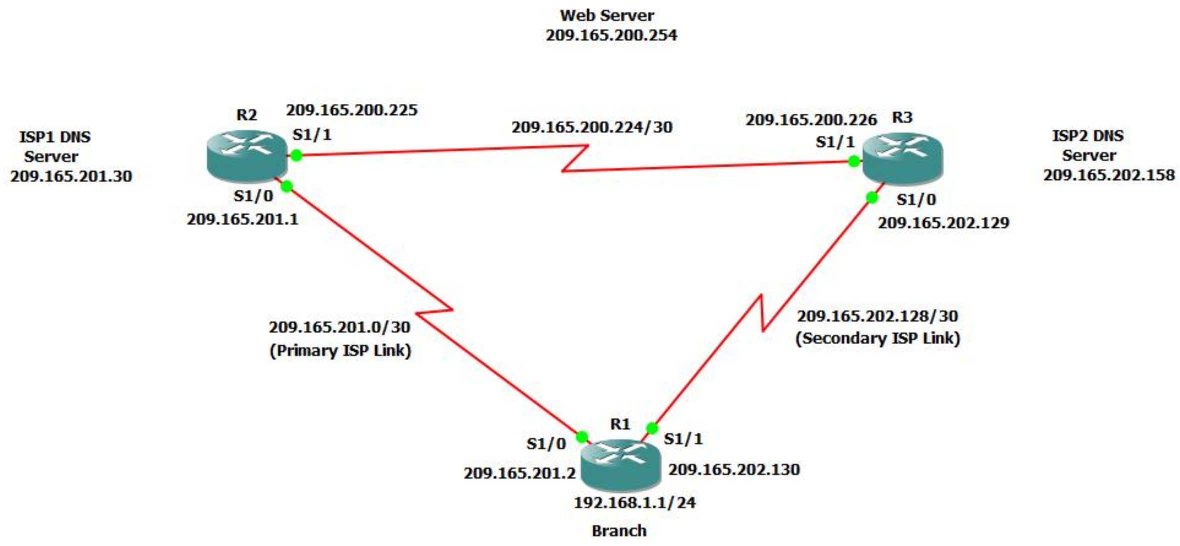
Prac 1

Aim:- Configure IP SLA Tracking and Path Control



Step 1:- Configure loopbacks and assign addresses.

Router R1 Console

interface Loopback0

description R1 LAN

ip address 192.168.1.1 255.255.255.0

exit

interface S1/0

description R1 → ISP1

ip address 209.165.201.2 255.255.255.252

clock rate 128000

bandwidth 128

no shutdown

exit

interface S1/1

description R1 → ISP2

ip address 209.165.202.130 255.255.255.252

bandwidth 128

no shutdown

exit

Router R2 Console (hostname ISP1)

hostname ISP1

interface Loopback0

description Simulated Internet Web Server

ip address 209.165.200.254 255.255.255.255

exit

interface Loopback1

description ISP1 DNS Server

ip address 209.165.201.30 255.255.255.255

exit

interface S1/0

description ISP1 → R1

ip address 209.165.201.1 255.255.255.252

bandwidth 128

no shutdown

exit

interface S1/1

description ISP1 → ISP2

ip address 209.165.200.225 255.255.255.252

clock rate 128000

bandwidth 128

no shutdown

exit

Router R3 Console (hostname ISP2)

hostname ISP2

interface Loopback0

description Simulated Internet Web Server

ip address 209.165.200.254 255.255.255.255

exit

interface Loopback1

description ISP2 DNS Server

ip address 209.165.202.158 255.255.255.255

exit

interface S1/0

description ISP2 → R1

ip address 209.165.202.129 255.255.255.252

clock rate 128000

bandwidth 128

no shutdown

exit

interface S1/1

description ISP2 → ISP1

ip address 209.165.200.226 255.255.255.252

bandwidth 128

no shutdown

exit

b) Verify the configuration by using the **show interfaces description** command. The output from router R1 is shown below.

Router R1 Console

show interfaces description | include up

Step 2:- Configure static routing.

The current routing policy in the topology is as follows:

1) Router R1 establishes connectivity to the Internet through ISP1 using a default static route.

2) ISP1 and ISP2 have dynamic routing enabled between them, advertising their respective public address pools.

3) ISP1 and ISP2 both have static routes back to the ISP LAN.

a) Implement the routing policies on the respective routers.

Router R1 Console

ip route 0.0.0.0 0.0.0.0 209.165.201.1

Router R2 Console (hostname ISP1)

router eigrp 1

network 209.165.200.224 0.0.0.3

network 209.165.201.0 0.0.0.31

no auto-summary

exit

ip route 192.168.1.0 255.255.255.0 209.165.201.2

Router R3 Console (hostname ISP2)

router eigrp 1

network 209.165.200.224 0.0.0.3

network 209.165.202.128 0.0.0.31

no auto-summary

exit

ip route 192.168.1.0 255.255.255.0 209.165.202.130

b) The Cisco IOS IP SLA feature enables an administrator to monitor network performance between Cisco devices (switches or routers) or from a Cisco device to a remote IP device.

Router R1 Console

tclsh

foreach address {

209.165.200.254

209.165.201.30

209.165.202.158

} { ping $address source 192.168.1.1 }

c) Trace the path taken to the web server, ISP1 DNS server, and ISP2 DNS server.

Router R1 Console

tclsh

foreach address {

209.165.200.254

209.165.201.30

209.165.202.158

} { trace $address source 192.168.1.1 }

Step 3:- Configure IP SLA probes.

a) Create an ICMP echo probe on R1 to the primary DNS server on ISP1 using the ip sla command.

Router R1 Console

ip sla 11

icmp-echo 209.165.201.30

frequency 10

exit

ip sla schedule 11 life forever start-time now

b) Verify the IP SLAs configuration of operation 11 using the **show ip sla configuration 11** command.

Router R1 Console

show ip sla configuration 11

c) Issue the **show ip sla statistics** command to display the number of successes, failures, and results of the latest operations.

Router R1 Console

show ip sla statistics

Router R1 Console

ip sla 22

icmp-echo 209.165.202.158

frequency 10

exit

ip sla schedule 22 life forever start-time now

exit

e) Verify the new probe using the **show ip sla configuration** and **show ip sla statistics** commands.

Router R1 Console

show ip sla configuration 22

show ip sla statistics 22

Step 4:- Configure tracking options.

a) On R1, remove the current default route and replace it with a floating static route having an administrative distance of 5.

Router R1 Console

no ip route 0.0.0.0 0.0.0.0 209.165.201.1

ip route 0.0.0.0 0.0.0.0 209.165.201.1 5

exit

b) Verify the routing table.

Router R1 Console

show ip route | begin Gateway

c) From global configuration mode on R1, use the **track 1 ip sla 11 reachability** command to enter the config-track subconfiguration mode.

Router R1 Console

track 1 rtr 11 reachability

delay down 10 up 1

exit

exit

debug ip routing

conf t

ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1

track 2 rtr 22 reachability

delay down 10 up 1

exit

exit

debug ip routing

conf t

ip route 0.0.0.0 0.0.0.0 209.165.202.129 3 track 2

exit

show ip route

Router R2 Console (hostname ISP1)

conf t

interface loopback 1

shutdown

Router R1 Console

show ip route

show ip sla statistics

trace 209.165.200.254 source 192.168.1.1

Router R2 Console (hostname ISP1)

no shutdown

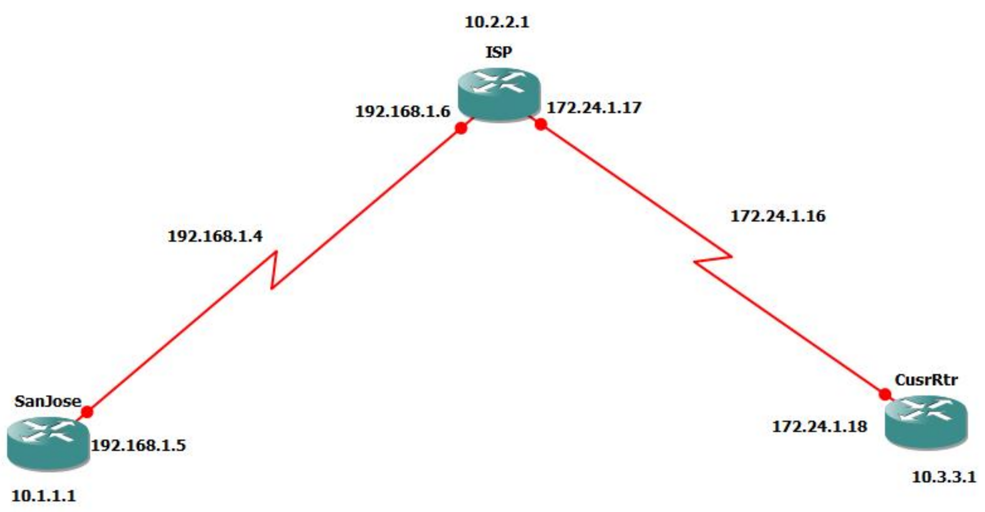
Router R1 Console

show ip route

show ip sla statistics

Prac 2

Aim:- Using the AS_PATH Attribute



Step 1:- Prepare the routers for the lab.

Router R1 (hostname SanJose)

hostname SanJose

interface Loopback0

ip address 10.1.1.1 255.255.255.0

exit

interface S1/0

ip address 192.168.1.5 255.255.255.252

clock rate 128000

no shutdown

Router R2 (hostname ISP)

hostname ISP

interface Loopback0

ip address 10.2.2.1 255.255.255.0

exit

interface S1/0

ip address 192.168.1.6 255.255.255.252

no shutdown

exit

interface S1/1

ip address 172.24.1.17 255.255.255.252

clock rate 128000

no shutdown

Router R3 (hostname CustRtr)

hostname CustRtr

interface Loopback0

ip address 10.3.3.1 255.255.255.0

exit

interface S1/1

ip address 172.24.1.18 255.255.255.252

no shutdown

b) Use **ping** to test the connectivity between the directly connected routers.

Ping 192.168.1.6

Step 3:- Configure BGP

Router R1 (hostname SanJose)

router bgp 100

neighbor 192.168.1.6 remote-as 300

network 10.1.1.0 mask 255.255.255.0

Router R2 (hostname ISP)

router bgp 300

neighbor 192.168.1.5 remote-as 100

neighbor 172.24.1.18 remote-as 65000

network 10.2.2.0 mask 255.255.255.0

Router R3 (hostname CustRtr)

router bgp 65000

neighbor 172.24.1.17 remote-as 300

network 10.3.3.0 mask 255.255.255.0

Router R2 (hostname ISP)

show ip bgp neighbors

Step 4:- Remove the private AS.

Router R1 (hostname SanJose)

show ip route

b) Ping the 10.3.3.1 address from the SanJose.

ping 10.3.3.1

c) Ping again, this time as an extended ping, sourcing from the Loopback0 interface address.

ping 10.3.3.1 source 10.1.1.1

d) Check the BGP table from SanJose by using the **show ip bgp** command. Note the AS path for the 10.3.3.0 network. The AS 65000 should be listed in the path to 10.3.3.0.

show ip bgp

Router R2 (hostname ISP)

router bgp 300

neighbor 192.168.1.5 remove-private-as

Router R2 (hostname ISP)

clear ip bgp *

Router R1 (hostname SanJose)

show ip route

Router R1 (hostname SanJose)

ping 10.3.3.1 source 10.1.1.1

Router R1 (hostname SanJose)

show ip bgp

Step 5:- Use the AS_PATH attribute to filter routes.

Router R2 (hostname ISP)

ip as-path access-list 1 deny ^100$

ip as-path access-list 1 permit .*

Router R2 (hostname ISP)

router bgp 300

neighbor 172.24.1.18 filter-list 1 out

Router R2 (hostname ISP)

clear ip bgp *

show ip route

Router R3 (hostname CustRtr)

show ip route

Router R2 (hostname ISP)

show ip bgp regexp ^100$

Router R2 (hostname ISP)

ISP# tclsh

ISP(tcl)# foreach address {

+> 10.1.1.1

+> 10.2.2.1

+> 10.3.3.1

+> 192.168.1.5

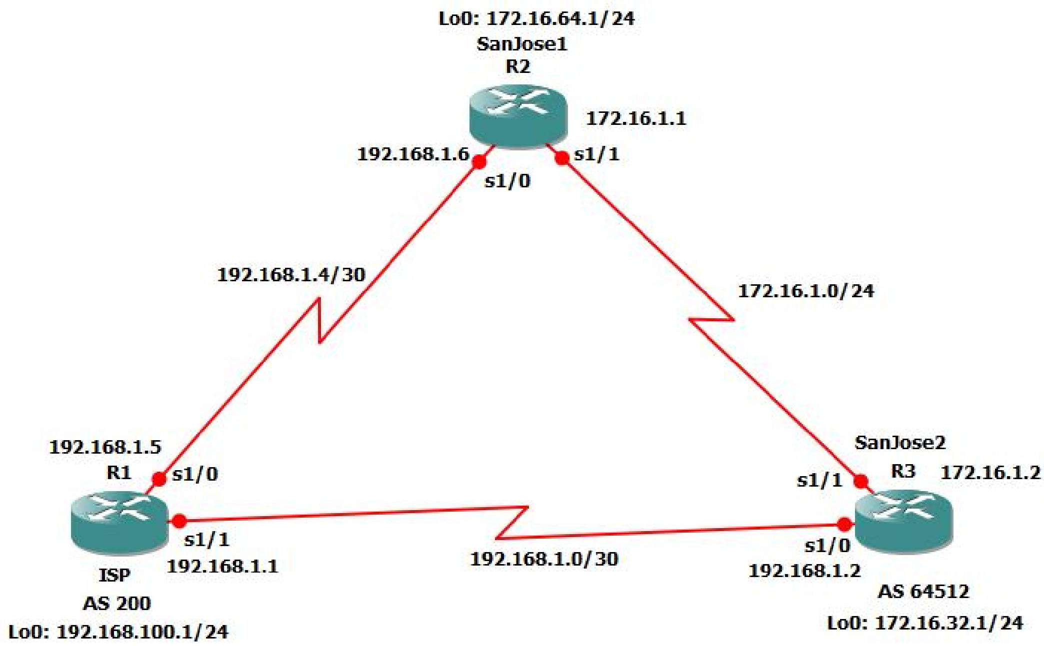
+> 192.168.1.6

+> 172.24.1.17

+> 172.24.1.18 } { ping $address }

Prac 3

Aim:- Configuring IBGP and EBGP Sessions, Local Preference, and MED



Code:-

Step 1: Configure interface addresses.

Router R1 Console (hostname ISP)

hostname ISP

interface Loopback0

ip address 192.168.100.1 255.255.255.0

exit

interface s1/0

ip address 192.168.1.5 255.255.255.252

clock rate 128000

no shutdown

exit

interface s1/1

ip address 192.168.1.1 255.255.255.252

no shutdown

exit

Router R2 Console (hostname SanJose1)

hostname SanJose1

interface Loopback0

ip address 172.16.64.1 255.255.255.0

exit

interface s1/0

ip address 192.168.1.6 255.255.255.252

no shutdown

exit

interface s1/1

ip address 172.16.1.1 255.255.255.0

clock rate 128000

no shutdown

exit

Router R3 Console (hostname SanJose2)

hostname SanJose2

interface Loopback0

ip address 172.16.32.1 255.255.255.0

exit

interface s1/0

ip address 192.168.1.2 255.255.255.252

clock rate 128000

no shutdown

exit

interface s1/1

ip address 172.16.1.2 255.255.255.0

no shutdown

exit

Step 2: Configure EIGRP.

Router R2 Console (hostname SanJose1)

router eigrp 1

network 172.16.0.0

Router R3 Console (hostname SanJose2)

router eigrp 1

network 172.16.0.0

Step 3: Configure IBGP and verify BGP neighbors.

a) Configure IBGP between the SanJose1 and SanJose2 routers.

Router R2 Console (hostname SanJose1)

router bgp 64512

neighbor 172.16.32.1 remote-as 64512

neighbor 172.16.32.1 update-source Loopback0

Router R3 Console (hostname SanJose2)

router bgp 64512

neighbor 172.16.64.1 remote-as 64512

neighbor 172.16.64.1 update-source Loopback0

show ip bgp neighbors

Step 4: Configure EBGP and verify BGP neighbors.

a) Configure ISP to run EBGP with SanJose1 and SanJose2. Enter the following commands on ISP.

Router R1 Console (hostname ISP)

router bgp 200

neighbor 192.168.1.6 remote-as 64512

neighbor 192.168.1.2 remote-as 64512

network 192.168.100.0

b) Configure a discard static route for the 172.16.0.0/16 network

Router R2 Console (hostname SanJose1)

ip route 172.16.0.0 255.255.0.0 null0

c) Configure SanJose1 as an EBGP peer to ISP.

Router R2 Console (hostname SanJose1)

router bgp 64512

neighbor 192.168.1.5 remote-as 200

network 172.16.0.0

d) Use the show ip bgp neighbors command to verify that SanJose1 and ISP have reached the established state. Troubleshoot if necessary.

Router R2 Console (hostname SanJose1)

show ip bgp neighbors

Router R3 Console (hostname SanJose2)

ip route 172.16.0.0 255.255.0.0 null0

router bgp 64512

neighbor 192.168.1.1 remote-as 200

network 172.16.0.0

Step 5: View BGP summary output.

Router R2 Console (hostname SanJose2)

show ip bgp summary

Step 6: Verify which path the traffic takes.

Router R1 Console (hostname ISP)

clear ip bgp *

ping 172.16.64.1

ping 172.16.1.1

ping 172.16.32.1

ping 172.16.1.2

show ip bgp

ping 172.16.1.1 source 192.168.100.1

ping 172.16.32.1 source 192.168.100.1

ping 172.16.1.2 source 192.168.100.1

ping 172.16.64.1 source 192.168.100.1

ping

Step 7: Configure the BGP next-hop-self feature.

Router R1 Console (hostname ISP)

a) Issue the following commands on the ISP router.

router bgp 200

network 192.168.1.0 mask 255.255.255.252

network 192.168.1.4 mask 255.255.255.252

end

b) Issue the show ip bgp command to verify that the ISP is correctly injecting its own WAN links into BGP.

show ip bgp

c) Verify on SanJose1 and SanJose2 that the opposite WAN link is included in the routing table. The output from SanJose2 is as follows.

Router R3 Console (hostname SanJose2)

show ip route

d) To better understand the next-hop-self command

Router R1 Console (hostname ISP)

router bgp 200

no network 192.168.1.0 mask 255.255.255.252

no network 192.168.1.4 mask 255.255.255.252

exit

interface s1/1

shutdown

e) Display SanJose2's BGP table using the show ip bgp command and the IPv4 routing table with show ip route.

Router R3 Console (hostname SanJose2)

show ip bgp

show ip route

f) Issue the next-hop-self command on SanJose1 and SanJose2 to advertise themselves as the next hop to their IBGP peer.

Router R2 Console (hostname SanJose1)

router bgp 64512

neighbor 172.16.32.1 next-hop-self

Router R3 Console (hostname SanJose2)

router bgp 64512

neighbor 172.16.64.1 next-hop-self

g) Reset BGP operation on either router with the clear ip bgp * command.

Router R2 Console (hostname SanJose1)

clear ip bgp *

Router R3 Console (hostname SanJose2)

clear ip bgp *

h) After the routers have returned to established BGP speakers, issue the show ip bgp command on SanJose2 and notice that the next hop is now SanJose1 instead of ISP.

Router R3 Console (hostname SanJose2)

show ip bgp

i) The show ip route command on SanJose2 now displays the 192.168.100.0/24 network because SanJose1 is the next hop, 172.16.64.1, which is reachable from SanJose2.

Router R3 Console (hostname SanJose2)

show ip route

Router R1 Console (hostname ISP)

interface s1/1

no shutdown

Router R3 Console (hostname SanJose2)

show ip route

Step 8: Set BGP local preference.

Router R2 Console (hostname SanJose1)

route-map PRIMARY_T1_IN permit 10

set local-preference 150

exit

router bgp 64512

neighbor 192.168.1.5 route-map PRIMARY_T1_IN in

Router R3 Console (hostname SanJose2)

route-map SECONDARY_T1_IN permit 10

set local-preference 125

exit

router bgp 64512

neighbor 192.168.1.1 route-map SECONDARY_T1_IN in

Router R2 Console (hostname SanJose1)

clear ip bgp * soft

show ip bgp

Router R3 Console (hostname SanJose2)

clear ip bgp * soft

show ip bgp

Step 9: Set BGP MED.

Router R1 Console (hostname ISP)

show ip bgp

show ip route

Router R3 Console (hostname SanJose2)

ping

c) Create a new policy to force the ISP router to return all traffic via SanJose1. Create a second route map utilizing the MED (metric) that is shared between EBGP neighbors.

Router R2 Console (hostname SanJose1)

route-map PRIMARY_T1_MED_OUT permit 10

set Metric 50

exit

router bgp 64512

neighbor 192.168.1.5 route-map PRIMARY_TI_MED_OUT out

Router R3 Console (hostname SanJose2)

route-map SECONDARY_T1_MED_OUT permit 10

set Metric 75

exit

router bgp 64512

neighbor 192.168.1.1 route-map SECONDARY_T1_MED_OUT out

d) Use the clear ip bgp * soft command after issuing this new policy. Issuing the show ip bgp command as follows on SanJose1 or SanJose2 does not indicate anything about this newly defined policy.

Router R2 Console (hostname SanJose1)

clear ip bgp * soft

show ip bgp

Router R3 Console (hostname SanJose2)

clear ip bgp * soft

show ip bgp

Router R3 Console (hostname SanJose2)

ping

Step 10: Establish a default route.

Router R1 Console (hostname ISP)

show ip bgp

router bgp 200

neighbor 192.168.1.6 default-originate

neighbor 192.168.1.2 default-originate

exit

interface loopback 10

ip address 10.0.0.1 255.255.255.0

Router R2 Console (hostname SanJose1)

show ip route

Router R3 Console (hostname SanJose2)

show ip route

Router R3 Console (hostname SanJose2)

show ip bgp

Router R3 Console (hostname SanJose2)

traceroute 10.0.0.1

e) Next, test how BGP adapts to using a different default route when the path between SanJose1 and ISP goes down.

Router R1 Console (hostname ISP)

interface s1/0

shutdown

f) Verify that both routers are modified their routing tables with the default route using the path between SanJose2 and ISP.

Router R2 Console (hostname SanJose1)

show ip route

Router R3 Console (hostname SanJose2)

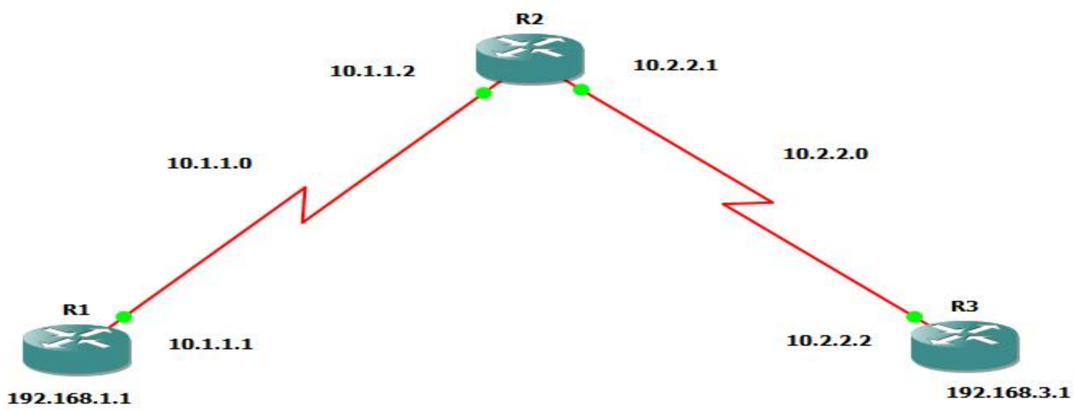
show ip route

Router R2 Console (hostname SanJose1)

traceroute 10.0.0.1

Prac 4

Aim:- Secure the Management Plane



Step 1:- Configure loopbacks and assign addresses.

Router R1 Console

hostname R1

interface Loopback0

description R1 LAN

ip address 192.168.1.1 255.255.255.0

exit

interface S1/0

description R1 → R2

ip address 10.1.1.1 255.255.255.252

clock rate 128000

no shutdown

end

Router R2 Console

hostname R2

interface S1/0

description R2 → R1

interface S1/0

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

interface S1/1

description R2 → R3

ip address 10.2.2.1 255.255.255.252

clock rate 128000

no shutdown

end

Router R3 Console

hostname R3

interface Loopback0

description R3 LAN

ip address 192.168.3.1 255.255.255.0

exit

interface S1/1

description R3 → R2

ip address 10.3.3.1 255.255.255.252

no shutdown

end

Step 2:- Configure Static Routes.

a) On R1, configure a default static route to R2.

Router R1 Console

ip route 0.0.0.0 0.0.0.0 10.1.1.2

b) On R3, configure a default static route to R2.

Router R3 Console

ip route 0.0.0.0 0.0.0.0 10.2.2.1

c) On R2, configure two static routes

Router R2 Console

ip route 192.168.1.0 255.255.255.0 10.1.1.1

ip route 192.168.3.0 255.255.255.0 10.2.2.2

d) From the R1 router, run the following Tcl script to verify connectivity.

R1# tclsh

R1(tcl)# foreach address {

+> (tcl)# 192.168.1.1

+> (tcl)# 10.1.1.1

+> (tcl)# 10.1.1.2

+> (tcl)# 10.2.2.1

+> (tcl)# 10.2.2.2

+> (tcl)# 192.168.3.1

+> (tcl)# } { ping $address }

Step 3:- Secure management access.

Router R1 Console

security passwords min-length 10

Router R1 Console

enable secret class12345

Router R1 Console

line console 0

password ciscoconpass

exec-timeout 5 0

login

logging synchronous

exit

d) Configure the password on the vty lines for router R1

Router R1 Console

line vty 0 4

password ciscovtypass

exec-timeout 5 0

login

logging synchronous

exit

Router R1 Console

line aux 0

no exec

end

f) Enter privileged EXEC mode and issue the **show run** command. Can you read the enable secret password?

Router R1 Console

show run

g) Use the **service password-encryption** command to encrypt the line console and vty passwords.

Router R1 Console

service password-encryption

h) Issue the **show run** command. Can you read the console, aux, and vty passwords?

Router R1 Console

show run

Router R1 Console

banner motd $Unauthorized access strictly prohibited!$

exit

j) Issue the **show run** command. What does the $ convert to in the output?

Step 4:- Configure enhanced username password security.

Router R1 Console

username JR-ADMIN secret class12345

username ADMIN secret class54321

Note:- An older method for creating local database entries is to use the **username name password password** command.

b) Set the console line to use the locally defined login accounts.

Router R1 Console

line console 0

login local

exit

c) Set the vty lines to use the locally defined login accounts.

Router R1 Console

Line vty 0 4

login local

exit

d) Repeat the steps 4a to 4c on R3.

e) To verify the configuration, telnet to R3 from R1 and login using the ADMIN local database account.

Router R1 Console

telnet 10.2.2.2

Step 5:- Enabling AAA RADIUS Authentication with Local User for Backup.

a) Always have local database accounts created before enabling AAA. Since we created two local database accounts in the previous step, then we can proceed and enable AAA on R1.

Router R1 Console

aaa new-model

b) Configure the specifics for the first RADIUS server located at 192.168.1.101. Use **RADIUS-1-pa55w0rd** as the server password.

Router R1 Console

radius-server host 192.168.1.101 key RADIUS-1-pa55w0rd

c) Configure the specifics for the second RADIUS server located at 192.168.1.102. Use **RADIUS-2-pa55w0rd** as the server password.

Router R1 Console

radius-server host 192.168.1.102 key RADIUS-2-pa55w0rd

d) Assign both RADIUS servers to a server group.

Router R1 Console

aaa group server radius RADIUS-GROUP

server 192.168.1.101

server 192.168.1.102

exit

e) Enable the default AAA authentication login to attempt to validate against the server group. If they are not available, then authentication should be validated against the local database.

Router R1 Console

aaa authentication login default group RADIUS-GROUP local

Note:- Once this command is configured, all line access methods default to the default authentication method. The local option enables AAA to refer to the local database. Only the password is case sensitive.

f) Enable the default AAA authentication Telnet login to attempt to validate against the server group. If they are not available, then authentication should be validated against a case sensitive local database.

Router R1 Console

aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case

g) Alter the vty lines to use the TELNET-LOGIN AAA authentication method.

Router R1 Console

line vty 0 4

login authentication TELNET-LOGIN

exit

h) Repeat the steps 5a to 5g on R3.

i) To verify the configuration, telnet to R3 from R1 and login using the ADMIN local database account.

Router R1 Console

telnet 10.2.2.2

Step 6:- Enabling secure remote management using SSH

In this step, you will enable R1 and R3 to support SSH instead of Telnet.

a) SSH requires that a device name and a domain name be configured. Since the router already has a name assigned, configure the domain name.

Router R1 Console

ip domain-name ccnasecurity.com

b) The router uses the RSA key pair for authentication and encryption of transmitted SSH data. Although optional it may be wise to erase any existing key pairs on the router.

Router R1 Console

crypto key zeroize rsa

Note:- If no keys exist, you might receive this message: % No Signature RSA Keys found in configuration.

c) Generate the RSA encryption key pair for the router. Configure the RSA keys with 1024 for the number of modulus bits. The default is 512, and the range is from 360 to 2048.

Router R1 Console

crypto key generate rsa general-keys modulus 1024

d) Cisco routers support two versions of SSH:

• SSH version 1 (SSHv1): Original version but has known vulnerabilities.

• SSH version 2 (SSHv2): Provides better security using the Diffie-Hellman key exchange and the strong integrity-checking message authentication code (MAC).

Configure SSH version 2 on R1.

Router R1 Console

ip ssh version 2

e) Configure the vty lines to use only SSH connections.

Router R1 Console

line vty 0 4

transport input ssh

end

f) Verify the SSH configuration using the **show ip ssh** command.

Router R1 Console

show ip ssh

g) Repeat the steps from 6a to 6f on R3

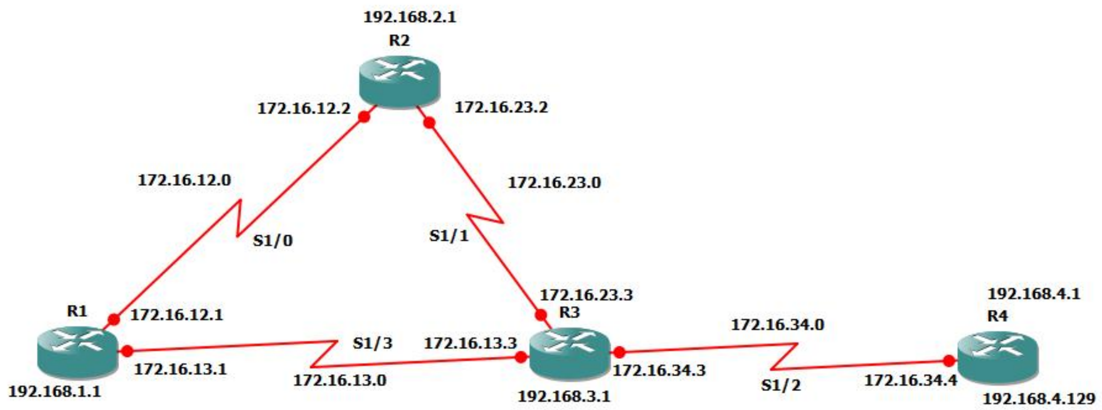
h) Although a user can SSH from a host using the SSH option of TeraTerm of PuTTY, a router can also SSH to another SSH enabled device. SSH to R3 from R1.

Router R1 Console

ssh –l ADMIN 10.2.2.2

Prac 5

Aim:- Configure and Verify Path Control Using PBR



Step 1:- Configure loopbacks and assign addresses.

Router R1 Console

interface Lo1

description R1 LAN

ip address 192.168.1.1 255.255.255.0

exit

interface S1/0

description R1 → R2

ip address 172.16.12.1 255.255.255.248

clock rate 128000

bandwidth 128

no shutdown

exit

interface S1/3

description R1 → R3

ip address 172.16.13.1 255.255.255.248

bandwidth 64

no shutdown

exit

Router R2 Console

interface Lo2

description R2 LAN

ip address 192.168.2.1 255.255.255.0

exit

interface S1/0

description R2 → R1

ip address 172.16.12.2 255.255.255.248

bandwidth 128

no shutdown

exit

interface S1/1

description R2 → R3

ip address 172.16.23.2 255.255.255.248

clock rate 128000

bandwidth 128

no shutdown

exit

Router R3 Console

interface Lo3

description R3 LAN

ip address 192.168.3.1 255.255.255.0

exit

interface S1/3

description R3 → R1

ip address 172.16.13.3 255.255.255.248

clock rate 64000

bandwidth 64

no shutdown

exit

interface S1/1

description R3 → R2

ip address 172.16.23.3 255.255.255.248

bandwidth 128

no shutdown

exit

interface S1/2

description R3 → R4

ip address 172.16.34.3 255.255.255.248

clock rate 64000

bandwidth 64

no shutdown

exit

Router R4 Console

interface Lo4

description R4 LAN A

ip address 192.168.4.1 255.255.255.128

exit

interface Lo5

description R4 LAN B

ip address 192.168.4.129 255.255.255.128

exit

interface S1/2

description R4 → R3

ip address 172.16.34.4 255.255.255.248

bandwidth 64

no shutdown

exit

c) Verify the configuration with the **show ip interface brief**, **show interfaces description** commands. The output from router R3 is shown below.

Router R3 Console

show ip interface brief | include up

show interfaces description | include up

Step 3:- Configure basic EIGRP

a) Implement EIGRP AS 1 over the serial and loopback interfaces as you have configured it for the other EIGRP labs.

Router R1 Console

router eigrp 1

network 192.168.1.0

network 172.16.12.0 0.0.0.7

network 172.16.13.0 0.0.0.7

no auto-summary

Router R2 Console

router eigrp 1

network 192.168.2.0

network 172.16.12.0 0.0.0.7

network 172.16.23.0 0.0.0.7

no auto-summary

Router R3 Console

router eigrp 1

network 192.168.3.0

network 172.16.13.0 0.0.0.7

network 172.16.23.0 0.0.0.7

network 172.16.34.0 0.0.0.7

no auto-summary

Router R4 Console

router eigrp 1

network 192.168.4.0

network 172.16.34.0 0.0.0.7

no auto-summary

Step 4:- Verify EIGRP connectivity.

a) Verify the configuration by using the **show ip eigrp neighbors** command to check which routers have EIGRP adjacencies.

Router R1 Console

show ip eigrp neighbors

Router R2 Console

show ip eigrp neighbors

Router R3 Console

show ip eigrp neighbors

Router R4 Console

show ip eigrp neighbors

b) Run the following Tcl script on all routers to verify full connectivity.

Router R1 Console

R1# tclsh

foreach address {

172.16.12.1

172.16.12.2

172.16.13.1

172.16.13.3

172.16.23.2

172.16.23.3

172.16.34.3

172.16.34.4

192.168.1.1

192.168.2.1

192.168.3.1

192.168.4.1

192.168.4.129

} { ping $address }

Step 5:- Verify the current path.

Before you configure PBR, verify the routing table on R1.

a) On R1, use the **show ip route** command. Notice the next-hop IP address for all networks discovered by EIGRP.

Router R1 Console

show ip route | begin Gateway

Router R4 Console

traceroute 192.168.1.1 source 192.168.4.1 (R4 LAN A)

traceroute 192.168.1.1 source 192.168.4.129 (R4 LAN B)

Router R3 Console

show ip route | begin Gateway

d) On R3, use the **show interfaces S1/3** and **show interfaces S1/1** commands.

Router R3 Console

show interfaces S1/3

Router R3 Console

show interfaces S1/1

e) Confirm that R3 has a valid route to reach R1 from its serial 0/0/0 interface using the **show ip eigrp topology 192.168.1.0** command.

Router R3 Console

show ip eigrp topology 192.168.1.0

Step 6:- Configure PBR to provide path control.

a) On router R3, create a standard access list called **PBR-ACL** to identify the R4 LAN B network.

Router R3 Console

ip access-list standard PBR-ACL

remark ACL matches R4 LAN B traffic

permit 192.168.4.128 0.0.0.127

exit

b) Create a route map called **R3-to-R1** that matches PBR-ACL and sets the next-hop interface to the R1 S1/1 interface.

Router R3 Console

route-map R3-to-R1 permit

description RM to forward LAN B traffic to R1

match ip address PBR-ACL

set ip next-hop 172.16.13.1

exit

c) Apply the R3-to-R1 route map to the serial interface on R3 that receives the traffic from R4. Use the **ip policy route-map** command on interface S1/2.

Router R3 Console

interface S1/2

ip policy route-map R3-to-R1

end

d) On R3, display the policy and matches using the **show route-map** command.

Router R3 Console

show route-map

Step 7:- Test the policy.

a) On R3, create a standard ACL which identifies all of the R4 LANs.

Router R3 Console

access-list 1 permit 192.168.4.0 0.0.0.255

exit

b) Enable PBR debugging only for traffic that matches the R4 LANs.

Router R3 Console

debug ip policy ?

debug ip policy 1

c) Test the policy from R4 with the traceroute command, using R4 LAN A as the source network.

Router R4 Console

traceroute 192.168.1.1 source 192.168.4.1

d) Test the policy from R4 with the **traceroute** command, using R4 LAN B as the source network.

Router R4 Console

traceroute 192.168.1.1 source 192.168.4.129

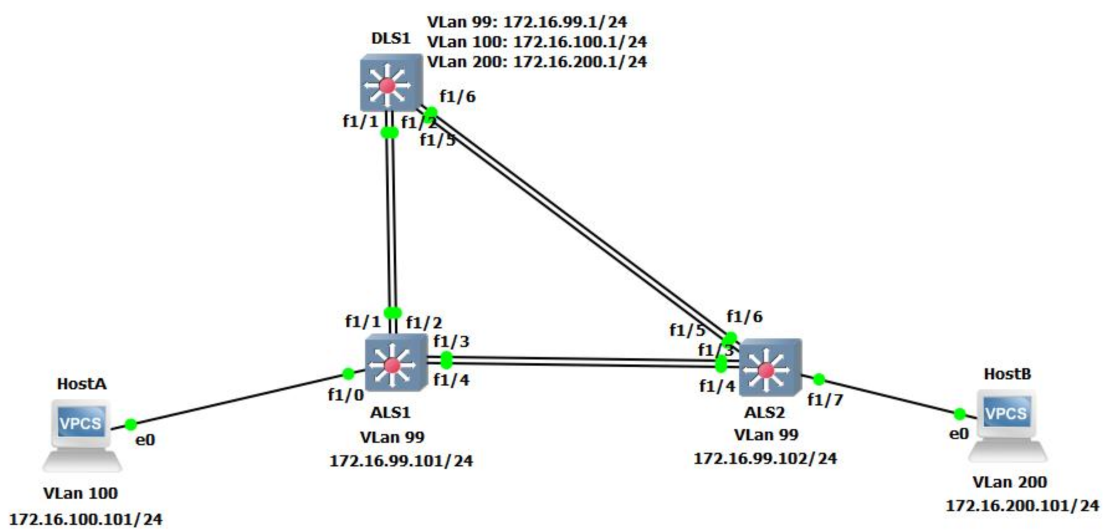
e) On R3, display the policy and matches using the show route-map command.

Router R3 Console

show route-map

Prac 6

Aim:- To Simulate IP Service Level Agreements and Remote SPAN in a Campus Environment



Part 1: Prepare for the Lab

Step 1: Configure basic switch parameters.

Enter basic configuration commands on each switch according to the diagram.

DSL1 Console:

interface vlan 99

ip address 172.16.99.1 255.255.255.0

no shutdown

enable secret password

line vty 0 15

no login

privilege level 15

ALS1 Console:

interface vlan 99

ip address 172.16.99.1 255.255.255.0

no shutdown

exit

enable secret password

line vty 0 15

no login

privilege level 15

ALS2 Console:

interface vlan 99

ip address 172.16.99.1 255.255.255.0

no shutdown

exit

enable secret password

line vty 0 15

no login

privilege level 15

ALS1 Console:

ip default-gateway 172.16.99.1

ALS2 Console:

ip default-gateway 172.16.99.1

Step 2: Configure host PCs.

Configure PCs Host A and Host B with the IP address and subnet mask shown in the topology. Host A is in VLAN 100 with a default gateway of 172.16.100.1. Host B is in VLAN 200 with a default gateway of 172.16.200.1.

hostA Console:

ip 172.16.100.101/24 172.16.100.1

hostB Console:

ip 172.16.200.101/24 172.16.200.1

Step 3: Configure trunks and EtherChannels between switches.

Configure the trunks and EtherChannel from DLS1 to ALS1

DLS1 Console:

interface ran f 1/1 – 2

switchport trunk encapsulation dot1q

switchport mode trunk

channel-group 1 mode on

no shutdown

exit

Configure the trunks and EtherChannel from DLS1 to ALS2

DLS1 Console:

interface ran f 1/5 – 6

switchport trunk encapsulation dot1q

switchport mode trunk

channel-group 2 mode on

no shutdown

exit

Configure the trunks and EtherChannel from ALS1 and DLS1

ALS1 Console:

interface range f 1/3 – 4

switchport mode trunk

channel-group 3 mode on

no shutdown

exit

Configure the trunks and EtherChannel from ALS1 and ALS2

ALS1 Console:

interface range f 1/1 – 2

switchport mode trunk

channel-group 2 mode on

no shutdown

exit

Configure the trunks and EtherChannel from ALS2 and DLS1

ALS2 Console:

interface range f 1/3 – 4

switchport mode trunk

channel-group 3 mode on

no shutdown

exit

Configure the trunks and EtherChannel from ALS2 and ALS1

interface range f 1/5 – 6

switchport mode trunk

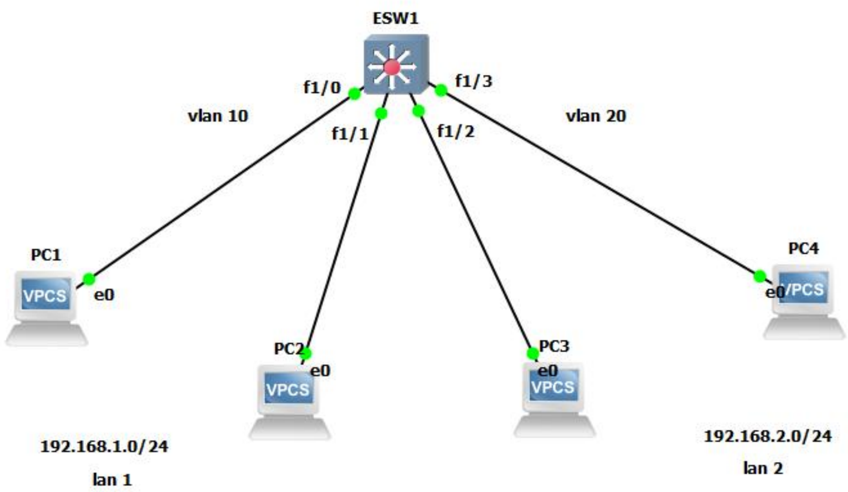
channel-group 2 mode on

no shutdown

exit

Prac 7

Aim:- Inter-VLAN Routing.



pc1> ip 192.168.1.1/24

PC2> ip 192.168.1.2/24

PC3> ip 192.168.2.1

PC4> ip 192.168.2.2/24

ESW1#vlan database

ESW1(vlan)#vlan 10

ESW1(vlan)#vlan 20

ESW1#

conf t

interface f1/0

switchport mode access

switchport access vlan 10

exit

interface f1/1

switchport mode access

switchport access vlan 10

exit

interface f1/2

switchport mode access

switchport access vlan 10

exit

interface f1/3

switchport mode access

switchport access vlan 10

exit

ESW1#show vlan-switch

PC1> ping 192.168.1.2

PC1> ping 192.168.2.1

PC1> show ip

PC1> ip 192.168.1.1/24 192.168.1.254

PC1> show ip

PC2> ip 192.168.1.2/24 192.168.1.254

PC2> show ip

PC3> ip 192.168.2.1/24 192.168.2.254

PC3> show ip

PC4> ip 192.168.2.2/24 192.168.2.254

PC4> show ip

ESW1#

conf t

interface vlan 10

ip address 192.168.1.254 255.255.255.0

no shut

exit

interface vlan 20

ip address 192.168.2.254 255.255.255.0

no shut

exit

ESW1#conf t

ESW1(config)#ip routing

ESW1(config)#end

Show ip route

pc1>ping 192.168.2.1

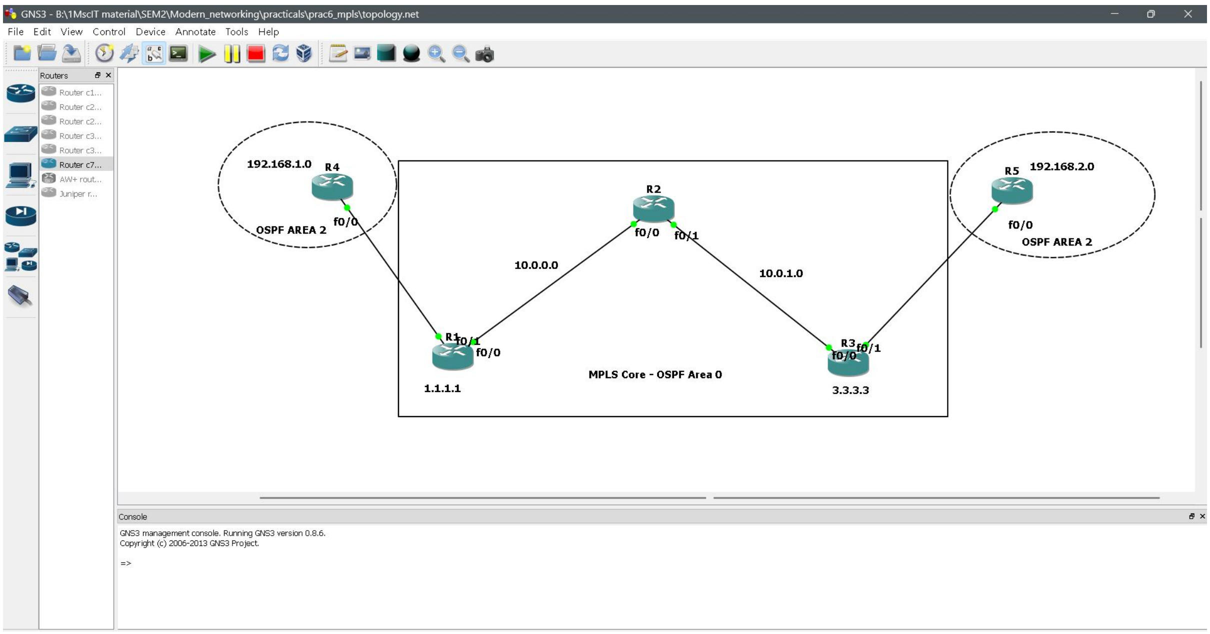
pc1>ping 192.168.2.2

pc4>ping 192.168.1.1

pc4>ping 192.168.1.2

Prac 8

Aim:- Simulating MPLS



Router R1 Console

interface Loopback0

ip address 1.1.1.1 255.255.255.255

ip ospf 1 area 0

exit

interface f0/0

ip address 10.0.0.1 255.255.255.0

no shutdown

ip ospf 1 area

exit

Router R2 Console

interface Loopback0

ip address 2.2.2.2 255.255.255.255

ip ospf 1 area 0

exit

interface f0/0

ip address 10.0.0.2 255.255.255.0

no shutdown

ip ospf 1 area 0

exit

interface f0/1

ip address 10.0.1.2 255.255.255.0

no shutdown

ip ospf 1 area 0

exit

Router R3 Console

interface Loopback0

ip address 3.3.3.3 255.255.255.255

ip ospf 1 area 0

exit

interface f0/0

ip address 10.0.1.3 255.255.255.0

no shutdown

ip ospf 1 area 0

exit

Router R1 Console

ping 3.3.3.3 source Loopback0

router ospf 1

mpls ldp autoconfig

Router R3 Console

router ospf 1

mpls ldp autoconfig

Router R2 Console

router ospf 1

mpls ldp autoconfig

show mpls interface

show mpls ldp neighbor

Router R1 Console

trace 3.3.3.3

Router R1 Console

router bgp 1

neighbor 3.3.3.3 remote-as 1

neighbor 3.3.3.3 update-source Loopback0

no auto-summary

address-family vpnv4

neighbor 3.3.3.3 activate

Router R3 Console

router bgp 1

neighbor 1.1.1.1 remote-as 1

neighbor 1.1.1.1 update-source Loopback0

no auto-summary

address-family vpnv4

neighbor 1.1.1.1 activate

Router R1 Console

show bgp vpnv4 unicast all summary

Router R4 Console

interface Loopback0

ip address 4.4.4.4 255.255.255.255

ip ospf 2 area 2

exit

interface f0/0

ip address 192.168.1.4 255.255.255.0

ip ospf 2 area 2

no shutdown

Router R1 Console

interface f0/1

ip address 192.168.1.1 255.255.255.0

no shutdown

Router R1 Console

ip vrf RED

rd 4:4

route-target both 4:4

interface f0/1

ip vrf forwarding RED

interface f0/1

ip address 192.168.1.1 255.255.255.0

no shutdown

show run interface f0/1

show ip route

show ip route vrf RED

int f0/1

ip ospf 2 area 2

show ip route vrf RED

Router R5 Console

interface Loopback0

ip address 5.5.5.5 255.255.255.255

ip ospf 2 area 2

exit

interface f0/0

ip address 192.168.2.5 255.255.255.0

ip ospf 2 area 2

no shutdown

Router R3 Console

interface f0/1

ip address 192.168.2.3 255.255.255.0

no shutdown

ip vrf RED

rd 4:4

route-target both 4:4

interface f0/1

ip vrf forwarding RED

interface f0/1

ip address 192.168.2.3 255.255.255.0

no shutdown

show run interface f0/1

interface f0/1

ip ospf 2 area 2

show ip route vrf RED

Router R4 Console

show ip route

Router R1 Console

show ip route

show ip route vrf RED

router bgp 1

address-family ipv4 vrf RED

redistribute ospf 2

Router R3 Console

router bgp 1

address-family ipv4 vrf RED

redistribute ospf 2

Router R1 Console

show ip bgp vpnv4 vrf RED

Router R3 Console

show ip bgp vpnv4 vrf RED

Router R1 Console

router ospf 2

redistribute bgp 1 subnets

Router R3 Console

router ospf 2

redistribute bgp 1 subnets

Router R4 Console

show ip route

Router R5 Console

show ip route

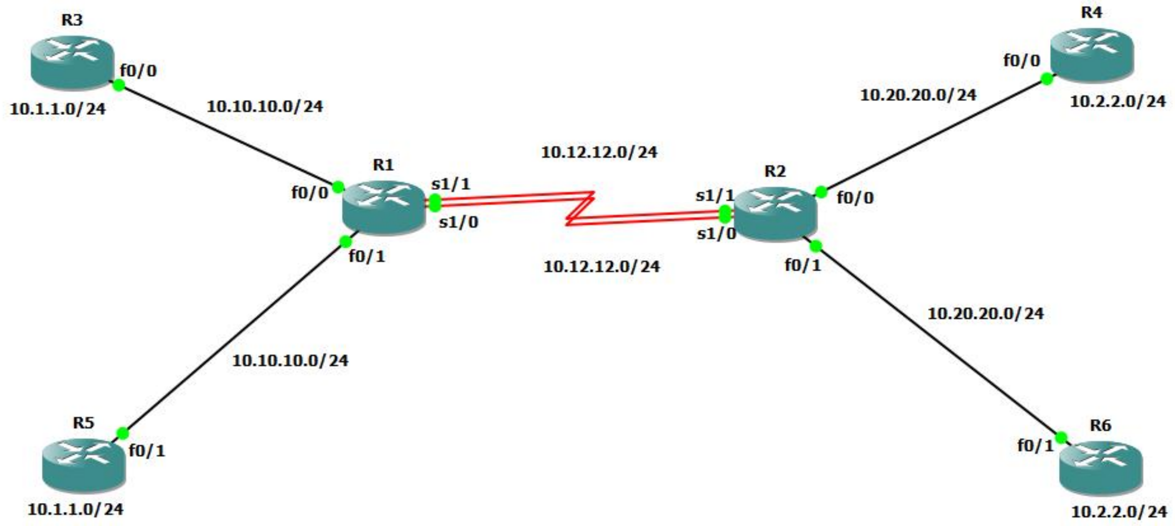
Router R4 Console

ping 5.5.5.5

trace 5.5.5.5

Prac 9

Aim:- Simulating Virtual Routing and Forwarding (VRF)



Step 1:- Prepare the routers for the lab.

Step 1:- Prepare the routers for the lab.

Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations.

Step 2:- Configure Virtual Routing and Forwarding.

Router R1 Console

ip vrf cust-A

exit

ip vrf cust-B

exit

Step 3:- Configure interface addresses.

interface f0/0

ip vrf forwarding cust-A

ip address 10.10.10.1 255.255.255.0

no shutdown

exit

interface S1/1

ip vrf forwarding cust-A

ip address 10.12.12.1 255.255.255.0

no shutdown

exit

interface f0/1

ip vrf forwarding cust-B

ip address 10.10.10.1 255.255.255.0

no shutdown

exit

interface S1/0

ip vrf forwarding cust-B

ip address 10.12.12.1 255.255.255.0

no shutdown

exit

Router R2 Console

ip vrf cust-A

exit

ip vrf cust-B

exit

interface f0/0

ip vrf forwarding cust-A

ip address 10.20.20.2 255.255.255.0

no shutdown

exit

interface S1/1

ip vrf forwarding cust-A

ip address 10.12.12.2 255.255.255.0

no shutdown

exit

interface f0/1

ip vrf forwarding cust-B

ip address 10.20.20.2 255.255.255.0

no shutdown

exit

interface S1/0

ip vrf forwarding cust-B

ip address 10.12.12.2 255.255.255.0

no shutdown

exit

Router R3 Console

interface Loopback0

ip address 10.1.1.3 255.255.255.0

no shutdown

exit

interface f0/0

ip address 10.10.10.3 255.255.255.0

no shutdown

exit

router eigrp 100

no auto

net 10.0.0.0

Router R4 Console

interface Loopback0

ip address 10.2.2.4 255.255.255.0

no shutdown

exit

interface f0/0

ip address 10.20.20.4 255.255.255.0

no shutdown

exit

router eigrp 100

no auto

net 10.0.0.0

Router R5 Console

interface Loopback0

ip address 10.1.1.5 255.255.255.0

no shutdown

exit

interface f0/1

ip address 10.10.10.5 255.255.255.0

no shutdown

exit

router eigrp 100

no auto

net 10.0.0.0

Router R6 Console

interface Loopback0

ip address 10.2.2.6 255.255.255.0

no shutdown

exit

interface f0/1

ip address 10.20.20.6 255.255.255.0

no shutdown

exit

router eigrp 100

no auto

net 10.0.0.0

Router R1 Console

router eigrp 1

address-family ipv4 vrf cust-A

autonomous-system 100

no auto

network 10.0.0.0

exit

address-family ipv4 vrf cust-B

autonomous-system 100

no auto

network 10.0.0.0

exit

Router R1 Console

show ip route

Note:- Since we have configured virtual routing and forwarding it will not display the connections.

To check the routes we have to write the following command.

show ip route vrf cust-A

Note:- Now it will display all the connections.

ping vrf cust-A 10.1.1.3

Router R2 Console

router eigrp 1

address-family ipv4 vrf cust-A

autonomous-system 100

no auto

network 10.0.0.0

exit

address-family ipv4 vrf cust-B

autonomous-system 100

no auto

network 10.0.0.0

exit

Router R3 Console

Since we have not configured virtual routing and forwarding on R3,R4,R5 and R6, to ping we simply have to write the following command.

ping 10.2.2.4