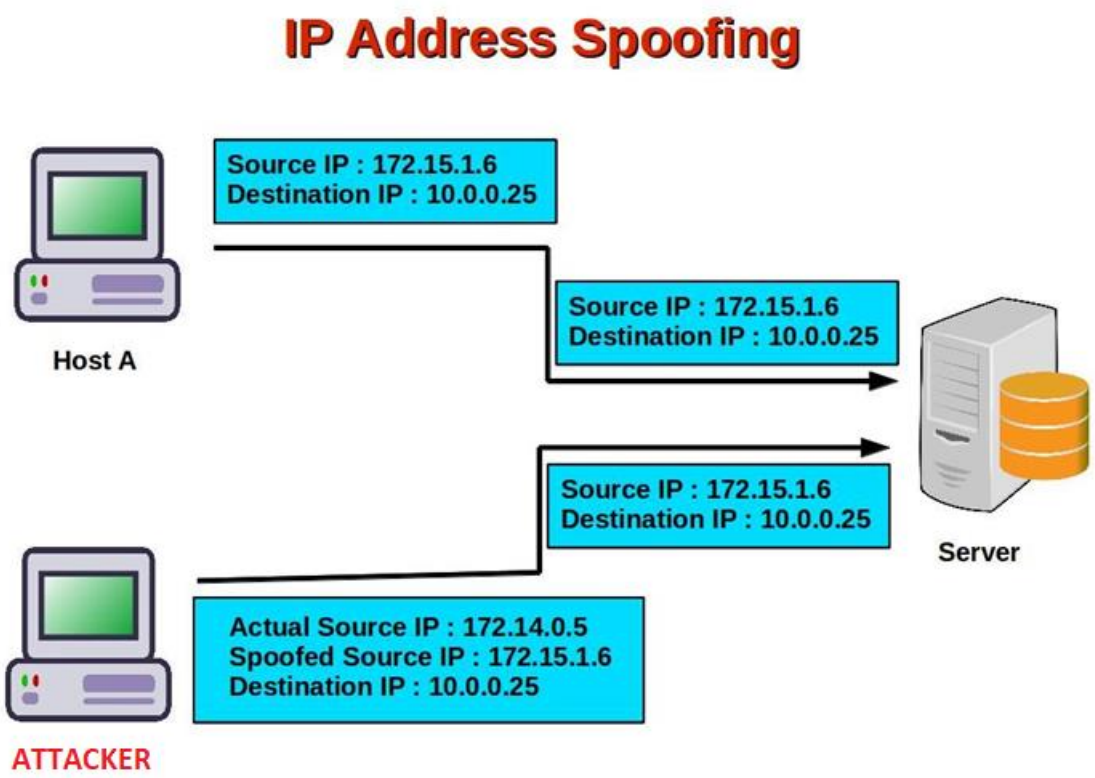
```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------
-----
00:50:79:66:68:04   192.168.10.2     86370       dhcp-snooping   1     Ethernet1/0
Total number of bindings: 1
```

In this image you can see the VLAN & INTERFACE heading and it actually adds up that information to the data packet.

We implement this security on global mode to untrust all the ports. We make interface trust only for actual port which is connected to DHCP server and the trunk ports from where the traffic is ingresses.

6.IP SPPOFING

In this type of attack we spoof the IP of targeted pc with some malicious intent. if we able to spoof that IP we will represent ourselves as same as that pc



In this scenario attacker successfully spoofed the IP of Host A. by spoofing the IP attacker can bypass the ACL.

We change the IP by assigning static ip .then, only we can change the actual ip with spoofed ip.to stop all such attack we implement a security called IP SOURCE GUARD

IP SOURCE GUARD

IP Source Guard (IPSG) is **a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings**

To implement security

Switch(config-if)#interface ethernet 1/0

Switch(config-if)#ip verify source

Switch(config-if)#exit

VERIFICATION OF DHCP SNOOPING BINDING

Switch#show ip dhcp snooping binding

OR

Manual IP SOURCE BINDING

Switch(config)#ip source binding 00:50:00:00:02:00 vlan 1 192.168.10.100 interface ethernet 0/1

OR

This IP SOURCE GUARD we verify with the port-security

Switch(config-if)#interface ethernet 1/0

Switch(config-if)#ip verify source port-security

Switch(config-if)#exit

VERIFICATION

Switch# show ip verify source

DYNAMIC ARP INSPECTION (DAI)

Dynamic ARP inspection is a security feature we used reduce a risk platform regarding arp requests. Like ARP flooding, ARP poisoning, etc

Implementation

Switch(config)#ip arp inspection vlan 1

By applying this command switch untrust all the ports for ARP requests. we left all the ports as untrust for PC's . we most probably make port trust for the Servers and trunk ports which is only connected with the other switch.If port is in trust then it bypass arp inspection validation check.

How to do it

Switch(config)#interface ethernet 0/2

Switch(config-if)#ip arp inspection trust .....(to make interface trust for ARP inspection)

Switch(config-if)#ip arp inspection limit rate 5 ……(to limit the arp packet per sec)[OPTIONAL]

Switch(config-if)#exit

DYNAMIC ARP INSPECTION VERIFY THE ARP PACKET WITH THE DHCP SNOOPING BINDING TABLE

to statically verifies the ARP entries

Switch(config)#arp access-list ARP-LIST

Switch(config-arp-nacl)# permit ip host 192.168.10.253 mac host aabb.cc00.2000

Switch(config-arp-nacl)#exit

Switch(config)#ip arp inspection filter ARP-LIST vlan 1

VERIFICATION

Switch# show ip arp inspection

Switch# show ip arp inspection statistics

7.STP ATTACKS

Spanning tree protocol is also a attackable platform on a switch. so, what kind of attacks will perform on a switch. spanning tree root status stealing/spoofing , BPDU flooding ,etc.

Just to save our network from such types of attack we will implement some sort of security

BPDU GUARD

Switch(config)#interface ethernet 1/0

Switch(config-if)# spanning-tree portfast

Switch(config-if)# spanning-tree bpduguard enable

Switch(config-if)# exit

We enable BPDUGUARD with PORTFAST because, when enable PORTFAST switch won't sends BPDU on that interface and when we enable BPDU GUARD switch won't receive any BPDU's on that interface

BPDU FILTER

Switch(config)#interface ethernet 1/0

Switch(config-if)#spanning-tree portfast

Switch(config-if)#spanning-tree bpdufilter enable

Switch(config-if)#exit

If we use BPDUFILTER only then what does BPDUFILTER do is it will listen the BPDU's but won't reply it back and PORTFAST won't send an update on that interface. and when we implement BPDUFILTER with PORTFAST it will create some mess around like if we receive a BPDU from an unexpected interface it will lose its status of PORTFAST and it will create a temporary looping.

So, in most cases we prefer BPDU GUARD with PORTFAST

ROOT GUARD

We do use root guard because we don't want that any lowest priority or lowest mac address will MAC address will influence the switch STP selection process. what does root guard do is it will ignore the bpdu which consist the lowest priority and lowest mac

Switch(config)#interface ethernet 1/0

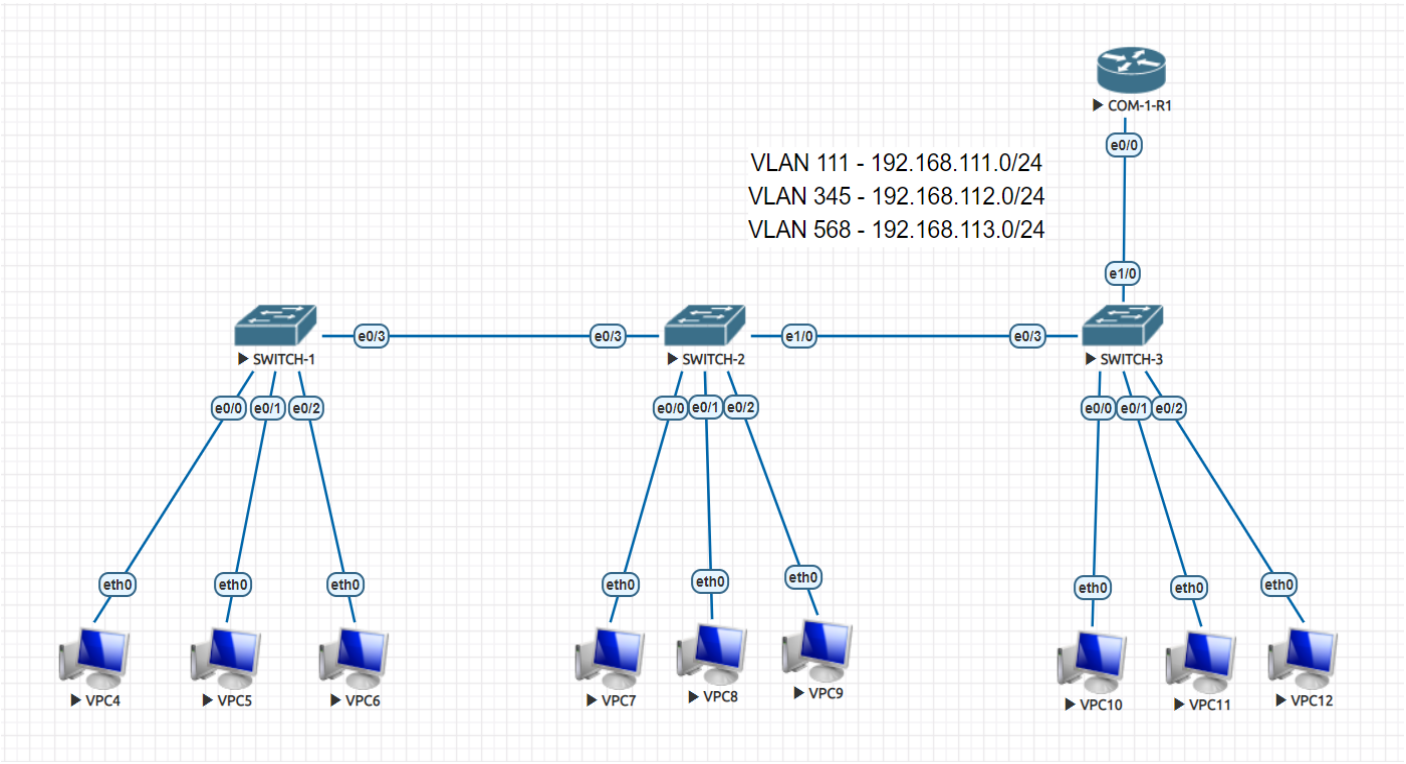
Switch(config-if)#spanning-tree guard root

Switch(config-if)#exit

VERIFICATION

Switch#show running-config | section interface ethernet 1/0

L2 SECURITY LAB



TASK – 16

Task 16.1 Host Name Should Be Same As Mention In First Look Name

Task 16.2 Create and Implement

VLAN - 111 => SALES_DEPT = 192.168.111.0/24

VLAN - 345 => MRKT_DEPT = 192.168.112.0/24

VLAN - 568 => IT_DEPT = 192.168.113.0/24

VTP DOMAIN - ccn.com

VTP PASSWORD - ccn@123

VTP mode - SWITCH-1=SERVER, SWITCH-2 =CLIENTS , SWITCH-3 = CLIENTS

Task 16.3 Secure Network from MAC BASED ATTACK

Task 16.4 Secure Network from DHCP SPOOFING ATTACK

Task 16.5 Secure Network from IP SPOOFING ATTACK

Task 16.6 Secure Network Form ARP ATTACKS

Task 16.7 secure network from BPDU FLOODING ATTACKS

Task 16.8 MAKE SWITCH-1 AS ROOT BRIDGE AND make sure no infirioe BPDU WILL AFFECT THE NETWORK

VERIFICATION

Switch-1

```
hostname SWITCH-1
```

```
ip arp inspection vlan 111,345,568
!
!
!
ip dhcp snooping vlan 111,345,568
```

```
spanning-tree vlan 111,345,568 priority 24576
!
```

```
interface Ethernet0/0
 switchport access vlan 111
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.6804
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 spanning-tree guard root
 ip verify source
!
interface Ethernet0/1
 switchport access vlan 345
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.6805
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 spanning-tree guard root
 ip verify source
```

```
interface Ethernet0/2
 switchport access vlan 568
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.6806
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 spanning-tree guard root
 ip verify source
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree guard root
 ip dhcp snooping trust
```

SWITCH-2

```
hostname SWITCH-2
```

```
ip arp inspection vlan 111,345,568
!
!
!
ip dhcp snooping vlan 111,345,568
```

```
interface Ethernet0/0
 switchport access vlan 111
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 ip verify source
!
interface Ethernet0/1
 switchport access vlan 345
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 ip verify source
!
```

```
interface Ethernet0/2
 switchport access vlan 568
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 ip verify source
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
!
```

SWITCH-3

```
hostname SWITCH-3
!
```

```
ip arp inspection vlan 111,345,568
!
!
!
ip dhcp snooping vlan 111,345,568
```

```
interface Ethernet0/0
 switchport access vlan 111
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.680a
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 ip verify source
!
interface Ethernet0/1
 switchport access vlan 345
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 ip verify source
```

```
interface Ethernet0/2
 switchport access vlan 568
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
 ip verify source
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip dhcp snooping trust
```

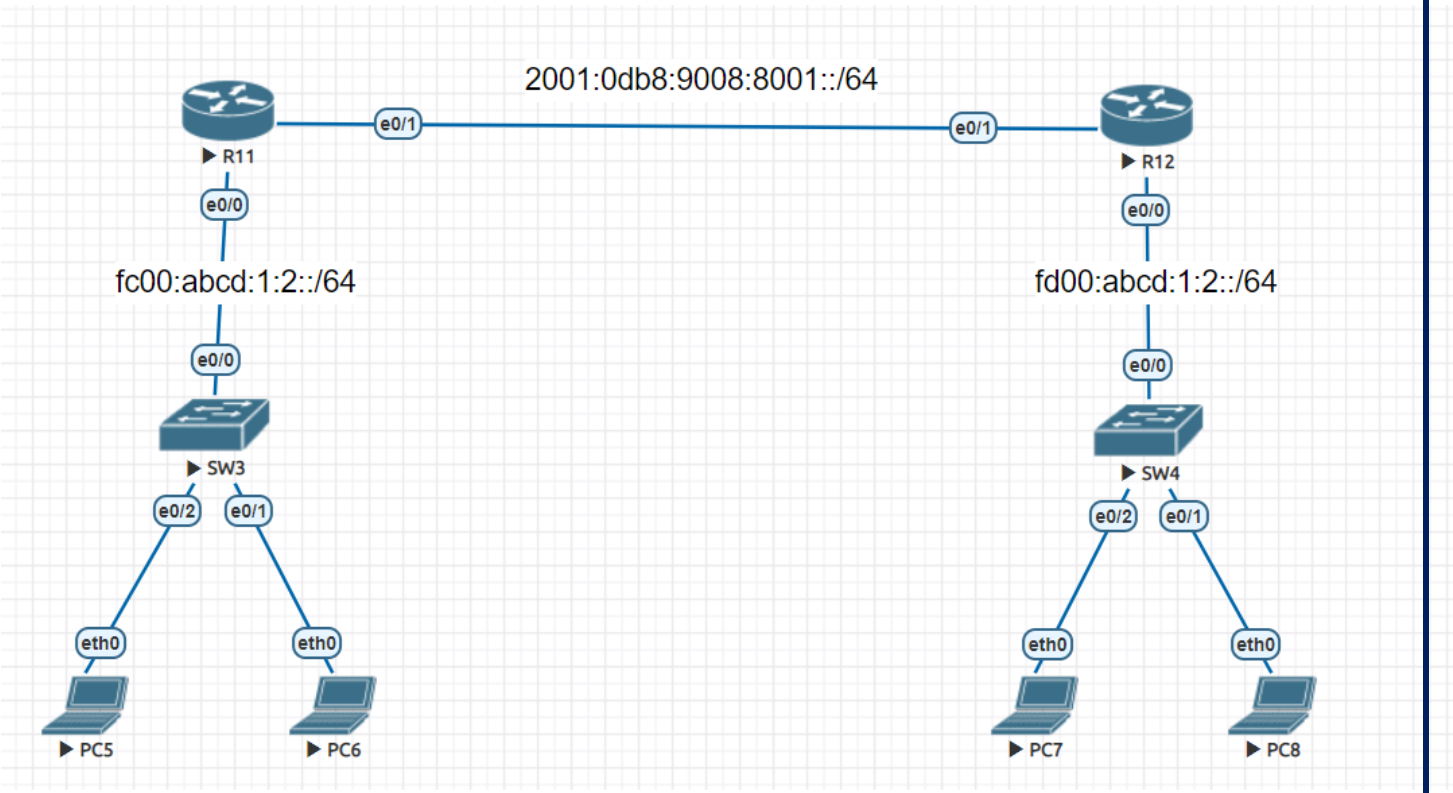
COM-1-R1

```
hostname COM-1-R1
!
```

```
ip dhcp relay information trust-all
!
ip dhcp pool CCN-SALES
 network 192.168.111.0 255.255.255.0
 default-router 192.168.111.254
 dns-server 8.8.8.8
!
ip dhcp pool CCN-MRKT
 network 192.168.112.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.112.254
!
ip dhcp pool CCN-IT
 network 192.168.113.0 255.255.255.0
 default-router 192.168.113.254
 dns-server 8.8.8.8
!
```

```
interface Ethernet0/0
 no ip address
!
interface Ethernet0/0.111
 encapsulation dot1Q 111
 ip address 192.168.111.254 255.255.255.0
!
interface Ethernet0/0.345
 encapsulation dot1Q 345
 ip address 192.168.112.254 255.255.255.0
!
interface Ethernet0/0.568
 encapsulation dot1Q 568
 ip address 192.168.113.254 255.255.255.0
!
```

IPv6



TASK - 17

Task 17.1 Configure hostname as per the lab

Task 17.2 Configure the routers LAN interfaces with given IPv6 network and EUI-64. Now, fetch IP from it

Task 17.3 Configure the routers R11-eth 0/1, R12-eth 0/1

Task 17.4 Configure routers with the static ipv6 routing

Task 17.5 Configure routers with the OSPFv3

Task 17.6 Configure the router with EIGRP-ng

Task 17.7 Configure the routers with RIP-ng

After doing routing try to ping other network pc with each type of routing

VERIFICATION

R11

```
hostname R11
```

ROUTEING

```
ipv6 unicast-routing
```

By applying this command router start IPv6 routing

```
ipv6 route FD00:ABCD:1:2::/64 2001:DB8:9008:8001::2
ipv6 router eigrp 90
 eigrp router-id 10.1.1.1
!
ipv6 router ospf 100
 router-id 10.1.1.1
!
ipv6 router rip IPV6
```

```
interface Ethernet0/0
 no ip address
 ipv6 address FC00:ABCD:1:2::/64 eui-64
 ipv6 enable
 ipv6 eigrp 90
 ipv6 rip IPV6 enable
 ipv6 ospf 100 area 1
!
interface Ethernet0/1
 no ip address
 ipv6 address 2001:DB8:9008:8001::1/64
 ipv6 enable
 ipv6 eigrp 90
 ipv6 rip IPV6 enable
 ipv6 ospf 100 area 0
```

```
VPCS> ip auto
GLOBAL SCOPE      : fc00:abcd:1:2:2050:79ff:fe66:6805/64
ROUTER LINK-LAYER : aa:bb:cc:00:10:00
```

R12

```
hostname R12
```

ROUTING

```
ipv6 unicast-routing
```

```
ipv6 route FC00:ABCD:1:2::/64 2001:DB8:9008:8001::1
ipv6 router eigrp 90
 eigrp router-id 10.1.1.2
!
ipv6 router ospf 100
 router-id 10.1.1.2
!
ipv6 router rip IPV6
!
```

```
interface Ethernet0/0
 no ip address
 ipv6 address FD00:ABCD:1:2::/64 eui-64
 ipv6 enable
 ipv6 eigrp 90
 ipv6 rip IPV6 enable
 ipv6 ospf 100 area 1
!
interface Ethernet0/1
 no ip address
 ipv6 address 2001:DB8:9008:8001::2/64
 ipv6 enable
 ipv6 eigrp 90
 ipv6 rip IPV6 enable
 ipv6 ospf 100 area 0
!
```

```
VPCS> ip auto
GLOBAL SCOPE      : fd00:abcd:1:2:2050:79ff:fe66:6807/64
ROUTER LINK-LAYER : aa:bb:cc:00:20:00
```

Ping form PC5 to PC7

```
VPCS> ping fd00:abcd:1:2:2050:79ff:fe66:6807

fd00:abcd:1:2:2050:79ff:fe66:6807 icmp6_seq=1 ttl=60 time=1.916 ms
fd00:abcd:1:2:2050:79ff:fe66:6807 icmp6_seq=2 ttl=60 time=0.990 ms
fd00:abcd:1:2:2050:79ff:fe66:6807 icmp6_seq=3 ttl=60 time=1.355 ms
fd00:abcd:1:2:2050:79ff:fe66:6807 icmp6_seq=4 ttl=60 time=1.090 ms
fd00:abcd:1:2:2050:79ff:fe66:6807 icmp6_seq=5 ttl=60 time=1.490 ms
```

How to check routing table

Router# show ipv6 route