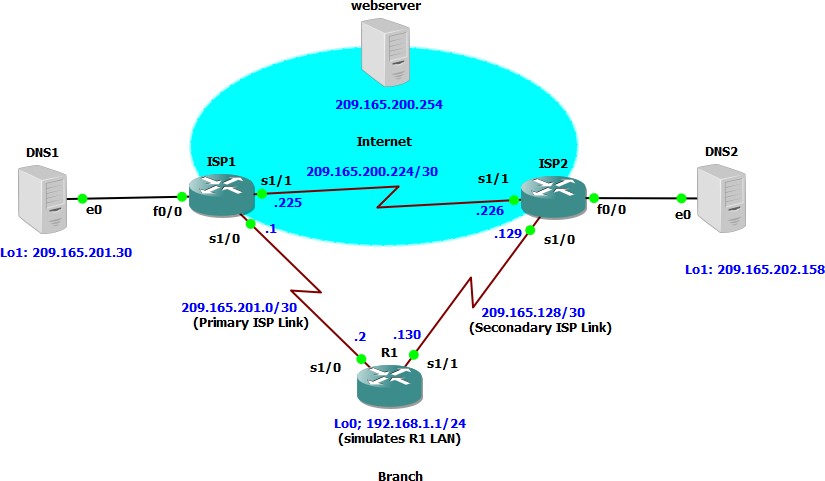
INDEX

|  |  |  |
| --- | --- | --- |
| **Prac.**  **No.** | **Practical** | **Date** |
| **1** | **Configure IP SLA Tracking and Path Control Topology** | **29/05/24** |
| **2** | **Using the AS\_PATH Attribute** | **1/06/24** |
| **3** | **Configuring IBGP and EBGP Sessions, Local Preference, and**  **MED** | **13/06/24** |
| **4** | **Secure the Management Plane** | **27/06/24** |
| **5** | **Configure and Verify Path Control Using PBR s** | **29/06/24** |
| **6** | **Configure IP SLA Tracking and Path Control** | **4/06/24** |
| **7** | **Inter-VLAN routing** | **24/06/24** |
| **8** | **Simulating MPLS environment** | **11/06/24** |

**Practical No - 1**

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

**Topology :**



## Objectives

* Configure and verify the IP SLA feature.
* Test the IP SLA tracking feature.
* Verify the configuration and operation using show and debug commands.

**Step 1: Prepare the routers and configure the router hostname and interface addresses.**

**Router R1**

interface Loopback 0

ip address 192.168.1.1 255.255.255.0

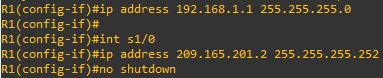
interface Serial0/0/0

ip address 209.165.201.2 255.255.255.252

no shutdown interface Serial0/0/1

ip address 209.165.202.130 255.255.255.252

no shutdown



#### Router ISP1 (R2)

interface Loopback0

ip address 209.165.200.254 255.255.255.255

interface Loopback1

ip address 209.165.201.30 255.255.255.255

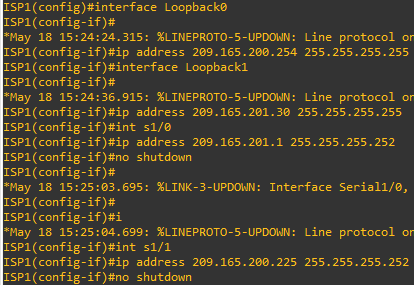
interface Serial0/0/0

ip address 209.165.201.1 255.255.255.252

no shutdown interface Serial0/0/1

ip address 209.165.200.225 255.255.255.252

no shutdown



#### Router ISP2 (R3)

interface Loopback0

ip address 209.165.200.254 255.255.255.255

interface Loopback1

ip address 209.165.202.158 255.255.255.255

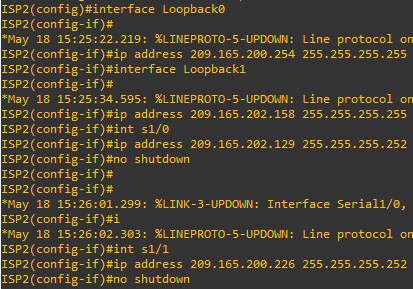
interface Serial0/0/0 description ISP2 --> R1

ip address 209.165.202.129 255.255.255.252

no shutdown interface Serial0/0/1

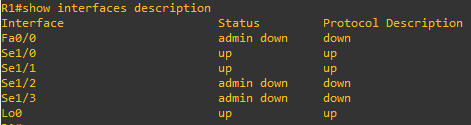
ip address 209.165.200.226 255.255.255.252

no shutdown



b. Verify the configuration by using the show interfaces description command. The output from router R1 is shown here as an example.

R1# show interfaces description



c. The current routing policy in the topology is as follows:

* Router R1 establishes connectivity to the Internet through ISP1 using a default static route.
* ISP1 and ISP2 have dynamic routing enabled between them, advertising their respective public address pools.
* ISP1 and ISP2 both have static routes back to the ISP LAN.

#### Router R1

ip route 0.0.0.0 0.0.0.0 209.165.201.1



#### Router ISP1 (R2)

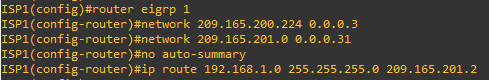
router eigrp 1

network 209.165.200.224 0.0.0.3

network 209.165.201.0 0.0.0.31

no auto-summary

ip route 192.168.1.0 255.255.255.0 209.165.201.2



#### Router ISP2 (R3)

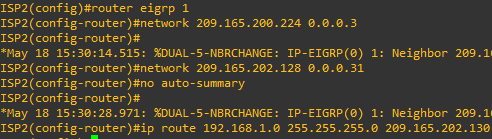
router eigrp 1

network 209.165.200.224 0.0.0.3

network 209.165.202.128 0.0.0.31

no auto-summary

ip route 192.168.1.0 255.255.255.0 209.165.202.130



#### Step 2: Verify server reachability.

1. 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. You can copy the following Tcl script and paste it intoR1.

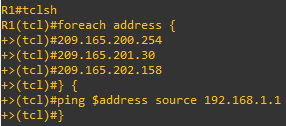
R1(tcl)# foreach address {

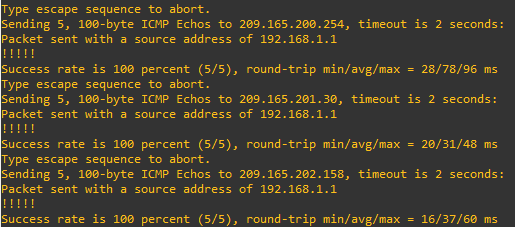
+>(tcl)# 209.165.200.254

+>(tcl)# 209.165.201.30

+>(tcl)# 209.165.202.158

+>(tcl)# } { ping $address source 192.168.1.1 }





1. Trace the path taken to the web server, ISP1 DNS server, and ISP2 DNS server. You can copy the following Tcl script and paste it into R1.

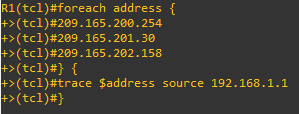
R1(tcl)# foreach address {

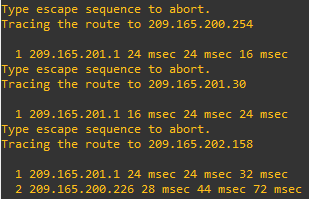
+>(tcl)# 209.165.200.254

+>(tcl)# 209.165.201.30

+>(tcl)# 209.165.202.158

+>(tcl)# } { trace $address source 192.168.1.1 }





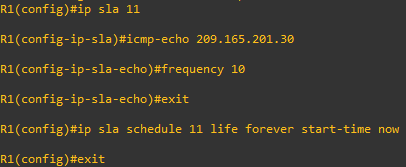
#### Step 3: Configure IP SLA probes.

1. Create an ICMP echo probe on R1 to the primary DNS server on ISP1 using the ip sla command. the previous ip sla monitor command. In addition, the icmp-echo command has replaced the type echo protocol ipIcmpEcho command.

R1(config)# ip sla 11

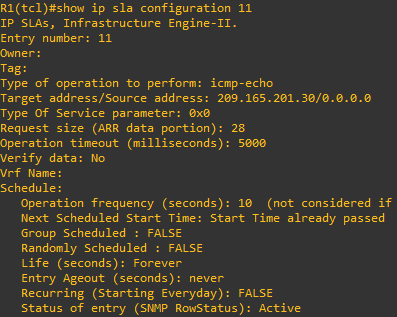
R1(config-ip-sla)# icmp-echo 209.165.201.30 R1(config-ip-sla-echo)# frequency 10 R1(config-ip-sla-echo)# exit

R1(config)# ip sla schedule 11 life forever start-time now



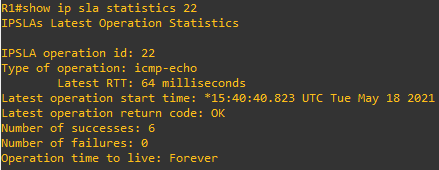
1. Verify the IP SLAs configuration of operation 11 using the show ip sla configuration 11 command.

R1# show ip sla configuration 11

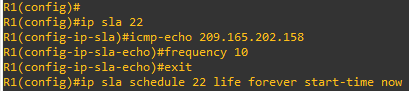


1. Issue the show ip sla statistics command to display the number of successes, failures, and results of the latest operations.

R1# show ip sla statistics

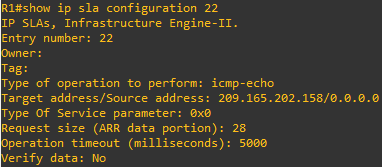


1. Although not actually required because IP SLA session 11 alone could provide the desired fault tolerance, create a second probe, 22, to test connectivity to the second DNS server located on router ISP2. You can copy and paste the following commands on R1.

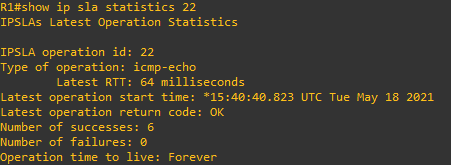


1. Verify the new probe using the show ip sla configuration and show ip sla statistics commands.

R1# show ip sla configuration 22



R1# show ip sla statistics 22

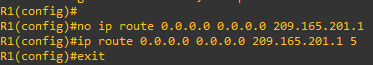


#### Step 4: Configure tracking options.

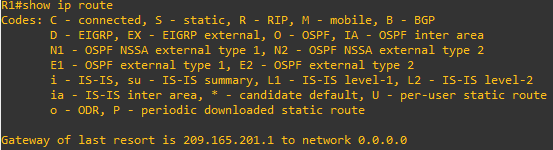
1. Remove the current default route on R1, and replace it with a floating static route having an administrative distance of 5.

R1(config)# no ip route 0.0.0.0 0.0.0.0 209.165.201.1 R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.1 5

R1(config)# exit



1. Verify the routing table. R1# show ip route



1. Use the track 1 ip sla 11 reachability command to enter the config-track subconfiguration mode.

R1(config)# track 1 ip sla 11 reachability R1(config-track)#

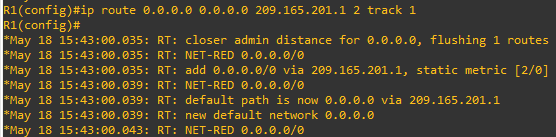


1. Configure the floating static route that will be implemented when tracking object 1 is active. To view routing table changes as they happen, first enable the debug ip routing command. Next, use the ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1 command to create a floating static default route via 209.165.201.1 (ISP1). Notice that this command references the tracking object number 1, which in turn references IP SLA operation number 11.

R1# debug ip routing

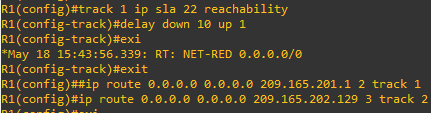


R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1



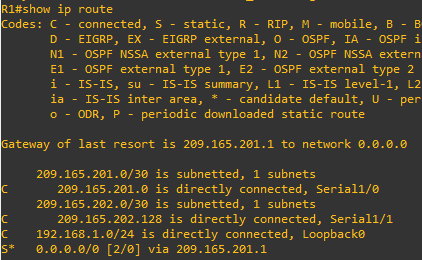
1. Repeat the steps for operation 22, track number 2, and assign the static route an admin distance higher than track 1 and lower than 5. On R1, copy the following configuration, which sets an admin distance of 3. track 2 ip sla 22 reachability delay down 10 up 1 exit

ip route 0.0.0.0 0.0.0.0 209.165.202.129 3 track 2



1. Verify the routing table again.

R1# show ip route



#### Step 5: Verify IP SLA operation.

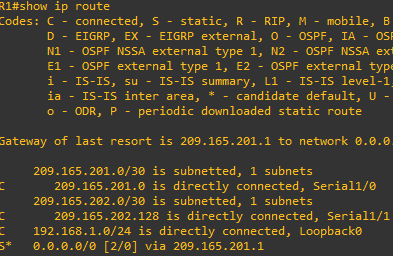
The following summarizes the process:

* Disable the DNS loopback interface on ISP1 (R2).
* Observe the output of the debug command on R1.
* Verify the static route entries in the routing table and the IP SLA statistics of R1.
* Re-enable the loopback interface on ISP1 (R2) and again observe the operation of the IP SLA tracking feature.

ISP1(config)# interface loopback 1 ISP1(config-if)# shutdown

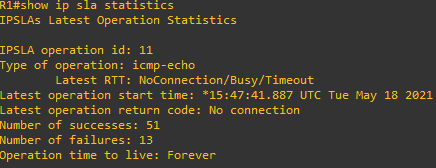


1. Verify the routing table. R1# show ip route



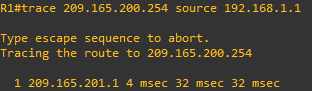
1. Verify the IP SLA statistics.

R1# show ip sla statistics

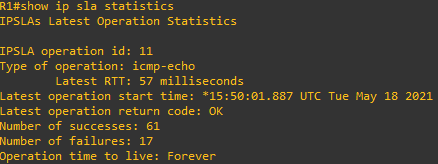


1. Initiate a trace to the web server from the internal LAN IP address.

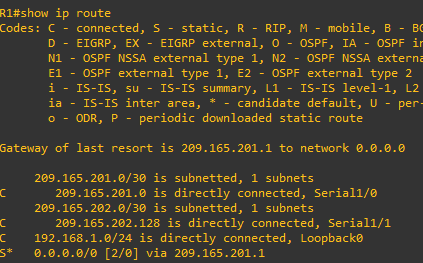
R1# trace 209.165.200.254 source 192.168.1.1



f. Again examine the IP SLA statistics. R1# show ip sla statistics



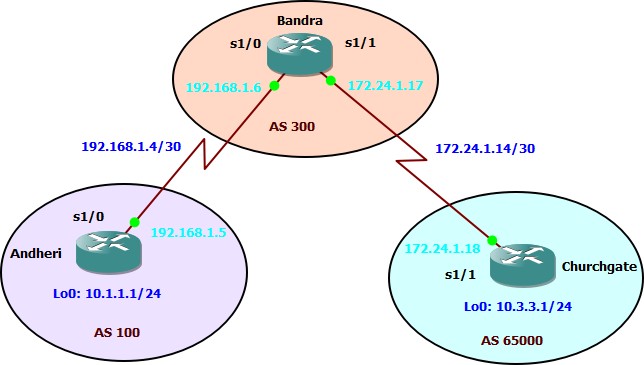
g. Verify the routing table. R1# show ip route



# Practical No - 2

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

**Topology :**



**Objective :**

* Use BGP commands to prevent private AS numbers from being advertised to the outside world.
* Use the AS\_PATH attribute to filter BGP routes based on their source AS number

**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.

1. You can copy and paste the following configurations into your routers to begin.

**Router R1 (hostname Andheri)**

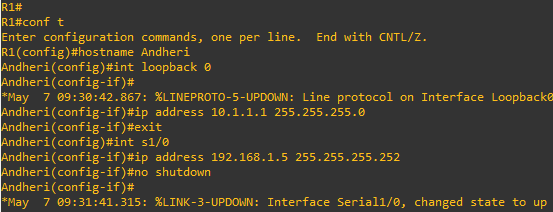
Andheri(config)# interface Loopback0

Andheri(config-if)# ip address 10.1.1.1 255.255.255.0 Andheri(config-if)# exit

Andheri(config)# interface Serial0/0/0

Andheri(config-if)# ip address 192.168.1.5 255.255.255.252 Andheri(config-if)# no shutdown

Andheri(config-if)# end Andheri#



#### Router R2 (hostname Bandra)

Bandra(config)# interface Loopback0

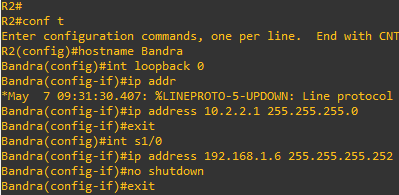
Bandra(config-if)# ip address 10.2.2.1 255.255.255.0 Bandra(config-if)# interface Serial0/0/0

Bandra(config-if)# ip address 192.168.1.6 255.255.255.252 Bandra(config-if)# no shutdown

Bandra(config-if)# exit Bandra(config)# interface Serial0/0/1

Bandra(config-if)# ip address 172.24.1.17 255.255.255.252 Bandra(config-if)# no shutdown

Bandra(config-if)# end Bandra#



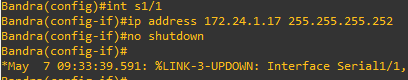
**Router R3 (hostname ChurchGate)** Churchgate(config)# interface Loopback0 Churchgate(config-if)# ip address 10.3.3.1 255.255.255.0 Churchgate(config-if)# exit

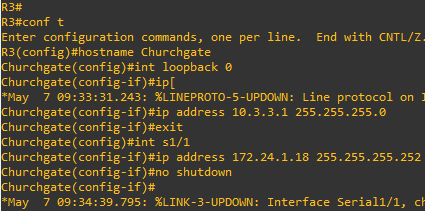
Churchgate(config)# interface Serial0/0/1

Churchgate(config-if)# ip address 172.24.1.18 255.255.255.252 Churchgate(config-if)# no shutdown

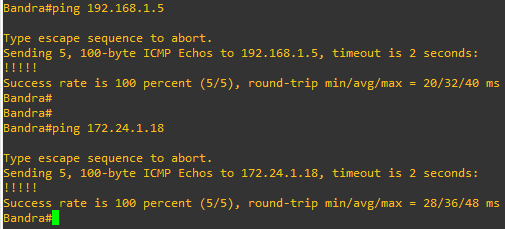
Churchgate(config-if)# end

Churchgate#





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

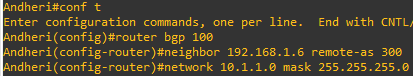


### Step 3 : Configure BGP.

1. 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.

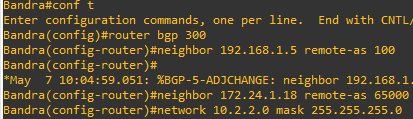
Andheri(config)# router bgp 100

Andheri(config-router)# neighbor 192.168.1.6 remote-as 300 Andheri(config-router)# network 10.1.1.0 mask 255.255.255.0



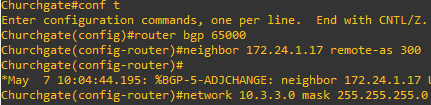
Bandra(config)# router bgp 300

Bandra(config-router)# neighbor 192.168.1.5 remote-as 100 Bandra(config-router)# neighbor 172.24.1.18 remote-as 65000 Bandra(config-router)# network 10.2.2.0 mask 255.255.255.0



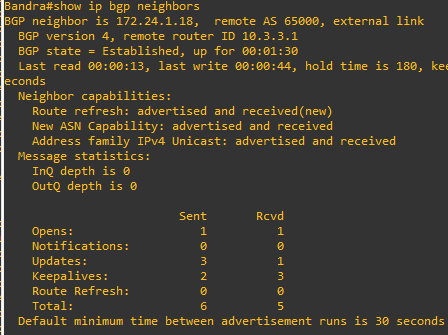
Churchgate(config)# router bgp 65000

Churchgate(config-router)# neighbor 172.24.1.17 remote-as 300 Churchgate(config-router)# network 10.3.3.0 mask 255.255.255.0



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

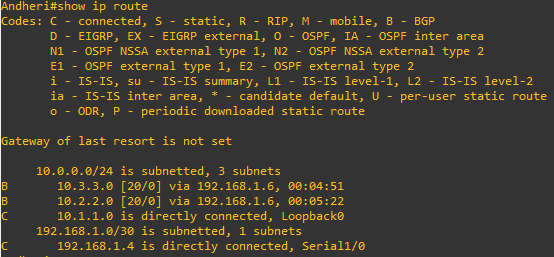
Bandra# show ip bgp neighbors



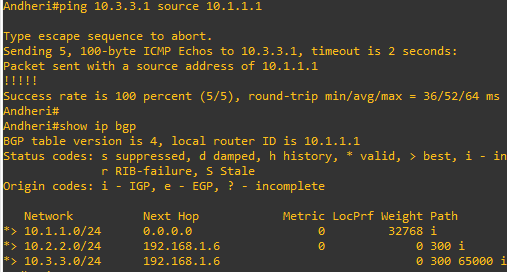
### Step 4 : Remove the private AS.

a. DBandralay the Andheri routing table using the show ip route command. Andheri should have a route to both 10.2.2.0 and 10.3.3.0. Troubleshoot if necessary.

Andheri#show ip route

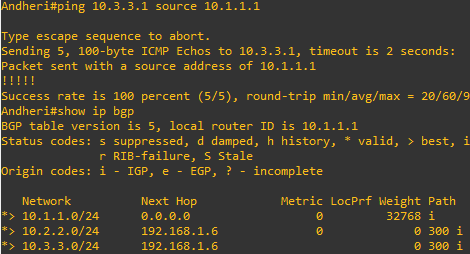


b . Ping again, this time as an extended ping, sourcing from the Loopback0 interface address. **ping 10.3.3.1 source 10.1.1.1 or ping 10.3.3.1 source Lo0**



c.Now check the BGP table on Andheri. The AS\_ PATH to the 10.3.3.0 network should be AS 300. It no longer has the private AS in the path.

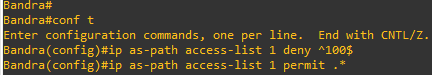
Andheri# show ip bgp



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

1. 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 Bandra.

Bandra(config)# ip as-path access-list 1 deny ^100$ Bandra(config)# ip as-path access-list 1 permit .\*



1. Apply the configured access list using the neighbor command with the filter-list option.

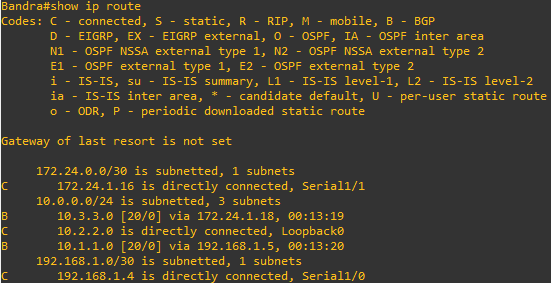
Bandra(config)# router bgp 300

Bandra (config-router)# neighbor 192.168.1.5 remove-private-as



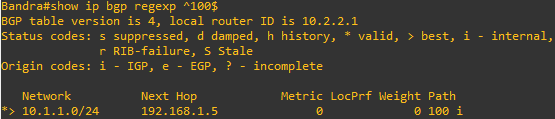
1. Use the clear ip bgp \* command to reset the routing information. Wait several seconds and then check the routing table for BANDRA. The route to 10.1.1.0 should be in the routing table.

Andheri# show ip route

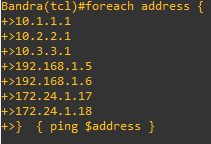


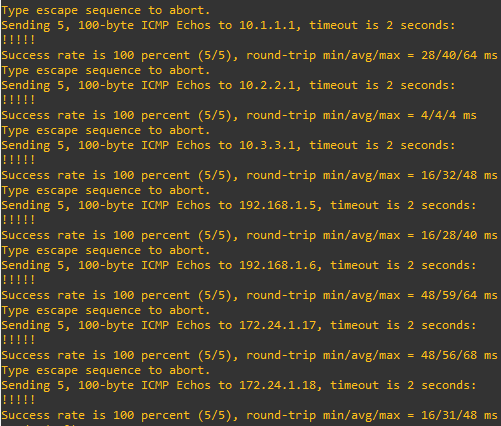
1. Return to BANDRA and verify that the filter is working as intended.

Bandra# show ip bgp regexp ^100$



1. Run the following Tcl script on all routers to verify whether there is connectivity. All pings from BANDRA should be successful. Andheri should not be able to ping the Churchgate loopback 10.3.3.1 or the WAN link 172.24.1.16/30. Churchgate should not be able to ping the Andheri loopback 10.1.1.1 or the WAN link 192.168.1.4/30.

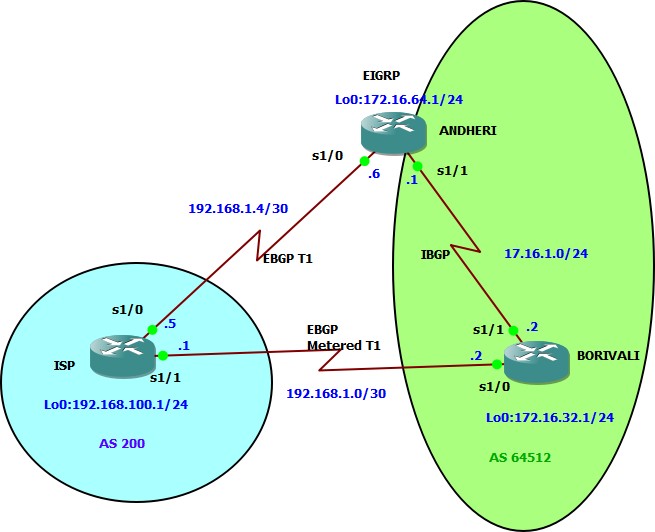




# Practical No - 3

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

**Topology :**



**Objectives**

* For IBGP peers to correctly exchange routing information, use the **next-hop-self** command with the **Local-Preference** and **MED** attributes.
* Ensure that the flat-rate, unlimited-use T1 link is used for sending and receiving data to and from the AS 200 on ISP and that the metered T1 only be used in the event that the primary T1 link has failed.

#### Step 1: Configure interface addresses.

##### Router R1 (hostname ISP)

ISP(config)# **interface Loopback0**

ISP(config-if)# **ip address 192.168.100.1 255.255.255.0**

ISP(config-if)# **exit**

ISP(config)# **interface Serial0/0/0**

ISP(config-if)# **ip address 192.168.1.5 255.255.255.252**

ISP(config-if)# **no shutdown**

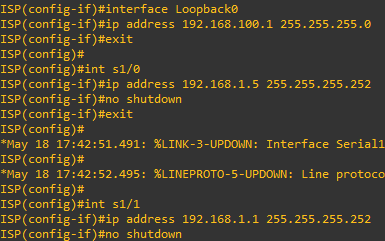
ISP(config-if)# **exit**

ISP(config)# **interface Serial0/0/1**

ISP(config-if)# **ip address 192.168.1.1 255.255.255.252**

ISP(config-if)# **no shutdown**

ISP(config-if)# **end**



##### Router R2 (hostname Andheri)

Andheri(config)# **interface Loopback0**

Andheri(config-if)# **ip address 172.16.64.1 255.255.255.0**

Andheri (config-if)# **exit**

Andheri (config)# **interface Serial0/0/0**

Andheri (config-if)# **ip address 192.168.1.6 255.255.255.252**

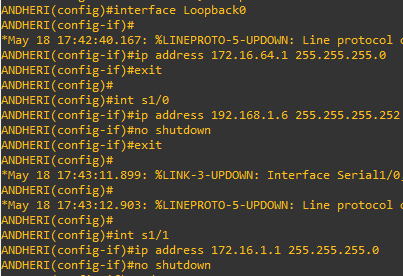
Andheri (config-if)# **no shutdown**

Andheri (config-if)# **exit** Andheri (config)# **interface Serial0/0/1**

Andheri(config-if)# **ip address 172.16.1.1 255.255.255.0**

Andheri(config-if)# **no shutdown**

Andheri(config-if)# **end**



##### Router R3 (hostname Borivali)

Borivali (config)# **interface Loopback0**

Borivali (config-if)# **ip address 172.16.32.1 255.255.255.0**

Borivali (config-if)# **exit**

SanJose2(config)# **interface Serial0/0/0**

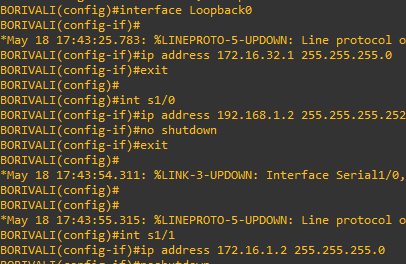
SanJose2(config-if)# **ip address 192.168.1.2 255.255.255.252**

SanJose2(config-if)# **no shutdown** SanJose2(config-if)# **exit** SanJose2(config)# **interface Serial0/0/1**

SanJose2(config-if)# **ip address 172.16.1.2 255.255.255.0**

SanJose2(config-if)# **no shutdown**

SanJose2(config-if)# **end**



#### 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.)

SanJose1(config)# **router eigrp 1**

SanJose1(config-router)# **network 172.16.0.0**



SanJose2(config)# **router eigrp 1**

SanJose2(config-router)# **network 172.16.0.0**



#### Step 3: Configure IBGP and verify BGP neighbors.

* 1. Configure IBGP between the SanJose1 and SanJose2 routers. On the SanJose1 router, enter the following configuration.

SanJose1(config)# **router bgp 64512**

SanJose1(config-router)# **neighbor 172.16.32.1 remote-as 64512**

SanJose1(config-router)# **neighbor 172.16.32.1 update-source lo0**



If multiple pathways to the BGP neighbor exist, the router can use multiple IP interfaces to communicate with the neighbor. The source IP address therefore depends on the outgoing interface. The **update-source**

**lo0** command instructs the router to use the IP address of the interface Loopback0 as the source IP address for all BGP messages sent to that neighbor.

* 1. Complete the IBGP configuration on SanJose2 using the following commands. SanJose2(config)# **router bgp 64512**

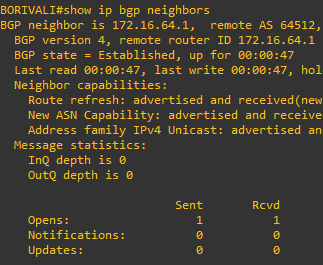
SanJose2(config-router)# **neighbor 172.16.64.1 remote-as 64512**

SanJose2(config-router)# **neighbor 172.16.64.1 update-source lo0**



* 1. Verify that SanJose1 and SanJose2 become BGP neighbors by issuing the **show ip bgp neighbors** command on SanJose1. View the following partial output. If the BGP state is not established, troubleshoot the connection.

SanJose2# **show ip bgp neighbors**



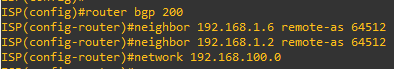
#### Step 4: Configure EBGP and verify BGP neighbors.

* 1. Configure ISP to run EBGP with SanJose1 and SanJose2. Enter the following commands on ISP. ISP(config)# **router bgp 200**

ISP(config-router)# **neighbor 192.168.1.6 remote-as 64512**

ISP(config-router)# **neighbor 192.168.1.2 remote-as 64512**

ISP(config-router)# **network 192.168.100.0**



* 1. 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.

SanJose1(config)# **ip route 172.16.0.0 255.255.0.0 null0**



* 1. Configure SanJose1 as an EBGP peer to ISP. SanJose1(config)# **router bgp 64512**

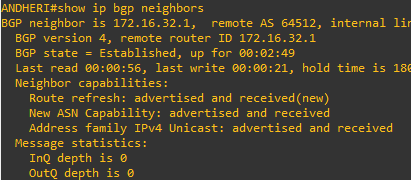
SanJose1(config-router)# **neighbor 192.168.1.5 remote-as 200**

SanJose1(config-router)# **network 172.16.0.0**



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

SanJose1# **show ip bgp neighbors**

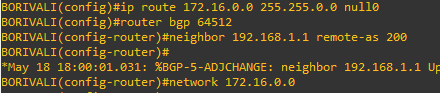


Configure a discard static route for 172.16.0.0/16 on SanJose2 and as an EBGP peer to ISP. SanJose2(config)# **ip route 172.16.0.0 255.255.0.0 null0**

SanJose2(config)# **router bgp 64512**

SanJose2(config-router)# **neighbor 192.168.1.1 remote-as 200**

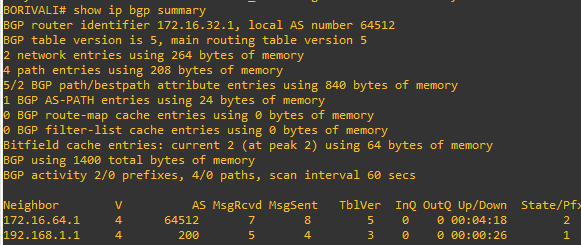
SanJose2(config-router)# **network 172.16.0.0**



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

In Step 4, the **show ip bgp neighbors** command was used to verify that SanJose1 and ISP had reached the established state. A useful alternative command is **show ip bgp summary**. The output should be similar to the following.

SanJose2# **show ip bgp summary**



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

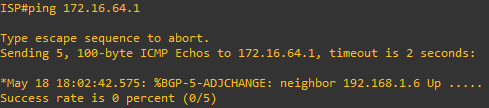
1. Clear the IP BGP conversation with the **clear ip bgp \*** command on ISP. Wait for the conversations to reestablish with each SanJose router.

ISP# **clear ip bgp \***

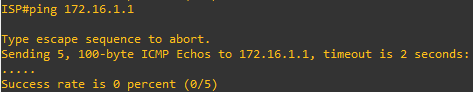


1. Test whether ISP can ping the loopback 0 address of 172.16.64.1 on SanJose1 and the serial link between SanJose1 and SanJose2, 172.16.1.1.

ISP# **ping 172.16.64.1**

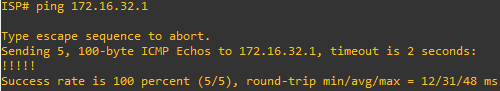


ISP# **ping 172.16.1.1**

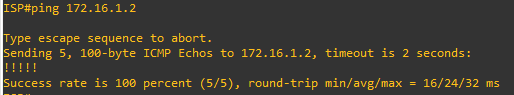


1. Now ping from ISP to the loopback 0 address of 172.16.32.1 on SanJose2 and the serial link between SanJose1 and SanJose2, 172.16.1.2.

ISP# **ping 172.16.32.1**

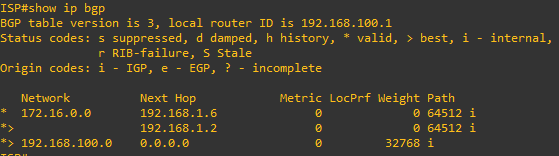


ISP# **ping 172.16.1.2**



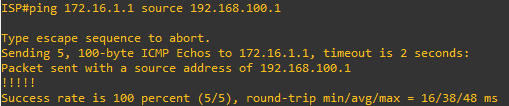
1. Issue the **show ip bgp** command on ISP to verify BGP routes and metrics.

ISP# **show ip bgp**

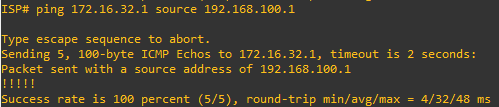


* 1. At this point, the ISP router should be able to get to each network connected to SanJose1 and SanJose2 from the loopback address 192.168.100.1. Use the extended **ping** command and specify the source address of ISP Lo0 to test.

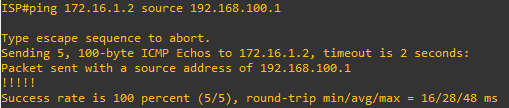
##### ISP# ping 172.16.1.1 source 192.168.100.1



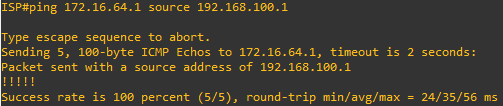
ISP# **ping 172.16.32.1 source 192.168.100.1**



##### ISP# ping 172.16.1.2 source 192.168.100.1



ISP# **ping 172.16.64.1 source 192.168.100.1**

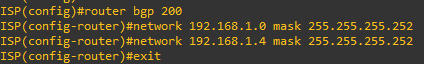


#### Step 7: Configure the BGP next-hop-self feature.

1. Issue the following commands on the ISP router. ISP(config)# **router bgp 200**

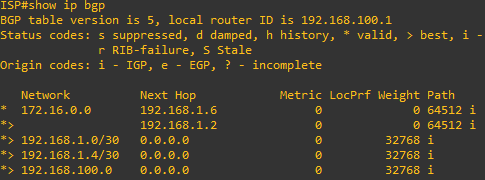
ISP(config-router)# **network 192.168.1.0 mask 255.255.255.252**

ISP(config-router)# **network 192.168.1.4 mask 255.255.255.252**



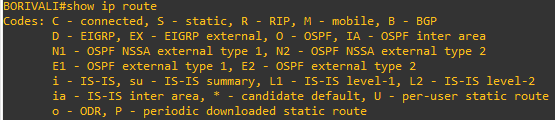
1. Issue the **show ip bgp** command to verify that the ISP is correctly injecting its own WAN links into BGP.

ISP# **show ip bgp**



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

SanJose2# **show ip route**



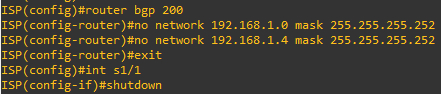
1. To better understand the **next-hop-self** command we will remove ISP advertising its two WAN links and shutdown the WAN link between ISP and SanJose2. The only possible path from SanJose2 to ISP’s 192.168.100.0/24 is through SanJose1.

ISP(config)# **router bgp 200**

ISP(config-router)# **no network 192.168.1.0 mask 255.255.255.252**

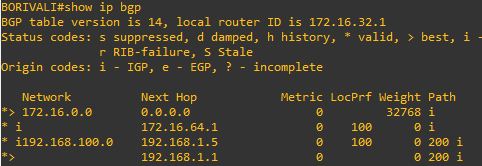
ISP(config-router)# **no network 192.168.1.4 mask 255.255.255.252**

ISP(config-router)# **exit** ISP(config)# **interface serial 0/0/1** ISP(config-if)# **shutdown**

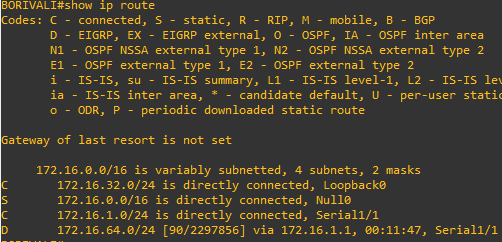


1. Display SanJose2’s BGP table using the **show ip bgp** command and the IPv4 routing table with

**show ip route**. SanJose2# **show ip bgp**



SanJose2# **show ip route**



SanJose1(config)# **router bgp 64512**

SanJose1(config-router)# **neighbor 172.16.32.1 next-hop-self**



SanJose2(config)# **router bgp 64512**

SanJose2(config-router)# **neighbor 172.16.64.1 next-hop-self**



1. Reset BGP operation on either router with the **clear ip bgp \*** command. SanJose1# **clear ip bgp \***

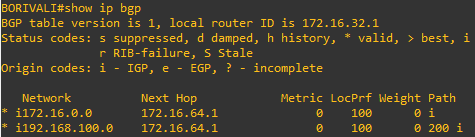


SanJose2# **clear ip bgp \***



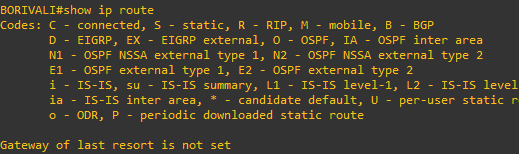
1. After the routers have returned to established BGP speakers, issue the **show ip bgp** command on SanJose2 and notice that the next hop is now SanJose1 instead of ISP.

SanJose2# **show ip bgp**



1. 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.

SanJose2# **show ip route**



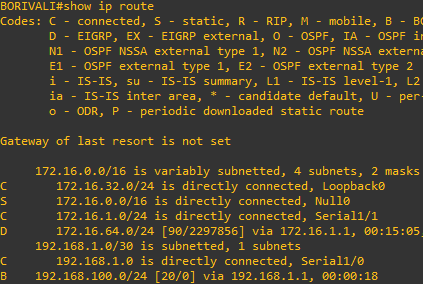
1. Before configuring the next BGP attribute, restore the WAN link between ISP and SanJose3. This will change the BGP table and routing table on both routers. For example, SanJose2’s routing table shows 192.168.100.0/24 will now have a better path through ISP.

ISP(config)# **interface serial 0/0/1**

ISP(config-if)# **no shutdown**



SanJose2# **show ip route**



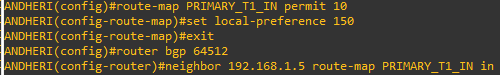
#### Step 8: Set BGP local preference.

1. 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.

SanJose1(config)# **route-map PRIMARY\_T1\_IN permit 10** SanJose1(config-route-map)# **set local-preference 150** SanJose1(config-route-map)# **exit**

SanJose1(config)# **router bgp 64512**

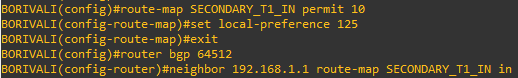
SanJose1(config-router)# **neighbor 192.168.1.5 route-map PRIMARY\_T1\_IN in**



SanJose2(config)# **route-map SECONDARY\_T1\_IN permit 10** SanJose2(config-route-map)# **set local-preference 125** SanJose1(config-route-map)# **exit**

SanJose2(config)# **router bgp 64512**

SanJose2(config-router)# **neighbor 192.168.1.1 route-map SECONDARY\_T1\_IN in**



1. 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.

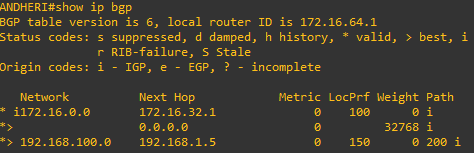
SanJose1# **clear ip bgp \* soft**



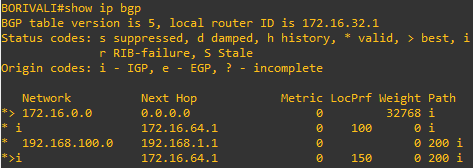
SanJose2# **clear ip bgp \* soft**



SanJose1# **show ip bgp**



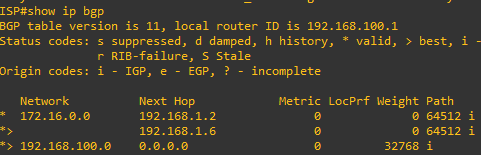
SanJose2# **show ip bgp**



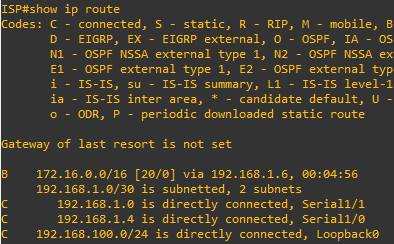
#### Step 9: Set BGP MED.

1. 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.

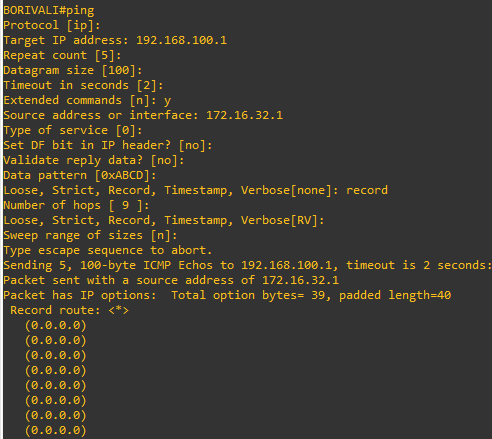
ISP# **show ip bgp**

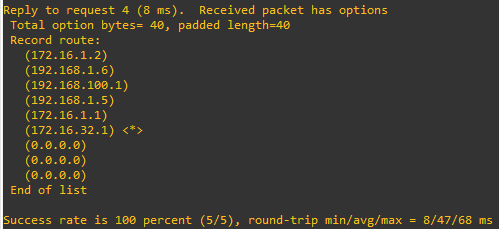


ISP# **show ip route**



1. 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





If you are unfamiliar with the **record** option, the important thing to note is that each IP address in

brackets is an outgoing interface. The output can be interpreted as follows:

1. A ping that is sourced from 172.16.32.1 exits SanJose2 through s0/0/1, 172.16.1.2. It then arrives at the s0/0/1 interface for SanJose1.
2. SanJose1 S0/0/0, 192.168.1.6, routes the packet out to arrive at the S0/0/0 interface of ISP. 3. The target of 192.168.100.1 is reached: 192.168.100.1.
3. The packet is next forwarded out the S0/0/1, 192.168.1.1 interface for ISP and arrives at the S0/0/0 interface for SanJose2.
4. SanJose2 then forwards the packet out the last interface, loopback 0, 172.16.32.1.

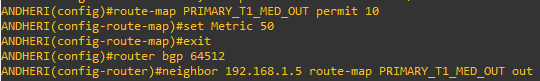
Although the unlimited use of the T1 from SanJose1 is preferred here, ISP currently takes the link from SanJose2 for all return traffic.

1. 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.

SanJose1(config)#**route-map PRIMARY\_T1\_MED\_OUT permit 10**

SanJose1(config-route-map)#**set Metric 50** SanJose1(config-route-map)#**exit** SanJose1(config)#**router bgp 64512**

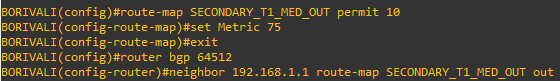
SanJose1(config-router)#**neighbor 192.168.1.5 route-map PRIMARY\_T1\_MED\_OUT out**



SanJose2(config)#**route-map SECONDARY\_T1\_MED\_OUT permit 10**

SanJose2(config-route-map)#**set Metric 75** SanJose2(config-route-map)#**exit** SanJose2(config)#**router bgp 64512**

SanJose2(config-router)#**neighbor 192.168.1.1 route-map SECONDARY\_T1\_MED\_OUT out**



1. 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.

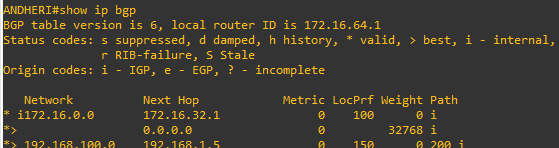
SanJose1# **clear ip bgp \* soft**



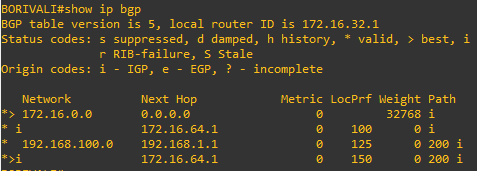
SanJose2# **clear ip bgp \* soft**



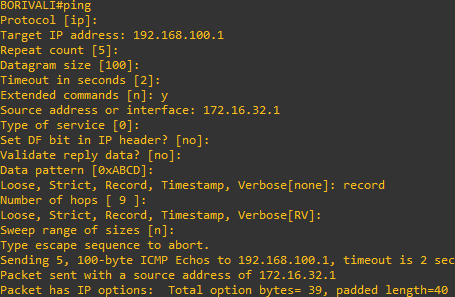
SanJose1# **show ip bgp**

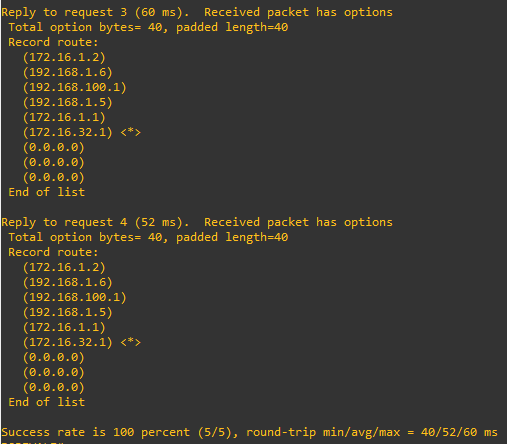


SanJose2# **show ip bgp**

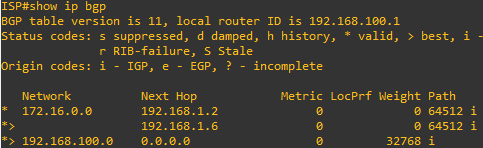


Reissue an extended **ping** command with the **record** command. Notice the change in return path using the exit interface 192.168.1.5 to SanJose1.





ISP# **show ip bgp**



#### 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.

1. 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.

ISP(config)# **router bgp 200**

ISP(config-router)# **neighbor 192.168.1.6 default-originate**

ISP(config-router)# **neighbor 192.168.1.2 default-originate**

ISP(config-router)# **exit**

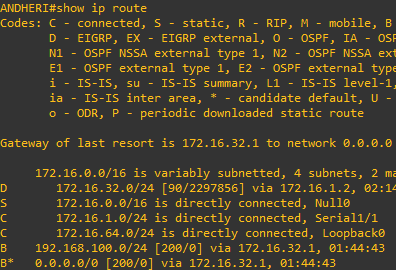
ISP(config)# **interface loopback 10**

ISP(config-if)# **ip address 10.0.0.1 255.255.255.0**

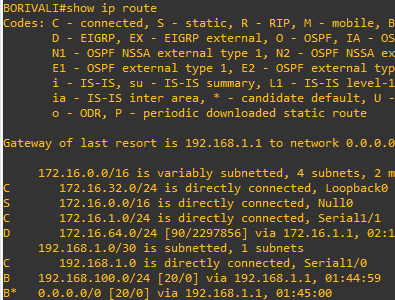


1. Verify that both routers have received the default route by examining the routing tables on SanJose1 and SanJose2. Notice that both routers prefer the route between SanJose1 and ISP.

SanJose1# **show ip route**

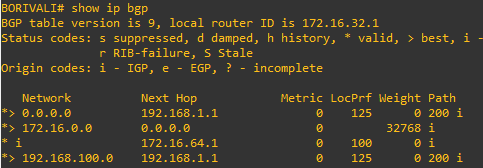


SanJose2# **show ip route**



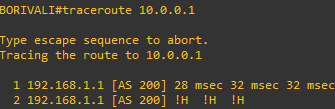
1. The preferred default route is by way of SanJose1 because of the higher local preference attribute configured on SanJose1 earlier.

SanJose2# **show ip bgp**



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

SanJose2# **traceroute 10.0.0.1**



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

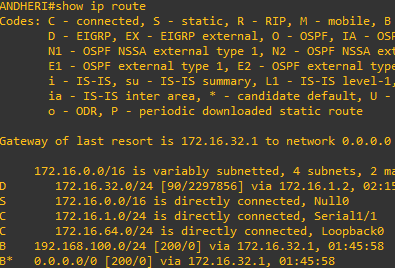
ISP(config)# **interface serial 0/0/0**

ISP(config-if)# **shutdown**

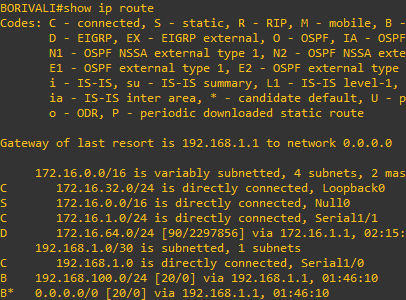


1. Verify that both routers are modified their routing tables with the default route using the path between SanJose2 and ISP.

SanJose1# **show ip route**

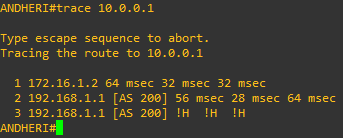


SanJose2# **show ip route**



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

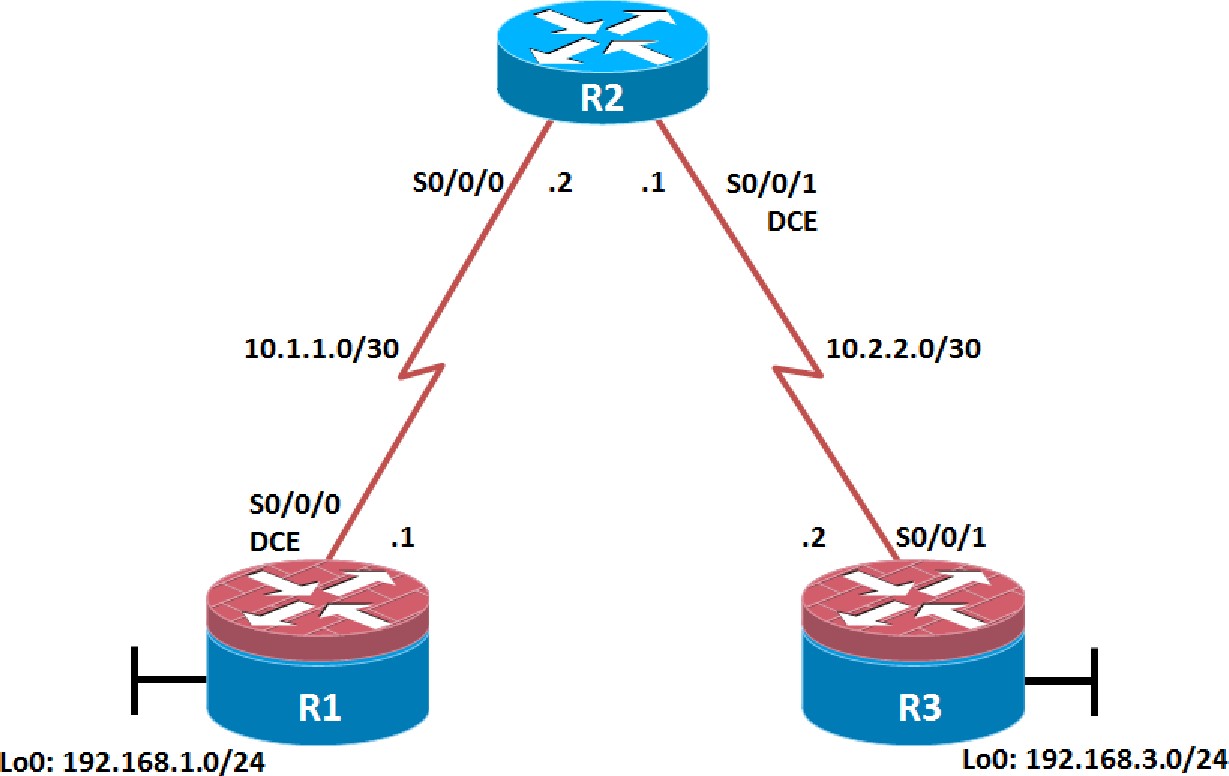
SanJose1# **trace 10.0.0.1**



**Practical No – 4**

**Aim**: Secure the Management Plane

**Topology:**



## Objectives :

* Secure management access.
* Configure enhanced username password security.
* Enable AAA RADIUS authentication.
* Enable secure remote management.

#### 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. You can copy and paste the following configurations into your routers to begin.

##### Router R1

interface Loopback 0

ip address 192.168.1.1 255.255.255.0

exit

interface Serial0/0/0

ip address 10.1.1.1 255.255.255.252

no shutdown exit

end

##### Router R2

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

no shutdown exit

interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

no shutdown exit

end

##### Router R3

interface Loopback0

ip address 192.168.3.1 255.255.255.0

exit

interface Serial0/0/1

ip address 10.2.2.2 255.255.255.252

no shutdown exit

end

#### Step 2: Configure static routes.

R1(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.2**

R3(config)# **ip route 0.0.0.0 0.0.0.0 10.2.2.1**

R2(config)# **ip route 192.168.1.0 255.255.255.0 10.1.1.1**

R2(config)# **ip route 192.168.3.0 255.255.255.0 10.2.2.2**

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 } Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:

!!!!!

#### Step 3: Secure management access.

1. On R1, use the **security passwords** command to set a minimum password length of 10 characters. R1(config)# **security passwords min-length 10**
2. Configure the enable secret encrypted password on both routers. R1(config)# **enable secret class12345**
3. 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.

R1(config)# **line console 0**

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

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

R1(config-line)# **exit**

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

R1(config-line)# **password ciscovtypass**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **login**

R1(config-line)# **exit**

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

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

1. Enter privileged EXEC mode and issue the **show run** command. Can you read the enable secret password? Why or why not?

R1(config) # **service password-encryption**

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

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

R1(config)# **exit**

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

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

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

R1(config)# **username ADMIN secret class54321**

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

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

R1(config-line)# **exit**

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

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

R1(config-line)# **end**

1. Repeat the steps 4a to 4c on R3.
2. To verify the configuration, telnet to R3 from R1 and login using the ADMIN local database account.

R1# **telnet 10.2.2.2**

Trying 10.2.2.2 ... Open

Unauthorized access strictly prohibited! User Access Verification

Username: **ADMIN**

Password:

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

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

R1(config)# **radius server RADIUS-1**

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

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

R1(config)# **radius server RADIUS-2**

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

1. Assign both RADIUS servers to a server group. R1(config)# **aaa group server radius RADIUS-GROUP** R1(config-sg-radius)# **server name RADIUS-1** R1(config-sg-radius)# **server name RADIUS-2**

R1(config-sg-radius)# **exit**

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

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

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

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

Alter the VTY lines to use the TELNET-LOGIN AAA authentiaito0n method. R1(config)# **line vty 0 4**

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

R1(config-line)# **exit**

Repeat the steps 5a to 5g on R3.

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

R1# **telnet 10.2.2.2**

Trying 10.2.2.2 ... Open

Unauthorized access strictly prohibited! User Access Verification

Username: **admin**

Password:

Authentication failed

Username: **ADMIN**

Password:

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

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

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

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

R1(config)# **crypto key zeroize rsa**

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

##### R1(config)# crypto key generate rsa general-keys modulus 1024

The name for the keys will be: R1.ccnasecurity.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK] R1(config)#

Jan 10 13:44:44.711: %SSH-5-ENABLED: SSH 1.99 has been enabled

1. Cisco routers support two versions of SSH:

* **SSH version 1 (SSHv1)**: Original version but has known vulnerabilities.
* **SSH version 2 (SSHv2)**: Provides better security using the Diffie-Hellman key exchange and the strong integrity-checking message authentication code (MAC).

Configure SSH version 2 on R1. R1(config)# **ip ssh version 2** R1(config)#

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

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

R1(config-line)# **end**

1. Verify the SSH configuration using the **show ip ssh** command. R1# **show ip ssh**

SSH Enabled - version 2.0

Authentication timeout: 120 secs; Authentication retries: 3 Minimum expected Diffie Hellman key size : 1024 bits IOS Keys in SECSH format(ssh-rsa, base64 encoded):

ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAAAgQC3Lehh7ReYlgyDzls6wq+mFzxqzoaZFr9XGx+Q/ yio

dFYw00hQo80tZy1W1Ff3Pz6q7Qi0y00urwddHZ0kBZceZK9EzJ6wZ+9a87KKDETCWrGSLi6c8lE/y4K+ Z/oVrMMZk7bpTM1MFdP41YgkTf35utYv+TcqbsYo++KJiYk+xw==

1. Repeat the steps 6a to 6f on R3.
2. 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.

##### R1# ssh -l ADMIN 10.2.2.2

Password:

Unauthorized access strictly prohibited! R3>

R3> **en**

Password:

R3#

##### Device Configurations Router R1

service password-encryption hostname R1

security passwords min-length 10

enable secret 5 $1$t6eK$FZ.JdmMLj8QSgNkpChyZz. aaa new-model

aaa group server radius RADIUS-GROUP server name RADIUS-1

server name RADIUS-2

aaa authentication login default group RADIUS-GROUP local

aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case ip domain name ccnasecurity.com

username JR-ADMIN secret 5 $1$0u0q$lwimCZIAuQtV4C1ezXL1S0 username ADMIN secret 5 $1$NSVD$/YjzB7Auyes1sAt4qMfpd.

ip ssh version 2 interface Loopback0 description R1 LAN

ip address 192.168.1.1 255.255.255.0

interface Serial0/0/0 description R1 --> R2

ip address 10.1.1.1 255.255.255.252

no fair-queue

ip route 0.0.0.0 0.0.0.0 10.1.1.2

radius server RADIUS-1

address ipv4 192.168.1.101 auth-port 1645 acct-port 1646

key 7 107C283D2C2221465D493A2A717D24653017

radius server RADIUS-2

address ipv4 192.168.1.102 auth-port 1645 acct-port 1646

key 7 03367A2F2F3A12011C44090442471C5C162E

banner motd ^CUnauthorized access strictly prohibited!^C

line con 0

exec-timeout 5 0

password 7 070C285F4D061A0A19020A1F17

logging synchronous line aux 0

no exec

password 7 060506324F411F0D1C0713181F

login authentication TELNET-LOGIN transport input ssh

end

##### Router R2

hostname R2

enable secret 5 $1$DJS7$xvJDW87zLs8pSJDFUlCPB1 interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

no fair-queue

interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

clock rate 128000

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

line con 0

exec-timeout 0 0 logging synchronous

line vty 0 4 password cisco login

end

##### Router R3

service password-encryption

hostname R3

security passwords min-length 10

enable secret 5 $1$5OY4$4J6VFlvGNKjwQ8XtajgUk1 aaa new-model

aaa group server radius RADIUS-GROUP server name RADIUS-1

server name RADIUS-2

aaa authentication login default group RADIUS-GROUP local

aaa authentication login TELNET-LOGIN group RADIUS-GROUP local-case ip domain name ccnasecurity.com

username JR-ADMIN secret 5 $1$b4m1$RVmjL9S3gxKh1xr8qzNqr/ username ADMIN secret 5 $1$zGV7$pVgSEbinvXQ7f7uyxeKBj

ip ssh version 2

interface Loopback0 description R3 LAN

ip address 192.168.3.1 255.255.255.0

interface Serial0/0/1 description R3 --> R2

ip address 10.2.2.2 255.255.255.252

ip route 0.0.0.0 0.0.0.0 10.2.2.1

radius server RADIUS-1

address ipv4 192.168.1.101 auth-port 1645 acct-port 1646

key 7 01212720723E354270015E084C5000421908

radius server RADIUS-2

address ipv4 192.168.1.102 auth-port 1645 acct-port 1646

key 7 003632222D6E384B5D6C5C4F5C4C1247000F

banner motd ^CUnauthorized access strictly prohibited!^C

line con 0

exec-timeout 5 0

password 7 104D000A0618110402142B3837

logging synchronous

line aux 0 no exec

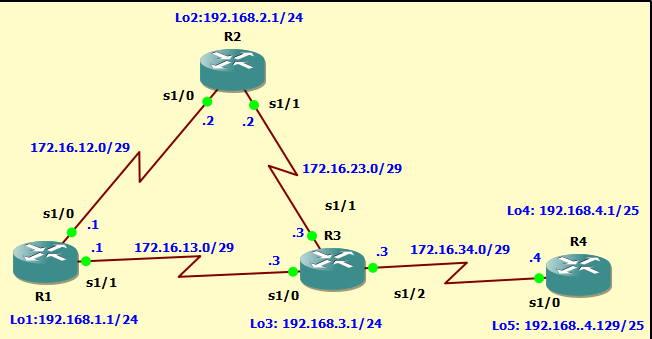
line vty 0 4

exec-timeout 5 0

password 7 070C285F4D060F110E020A1F17

login authentication TELNET-LOGIN transport input ssh

end

**Practical No - 5**

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

## Objectives

* Configure and verify policy-based routing.
* Select the required tools and commands to configure policy-based routing operations.
* Verify the configuration and operation by using the proper show and debug commands.

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

1. Cable the network as shown in the topology diagram. Erase the startup configuration, and reload each router to clear previous configurations.
2. 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.

You can copy and paste the following configurations into your routers to begin.

**Note**: Depending on the router model, interfaces might be numbered differently than those listed. You might need to alter them accordingly.

##### Router R1

interface Lo1

ip address 192.168.1.1 255.255.255.0

nterface Serial0/0/0

ip address 172.16.12.1 255.255.255.248

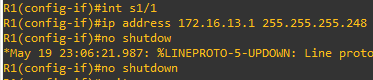
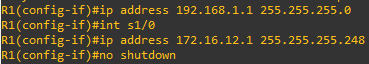
no shutdown

interface Serial0/0/1

ip address 172.16.13.1 255.255.255.248

no shutdown End





##### Router R2

interface Lo2

ip address 192.168.2.1 255.255.255.0

interface Serial0/0/0

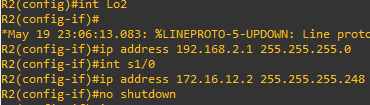
ip address 172.16.12.2 255.255.255.248

no shutdown

interface Serial0/0/1

ip address 172.16.23.2 255.255.255.248

no shutdown End





##### Router R3

interface Lo3

ip address 192.168.3.1 255.255.255.0

interface Serial0/0/0

ip address 172.16.13.3 255.255.255.248

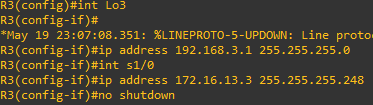
no shutdown interface Serial0/0/1

ip address 172.16.23.3 255.255.255.248

no shutdown interface Serial0/1/0

ip address 172.16.34.3 255.255.255.248

no shutdown End





##### Router R4

interface Lo4

ip address 192.168.4.1 255.255.255.128

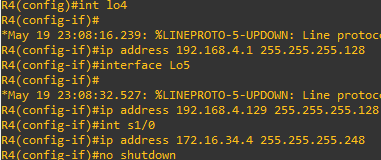
interface Lo5

ip address 192.168.4.129 255.255.255.128

interface Serial0/0/0

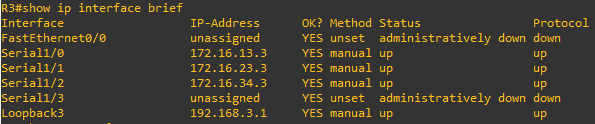
ip address 172.16.34.4 255.255.255.248

no shutdown End

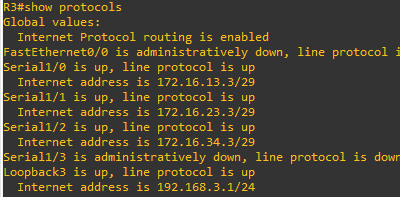


1. Verify the configuration with the **show ip interface brief**, **show protocols,** and **show interfaces description** commands. The output from router R3 is shown here as an example.

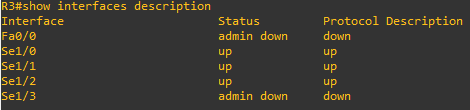
##### R3# show ip interface brief



R3# **show protocols**



R3# **show interfaces description**



**Step 3: Configure basic EIGRP.**

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

bb. 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.

You can copy and paste the following configurations into your routers.

##### Router R1

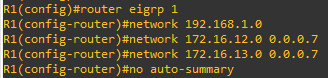
router eigrp 1

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

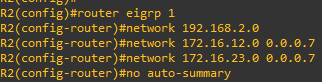
router eigrp 1

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

router eigrp 1

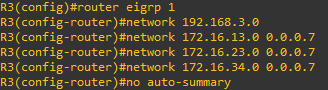
network 192.168.3.0

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



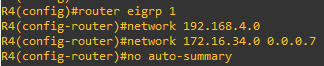
##### Router R4

router eigrp 1

network 192.168.4.0

network 172.16.34.0 0.0.0.7

no auto-summary

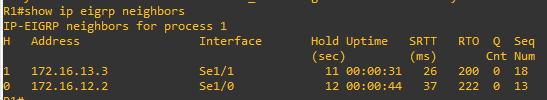


You should see EIGRP neighbor relationship messages being generated.

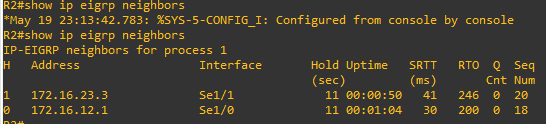
#### Step 4: Verify EIGRP connectivity.

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

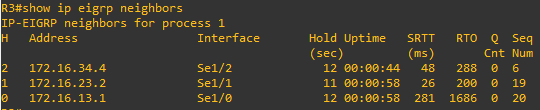
##### R1# show ip eigrp neighbors



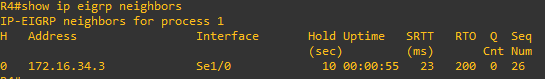
R2# **show ip eigrp neighbors**



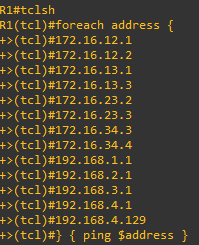
##### R3# show ip eigrp neighbors

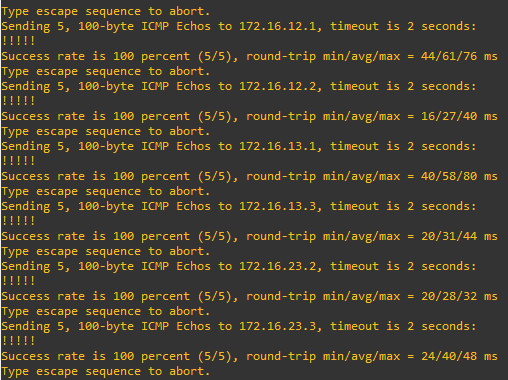


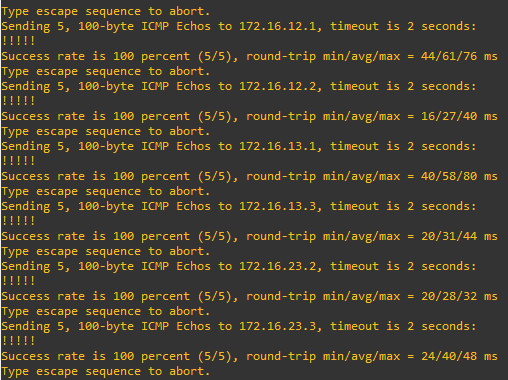
R4# **show ip eigrp neighbors**



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

R1# **tclsh**



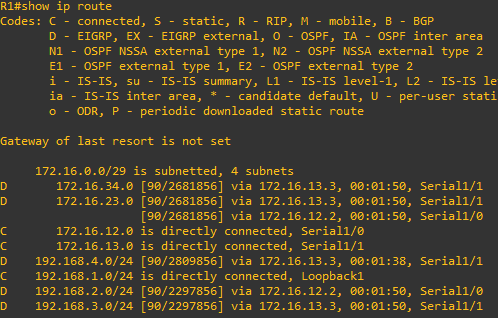


#### Step 5: Verify the current path.

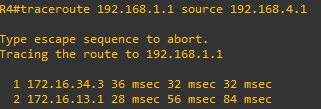
Before you configure PBR, verify the routing table on R1.

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

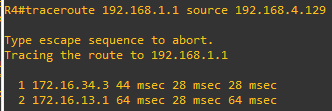
R1# **show ip route**



##### R4# traceroute 192.168.1.1 source 192.168.4.1

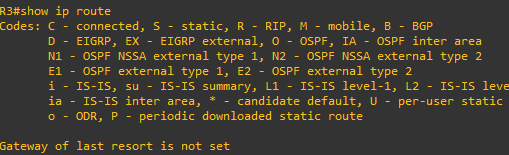


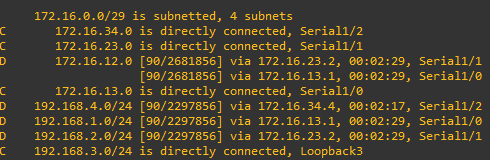
R4# **traceroute 192.168.1.1 source 192.168.4.129**



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 S0/0/1.

R3# **show ip route**

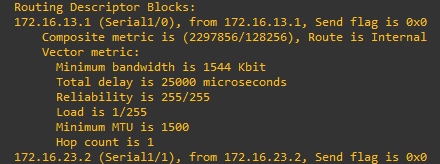
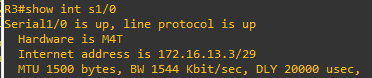




R3#

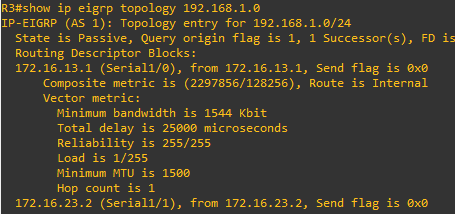
ff. On R3, use the **show interfaces serial 0/0/0** and **show interfaces s0/0/1** commands.

##### R3# show interfaces serial0/0/0



gg. 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.

R3# **show ip eigrp topology 192.168.1.0**



#### Step 6: Configure PBR to provide path control.

The steps required to implement path control include the following:

* Choose the path control tool to use. Path control tools manipulate or bypass the IP routing table. For PBR, **route-map** commands are used.
* Implement the traffic-matching configuration, specifying which traffic will be manipulated. The

**match** commands are used within route maps.

* Define the action for the matched traffic using **set** commands within route maps.
* Apply the route map to incoming traffic.

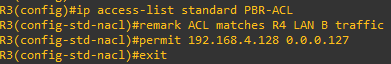
As a test, you will configure the following policy on router R3:

* All traffic sourced from R4 LAN A must take the R3 --> R2 --> R1 path.
* All traffic sourced from R4 LAN B must take the R3 --> R1 path.

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

R3(config)# **ip access-list standard PBR-ACL**

R3(config-std-nacl)# **remark ACL matches R4 LAN B traffic** R3(config-std-nacl)# **permit 192.168.4.128 0.0.0.127** R3(config-std-nacl)# **exit**



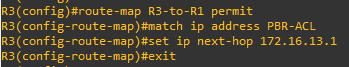
R3(config)#

* 1. Create a route map called **R3-to-R1** that matches PBR-ACL and sets the next-hop interface to the R1 serial 0/0/1 interface.

R3(config)# **route-map R3-to-R1 permit**

R3(config-route-map)# **description RM to forward LAN B traffic to R1**

R3(config-route-map)# **match ip address PBR-ACL** R3(config-route-map)# **set ip next-hop 172.16.13.1** R3(config-route-map)# **exit**



jj. 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 S0/1/0.

R3(config)# **interface s0/1/0**

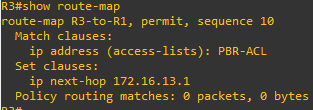
R3(config-if)# **ip policy route-map R3-to-R1**

R3(config-if)# **end**



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

R3# **show route-map**



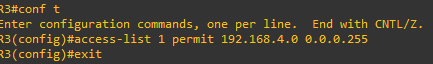
#### Step 7: Test the policy.

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

R3# **conf t**

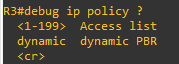
Enter configuration commands, one per line. End with CNTL/Z. R3(config)# **access-list 1 permit 192.168.4.0 0.0.0.255**

R3(config)# **exit**



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

##### R3# debug ip policy ?

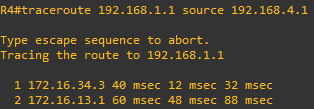


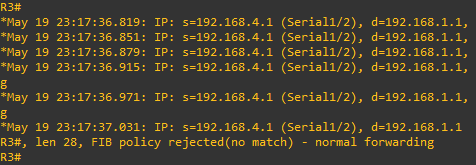
R3# **debug ip policy 1**



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

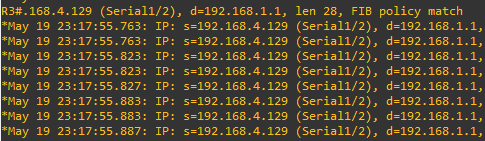
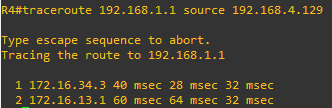
##### R4# traceroute 192.168.1.1 source 192.168.4.1





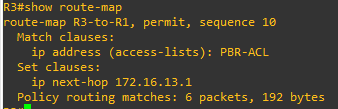
oo. Test the policy from R4 with the **traceroute** command, using R4 LAN B as the source network.

##### R4# traceroute 192.168.1.1 source 192.168.4.129



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

R3# **show route-map**



# Practical No – 6

# Aim: Configure IP SLA Tracking and Path Control

# Topology :

# 

### Objectives

* Configure and verify the IP SLA feature.
* Test the IP SLA tracking feature.
* Verify the configuration and operation using **show** and **debug** commands.

### Background

You want to experiment with the Cisco IP Service Level Agreement (SLA) feature to study how it could be of value to your organization.

At times, a link to an ISP could be operational, yet users cannot connect to any other outside Internet resources. The problem might be with the ISP or downstream from them. Although policy-based routing (PBR) can be implemented to alter path control, you will implement the Cisco IOS SLA feature to monitor this behavior and intervene by injecting another default route to a backup ISP.

To test this, you have set up a three-router topology in a lab environment. Router R1 represents a branch office connected to two different ISPs. ISP1 is the preferred connection to the Internet, while ISP2 provides a backup link. ISP1 and ISP2 can also interconnect, and both can reach the web server. To monitor ISP1 for failure, you will configure IP SLA probes to track the reachability to the ISP1 DNS server. If connectivity to the ISP1 server fails, the SLA probes detect the failure and alter the default static route to point to the ISP2 server.

**Note:** This lab uses Cisco 1941 routers with Cisco IOS Release 15.2 with IP Base. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

### Required Resources

* 3 routers (Cisco IOS Release 15.2 or comparable)
* Serial and Ethernet cables

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

1. 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.

You can copy and paste the following configurations into your routers to begin.

**Note**: Depending on the router model, interfaces might be numbered differently than those listed. You might need to alter them accordingly.

**Router R1**

hostname R1

interface Loopback 0

description R1 LAN

ip address 192.168.1.1 255.255.255.0

interface Serial0/0/0

description R1 --> ISP1

ip address 209.165.201.2 255.255.255.252

clock rate 128000

bandwidth 128

no shutdown

interface Serial0/0/1

description R1 --> ISP2

ip address 209.165.202.130 255.255.255.252

bandwidth 128

no shutdown

**Router ISP1 (R2)**

hostname ISP1

interface Loopback0

description Simulated Internet Web Server

ip address 209.165.200.254 255.255.255.255

interface Loopback1

description ISP1 DNS Server

ip address 209.165.201.30 255.255.255.255

interface Serial0/0/0

description ISP1 --> R1

ip address 209.165.201.1 255.255.255.252

bandwidth 128

no shutdown

interface Serial0/0/1

description ISP1 --> ISP2

ip address 209.165.200.225 255.255.255.252

clock rate 128000

bandwidth 128

no shutdown

**Router ISP2 (R3)**

hostname ISP2

interface Loopback0

description Simulated Internet Web Server

ip address 209.165.200.254 255.255.255.255

interface Loopback1

description ISP2 DNS Server

ip address 209.165.202.158 255.255.255.255

interface Serial0/0/0

description ISP2 --> R1

ip address 209.165.202.129 255.255.255.252

clock rate 128000

bandwidth 128

no shutdown

interface Serial0/0/1

description ISP2 --> ISP1

ip address 209.165.200.226 255.255.255.252

bandwidth 128

no shutdown

1. Verify the configuration by using the **show interfaces description** command. The output from router R1 is shown here as an example.

R1# **show interfaces description | include up**

Se0/0/0 up up R1 --> ISP1

Se0/0/1 up up R1 --> ISP2

Lo0 up up R1 LAN

R1#

All three interfaces should be active. Troubleshoot if necessary.

### Step 2: Configure static routing.

The current routing policy in the topology is as follows:

* Router R1 establishes connectivity to the Internet through ISP1 using a default static route.
* ISP1 and ISP2 have dynamic routing enabled between them, advertising their respective public address pools.
* ISP1 and ISP2 both have static routes back to the ISP LAN.

**Note:** For the purpose of this lab, the ISPs have a static route to an RFC 1918 private network address on the branch router R1. In an actual branch implementation, Network Address Translation (NAT) would be configured for all traffic exiting the branch LAN. Therefore, the static routes on the ISP routers would be pointing to the provided public pool of the branch office.

1. Implement the routing policies on the respective routers. You can copy and paste the following configurations.

**Router R1**

R1(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.1**

R1(config)#

**Router ISP1 (R2)**

ISP1(config)# **router eigrp 1**

ISP1(config-router)# **network 209.165.200.224 0.0.0.3**

ISP1(config-router)# **network 209.165.201.0 0.0.0.31**

ISP1(config-router)# **no auto-summary**

ISP1(config-router)# **exit**

ISP1(config)#

ISP1(config-router)# **ip route 192.168.1.0 255.255.255.0 209.165.201.2**

ISP1(config)#

**Router ISP2 (R3)**

ISP2(config)# **router eigrp 1**

ISP2(config-router)# **network 209.165.200.224 0.0.0.3**

ISP2(config-router)# **network 209.165.202.128 0.0.0.31**

ISP2(config-router)# **no auto-summary**

ISP2(config-router)# **exit**

ISP2(config)#

ISP2(config)# **ip route 192.168.1.0 255.255.255.0 209.165.202.130**

ISP2(config)#

EIGRP neighbor relationship messages on ISP1 and ISP2 should be generated. Troubleshoot if necessary.

1. 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. You can copy the following Tcl script and paste it into R1.

**foreach address {**

**209.165.200.254**

**209.165.201.30**

**209.165.202.158**

**} {**

**ping $address source 192.168.1.1**

**}**

All pings should be successful. Troubleshoot if necessary.

1. Trace the path taken to the web server, ISP1 DNS server, and ISP2 DNS server. You can copy the following Tcl script and paste it into R1.

**foreach address {**

**209.165.200.254**

**209.165.201.30**

**209.165.202.158**

**} {**

**trace $address source 192.168.1.1**

**}**

Through which ISP is traffic flowing?

### 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.

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

R1(config)# **ip sla 11**

R1(config-ip-sla)# **icmp-echo 209.165.201.30**

R1(config-ip-sla-echo)# **frequency 10**

R1(config-ip-sla-echo)# **exit**

R1(config)#

R1(config)# **ip sla schedule 11 life forever start-time now**

R1(config)#

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.

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

R1# **show ip sla configuration 11**

IP SLAs Infrastructure Engine-III

Entry number: 11

Owner:

Tag:

Operation timeout (milliseconds): 5000

Type of operation to perform: icmp-echo

Target address/Source address: 209.165.201.30/0.0.0.0

Type Of Service parameter: 0x0

Request size (ARR data portion): 28

Verify data: No

Vrf Name:

Schedule:

Operation frequency (seconds): 10 (not considered if randomly scheduled)

Next Scheduled Start Time: Start Time already passed

Group Scheduled : FALSE

Randomly Scheduled : FALSE

Life (seconds): Forever

Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE

Status of entry (SNMP RowStatus): Active

Threshold (milliseconds): 5000

Distribution Statistics:

Number of statistic hours kept: 2

Number of statistic distribution buckets kept: 1

Statistic distribution interval (milliseconds): 20

Enhanced History:

History Statistics:

Number of history Lives kept: 0

Number of history Buckets kept: 15

History Filter Type: None

R1#

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).

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

R1# **show ip sla statistics**

IPSLAs Latest Operation Statistics

IPSLA operation id: 11

Latest RTT: 8 milliseconds

Latest operation start time: 10:33:18 UTC Sat Jan 10 2015

Latest operation return code: OK

Number of successes: 51

Number of failures: 0

Operation time to live: Forever

R1#

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

1. 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.

R1(config)# **ip sla 22**

R1(config-ip-sla)# **icmp-echo 209.165.202.158**

R1(config-ip-sla-echo)# **frequency 10**

R1(config-ip-sla-echo)# **exit**

R1(config)#

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

R1(config)# **end**

R1#

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

R1# **show ip sla configuration 22**

IP SLAs Infrastructure Engine-III

Entry number: 22

Owner:

Tag:

Operation timeout (milliseconds): 5000

Type of operation to perform: icmp-echo

Target address/Source address: 209.165.202.158/0.0.0.0

Type Of Service parameter: 0x0

Request size (ARR data portion): 28

Verify data: No

Vrf Name:

Schedule:

Operation frequency (seconds): 10 (not considered if randomly scheduled)

Next Scheduled Start Time: Start Time already passed

Group Scheduled : FALSE

Randomly Scheduled : FALSE

Life (seconds): Forever

Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE

Status of entry (SNMP RowStatus): Active

Threshold (milliseconds): 5000

Distribution Statistics:

Number of statistic hours kept: 2

Number of statistic distribution buckets kept: 1

Statistic distribution interval (milliseconds): 20

Enhanced History:

History Statistics:

Number of history Lives kept: 0

Number of history Buckets kept: 15

History Filter Type: None

R1# **show ip sla configuration 22**

IP SLAs, Infrastructure Engine-II.

Entry number: 22

Owner:

Tag:

Type of operation to perform: icmp-echo

Target address/Source address: 209.165.201.158/0.0.0.0

Type Of Service parameter: 0x0

Request size (ARR data portion): 28

Operation timeout (milliseconds): 5000

Verify data: No

Vrf Name:

Schedule:

Operation frequency (seconds): 10 (not considered if randomly scheduled)

Next Scheduled Start Time: Start Time already passed

Group Scheduled : FALSE

Randomly Scheduled : FALSE

Life (seconds): Forever

Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE

Status of entry (SNMP RowStatus): Active

Threshold (milliseconds): 5000 (not considered if react RTT is configured)

Distribution Statistics:

Number of statistic hours kept: 2

Number of statistic distribution buckets kept: 1

Statistic distribution interval (milliseconds): 20

History Statistics:

Number of history Lives kept: 0

Number of history Buckets kept: 15

History Filter Type: None

Enhanced History:

R1#

R1# **show ip sla statistics 22**

IPSLAs Latest Operation Statistics

IPSLA operation id: 22

Latest RTT: 16 milliseconds

Latest operation start time: 10:38:29 UTC Sat Jan 10 2015

Latest operation return code: OK

Number of successes: 82

Number of failures: 0

Operation time to live: Forever

R1#

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.

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

R1(config)# **no ip route 0.0.0.0 0.0.0.0 209.165.201.1**

R1(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.1 5**

R1(config)# **exit**

1. Verify the routing table.

R1# **show ip route | begin Gateway**

Gateway of last resort is 209.165.201.1 to network 0.0.0.0

S\* 0.0.0.0/0 [5/0] via 209.165.201.1

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, Loopback0

L 192.168.1.1/32 is directly connected, Loopback0

209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.201.0/30 is directly connected, Serial0/0/0

L 209.165.201.2/32 is directly connected, Serial0/0/0

209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.202.128/30 is directly connected, Serial0/0/1

L 209.165.202.130/32 is directly connected, Serial0/0/1

R1#

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.

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

R1(config)# **track 1 ip sla 11 reachability**

R1(config-track)#

1. Specify the level of sensitivity to changes of tracked objects to 10 seconds of down delay and 1 second of up delay using the **delay down 10 up 1** command. The delay helps to alleviate the effect of flapping objects—objects that are going down and up rapidly. In this situation, if the DNS server fails momentarily and comes back up within 10 seconds, there is no impact.

R1(config-track)# **delay down 10 up 1**

R1(config-track)# **exit**

R1(config)#

1. To view routing table changes as they happen, first enable the **debug ip routing** command.

R1# **debug ip routing**

IP routing debugging is on

R1#

1. Configure the floating static route that will be implemented when tracking object 1 is active. Use the **ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1** command to create a floating static default route via 209.165.201.1 (ISP1). Notice that this command references the tracking object number 1, which in turn references IP SLA operation number 11.

R1(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1**

R1(config)#

Jan 10 10:45:39.119: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.201.1 0 1048578

Jan 10 10:45:39.119: RT: closer admin distance for 0.0.0.0, flushing 1 routes

Jan 10 10:45:39.119: RT: add 0.0.0.0/0 via 209.165.201.1, static metric [2/0]

Jan 10 10:45:39.119: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.201.1 0 1048578

Jan 10 10:45:39.119: RT: rib update return code: 17

Jan 10 10:45:39.119: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.201.1 0 1048578

Jan 10 10:45:39.119: RT: rib update return code: 17

R1(config)#

Notice that the default route with an administrative distance of 5 has been immediately flushed because of a route with a better admin distance. It then adds the new default route with the admin distance of 2.

1. Repeat the steps for operation 22, track number 2, and assign the static route an admin distance higher than track 1 and lower than 5. On R1, copy the following configuration, which sets an admin distance of 3.

R1(config)# **track 2 ip sla 22 reachability**

R1(config-track)# **delay down 10 up 1**

R1(config-track)# **exit**

R1(config)#

R1(config)# **ip route 0.0.0.0 0.0.0.0 209.165.202.129 3 track 2**

R1(config)#

1. Verify the routing table again.

R1#show ip route | begin Gateway

Gateway of last resort is 209.165.201.1 to network 0.0.0.0

S\* 0.0.0.0/0 [2/0] via 209.165.201.1

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, Loopback0

L 192.168.1.1/32 is directly connected, Loopback0

209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.201.0/30 is directly connected, Serial0/0/0

L 209.165.201.2/32 is directly connected, Serial0/0/0

209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.202.128/30 is directly connected, Serial0/0/1

L 209.165.202.130/32 is directly connected, Serial0/0/1

R1#

Although a new default route was entered, its administrative distance is not better than 2. Therefore, it does not replace the previously entered default route.

### Step 5: Verify IP SLA operation.

In this step you observe and verify the dynamic operations and routing changes when tracked objects fail. The following summarizes the process:

* Disable the DNS loopback interface on ISP1 (R2).
* Observe the output of the **debug** command on R1.
* Verify the static route entries in the routing table and the IP SLA statistics of R1.
* Re-enable the loopback interface on ISP1 (R2) and again observe the operation of the IP SLA tracking feature.

1. On ISP1, disable the loopback interface 1.

ISP1(config-if)# **int lo1**

ISP1(config-if)# **shutdown**

ISP1(config-if)#

Jan 10 10:53:25.091: %LINK-5-CHANGED: Interface Loopback1, changed state to administratively down

Jan 10 10:53:26.091: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to down

ISP1(config-if)#

1. On R1, observe the **debug** output being generated. Recall that R1 will wait up to 10 seconds before initiating action therefore several seconds will elapse before the output is generated.

R1#

Jan 10 10:53:59.551: %TRACK-6-STATE: 1 ip sla 11 reachability Up -> Down

Jan 10 10:53:59.551: RT: del 0.0.0.0 via 209.165.201.1, static metric [2/0]

Jan 10 10:53:59.551: RT: delete network route to 0.0.0.0/0

Jan 10 10:53:59.551: RT: default path has been cleared

Jan 10 10:53:59.551: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.202.129 0 1048578

Jan 10 10:53:59.551: RT: add 0.0.0.0/0 via 209.165.202.129, static metric [3/0]

Jan 10 10:53:59.551: RT: default path is now 0.0.0.0 via 209.165.202.129

Jan 10 10:53:59.551: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.201.1 0 1048578

Jan 10 10:53:59.551: RT: rib update return code: 17

Jan 10 10:53:59.551: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.202.129 0 1048578

Jan 10 10:53:59.551: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.201.1 0 1048578

Jan 10 10:53:59.551: RT: rib update return code: 17

R1#

The tracking state of track 1 changes from up to down. This is the object that tracked reachability for IP SLA object 11, with an ICMP echo to the ISP1 DNS server at 209.165.201.30.

R1 then proceeds to delete the default route with the administrative distance of 2 and installs the next highest default route to ISP2 with the administrative distance of 3.

1. On R1, verify the routing table.

R1# **show ip route | begin Gateway**

Gateway of last resort is 209.165.202.129 to network 0.0.0.0

S\* 0.0.0.0/0 [3/0] via 209.165.202.129

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, Loopback0

L 192.168.1.1/32 is directly connected, Loopback0

209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.201.0/30 is directly connected, Serial0/0/0

L 209.165.201.2/32 is directly connected, Serial0/0/0

209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.202.128/30 is directly connected, Serial0/0/1

L 209.165.202.130/32 is directly connected, Serial0/0/1

R1#

The new static route has an administrative distance of 3 and is being forwarded to ISP2 as it should.

1. Verify the IP SLA statistics.

R1# **show ip sla statistics**

IPSLAs Latest Operation Statistics

IPSLA operation id: 11

Latest RTT: NoConnection/Busy/Timeout

Latest operation start time: 11:01:08 UTC Sat Jan 10 2015

Latest operation return code: Timeout

Number of successes: 173

Number of failures: 45

Operation time to live: Forever

IPSLA operation id: 22

Latest RTT: 8 milliseconds

Latest operation start time: 11:01:09 UTC Sat Jan 10 2015

Latest operation return code: OK

Number of successes: 218

Number of failures: 0

Operation time to live: Forever

R1#

Notice that the latest return code is **Timeout** and there have been 45 failures on IP SLA object 11.

1. On R1, initiate a trace to the web server from the internal LAN IP address.

R1# **trace 209.165.200.254 source 192.168.1.1**

Type escape sequence to abort.

Tracing the route to 209.165.200.254

VRF info: (vrf in name/id, vrf out name/id)

1 209.165.202.129 4 msec \* \*

R1#

This confirms that traffic is leaving router R1 and being forwarded to the ISP2 router.

1. On ISP1, re-enable the DNS address by issuing the **no shutdown** command on the loopback 1 interface to examine the routing behavior when connectivity to the ISP1 DNS is restored.

ISP1(config-if)# **no shutdown**

Jan 10 11:05:45.847: %LINK-3-UPDOWN: Interface Loopback1, changed state to up

Jan 10 11:05:46.847: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

ISP1(config-if)#

Notice the output of the **debug ip routing** command on R1.

R1#

Jan 10 11:06:20.551: %TRACK-6-STATE: 1 ip sla 11 reachability Down -> Up

Jan 10 11:06:20.551: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.201.1 0 1048578

Jan 10 11:06:20.551: RT: closer admin distance for 0.0.0.0, flushing 1 routes

Jan 10 11:06:20.551: RT: add 0.0.0.0/0 via 209.165.201.1, static metric [2/0]

Jan 10 11:06:20.551: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.202.129 0 1048578

Jan 10 11:06:20.551: RT: rib update return code: 17

Jan 10 11:06:20.551: RT: u

R1#pdating static 0.0.0.0/0 (0x0) :

via 209.165.202.129 0 1048578

Jan 10 11:06:20.551: RT: rib update return code: 17

Jan 10 11:06:20.551: RT: updating static 0.0.0.0/0 (0x0) :

via 209.165.201.1 0 1048578

Jan 10 11:06:20.551: RT: rib update return code: 17

R1#

Now the IP SLA 11 operation transitions back to an up state and reestablishes the default static route to ISP1 with an administrative distance of 2.

1. Again examine the IP SLA statistics.

R1# **show ip sla statistics**

IPSLAs Latest Operation Statistics

IPSLA operation id: 11

Latest RTT: 8 milliseconds

Latest operation start time: 11:07:38 UTC Sat Jan 10 2015

Latest operation return code: OK

Number of successes: 182

Number of failures: 75

Operation time to live: Forever

IPSLA operation id: 22

Latest RTT: 16 milliseconds

Latest operation start time: 11:07:39 UTC Sat Jan 10 2015

Latest operation return code: OK

Number of successes: 257

Number of failures: 0

Operation time to live: Forever

R1#

The IP SLA 11 operation is active again, as indicated by the OK return code, and the number of successes is incrementing.

1. Verify the routing table.

R1# **show ip route | begin Gateway**

Gateway of last resort is 209.165.201.1 to network 0.0.0.0

S\* 0.0.0.0/0 [2/0] via 209.165.201.1

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, Loopback0

L 192.168.1.1/32 is directly connected, Loopback0

209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.201.0/30 is directly connected, Serial0/0/0

L 209.165.201.2/32 is directly connected, Serial0/0/0

209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.202.128/30 is directly connected, Serial0/0/1

L 209.165.202.130/32 is directly connected, Serial0/0/1

R1#

The default static through ISP1 with an administrative distance of 2 is reestablished.

There are many possibilities available with object tracking and Cisco IOS IP SLAs. As shown in this lab, a probe can be based on reachability, changing routing operations, and path control based on the ability to reach an object. However, Cisco IOS IP SLAs also allow paths to be changed based on network conditions such as delay, load, and other factors.

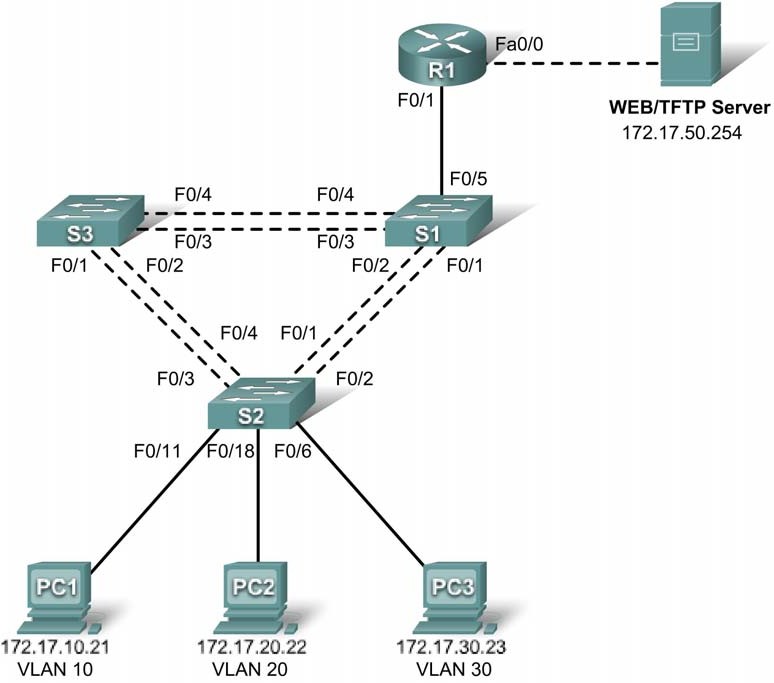
Before deploying a Cisco IOS IP SLA solution, the impact of the additional probe traffic being generated should be considered, including how that traffic affects bandwidth utilization, and congestion levels. Tuning the configuration (for example, with the **delay** and **frequency** commands) is critical to mitigate possible issues related to excessive transitions and route changes in the presence of flapping tracked objects.

The benefits of running IP SLAs should be carefully evaluated. The IP SLA is an additional task that must be performed by the router’s CPU. A large number of intensive SLAs could be a significant burden on the CPU, possibly interfering with other router functions and having detrimental impact on the overall router performance. The CPU load should be monitored after the SLAs are deployed to verify that they do not cause excessive utilization of the router CPU.

# Practical No - 7

**Aim:** Basic Inter-VLAN Routing

**Topology Diagram**



**Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| **S1** | **VLAN 99** | 172.17.99.11 | 255.255.255.0 | 172.17.99.1 |
| **S2** | **VLAN 99** | 172.17.99.12 | 255.255.255.0 | 172.17.99.1 |
| **S3** | **VLAN 99** | 172.17.99.13 | 255.255.255.0 | 172.17.99.1 |
| **R1** | **Fa0/0** | See Interface Configuration Table | | N/A |
| **Fa0/1** | 172.17.50.1 | 255.255.255.0 | N/A |
| **PC1** | **NIC** | 172.17.10.21 | 255.255.255.0 | 172.17.10.1 |
| **PC2** | **NIC** | 172.17.20.22 | 255.255.255.0 | 172.17.20.1 |
| **PC3** | **NIC** | 172.17.30.23 | 255.255.255.0 | 172.17.30.1 |
| **Server** | **NIC** | 172.17.50.254 | 255.255.255.0 | 172.17.50.1 |

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

# Port Assignments – S2

|  |  |  |
| --- | --- | --- |
| **Ports** | **Assignment** | **Network** |
| **Fa0/1 - 0/5** | 802.1q Trunks (Native VLAN 99) | 172.17.99.0 /24 |
| **Fa0/6 - 0/10** | VLAN 30 – Guests(Default) | 172.17.30.0 /24 |
| **Fa0/11 - 0/17** | VLAN 10 – Faculty/Staff | 172.17.10.0 /24 |
| **Fa0/18 - 0/24** | VLAN 20 - Students | 172.17.20.0 /24 |

**Subinterface Configuration Table – R1**

|  |  |  |
| --- | --- | --- |
| **Interface** | **Assignment** | **IP Address** |
| **Fa0/0.1** | VLAN 1 | 172.17.1.1 /24 |
| **Fa0/0.10** | VLAN 10 | 172.17.10.1 /24 |
| **Fa0/0.20** | VLAN 20 | 172.17.20.1 /24 |
| **Fa0/0.30** | VLAN 30 | 172.17.30.1 /24 |
| **Fa0/0.99** | VLAN 99 | 172.17.99.1 /24 |

# Learning Objectives

* Perform basic switch configurations
* Configure the Ethernet interfaces on the host PCs
* Configure VTP on the switches
* Configure the router and the remote server LAN

# Introduction

In this activity, you will perform basic switch configurations, configure addressing on PCs, configure VTP and inter-VLAN routing.

## Task 1: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the addressing table and the following guidelines:

* Configure the switch hostname.
* Disable DNS lookup.
* Configure the default gateway.
* Configure an EXEC mode password of **class**.
* Configure a password of **cisco** for console connections.
* Configure a password of **cisco** for vty connections.
* Configure the default gateway on each switch.

Switch>**enable** Switch#**config term**

Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#**hostname S1**

S1(config)#**enable secret class**

S1(config)#**no ip domain-lookup**

S1(config)#**ip default-gateway 172.17.99.1**

S1(config)#**line console 0** S1(config-line)#**password cisco** S1(config-line)#**login** S1(config-line)#**line vty 0 15** S1(config-line)#**password cisco** S1(config-line)#**login** S1(config-line)#**end**

%SYS-5-CONFIG\_I: Configured from console by console S1#**copy running-config startup-config**

Destination filename [startup-config]? [enter] Building configuration...

## Task 2: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2 and PC3 with the IP addresses from the addressing table.

## Task 3: Configure VTP on the Switches

### Step 1. Enable the user ports on S2 in access mode.

S2(config)#**interface fa0/6** S2(config-if)#**switchport mode access** S2(config-if)#**no shutdown**

S2(config-if)#**interface fa0/11** S2(config-if)#**switchport mode access** S2(config-if)#**no shutdown**

S2(config-if)#**interface fa0/18** S2(config-if)#**switchport mode access** S2(config-if)#**no shutdown**

### Step 2. Configure VTP.

Configure VTP on the three switches using the following table. Remember that VTP domain names and passwords are case-sensitive.

|  |  |  |  |
| --- | --- | --- | --- |
| **Switch Name** | **VTP Operating Mode** | **VTP Domain** | **VTP**  **Password** |
| S1 | Server | Lab5 | cisco |
| S2 | Client | Lab5 | cisco |
| S3 | Client | Lab5 | cisco |

S1(config)#**vtp mode server** Device mode already VTP SERVER. S1(config)#**vtp domain Lab6**

Changing VTP domain name from NULL to Lab6 S1(config)#**vtp password cisco**

Setting device VLAN database password to cisco S1(config)#**end**

S2(config)#**vtp mode client** Setting device to VTP CLIENT mode S2(config)#**vtp domain Lab6**

Changing VTP domain name from NULL to LaB

|  |  |  |
| --- | --- | --- |
| S3(config)#**interface fa0/1**  S3(config-if#**switchport mode trunk**  S3(config-if)#**switchport trunk native** | **vlan** | **99** |
| S3(config-if)#**no shutdown**  S3(config-if-#**end** |  | |
| **Step 4. Configure the VTP server with VLANs.** |
| Configure the following VLANS on the VTP server: |

|  |  |
| --- | --- |
| **VLAN** | **VLAN Name** |
| VLAN 99 | management |
| VLAN 10 | faculty-staff |
| VLAN 20 | students |
| VLAN 30 | guest |

S1(config)#**vlan 99**

S1(config-vlan)#**name management**

S1(config)#**vlan 10**

S1(config-vlan)#**name faculty-staff**

S1(config)#**vlan 20**

S1(config-vlan)#**name students**

S1(config)#**vlan 30**

S1(config-vlan)#**name guest**

S1(config-vlan)#**end**

Verify that the VLANs have been created on S1 with the show vlan brief command.

### Step 5. Verify that the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to verify that all four VLANs have been distributed to the client switches.

### S2#show vlan brief

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VLAN Name |  | Status |  | Ports |
| 1 default  10 faculty/staff |  | active  active |  | Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12,Fa0/13 Fa0/14, Fa0/15, Fa0/16,Fa0/17 Fa0/18, Fa0/19, Fa0/20,Fa0/21  Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2 |
| 20 students  30 guest  99 management |  | active active active |  |  |
| VLAN |  | Name |  | Status |  | Ports |
| 1 |  | default |  | active |  | Fa0/5, Fa0/6, Fa0/7, Fa0/8 |
|  |  |  |  |  |  | Fa0/9, Fa0/10, Fa0/11, Fa0/12 |
|  |  |  |  |  |  | Fa0/13, Fa0/14, Fa0/15, Fa0/16 |
|  |  |  |  |  |  | Fa0/17, Fa0/18, Fa0/19, Fa0/20 |
|  |  |  |  |  |  | Fa0/21, Fa0/22, Fa0/23, Fa0/24 |
|  |  |  |  |  |  | Gig1/1, Gig1/2 |
| 10 |  | faculty-staff |  | active |  |  |
| 20 |  | students |  | active |  |  |
| 30 |  | guest |  | active |  |  |
| 99 |  | management |  | active |  |  |
| 1002 |  | fddi-default |  | active |  |  |
| 1003 |  | token-ring-default |  | active |  |  |
| 1004 |  | fddinet-default |  | active |  |  |
| 1005 |  | trnet-default |  | active |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 10 |  | faculty-staff |  | active |  |  |
| 20 |  | students |  | active |  |  |
| 30 |  | guest |  | active |  |  |
| 99 |  | management |  | active |  |  |
| 1002 |  | fddi-default |  | active |  |  |
| 1003 |  | token-ring-default |  | active |  |  |
| 1004 |  | fddinet-default |  | active |  |  |
| 1005 |  | trnet-default |  | active |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Step 6. Configure the management interface address on all three switches.**

S1(config)#**interface vlan99**

|  |  |
| --- | --- |
| S1(config-if)#**ip address 172.17.99.11** | **255.255.255.0** |
| S2(config)#**interface vlan99**  S2(config-if)#**ip address 172.17.99.12** | **255.255.255.0** |
| S3(config)#**interface vlan99**  S3(config-if)#**ip address 172.17.99.13** | **255.255.255.0** |

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful?

If not, troubleshoot the switch configurations and try again.

### Step 7. Assign switch ports to VLANs on S2.

Port assignments are listed in the table at the beginning of the activity. However, since Packet Tracer

4.11 does not support the **interface range** command, only assign the first port from each range.

S2(config)#**interface fa0/6**

S2(config-if)#**switchport access vlan 30** S2(config-if)#**interface fa0/11** S2(config-if)#**switchport access vlan 10** S2(config-if)#**interface fa0/18** S2(config-if)#**switchport access vlan 20** S2(config-if)#**end**

S2#**copy running-config startup-config** Destination filename [startup-config]? [enter] Building configuration...

[OK] S2#

### Step 8. Check connectivity between VLANs.

Open the Command Prompt on the three PCs.

* Ping from PC1 to PC2 (172.17.20.22)
* Ping from PC2 to PC3 (172.17.30.23)
* Ping from PC3 to PC1 (172.17.30.21) Are the pings successful?

If not, why do these pings fail?

## Task 4: Configure the Router and the Remote Server LAN

### Step 1. Create a basic configuration on the router.

* Configure the router with hostname R1.
* Disable DNS lookup.
* Configure an EXEC mode password of **class**.
* Configure a password of **cisco** for console connections.
* Configure a password of **cisco** for vty connections.

### Step 2. Configure the trunking interface on R1.

You have demonstrated that connectivity between VLANs requires routing at the network layer, exactly like connectivity between any two remote networks. There are a couple of options for configuring routing between VLANs.

The first is something of a brute force approach. An L3 device, either a router or a Layer 3 capable switch, is connected to a LAN switch with multiple connections--a separate connection for each VLAN that requires inter-VLAN connectivity. Each of the switch ports used by the L3 device are configured in a different VLAN on the switch. After IP addresses are assigned to the interfaces on the L3 device, the routing table has directly connected routes for all VLANs, and inter-VLAN routing is enabled. The limitations to this approach are the lack of sufficient Fast Ethernet ports on routers, under-utilization of ports on L3 switches and routers, and excessive wiring and manual configuration. The topology used in this lab does not use this approach.

An alternative approach is to create one or more Fast Ethernet connections between the L3 device (the router) and the distribution layer switch, and to configure these connections as **dot1q** trunks. This allows all inter-VLAN traffic to be carried to and from the routing device on a single trunk. However, it requires that the L3 interface be configured with multiple IP addresses. This can be done by creating virtual interfaces, called subinterfaces, on one of the router Fast Ethernet ports and configuring them to be **dot1q** aware.

Using the subinterface configuration approach requires these steps:

* Enter subinterface configuration mode
* Establish trunking encapsulation
* Associate a VLAN with the subinterface
* Assign an IP address from the VLAN to the subinterface The commands are as follows:

R1(config)#**interface fastethernet 0/0**

R1(config-if)#**no shutdown**

R1(config-if)#**interface fastethernet 0/0.1**

R1(config-subif)#**encapsulation dot1q 1**

R1(config-subif)#**ip address 172.17.1.1 255.255.255.0** R1(config-subif)#**interface fastethernet 0/0.10** R1(config-subif)#**encapsulation dot1q 10**

R1(config-subif)#**ip address 172.17.10.1 255.255.255.0** R1(config-subif)#**interface fastethernet 0/0.20** R1(config-subif)#**encapsulation dot1q 20**

R1(config-subif)#**ip address 172.17.20.1 255.255.255.0** R1(config-subif)#**interface fastethernet 0/0.30** R1(config-subif)#**encapsulation dot1q 30**

R1(config-subif)#**ip address 172.17.30.1 255.255.255.0** R1(config-subif)#**interface fastethernet 0/0.99** R1(config-subif)#**encapsulation dot1q 99 native** R1(config-subif)#**ip address 172.17.99.1 255.255.255.0**

Note the following points in this configuration:

* The physical interface is enabled using the **no shutdown** command, because router interfaces are down by default. The subinterface will then be up by default.
* The subinterface can use any number that can be described with 32 bits, but it is good practice to assign the number of the VLAN as the interface number, as has been done here.
* The native VLAN is specified on the L3 device so that it is consistent with the switches. Otherwise, VLAN 1 is native by default, and there is no communication between the router and the management VLAN on the switches.

### Step 3. Configure the server LAN interface on R1.

R1(config)#**interface FastEthernet0/1**

R1(config-if)#**ip address 172.17.50.1 255.255.255.0** R1(config-if)#**description server interface** R1(config-if)#**no shutdown**

R1(config-if)#**end**

There are now six networks configured. Verify that you can route packets to all six by checking the routing table on R1.

### R1#show ip route

<output omitted

Gateway of last resort is not set 172.17.0.0/24 is subnetted, 6 subnets

C 172.17.1.0 is directly connected, FastEthernet0/0.1 C 172.17.10.0 is directly connected, FastEthernet0/0.10 C 172.17.20.0 is directly connected, FastEthernet0/0.20 C 172.17.30.0 is directly connected, FastEthernet0/0.30 C 172.17.50.0 is directly connected, FastEthernet0/1

C 172.17.99.0 is directly connected, FastEthernet0/0.99

If your routing table does not show all six networks, troubleshoot your configuration and resolve the problem before proceeding.

### Step 4. Verify Inter-VLAN routing.

From PC1, verify that you can ping the remote server (172.17.50.254) and the other two hosts (172.17.20.22 and 172.17.30.23). It may take a couple of pings before the end-to-end path is established.

These pings should be successful. If not, troubleshoot your configuration. Check to make sure that the default gateways have been set on all PCs and all switches.

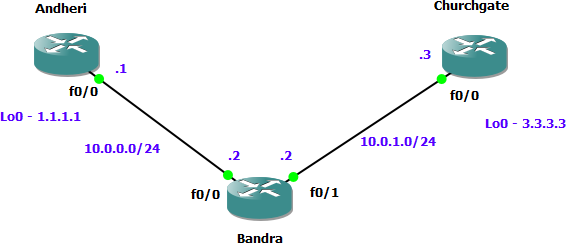
## Task 5: Reflection

In Task 4, you configured VLAN 99 as the native VLAN in the router Fa0/0.99 interface configuration. Why would packets from the router or hosts fail when trying to reach the switch management interfaces if the native VLAN were left in default?

**Practical No - 8**

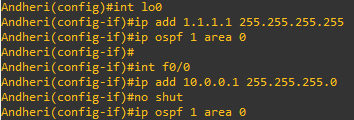
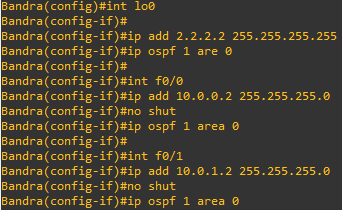
**Aim: Cisco MPLS Configuration**

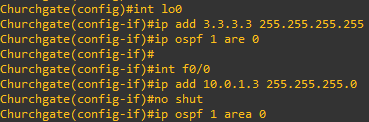
**Topology :**



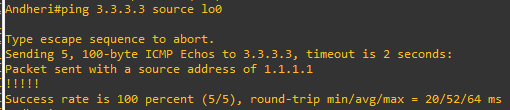
#### Step 1 *–* IP addressing of MPLS Core and OSPF

First bring 3 routers into your topology R1, R2, R3 position them as below. We are going to address the routers and configure ospf to ensure loopback to loopback connectivity between R1 and R3



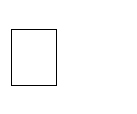


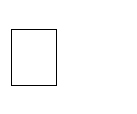
You should now have full ip connectivity between R1, R2, R3 to verify this we need to see if we can ping between the loopbacks of R1 and R3



#### Step 2 *–* Configure LDP on all the interfaces in the MPLS Core

In order to run MPLS you need to enable it, there are two ways to do this.

At each interface enter the mpls ip command

Under the ospf process use the mpls ldp autoconfig command

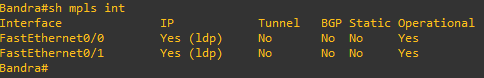


You should see log messages coming up showing the LDP neighbors are up.

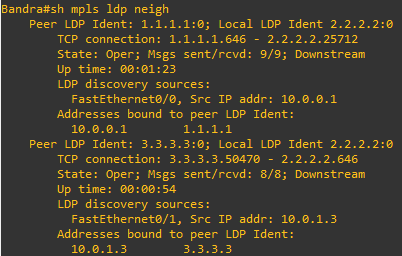


To verify the mpls interfaces the command is very simple – sh mpls interface

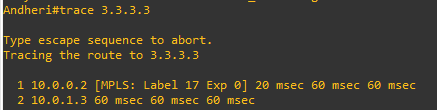
This is done on R2 and you can see that both interfaces are running mpls and using LDP



You can also verify the LDP neighbors with the sh mpls ldp neighbors command.

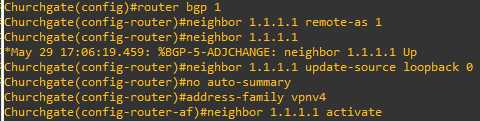


One more verification to confirm LDP is running ok is to do a trace between R1 and R3 and verify if you get MPLS Labels show up in the trace.

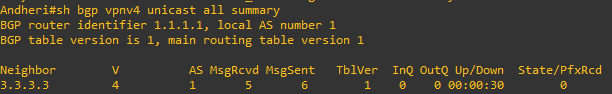


#### Step 3 *–* MPLS BGP Configuration between R1 and R3

We need to establish a Multi Protocol BGP session between R1 and R3 this is done by configuring the vpnv4 address family as below

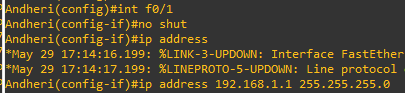
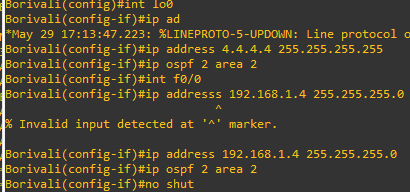


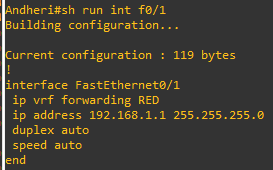
To verify the BGP session between R1 and R3 issue the command sh bgp vpnv4 unicast all summary



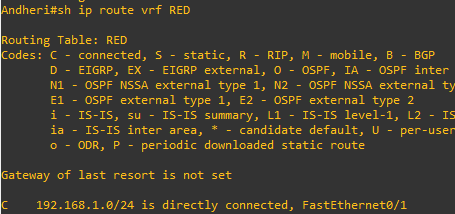
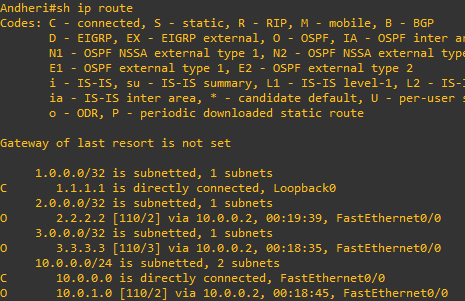
#### Step 4 *–* Add two more routers, create VRFs

We will add two more routers into the topology so it now looks like the final topology





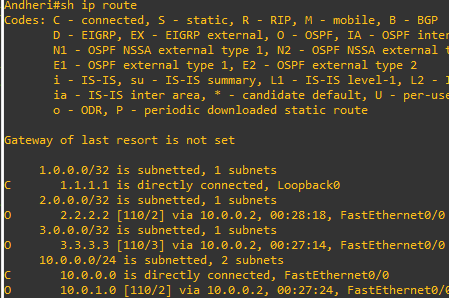
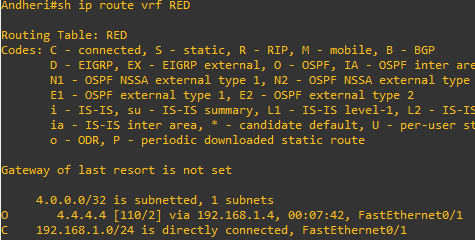
If you issue the command sh ip route this shows the routes in the global table and you will notice that you do not see 192.168.1.0/24



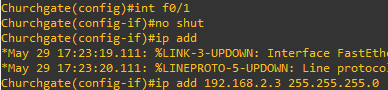
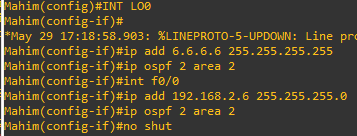
We just need to enable OSPF on this interface and get the loopback address for R4 in the VRF RED routing table before proceeding.



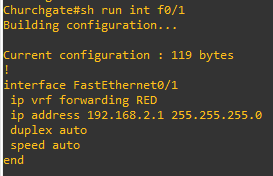
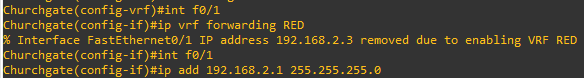
If we now check the routes in the VRF RED routing table you should see 4.4.4.4 in there as well.



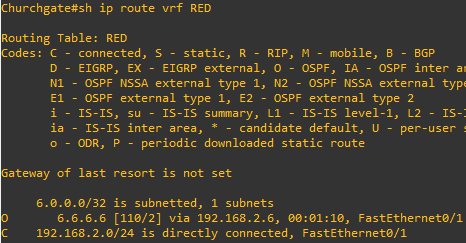
We now need to repeat this process for R3 & R6 Router 6 will peer OSPF using process number 2 to a VRF configured on R3. It will use the local site addressing to 192.168.2.0/24



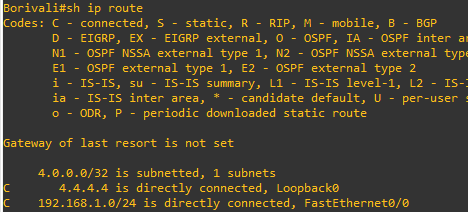
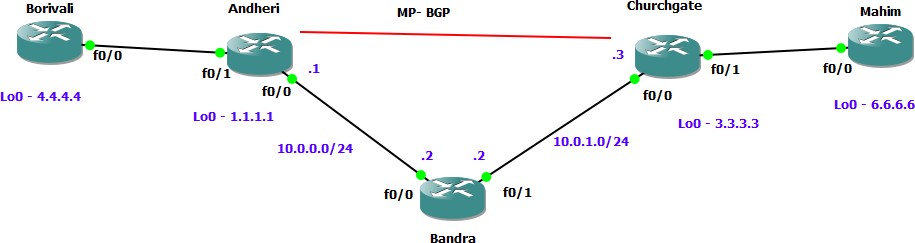
We also need to configure a VRF onto R3 as well.



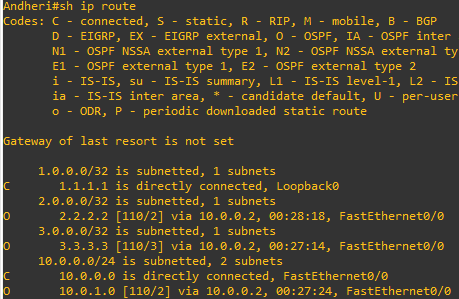
Check the router in vrf RED

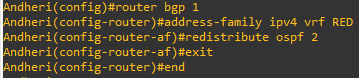
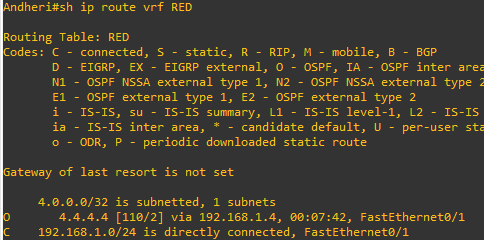


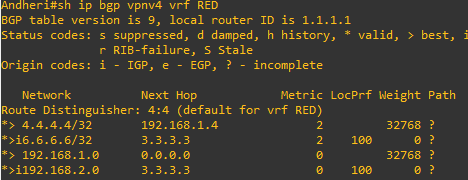
Ok so we have come a long way now let’s review the current situation. We now have this setup

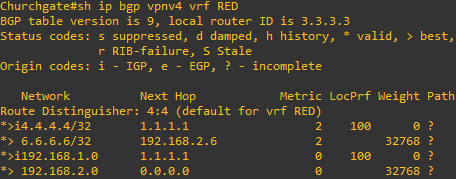


As expected we have the local interface and the loopback address. When we are done we want to see 6.6.6.6 in there so we can ping across the MPLS Check the routes on R1





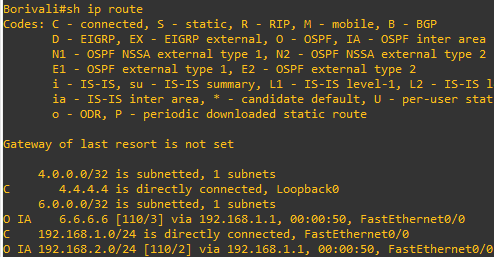




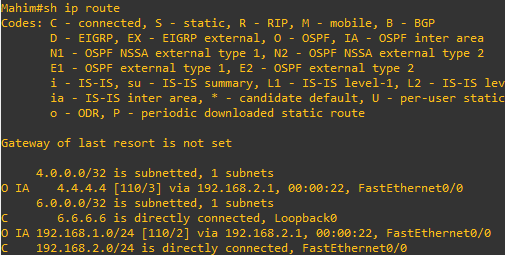
Which it is! 6.6.6.6 is now in the BGP table in VRF RED on R3 with a next hop of 192.168.2.6 (R6) and also 4.4.4 is in there as well with a next hop of 1.1.1.1 (which is the loopback of R1 – showing that it is going over the MPLS and R2 is not in the picture)



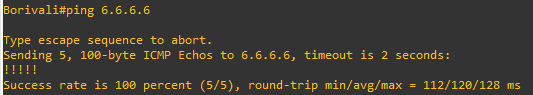
Before we do let’s see what the routing table look like on R4



Do the same step of on R6



Lets chevk ping command



Which we can – to prove this is going over the mpls and be label switched and not routed, lets do a trace

