MODERN NETWORKING

**MASTERS OF SCIENCE (INFORMATION TECHNOLOGY)**

# By

**SHASTRI VIKRAM NAGNATH**

# Seat No.

**Under the esteemed guidance of**

**MRS. PROF. DORRIES GONSALVES**

****

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**VIDYAVARDHINI’S**

**ANNA SAHEB VARTAK COLLEGE OF ARTS,KEDARNATH MALHOTRA COLLEGEOF COMMERCE,&E.S.ANDRADES COLLEGE OF SCIENCE**

**(*Affiliated to University of Mumbai*) VASAI ROAD,DIST.PALGHAR- 401202**

**MAHARASHTRA**

**2024-2025**

****

**Vidyavardhini’s**

**AnnaSaheb Vartak College of Arts, Kedarnath Malhotra College of Commerce,& E.S.Andrades College of Science**

Vasai Road, Dist. Palghar -401202

**CERTIFICATE**

This is to certify that Mr./Miss. **Vikram Nagnath Shastri** Exam Seat No. has satisfactorily completed practical’s of the subject **“Modern Networking”** as part of the practical fulfillment of MSc.IT Sem I as prescribed by the university of Mumbai for the year 2024-2025.

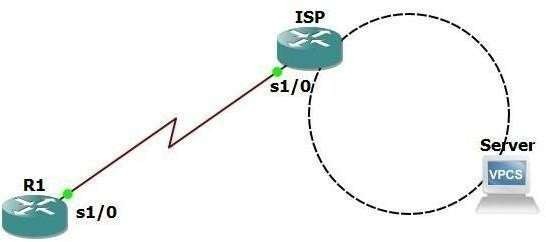
Subject Teacher External Examiner H.O.D

**INDEX**

|  |  |  |
| --- | --- | --- |
| **Practical No** | **Details** | **Page No.** |
| **1** | **Configure IP SLA (On GNS3)** | **1** |
| **2** | **Using the AS\_PATH Attribute (On GNS3)** | **5** |
| **3** | **Configuring IBGP and EBGP sessions, Local Preference and MED** | **15** |
| **4** | **Configuring Secure Management Plane (On GNS3)** | **35** |
| **5** | **configuring PBR (on GNS3)** | **46** |
| **6** | **Configuring remote SPAN (On Cisco Packet Tracer)** | **53** |
| **7** | **Configuring Inter-VLAN Routing(On Packet Tracer)** | **57** |
| **8(A)** | **Configuring MPLS (On GNS3)** | **68** |
| **8(B)** | **Implement VRF** | **73** |

**Practical No: 1**

**Aim: Configure IP SLA (On GNS3).**

****

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP address** | **Network Mask** |
| R1 | s1/0 | 209.165.200.9 | 255.255.255.252 |
| ISP | s1/0 | 209.165.200.10 | 255.255.255.252 |
| Lo 0 | 198.133.209.1 | 255.255.255.255 |

**Configure R1** R1#conf t R1(config)#int s1/0

R1(config-if)#ip add 209.165.200.9 255.255.255.252

R1(config-if)#no shut R1(config-if)#ip route

R1(config-if)#ip route 0.0.0.0 0.0.0.0 209.165.200.10 R1(config)#exit

**Configure ISP**

R2#conf t R2(config)#hostname ISP ISP(config)#int s1/0

ISP(config-if)#ip add 209.165.200.10 255.255.255.252

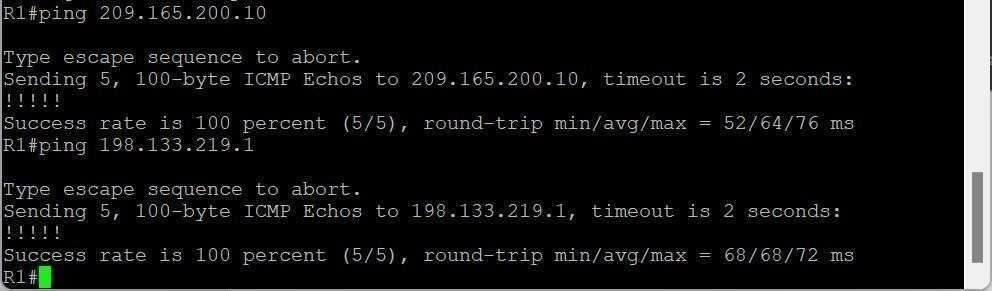
ISP(config-if)#clock rate 4032000 ISP(config-if)#exit ISP(config)#no ip domain-lookup ISP(config)#int loopback 0

ISP(config-if)#ip add 198.133.219.1 255.255.255.255

ISP(config-if)#no shut ISP(config-if)#exit ISP(config)#int s1/0 ISP(config-if)#no shut ISP(config-if)#exit

**Check connectivity on ISP server**

**Check connectivity on R1 to ISP and server**



**Configure IP SLA on R1**

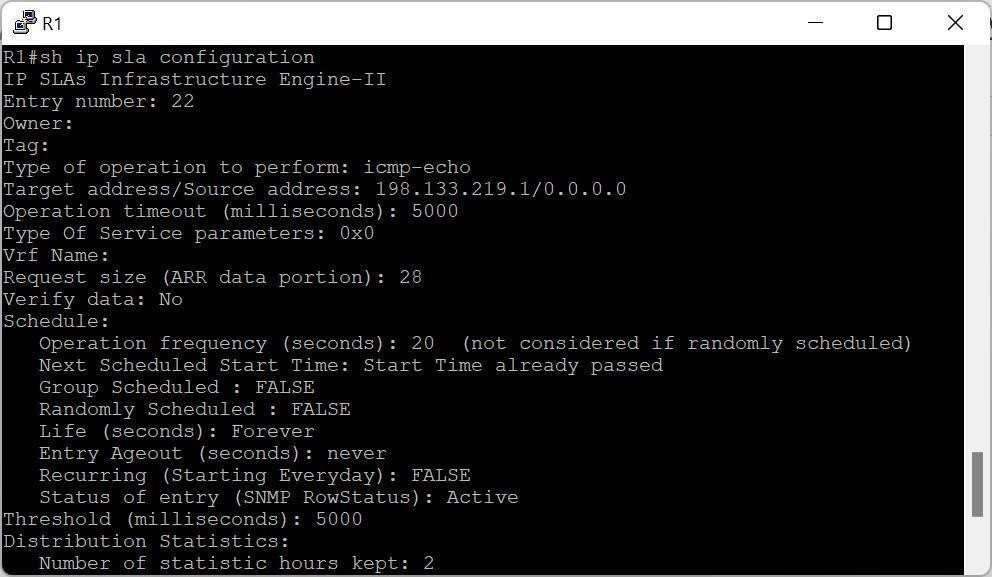
R1#conf t

R1(config)#ip sla 22

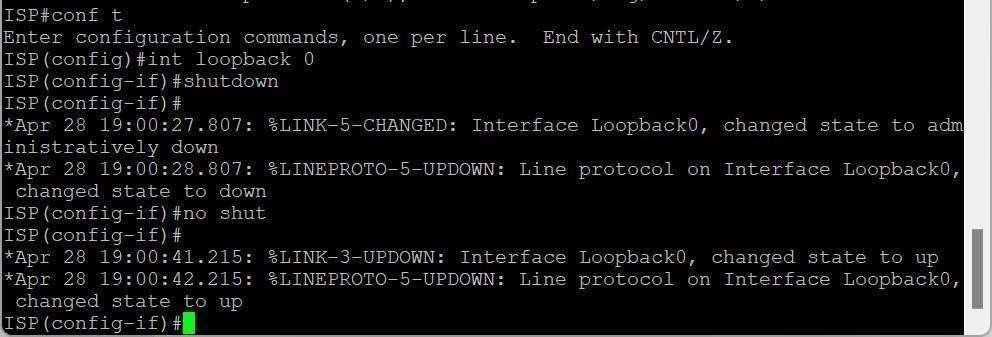
R1(config-ip-sla)#icmp-echo 198.133.219.1

R1(config-ip-sla-echo)#frequency 20

R1(config-ip-sla-echo)#ip sla schedule 22 start-time now life forever R1(config)#end

**Check IP SLA configuration**

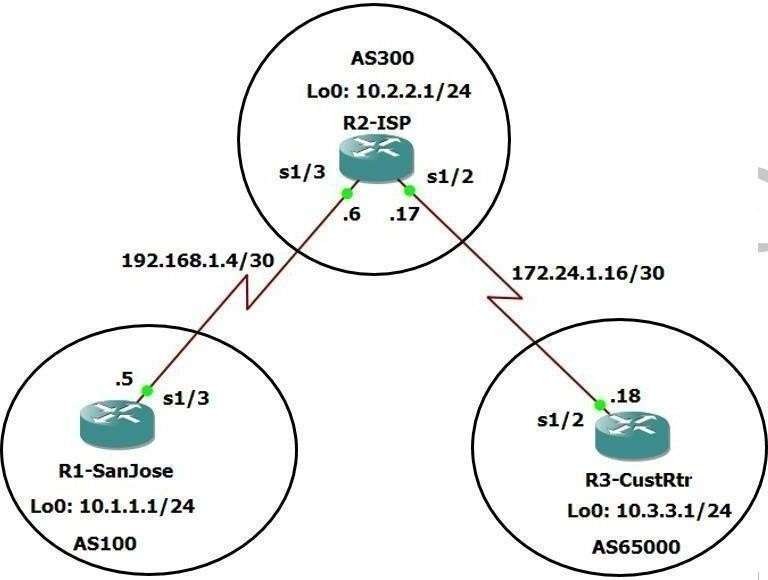
**Refresh ISP**



**Check IP SLA statistics**

**Practical No: 2**

**Aim: Using the AS\_PATH Attribute (On GNS3).**

****

**Step 1: Configure hostname and interfaces on all routers. Router 1-SanJose**

R1#en

R1#conf t

R1(config)#hostname R1-SanJose R1-SanJose(config)#int lo 0

R1-SanJose(config-if)#ip add 10.1.1.1 255.255.255.0 R1-SanJose(config-if)#no shut

R1-SanJose(config-if)#int se1/3

R1-SanJose(config-if)#ip add 192.168.1.5 255.255.255.252 R1-SanJose(config-if)#no shut

R1-SanJose(config-if)#exit R1-SanJose(config)#exit R1-SanJose#

**Router 2-ISP** R2#en R2#conf t

R2-ISP(config)#int lo 0

R2-ISP(config-if)#ip add 10.2.2.1 255.255.255.0

R2-ISP(config-if)#no shut R2-ISP(config-if)#int se1/3

R2-ISP(config-if)#ip add 192.168.1.6 255.255.255.252

R2-ISP(config-if)#no shut R2-ISP(config-if)#int se1/2

R2-ISP(config-if)#ip add 172.24.1.17 255.255.255.252

R2-ISP(config-if)#no shut R2-ISP(config-if)#exit R2-ISP(config)#exit

**Router 3-CustRtr**

R3#en R3#conf t

R3(config)#hostname R3-CustRtr R3-CustRtr(config)#int lo 0

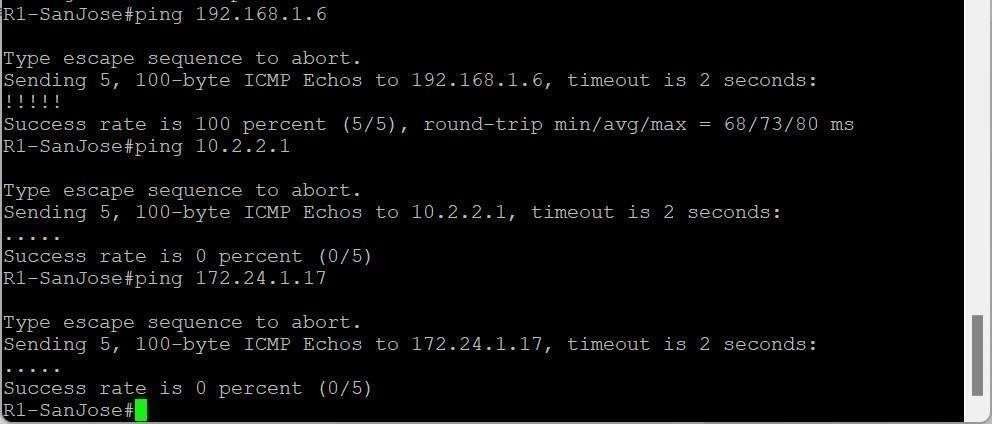
R3-CustRtr(config-if)#ip add 10.3.3.1 255.255.255.0 R3-CustRtr(config-if)#no shut

R3-CustRtr(config-if)#int se1/2

R3-CustRtr(config-if)#ip add 172.24.1.18 255.255.255.252 R3-CustRtr(config-if)#no shut

R3-CustRtr(config-if)#exit R3-CustRtr(config)#exit **Step 2: Check Connectivity**

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

SanJose will not be able to reach either Iso’s loopback (10.2.2.1) or CustRtr’s loopback (10.3.3.1), nor will it be reach either end of the link joining ISP to CustRtr (172.24.1.17) and (172.24.1.18).

**Step 3: Configure BGP**

R1-SanJose#conf t

R1-SanJose(config)#router bgp 100

R1-SanJose(config-router)#neighbor 192.168.1.6 remote-as 300

R1-SanJose(config-router)#network 10.1.1.0 mask 255.255.25.0 R1-SanJose(config-router)#^Z

R1-SanJose#

R2-ISP#conf t

Enter configuration commands, one per line. End with CNTL/Z. R2-ISP(config)#router bgp 300

R2-ISP(config-router)#neighbor 192.168.1.5 remote-as 100

R2-ISP(config-router)#%BGP-5-ADJCHANGE: neighbor 192.168.1.5 Up R2-ISP(config-router)#neighbor 172.24.1.18 remote-as 65000

R2-ISP(config-router)#network 10.2.2.0 mask 255.255.255.0 R2-ISP(config-router)#^Z

R2-ISP#

R3-CustRtr#conf t

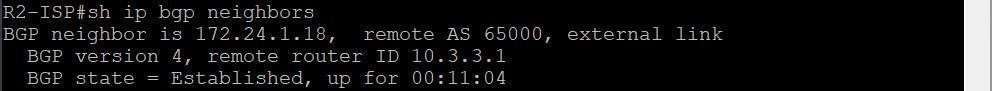
R3-CustRtr(config)#router bgp 65000

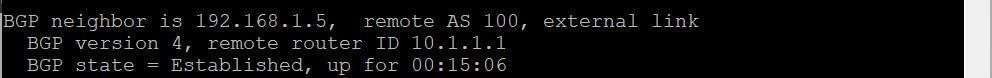
R3-CustRtr(config-router)#neighbor 172.24.1.17 remote-as 300

R3-CustRtr(config-router)#%BGP-5-ADJCHANGE: neighbor 172.24.1.17 Up R3-CustRtr(config-router)#network 10.3.3.0 mask 255.255.255.0

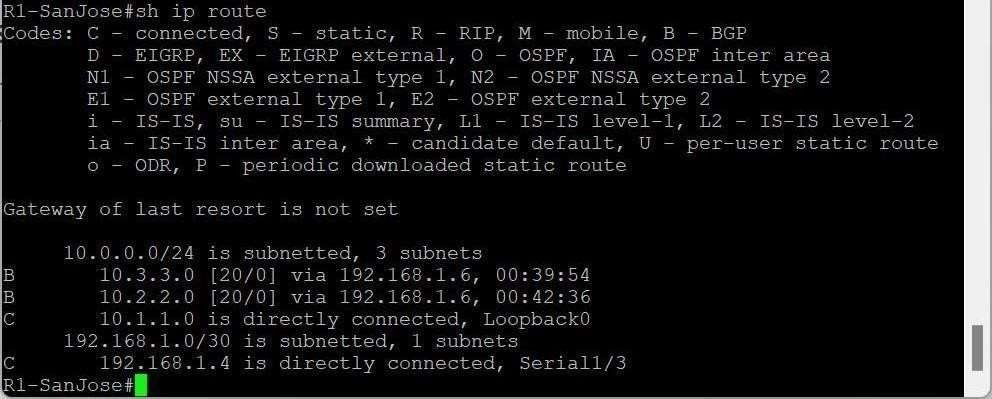
R3-CustRtr(config-router)#^Z R3-CustRtr#

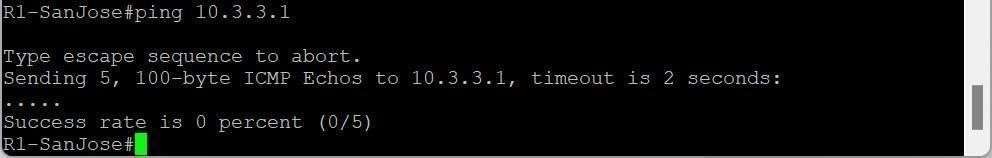
**Step 4: Verify that these routers have establish the appropriate neighbor relationships by issuing the show ip bgp neighbors command on each router.**



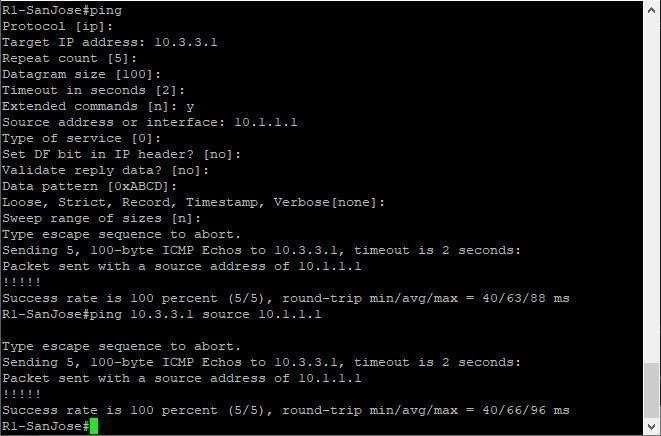
****

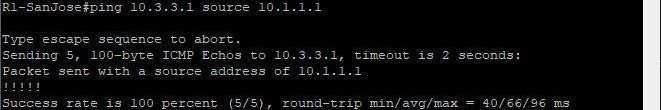
**Step 5: remove the private AS**

1. Display the SanJose routing table using the **show ip route** command. SanJose should have a route to both 10.2.2.0 and 10.3.3.0
2. Ping the 10.3.3.1 address from SanJose.

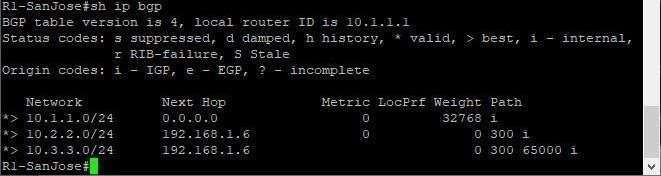


1. Ping again.



**OR**

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



1. Configure ISP to strip the private numbers from BGP routes exchanged with SanJose using the following commands.

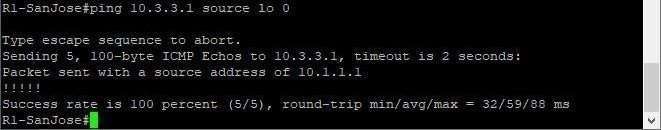
R2-ISP#conf t

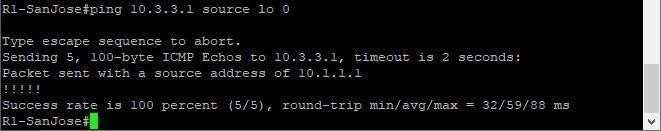
R2-ISP(config)#router bgp 300

R2-ISP(config-router)#neighbor 192.168.1.5 remove-private-as R2-ISP(config- router)#^Z



1. SanJose should be able to ping 10.3.3.1 using its loopback 0 interface as the source ofthe ping.



1. Now check the BGP table on SanJose. The AS\_PATH to the 10.3.3.0 network should bs AS 300. It no longer has the private As in the path.

**Step 6: Use AS\_PATH attribute to filter routes.**

* 1. Configure a special kind of access list to match BGP with an AS\_PATH attribute that both begins and ends with the number 100. Enter the following commands on ISP.

R2-ISP#conf t

R2-ISP(config)#ip as-path access-list 1 deny ^100$

R2-ISP(config)#ip as-path access-list 1 permit .\* R2- ISP(config)#

The first command uses the ^ character to indicate the the AS path must begin with the given number 100. The $ character indicates that the AS\_PATH attribute must also end with 100.

Essentially, this statement matches only paths that are sources from AS 100. Other paths, which might include AS 100 along the way, will not match this list.

In the second statement, the . (period) is a wildcard, and the \* (asterisk) stand for a repetition Of the wildcard. Together, .\* matches any value of the AS\_PATH attribute, which in effect permits any update that has not been denied by the previous **access-list** statement.

* 1. Apply the cpnfigured access list using the **neighbor** command with the **filterlist**

option.

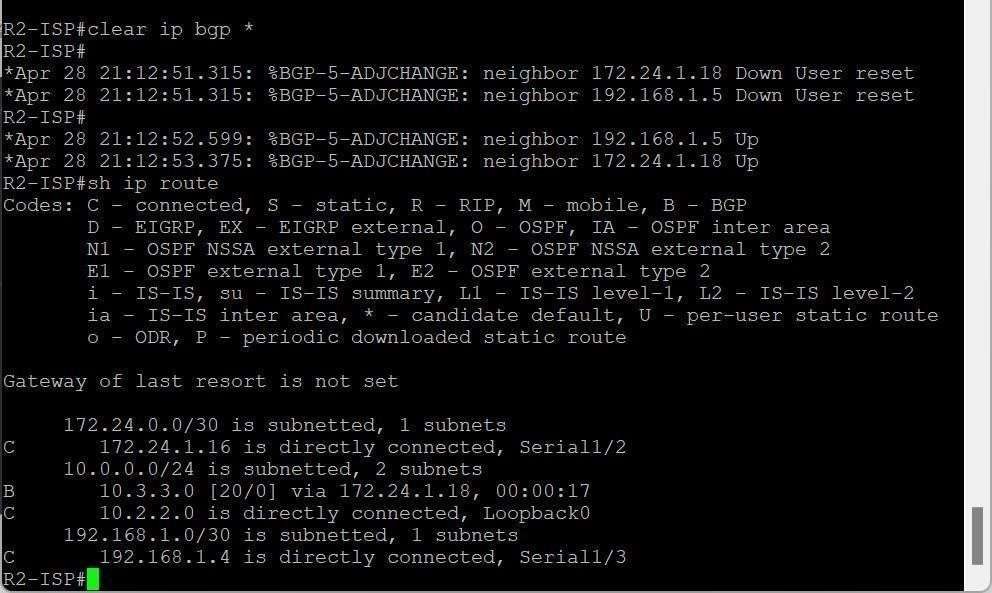
R2-ISP#conf t

R2-ISP(config)#router bgp 300

R2-ISP(config-router)#neighbor 172.24.1.18 filter-list 1 out R2-ISP(config-router)#^Z R2-ISP#

The out keyword specifies that the list is applied to routing information sent to this neighbor.

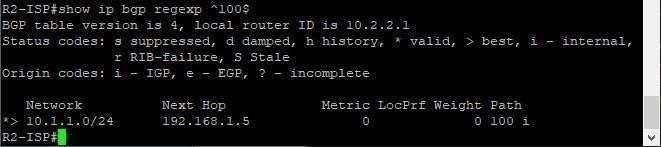
C. Use the **clear ip bgp \*** command to reset the routing information. Wait several seconds and then check the routing table for ISP. The route to 10.1.1.0 should be in the routing table.



* 1. Check the routing table for CustRtr . It should not have a route to 10.1.1.0 in its routing table.



e. Return to ISP and verify that the filter is working as intended. Issue **the show ip bgp regexp ^100$** command.

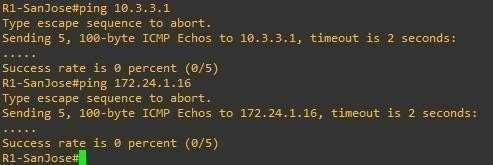


The output of this command shows all matches for the regular expression that were used in the access list. The path to 10.1.1.0 matches the access list and is filtered from updates to CustRtr.

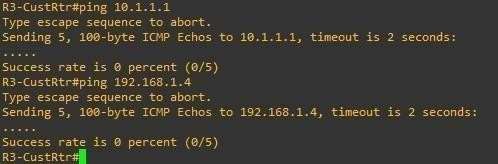
Now all pings from ISP should be successful.



SanJose should not be able to ping the CustRtr loopback 10.3.3.1 or the WAN link 172.24.1.16/30.

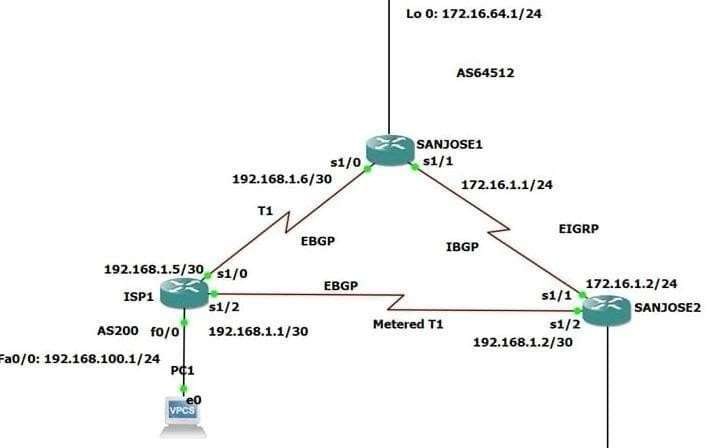


CustRtr should not be able to ping the Sanjose loopback 10.1.1.1 or the WAN link 192.168.1.4/30.



**Practical No : 3**

**Aim: Configuring IBGP and EBGP Sessions, Local Preference and MED .**

****

**Step 1: Configure all routers and test Connectivity to connected interfaces.**

ISP1#

ISP1#conf t

Enter configuration commands, one per line. End with CNTL/Z. ISP1(config)#int s1/0

ISP1(config-if)#ip add 192.168.1.5 255.255.255.252

ISP1(config-if)#no shut ISP1(config-if)#

\*Jun 24 09:43:40.579: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up ISP1(config-if)#

\*Jun 24 09:43:40.579: %ENTITY\_ALARM-6-INFO: CLEAR INFO Se1/0 Physical Port Administrative State Down

ISP1(config-if)#

\*Jun 24 09:43:41.583: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

ISP1(config-if)#int s1/2

ISP1(config-if)#ip add 192.168.1.1 255.255.255.252

\*Jun 24 09:44:08.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down

ISP1(config-if)#ip add 192.168.1.1 255.255.255.252

ISP1(config-if)#no shut ISP1(config-if)#int fa0/0

ISP1(config-if)#ip add 192.168.100.1 255.255.255.252

ISP1(config-if)#ip add 192.168.100.1 255.255.255.0

ISP1(config-if)#no shut ISP1(config-if)#

SANJOSE1#

SANJOSE1#conf t

Enter configuration commands, one per line. End with CNTL/Z. SANJOSE1(config)#int s1/0

SANJOSE1(config-if)#ip add 192.168.1.6 255.255.255.252

SANJOSE1(config-if)#no shut SANJOSE1(config-if)#int s1/1

SANJOSE1(config-if)#ip add 172.16.1.1 255.255.255.0

SANJOSE1(config-if)#no shut SANJOSE1(config-if)#int lo 0

SANJOSE1(config-if)#ip add 172.16.64.1 255.255.255.0

SANJOSE1(config-if)#no shut SANJOSE1(config-if)#^Z SANJOSE1#

SANJOSE2#conf t

Enter configuration commands, one per line. End with CNTL/Z. SANJOSE2(config)#int s1/1

SANJOSE2(config-if)#ip add 172.16.1.2 255.255.255.0

SANJOSE2(config-if)#no shut SANJOSE2(config-if)#int s1/2

SANJOSE2(config-if)#ip add 172.168.1.2 255.255.255.252

SANJOSE2(config-if)#no shut SANJOSE2(config-if)#int lo 0

SANJOSE2(config-if)#ip add 172.16.32.1 255.255.255.0

SANJOSE2(config-if)#no shut SANJOSE2(config-if)#^Z SANJOSE2#

**Step2 Configure EIGRP between the SanJose1 and SanJose2 routers with the same commands as follows:**

SANJOSE1#conf t

Enter configuration commands, one per line. End with CNTL/Z. SANJOSE1(config)#router eigrp 64512

SANJOSE1(config-router)#network 172.16.0.0 SANJOSE1(config-router)#exit SANJOSE1(config)#

SANJOSE2#conf t

Enter configuration commands, one per line. End with CNTL/Z. SANJOSE2(config)#router eigrp 64512

SANJOSE2(config-router)#network 172.16.0.0 SANJOSE2(config-router)#exit SANJOSE2(config)#

**Step3 Configure IBGP between the SanJose1 and SanJose2 routers. On the SanJose1 router, enter the followings :**

SANJOSE1#

SANJOSE1#conf t

Enter configuration commands, one per line. End with CNTL/Z. SANJOSE1(config)#router bgp 64512

SANJOSE1(config-router)#no auto-summary

SANJOSE1(config-router)#neighbor 172.16.32.1 remote-as 64512

SANJOSE1(config-router)#neighbor 172.16.32.1 update-source lo 0 SANJOSE1(config-router)#^Z

SANJOSE1#

\*Jun 24 10:03:18.479: %SYS-5-CONFIG\_I: Configured from console by console

SANJOSE1#

SANJOSE1#conf t

Enter configuration commands, one per line. End with CNTL/Z. SANJOSE1(config)#router bgp 64512

SANJOSE1(config-router)#no synchronization SANJOSE1(config-router)#

SANJOSE2#conf t

Enter configuration commands, one per line. End with CNTL/Z. SANJOSE2(config)#router bgp 64512

SANJOSE2(config-router)#no synchronization SANJOSE2(config-router)# SANJOSE2(config-router)#

**Step-4 Complete the Ibgp Configurations on Sanjose2 by entering the commands.**

SANJOSE2#

SANJOSE2#conf t

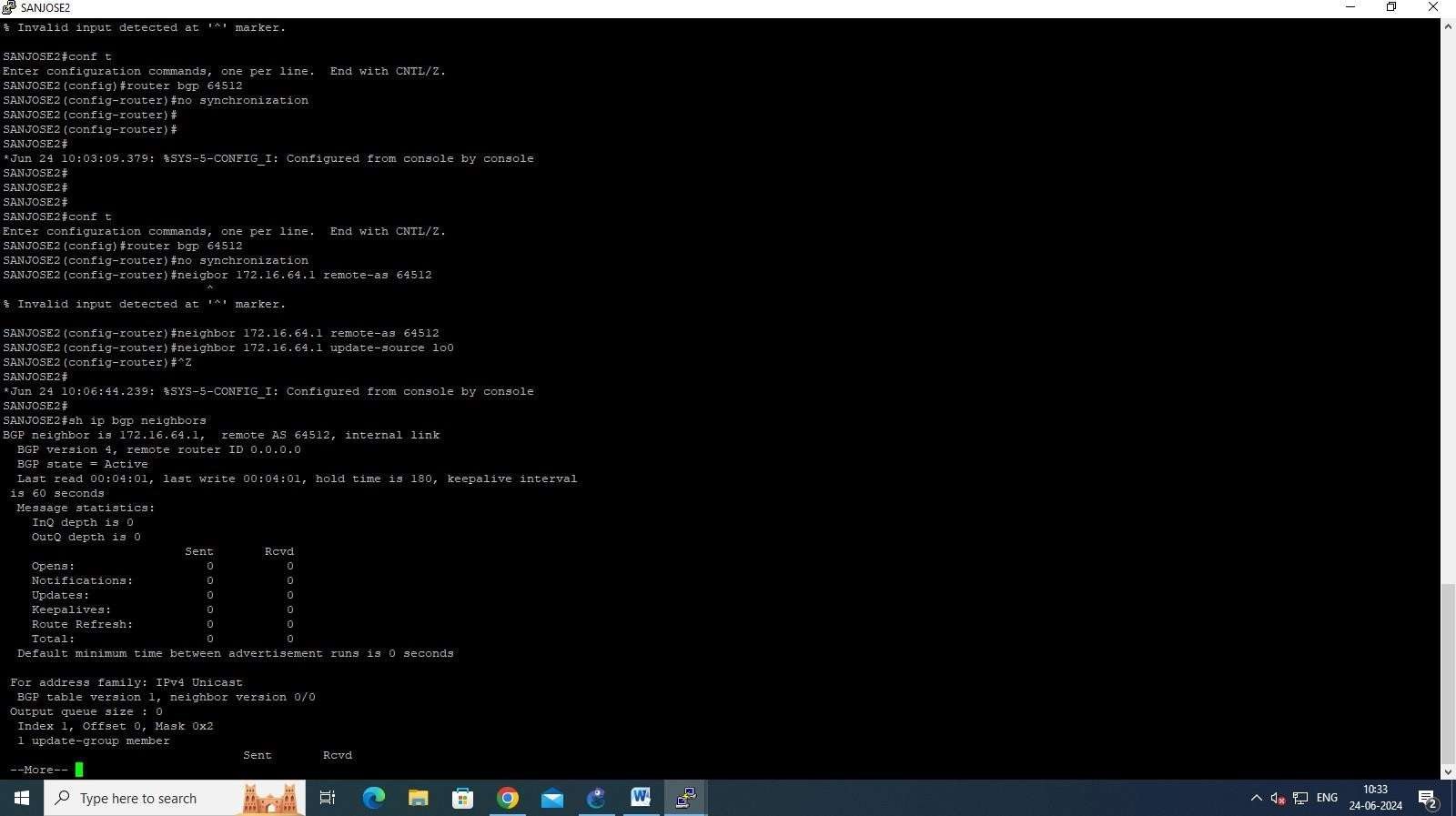
Enter configuration commands, one per line. End with CNTL/Z. SANJOSE2(config)#router bgp 64512

SANJOSE2(config-router)#no synchronization SANJOSE2(config-router)#neighbor 172.16.64.1 remote-as 64512

SANJOSE2(config-router)#neighbor 172.16.64.1 update-source lo0 SANJOSE2(config-router)#^Z

SANJOSE2#





**Step 5: Configure ISP1 to run EBGP with SanJose1 and SanJose2. Enter the following Commonds on ISP1 as shown in the following:**

ISP1#

ISP1#conf t

Enter configuration commands, one per line. End with CNTL/Z. ISP1(config)#router bgp 200

ISP1(config-router)#no auto-summary

ISP1(config-router)#neighbor 192.168.1.6 remote-as 64512

ISP1(config-router)#neighbor 192.168.1.2 remote-as 64512

ISP1(config-router)#network 192.168.100.0 ISP1(config-router)#

**Step6: Configure SanJose1 as an EBGP peer to ISP1 as shown in the following:**

SANJOSE1#conf t

Enter configuration commands, one per line. End with CNTL/Z. SANJOSE1(config)#ip route 172.16.0.0 255.255.0.0 null0

SANJOSE1(config)#router bgp 64512

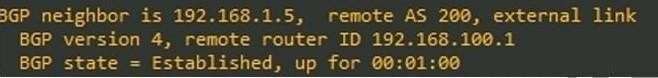
SANJOSE1(config-router)#neighbor 192.168.1.5 remote-as 200 SANJOSE1(config-router)#

SANJOSE1(config-router)#network 172.16.0.0 SANJOSE1(config-router)#

\*Jun 24 11:00:14.303: %BGP-5-ADJCHANGE: neighbor 192.168.1.5 Up

SANJOSE1(config-router)#^Z SANJOSE1#

**Use the Show ip bgp neighbors:**

****

**Step7: Configure SAnJose1 As an EBGP peer to ISP1:-**

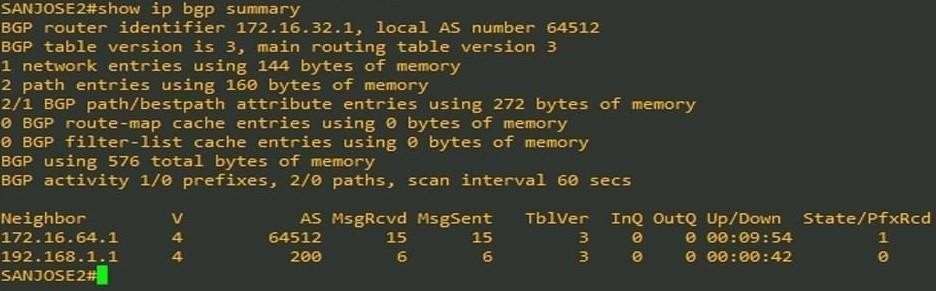
SANJOSE2#conf t

Enter configuration commands, one per line. End with CNTL/Z. SANJOSE2(config)#ip route 172.16.0.0 255.255.0.0 null0

SANJOSE2(config)#router bgp 64512

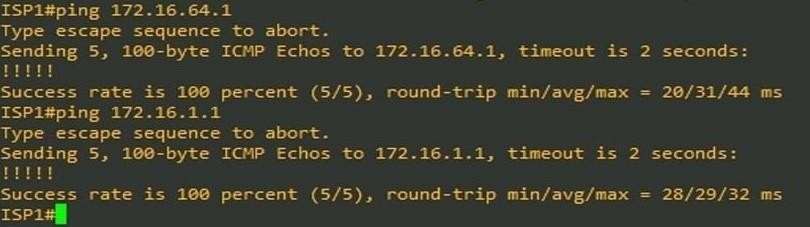
SANJOSE2(config-router)#neighbor 192.168.1.1 remote-as 200 SANJOSE2(config-router)#

SANJOSE2(config-router)#network 172.16.0.0 SANJOSE2(config-router)#

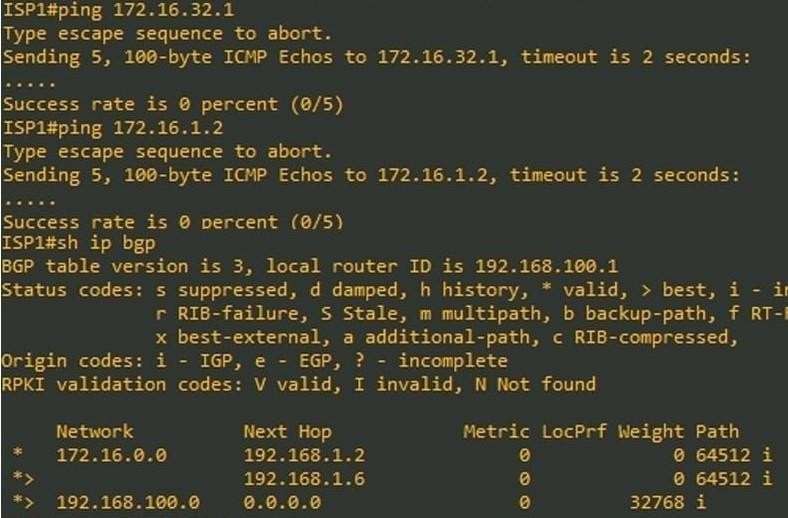


**Step8:**

Test whether ISP1 can ping the Loopback 0 address of 172.16.64.1 from SanJosel, as well as the serial link between San Josel and San Jose2, 172.16.1.1.



Now ping from ISP1 to the Loopback 0 address of 172.16.32.1 from San Jose2, as well as the serial link between San Josel and SanJose2. This time try 172.16.1.2.



At this point, the be able to get to each network connected to San Jose2 from the FastEthernet address 192.168.100.1.

ISP1#ping Protocol [ip]:

Target IP address: 172.16.64.1 Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 192.168.100.1 Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose [none]: Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.64.1, timeout is 2 seconds: Packet sent with a source address of 192.168.100.1

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/27/36 ms

ISP1#ping Protocol [ip]:

Target IP address: 172.16.1.1 Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Source address or interface: 192.168.100.1 Extended commands [n]: y

Set DF bit in IP header? [no]:

Type of service [0]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds: Packet sent with a source address of 192.168.100.1 Thakkar

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/29/40 ms

ISP1#ping Protocol [ip]:

Target IP address: 172.16.32.1 Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 192.168.100.1 Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD] Binita

Loose, Strict, Record, Timestamp, Verbose [none]: Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.32.1, timeout is 2 seconds: Packet sent with a source address of 192.168.100.1

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms

ISP1#ping Protocol [ip]:

Target IP address: 172.16.1.2 Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 192.168.100.1 Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp. Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: Packet sent with a source address of 192.168.100.1

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/48 ms ISP1#

Complete reachability was proven between the ISP1 router and both San Josel and SanJose2.

**Step9:**

Before the ISP can successfully ping the internal serial interfaces of AS 64512, two issues need to be resolved. First, SanJosel does not know about the link between the ISP and SanJose2. Second, San Jose2 is unaware of the link between the ISP and San Josel. This can be resolved by an advertisement of these serial links by way of BGP router. This can also be resolved by way of EIGRP on each of the San Jose routers. The preferred method is for the ISP to advertise these links. If they are advertised and then, at a future date, a BGP link is activated to another ISP in addition to a risk of becoming a Transit AS. Binita AS 200, then there is

ISP1#conf t

ISP1 (config)#router bgp 200

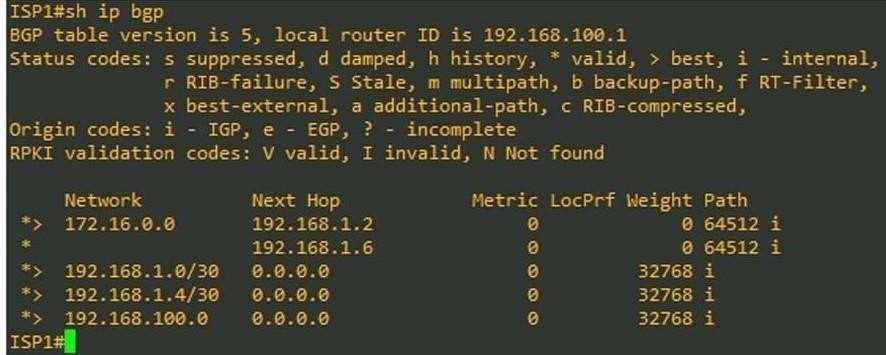
ISP1 (config-router)#network 192.168.1.0 mask 255.255.255.252

ISP1(config-router)#network 192.168.1.4 mask 255.255.255.252 ISP1 (config-router)#^Z

ISP1#

\*May 15 09:41:45.207: %SYS-5-CONFIG\_I: Configured from console by console ISP1#





Verify on San Josel and San Jose2 that the opposite WAN link is included in the routing table. The output from San Jose2 is shown as follows:



2nd last line of output

The next issue to consider is BGP policy routing between AS systems. BGP routers do not increment the next hop address to their IBGP peers. The San Jose2 router is passing a policy to SanJosel and vice versa. The policy for routing from AS 64512 to AS 200 is to forward packets to the 192.168.1.1 interface. SanJosel has a similar yet opposite policy, forwarding requests to the 192.168.1.5 interface. In the event that either WAN link fails, it is critical that the opposite router become a valid gateway. This is only achieved if the next-hop-self command is configured on SanJosel and San Jose2.



SANJOSE1 #conf t

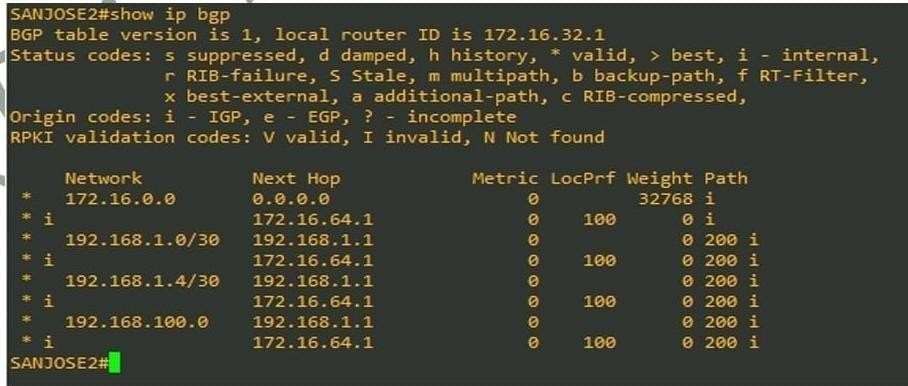
SANJOSE1 (config)#router bgp 64512

SANJOSE1 (config-router)#neighbor 172.16.32.1 next-hop-self Tha SANJOSE1 (config-router)#^Z

SANJOSE2#conf t

SANJOSE2 (config)#router bgp 64512

SANJOSE2 (config-router) #neighbor 172.16.64.1 next-hop-self SANJOSE2(config-router)#^Z



**Step10:**

At this point, everything looks good with the exception of default routes, the outbound flow of data, and inbound packet flow. Since the local preference value is shared between IBGP neighbors, configure a simple route-map that references local preference value on SanJosel and San Jose2. This policy will adjustoutbound traffic to prefer the link off the SanJosel router instead of the metered T1 off San Jose2.

SANJOSE1#conf t

SANJOSE1 (config)#route-map PRIMARY\_T1\_IN permit 10 SANJOSE1 (config-route-map) #set local-preference 150 SANJOSE1 (config-route-map)#

SANJOSE1 (config)#router bgp 64512

SANJOSE1 (config-router)#neighbor 192.168.1.5 route-map PRIMARY\_T1\_IN i SANJOSE1 (config-router)#^Z

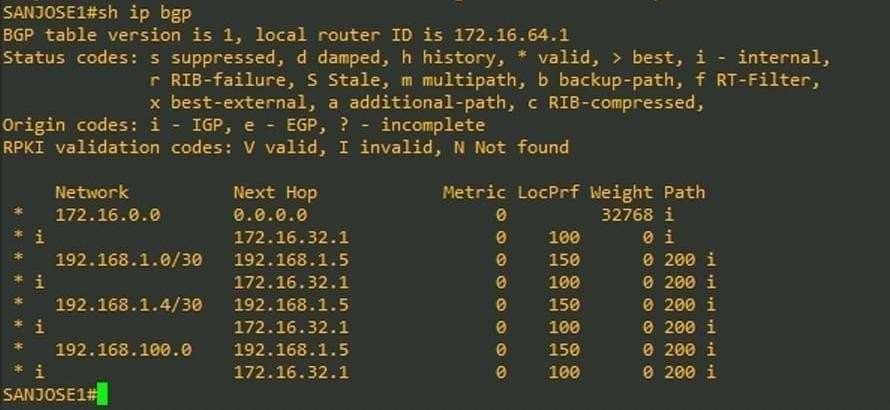
SANJOSE2#conf t

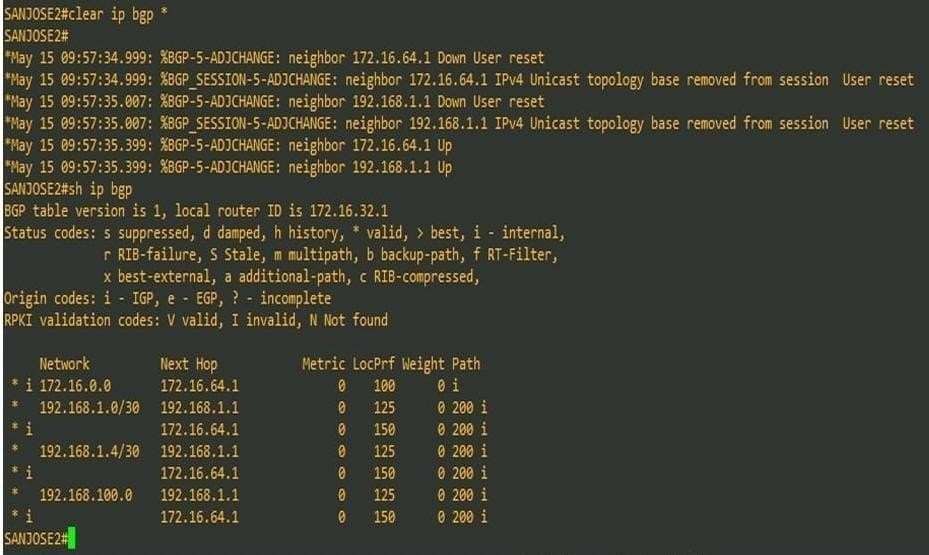
SANJOSE2 (config)#route-map SECONDARY\_T1\_IN permit 10 SANJOSE2 (config-route-map) #set local-preference 125 SANJOSE2 (config-route-map) #router bgp 64512

SANJOSE2 (config-router)#neighbor 192.168.1.1 route-map SECONDARY\_T1\_IN in SANJOSE2 (config-router)#^Z

Use clear ip bgp \*







**Step11:**

How will traffic return from network 192.168.100.0/24? Through San Josel or SanJose2? Issue s hip bgp on ISP1.

SANJOSE2#ping Protocol [ip]:

Target IP address: 192.168.100.1 Repeat count [5]: 2

Datagram size [100]: Timeout in seconds [2]:

Extended commands [n]: y Source

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose. Strict, Record, Timestamp, Verbose[none]: record Number of hops [9]:

Loose, Strict, Record, Timestamp, Verbose [RV]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 2, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds: Packet sent with a source address of 172.16.32.1

Packet has IP options: Total option bytes= 39, padded length=40 Record route: <\*>

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

Reply to request 0 (52 ms). Received packet has options Total option bytes= 40, padded length=40

Record route:

(172.16.1.2)

(192.168.1.6)

(192.168.1.5)

(192.168.1.5)

(172.16.1.1)

(172.16.1.2) <\*>

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

End of list

Reply to request 1 (52 ms). Received packet has options Total option bytes= 40. padded length

Record route:

(172.16.1.2)

(192.168.1.6)

(192.168.1.5)

(192.168.1.5)

(172.16.1.1)

(172.16.1.2) <\*>

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

End of list

Success rate is 100 percent (2/2), round-trip min/avg/max = 52/52/52 ms SANJOSE2#

The next step is to create a new policy to force ISP to return all traffic via SanJosel. Create a second route-map utilizing MED (metric) which is shared between EBGP neighbors.

SANJOSE1#conf t

SANJOSE1 (config)#route-map PRIMARY\_T1\_MED\_OUT permit 10 SANJOSE1 (config-route-map) #set Metric 50

SANJOSE1 (config-route-map)#exit SANJOSE1 (config)#router bgp 64512

SANJOSE1 (config-router)#neighbor 192.168.1.5 route-map PRIMARY\_T1\_MED\_OUT out SANJOSE1 (config-router)#

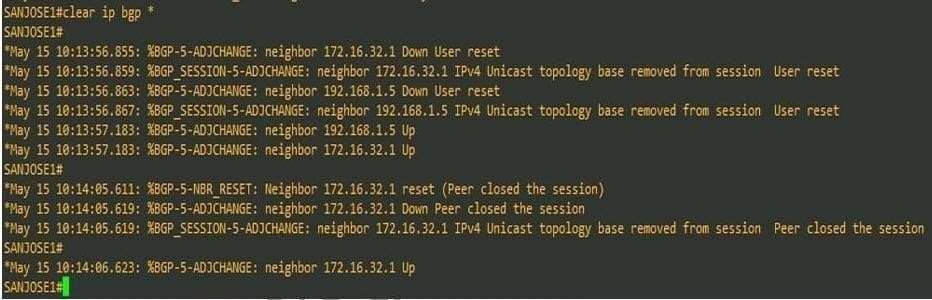
SANJOSE2#conf t

SANJOSE2 (config)#route-map SECONDARY\_T1\_MED\_OUT permit 10 SANJOSE2 (config-route-map) #set Metric 75

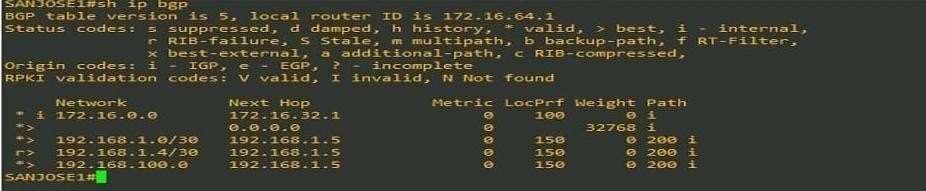
SANJOSE2 (config-route-map)#exit SANJOSE2 (config)#router bgp 64512

SANJOSE2(config-router)#$2.168.1.1 route-map SECONDARY\_T1\_MED\_OUT out SANJOSE2(config-router)#

**As before, issue clear ip bgp \* after issuing new policy**



****



Reissue extended ping command with record command SANJOSE2#ping

Protocol [ip]:

Target IP address: 192.168.100.1 Repeat count [5]: 2

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 172.16.32.1 Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none ]: record Number of hops [9]:

Loose, Strict, Record, Timestamp, Verbose[RV]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 2, 100-byte ICMP Echos to 192.168.100.1. timeout is 2 seconds: Packet sent with a source address of 172.16.32.1

Packet has IP options: Total option bytes= 39, padded length-40 Record route: <\*>

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

Reply to request 0 (56 ms). Received packet has options

Total option bytes 40, padded length-40 Record route:

(172.16.1.2)

(192.168.1.6)

(192.168.1.5)

(192.168.1.5)

(172.16.1.1)

(172.16.1.2) <\*>

(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

End of list

Reply to request 1 (48 ms). Received packet has options Total option bytes=40, padded length=40

Record route:

(172.16.1.2)

(192.168.1.6)

(192.168.1.5)

(192.168.1.5)

(172.16.1.1)

(172.16.1.2) <\*>

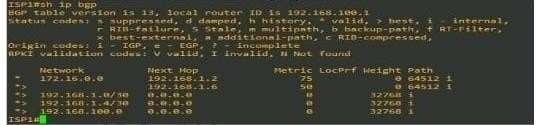
(0.0.0.0)

(0.0.0.0)

(0.0.0.0)

End of list

Issue sh ip bgp on ISP to check the updated MED value used,



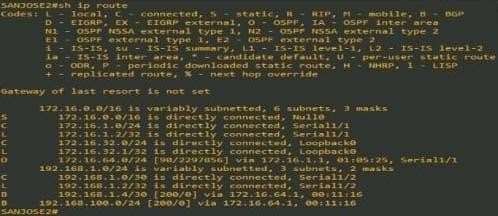
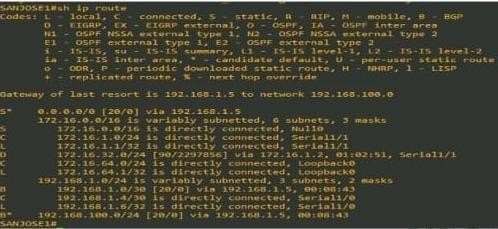
**Step 12:**

Establish a default route that uses a policy statement that will adjust to changes in the network. Configure both San Josel and Sanjose2 to use 192.168.100.0/24 as the default network.



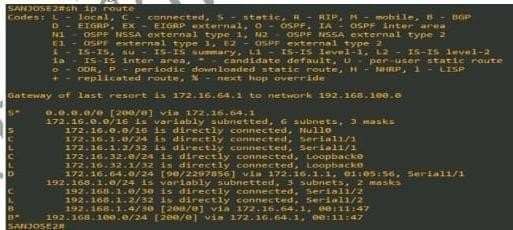
SANJOSEI#conft

SANJOSEI (config)#ip default-network 192.168.100.0



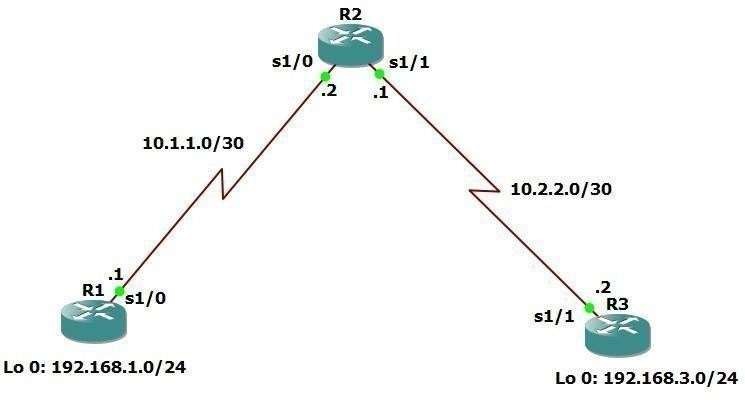
SANJOSE2#conf t

SANJOSE2 (config)#ip default-network 192.168.100.0 SANJOSE2 (config)



**Practical :04**

**Aim: Configuring Secure Management Plane (On GNS3)**

****

**Step 1: Configure loopbacks and assign addresses.**

R1#conf t R1(config)#int lo 0

R1(config-if)#ip add 192.168.1.1 255.255.255.0 R1(config-if)#exit

R1(config)#int se1/0

R1(config-if)#ip add 10.1.1.1 255.255.255.252 R1(config-if)#no shut

R1(config-if)#exit

R2#conf t R2(config)#int se1/0

R2(config-if)#ip add 10.1.1.2 255.255.255.252 R2(config-if)#no shut

R2(config-if)#exit R2(config)#int se1/1

R2(config-if)#ip add 10.2.2.1 255.255.255.252 R2(config-if)#no shut

R2(config-if)#exit

R3#conf t R3(config)#int lo 0

R3(config-if)#ip add 192.168.3.1 255.255.255.0 R3(config-if)#exit

R3(config)#int se1/1

R3(config-if)#ip add 10.2.2.2 255.255.255.252

R3(config-if)#no shut R3(config-if)#exit

**Step 2: Configure static routes.**

R1#conf t

R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2

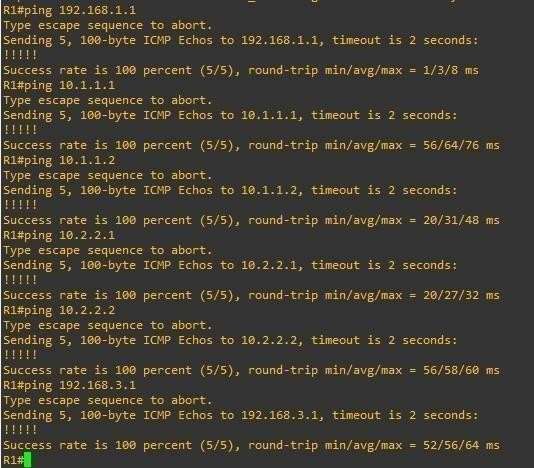
R3#conf t

R3(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.1

R2#conf t

R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1

R2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.2

Verify connectivity from R1

**Step 3: Secure management access.**

1. On R1, use the **security passwords** command to set a minimum password length of 10 characters.

R1(config)#security passwords min-length 10

1. Configure the enable secret encrypted password on both routers. R1(config)#enable secret class12345
2. Configure a console password and enable login for routers. For additional security, the **exectimeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry. **Note**: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring.

R1(config)#line console 0

R1(config-line)#password ciscoconpass R1(config-line)#exec-timeout 5 0 R1(config-line)#login

R1(config-line)#logging synchronous R1(config-line)#exit

1. Configure the password on the vty lines for router R1. R1(config)#line vty 0 4

R1(config-line)#password ciscovtypass R1(config-line)#exec-timeout 5 0 R1(config-line)#login

R1(config-line)#exit

1. The aux port is a legacy port used to manage a router remotely using a modem and is hardly ever used. Therefore, disable the aux port.

R1(config)#line aux 0 R1(config-line)#no exec R1(config-line)#end

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

R1#conf t

R1(config)#service password-encryption

1. Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner using the **banner motd** command. When a user connects to one of the routers, the MOTD banner appears before the login prompt. In this example, the dollar sign ($) is used to start and end the message.

R1(config)#banner motd $Unauthorized access strictly prohibited!$ R1(config)#exit

Repeat the configuration portion of steps 3a through 3g on router R3. R3#conf t

R3(config)#security passwords min-length 10

R3(config)#enable secret class12345 R3(config)#line console 0

R3(config-line)#password ciscoconpass

R3(config-line)#exec-timeout 5 0 R3(config-line)#login

R3(config-line)#logging synchronous R3(config-line)#exit

R3(config)#line vty 0 4

R3(config-line)#password ciscovtypass R3(config-line)#exec-timeout 5 0 R3(config-line)#login

R3(config-line)#exit

R3(config)#line aux 0 R3(config-line)#no exec R3(config-line)#end

R3#conf t

R3(config)#service password-encryption

R3(config)#banner motd $Unauthorized access strictly prohibited!$ R3(config)#exit

**Step 4: Configure enhanced username password security.**

1. To create local database entry encrypted to level 4 (SHA256), use the **username** *name* **secret** *password* global configuration command. In global configuration mode, enter the following command:

R1#conf t

R1(config)#username JR-ADMIN secret class12345 R1(config)#username ADMIN secret class54321

1. Set the console line to use the locally defined login accounts. R1(config)#line console 0

R1(config-line)#login local R1(config-line)#exit

1. Set the vty lines to use the locally defined login accounts. R1(config)#line vty 0 4

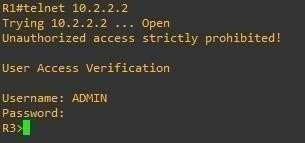
R1(config-line)#login local R1(config-line)#end

R1#

1. Repeat the steps 4a to 4c on R3. R3#conf t

R3(config)#username JR-ADMIN secret class12345 R3(config)#username ADMIN secret class54321 R3(config)#line console 0

R3(config-line)#login local R3(config-line)#exit R3(config)#line vty 0 4 R3(config-line)#login local R3(config-line)#end

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

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

1. 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.

R1(config)#aaa new-model

1. Configure the specifics for the first RADIUS server located at 192.168.1.101. Use

**RADIUS1-pa55w0rd** as the server password.

R1(config)#radius server RADIUS-1

R1(config-radius-server)#address ipv4 192.168.1.101 R1(config-radius-server)#key RADIUS-1-pa55w0rd R1(config-radius-server)#exit

1. Configure the specifics for the second RADIUS server located at 192.168.1.102. Use

**RADIUS-2-pa55w0rd** as the server password.

R1(config)#radius server RADIUS-2

R1(config-radius-server)#address ipv4 192.168.1.102 R1(config-radius-server)#key RADIUS-2-pa55w0rd R1(config-radius-server)#exit

1. Assign both RADIUS servers to a server group. R1(config)#aaa group server radius RADIUS-GROUP

R1(config-sg-radius)#server name RADIUS-1 R1(config-sg-radius)#server name RADIUS-2 R1(config-sg-radius)#exit

1. 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.. R1(config)#aaa authentication login default group RADIUS-GROUP local
2. 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.

R1(config)#aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case

1. Alter the VTY lines to use the TELNET-LOGIN AAA authentiaiton method. R1(config)#line vty 0 4

R1(config-line)#login authentication TELNET-LOGIN R1(config-line)#exit

R1(config)#

1. Repeat the steps 5a to 5g on R3. R3#conf t

R3(config)#aaa new-model R3(config)#radius server RADIUS-1

R3(config-radius-server)#address ipv4 192.168.1.101 R3(config-radius-server)#key RADIUS-1-pa55w0rd R3(config-radius-server)#exit

R3(config)#radius server RADIUS-2

R3(config-radius-server)#address ipv4 192.168.1.102 R3(config-radius-server)#key RADIUS-2-pa55w0rd R3(config-radius-server)#exit

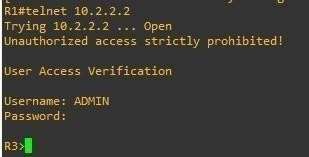
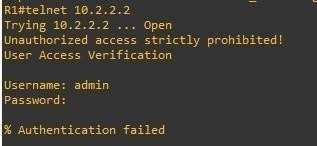
R3(config)#aaa group server radius RADIUS-GROUP R3(config-sg-radius)#server name RADIUS-1 R3(config-sg-radius)#server name RADIUS-2 R3(config-sg-radius)#exit

R3(config)#aaa authentication login default group RADIUS-GROUP local R3(config)#aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case R3(config)#line vty 0 4

R3(config-line)#login authentication TELNET-LOGIN R3(config-line)#exit

R3(config)#

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



**Note:** The actual login time is longer since the RADIUS servers are not available.

**Step 6: Enabling secure remote management using SSH.**

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

R1#conf t

R1(config)#ip domain-name ccnasecurity.com

1. 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.

R1(config)#crypto key zeroize rsa

% No Signature Keys found in configuration.

1. 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.

R1(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: R1.ccnasecurity.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 1 seconds)

R1(config)#

\*Apr 9 18:21:15.683: %SSH-5-ENABLED: SSH 1.99 has been enabled

1. Configure SSH version 2 on R1. R1#conf t

R1(config)#ip ssh version 2

1. Configure the vty lines to use only SSH connections. R1(config)#line vty 0 4

R1(config-line)#transport input ssh R1(config-line)#end

R1#

1. Verify the SSH configuration using the **show ip ssh** command.
2. Repeat the steps 6a to 6f on R3. R3#conf t

R3(config)#ip domain-name ccnasecurity.com R3(config)#crypto key zeroize rsa

% No Signature Keys found in configuration.

R3(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: R3.ccnasecurity.com

% The key modulus size is 1024 bits

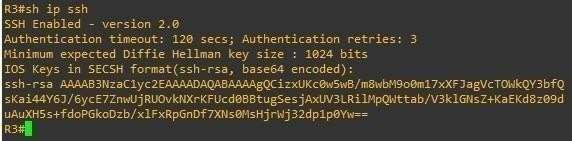
% Generating 1024 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 0 seconds)

R3(config)#

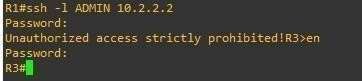
\*Apr 9 18:24:19.763: %SSH-5-ENABLED: SSH 1.99 has been enabled R3(config)#ip ssh version 2

R3(config)#line vty 0 4

R3(config-line)#transport input ssh R3(config-line)#end

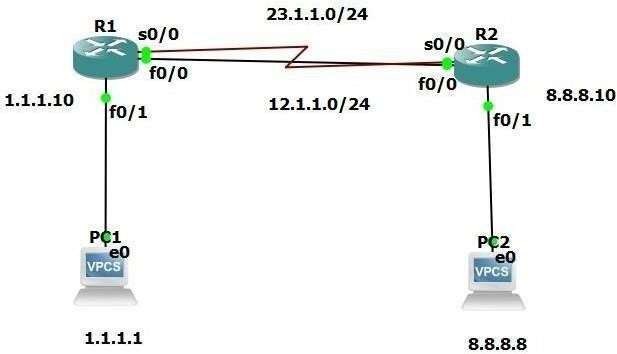
R3#

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



**Practical 5:**

**Aim: configuring PBR (on GNS3)**

****

**Configure R1:**

R1#conf t R1(config)#int fa0/0

R1(config-if)#ip add 12.1.1.1 255.255.255.0 R1(config-if)#no shut

R1(config-if)#exit R1(config)#int s2/0 R1(config-if)#ip add 23.1.1.1 255.255.255.0 R1(config-if)#no shut

R1(config-if)#exit R1(config)#int f1/0

R1(config-if)#ip add 1.1.1.10 255.255.255.0 R1(config-if)#no shut

R1(config)#exit

**Configure R2:**

R2#conf t R2(config)#int fa0/0

R2(config-if)#ip add 12.1.1.2 255.255.255.0 R2(config-if)#no shut

R2(config-if)#exit R2(config)#int se2/0

R2(config-if)#ip add 23.1.1.2 255.255.255.0 R2(config-if)#no shut

R2(config-if)#exit R2(config)#int fa1/0

R2(config-if)#ip add 8.8.8.10 255.255.255.0 R2(config-if)#no shut

R2(config-if)#exit

**Configure OSPF ON R1** R1#conf t R1(config)#router ospf 100

R1(config-router)#network 12.1.1.0 0.0.0.255 area 1

R1(config-router)#network 23.1.1.0 0.0.0.255 area 1

R1(config-router)#network 1.1.1.0 0.0.0.255 area 1 R1(config-router)#exit R1(config)#

**Configure OSPF ON R2** R2#conf t R2(config)#router ospf 100

R2(config-router)#network 12.1.1.0 0.0.0.255 area 1

R2(config-router)#network 12.1.1.0 0.0.0.255 area 1 R2(config-router)#network 23.1.1.0

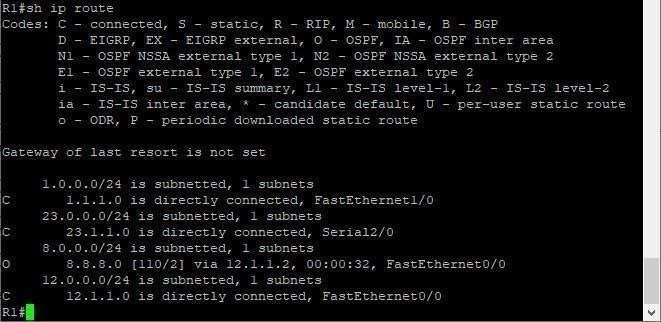
0.0.0.255 area 1

R2(config-router)#network 23.1.1.0 0.0.0.255 area 1

R2(config-router)#network 8.8.8.0 0.0.0.255 area 1 R2(config-router)#exit

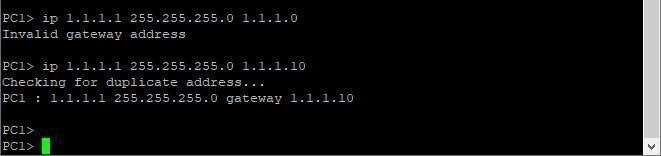
R2(config)#exit

**Check connectivity on R1**

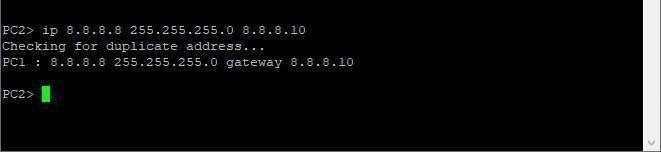
****

**Check connectivity on R2**



**Configure PC1**

**Configure PC2**



PC1> ping 8.8.8.8

8.8.8.8 icmp\_seq=1 timeout

84 bytes from 8.8.8.8 icmp\_seq=2 ttl=62 time=72.629 ms 84 bytes from 8.8.8.8 icmp\_seq=3 ttl=62 time=44.246 ms 84 bytes from 8.8.8.8 icmp\_seq=4 ttl=62 time=76.415 ms 84 bytes from 8.8.8.8 icmp\_seq=5 ttl=62 time=55.456 ms

**Configure PBR on R2**

R2#conf t

R2(config)#access-list 100 permit icmp host 1.1.1.1 host 8.8.8.8 R2(config)#access-list 100 permit ip any any R2(config)#access-list 101 permit icmp host 1.1.1.1 host 8.8.8.8 R2(config)#access-list 101 permit ip any any

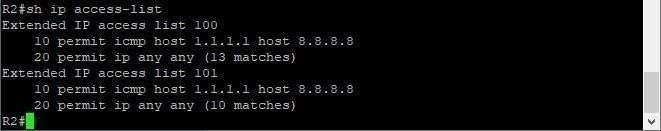
R2(config)#int s2/0

R2(config-if)#ip access-group 100 in R2(config-if)#exit

R2(config)#int fa0/0

R2(config-if)#ip access-group 101 in R2(config-if)#exit

R2(config)#exit

**Check access-list on R2**

**Configure PBR on R1**

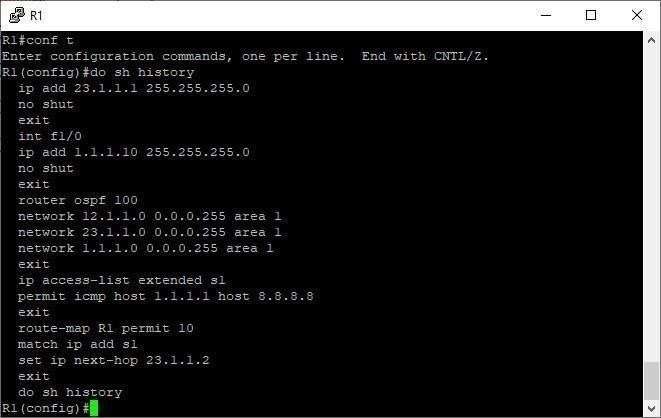
R1#conf t

R1(config)#ip access-list extended s1

R1(config-ext-nacl)#permit icmp host 1.1.1.1 host 8.8.8.8 R1(config-ext-nacl)#exit

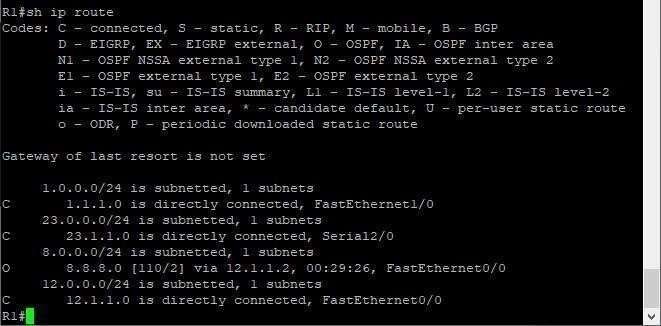
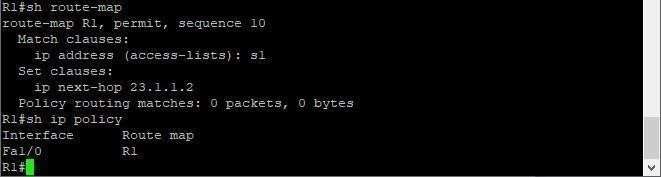
R1(config)#route-map R1 permit 10 R1(config-route-map)#match ip add s1 R1(config-route-map)#set ip next-hop 23.1.1.2 R1(config-route-map)#exit

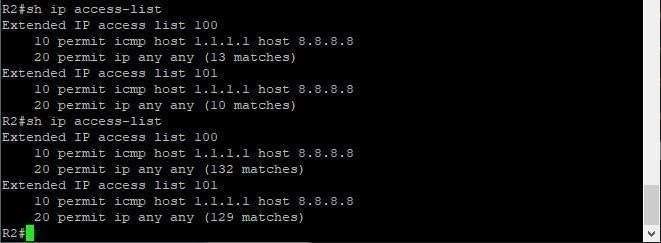
R1(config)#



R1(config)#int f1/0

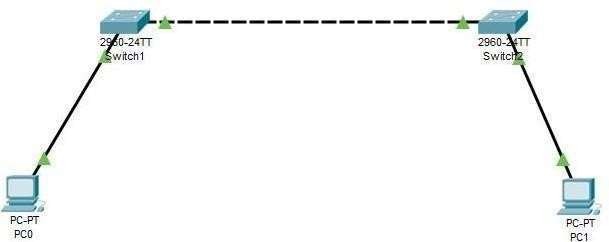
R1(config-if)#ip policy route-map R1 R1(config-if)#do sh history





**Practical No. : 6**

**Aim: Configuring remote SPAN (On Cisco Packet Tracer)**

****

**Configure S1** Switch>en Switch#conf t Switch(config)#vlan 8

Switch(config-vlan)#remote-span

Switch(config-vlan)#monitor session 1 source int fa0/2 Switch(config)#monitor session 1 destination remote vlan 8 reflector-port fa0/5 Switch(config)#^Z

**Configure S2** Switch>en Switch#conf t Switch(config)#vlan 8

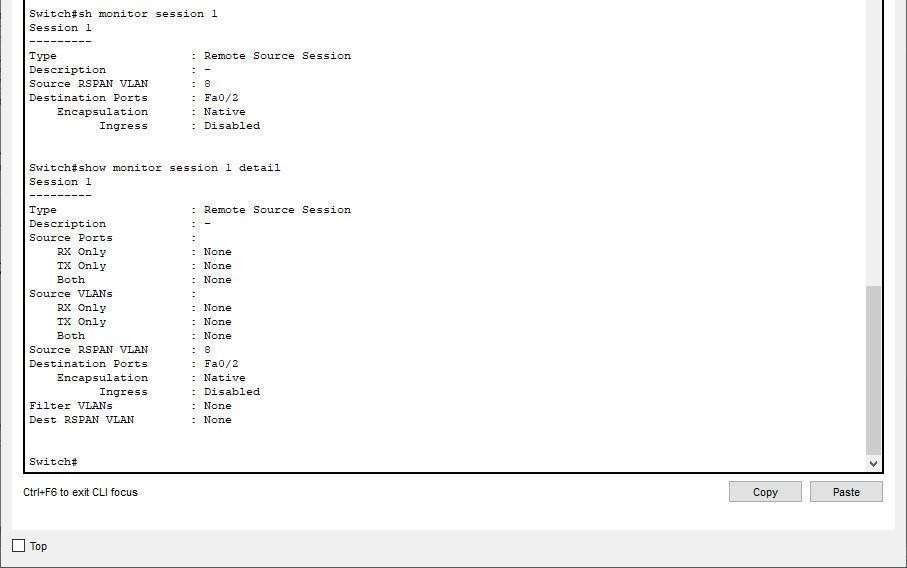
Switch(config-vlan)#remote-span

Switch(config-vlan)#monitor session 1 source remote vlan 8 Switch(config)#monitor session 1 destination int fa0/2 Switch(config)#^Z

**Output S1:**

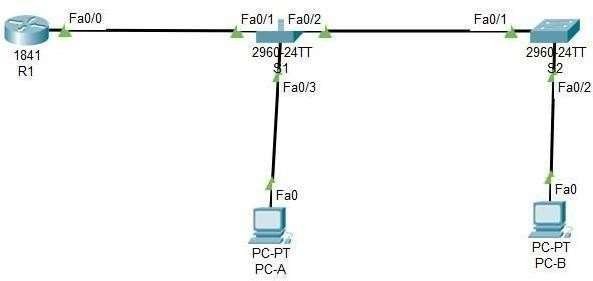
****

**Output S2:**

****

**Practical :7**

**Aim: Configuring Inter-VLAN Routing(On Packet Tracer).**

****

**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interfaces** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| R1 | F0/0.10 | 192.168.10.1 | 255.255.255.0 | N/A |
| F0/0.20 | 192.168.20.1 | 255.255.255.0 |
| F0/0.30 | 192.168.30.1 | 255.255.255.0 |
| F0/0.1000 | N/A | N/A |
| S1 | VLAN 10 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S2 | VLAN 10 | 192.168.10.12 | 255.255.255.0 | 192.168.10.1 |
| PC-A | NIC | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |
| PC-B | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |

**VLAN Table**

|  |  |  |
| --- | --- | --- |
| **VLAN** | **Name** | **Interface Assigned** |
| 10 | Management | S1: VLAN 10 |
| S2: VLAN 10 |
| 20 | Sales | S1: F0/3 |
| 30 | Operations | S2: F0/2 |
| 999 | Parking-Lot | S1: F0/4-24, G0/1-2 |
| S2: F0/3-24, G0/1-2 |
| 1000 | Native | N/A |

**Assgining switch 1 for VLAN**

Switch>en Switch#conf t

Switch(config)#hostname S1 S1(config)#vlan 10

S1(config-vlan)#name Management S1(config-vlan)#exit S1(config)#vlan 20

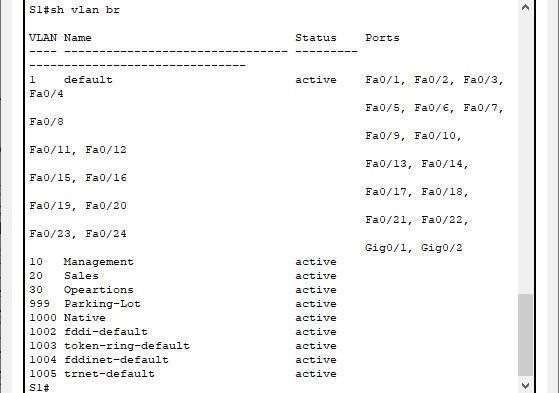
S1(config-vlan)#name Sales S1(config-vlan)#exit S1(config)#vlan 30

S1(config-vlan)#name Opeartions S1(config-vlan)#exit S1(config)#vlan 999

S1(config-vlan)#name Parking-Lot S1(config-vlan)#exit S1(config)#vlan 1000

S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#end

**Check VLAN on S1**

****

**Configure S1 for VLAN 10**

S1#conf t S1(config)#int vlan 10

ip add 192.168.10.11 255.255.255.0

S1(config-if)#exit

S1(config)#ip default-gateway 192.168.10.1

S1(config)#int vlan 10 S1(config-if)#no shut S1(config-if)#exit S1(config)#end S1#conf t

S1(config)#int range f0/4-24, g0/1-2 S1(config-if-range)#switchport mode access

S1(config-if-range)#switchport access vlan 999 S1(config-if-range)#shutdown

**OUTPUT:**

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

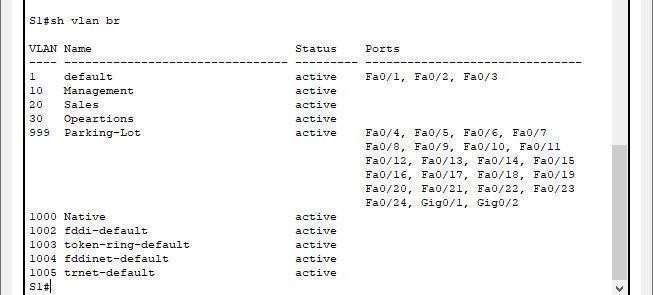
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down



**Assign switch 2 for VLAN**

Switch>en Switch#conf t

Switch(config)#hostname S2 S2(config)#vlan 10

S2(config-vlan)#name Management S2(config-vlan)#exit S2(config)#vlan 20

S2(config-vlan)#name sales S2(config-vlan)#exit S2(config)#vlan 30

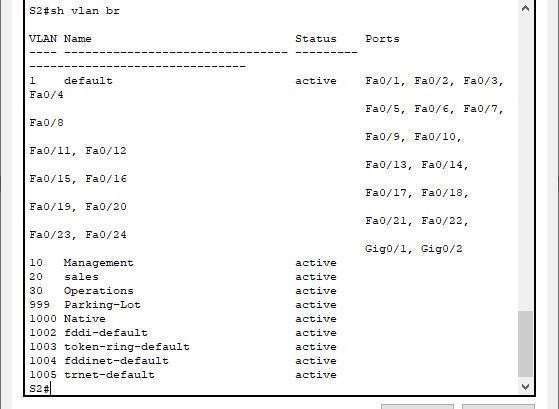
S2(config-vlan)#name Operations S2(config-vlan)#exit

S2(config)#vlan 999

S2(config-vlan)#name Parking-Lot S2(config-vlan)#exit S2(config)#vlan 1000

S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#end

**Check VLAN on S2**

****

**Configure S2 for VLAN 10**

S2#conf t

S2(config-if)#ip add 192.168.10.12 255.255.255.0

S2(config-if)#int vlan 10 S2(config-if)#no shut S2(config-if)#exit

S2(config)#int range f0/3-24,g0/1-2 S2(config-if-range)#switchport mode access

S2(config-if-range)#switchport access vlan 999 S2(config-if-range)#shutdown

**OUTPUT:**

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

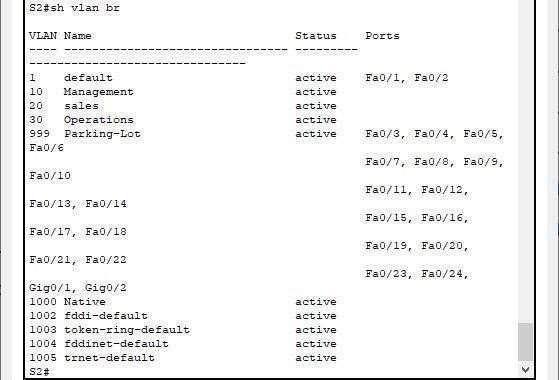
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

S2(config-if-range)#end S2#

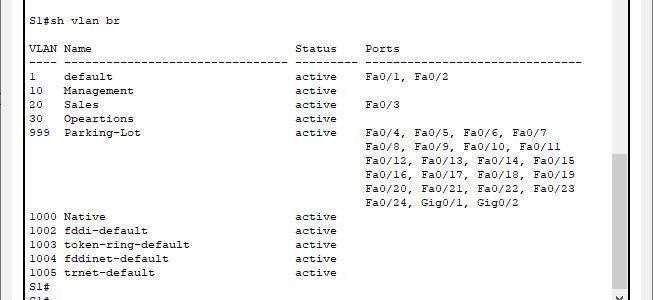


**Assign vlan 20 to f0/3on S1**

S1>en S1#conf t

S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20 S1(config-if)#exit

S1(config)#end S1#

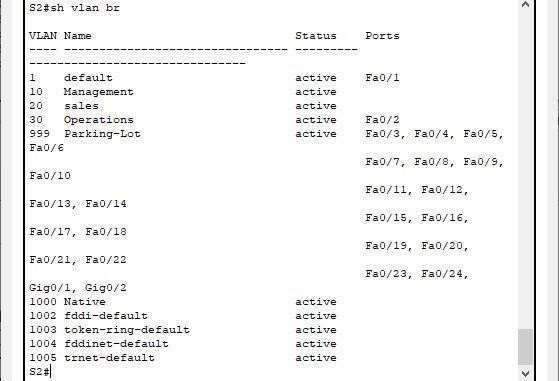


**Assign VLAN 30 to f0/2 on S2**

S2#en S2#conf t

Enter configuration commands, one per line. End with CNTL/Z. S2(config)#int f0/2

S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30 S2(config-if)#exit

S2(config)#end S2#

**S1 to S2 connection and vice-versa**

S1#en S1#conft

Enter configuration commands, one per line. End with CNTL/Z. S1(config)#int f0/2

S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk allowed vlan 10,20,30,1000 S1(config-if)#exit

S1(config)#end

**OUTPUT:**

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up S2#conf t

S2(config)#int f0/1

S2(config-if)#switchport mode trunk

S2(config-if)#switchport trunk Native vlan 1000 S2(config-if)#switchport trunk allowed vlan 10,20,30,1000 S2(config-if)#exit

S2(config)#end

**Configure R1** Router>en Router#conf t

Router(config)#int f0/0.10 Router(config-subif)#description vlan 10

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip add 192.168.10.1 255.255.255.0 Router(config-subif)#exit

Router(config)#int f0/0.20 Router(config-subif)#description vlan 20

Router(config-subif)#encapsulation dot1q 20

Router(config-subif)#ip add 192.168.20.1 255.255.255.0 Router(config-subif)#exit

Router(config)#int f0/0.30 Router(config-subif)#description vlan 30

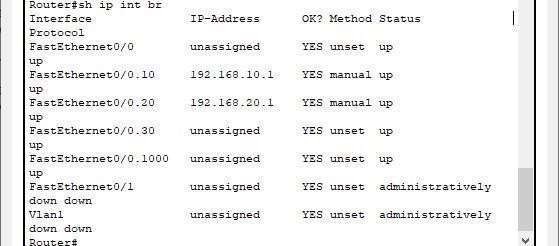
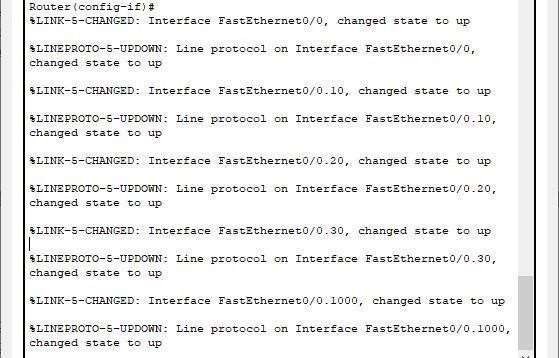
Router(config-subif)#ip add 192.168.30.1 255.255.255.0 Router(config-subif)#exit

Router(config)#int f0/0.1000 Router(config-subif)#description NATIVE

Router(config-subif)#encapsulation dot1q 1000 native Router(config-subif)#exit

Router(config)#int f0/0 Router(config-if)#no shutdown

Router(config-if)#exit Router(config)#end



**Practical No : 8 A**

**Aim: Configuring MPLS (On GNS3).**

****

**Configure router R1:-**

R1#conf t R1(config)#int se1/0

R1(config-if)#ip add 192.168.13.1 255.255.255.0

R1(config-if)#no shut R1(config-if)#exit R1(config)#int se1/2

R1(config-if)#ip add 192.168.12.1 255.255.255.0

R1(config-if)#no shut R1(config-if)#exit

**Configure router R2** R2#conf t R2(config)#int se1/2

R2(config-if)#ip add 192.168.12.2 255.255.255.0

R2(config-if)#no shut R2(config-if)#exit R2(config)#int se1/3

R2(config-if)#ip add 192.168.23.1 255.255.255.0

R2(config-if)#no shut R2(config-if)#exit

**Configure Router R3** R3#conf t R3(config)#int se1/0

R3(config-if)#ip add 192.168.13.2 255.255.255.0

R3(config-if)#no shut R3(config-if)#exit R3(config)#int se1/3

R3(config-if)#ip add 192.168.23.2 255.255.255.0

R3(config-if)#no shut R3(config-if)#exit

**Configure OSPF on R1** R1#conf t R1(config)#router ospf 1

R1(config-router)#network 192.168.12.0 255.255.255.0 area 0

R1(config-router)#network 192.168.13.0 255.255.255.0 area 0 R1(config-router)#end

**Configure OSPF on R2** R2#conf t R2(config)#router ospf 1

R2(config-router)#network 192.168.12.0 255.255.255.0 area 0

R2(config-router)#network 192.168.23.0 255.255.255.0 area 0 R2(config-router)#end

**Configure OSPF on R3** R3#conf t R3(config)#router ospf 1

R3(config-router)#network 192.168.13.0 255.255.255.0 area 0

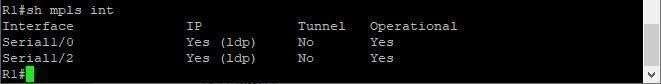
R3(config-router)#network 192.168.13.0 255.255.255.0 area 0

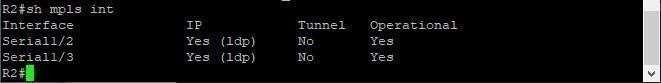
R3(config-router)#network 192.168.23.0 255.255.255.0 area 0 R3(config-router)#end

**Enable MPLS on R1** R1#conf t R1(config)#int se1/0 R1(config-if)#mpls ip R1(config-if)#int se1/2 R1(config-if)#mpls ip

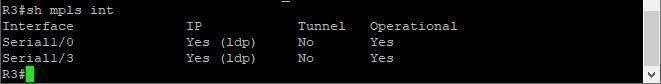
**Enable MPLS on R2** R2#conf t R2(config)#int se1/2 R2(config-if)#mpls ip R2(config-if)#int se1/3 R2(config-if)#mpls ip

**Enable MPLS on R3** R3#conf t R3(config)#int se1/0 R3(config-if)#mpls ip R3(config-if)#int se1/3 R3(config-if)#mpls ip

**Check MPLS interface**

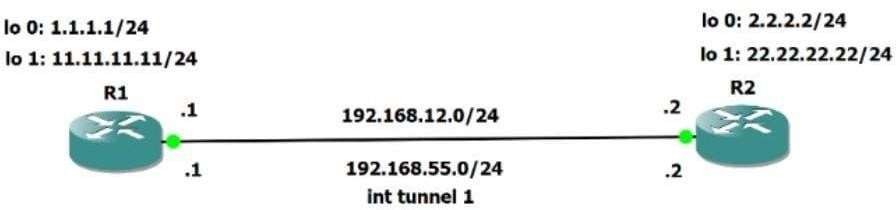
**Check MPLS interface**

**Check MPLS interface**



# Practical 8B

**Aim: Implement VRF**

****

**Configure R1/Dahanu:**

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z. R1(config)#hostname R1

R1(config)#int fa0/0

R1(config-if)#ip add 192.168.12.1 255.255.255.0

R1(config-if)#no shut R1(config-if)#exit

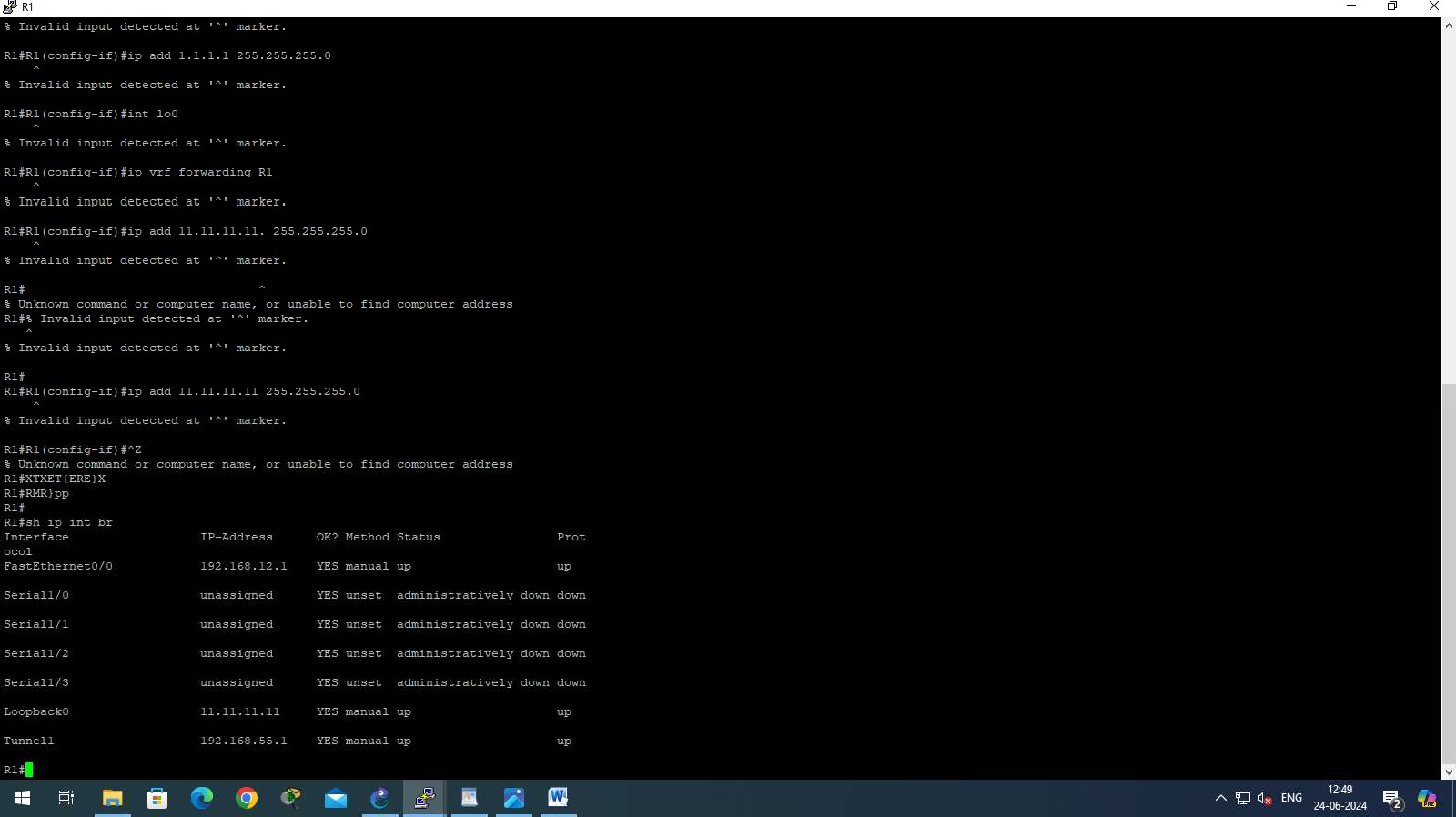
\*Jun 24 11:39:17.951: %ENTITY\_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Administrative State Down

\*Jun 24 11:39:18.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1(config-if)#exit R1(config)#ip vrf R1 R1(config-vrf)#exit R1(config)#int lo0 R1(config-if)#int lo0

R1(config-if)#ip vrf forwarding R1 R1(config-if)#ip add 1.1.1.1 255.255.255.0 R1(config-if)#int lo0

R1(config-if)#ip vrf forwarding R1

R1(config-if)#ip add 11.11.11.11 255.255.255.0 R1(config-if)#^Z

# Configure R2/Virar:

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z. R2(config)#hostname R2

R2(config)#int fa0/0

R2(config-if)#ip add 192.168.12.2 255.255.255.0

R2(config-if)#no shut

R2(config-if)#

\*Jun 24 11:41:01.651: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up R2(config-if)#

\*Jun 24 11:41:01.651: %ENTITY\_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Administrative State Down

\*Jun 24 11:41:02.651: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R2(config-if)#exit R2(config)#ip vrf R2 R2(config-vrf)#exit R2(config)#int lo0 R2(config-if)#ip

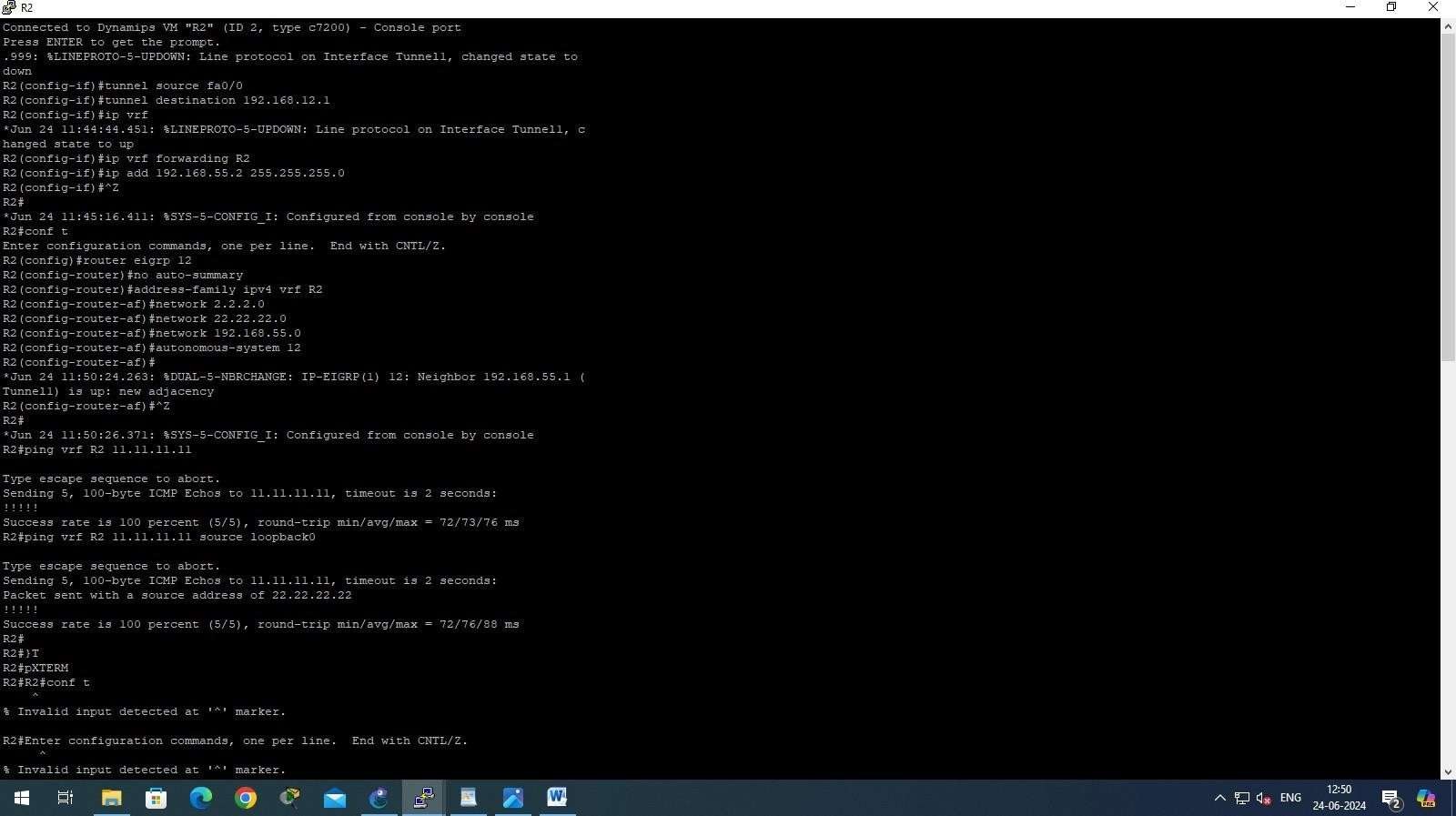
\*Jun 24 11:41:26.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip vrf forwarding R2 R2(config-if)#ip add 2.2.2.2 255.255.255.0 R2(config-if)#int lo0

R2(config-if)#int lo0

R2(config-if)#ip vrf forwarding R2

R2(config-if)#ip add 22.22.22.22 255.255.255.0 R2(config-if)#^Z



**Configure VRF on R1/Dahanu:**

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z. R1(config)#int tunnel 1

R1(config-if)#t

\*Jun 24 11:44:54.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down

R1(config-if)#tunnel source fa0/0

R1(config-if)#tunnel destination 192.168.12.2 R1(config-if)#ip v

\*Jun 24 11:45:20.927: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up

R1(config-if)#ip vrf forwarding R1

R1(config-if)#ip add 192.168.55.1 255.255.255.0

R1(config-if)#^Z

**Configure VRF on R2/Virar:**

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z. R2(config)#int tunnel 1

R2(config-if)#tunnel source fa0/0

R2(config-if)#tunnel destination 192.168.12.1 R2(config-if)#ip vrf forwarding R2

R2(config-if)#ip add 192.168.55.2 255.255.255.0

R2(config-if)#^Z

**Configure VRF on R1/Dahanu:**

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router eigrp 12

R1(config-router)#no auto-summary R1(config-router)#address-family ipv4 vrf R1 R1(config-router-af)#network 1.1.1.0

R1(config-router-af)#network 11.11.11.0

R1(config-router-af)#network 192.168.55.0

R1(config-router-af)#autonomous-system 12 R1(config-router-af)#^Z

**Configure EIGRP on R2/Virar**

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z. R2(config)#router eigrp 12

R2(config-router)#no auto-summary R2(config-router)#address-family ipv4 vrf R2 R2(config-router-af)#network 2.2.2.0

R2(config-router-af)#network 22.22.22.0

R2(config-router-af)#network 192.168.55.0

R2(config-router-af)#autonomous-system 12 R2(config-router-af)#^Z

\*Jun 24 11:50:26.371: %SYS-5-CONFIG\_I: Configured from console by console

