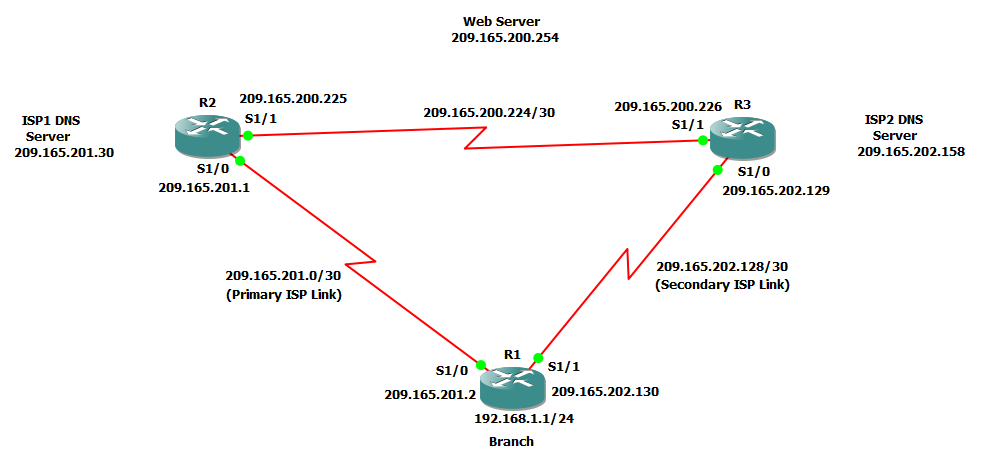
**Practical 1**

**Aim:- Configure IP SLA Tracking and Path Control**

**Topology:-**



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

a) Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear the previous configurations. Using the addressing scheme in the diagram, create the loopback interfaces and apply IP addresses to them as well as the serial interfaces on R1, ISP1, and ISP2.

**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

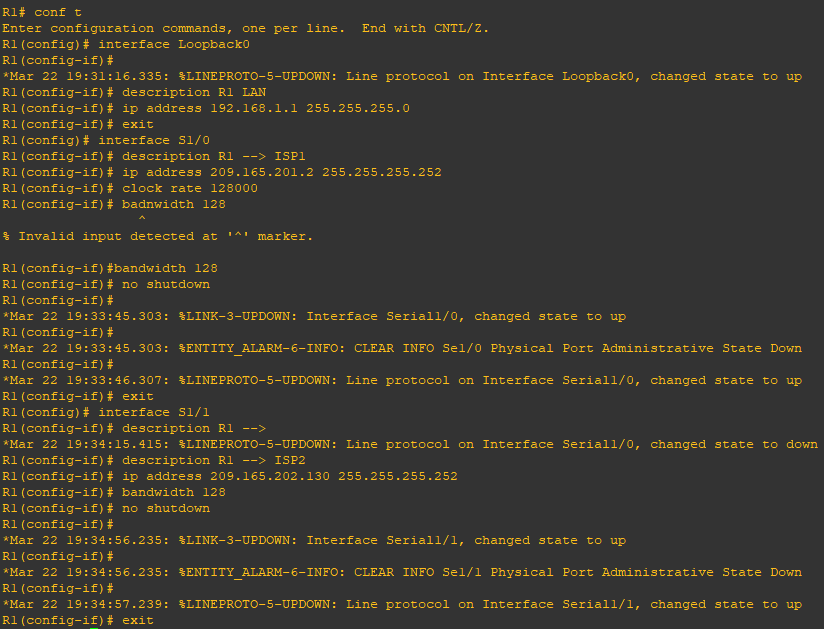
description R1 🡪 ISP2

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

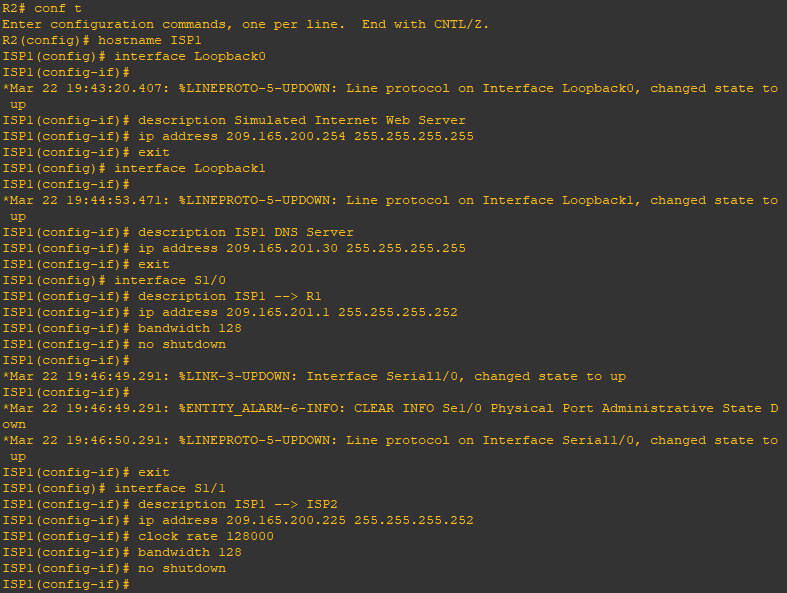
ip address 209.165.200.225 255.255.255.252

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

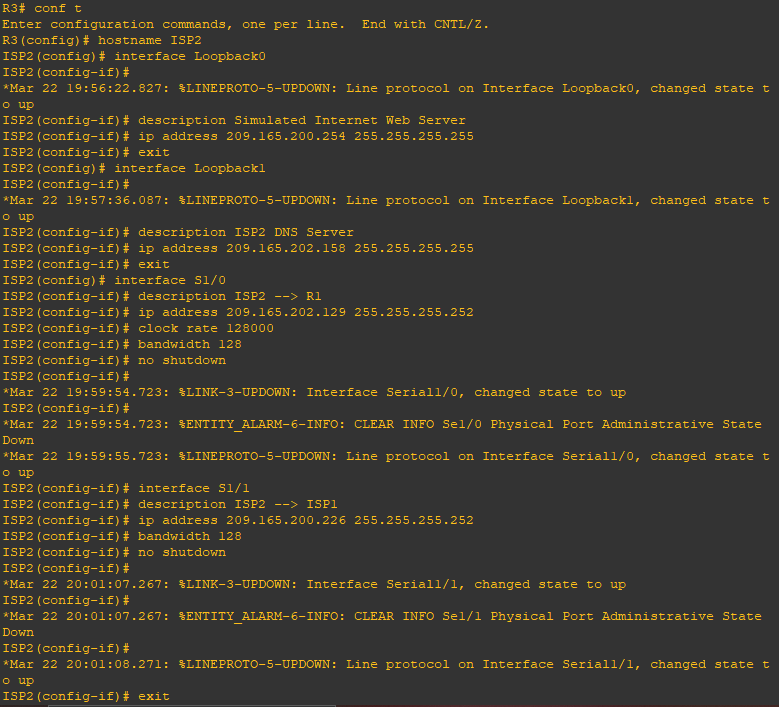
description ISP2 🡪 ISP1

ip address 209.165.200.226 255.255.255.252

bandwidth 128

no shutdown

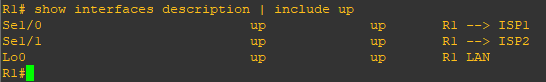
exit



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



All three interfaces should be active. Troubleshoot if necessary.

**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.

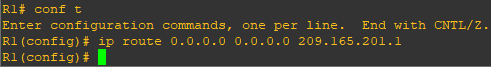
2) ISP1 and ISP2 have dynamic routing enabled between them, advertising their respective public address pools.

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

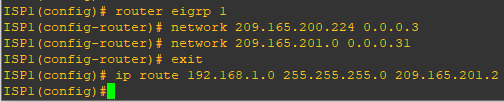
network 209.165.200.224 0.0.0.3

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

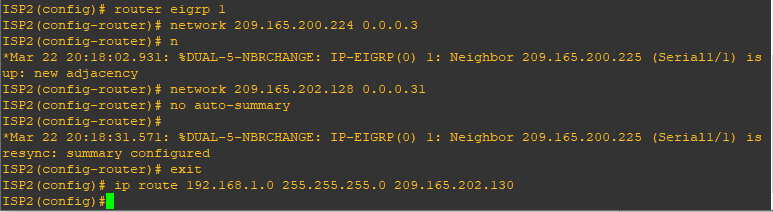
network 209.165.200.224 0.0.0.3

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. IP SLA probes continuously check the reachability of a specific destination, such as a provider edge router interface, the DNS server of the ISP, or any other specific destination, and can conditionally announce a default route only if the connectivity is verified.

Before implementing the Cisco IOS SLA feature, you must verify reachability to the Internet servers. From router R1, ping the web server, ISP1 DNS server, and ISP2 DNS server to verify connectivity.

**Router R1 Console**

tclsh

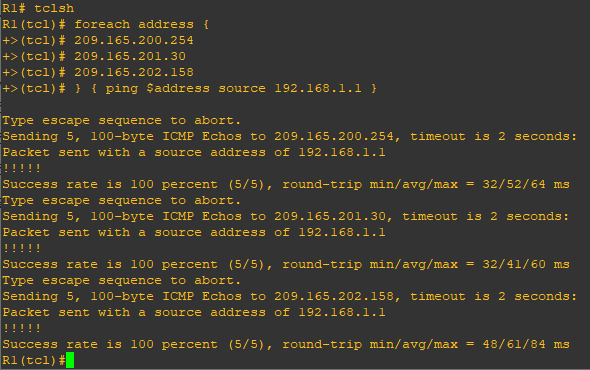
foreach address {

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

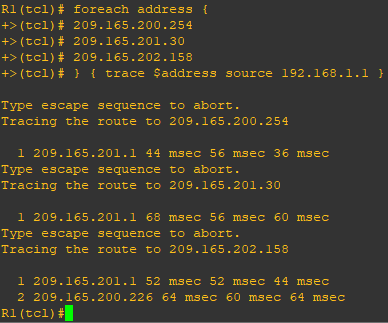
foreach address {

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.**

When the reachability tests are successful, you can configure the Cisco IOS IP SLAs probes. Different types of probes can be created, including FTP, HTTP, and jitter probes.

In this scenario, you will configure ICMP echo probes.

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

**Router R1 Console**

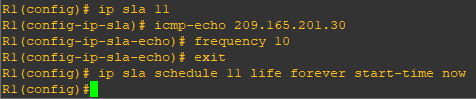
ip sla 11

icmp-echo 209.165.201.30

frequency 10

exit

ip sla schedule 11 life forever start-time now

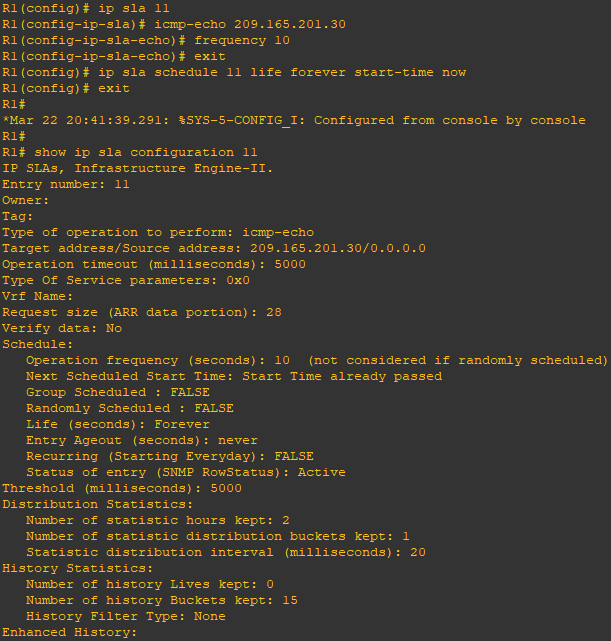


The operation number of 11 is only locally significant to the router. The **frequency 10** command schedules the connectivity test to repeat every 10 seconds. The probe is scheduled to start now and to run forever.

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



The output lists the details of the configuration of operation 11. The operation is an ICMP echo to 209.165.201.30, with a frequency of 10 seconds, and it has already started (the start time has already passed).

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



You can see that operation 11 has already succeeded five times, has had no failures, and the last operation returned an OK result.

d) Although not actually required because IP SLA session 11 alone could provide the desired fault tolerance, create a second probe, 22, to test connectivity to the second DNS server located on router ISP2.

**Router R1 Console**

ip sla 22

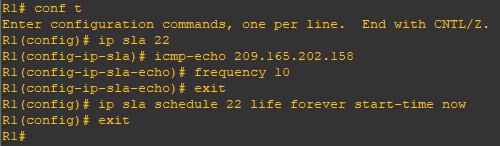
icmp-echo 209.165.202.158

frequency 10

exit

ip sla schedule 22 life forever start-time now

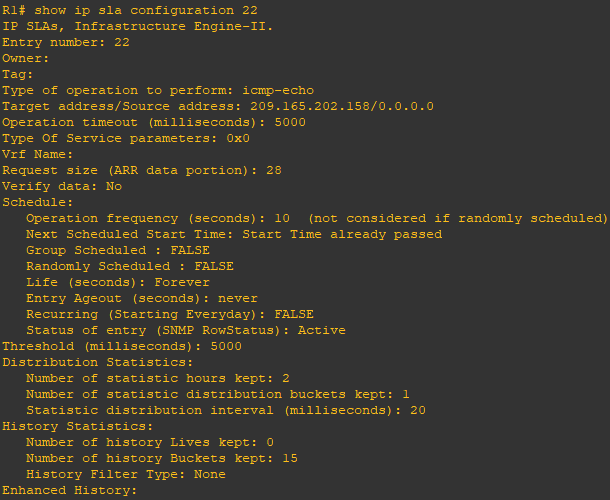
exit



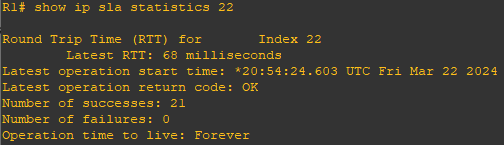
e) Verify the new probe using the **show ip sla configuration** and **show ip sla statistics** commands.

**Router R1 Console**

show ip sla configuration 22



show ip sla statistics 22



The output lists the details of the configuration of operation 22. The operation is an ICMP echo to 209.165.202.158, with a frequency of 10 seconds, and it has already started (the start time has already passed). The statistics also prove that operation 22 is active.

**Step 4:- Configure tracking options.**

Although PBR could be used, you will configure a floating static route that appears or disappears depending on the success or failure of the IP SLA.

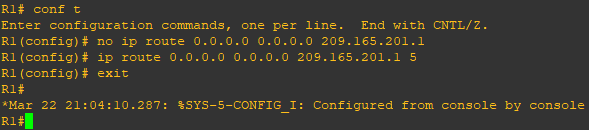
a) On R1, remove the current default route and replace it with a floating static route having an administrative distance of 5.

**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

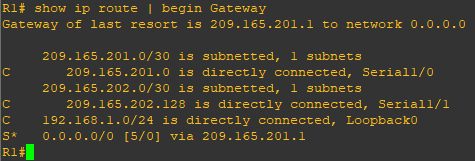
exit



b) Verify the routing table.

**Router R1 Console**

show ip route | begin Gateway



Notice that the default static route is now using the route with the administrative distance of 5. The first tracking object is tied to IP SLA object 11.

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

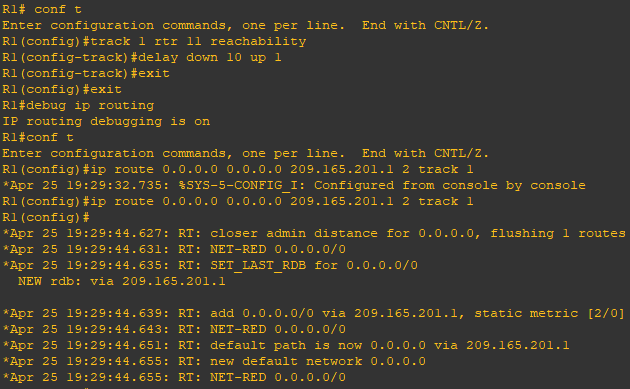
exit

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

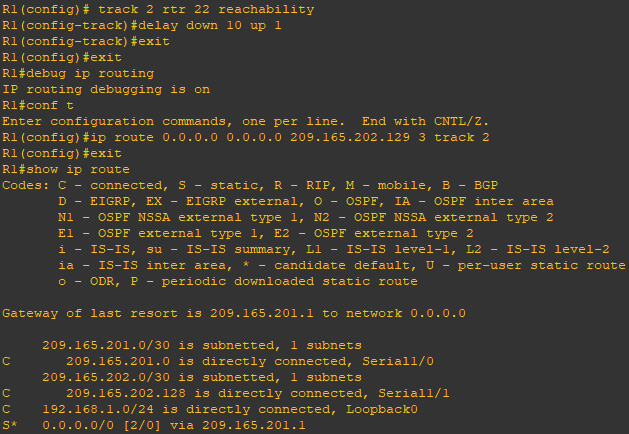
debug ip routing

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)**

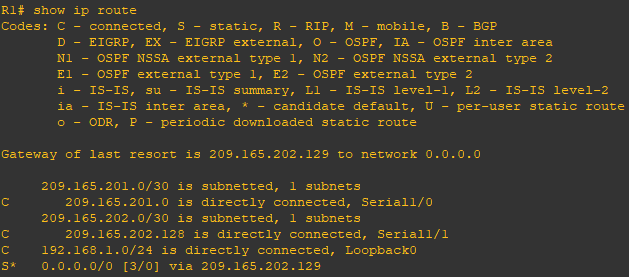
conf t

interface loopback 1

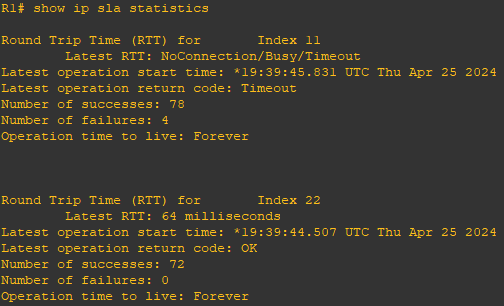
shutdown

**Router R1 Console**

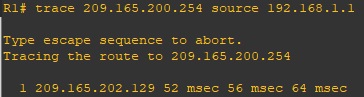
show ip route



show ip sla statistics



trace 209.165.200.254 source 192.168.1.1

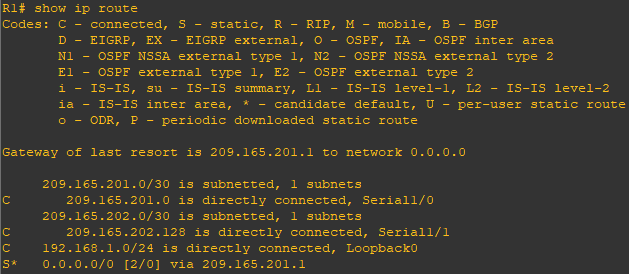


**Router R2 Console (hostname ISP1)**

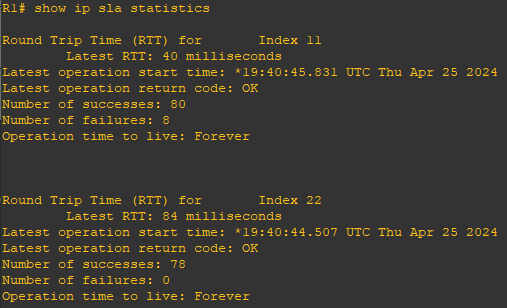
no shutdown

**Router R1 Console**

show ip route



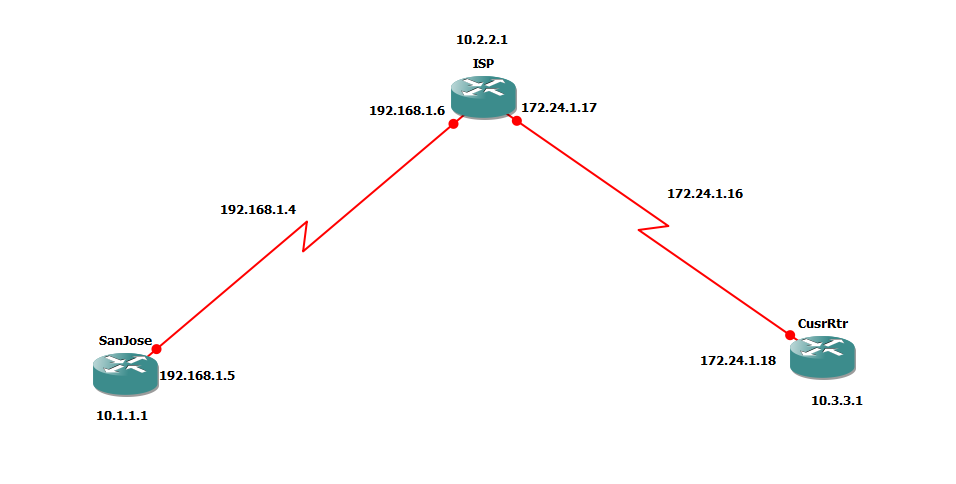
show ip sla statistics



**Practical 2**

**Aim:- Using the AS\_PATH Attribute**

**Topology:-**



**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 the hostname and interface addresses.**

a) Enter the following configurations into your routers to begin.

**Router R1 (hostname SanJose)**

hostname SanJose

interface Loopback0

ip address 10.1.1.1 255.255.255.0

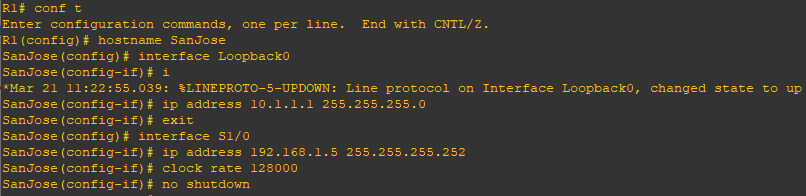
exit

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

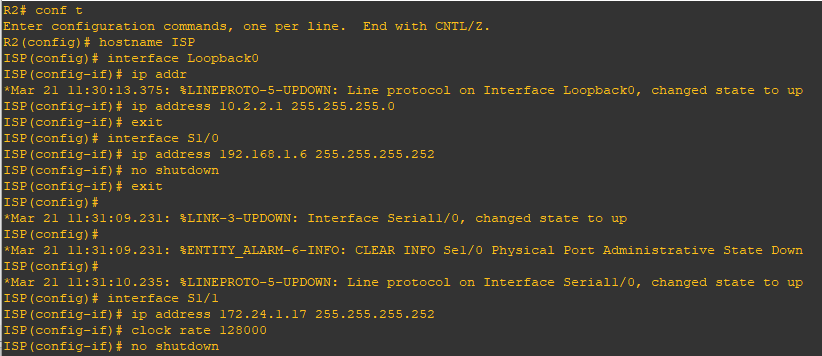
exit

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

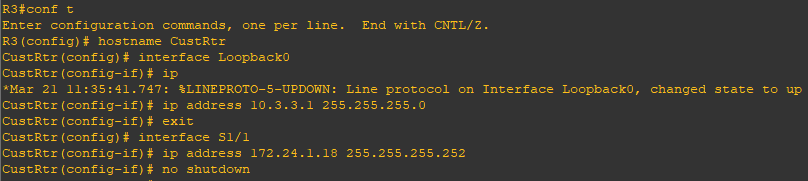
ip address 10.3.3.1 255.255.255.0

exit

interface S1/1

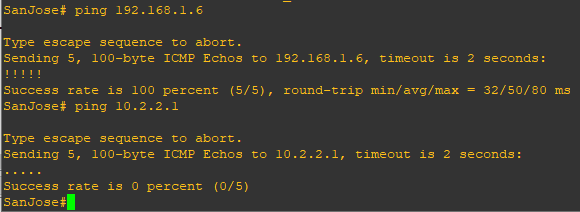
ip address 172.24.1.18 255.255.255.252

no shutdown



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

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



**Step 3:- Configure BGP**

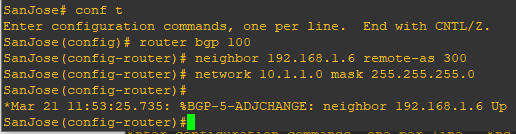
a) Configure BGP for normal operation. Enter the appropriate BGP commands on each router so that they identify their BGP neighbors and advertise their loopback networks.

**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



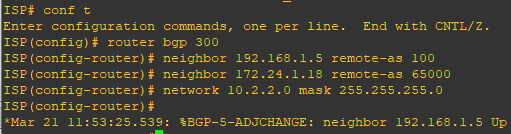
**Router R2 (hostname ISP)**

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

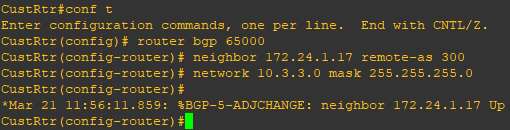


**Router R3 (hostname CustRtr)**

router bgp 65000

neighbor 172.24.1.17 remote-as 300

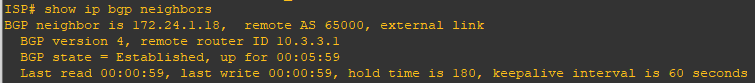
network 10.3.3.0 mask 255.255.255.0

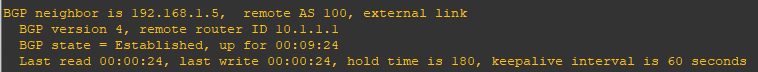


b) Verify that these routers have established the appropriate neighbor relationships by issuing the **show ip bgp neighbors** command on each router.

**Router R2 (hostname ISP)**

show ip bgp neighbors



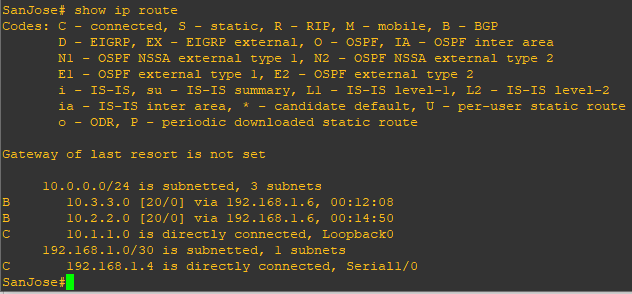


**Step 4:- Remove the private AS.**

a) 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. Troubleshoot if necessary.

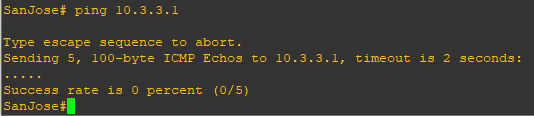
**Router R1 (hostname SanJose)**

show ip route



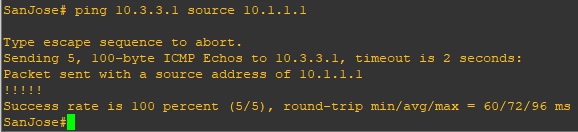
b) Ping the 10.3.3.1 address from the SanJose.

ping 10.3.3.1



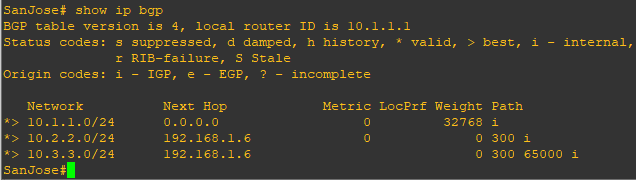
c) Ping again, this time as an extended ping, sourcing from the Loopback0 interface address.

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

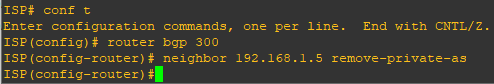


e) Configure ISP to strip the private AS numbers from BGP routes exchanged with SanJose using the following commands.

**Router R2 (hostname ISP)**

router bgp 300

neighbor 192.168.1.5 remove-private-as

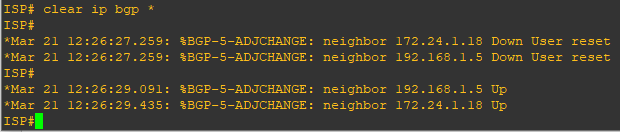


f) After issuing these commands, use the **clear ip bgp \*** command on ISP to re-establish the BGP relationship between the three routers. Wait several seconds and then return to SanJose to check its routing table.

Note:- The **clear ip bgp \* soft** command can also be used to force each router to resend its BGP table.

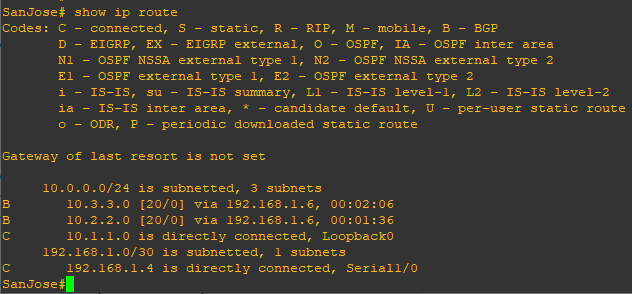
**Router R2 (hostname ISP)**

clear ip bgp \*



**Router R1 (hostname SanJose)**

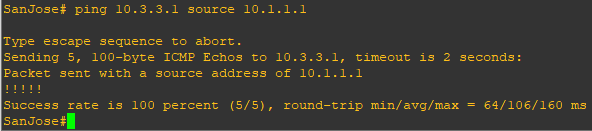
show ip route



SanJose should be able to ping 10.3.3.1 using its loopback0 interface as the source of the ping.

**Router R1 (hostname SanJose)**

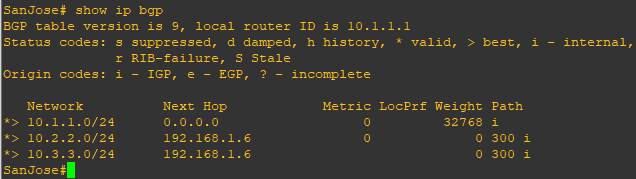
ping 10.3.3.1 source 10.1.1.1



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

**Router R1 (hostname SanJose)**

show ip bgp



**Step 5:- Use the AS\_PATH attribute to filter routes.**

As a final configuration, use the AS\_PATH attribute to filter routes based on their origin. In a complex environment, you can use this attribute to enforce routing policy. In this case, the provider router, ISP, must be configured so that it does not propagate routes that originate from AS 100 to the customer router CustRtr.

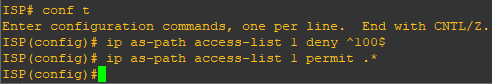
AS-path access lists are read like regular access lists. The statements are read sequentially, and there is an implicit deny at the end. Rather than matching an address in each statement like a conventional access list, AS path access lists match on something called a regular expression. Regular expressions are a way of matching text patterns and have many uses. In this case, you will be using them in the AS path access list to match text patterns in AS paths.

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

**Router R2 (hostname ISP)**

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

ip as-path access-list 1 permit .\*



The first command uses the ^ character to indicate that 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 sourced 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) stands 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.

b) Apply the configured access list using the neighbor command with **filter-list** option.

**Router R2 (hostname ISP)**

router bgp 300

neighbor 172.24.1.18 filter-list 1 out



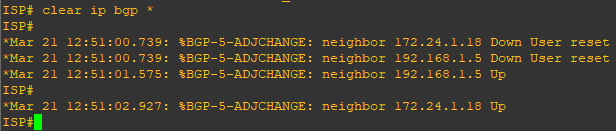
The **out** keyword specifies that the list is applied to routing information sent to this neighbor.

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.

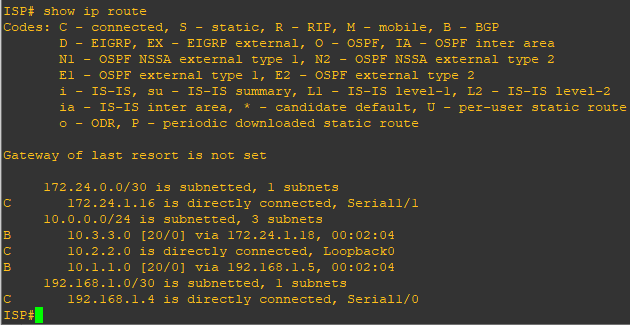
Note:- To force the local router to resend its BGP table, a less disruptive option is to use the **clear ip bgp \* out** or **clear ip bgp \* soft** command (the second command performs both outgoing and incoming route resync).

**Router R2 (hostname ISP)**

clear ip bgp \*



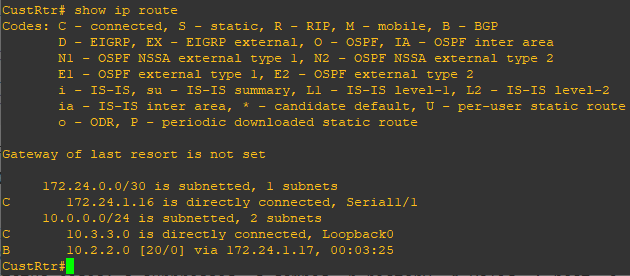
show ip route



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

**Router R3 (hostname CustRtr)**

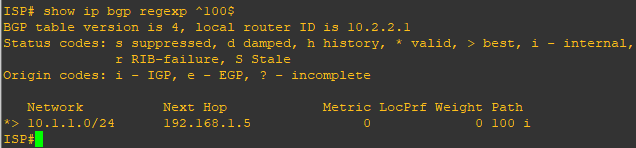
show ip route



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

**Router R2 (hostname ISP)**

show ip bgp regexp ^100$



The output of this command shows all matches for the regular expressions 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.

f) Run the following Tcl script on all routers to verify whether there is connectivity. 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.

**Router R2 (hostname ISP)**

ISP# tclsh

ISP(tcl)# foreach address {

+> 10.1.1.1

+> 10.2.2.1

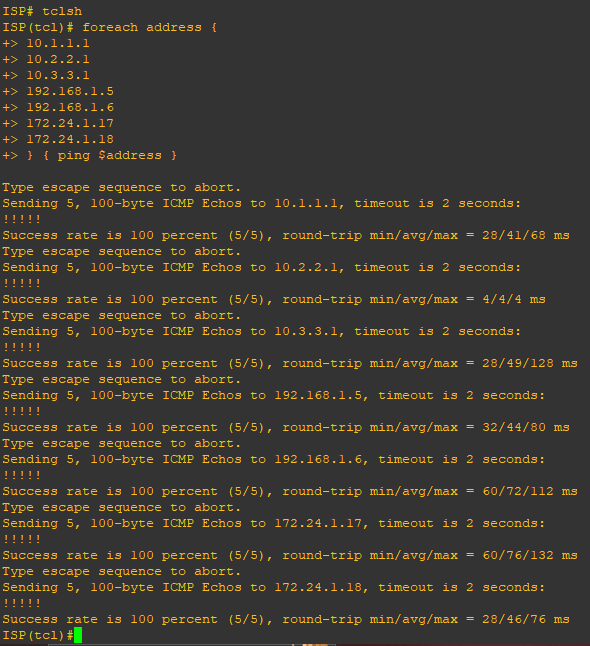
+> 10.3.3.1

+> 192.168.1.5

+> 192.168.1.6

+> 172.24.1.17

+> 172.24.1.18 } { ping $address }



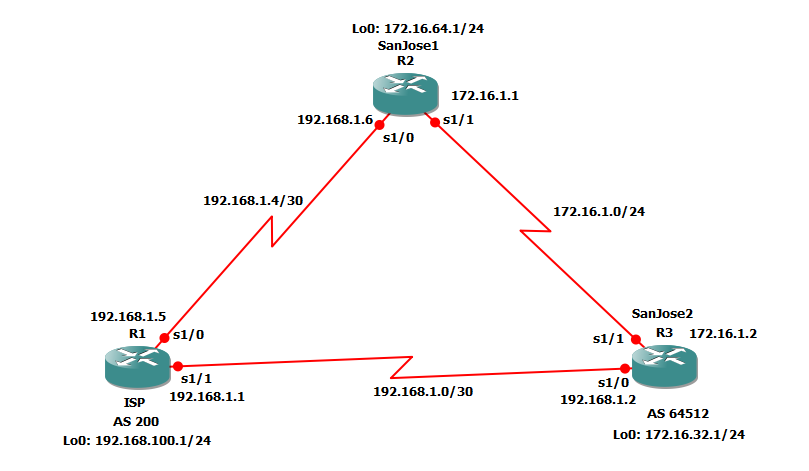
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Router Interface Summary** | | | | |
| **Router Model** | **Ethernet Interface #1** | **Ethernet Interface #2** | **Serial Interface #1** | **Serial Interface #2** |
| **1700** | Fast Ethernet 0 (FA0) | Fast Ethernet 1 (FA1) | Serial 0 (S0) | Serial 1 (S1) |
| **1800** | Fast Ethernet 0/0 (FA0/0) | Fast Ethernet 0/1 (FA0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **2600** | Fast Ethernet 0/0 (FA0/0) | Fast Ethernet 0/1 (FA0/1) | Serial 0/0 (S0/0) | Serial 0/1 (S0/1) |
| **2800** | Fast Ethernet 0/0 (FA0/0) | Fast Ethernet 0/1 (FA0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

Note:- To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. Rather than list all combinations of configurations for each router class, this table includes identifiers for the possible combinations of Ethernet and serial interfaces in the device. The table does not include any other type of interface, even though a specific router might contain one. For example, for an ISDN BRI interface, the string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

**Practical 3**

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

**Topology:-**



**Code:-**

**Step 1: Configure interface addresses.**

a) Using the addressing scheme in the diagram, create the loopback interfaces and apply IPv4

addresses to these and the serial interfaces on ISP (R1), SanJose1 (R2), and SanJose2 (R3).

Apply the following configuration to each router along with the appropriate hostname.

**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

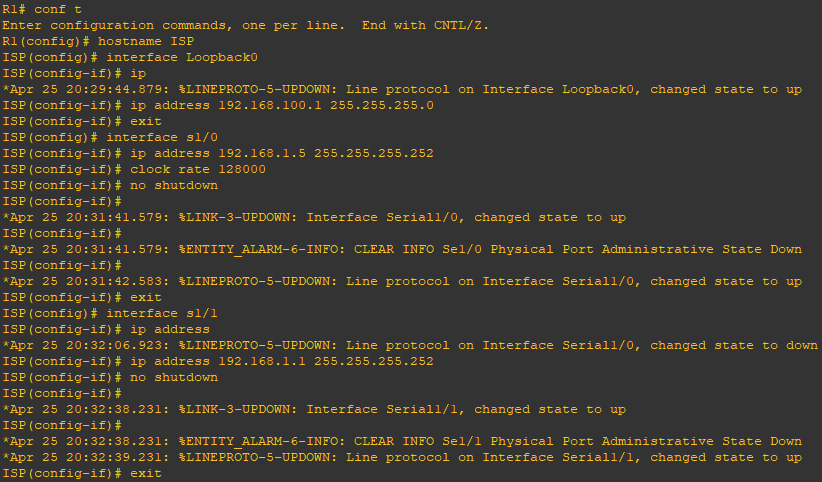
exit

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

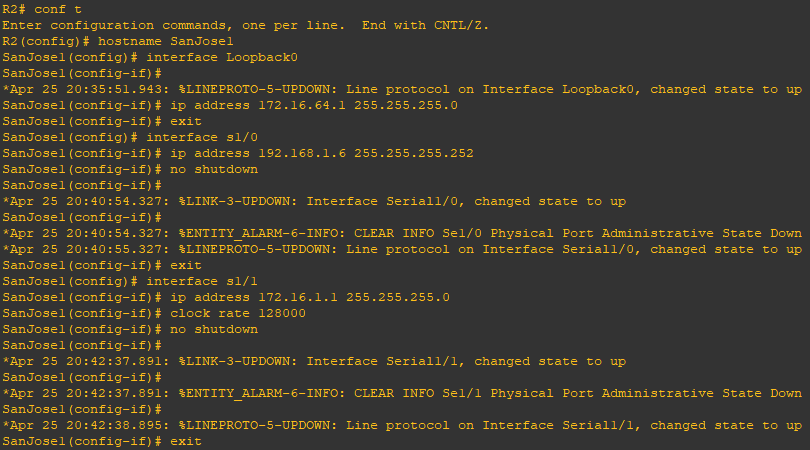
interface s1/1

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

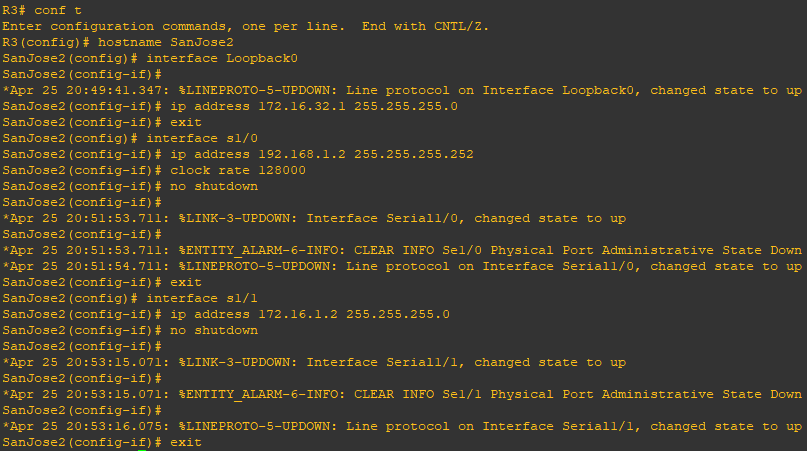
exit

interface s1/1

ip address 172.16.1.2 255.255.255.0

no shutdown

exit



**Step 2: Configure EIGRP.**

Configure EIGRP between the SanJose1 and SanJose2 routers. (Note: If using an IOS prior to

15.0, use the no auto-summary router configuration command to disable automatic

summarization. This command is the default beginning with IOS 15.)

**Router R2 Console (hostname SanJose1)**

router eigrp 1

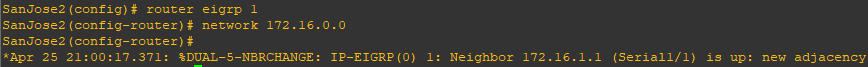
network 172.16.0.0



**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

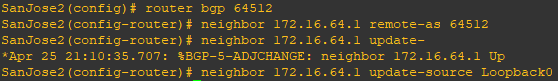


**Router R3 Console (hostname SanJose2)**

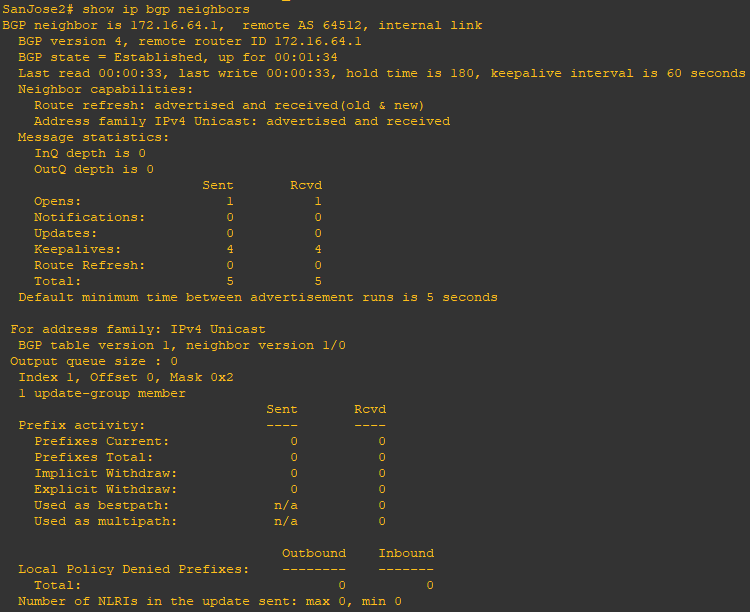
router bgp 64512

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.

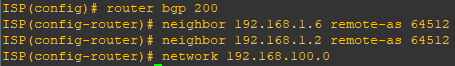
**Router R1 Console (hostname ISP)**

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. Any packets that do not

have a more specific match (longer match) for a 172.16.0.0 subnet will be dropped instead of

sent to the ISP. Later in this lab we will configure a default route to the ISP.

**Router R2 Console (hostname SanJose1)**

ip route 172.16.0.0 255.255.0.0 null0



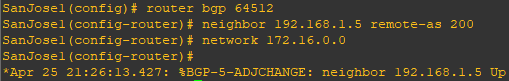
c) Configure SanJose1 as an EBGP peer to ISP.

**Router R2 Console (hostname SanJose1)**

router bgp 64512

neighbor 192.168.1.5 remote-as 200

network 172.16.0.0

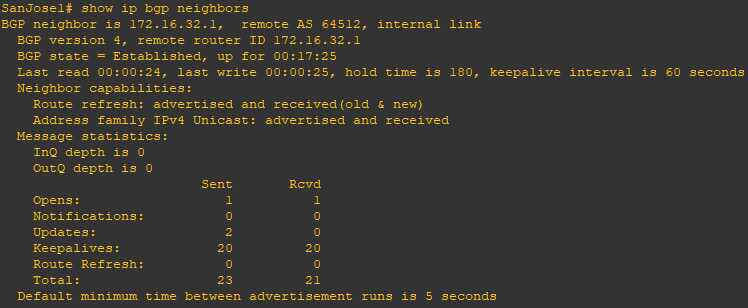


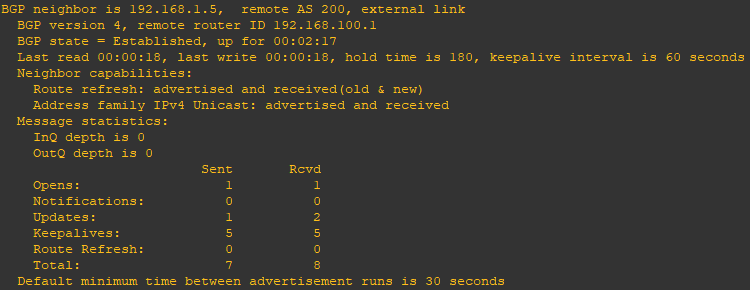
d) Use the show ip bgp neighbors command to verify that SanJose1 and ISP have reached the

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

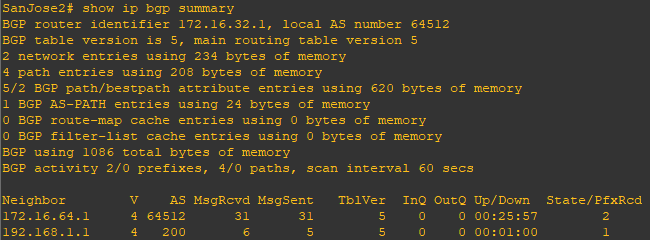
network 172.16.0.0



**Step 5: View BGP summary output.**

**Router R2 Console (hostname SanJose2)**

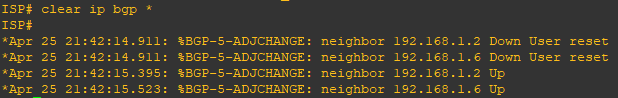
show ip bgp summary



**Step 6: Verify which path the traffic takes.**

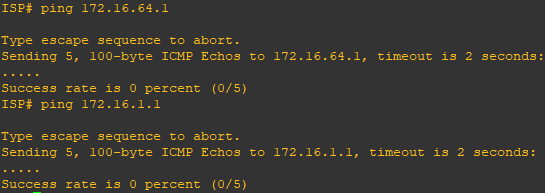
**Router R1 Console (hostname ISP)**

clear ip bgp \*



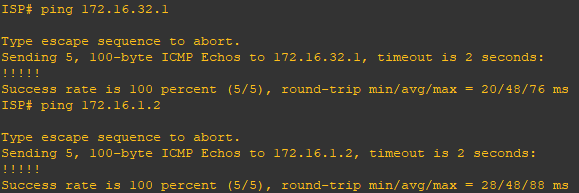
ping 172.16.64.1

ping 172.16.1.1

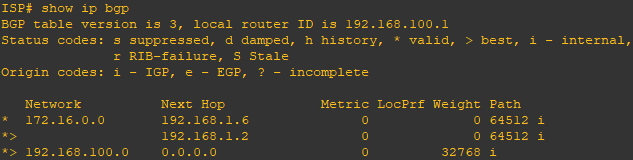


ping 172.16.32.1

ping 172.16.1.2



show ip bgp

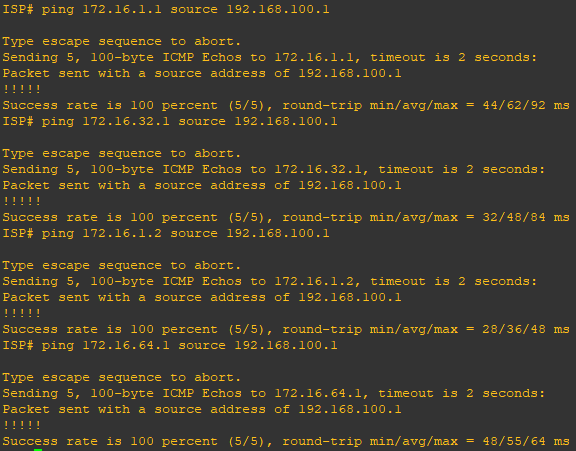


ping 172.16.1.1 source 192.168.100.1

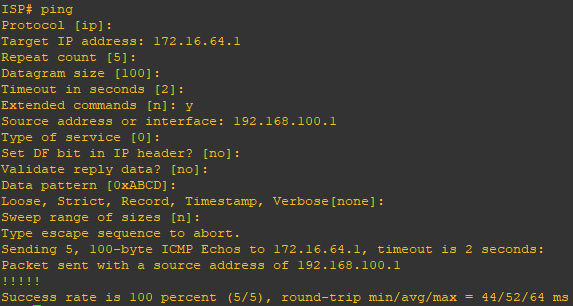
ping 172.16.32.1 source 192.168.100.1

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)**

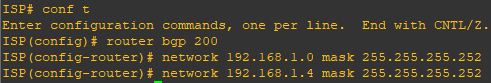
a) Issue the following commands on the ISP router.

router bgp 200

network 192.168.1.0 mask 255.255.255.252

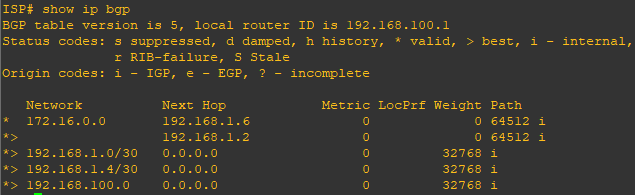
network 192.168.1.4 mask 255.255.255.252

end



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

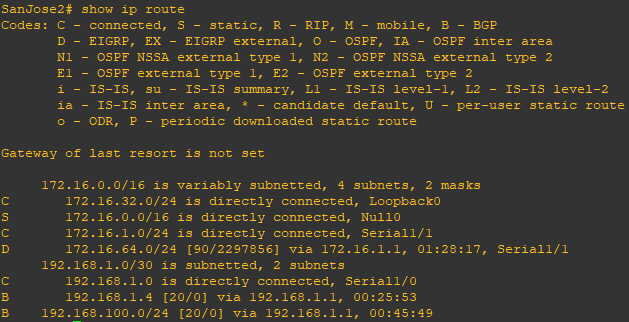
show ip bgp



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 we will remove ISP advertising its two WAN links and shutdown the WAN link between ISP and SanJose2. The only possible path from SanJose2 to ISP’s 192.168.100.0/24 is through SanJose1.

**Router R1 Console (hostname ISP)**

router bgp 200

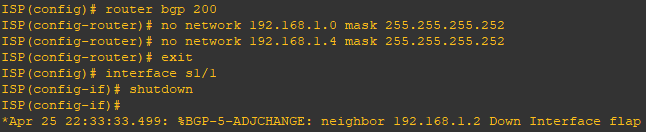
no network 192.168.1.0 mask 255.255.255.252

no network 192.168.1.4 mask 255.255.255.252

exit

interface s1/1

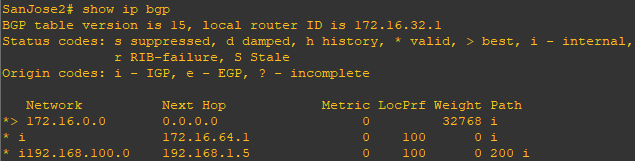
shutdown



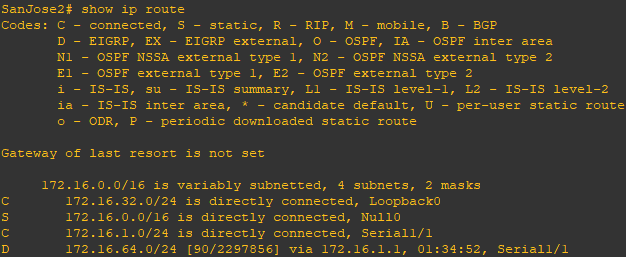
e) Display SanJose2’s BGP table using the show ip bgp command and the IPv4 routing table with show ip route.

**Router R3 Console (hostname SanJose2)**

show ip bgp



show ip route

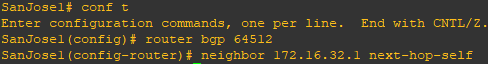


f) Issue the next-hop-self command on SanJose1 and SanJose2 to advertise themselves as the next hop to their IBGP peer.

**Router R2 Console (hostname SanJose1)**

router bgp 64512

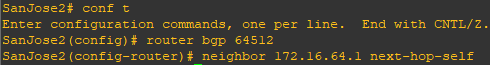
neighbor 172.16.32.1 next-hop-self



**Router R3 Console (hostname SanJose2)**

router bgp 64512

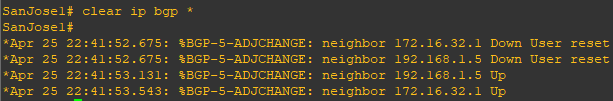
neighbor 172.16.64.1 next-hop-self



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

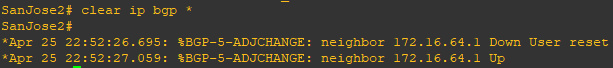
**Router R2 Console (hostname SanJose1)**

clear ip bgp \*



**Router R3 Console (hostname SanJose2)**

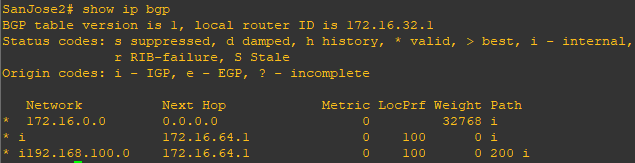
clear ip bgp \*



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)**

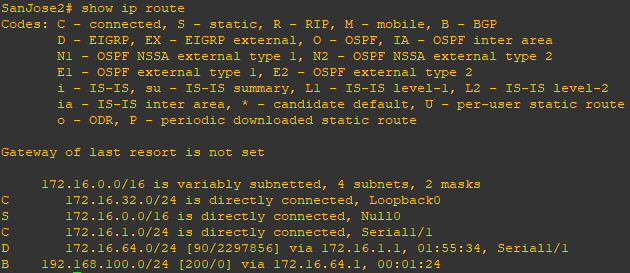
show ip bgp



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

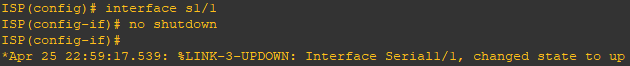


j) Before configuring the next BGP attribute, restore the WAN link between ISP and SanJose3. This will change the BGP table and routing table on both routers. For example, SanJose2’s routing table shows 192.168.100.0/24 will now have a better path through ISP.

**Router R1 Console (hostname ISP)**

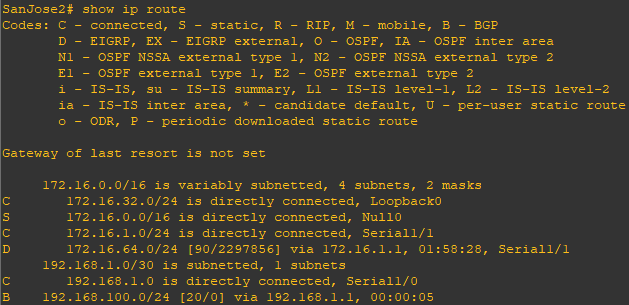
interface s1/1

no shutdown



**Router R3 Console (hostname SanJose2)**

show ip route



**Step 8: Set BGP local preference.**

At this point, everything looks good, with the exception of default routes, the outbound flow of data, and inbound packet flow.

a) Because the local preference value is shared between IBGP neighbors, configure a simple route map that references the local preference value on SanJose1 and SanJose2. This policy adjusts outbound traffic to prefer the link off the SanJose1 router instead of the metered T1 off SanJose2.

**Router R2 Console (hostname SanJose1)**

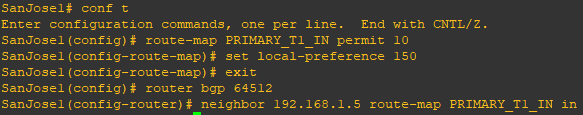
route-map PRIMARY\_T1\_IN permit 10

set local-preference 150

exit

router bgp 64512

neighbor 192.168.1.5 route-map PRIMARY\_T1\_IN in



**Router R3 Console (hostname SanJose2)**

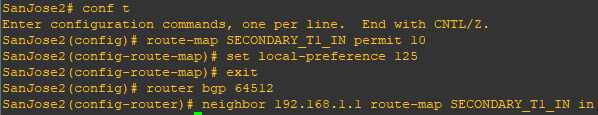
route-map SECONDARY\_T1\_IN permit 10

set local-preference 125

exit

router bgp 64512

neighbor 192.168.1.1 route-map SECONDARY\_T1\_IN in

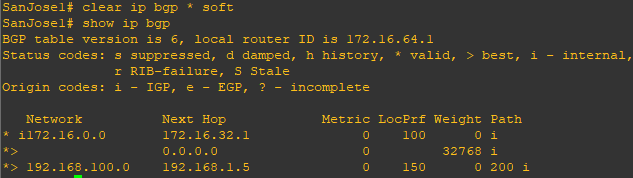


b) Use the clear ip bgp \* soft command after configuring this new policy. When the conversations have been reestablished, issue the show ip bgp command on SanJose1 and SanJose2.

**Router R2 Console (hostname SanJose1)**

clear ip bgp \* soft

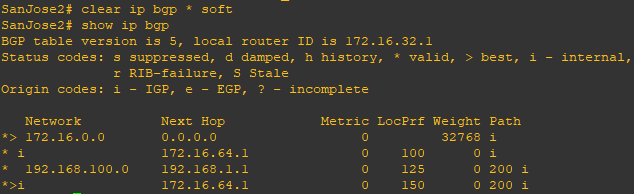
show ip bgp



**Router R3 Console (hostname SanJose2)**

clear ip bgp \* soft

show ip bgp

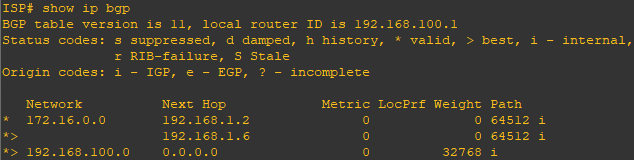


**Step 9: Set BGP MED.**

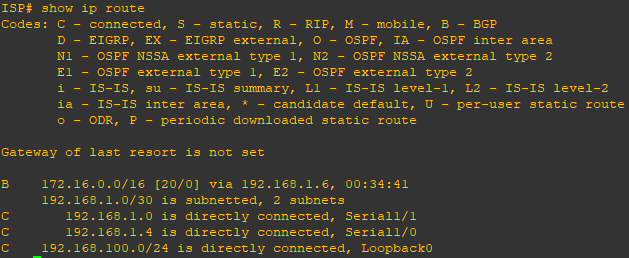
a) In the previous step we saw that SanJose1 and SanJose2 will route traffic for 192.168.100.0/24 using the link between SanJose1 and ISP. Examine what the return path ISP takes to reach AS 64512. Notice that the return path is different from the original path. This is known as asymmetric routing and is not necessarily an unwanted trait.

**Router R1 Console (hostname ISP)**

show ip bgp



show ip route

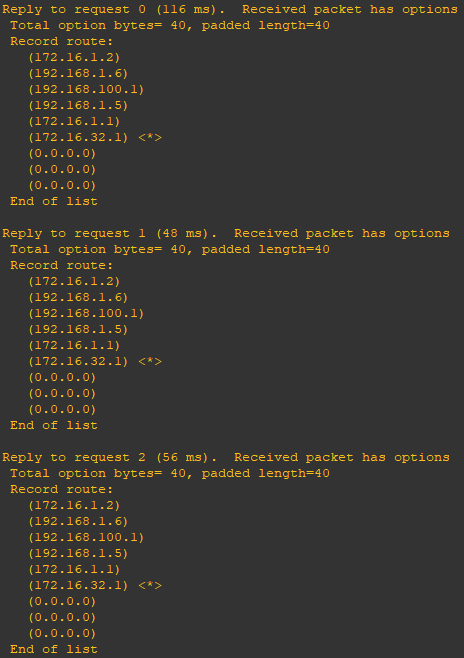


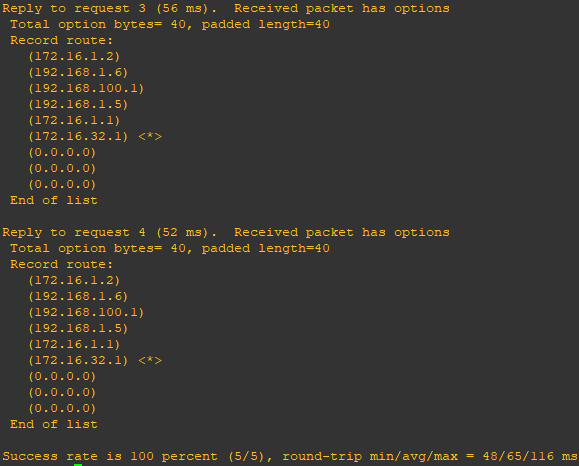
b) Use an extended ping command to verify this situation. Specify the record option and compare your output to the following. Notice the return path using the exit interface 192.168.1.1 to SanJose2.

**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)**

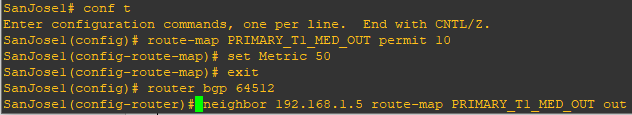
route-map PRIMARY\_T1\_MED\_OUT permit 10

set Metric 50

exit

router bgp 64512

neighbor 192.168.1.5 route-map PRIMARY\_TI\_MED\_OUT out



**Router R3 Console (hostname SanJose2)**

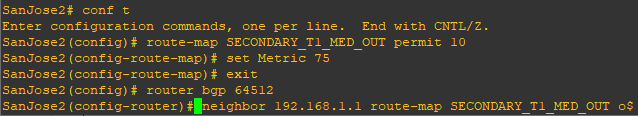
route-map SECONDARY\_T1\_MED\_OUT permit 10

set Metric 75

exit

router bgp 64512

neighbor 192.168.1.1 route-map SECONDARY\_T1\_MED\_OUT out

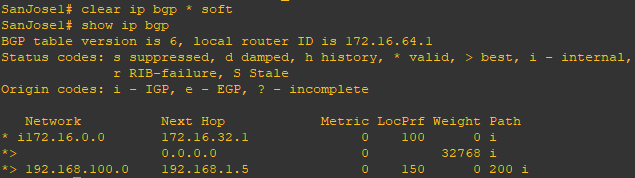


d) Use the clear ip bgp \* soft command after issuing this new policy. Issuing the show ip bgp command as follows on SanJose1 or SanJose2 does not indicate anything about this newly defined policy.

**Router R2 Console (hostname SanJose1)**

clear ip bgp \* soft

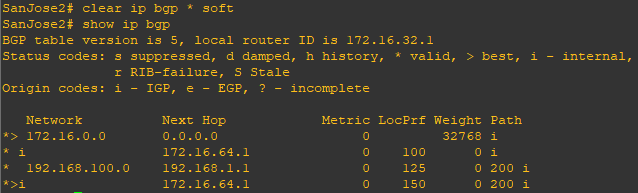
show ip bgp



**Router R3 Console (hostname SanJose2)**

clear ip bgp \* soft

show ip bgp

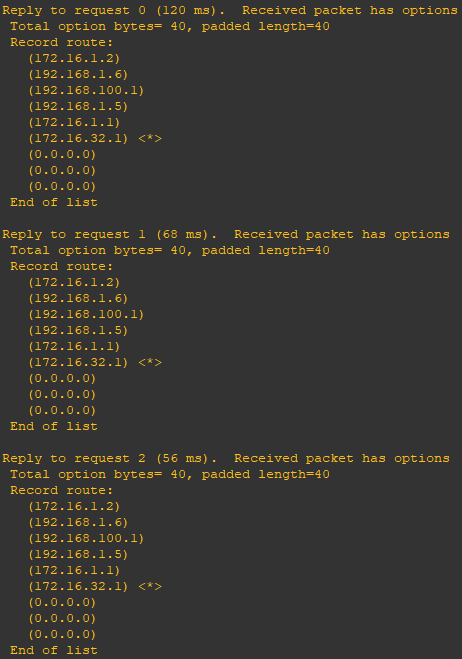


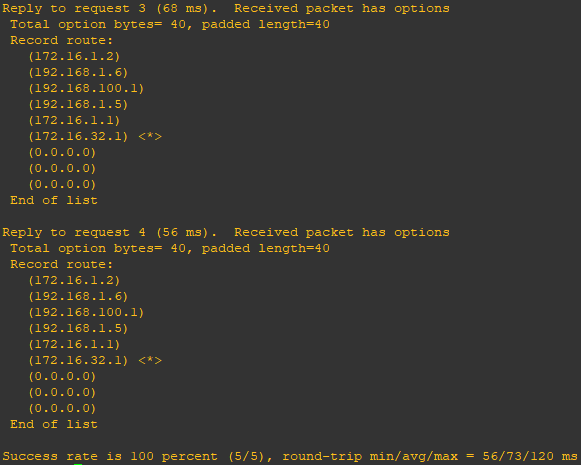
e) Reissue an extended ping command with the record command. Notice the change in return path using the exit interface 192.168.1.5 to SanJose1.

**Router R3 Console (hostname SanJose2)**

ping







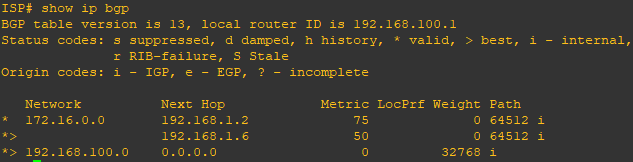
**Step 10: Establish a default route.**

The final step is to establish a default route that uses a policy statement that adjusts to changes in the network.

a) Configure ISP to inject a default route to both SanJose1 and SanJose2 using BGP using the default-originate command. This command does not require the presence of 0.0.0.0 in the ISP router. Configure the 10.0.0.0/8 network which will not be advertised using BGP. This network will be used to test the default route on SanJose1 and SanJose2.

**Router R1 Console (hostname ISP)**

show ip bgp



router bgp 200

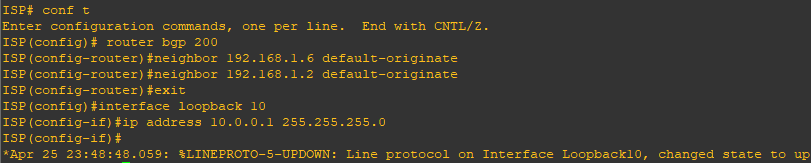
neighbor 192.168.1.6 default-originate

neighbor 192.168.1.2 default-originate

exit

interface loopback 10

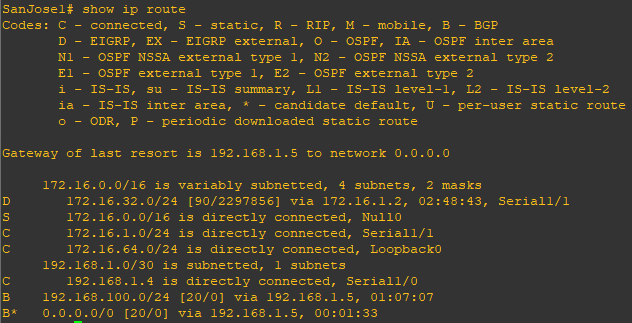
ip address 10.0.0.1 255.255.255.0



b) Verify that both routers have received the default route by examining the routing tables on SanJose1 and SanJose2. Notice that both routers prefer the route between SanJose1 and ISP.

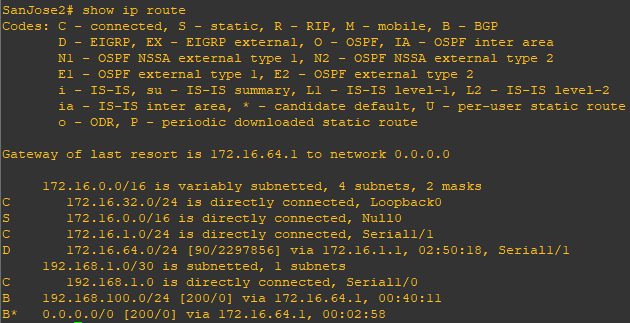
**Router R2 Console (hostname SanJose1)**

show ip route



**Router R3 Console (hostname SanJose2)**

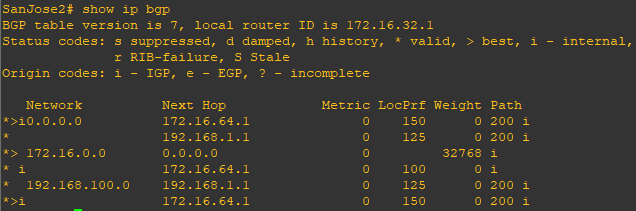
show ip route



c) The preferred default route is by way of SanJose1 because of the higher local preference attribute configured on SanJose1 earlier.

**Router R3 Console (hostname SanJose2)**

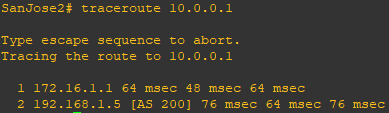
show ip bgp



d) Using the traceroute command verify that packets to 10.0.0.1 is using the default route through SanJose1.

**Router R3 Console (hostname SanJose2)**

traceroute 10.0.0.1

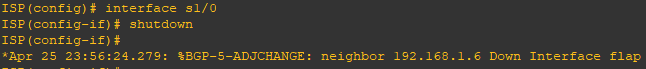


e) Next, test how BGP adapts to using a different default route when the path between SanJose1 and ISP goes down.

**Router R1 Console (hostname ISP)**

interface s1/0

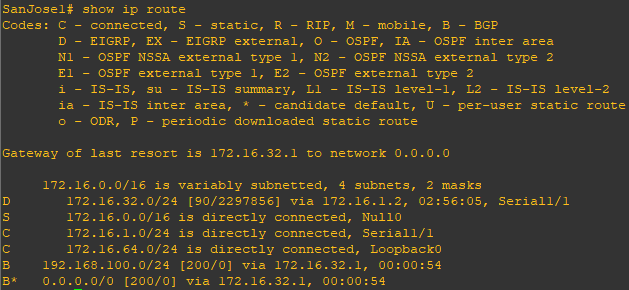
shutdown



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

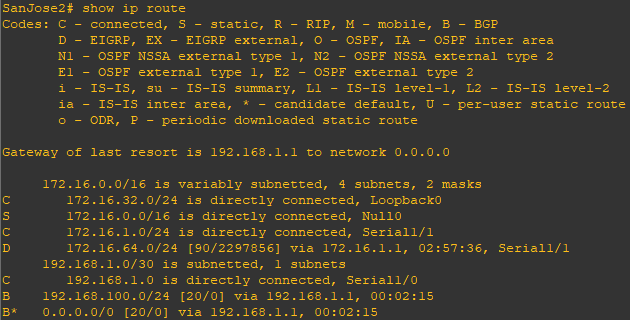
**Router R2 Console (hostname SanJose1)**

show ip route



**Router R3 Console (hostname SanJose2)**

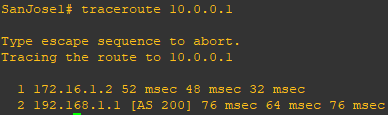
show ip route



g) Verify the new path using the traceroute command to 10.0.0.1 from SanJose1. Notice the default route is now through SanJose2.

**Router R2 Console (hostname SanJose1)**

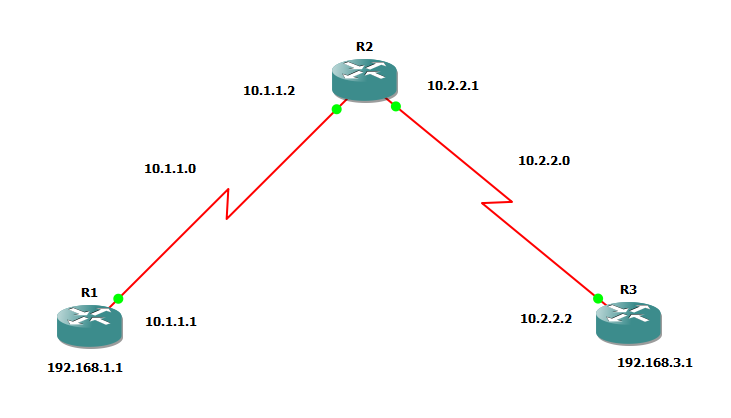
traceroute 10.0.0.1



**Practical 4**

**Aim:- Secure the Management Plane**

**Topology:-**



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

Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations. Using the addressing scheme in the diagram, apply the IP addresses to the interfaces on the R1, R2, and R3 routers.

**Router R1** **Console**

hostname R1

interface Loopback0

description R1 LAN

ip address 192.168.1.1 255.255.255.0

exit

interface S1/0

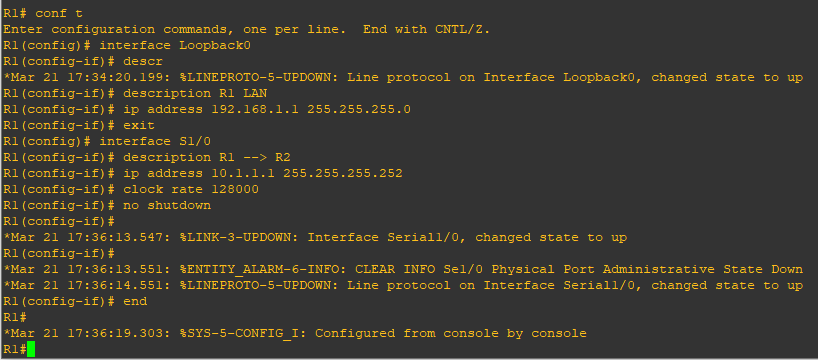
description R1 🡪 R2

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

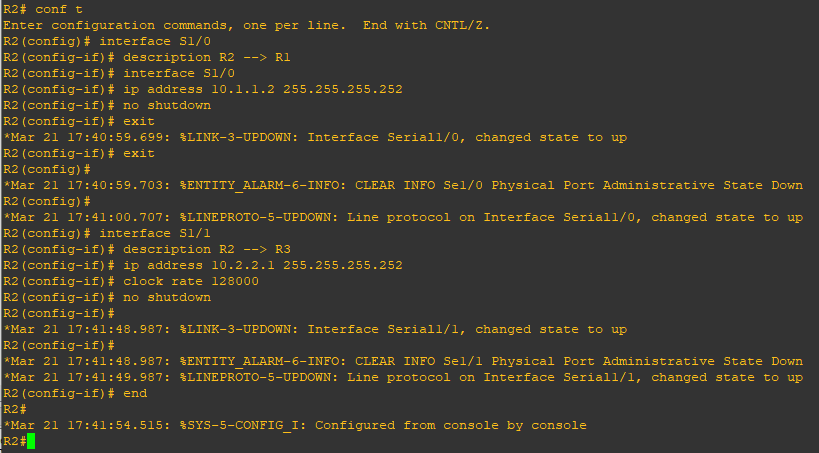
description R2 🡪 R3

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

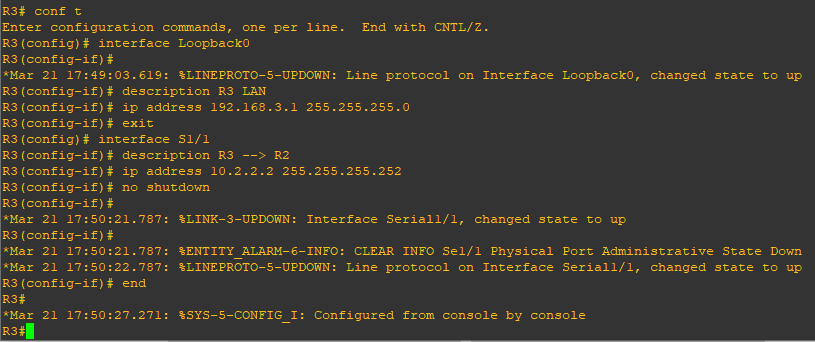
interface S1/1

description R3 🡪 R2

ip address 10.3.3.1 255.255.255.252

no shutdown

end

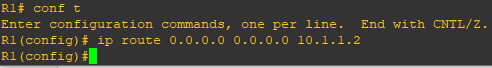


**Step 2:- Configure Static Routes.**

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

**Router R1 Console**

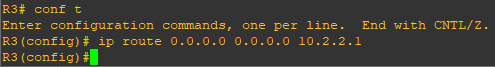
ip route 0.0.0.0 0.0.0.0 10.1.1.2



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

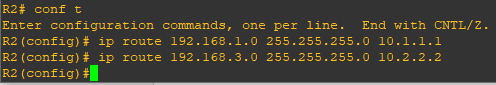


c) On R2, configure two static routes

**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

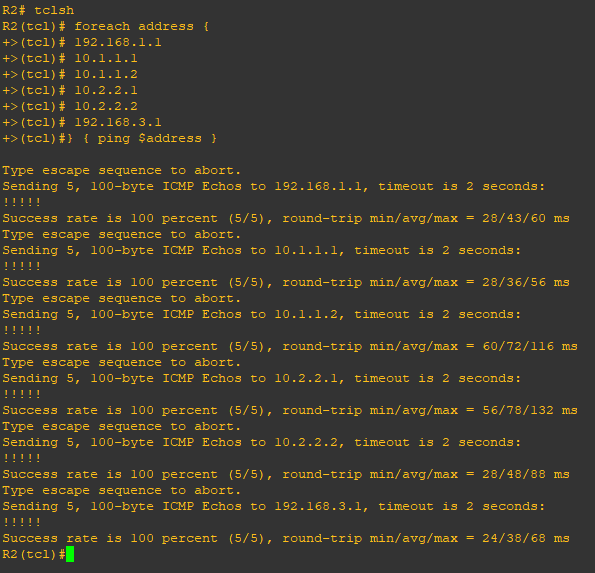
+> (tcl)# 10.1.1.2

+> (tcl)# 10.2.2.1

+> (tcl)# 10.2.2.2

+> (tcl)# 192.168.3.1

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



**Step 3:- Secure management access.**

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

**Router R1 Console**

security passwords min-length 10



b) Configure the enable secret encrypted password on both routers.

**Router R1 Console**

enable secret class12345



Note:- Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

c) Configure a console password and enable login for routers. For additional security, the **exec-timeout** 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. However, this is not considered a good security practice.

**Router R1 Console**

line console 0

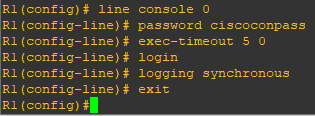
password ciscoconpass

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

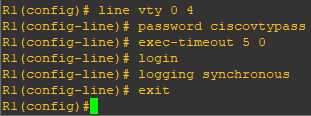
password ciscovtypass

exec-timeout 5 0

login

logging synchronous

exit



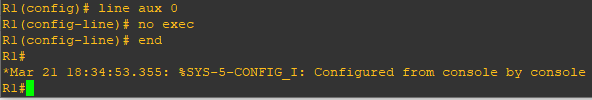
e) The aux port is a legacy port used to manage a router remotely using a modem and is hardly ever used. Therefore, disable the aux port.

**Router R1 Console**

line aux 0

no exec

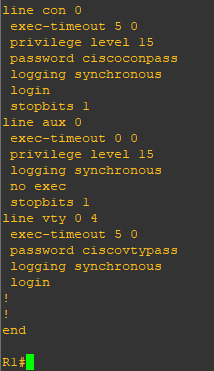
end



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

**Router R1 Console**

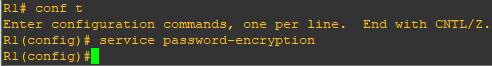
show run



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

**Router R1 Console**

service password-encryption

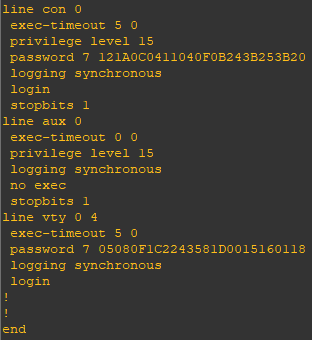


Note:- Password encryption is applied to all the passwords, including the username passwords, the authentication key passwords, the privileged command password, the console and the virtual terminal line access passwords, and the BGP neighbor passwords.

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

**Router R1 Console**

show run



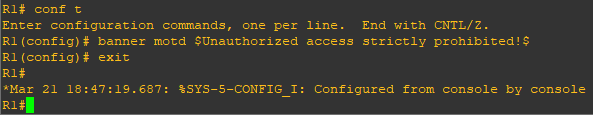
Note:- Type 7 passwords are encrypted using a Vigenère cipher which can be easily reversed. Therefore this command primarily protects from shoulder surfing attacks.

i) 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.

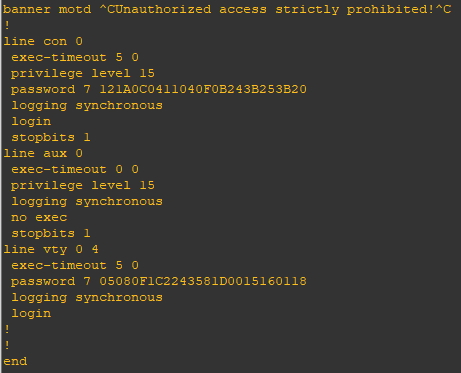
**Router R1 Console**

banner motd $Unauthorized access strictly prohibited!$

exit



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



k) Exit privileged EXEC mode using the **disable** or **exit** command and press **Enter** to get started. Does the MOTD banner look like what you created with the **banner motd** command? If the MOTD banner is not as you wanted it, recreate it using the **banner motd** command.

l) Repeat the configuration portion of steps 3a through 3k on router R3.

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

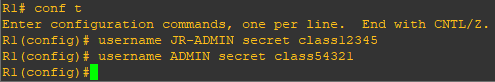
To increase the encryption level of console and VTY lines, it is recommended to enable authentication using the local database. The local database consists of usernames and password combinations that are created locally on each device. The local and VTY lines are configured to refer to the local database when authenticating a user.

a) 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:

**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.

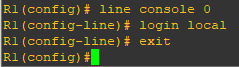
b) Set the console line to use the locally defined login accounts.

**Router R1 Console**

line console 0

login local

exit



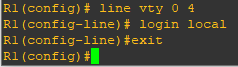
c) Set the vty lines to use the locally defined login accounts.

**Router R1 Console**

Line vty 0 4

login local

exit



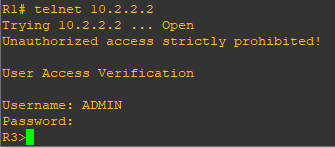
d) Repeat the steps 4a to 4c on R3.



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



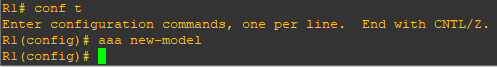
**Step 5:- Enabling AAA RADIUS Authentication with Local User for Backup.**

Authentication, authorization, and accounting (AAA) is a standards-based framework that can be implemented to control who is permitted to access a network (authenticate), what they can do on that network (authorize), and audit what they did while accessing the network (accounting).

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



Note:- Although the following configuration refers to two RADIUS servers, the actual RADIUS server implementation is beyond the scope. Therefore, the goal of this step is to provide an example of how to configure a router to access the servers.

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.

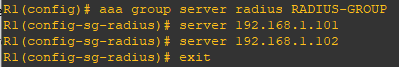
**Router R1 Console**

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



Note:- Unlike the local option that makes the password is case sensitive, local-case makes the username and password case sensitive.

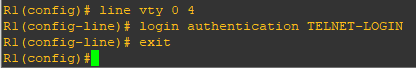
g) Alter the vty lines to use the TELNET-LOGIN AAA authentication method.

**Router R1 Console**

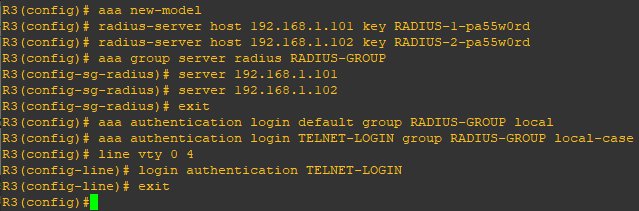
line vty 0 4

login authentication TELNET-LOGIN

exit



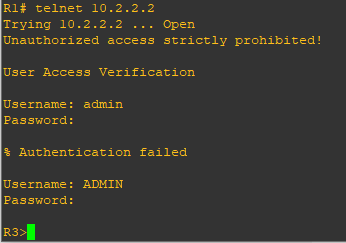
h) Repeat the steps 5a to 5g on R3.



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



Note:- The first login attempt did not use the correct username (i.e., ADMIN) which is why it failed.

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

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

Traditionally, remote access on routers was configured using Telnet on TCP port 23. However, Telnet was developed in the days when security was not an issue; therefore, all Telnet traffic is forwarded in plaintext.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals.

Note:- For a router to support SSH, it must be configured with local authentication, (AAA services, or username) or password authentication. In this task, you configure an SSH username and local authentication.

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

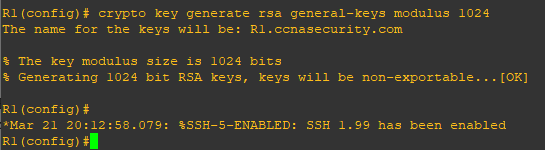
Note:- If no keys exist, you might receive this message: % No Signature RSA Keys found in configuration.



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).

The default setting for SSH is SSH version 1.99. This is also known as compatibility mode and is merely an indication that the server supports both SSH version 2 and SSH version 1. However, best practices are to enable version 2 only.

Configure SSH version 2 on R1.

**Router R1 Console**

ip ssh version 2



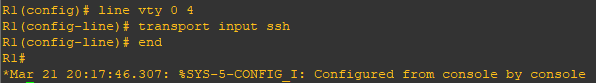
e) Configure the vty lines to use only SSH connections.

**Router R1 Console**

line vty 0 4

transport input ssh

end



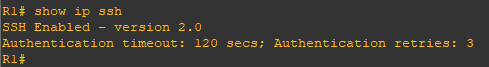
Note:- SSH requires that the **login local** command be configured. However, in the previous step we enabled AAA authentication using the TELNET-LOGIN authentication method, therefore **login local** is not necessary.

Note:- If you add the keyword **telnet** to the **transport input** command, users can log in using Telnet as well as SSH. However, the router will be less secure. If only SSH is specified, the connecting host must have an SSH client installed.

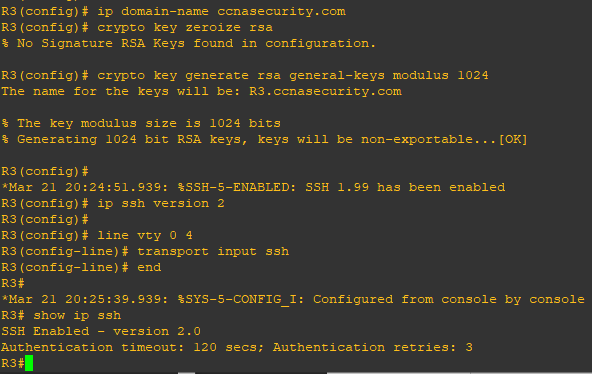
f) Verify the SSH configuration using the **show ip ssh** command.

**Router R1 Console**

show ip ssh



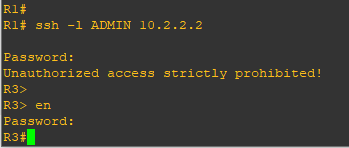
g) Repeat the steps from 6a to 6f on R3



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



**Practical 5**

**Aim:- Configure and Verify Path Control Using PBR**

**Topology:-**



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

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

b) Using the addressing scheme in the diagram, create the loopback interfaces and apply IP addresses to these and the serial interfaces on R1, R2, R3, and R4. On the serial interfaces connecting R1 to R3 and R3 to R4, specify the bandwidth as 64 Kb/s and set a clock rate on the DCE using the clock rate 64000 command. On the serial interfaces connecting R1 to R2 and R2 to R3, specify the bandwidth as 128 Kb/s and set a clock rate on the DCE using the clock rate 128000 command.

**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

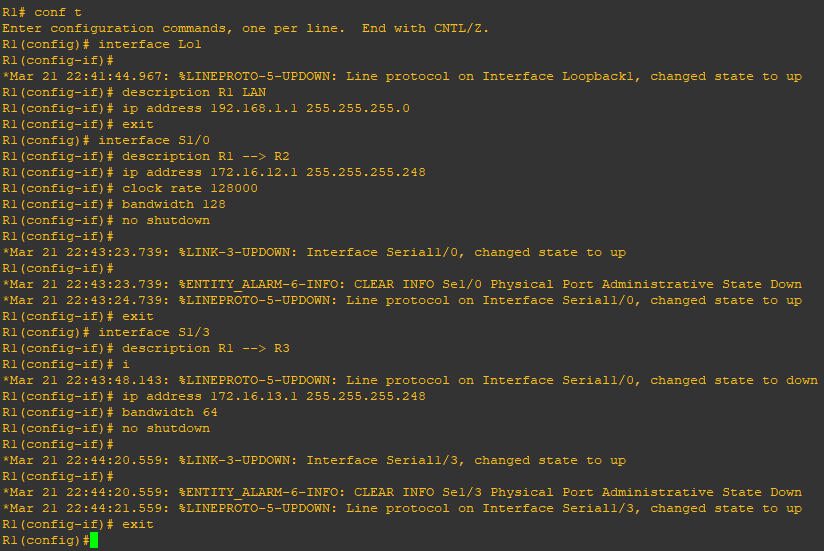
description R1 🡪 R3

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

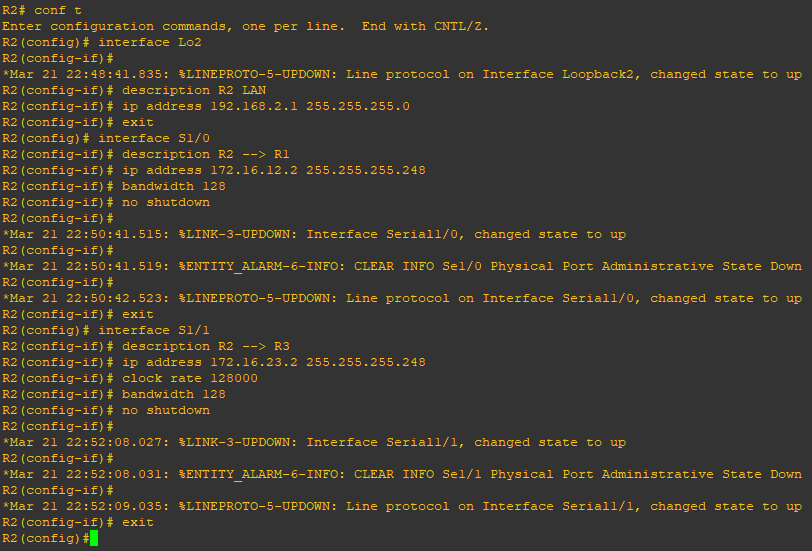
ip address 172.16.23.2 255.255.255.248

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

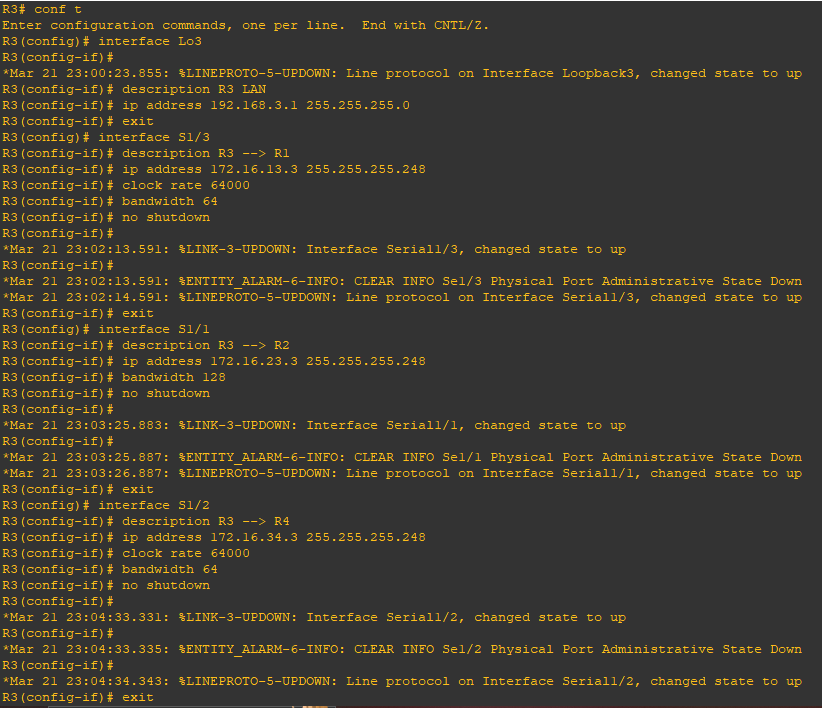
ip address 172.16.34.3 255.255.255.248

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

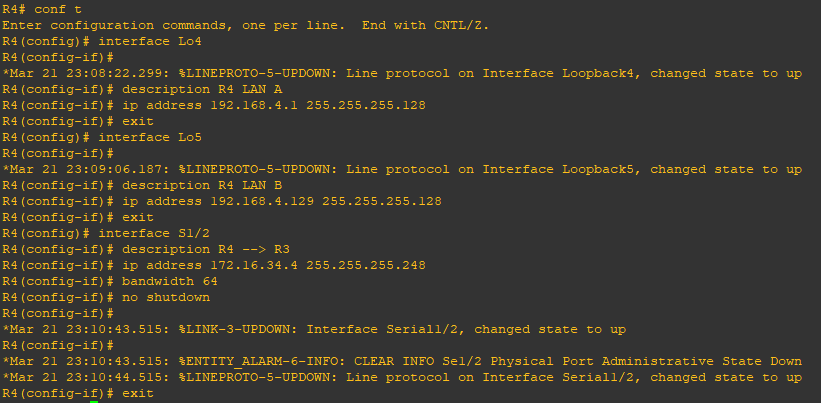
description R4 🡪 R3

ip address 172.16.34.4 255.255.255.248

bandwidth 64

no shutdown

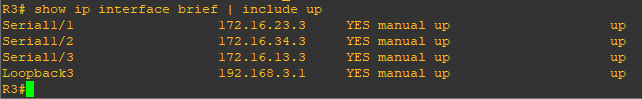
exit



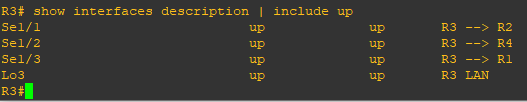
c) Verify the configuration with the **show ip interface brief**, **show** **interfaces description** commands. The output from router R3 is shown below.

**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.

b) Advertise networks 172.16.12.0/29, 172.16.13.0/29, 172.16.23.0/29, 172.16.34.0/29, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, and 192.168.4.0/24 from their respective routers.

**Router R1 Console**

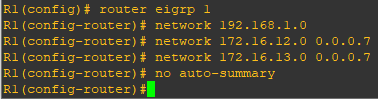
router eigrp 1

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**

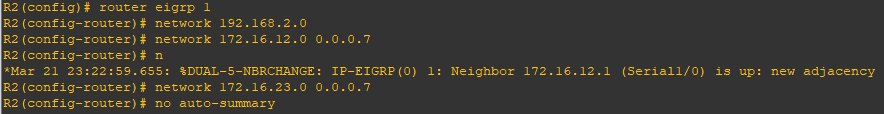
router eigrp 1

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

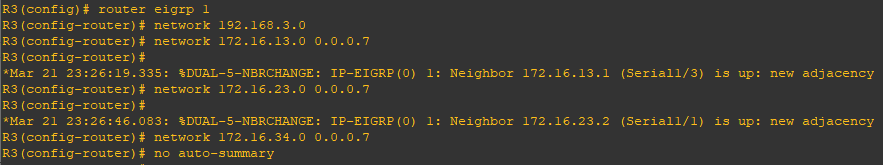
network 192.168.3.0

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



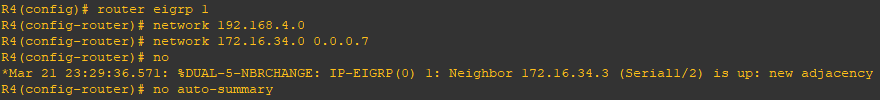
**Router R4 Console**

router eigrp 1

network 192.168.4.0

network 172.16.34.0 0.0.0.7

no auto-summary

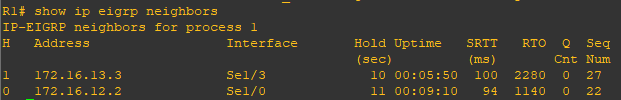


**Step 4:- Verify EIGRP connectivity.**

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



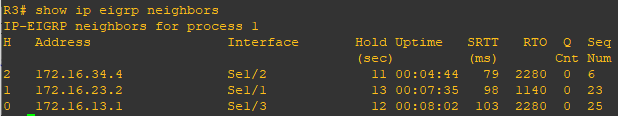
**Router R2 Console**

show ip eigrp neighbors



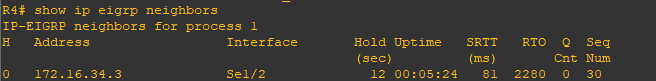
**Router R3 Console**

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

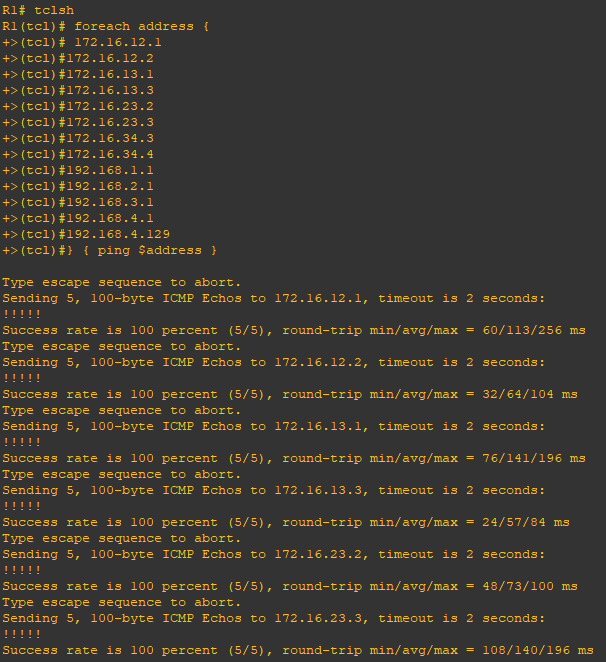
192.168.2.1

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



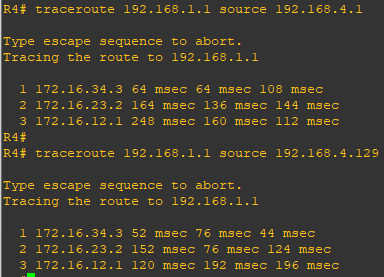
b) On R4, use the **traceroute** command to the R1 LAN address and source the ICMP packet from R4 LAN A and LAN B.

Note:- You can specify the source as the interface address (for example 192.168.4.1) or the interface designator (for example, Fa0/0).

**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)

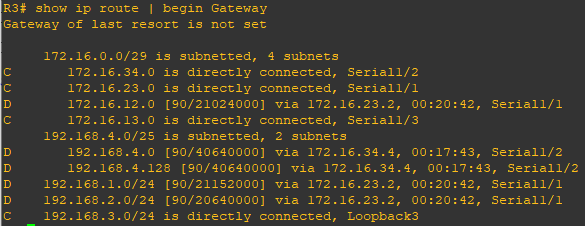


Notice that the path taken for the packets sourced from the R4 LANs are going through R3 🡪R2 🡪 R1.

c) On R3, use the show ip route command and note that the preferred route from R3 to R1 LAN 192.168.1.0/24 is via R2 using the R3 exit interface S1/1.

**Router R3 Console**

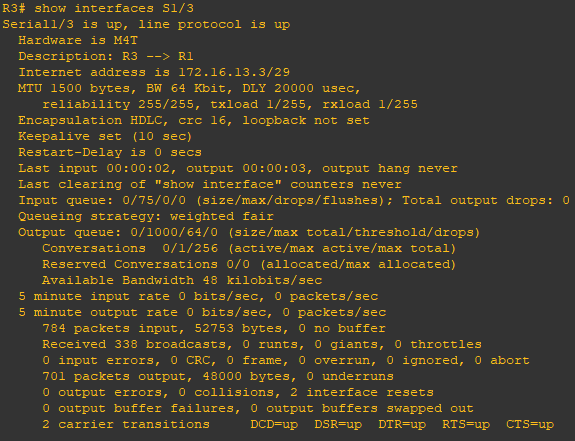
show ip route | begin Gateway



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

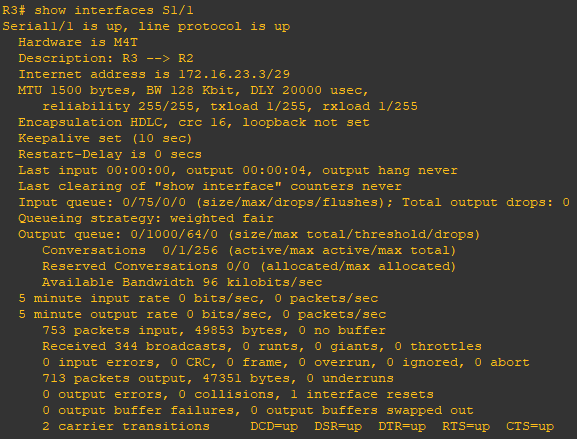
**Router R3 Console**

show interfaces S1/3



**Router R3 Console**

show interfaces S1/1

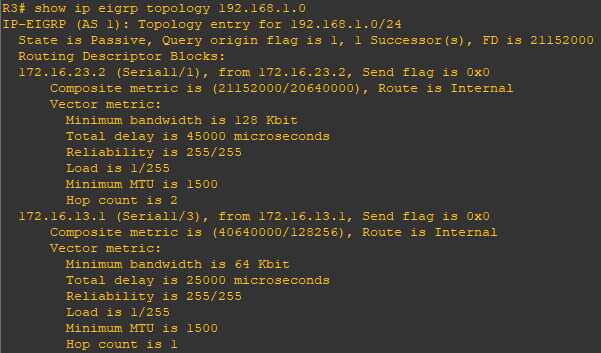


Notice that the bandwidth of the serial link between R3 and R1 (S1/3) is set to 64 Kb/s, while the bandwidth of the serial link between R3 and R2 (S1/1) is set to 128 Kb/s.

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



As indicated, R4 has two routes to reach 192.168.1.0. However, the metric for the route to R1 (172.16.13.1) is much higher (40640000) than the metric of the route to R2 (21152000), making the route through R2 the successor route.

**Step 6:- Configure PBR to provide path control.**

Now you will deploy source-based IP routing by using PBR. You will change a default IP routing decision based on the EIGRP-acquired routing information for selected IP source-to-destination flows and apply a different next-hop router.

Recall that routers normally forward packets to destination addresses based on information in their routing table. By using PBR, you can implement policies that selectively cause packets to take different paths based on source address, protocol type, or application type. Therefore, PBR overrides the router’s normal routing behavior.

Configuring PBR involves configuring a route map with match and set commands and then applying the route map to the interface.

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

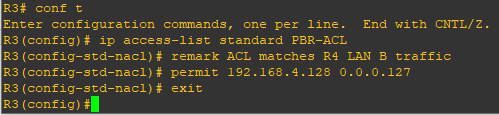
**Router R3 Console**

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**

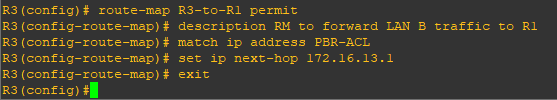
route-map R3-to-R1 permit

description RM to forward LAN B traffic to R1

match ip address PBR-ACL

set ip next-hop 172.16.13.1

exit



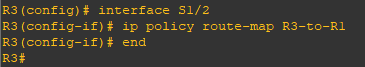
c) Apply the R3-to-R1 route map to the serial interface on R3 that receives the traffic from R4. Use the **ip policy route-map** command on interface S1/2.

**Router R3 Console**

interface S1/2

ip policy route-map R3-to-R1

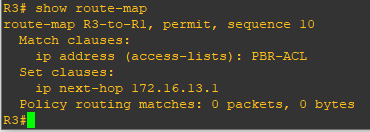
end



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

**Router R3 Console**

show route-map



Note:- There are currently no matches because no packets matching the ACL have passed through R3 S1/2.

**Step 7:- Test the policy.**

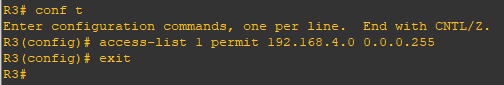
Now we are ready to test the policy configured on R3. Enable the **debug ip policy** command on R3 so that you can observe the policy decision-making in action. To help filter the traffic, first create a standard ACL that identifies all traffic from the R4 LANs.

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

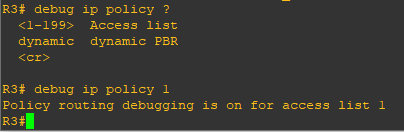


b) Enable PBR debugging only for traffic that matches the R4 LANs.

**Router R3 Console**

debug ip policy ?

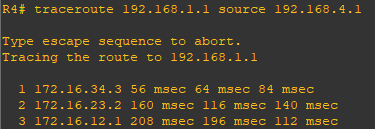
debug ip policy 1



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

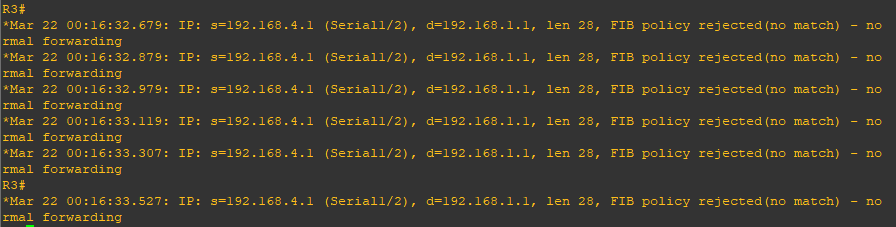
**Router R4 Console**

traceroute 192.168.1.1 source 192.168.4.1



Notice the path taken for the packet sourced from R4 LAN A is still going through R3 🡪 R2 🡪 R1.

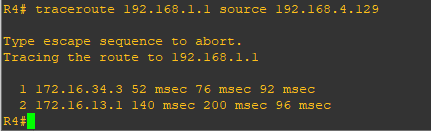
As the traceroute was being executed, router R3 should be generating the following debug output.



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

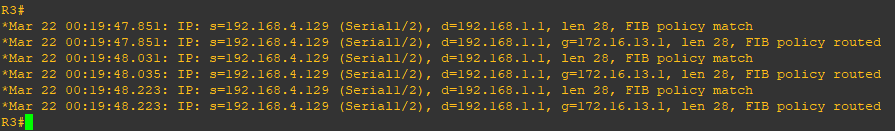
**Router R4 Console**

traceroute 192.168.1.1 source 192.168.4.129



Now the path taken for the packet sourced from R4 LAN B is R3 🡪 R1, as expected.

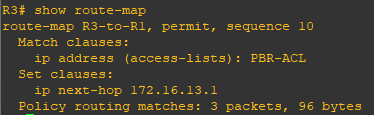
The debug output on R3 also confirms that the traffic meets the criteria of the R3-to-R1 policy.



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

**Router R3 Console**

show route-map

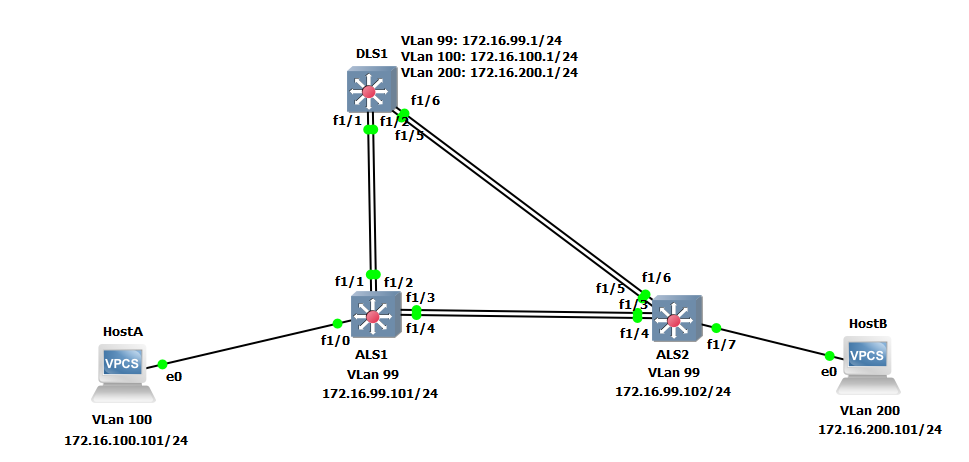


Note:- There are now matches to the policy because packets matching the ACL have passed through R3 S1/2.

**Practical 6**

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

**Topology:-**



**Part 1: Prepare for the Lab**

**Step 1: Configure basic switch parameters.**

Configure an IP address on the management VLAN according to the diagram. VLAN 1 is the default management VLAN, but following best practice, we will use a different VLAN. In this case, VLAN 99.

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

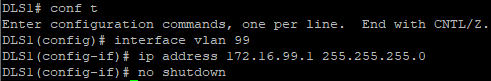
no shutdown

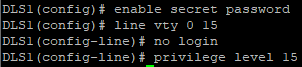
enable secret password

line vty 0 15

no login

privilege level 15





**ALS1 Console:**

interface vlan 99

ip address 172.16.99.101 255.255.255.0

no shutdown

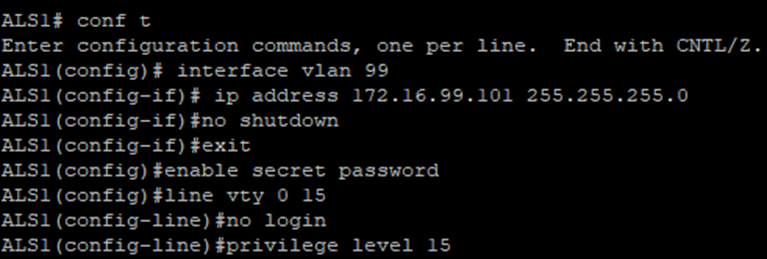
exit

enable secret password

line vty 0 15

no login

privilege level 15



**ALS2 Console:**

interface vlan 99

ip address 172.16.99.102 255.255.255.0

no shutdown

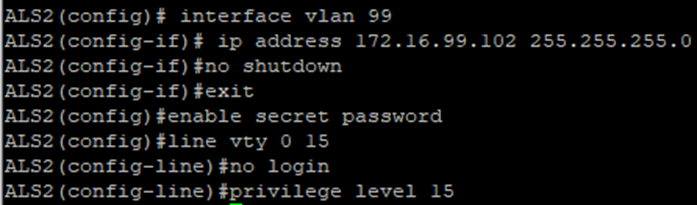
exit

enable secret password

line vty 0 15

no login

privilege level 15



Configure default gateways on ALS1 and ALS2. These are access layer switches operating as Layer 2 devices and need a default gateway to send traffic from their management interface to other networks. Configure both ALS1 and ALS2.

**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:**

vlan 666

name NATIVE\_DO\_NOT\_USE

exit

interface ran f 1/1 – 2

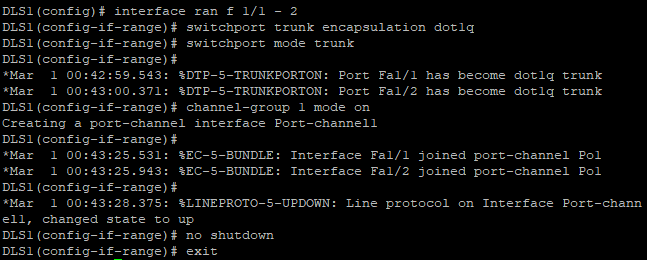
switchport trunk encapsulation dot1q

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

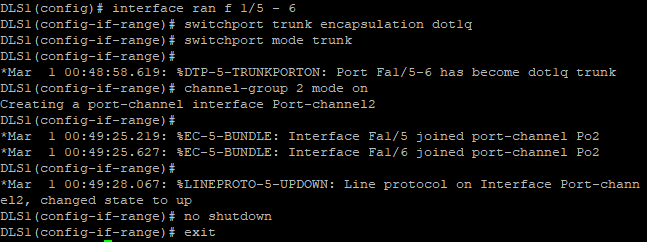
switchport trunk encapsulation dot1q

switchport mode trunk

channel-group 2 mode on

no shutdown

exit



Configure the trunks and EtherChannel from ALS1 and DLS1

**ALS1 Console:**

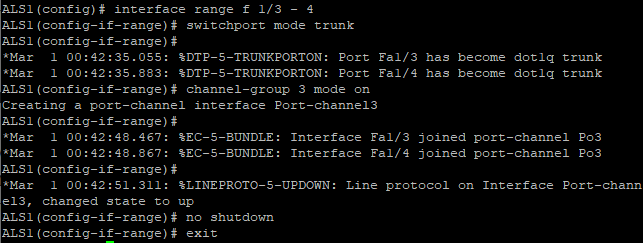
interface range f 1/3 – 4

switchport mode trunk

channel-group 3 mode on

no shutdown

exit



Configure the trunks and EtherChannel from ALS1 and ALS2

**ALS1 Console:**

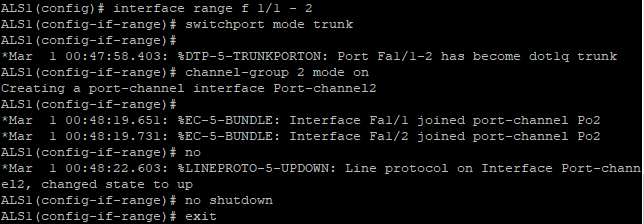
interface range f 1/1 – 2

switchport mode trunk

channel-group 2 mode on

no shutdown

exit



Configure the trunks and EtherChannel from ALS2 and DLS1

**ALS2 Console:**

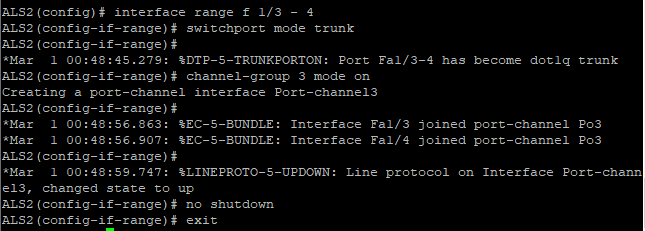
interface range f 1/3 – 4

switchport mode trunk

channel-group 3 mode on

no shutdown

exit



Configure the trunks and EtherChannel from ALS2 and ALS1

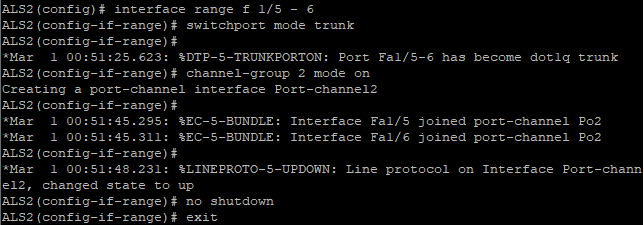
interface range f 1/5 – 6

switchport mode trunk

channel-group 2 mode on

no shutdown

exit



**Step 4: Configure VTP on ALS1 and ALS2.**

**ALS1 Console:**

vtp mode client



**ALS2 Console:**

vtp mode client



**Step 5: Configure VTP on DLS1.**

Create the VTP domain on DLS1, and create VLANs 100 and 200 for the domain.

vtp domain SWPOD

vtp version 2

vlan 99

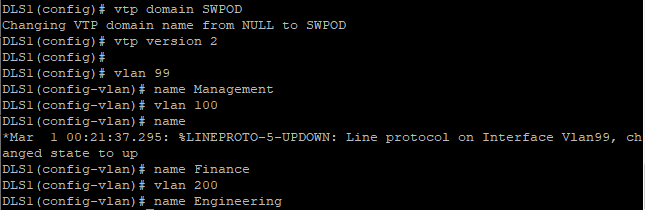
name Management

vlan 100

name Finance

vlan 200

name Engineering



**Step 6: Configure access ports.**

Configure the host ports for the appropriate VLANs according to the diagram.

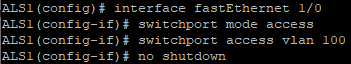
**ALS1 Console:**

interface fastEthernet 1/0

switchport mode access

switchport access vlan 100

no shutdown



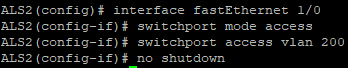
**ALS2 Console:**

interface fastEthernet 1/0

switchport mode access

switchport access vlan 200

no shutdown



**Step 7: Configure VLAN interfaces and enable routing.**

**DLS1 Console:**

interface vlan 100

ip address 172.16.100.1 255.255.255.0

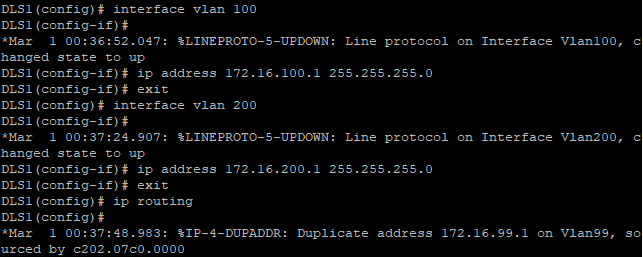
exit

interface vlan 200

ip address 172.16.200.1 255.255.255.0

exit

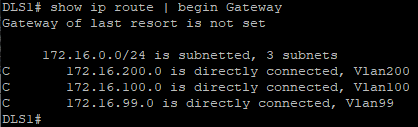
ip routing



Verify the configuration using the show ip route command on DLS1.

**DLS1 Console:**

show ip route | begin Gateway



Run the following Tcl script on DLS1 to verify full connectivity. If these pings are not successful, troubleshoot.

**DLS1 Console:**

tclsh

foreach address {

172.16.99.1

172.16.99.101

172.16.99.102

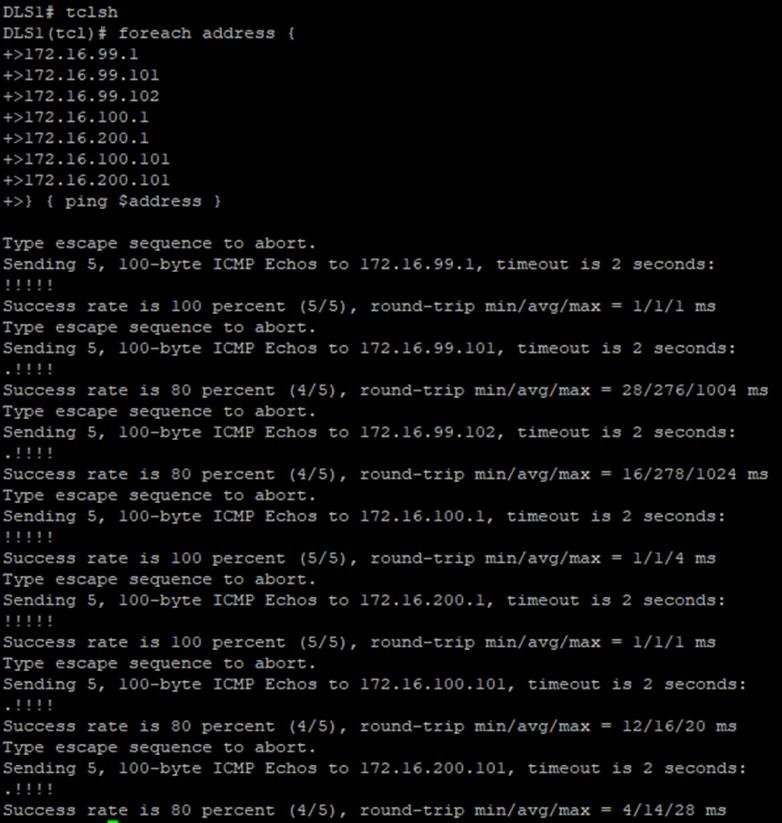
172.16.100.1

172.16.200.1

172.16.100.101

172.16.200.101

} { ping $address }



**Part 2: Configure Cisco IOS IP SLA**

**Step 1: Configure Cisco IOS IP SLA responders.**

Use the ip sla responder command on ALS1 and ALS2 to enable sending and receiving IP SLAs control packets.

**ALS1 Console:**

ip sla responder



**ALS2 Console:**

ip sla responder



Configure ALS1 and ALS2 as IP SLA responders for UDP jitter using the ip sla responder udp-echo ipaddress command. Specify the IP address of DLS1 VLAN 1 to act as the destination IP address for the reflected UDP traffic on both ALS1 and ALS2. Configure this on both ALS1 and ALS2.

**ALS1 Console:**

ip sla responder udp-echo ipaddress 172.16.99.101 port 5000



**ALS2 Console:**

ip sla responder udp-echo ipaddress 172.16.99.102 port 5000



**Step 2: Configure the Cisco IOS IP SLA source to measure network performance.**

On DLS1, create an IP SLA operation and enter IP SLA configuration mode with the ip sla operation-number command.

**DLS1 Console:**

ip sla 1



Configure an IP SLA ICMP echo operation using the icmp-echo command in IP SLA configuration mode. On DLS1, for ICMP echo operation 1, specify the IP address of Host A as the target. For ICMP echo operation 2, specify the IP address of Host B as the target.

**DLS1 Console:**

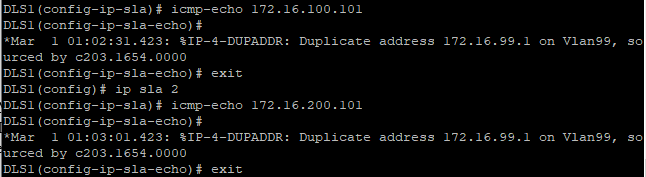
icmp-echo 172.16.100.101

exit

ip sla 2

icmp-echo 172.16.200.101

exit



To configure an IP SLA UDP jitter operation, use the udp-jitter command in IP SLA configuration mode. For UDP jitter operation 3, specify the destination IP address of the ALS1 VLAN 99 interface as the target. For operation 4, specify the destination IP address of the ALS2 VLAN 99 interface as the target. The IP SLA communication port is 5000 for both operations.

**DLS1 Console:**

ip sla 3

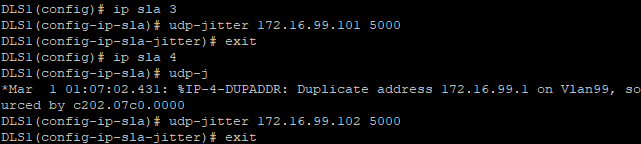
udp-jitter 172.16.99.101 5000

exit

ip sla 4

udp-jitter 172.16.99.102 5000

exit



Schedule the IP SLAs operations to run indefinitely beginning immediately using the ip sla schedule global configuration mode command.

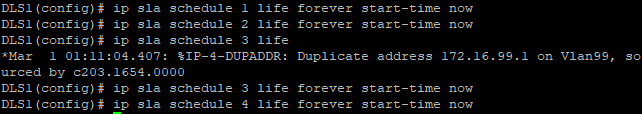
**DLS1 Console:**

ip sla schedule 1 life forever start-time now

ip sla schedule 2 life forever start-time now

ip sla schedule 3 life forever start-time now

ip sla schedule 4 life forever start-time now

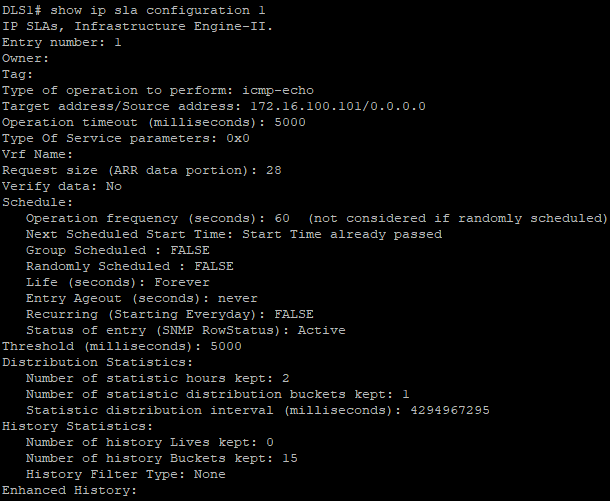


**Step 3: Monitor IP SLAs operations.**

View the IP SLA configuration for IP SLA 1 on DLS1. The output for IP SLA 2 is similar.

**DLS1 Console:**

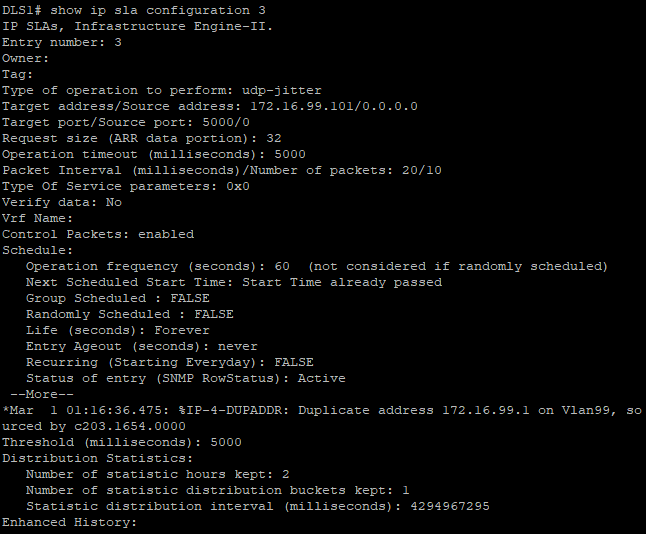
show ip sla configuration 1



View the IP SLA configuration for IP SLA 3 on DLS1. The output for IP SLA 4 is similar.

**DLS1 Console:**

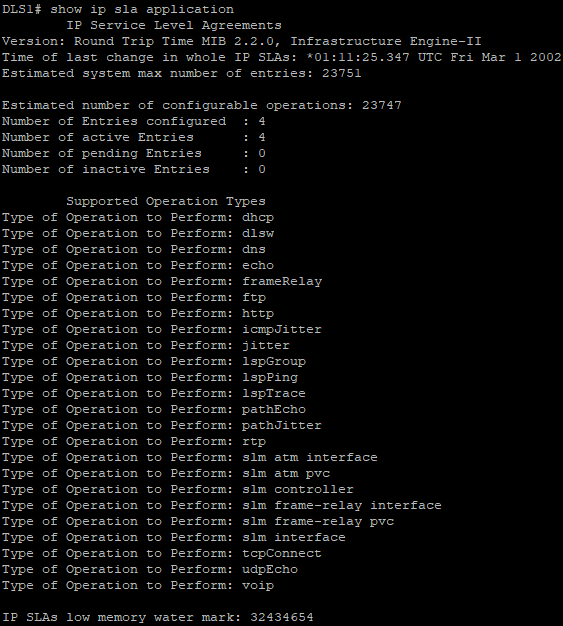
show ip sla configuration 3



Display global information about Cisco IOS IP SLAs on DLS1.

**DLS1 Console:**

show ip sla application



Display information about Cisco IOS IP SLA responders on ALS1. The ALS2 output is similar.

**ALS1 Console:**

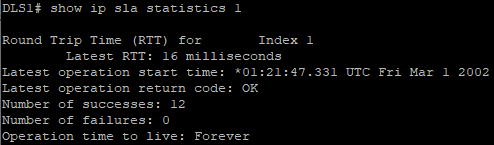
show ip sla responder



Display IP SLA statistics on DLS1 for IP SLA 1. The IP SLA 2 output is similar.

**DLS1 Console:**

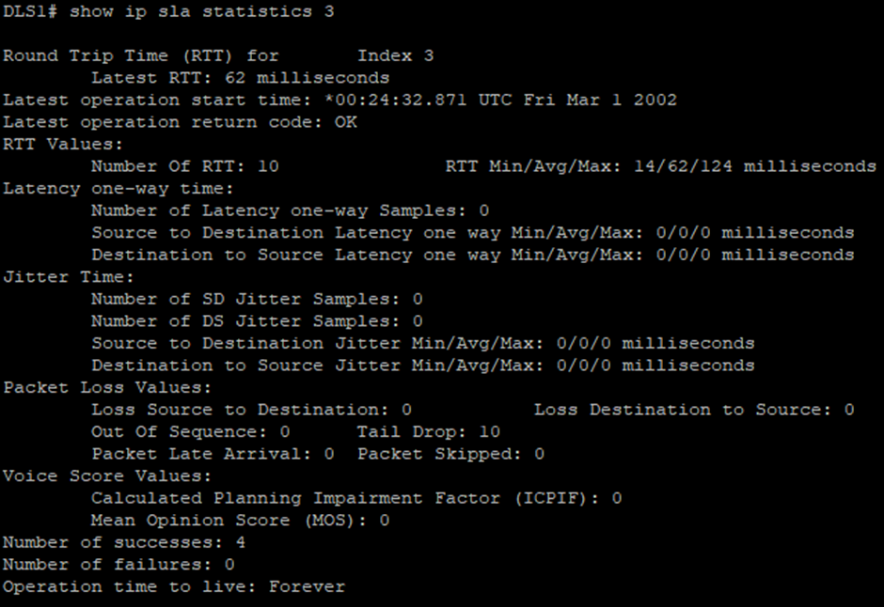
show ip sla statistics 1



Display IP SLA statistics on DLS1 for IP SLA 3. The IP SLA 4 output is similar.

**DLS1 Console:**

show ip sla statistics 3



Disable interface VLAN 99 on ALS1 using the shutdown command.

**ALS1 Console:**

interface vlan 99

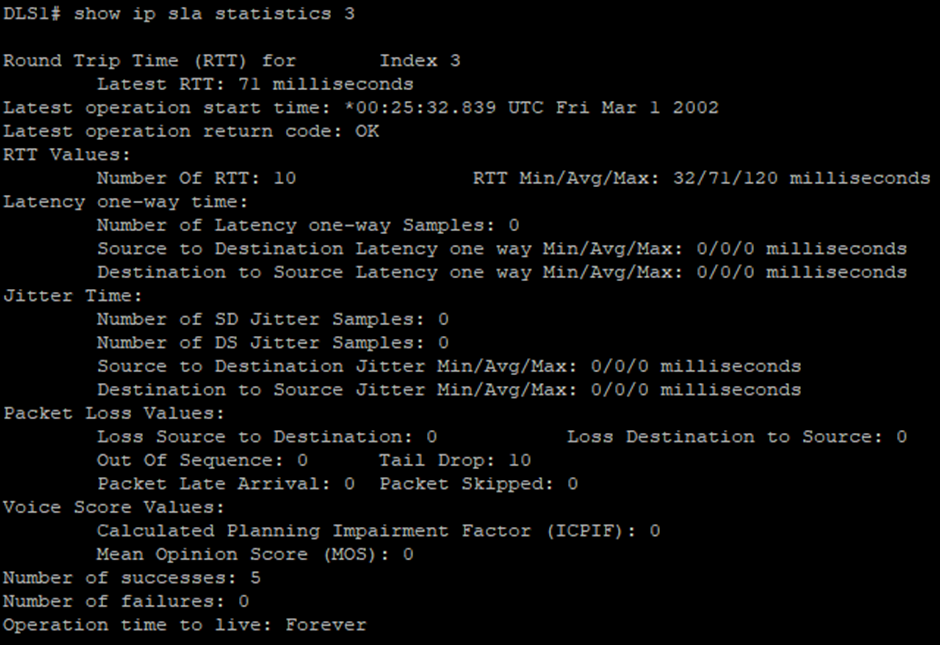
shutdown



Allow a few minutes to pass and then issue the show ip sla statistics 3 command on DLS1. The output should look similar to the following.

**DLS1 Console:**

show ip sla statistics 3



**Part 3: Switch Port Analyzer (SPAN) Feature.**

**Step 1: Configure Remote SPAN (RSPAN).**

Create the RSPAN VLAN on DLS1 using the VLAN 300 command from global configuration mode.

**DLS1 Console:**

vlan 300

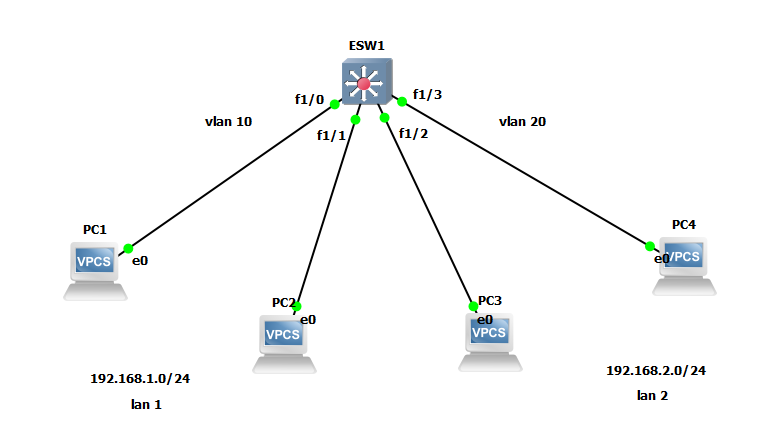
name REMOTE\_SPAN

remote-span

**Practical 7**

**Aim:- Inter-VLAN Routing.**

**Topology:-**



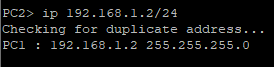
**Configuration for PC1:**

ip 192.168.1.1/24



**Configuration for PC2:**

ip 192.168.1.2/24



**Configuration for PC3:**

ip 192.168.2.1/24



**Configuration for PC4:**

ip 192.168.2.2/24

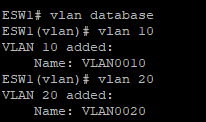


**Configuration for EtherSwitch:**

vlan database

vlan 10

vlan 20



show vlan-switch



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 20

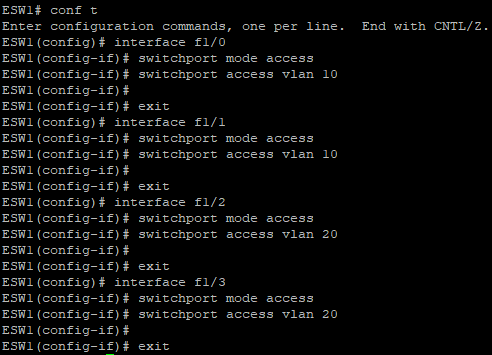
exit

interface f1/3

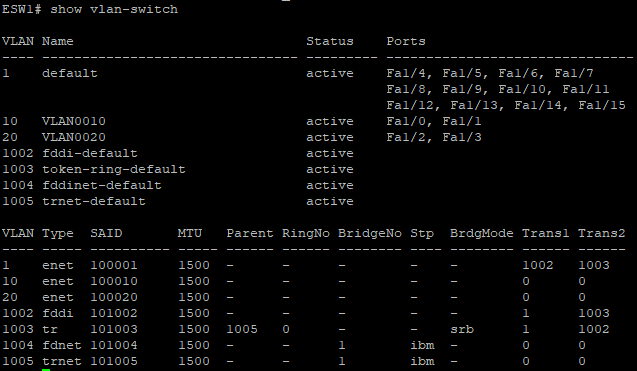
switchport mode access

switchport access vlan 20

exit

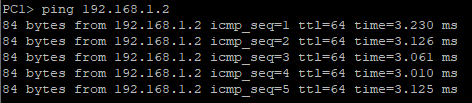


show vlan-switch



**PC1 Console:**

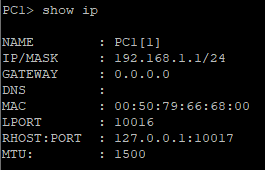
ping 192.168.1.2



ping 192.168.2.2



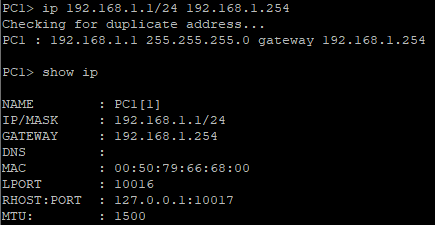
show ip

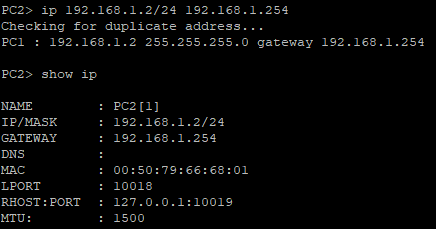


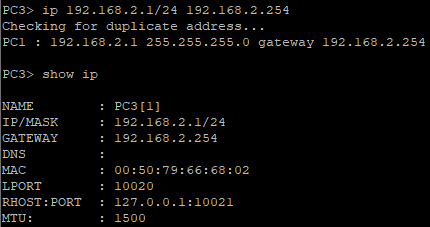
Since there is no gateway, we will create gateway in all PC’s.

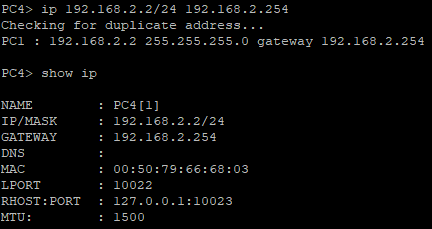
ip 192.168.1.1/24 192.168.1.254

show ip









**Configuration for EhterSwitch:**

interface vlan 10

ip address 192.168.1.254 255.255.255.0

no shutdown

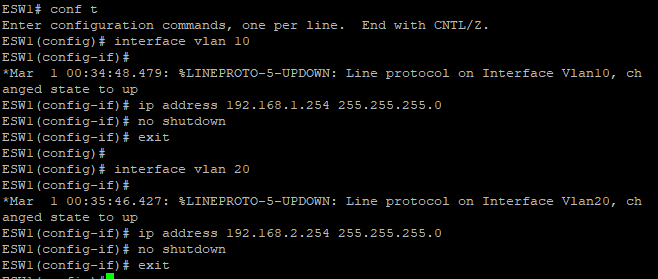
exit

interface vlan 20

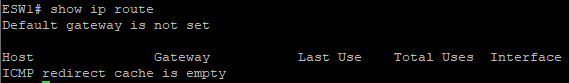
ip address 192.168.2.254 255.255.255.0

no shutdown

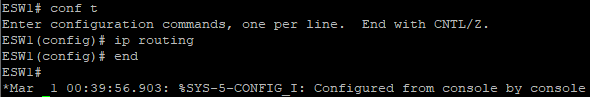
exit



show ip route



ip routing



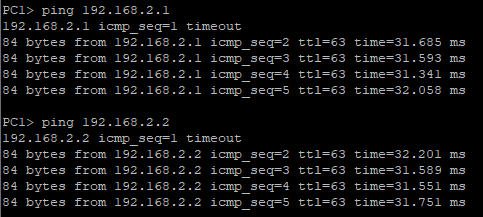
show ip route



Now since gateway is created we will ping again and check whether it is successful or not.

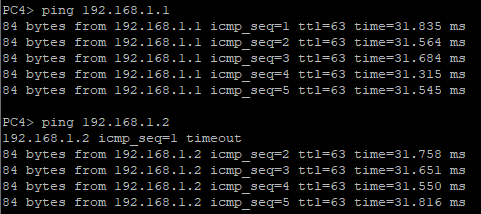
**PC1 Console:**

ping 192.168.2.1



**PC4 Console:**

ping 192.168.1.1



**Practical 8**

**Aim:- Simulating MPLS**

**Topology:-**

**Router R1 Console**

interface Loopback0

ip address 1.1.1.1 255.255.255.255

ip ospf 1 area 0

exit

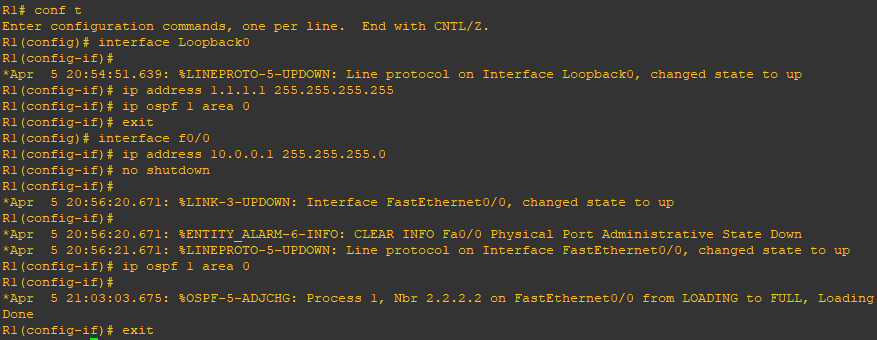
interface f0/0

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

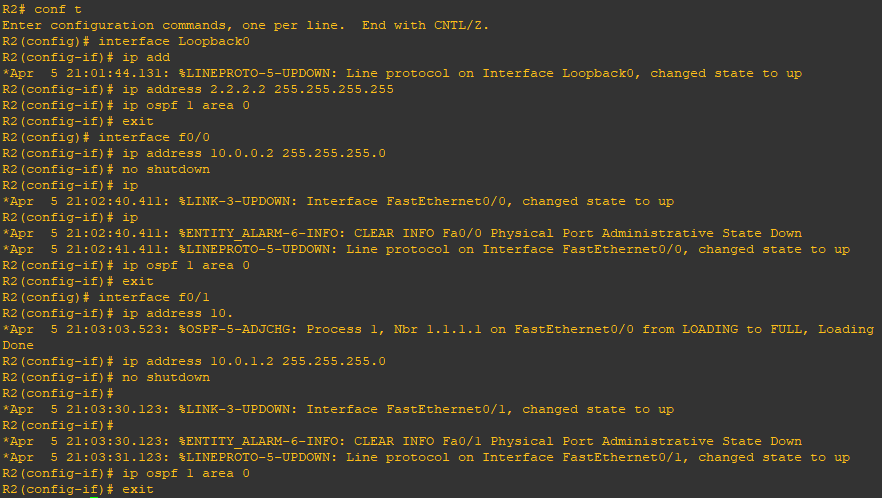
interface f0/1

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

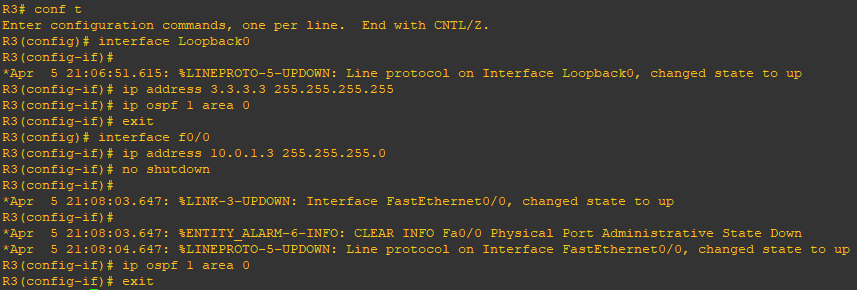
interface f0/0

ip address 10.0.1.3 255.255.255.0

no shutdown

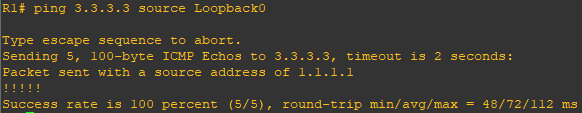
ip ospf 1 area 0

exit



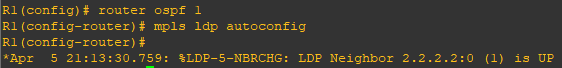
**Router R1 Console**

ping 3.3.3.3 source Loopback0



router ospf 1

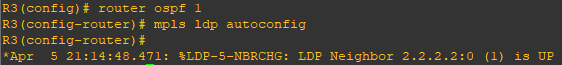
mpls ldp autoconfig



**Router R3 Console**

router ospf 1

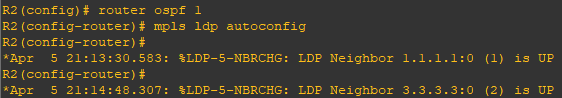
mpls ldp autoconfig



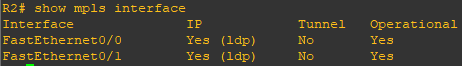
**Router R2 Console**

router ospf 1

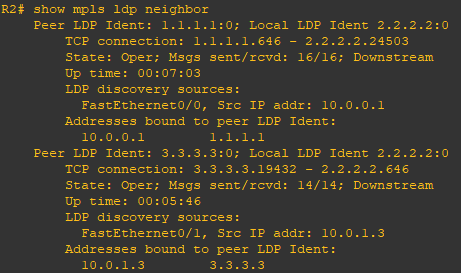
mpls ldp autoconfig



show mpls interface

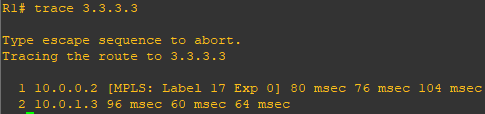


show mpls ldp neighbor



**Router R1 Console**

trace 3.3.3.3



**Router R1 Console**

router bgp 1

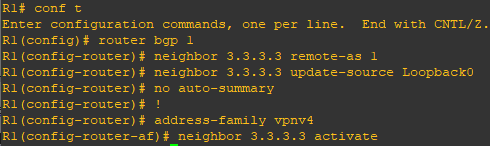
neighbor 3.3.3.3 remote-as 1

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

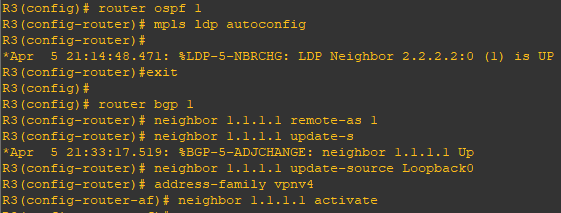
neighbor 1.1.1.1 remote-as 1

neighbor 1.1.1.1 update-source Loopback0

no auto-summary

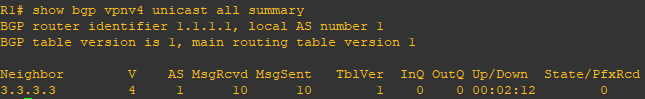
address-family vpnv4

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

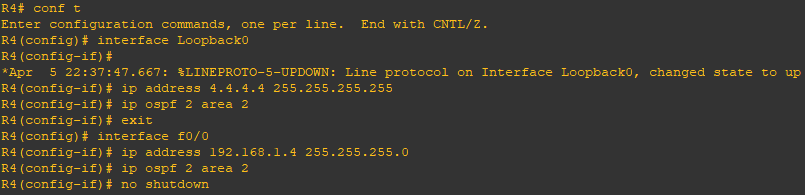
exit

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

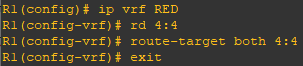


**Router R1 Console**

ip vrf RED

rd 4:4

route-target both 4:4



interface f0/1

ip vrf forwarding RED



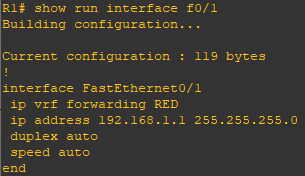
interface f0/1

ip address 192.168.1.1 255.255.255.0

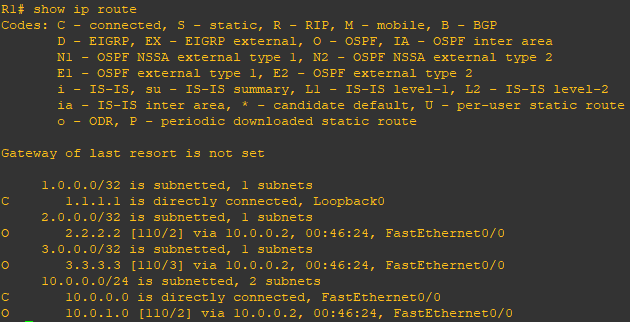
no shutdown



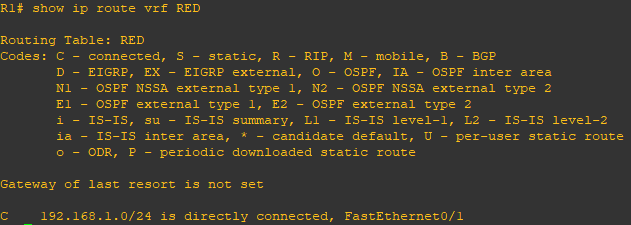
show run interface f0/1



show ip route

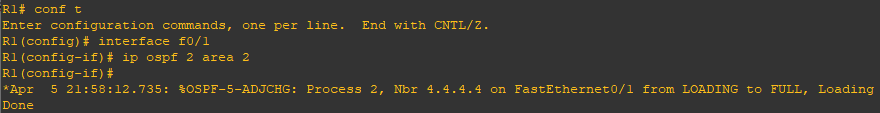


show ip route vrf RED

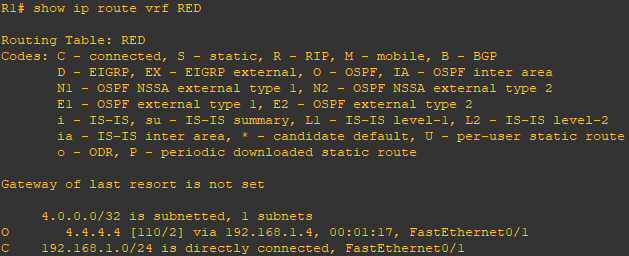


int f0/1

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

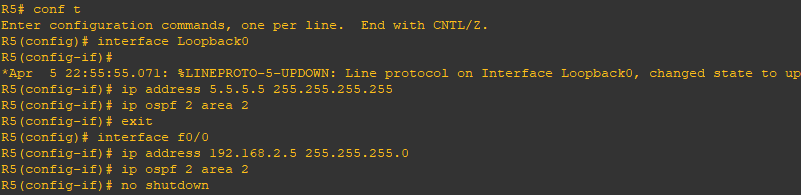
exit

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

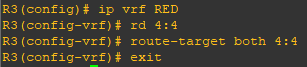
no shutdown



ip vrf RED

rd 4:4

route-target both 4:4



interface f0/1

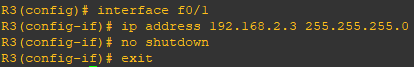
ip vrf forwarding RED



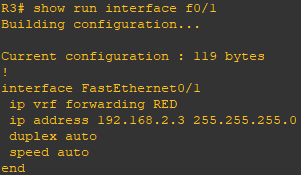
interface f0/1

ip address 192.168.2.3 255.255.255.0

no shutdown

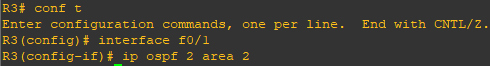


show run interface f0/1

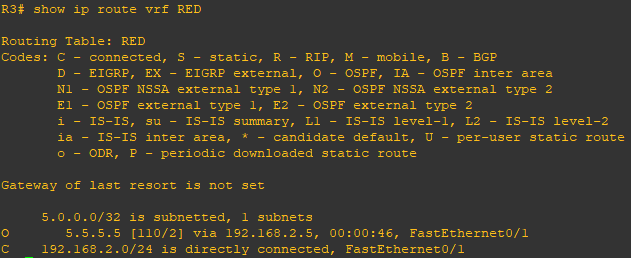


interface f0/1

ip ospf 2 area 2

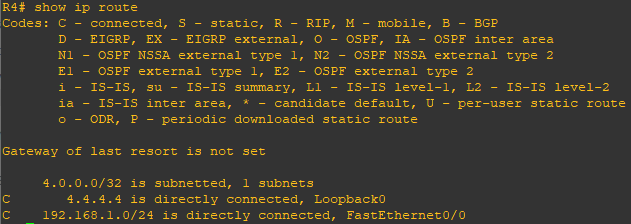


show ip route vrf RED



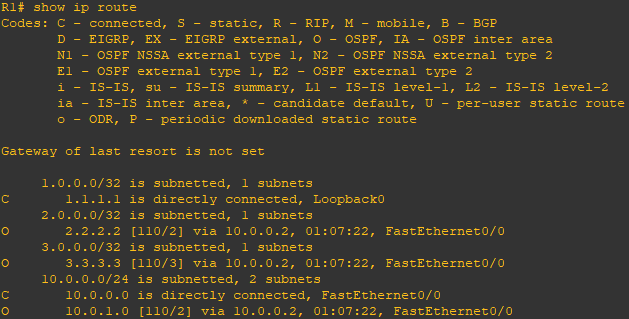
**Router R4 Console**

show ip route

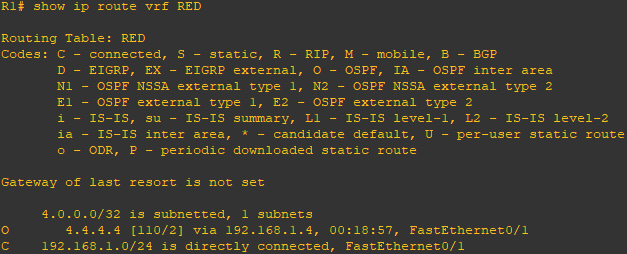


**Router R1 Console**

show ip route



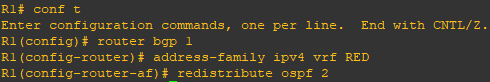
show ip route vrf RED



router bgp 1

address-family ipv4 vrf RED

redistribute ospf 2

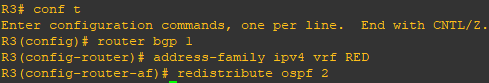


**Router R3 Console**

router bgp 1

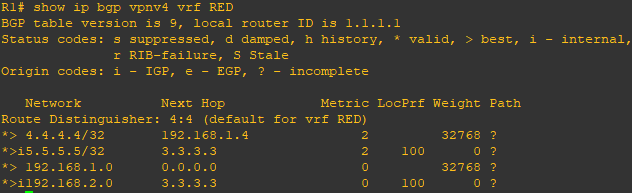
address-family ipv4 vrf RED

redistribute ospf 2



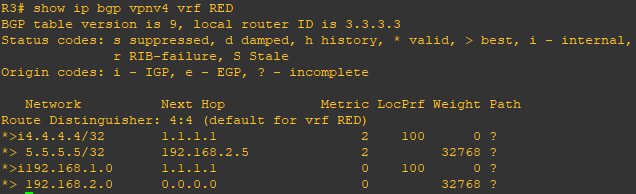
**Router R1 Console**

show ip bgp vpnv4 vrf RED



**Router R3 Console**

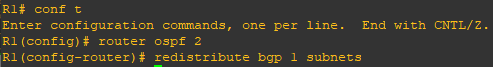
show ip bgp vpnv4 vrf RED



**Router R1 Console**

router ospf 2

redistribute bgp 1 subnets



**Router R3 Console**

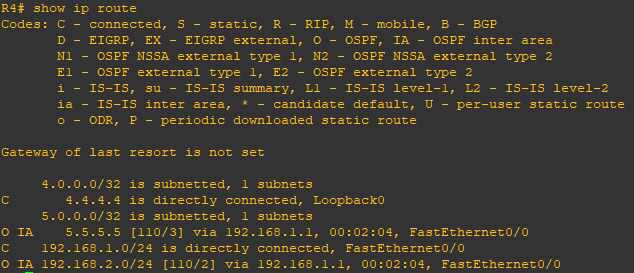
router ospf 2

redistribute bgp 1 subnets



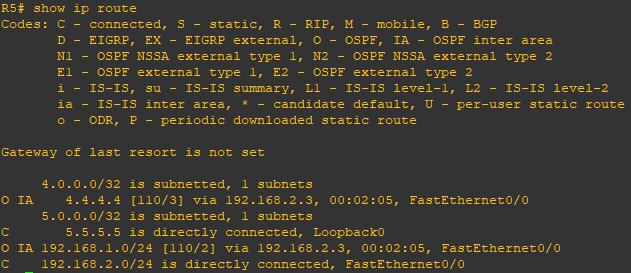
**Router R4 Console**

show ip route



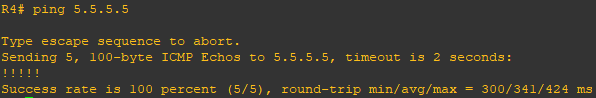
**Router R5 Console**

show ip route

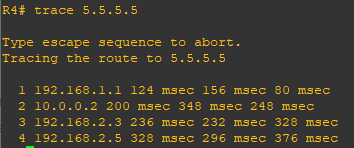


**Router R4 Console**

ping 5.5.5.5



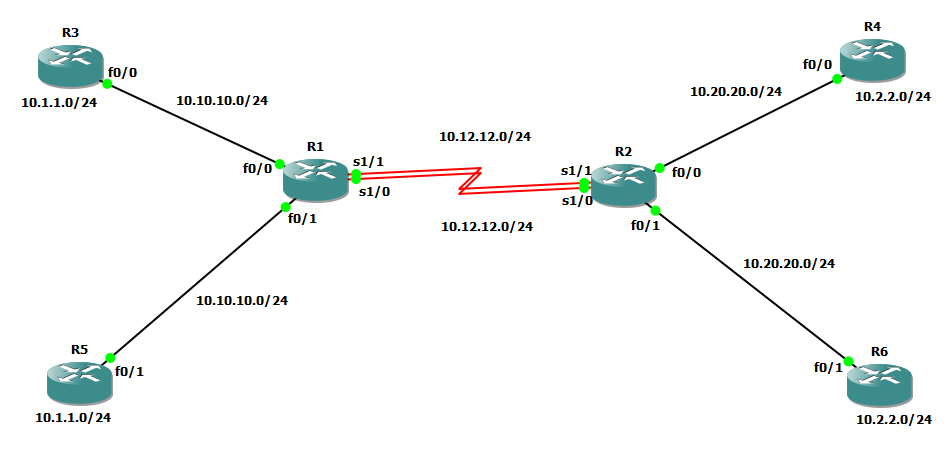
trace 5.5.5.5



**Practical 9**

**Aim:- Simulating Virtual Routing and Forwarding (VRF)**

**Topology:-**



**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.**

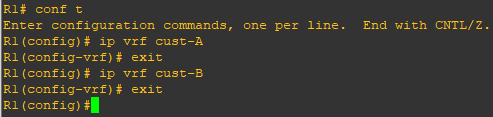
**Router R1 Console**

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

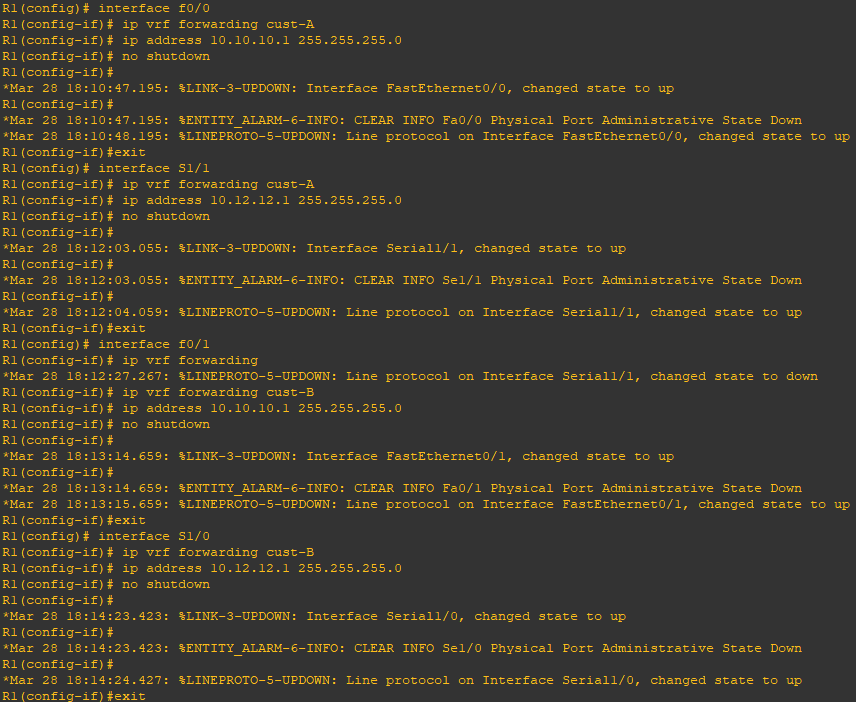
interface S1/0

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

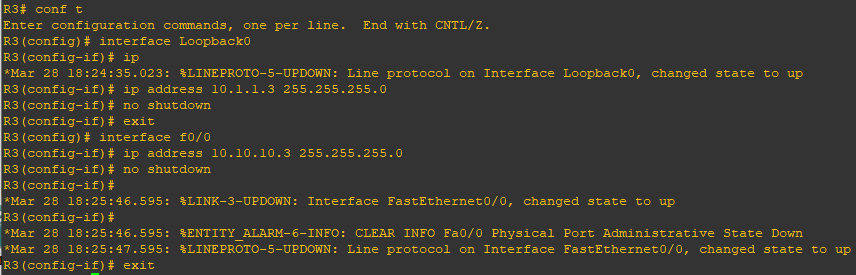
exit

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

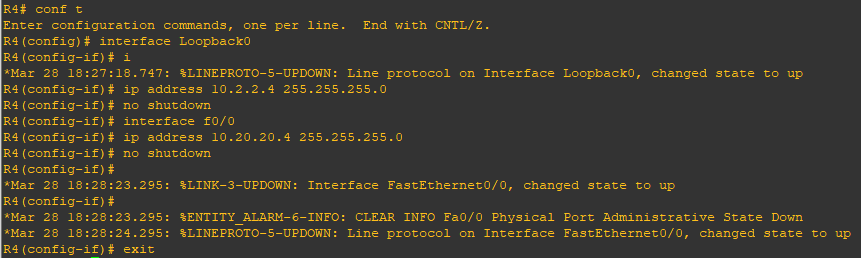
exit

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

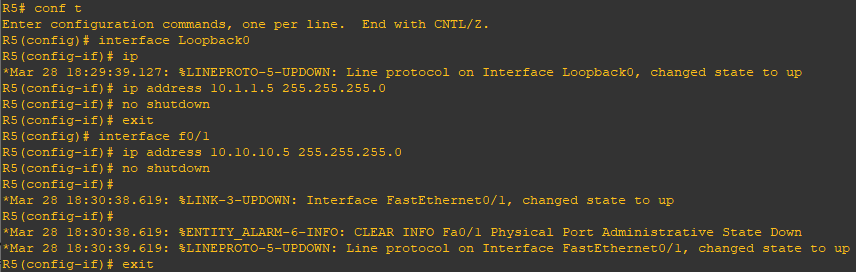
exit

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

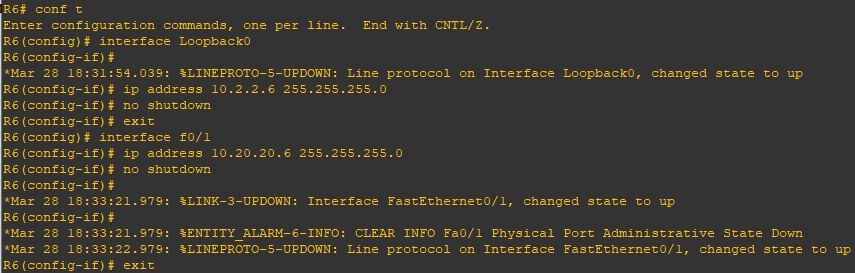
exit

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

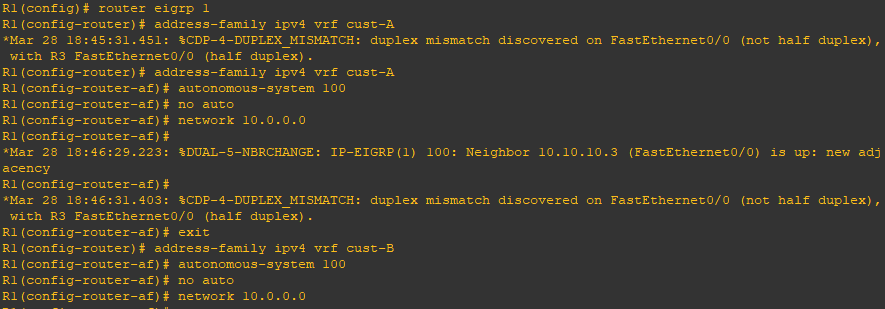
address-family ipv4 vrf cust-B

autonomous-system 100

no auto

network 10.0.0.0

exit



**Router R1 Console**

show ip route

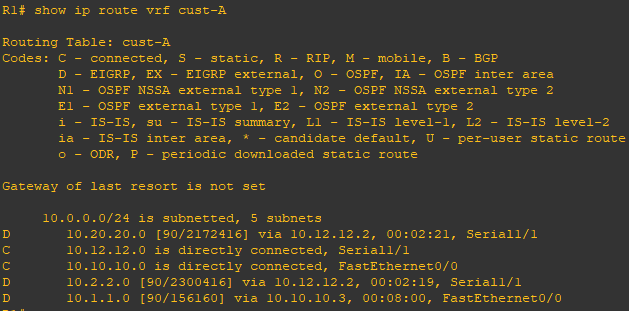
Note:- Since we have configured virtual routing and forwarding it will not display the connections.



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

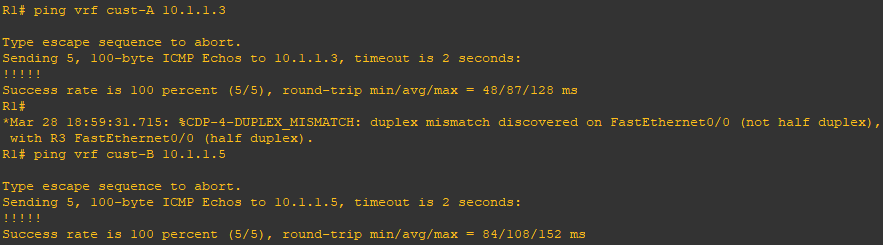
show ip route vrf cust-A

Note:- Now it will display all the connections.



Since we have configured virtual routing and forwarding on R1 and R2, to ping we have to write the following command.

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

