**MODERN NETWORKING**



PRACTICAL OF

MODERN NETWORKING

SUBMITTED

BY

AQDAS AHMED KHAN

(M.Sc I.T Part I Sem II)

ACADEMIC YEAR 2022-2023

UNDER THE GUIDANCE OF

**Miss. THIRU MENAGA**

Guru Nanak College of Arts, Science & Commerce

GTB Nagar, Mumbai – 37



**Department of Information Technology**

**Certificate**

This is to certify that **Ms. ADITI RAJE**, Seat No. **4132994** studying in **Master of Science in Information Technology Part I Semester II** has satisfactorily completed the Practical of **PSIT2P2 –** **MODERN NETWORKING** as prescribed by University of Mumbai, during the academic year **2022-23**.

\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Signature

Subject-In-Charge Head of Department

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

External Examiner

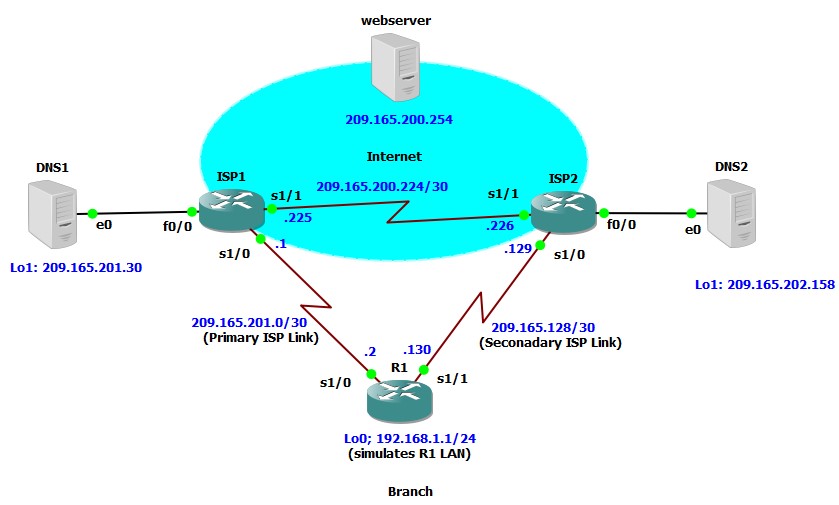
College Seal: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No.** | **INDEX** | **Date** | **Signature** |
| **1** | Configure IP SLA Tracking and Path Control Topology |  |  |
| **2** | Using the AS\_PATH Attribute |  |  |
| **3** | Configuring IBGP and EBGP Sessions, Local Preferences and MED |  |  |
| **4** | Secure the Management Plane |  |  |
| **5** | Configure and Verify Path Control Using PBRs |  |  |
| **6** | Simulating MPLS environment |  |  |

**Practical No - 1**

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

**Topology:**



**Objectives:**

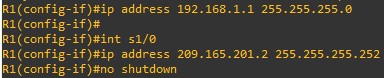
− Configure and verify the IP SLA feature.

− Test the IP SLA tracking feature.

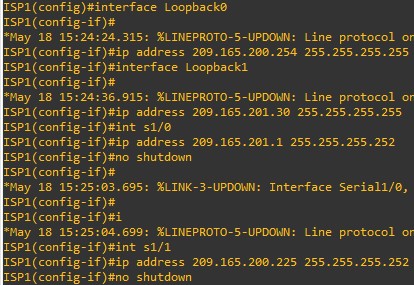
− Verify the configuration and operation using show and debug commands.

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

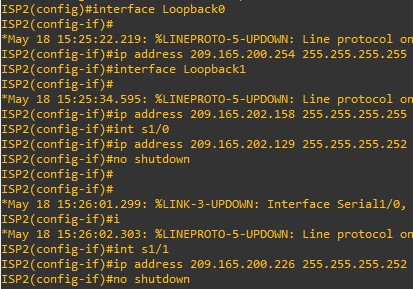
**Router R1:**



**Router ISP1 (R2):**



**Router ISP2 (R3):**



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



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.

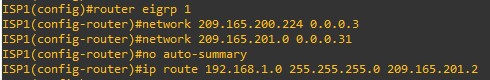
− ISP1 and ISP2 have dynamic routing enabled between them, advertising their respective public address pools.

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

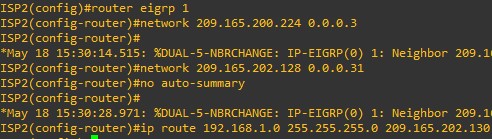
**Router R1:**



**Router ISP1 (R2):**

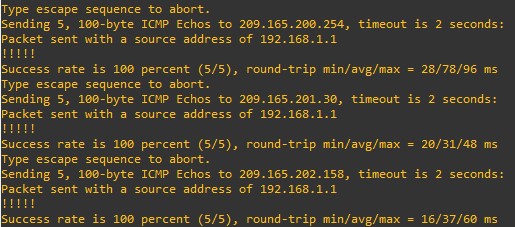
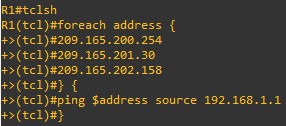


**Router ISP2 (R3):**

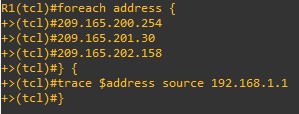


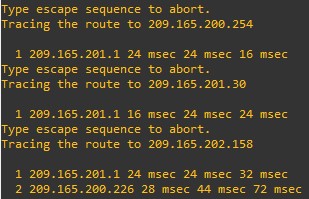
**Step 2: Verify server reachability.**

a) 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.



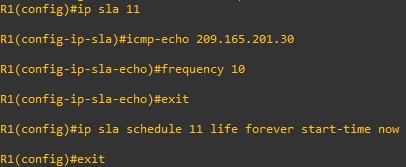
b) Trace the path taken to the web server, ISP1 DNS server, and ISP2 DNS server. You can copy the following Tcl script and paste it into R1.





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

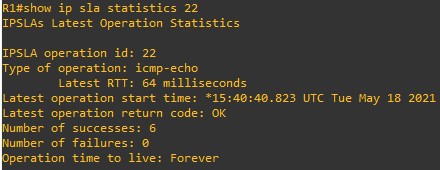
a) Create an ICMP echo probe on R1 to the primary DNS server on ISP1 using the ip sla command. the previous ip sla monitor command. In addition, the icmp-echo command has replaced the type echo protocol ipIcmpEcho command.



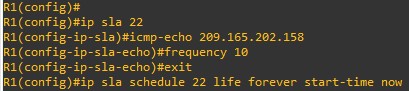
b) Verify the IP SLAs configuration of operation 11 using the show ip sla configuration 11 command.



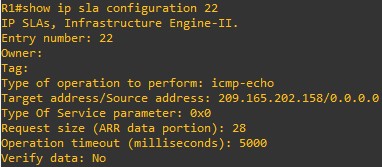
c) Issue the show ip sla statistics command to display the number of successes, failures, and results of the latest operations.

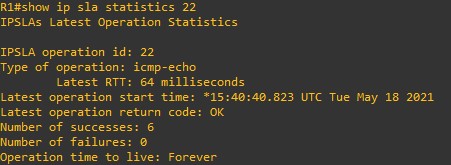


d) Although not actually required because IP SLA session 11 alone could provide the desired fault tolerance, create a second probe, 22, to test connectivity to the second DNS server located on router ISP2. You can copy and paste the following commands on R1.



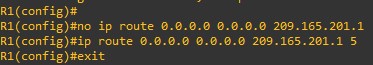
e) Verify the new probe using the show ip sla configuration and show ip sla statistics commands.



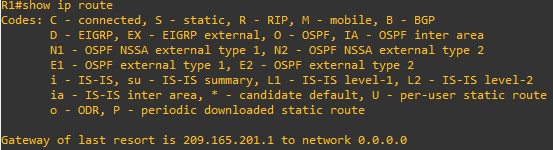


**Step 4: Configure tracking options.**

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



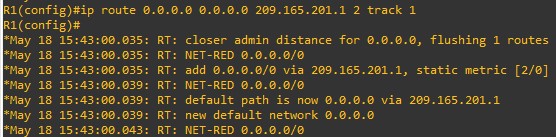
b) Verify the routing table.



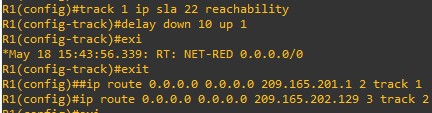
c) Use the track 1 ip sla 11 reachability command to enter the config-track subconfiguration mode.



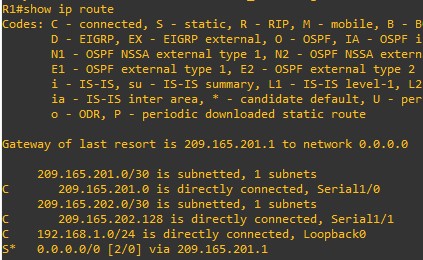
d) Configure the floating static route that will be implemented when tracking object 1 is active. To view routing table changes as they happen, first enable the debug ip routing command. Next, use the ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1 command to create a floating static default route via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



e) 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



f) Verify the routing table again.



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

a) The following summarizes the process:

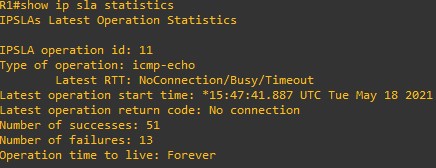
* Disable the DNS loopback interface on ISP1 (R2).
* Observe the output of the debug command on R1.
* Verify the static route entries in the routing table and the IP SLA statistics of R1.
* Re-enable the loopback interface on ISP1 (R2) and again observe the operation of the IP SLA tracking feature.



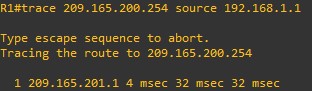
b) Verify the routing table.



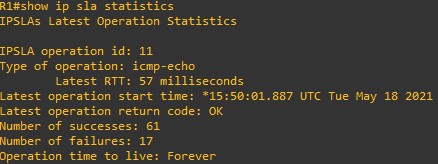
c) Verify the IP SLA statistics.



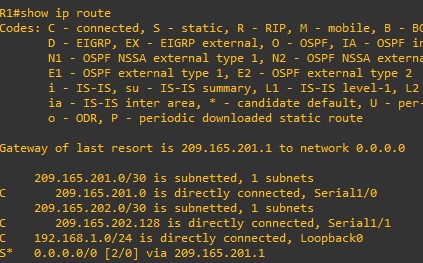
d) Initiate a trace to the web server from the internal LAN IP address.



e) Again examine the IP SLA statistics.



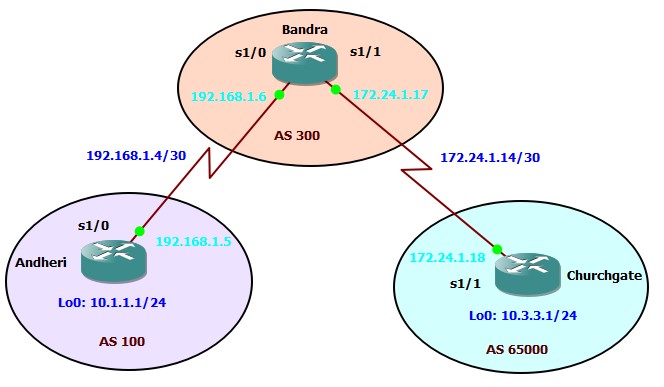
f) Verify the routing table.



**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

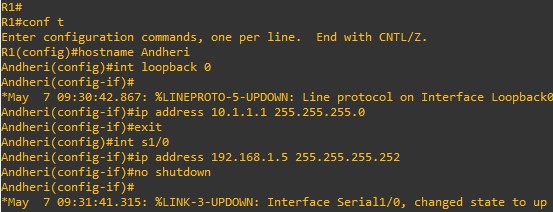
**Step 1: Prepare the routers for the lab.**

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

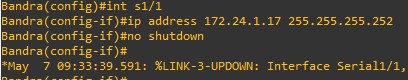
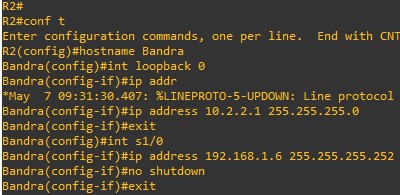
**Step 2: Configure the hostname and interface addresses.**

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

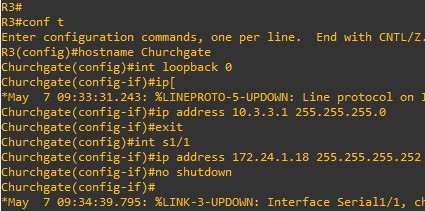
**Router R1 (hostname Andheri):**



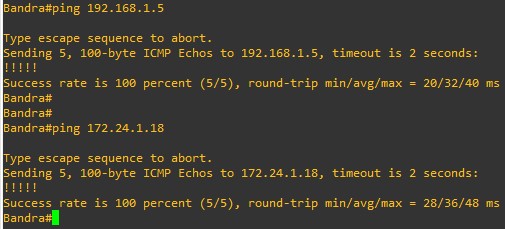
**Router R2 (hostname Bandra):**



**Router R3 (hostname Churchgate):**



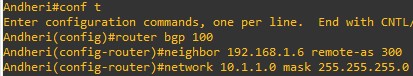
b) Use ping to test the connectivity between the directly connected routers.



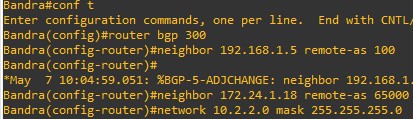
**Step 3: Configure BGP.**

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

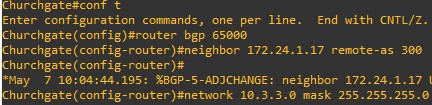
**Router R1 (Andheri):**



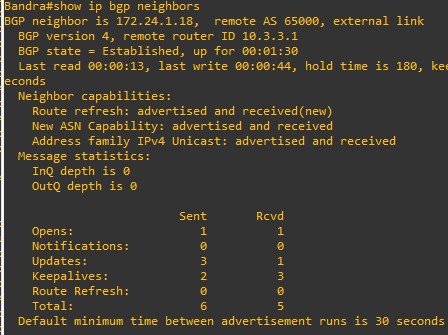
**Router R2 (Bandra):**



**Router R3 (Churchgate):**

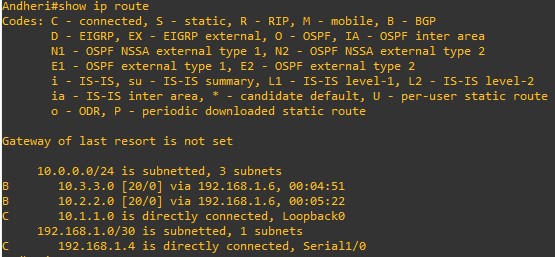


b) Verify that these routers have established the appropriate neighbor relationships by issuing the show ip bgp neighbors command on each router.

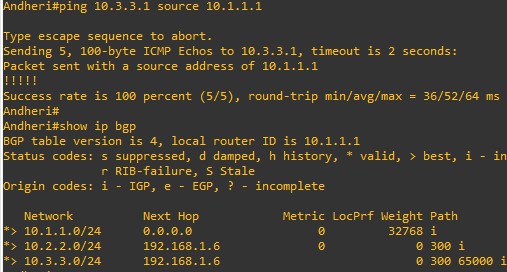


**Step 4: Remove the private AS.**

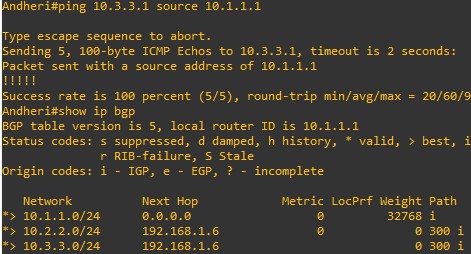
a) DBandralay the Andheri routing table using the show ip route command. Andheri should have a route to both 10.2.2.0 and 10.3.3.0. Troubleshoot if necessary.



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

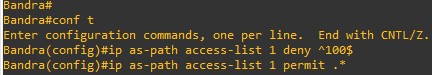


c) Now check the BGP table on Andheri. The AS\_ PATH to the 10.3.3.0 network should be AS 300. It no longer has the private AS in the path.



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

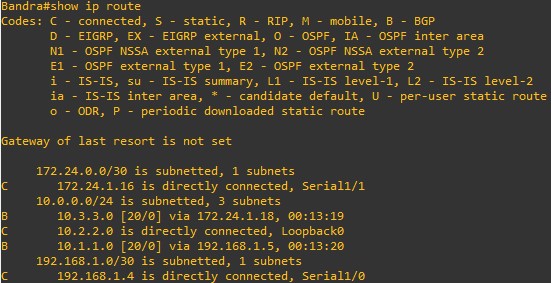
a) Configure a special kind of access list to match BGP routes with an AS\_PATH attribute that both begins and ends with the number 100. Enter the following commands on Bandra.



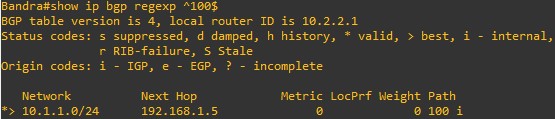
b) Apply the configured access list using the neighbor command with the filter-list option.



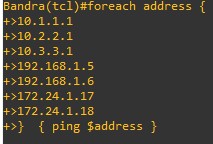
c) Use the clear ip bgp \* command to reset the routing information. Wait several seconds and then check the routing table for BANDRA. The route to 10.1.1.0 should be in the routing table.

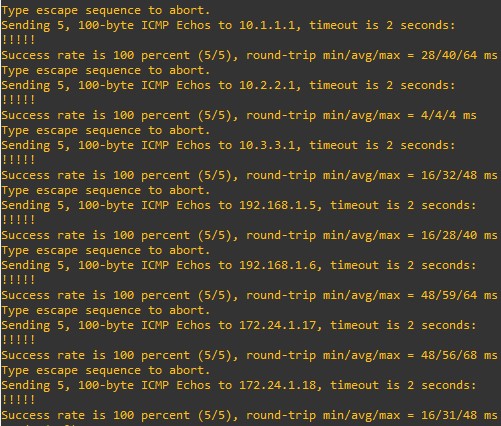


d) Return to BANDRA and verify that the filter is working as intended.



e) 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.

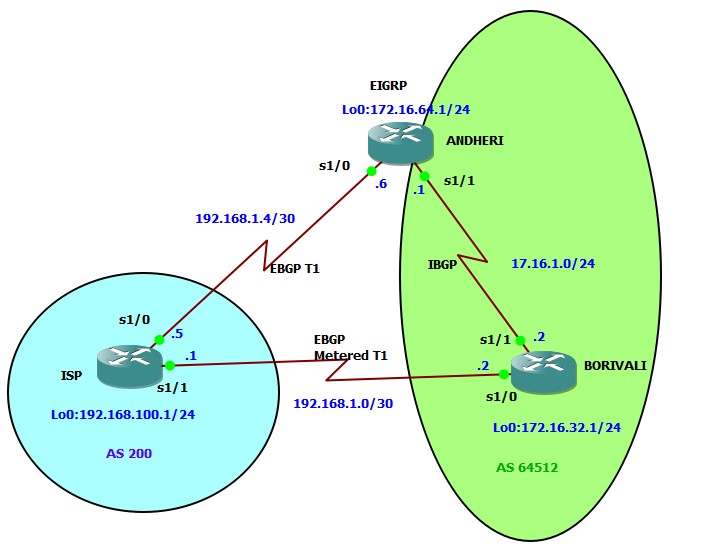




**Practical No - 3**

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

**Topology:**

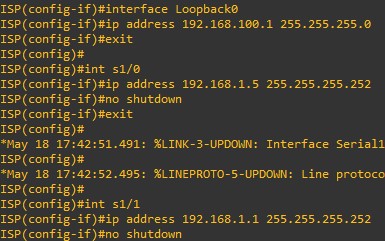


**Objectives:**

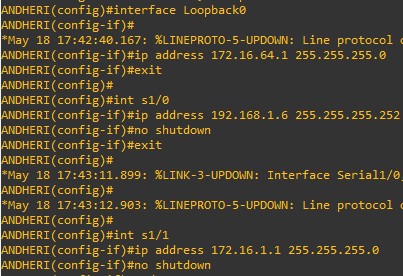
* For IBGP peers to correctly exchange routing information, use the **next-hop-self** command with the **Local-Preference** and **MED** attributes.
* Ensure that the flat-rate, unlimited-use T1 link is used for sending and receiving data to and from the AS 200 on ISP and that the metered T1 only be used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

**Step 1: Configure interface addresses.**

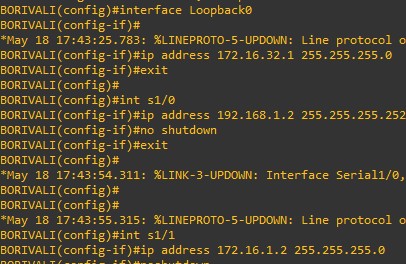
**Router R1 (hostname ISP):**



**Router R2 (hostname Andheri):**



**Router R3 (hostname Borivali):**



**Step 2: Configure EIGRP.**

Configure EIGRP between Andheri and Borvali routers. (Note: If using an IOS prior to 15.0, use the no auto-summary router configuration command to disable automatic summarization. This command is the default beginning with IOS 15.).

**Router R2 (hostname Andheri):**



**Router R3 (hostname Borivali):**



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

a) Configure IBGP between the Andheri and Borivali routers. On the Andheri router, enter the following configuration.

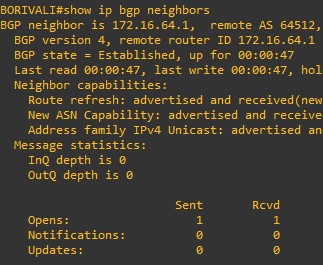


If multiple pathways to the BGP neighbor exist, the router can use multiple IP interfaces to communicate with the neighbor. The source IP address therefore depends on the outgoing interface. The **update-source lo0** command instructs the router to use the IP address of the interface Loopback0 as the source IP address for all BGP messages sent to that neighbor.

b) Complete the IBGP configuration on Borivali using the following commands.

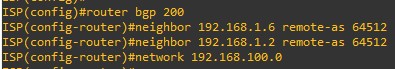


c) Verify that Andheri and Borivali become BGP neighbors by issuing the **show ip bgp neighbors** command on Andheri. View the following partial output. If the BGP state is not established, troubleshoot the connection.



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

a) Configure ISP to run EBGP with Andheri and Borivali. Enter the following commands on ISP.



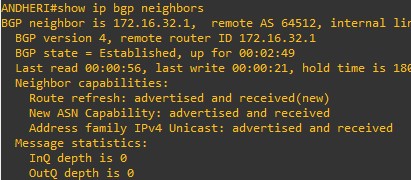
b) Configure a discard static route for the 172.16.0.0/16 network. Any packets that do not have a more specific match (longer match) for a 172.16.0.0 subnet will be dropped instead of sent to the ISP. Later in this lab we will configure a default route to the ISP.



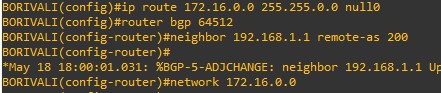
c) Configure Andheri as an EBGP peer to ISP.



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

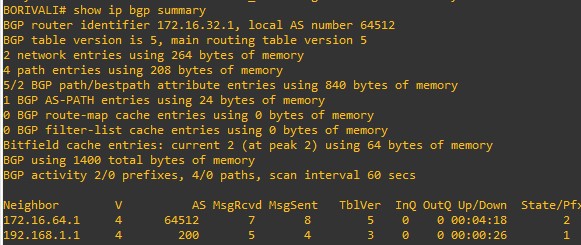


Configure a discard static route for 172.16.0.0/16 on Borivali and as an EBGP peer to ISP.



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

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

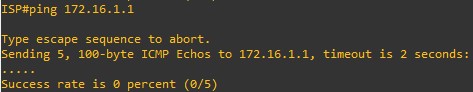
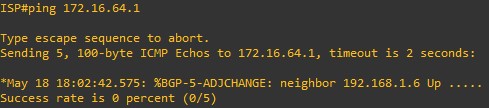


**Step 6: Verify which path the traffic takes.**

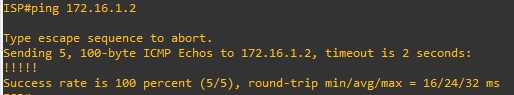
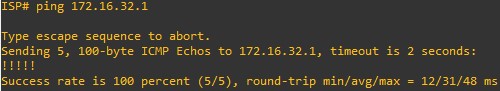
a) Clear the IP BGP conversation with the **clear ip bgp \*** command on ISP. Wait for the conversations to reestablish with each router.



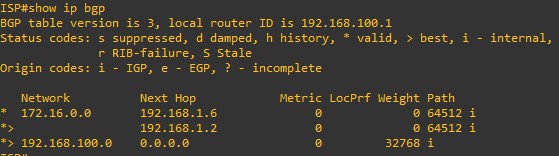
b) Test whether ISP can ping the loopback 0 address of 172.16.64.1 on Andheri and the serial link between Andheri and Borivali, 172.16.1.1.



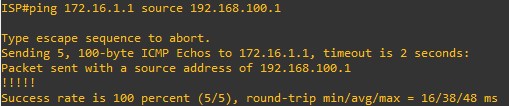
c) Now ping from ISP to the loopback 0 address of 172.16.32.1 on Borivali and the serial link between Andheri and Borivali, 172.16.1.2.

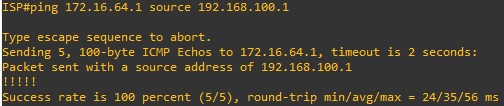
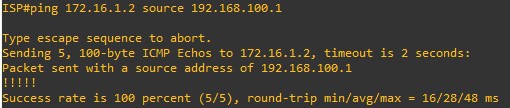
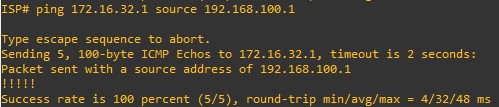


d) Issue the **show ip bgp** command on ISP to verify BGP routes and metrics.



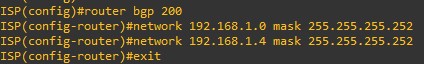
e) At this point, the ISP router should be able to get to each network connected to Andheri and Borivali from the loopback address 192.168.100.1. Use the extended **ping** command and specify the source address of ISP Lo0 to test.



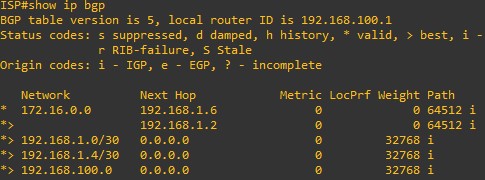


**Step 7: Configure the BGP next-hop-self feature.**

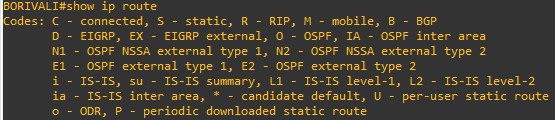
a) Issue the following commands on the ISP router.



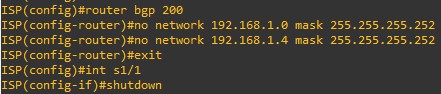
b) Issue the **show ip bgp** command to verify that the ISP is correctly injecting its own WAN links into BGP.



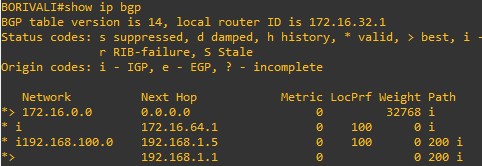
c) Verify on Andheri and Borivali that the opposite WAN link is included in the routing table. The output from Borivali is as follows.

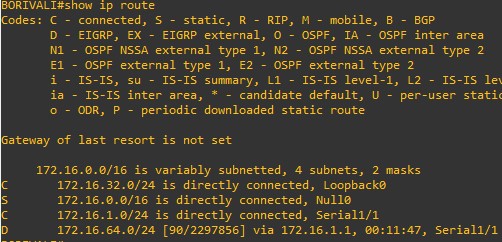


d) To better understand the **next-hop-self** command we will remove ISP advertising its two WAN links and shutdown the WAN link between ISP and Borivali. The only possible path from Borivali to ISP’s 192.168.100.0/24 is through Andheri.



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







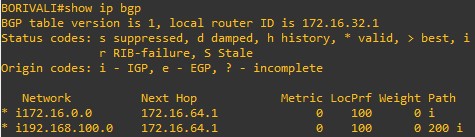


f) Reset BGP operation on either router with the **clear ip bgp \*** command.

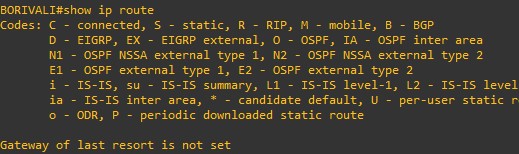




g) After the routers have returned to established BGP speakers, issue the **show ip bgp** command on Borivali and notice that the next hop is now Andheri instead of ISP.

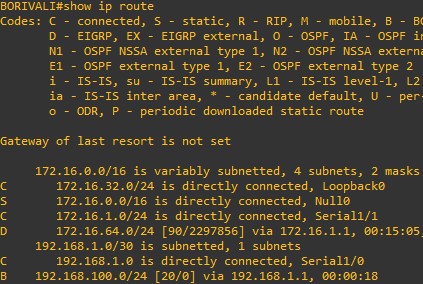


h) The **show ip route** command on Borivali now displays the 192.168.100.0/24 network because Andheri is the next hop, 172.16.64.1, which is reachable from Borivali.



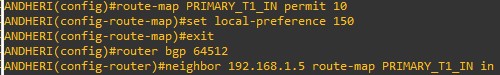
i) Before configuring the next BGP attribute, restore the WAN link between ISP and SanJose3. This will change the BGP table and routing table on both routers. For example, Borivali’s routing table shows 192.168.100.0/24 will now have a better path through ISP.

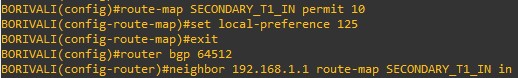




**Step 8: Set BGP local preference.**

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

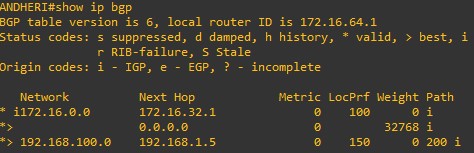


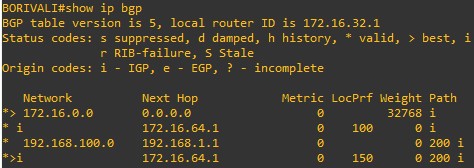


b) Use the **clear ip bgp \* soft** command after configuring this new policy. When the conversations have been reestablished, issue the **show ip bgp** command on Andheri and Borivali.



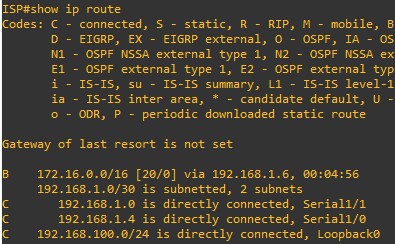
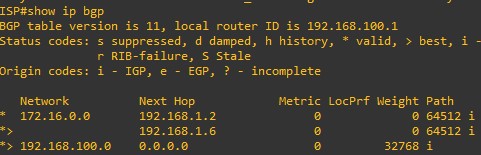




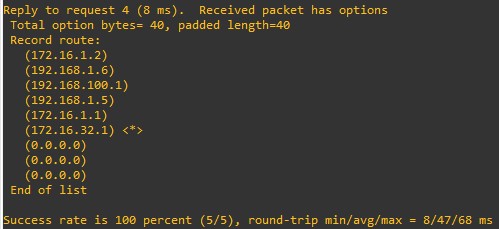


**Step 9: Set BGP MED.**

a) In the previous step we saw that Andheri and Borivali will route traffic for 192.168.100.0/24 using the link between Andheri 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.



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



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. Aping that is sourced from 172.16.32.1 exits Borivali through s0/0/1, 172.16.1.2. It then arrives at the s0/0/1 interface for Andheri.

2.Andheri S0/0/0, 192.168.1.6, routes the packet out to arrive at the S0/0/0 interface of ISP.

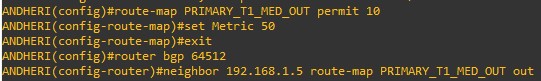
3. The target of 192.168.100.1 is reached: 192.168.100.1.

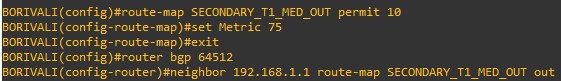
4. The packet is next forwarded out the S0/0/1, 192.168.1.1 interface for ISP and arrives at the S0/0/0 interface for Borivali.

5. Borivali then forwards the packet out the last interface, loopback 0, 172.16.32.1.

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

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

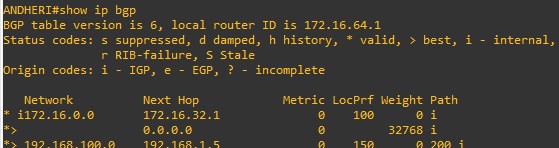


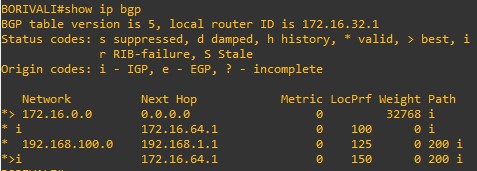


c) Use the **clear ip bgp \* soft** command after issuing this new policy. Issuing the **show ip bgp** command as follows on Andheri or Borivali does not indicate anything about this newly defined policy.

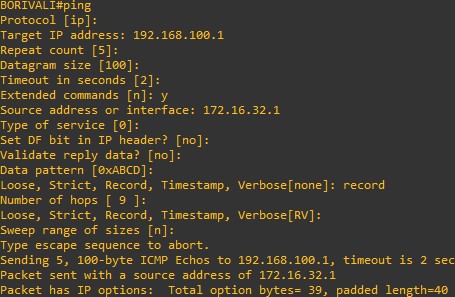


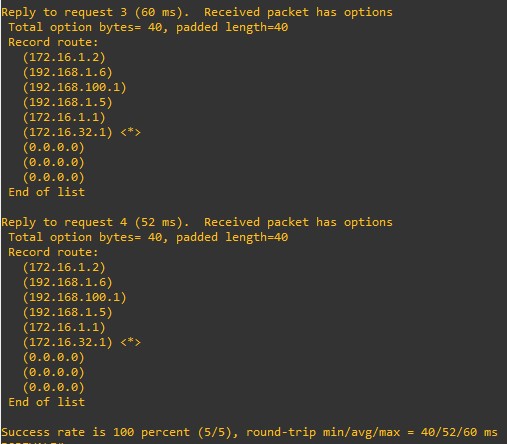


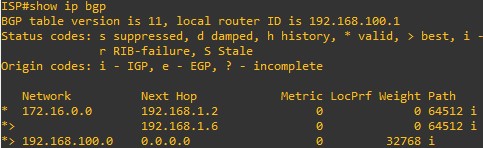




Reissue an extended **ping** command with the **record** command. Notice the change in return path using the exit interface 192.168.1.5 to Andheri.







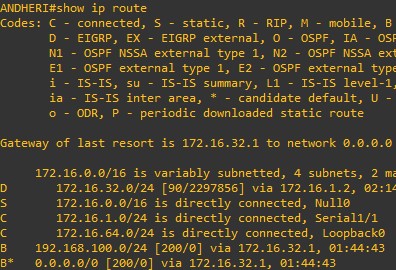
**Step 10: Establish a default route.**

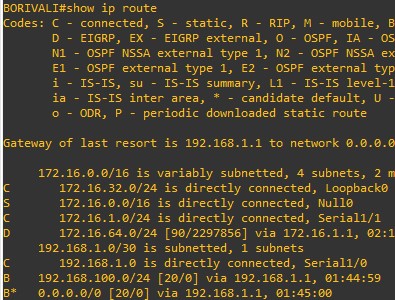
The final step is to establish a default route that uses a policy statement that adjusts to changes in the network.

a) Configure ISP to inject a default route to both Andheri and Borivali 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 Andheri and Borivali.

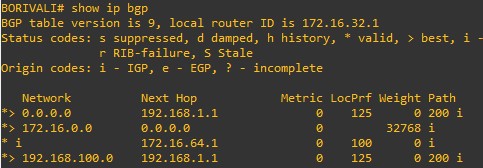


b) Verify that both routers have received the default route by examining the routing tables on Andheri and Borivali. Notice that both routers prefer the route between Andheri and ISP.





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



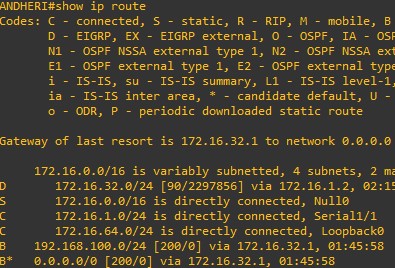
d) Using the traceroute command verify that packets to 10.0.0.1 is using the default route through Andheri.

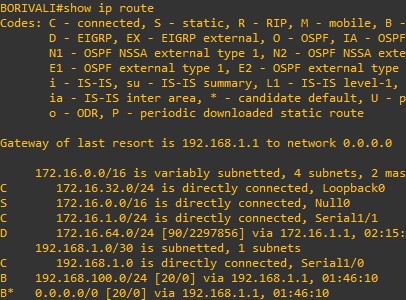


e) Next, test how BGP adapts to using a different default route when the path between Andheri and ISP goes down.

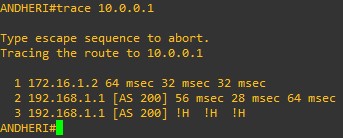


f) Verify that both routers are modified their routing tables with the default route using the path between Borivali and ISP.





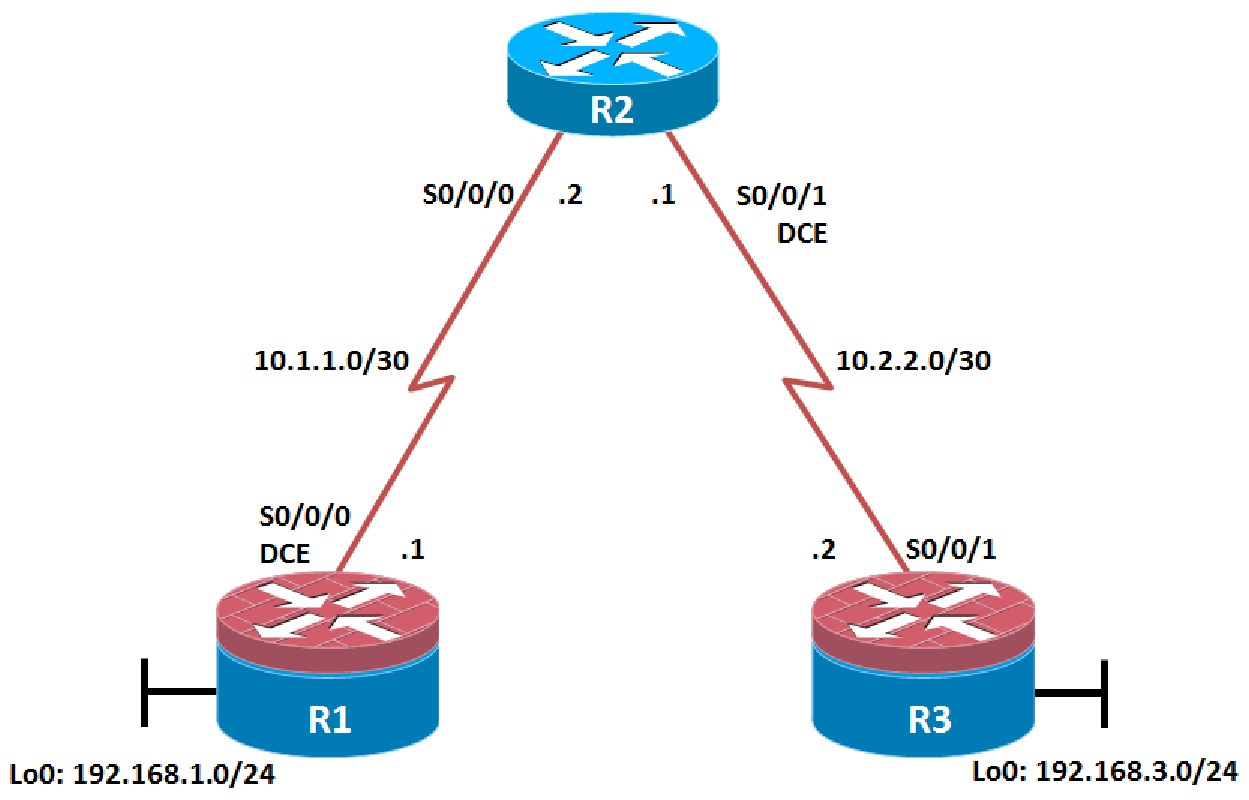
g) Verify the new path using the traceroute command to 10.0.0.1 from Andheri. Notice the default route is now through Borivali.



**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**

**foreach address {**

**192.168.1.1**

**10.1.1.1**

**10.1.1.2**

**10.2.2.1**

**10.2.2.2**

**192.168.3.1**

**} { ping $address }**

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**

1. Configure the enable secret encrypted password on both routers.

R1(config)# **enable secret class12345**

1. Configure a console password and enable login for routers. For additional security, the **exectimeout** command causes the line to log out after 5 minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

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**

R1(config)#

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.

w. 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-2pa55w0rd** 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.**

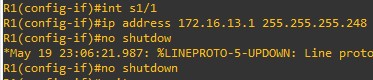
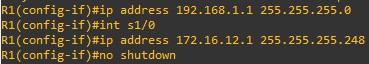
a) Cable the network as shown in the topology diagram. Erase the startup configuration, and reload each router to clear previous configurations.

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

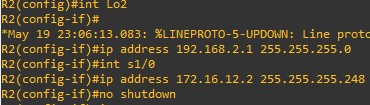
You can copy and paste the following configurations into your routers to begin.

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

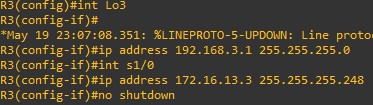
**Router R1**



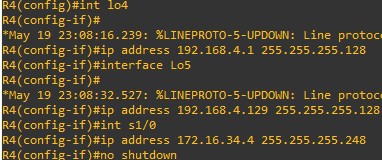
**Router R2**



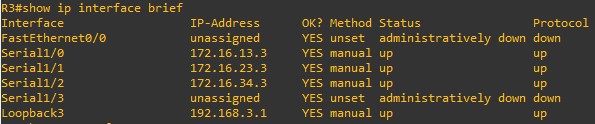
**Router R3**

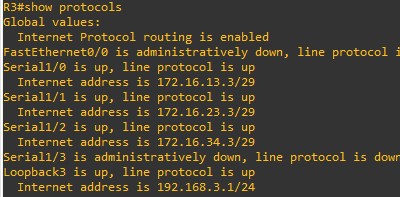


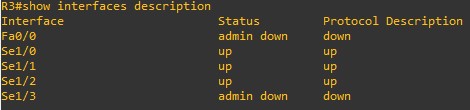
**Router R4**



c) 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.







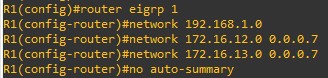
**Step 3: Configure basic EIGRP.**

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

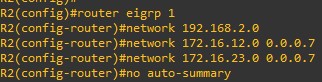
b) Advertise networks 172.16.12.0/29, 172.16.13.0/29, 172.16.23.0/29, 172.16.34.0/29, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, and 192.168.4.0/24 from their respective routers.

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

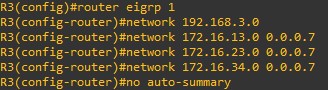
**Router R1**



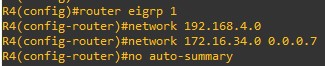
**Router R2**



**Router R3**



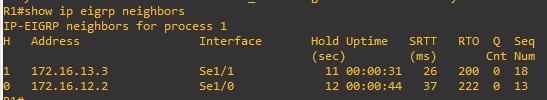
**Router R4**

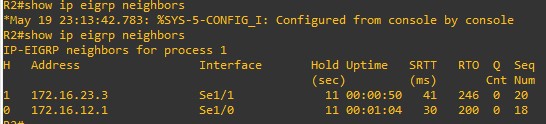


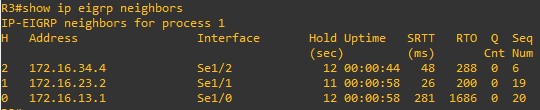
You should see EIGRP neighbor relationship messages being generated.

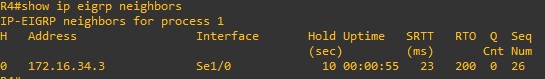
**Step 4: Verify EIGRP connectivity.**

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

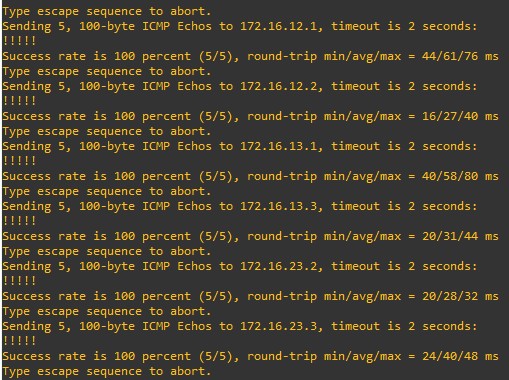
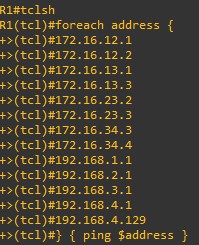








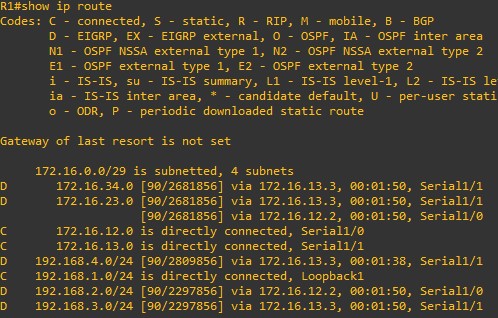
b) Run the following Tcl script on all routers to verify full connectivity.

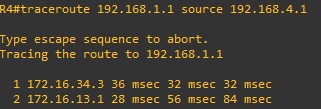


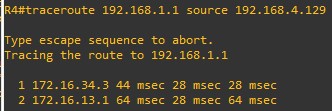
**Step 5: Verify the current path.**

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

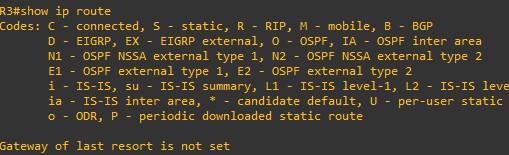
a) On R1, use the **show ip route** command. Notice the next-hop IP address for all networks discovered by EIGRP.

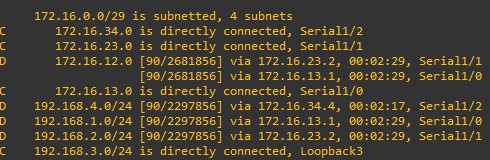




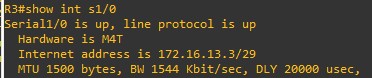


b) On R3, use the **show ip route** command and note that the preferred route from R3 to R1 LAN 192.168.1.0/24 is via R2 using the R3 exit interface S0/0/1.

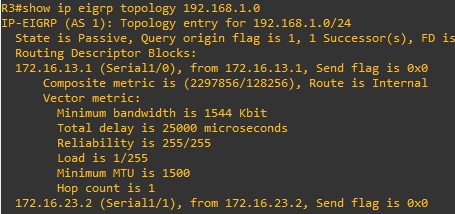




c) On R3, use the **show interfaces serial 0/0/0** and **show interfaces s0/0/1** commands. R3# **show interfaces serial0/0/0**



d) 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.



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

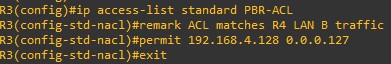
The steps required to implement path control include the following:

* 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.

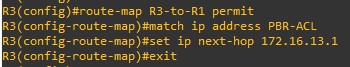
As a test, you will configure the following policy on router R3:

* 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.

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



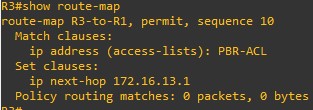
b) Create a route map called **R3-to-R1** that matches PBR-ACL and sets the next-hop interface to the R1 serial 0/0/1 interface.



c) Apply the R3-to-R1 route map to the serial interface on R3 that receives the traffic from R4. Use the **ip policy route-map** command on interface S0/1/0.

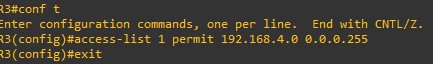


d) On R3, display the policy and matches using the **show route-map** command.

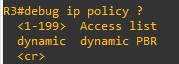


**Step 7: Test the policy.**

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

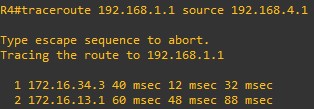


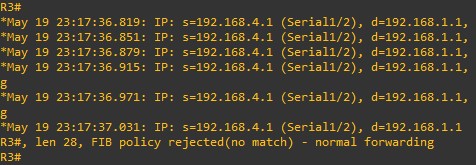
b) Enable PBR debugging only for traffic that matches the R4 LANs.



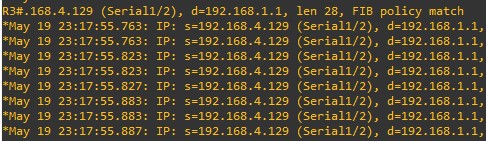
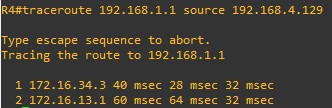


c) Test the policy from R4 with the **traceroute** command, using R4 LAN A as the source network.

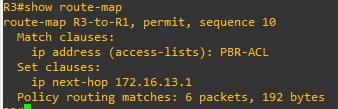




d) Test the policy from R4 with the **traceroute** command, using R4 LAN B as the source network.



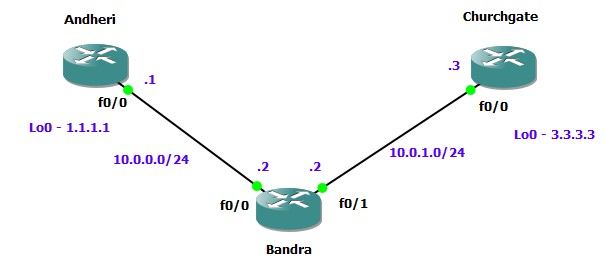
e) On R3, display the policy and matches using the **show route-map** command.



**Practical No - 6**

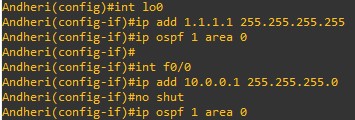
**Aim:**  Cisco MPLS Configuration

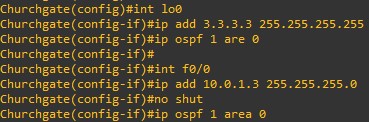
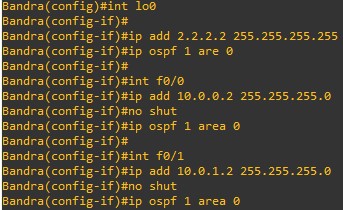
**Topology:**



**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

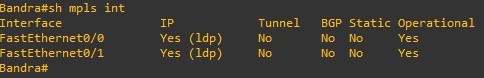


You should see log messages coming up showing the LDP neighbors are up.



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

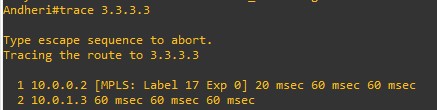
This is done on R2 and you can see that both interfaces are running mpls and using LDP



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

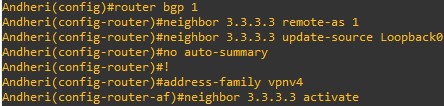


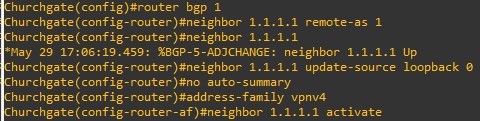
One more verification to confirm LDP is running ok is to do a trace between R1 and R3 and verify if you get MPLS Labels show up in the trace.



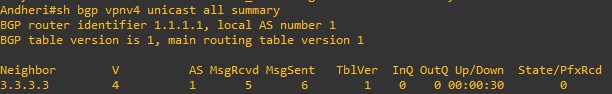
**Step 3: MPLS BGP Configuration between R1 and R3**

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



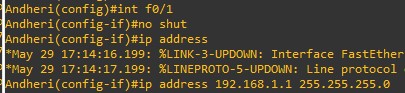
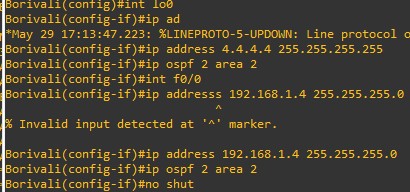


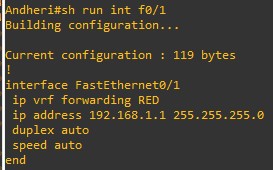
To verify the BGP session between R1 and R3 issue the command sh bgp vpnv4 unicast all summary



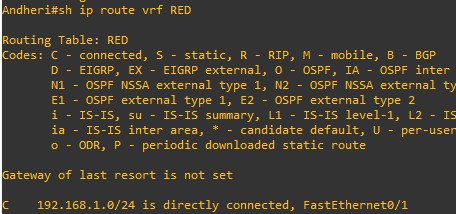
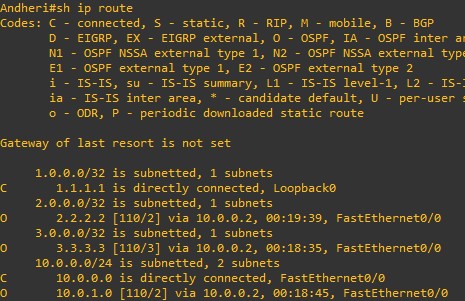
**Step 4: Add two more routers, create VRFs**

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





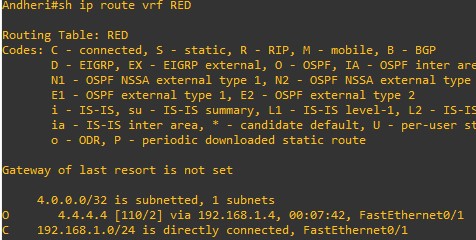
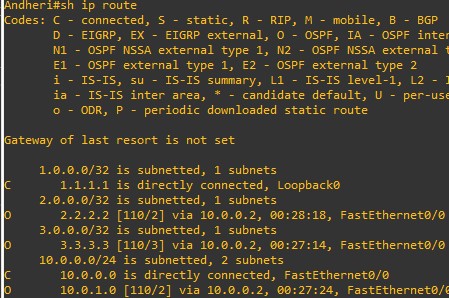
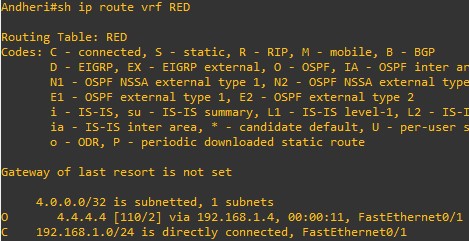
If you issue the command sh ip route this shows the routes in the global table and you will notice that you do not see 192.168.1.0/24



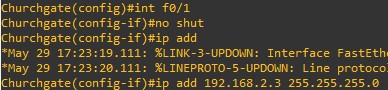
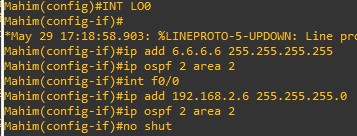
We just need to enable OSPF on this interface and get the loopback address for R4 in the VRF RED routing table before proceeding.



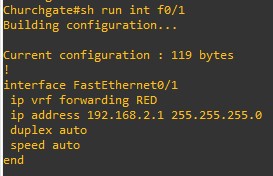
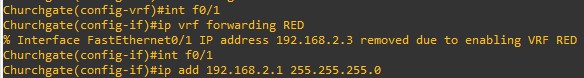
If we now check the routes in the VRF RED routing table you should see 4.4.4.4 in there as well.



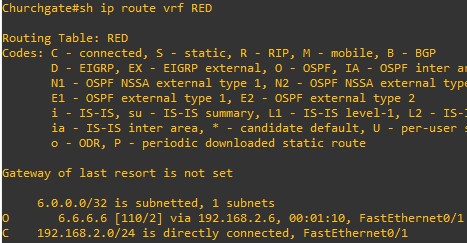
We now need to repeat this process for R3 & R6 Router 6 will peer OSPF using process number 2 to a VRF configured on R3. It will use the local site addressing to 192.168.2.0/24



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

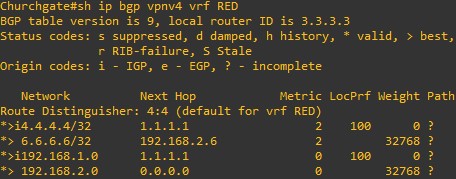
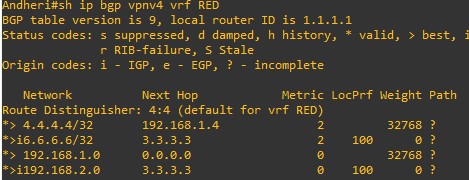
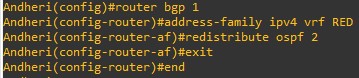
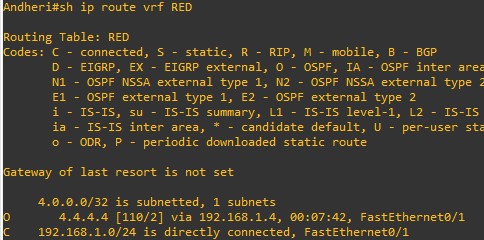
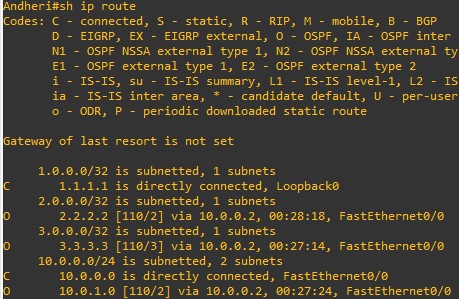
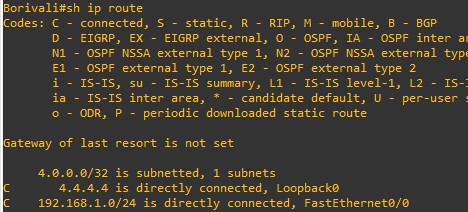
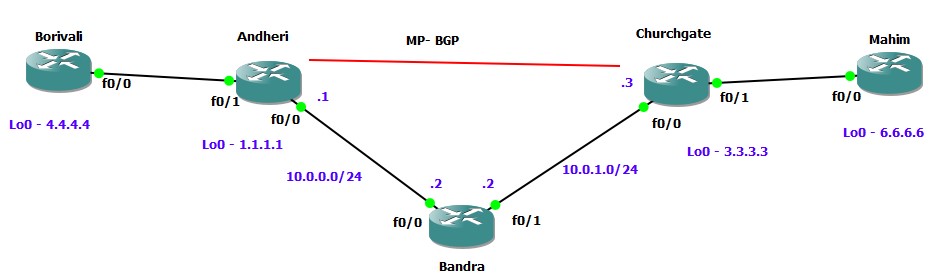


Check the router in vrf RED



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

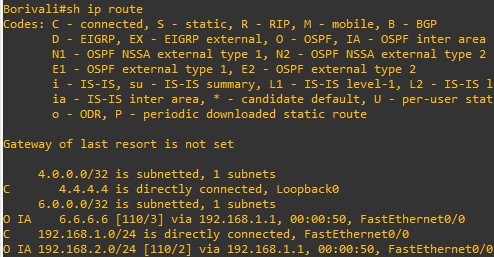
As expected we have the local interface and the loopback address. When we are done we want to see 6.6.6.6 in there so we can ping across the MPLS Check the routes on R1



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)



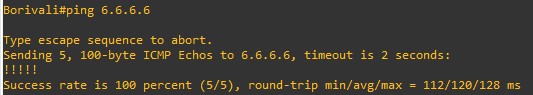
Before we do let’s see what the routing table look like on R4



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

