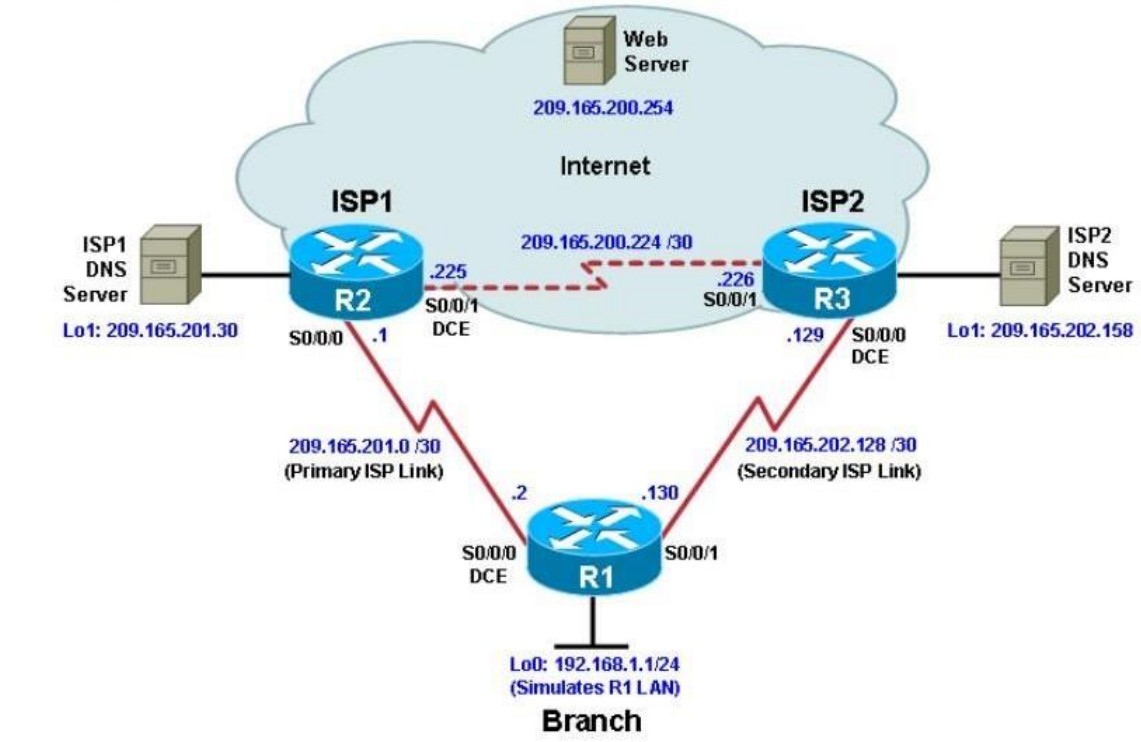
INDEX

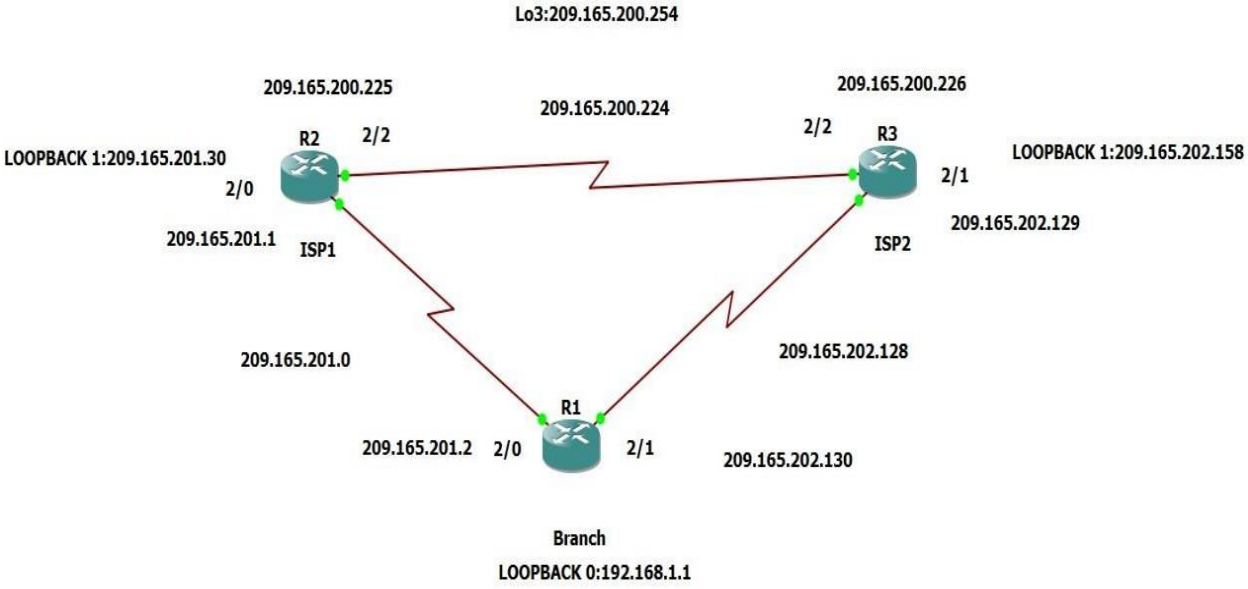
Sr. No.	Practical	Date	Signature
1	Configure IP SLA Tracking and Path Control T	18/02/23	
2	Using the AS_PATH Attribute	18/03/23	
3	Configuring IBGP and EBGP Sessions, Local Preference, and MED	08/04/23	
4	Secure the Management Plane	23/04/23	
5	Configure and Verify Path Control Using PBR	14/04/23	

Practical 1

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.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Services or comparable)
- Serial and console cables

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

a. Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear the previous configurations. Using the addressing scheme in the diagram, create the loopback interfaces and apply IP addresses to them as well as the serial interfaces on R1, ISP1, and ISP2. You can copy and paste the following configurations into your routers to begin.

R1:

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface loopback 0
R1(config-if)#
*Apr 10 14:09:07.235: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#description R1 LAN
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#interface serial 2/0
R1(config-if)#description R1 -->ISP1
R1(config-if)#ip address 209.165.201.2 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#bandwidth 128
R1(config-if)#no shutdown
R1(config-if)#
*Apr 10 14:13:23.995: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
R1(config-if)#
*Apr 10 14:13:24.999: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R1(config-if)#
*Apr 10 14:13:51.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
R1(config-if)#interface serial 2/1
R1(config-if)#description R1-->ISP2
R1(config-if)#ip address 209.165.202.130 255.255.255.252
R1(config-if)#bandwidth 128
R1(config-if)#no shutdown
```

ISP1:

```
R2(config)#hostname ISP1
ISP1(config)#interface loopback 0
ISP1(config-if)#
*Apr 10 14:18:19.655: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISP1(config-if)#description Simulated Internet Web Server
ISP1(config-if)#ip address 209.165.200.254 255.255.255.255
ISP1(config-if)#exit
ISP1(config)#interface loopback 1
ISP1(config-if)#
*Apr 10 14:46:55.423: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
ISP1(config-if)#description ISP1 DNS Server
ISP1(config-if)#ip address 209.165.201.30 255.255.255.255
ISP1(config-if)#exit
ISP1(config)#interface serial 2/0
ISP1(config-if)#description ISP1-->R1
ISP1(config-if)#ip address 209.165.201.30 255.255.255.255
Bad mask /32 for address 209.165.201.30
ISP1(config-if)#ip address 209.165.201.1 255.255.255.255
Bad mask /32 for address 209.165.201.1
ISP1(config-if)#ip address 209.165.201.1 255.255.255.255
Bad mask /32 for address 209.165.201.1
ISP1(config-if)#interface serial 2/0
ISP1(config-if)#description ISP1-->R1
ISP1(config-if)#ip address 209.165.201.1 255.255.255.252
ISP1(config-if)#bandwidth 128
ISP1(config-if)#no shut
ISP1(config-if)#e
*Apr 10 14:53:55.419: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
ISP1(config-if)#exit
*Apr 10 14:53:56.423: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
ISP1(config-if)#exit
ISP1(config)#interface serial 2/2
ISP1(config-if)#description ISP1-->ISP2
ISP1(config-if)#ip address 209.165.200.225 255.255.255.252
ISP1(config-if)#clock rate 128000
ISP1(config-if)#bandwidth 128
ISP1(config-if)#no shut
```

ISP2:

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#hostname ISP2
ISP2(config)#interface loopback 0
ISP2(config-if)#
*Apr 10 15:34:23.983: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISP2(config-if)#description ISP2 DNS Server
ISP2(config-if)#description Simulated Internet Web Server
ISP2(config-if)#ip address 209.165.200.254 255.255.255.255
ISP2(config-if)#exit
ISP2(config)#interface loopback 1
ISP2(config-if)#desc
*Apr 10 15:42:59.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
ISP2(config-if)#description ISP2 DNS Server
ISP2(config-if)#ip address 209.165.202.158 255.255.255.255
ISP2(config-if)#exit
ISP2(config)#interface serial 2/1
ISP2(config-if)#description ISP2-->R1
ISP2(config-if)#ip address 209.165.202.129 255.255.255.252
ISP2(config-if)#clock rate 128000
ISP2(config-if)#bandwidth 128
ISP2(config-if)#no shut
ISP2(config-if)#
*Apr 10 15:45:00.335: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
ISP2(config-if)#
*Apr 10 15:45:01.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
ISP2(config-if)#exit
ISP2(config)#interface se2/2
ISP2(config-if)#description ISP2-->ISP1
ISP2(config-if)#ip address 209.165.200.226 255.255.255.252
ISP2(config-if)#bandwidth 128
ISP2(config-if)#no shut
ISP2(config-if)#exit
```

b. Verify the configuration by using the show interfaces description command.

R1:

```
R1#show interfaces description | include up
Se2/0                          up             up       R1 -->ISP1
Se2/1                          up             up       R1-->ISP2
Lo0                            up             up       R1 LAN
```

ISP1:

```
ISP1#show interfaces description | include up
Se2/0                          up             up       ISP1-->R1
Se2/2                          up             up       ISP1-->ISP2
Lo0                            up             up       Simulated Internet Web Server
Lo1                            up             up       ISP1 DNS Server
```

ISP2:

```
ISP2#show interfaces description | include up
Se2/1                          up             up       ISP2-->R1
Se2/2                          up             up       ISP2-->ISP1
Lo0                            up             up       Simulated Internet Web Server
Lo1                            up             up       ISP2 DNS Server
```

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.

R1:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.1
R1(config)#end
R1#
*Apr 10 16:03:28.315: %SYS-5-CONFIG_I: Configured from console by consol
```

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.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.1
R1(config)#end
R1#
*Apr 10 16:03:28.315: %SYS-5-CONFIG_I: Configured from console by console
R1#tclsh
R1(tcl)#foreach address {
+>(tcl)#209.165.200.254
+>(tcl)#209.165.201.30
+>(tcl)#209.165.202.158
+>(tcl)#} {
+>(tcl)#ping $address source 192.168.1.1
+>(tcl)#}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.254, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/48/124 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/32/60 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.158, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/71/80 ms
```

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.

```
R1(tcl)#foreach address {
+>(tcl)#209.165.200.254
+>(tcl)#209.165.201.30
+>(tcl)#209.165.202.158
+>(tcl)#} {
+>(tcl)#trace $address source 192.168.1.1
+>(tcl)#}
Type escape sequence to abort.
Tracing the route to 209.165.200.254
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.201.1 144 msec 32 msec 28 msec
Type escape sequence to abort.
Tracing the route to 209.165.201.30
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.201.1 28 msec 24 msec 40 msec
Type escape sequence to abort.
Tracing the route to 209.165.202.158
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.201.1 16 msec 28 msec 32 msec
  2 209.165.200.226 44 msec 60 msec 44 msec
```

Step 3: Configure IP SLA probes.

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

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

```
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
R1(config)#end
R1#
```

b. 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
```

c. 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: 28 milliseconds
Latest operation start time: 16:15:06 UTC Mon Apr 10 2023
Latest operation return code: OK
Number of successes: 9
Number of failures: 0
Operation time to live: Forever
```

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.

```
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)#ip sla schedule 22 life forever start-time now
R1(config)#exit
R1#
*Apr 10 16:17:56.723: %SYS-5-CONFIG_I: Configured from console by console
```

e. 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
```

```
R1#show ip sla statistics 22
IPSLAs Latest Operation Statistics

IPSLA operation id: 22
        Latest RTT: 52 milliseconds
Latest operation start time: 16:18:42 UTC Mon Apr 10 2023
Latest operation return code: OK
Number of successes: 6
Number of failures: 0
Operation time to live: Forever
```

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.

```
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
R1#
*Apr 10 16:20:29.343: %SYS-5-CONFIG_I: Configured from console by console
```

b. 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, Serial2/0
L        209.165.201.2/32 is directly connected, Serial2/0
      209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.202.128/30 is directly connected, Serial2/1
L        209.165.202.130/32 is directly connected, Serial2/1
```

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

&

d. 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 1 ip sla 11 reachability
R1(config-track)#delay down 10 up 1
R1(config-track)#exit
R1(config)#end
```

e. 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).

```
R1#debug ip routing
IP routing debugging is on
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1
R1(config)#
*Apr 10 16:25:11.983: RT: updating static 0.0.0.0/0 (0x0):
    via 209.165.201.1   1048578

*Apr 10 16:25:11.987: RT: closer admin distance for 0.0.0.0, flushing 1 routes
*Apr 10 16:25:11.987: RT: add 0.0.0.0/0 via 209.165.201.1, static metric [2/0]
*Apr 10 16:25:11.991: RT: updating static 0.0.0.0/0 (0x0):
    via 209.165.201.1   1048578

*Apr 10 16:25:11.995: RT: rib update return code: 17
*Apr 10 16:25:11.999: RT: updating static 0.0.0.0/0 (0x0):
    via 209.165.201.1   1048578

*Apr 10 16:25:12.003: RT: rib update return code: 17
R1(config)#track 2 ip sla 22 reachability
R1(config-track)#delay down 10 up 1
R1(config-track)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.129 3 track 2
R1(config)#
*Apr 10 16:28:05.103: RT: updating static 0.0.0.0/0 (0x0):
    via 209.165.201.1   1048578

*Apr 10 16:28:05.107: RT: updating static 0.0.0.0/0 (0x0):
    via 209.165.201.1   1048578

*Apr 10 16:28:05.111: RT: rib update return code: 17
```

f. 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#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

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, Serial2/0
L        209.165.201.2/32 is directly connected, Serial2/0
      209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.202.128/30 is directly connected, Serial2/1
L        209.165.202.130/32 is directly connected, Serial2/1
```

Step 5: Verify IP SLA operation.

a. Shortly after the loopback interface is administratively down, observe the debug output being generated on R1.

b. Verify the routing table.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

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, Serial2/0
L        209.165.201.2/32 is directly connected, Serial2/0
      209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.202.128/30 is directly connected, Serial2/1
L        209.165.202.130/32 is directly connected, Serial2/1
```

c. 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: 16:32:36 UTC Mon Apr 10 2023
Latest operation return code: Timeout
Number of successes: 97
Number of failures: 17
Operation time to live: Forever



IPSLA operation id: 22
        Latest RTT: 20 milliseconds
```

d. 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 60 msec 64 msec 36 msec
R1#
```

e. To examine the routing behavior when connectivity to the ISP1 DNS is restored, re-enable the DNS address on ISP1 (R2) by issuing the no shutdown command on the loopback 1 interface on ISP2.

```
R1#
*Apr 10 16:34:10.799: %TRACKING-5-STATE: 1 ip sla 11 reachability Down->Up
*Apr 10 16:34:10.803: RT: updating static 0.0.0.0/0 (0x0):
    via 209.165.201.1   1048578

*Apr 10 16:34:10.807: RT: closer admin distance for 0.0.0.0, flushing 1 routes
*Apr 10 16:34:10.807: RT: add 0.0.0.0/0 via 209.165.201.1, static metric [2/0]
*Apr 10 16:34:10.811: RT: updating static 0.0.0.0/0 (0x0):
    via 209.165.202.129   1048578

*Apr 10 16:34:10.815: RT: rib update return code: 17
*Apr 10 16:34:10.819: RT: updating static 0.0.0.0/0 (0x0):
    via 209.165.202.129   1048578

*Apr 10 16:34:10.823: RT: rib update return code: 17
*Apr 10 16:34:10.823: RT: updating static 0.0.0.0/0 (0x0):
    via 209.165.201.1   1048578

*Apr 10 16:34:10.823: RT:
```

f. Again, examine the IP SLA statistics.

```
R1#show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 11
        Latest RTT: 20 milliseconds
Latest operation start time: 16:34:56 UTC Mon Apr 10 2023
Latest operation return code: OK
Number of successes: 103
Number of failures: 25
Operation time to live: Forever



IPSLA operation id: 22
        Latest RTT: 56 milliseconds
Latest operation start time: 16:35:02 UTC Mon Apr 10 2023
Latest operation return code: OK
Number of successes: 101
Number of failures: 3
Operation time to live: Forever
```

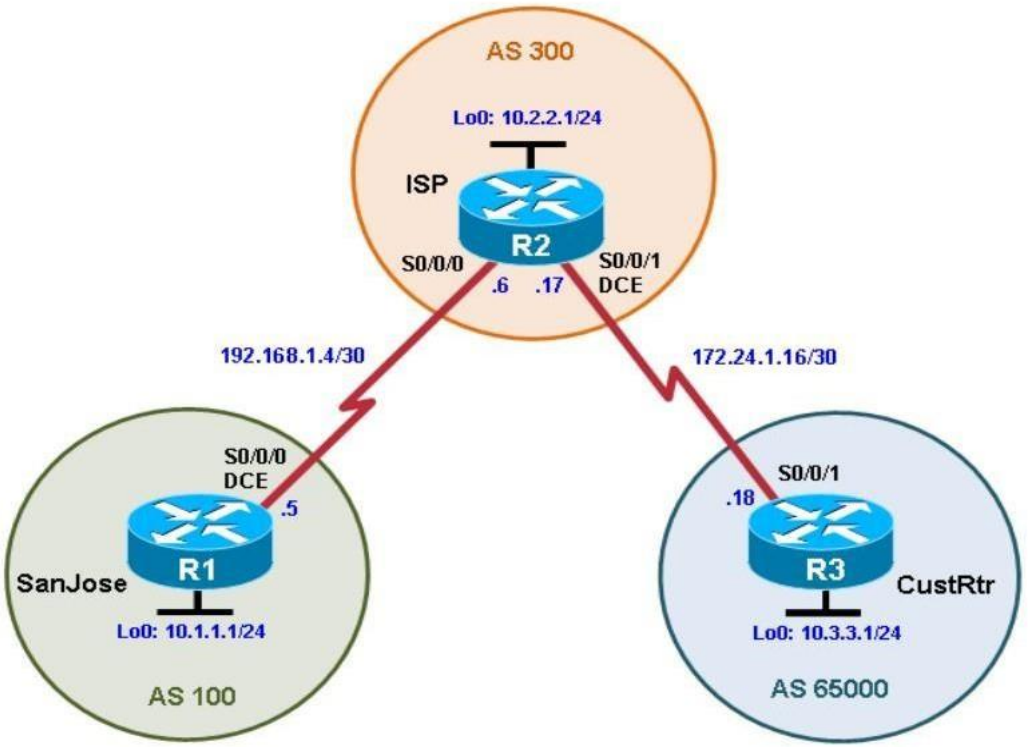
g. Verify the routing table.

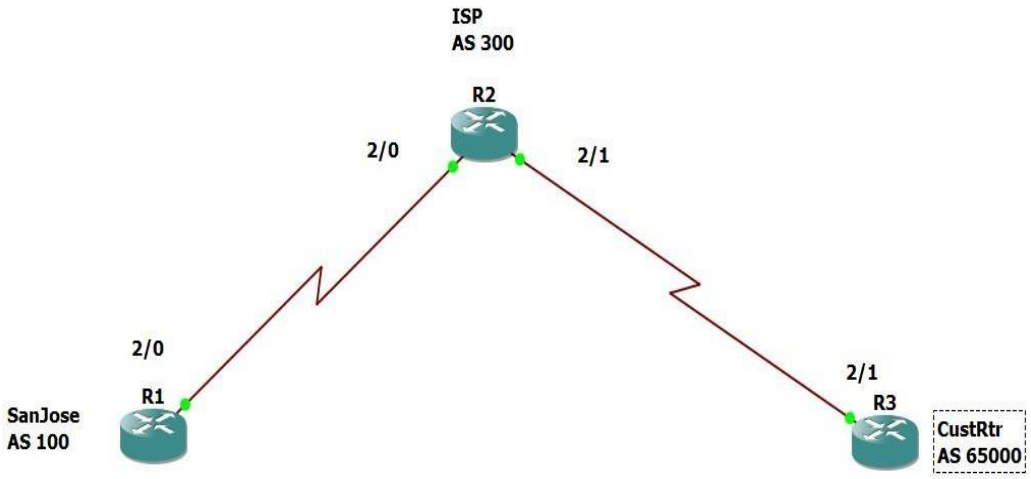
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

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, Serial2/0
L        209.165.201.2/32 is directly connected, Serial2/0
      209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.202.128/30 is directly connected, Serial2/1
L        209.165.202.130/32 is directly connected, Serial2/1
```

Practical 2

Using the AS_PATH Attribute

Topology





Objectives

- 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 numbers.

Background

The International Travel Agency's ISP has been assigned an AS number of 300. This provider uses BGP to exchange routing information with several customer networks. Each customer network is assigned an AS number from the private range, such as AS 65000. Configure the ISP router to remove the private AS numbers from the AS Path information of CustRtr. In addition, the ISP would like to prevent its customer networks from receiving route information from International Travel Agency's AS 100. Use the AS_PATH attribute to implement this policy.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Services or comparable)
- Serial and console cables

Step 1: Prepare the routers for the lab.

R1

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname SanJose
SanJose(config)#no ip domain-lookup
SanJose(config)#line con 0
SanJose(config-line)#logging synchronous
SanJose(config-line)#exec-timeout 0 0
SanJose(config-line)#exit
```

R2

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#line con 0
ISP(config-line)#logging synchronous
ISP(config-line)#exec-timeout 0 0
```

R3

```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#hostname CustRtr
CustRtr(config)#no ip domain-lookup
CustRtr(config)#line con 0
CustRtr(config-line)#logging synchronous
CustRtr(config-line)#exec-timeout 0 0
```

Step 2: Configure the hostname and interface addresses.

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

```
SanJose(config)#interface Loopback 0
SanJose(config-if)#
*Mar 19 01:03:18.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
SanJose(config-if)#ip address 10.1.1.1 255.255.255.0
SanJose(config-if)#exit
SanJose(config)#interface serial 2/0
SanJose(config-if)#ip address 192.168.1.5 255.255.255.252
SanJose(config-if)#clock rate 128000
SanJose(config-if)#no shutdown
SanJose(config-if)#end
*Mar 19 01:13:50.403: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
SanJose(config-if)#end
*Mar 19 01:13:51.411: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
SanJose(config-if)#end
SanJose#
*Mar 19 01:13:58.655: %SYS-5-CONFIG_I: Configured from console by console
```

```
ISP(config-line)#interface Loopback 0
ISP(config-if)#
*Mar 19 01:18:02.467: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISP(config-if)#ip address 10.2.2.1 255.255.255.0
ISP(config-if)#interface serial 2/0
ISP(config-if)#ip address 192.168.1.6 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#
*Mar 19 01:19:14.151: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
ISP(config)#
*Mar 19 01:19:15.159: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
ISP(config)#interface serial 2/0
ISP(config-if)#ip address 192.168.1.6 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#interface serial 2/1
ISP(config-if)#ip address 172.24.1.17 255.255.255.252
ISP(config-if)#clockrate 128000
ISP(config-if)#no shutdown
ISP(config-if)#end
ISP#
*Mar 19 01:21:29.875: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
ISP#
*Mar 19 01:21:30.575: %SYS-5-CONFIG_I: Configured from console by console
ISP#
*Mar 19 01:21:30.883: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
ISP#
*Mar 19 01:21:58.667: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to down
ISP#
```

```
CustRtr(config-line)#interface Loopback 0
CustRtr(config-if)#
*Mar 19 01:22:11.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
CustRtr(config-if)#ip address 10.3.3.1 255.255.255.0
CustRtr(config-if)#exit
CustRtr(config)#interface serial 2/1
CustRtr(config-if)#ip address 172.24.1.18 255.255.255.252
CustRtr(config-if)#no shutdown
CustRtr(config-if)#end
*Mar 19 01:24:01.263: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
CustRtr(config-if)#end
*Mar 19 01:24:02.271: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
CustRtr(config-if)#end
CustRtr#
*Mar 19 01:24:10.691: %SYS-5-CONFIG_I: Configured from console by console
```

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.

```
SanJose#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SanJose(config)#router bgp 100
SanJose(config-router)#neighbor 192.168
% Incomplete command.

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

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#router bgp 300
ISP(config-router)#neighbor 192.168.1.5 remote-as 100
ISP(config-router)#neighbor 192.168.1.5 remote-as 65000
*Mar 19 01:29:22.011: %BGP-5-ADJCHANGE: neighbor 192.168.1.5 Up
ISP(config-router)#neighbor 172.24.1.18 remote-as 65000
ISP(config-router)#network 10.2.2.0 mask 255.255.255.0
ISP(config-router)#
*Mar 19 01:31:36.139: %BGP-5-ADJCHANGE: neighbor 172.24.1.18 Up
ISP(config-router)#exit
ISP(config)#exit
ISP#
```

```
CustRtr#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CustRtr(config)#router bgp 65000
CustRtr(config-router)#neighbor 172.24.1.17 remote-as 300
CustRtr(config-router)#network
*Mar 19 01:31:36.235: %BGP-5-ADJCHANGE: neighbor 172.24.1.17 Up
CustRtr(config-router)#network 10.3.3.0 mask 255.255.255.0
CustRtr(config-router)#
*Mar 19 01:44:28.623: %BGP-5-NBR_RESET: Neighbor 172.24.1.17 reset (Peer closed the session)
*Mar 19 01:44:28.631: %BGP-5-ADJCHANGE: neighbor 172.24.1.17 Down Peer closed the session
*Mar 19 01:44:28.635: %BGP_SESSION-5-ADJCHANGE: neighbor 172.24.1.17 IPv4 Unicast topology base removed from session  Peer closed the session
CustRtr(config-router)#
*Mar 19 01:44:29.635: %BGP-5-ADJCHANGE: neighbor 172.24.1.17 Up
CustRtr(config-router)#
*Mar 19 01:50:55.563: %BGP-5-NBR_RESET: Neighbor 172.24.1.17 reset (Peer closed the session)
```

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

```
ISP#
*Mar 19 01:32:02.519: %SYS-5-CONFIG_I: Configured from console by console
ISP#show ip bgp neighbors
BGP neighbor is 172.24.1.18,  remote AS 65000, external link
  BGP version 4, remote router ID 10.3.3.1
```

Step 4: Remove the private AS.

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

```
SanJose#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Loopback0
L        10.1.1.1/32 is directly connected, Loopback0
B        10.2.2.0/24 [20/0] via 192.168.1.6, 00:02:30
B        10.3.3.0/24 [20/0] via 192.168.1.6, 00:01:11
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.4/30 is directly connected, Serial2/0
L        192.168.1.5/32 is directly connected, Serial2/0
```

b. Ping the 10.3.3.1 address from SanJose.

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

```
SanJose#ping
Protocol [ip]:
Target IP address: 10.3.3.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/61/84 ms
```

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

```
SanJose#show ip bgp
BGP table version is 4, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.1.1.0/24     0.0.0.0                  0         32768 i
 *>  10.2.2.0/24     192.168.1.6              0             0 300 i
 *>  10.3.3.0/24     192.168.1.6                            0 300 65000 i
```

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

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

```
SanJose#ping 10.3.3.1 source lo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/87/108 ms
```

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

```
SanJose#show ip bgp
BGP table version is 8, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.1.1.0/24     0.0.0.0                  0         32768 i
 *>  10.2.2.0/24     192.168.1.6              0             0 300 i
```

Step 5: Use the AS_PATH attribute to filter routes.

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

```
ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
B        10.1.1.0/24 [20/0] via 192.168.1.5, 00:00:13
C        10.2.2.0/24 is directly connected, Loopback0
L        10.2.2.1/32 is directly connected, Loopback0
B        10.3.3.0/24 [20/0] via 172.24.1.18, 00:00:13
      172.24.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.24.1.16/30 is directly connected, Serial2/1
L        172.24.1.17/32 is directly connected, Serial2/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.4/30 is directly connected, Serial2/0
L        192.168.1.6/32 is directly connected, Serial2/0
```

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

```
CustRtr#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
B        10.2.2.0/24 [20/0] via 172.24.1.17, 00:01:36
C        10.3.3.0/24 is directly connected, Loopback0
L        10.3.3.1/32 is directly connected, Loopback0
      172.24.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.24.1.16/30 is directly connected, Serial2/1
L        172.24.1.18/32 is directly connected, Serial2/1
CustRtr#
```

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

```
ISP#show ip bgp regexp ^100$
BGP table version is 4, local router ID is 10.2.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.1.1.0/24     192.168.1.5              0             0 100 i
```

d.Run the following Tcl script on all routers to verify whether there is connectivity. All pings from ISP should be successful. SanJose should not be able to ping the CustRtr loopback

10.3.3.1 or the WAN link 172.24.1.16/30. CustRtr should not be able to ping the SanJose loopback 10.1.1.1 or the WAN link 192.168.1.4/30.

```
ISP(tcl)#foreach address {
+>10.1.1.1
+>10.2.2.1
+>10.3.3.1
+>192.168.1.5
+>192.168.1.6
+>172.24.1.17
+>172.24.1.18
+>} {
+>ping $address }
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 = 20/34/48 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, 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 10.3.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/28/44 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/35/44 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/61/76 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.1.17, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/60/64 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.1.18, timeout is 2 seconds:
!!!!!
```

NOTES

- **BGP(Border Gateway Protocol):-**

- It is a protocol which directs packets between autonomous system.
- BGP creates network stability which guarantees routers to quickly adapt it to send packets through another network.
- There are various BGP protocols such as EIGRP, OSPF, RIP which works on various attributes.
- BGP is used to root the packet and it is exterior gateway protocol, which is used to root the packets between different networks.

- It makes routing decisions based on path's network policy rules set and configured by network administrator etc.

O BGP attributes:-

- BGP chooses a route to a network based on attributes of its path. Following are the 4 categories of attributes:

i) Well known mandatory

It must be recognized by all BGP routers present in all BGP updates and passed on to other BGP routers.
E.g AS_PATH origin and next hop.

ii) Well known discretionary:-

It must be recognized by all BGP routers and passed on to other BGP routers & need not be present in an update.
E.g Local preference

iii) Optional transitive:-

May or may not be recognized by BGP routers but is passed on to other BGP routers. If it is not recognized, it is marked as partial. E.g Aggregator & community.

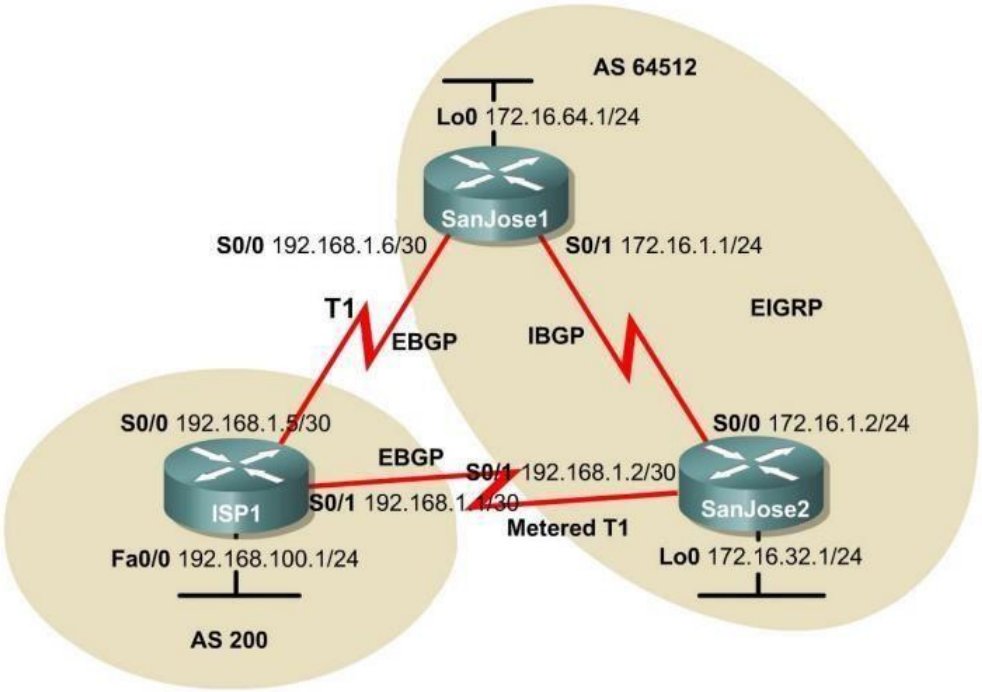
iv) Optional non-transitive:-

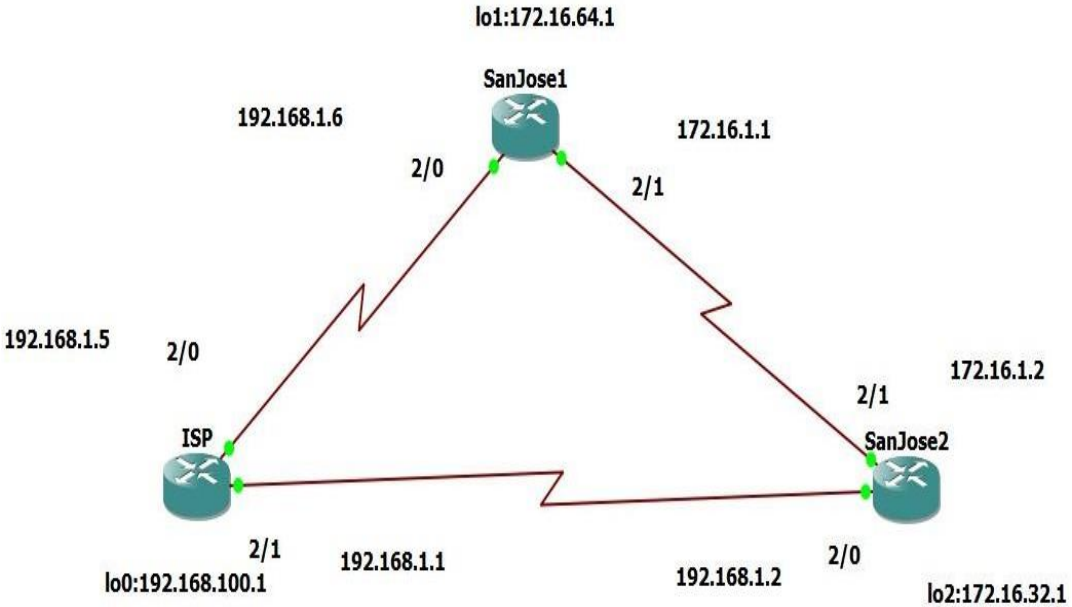
If the BGP process does not recognize the attributes then it can ignore the updates & not advertise the path to its peers.
E.g Multi Exit Discriminatory(MED) & Originator ID.

O AS_PATH :- It is an BGP attribute which is of type well known and mandatory.

Practical 3

Configuring IBGP and EBGP Sessions, Local Preference, and MED





Objective

In this lab, the student will configure both IBGP and EBGP. In order for IBGP peers to correctly exchange routing information, the next-hop-self command must be used. Use of LocalPreference and MED attributes must also be used. This is to insure that the flat rate unlimited use T1 link is used for sending and receiving data to and from the AS 200 on ISP. The metered T1 should only be used in the event that the primary T1 link has failed. Traffic sent across the metered T1 link offers the same bandwidth of the primary link but at a huge expense. Insure that this link is not used unnecessarily.

Background

The International Travel Agency runs BGP on its SanJose1 and SanJose2 routers externally with the ISP router in AS 200. IBGP is run internally between SanJose1 and SanJose2. Your job is to configure both EBGP and IBGP for this internetwork to allow for redundancy. The metered T1 should only be used in the event that the primary T1 link has failed. Traffic sent across the metered T1 link offers the same bandwidth of the primary link but at a huge expense. Ensure that this link is not used unnecessarily.

Required Resources

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

Step 0: Suggested starting configurations.

Apply the following configuration to each router along with the appropriate hostname. The exec-timeout 0 0 command should only be used in a lab environment.

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#no ip domain-lookup
ISP(config)#line con 0
ISP(config-line)#logging synchronous
ISP(config-line)#exec-timeout 0 0
ISP(config-line)#exit
```

```
SanJose1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SanJose1(config)#no ip domain-lookup
SanJose1(config)#line con 0
SanJose1(config-line)#logging synchronous
SanJose1(config-line)#exec-timeout 0 0
SanJose1(config-line)#exit
```

```
SanJose2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SanJose2(config)#no ip domain-lookup
SanJose2(config)#line con 0
SanJose2(config-line)#logging synchronous
SanJose2(config-line)#exec-timeout 0 0
SanJose2(config-line)#conf t
                     ^
% Invalid input detected at '^' marker.

SanJose2(config-line)#exit
```

Step 1: Configure interface addresses.

Using the addressing scheme in the diagram, create the loopback interfaces and apply IPv4 addresses to these and the serial interfaces on ISP (R1), SanJose1 (R2), and SanJose2 (R3).

```
ISP(config)#interface Loopback0
ISP(config-if)#
*Apr 12 20:37:17.251: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ISP(config-if)#ip address 192.168.100.1 255.255.255.0
ISP(config-if)#exit
ISP(config)#interface serial 2/0
ISP(config-if)#ip address 192.168.1.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#
*Apr 12 20:40:30.111: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
ISP(config)#
*Apr 12 20:40:31.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
ISP(config)#interface serial 2/1
ISP(config-if)#
*Apr 12 20:40:59.347: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
ISP(config-if)#ip address 192.168.1.1 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#end
*Apr 12 20:41:26.583: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
ISP(config-if)#end
ISP#
*Apr 12 20:41:27.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
ISP#
*Apr 12 20:41:27.939: %SYS-5-CONFIG_I: Configured from console by console
ISP#
*Apr 12 20:41:49.363: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to down
ISP#
*Apr 12 20:43:29.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
```

```
SanJose1(config)#interface Loopback0
SanJose1(config-if)#
*Apr 12 20:41:53.311: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
SanJose1(config-if)#ip address 172.16.64.1 255.255.255.0
SanJose1(config-if)#exit
SanJose1(config)#interface serial 2/0
SanJose1(config-if)#ip address 192.168.1.6 255.255.255.252
SanJose1(config-if)#no shutdown
SanJose1(config-if)#exit
SanJose1(config)#
*Apr 12 20:43:14.755: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
SanJose1(config)#
*Apr 12 20:43:15.763: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
SanJose1(config)#interface serial 2/1
SanJose1(config-if)#ip address 172.16.1.1 255.255.255.0
SanJose1(config-if)#clock rate 128000
SanJose1(config-if)#no shutdown
SanJose1(config-if)#end
*Apr 12 20:44:13.191: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
SanJose1(config-if)#end
SanJose1#
*Apr 12 20:44:14.199: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
SanJose1#
*Apr 12 20:44:14.427: %SYS-5-CONFIG_I: Configured from console by console
SanJose1#
*Apr 12 20:44:39.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to down
SanJose1#
*Apr 12 20:47:29.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
SanJose1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
SanJose2(config)#interface Loopback0
SanJose2(config-if)#ip
*Apr 12 20:44:46.395: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
SanJose2(config-if)#ip address 172.16.32.1 255.255.255.0
SanJose2(config-if)#exit
SanJose2(config)#interface serial 2/0
SanJose2(config-if)#ip address 192.168.1.2 255.255.255.252
SanJose2(config-if)#clock rate 128000
SanJose2(config-if)#no shutdown
SanJose2(config-if)#exi
*Apr 12 20:46:26.847: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
SanJose2(config-if)#exit
*Apr 12 20:46:27.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
SanJose2(config-if)#exit
SanJose2(config)#interface serial 2/1
SanJose2(config-if)#ip address 172.16.1.2 255.255.255.0
SanJose2(config-if)#no shutdown
SanJose2(config-if)#end
SanJose2#
*Apr 12 20:47:18.743: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
*Apr 12 20:47:19.287: %SYS-5-CONFIG_I: Configured from console by console
SanJose2#
*Apr 12 20:47:19.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
```

Step 2: Configure EIGRP.

```
SanJose1(config)#router eigrp 1
SanJose1(config-router)#network 172.16.0.0
SanJose1(config-router)#
*Apr 12 20:49:26.375: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.1.2 (Serial2/1) is up: new adjacency
SanJose1(config-router)#exit
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
SanJose2(config)#router eigrp 1
SanJose2(config-router)#network 172.16.0.0
SanJose2(config-router)#
*Apr 12 20:49:26.419: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.1.1 (Serial2/1) is up: new adjacency
SanJose2(config-router)#exit
```

Step 3: Configure IBGP and verify BGP neighbors.

a. 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
SanJose1(config-router)#
*Apr 12 20:51:42.815: %BGP-5-ADJCHANGE: neighbor 172.16.32.1 Up
SanJose1(config-router)#exit
```

b. 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 172.16.6
*Apr 12 20:51:42.863: %BGP-5-ADJCHANGE: neighbor 172.16.64.1 Up
SanJose2(config-router)#neighbor 172.16.64.1 update-source lo0
SanJose2(config-router)#end
SanJose2#sho
*Apr 12 20:52:06.715: %SYS-5-CONFIG_I: Configured from console by console
```

c. 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
BGP neighbor is 172.16.64.1,  remote AS 64512, internal link
  BGP version 4, remote router ID 172.16.64.1
  BGP state = Established, up for 00:00:34
  Last read 00:00:34, last write 00:00:34, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          1
    Keepalives:             2          2
```

Step 4: Configure EBGP and verify BGP neighbors.

a. 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
ISP(config-router)#
*Apr 12 20:55:43.019: %BGP-5-ADJCHANGE: neighbor 192.168.1.6 Up
ISP(config-router)#
*Apr 12 20:58:48.419: %BGP-5-ADJCHANGE: neighbor 192.168.1.2 Up
ISP(config-router)#end
ISP#
*Apr 12 20:59:31.871: %SYS-5-CONFIG_I: Configured from console by console
```

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

&

c.Configure SanJose1 as an EBGP peer to ISP.

```
SanJose1(config)#ip route 172.16.0.0 255.255.0.0 null0
SanJose1(config)#router bgp 64512
SanJose1(config-router)#neighbor 192.168.1.5 remote-as 200
SanJose1(config-router)#network
*Apr 12 20:55:42.631: %BGP-5-ADJCHANGE: neighbor 192.168.1.5 Up
SanJose1(config-router)#network 172.16.0.0
```

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

```
SanJose1#
*Apr 12 20:56:23.479: %SYS-5-CONFIG_I: Configured from console by console
SanJose1#show ip bgp neighbors
BGP neighbor is 172.16.32.1,  remote AS 64512, internal link
  BGP version 4, remote router ID 172.16.32.1
  BGP state = Established, up for 00:04:54
  Last read 00:00:27, last write 00:00:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
```

```
BGP neighbor is 192.168.1.5,  remote AS 200, external link
  BGP version 4, remote router ID 192.168.100.1
  BGP state = Established, up for 00:00:54
  Last read 00:00:03, last write 00:00:23, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                2          2
    Keepalives:             2          3
    Route Refresh:          0          0
    Total:                  5          6
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  Session: 192.168.1.5
  BGP table version 3, neighbor version 3/0
  Output queue size : 0
  Index 2, Advertise bit 1
  2 update-group member
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                               Sent       Rcvd
  Prefix activity:             ----       ----
```

e. Configure a discard static route for 172.16.0.0/16 on SanJose2 and as an EBGP peer to ISP.

```
SanJose2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SanJose2(config)#ip route 172.16.0.0 255.255.0.0 null0
SanJose2(config)#router bgp 64512
SanJose2(config-router)#neighbor 192.168.1.1 remote-as 200
SanJose2(config-router)#netwok
*Apr 12 20:58:48.079: %BGP-5-ADJCHANGE: neighbor 192.168.1.1 Up
SanJose2(config-router)#network 172.16.0.0
SanJose2(config-router)#end
SanJose2#
*Apr 12 20:59:03.683: %SYS-5-CONFIG_I: Configured from console by console
```

Step 5: View BGP summary output.

```
SanJose2#show ip bgp summary
BGP router identifier 172.16.32.1, local AS number 64512
BGP table version is 4, main routing table version 4
2 network entries using 288 bytes of memory
4 path entries using 320 bytes of memory
4/2 BGP path/bestpath attribute entries using 544 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1176 total bytes of memory
BGP activity 2/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.64.1     4        64512      13      13        4    0    0 00:07:31        2
192.168.1.1     4          200       7       5        2    0    0 00:00:25        1
SanJose2#
*Apr 12 20:59:41.127: %BGP-5-NBR_RESET: Neighbor 192.168.1.1 reset (Peer closed the session)
*Apr 12 20:59:41.135: %BGP-5-ADJCHANGE: neighbor 192.168.1.1 Down Peer closed the session
*Apr 12 20:59:41.135: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.1.1 IPv4 Unicast topology base removed from session  Peer closed the session
*Apr 12 20:59:41.367: %BGP-5-ADJCHANGE: neighbor 192.168.1.1 Up
```

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 SanJose router.

```
ISP#clear ip bgp *
ISP#
*Apr 12 20:59:41.411: %BGP-5-ADJCHANGE: neighbor 192.168.1.2 Down User reset
*Apr 12 20:59:41.415: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.1.2 IPv4 Unicast topology base removed from session  User reset
*Apr 12 20:59:41.419: %BGP-5-ADJCHANGE: neighbor 192.168.1.6 Down User reset
*Apr 12 20:59:41.423: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.1.6 IPv4 Unicast topology base removed from session  User reset
*Apr 12 20:59:41.723: %BGP-5-ADJCHANGE: neighbor 192.168.1.2 Up
*Apr 12 20:59:41.743: %BGP-5-ADJCHANGE: neighbor 192.168.1.6 Up
```

b. 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 and 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 172.16.64.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.64.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ISP#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ISP#ping 172.16.32.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.32.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/32/48 ms
ISP#ping 172.16.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
```

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

```
ISP#show ip bgp
BGP table version is 3, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *   172.16.0.0       192.168.1.6              0             0 64512 i
 *>                   192.168.1.2              0             0 64512 i
 *>  192.168.100.0    0.0.0.0                  0         32768 i
```

d.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
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/46/60 ms
ISP#ping 172.16.32.1 source 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.32.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/26/32 ms
ISP#ping 172.16.1.2 source 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/30/48 ms
ISP#ping 172.16.64.1 source 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.64.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/52/68 ms
```

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

a. Issue the following commands on the ISP router.

```
Enter configuration commands, one per line.  End with CNTL/Z.
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
ISP(config-router)#end
ISP#s
*Apr 12 21:04:43.691: %SYS-5-CONFIG_I: Configured from console by console
```

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

```
ISP#show ip bgp
BGP table version is 5, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *   172.16.0.0       192.168.1.6              0             0 64512 i
 *>                   192.168.1.2              0             0 64512 i
 *>  192.168.1.0/30   0.0.0.0                  0         32768 i
 *>  192.168.1.4/30   0.0.0.0                  0         32768 i
 *>  192.168.100.0    0.0.0.0                  0         32768 i
```

c. 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
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
S        172.16.0.0/16 is directly connected, Null0
C        172.16.1.0/24 is directly connected, Serial2/1
L        172.16.1.2/32 is directly connected, Serial2/1
C        172.16.32.0/24 is directly connected, Loopback0
L        172.16.32.1/32 is directly connected, Loopback0
D        172.16.64.0/24 [90/2297856] via 172.16.1.1, 00:15:48, Serial2/1
      192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial2/0
L        192.168.1.2/32 is directly connected, Serial2/0
B        192.168.1.4/30 [20/0] via 192.168.1.1, 00:00:24
B     192.168.100.0/24 [20/0] via 192.168.1.1, 00:04:59
```

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

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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 2/1
ISP(config-if)#shutdown
ISP(config-if)#
*Apr 12 21:15:40.739: %BGP-5-NBR_RESET: Neighbor 192.168.1.2 reset (Interface flap)
*Apr 12 21:15:40.767: %BGP-5-ADJCHANGE: neighbor 192.168.1.2 Down Interface flap
*Apr 12 21:15:40.767: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.1.2 IPv4 Unicast topology base removed from session  Interface flap
ISP(config-if)#
*Apr 12 21:15:42.707: %LINK-5-CHANGED: Interface Serial2/1, changed state to administratively down
*Apr 12 21:15:43.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to down
```

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

```
SanJose2#show ip bgp
BGP table version is 12, local router ID is 172.16.32.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  172.16.0.0       0.0.0.0                  0         32768 i
 * i                  172.16.64.1              0    100      0 i
 * i 192.168.100.0    192.168.1.5              0    100      0 200 i
 *>                   192.168.1.1              0             0 200 i
SanJose2#
*Apr 12 21:16:09.327: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
SanJose2#
*Apr 12 21:16:09.339: %BGP-5-NBR_RESET: Neighbor 192.168.1.1 reset (Interface flap)
*Apr 12 21:16:09.363: %BGP-5-ADJCHANGE: neighbor 192.168.1.1 Down Interface flap
*Apr 12 21:16:09.367: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.1.1 IPv4 Unicast topology base removed from session  Interface flap
SanJose2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
S        172.16.0.0/16 is directly connected, Null0
C        172.16.1.0/24 is directly connected, Serial2/1
L        172.16.1.2/32 is directly connected, Serial2/1
C        172.16.32.0/24 is directly connected, Loopback0
L        172.16.32.1/32 is directly connected, Loopback0
```

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

```
*Apr 13 00:42:04.879: %BGP-5-ADJCHANGE: neighbor 192.168.1.5 Up
SanJose1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SanJose1(config)#router bgp 64512
SanJose1(config-router)#neighbor 172.16.32.1 next-hop-self
SanJose1(config-router)#end
SanJose1#clear
*Apr 13 00:59:53.663: %SYS-5-CONFIG_I: Configured from console by console
SanJose1#clear ip bgp *
SanJose1#
*Apr 13 01:00:00.379: %BGP-5-ADJCHANGE: neighbor 172.16.32.1 Down User reset
*Apr 13 01:00:00.379: %BGP_SESSION-5-ADJCHANGE: neighbor 172.16.32.1 IPv4 Unicast topology base removed from session  User reset
*Apr 13 01:00:00.387: %BGP-5-ADJCHANGE: neighbor 192.168.1.5 Down User reset
*Apr 13 01:00:00.387: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.1.5 IPv4 Unicast topology base removed from session  User reset
*Apr 13 01:00:01.179: %BGP-5-ADJCHANGE: neighbor 172.16.32.1 Up
*Apr 13 01:00:01.287: %BGP-5-ADJCHANGE: neighbor 192.168.1.5 Up
SanJose1#
*Apr 13 01:00:17.431: %BGP-5-NBR_RESET: Neighbor 172.16.32.1 reset (Peer closed the session)
*Apr 13 01:00:17.431: %BGP-5-ADJCHANGE: neighbor 172.16.32.1 Down Peer closed the session
*Apr 13 01:00:17.431: %BGP_SESSION-5-ADJCHANGE: neighbor 172.16.32.1 IPv4 Unicast topology base removed from session  Peer closed the session
*Apr 13 01:00:17.647: %BGP-5-ADJCHANGE: neighbor 172.16.32.1 Up
```

```
SanJose2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SanJose2(config)#router bgp 64512
SanJose2(config-router)#neighbor 172.16.64.1 next-hop-self
SanJose2(config-router)#
*Apr 13 01:00:00.139: %BGP-5-NBR_RESET: Neighbor 172.16.64.1 reset (Peer closed the session)
*Apr 13 01:00:00.147: %BGP-5-ADJCHANGE: neighbor 172.16.64.1 Down Peer closed the session
*Apr 13 01:00:00.151: %BGP_SESSION-5-ADJCHANGE: neighbor 172.16.64.1 IPv4 Unicast topology base removed from session  Peer closed the session
*Apr 13 01:00:00.891: %BGP-5-ADJCHANGE: neighbor 172.16.64.1 Up
SanJose2(config-router)#end
```

g. 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
BGP table version is 1, local router ID is 172.16.32.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *   172.16.0.0       0.0.0.0                  0         32768 i
 * i                  172.16.64.1        2169856    100      0 i
 * i 192.168.100.0    172.16.64.1              0    100      0 200 i
```

h. 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
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
S        172.16.0.0/16 is directly connected, Null0
C        172.16.1.0/24 is directly connected, Serial2/1
L        172.16.1.2/32 is directly connected, Serial2/1
C        172.16.32.0/24 is directly connected, Loopback0
L        172.16.32.1/32 is directly connected, Loopback0
D        172.16.64.0/24 [90/2297856] via 172.16.1.1, 00:30:04, Serial2/1
B     192.168.100.0/24 [200/0] via 172.16.64.1, 00:01:15
```

i. Before configuring the next BGP attribute, restore the WAN link between ISP and SanJose3.

```
ISP(config)#interface serial 2/1
ISP(config-if)#no shutdown
ISP(config-if)#
*Apr 13 01:03:23.259: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
ISP(config-if)#
*Apr 13 01:03:24.267: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
ISP(config-if)#
*Apr 13 01:03:40.303: %BGP-5-ADJCHANGE: neighbor 192.168.1.2 Up
ISP(config-if)#end
```

```
SanJose2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
S        172.16.0.0/16 is directly connected, Null0
C        172.16.1.0/24 is directly connected, Serial2/1
```

```
L        172.16.32.1/32 is directly connected, Loopback0
D        172.16.64.0/24 [90/2297856] via 172.16.1.1, 00:30:58, Serial2/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial2/0
L        192.168.1.2/32 is directly connected, Serial2/0
B     192.168.100.0/24 [200/0] via 172.16.64.1, 00:02:09
SanJose2#
*Apr 13 01:03:40.143: %BGP-5-ADJCHANGE: neighbor 192.168.1.1 Up
SanJose2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
S        172.16.0.0/16 is directly connected, Null0
C        172.16.1.0/24 is directly connected, Serial2/1
L        172.16.1.2/32 is directly connected, Serial2/1
C        172.16.32.0/24 is directly connected, Loopback0
L        172.16.32.1/32 is directly connected, Loopback0
D        172.16.64.0/24 [90/2297856] via 172.16.1.1, 00:31:47, Serial2/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial2/0
L        192.168.1.2/32 is directly connected, Serial2/0
B     192.168.100.0/24 [20/0] via 192.168.1.1, 00:00:46
```

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 SanJose1 and SanJose2. This policy adjusts outbound traffic to prefer the link off the SanJose1 router instead of the metered T1 off SanJose2.

```
SanJose1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
SanJose1(config-router)#end
SanJose1#
*Apr 13 01:08:13.791: %SYS-5-CONFIG_I: Configured from console by console
```

```
SanJose2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SanJose2(config)#route-map SECONDARY_T1_IN permit 10
SanJose2(config-route-map)#set local-preference 125
SanJose2(config-route-map)#exit
SanJose2(config)#router bgp 64512
SanJose2(config-router)#neighbor 192.168.1.1 route-map SECONDARY_T1_IN in
SanJose2(config-router)#end
```

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

```
SanJose1#clear ip bgp * soft
SanJose1#show ip bgp
BGP table version is 6, local router ID is 172.16.64.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 * i 172.16.0.0       172.16.32.1              0    100      0 i
 *>                   172.16.1.2         2169856         32768 i
 *>  192.168.100.0    192.168.1.5              0    150      0 200 i
```

```
SanJose2#clear
*Apr 13 01:08:30.639: %SYS-5-CONFIG_I: Configured from console by console
SanJose2#clear ip bgp * soft
SanJose2#show ip bgp
BGP table version is 5, local router ID is 172.16.32.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  172.16.0.0       0.0.0.0                  0         32768 i
 * i                  172.16.64.1        2169856    100      0 i
 *   192.168.100.0    192.168.1.1              0    125      0 200 i
 *>i                  172.16.64.1              0    150      0 200 i
```

Step 9: Set BGP MED.

a. Examine what the return path ISP takes to reach AS 64512.

```
ISP#show ip bgp
BGP table version is 12, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  172.16.0.0       192.168.1.2              0             0 64512 i
 *                    192.168.1.6        2169856             0 64512 i
 *>  192.168.100.0    0.0.0.0                  0         32768 i
ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     172.16.0.0/16 [20/0] via 192.168.1.2, 00:06:23
      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial2/1
L        192.168.1.1/32 is directly connected, Serial2/1
C        192.168.1.4/30 is directly connected, Serial2/0
L        192.168.1.5/32 is directly connected, Serial2/0
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, Loopback0
L        192.168.100.1/32 is directly connected, Loopback0
```

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

```
SanJose2#ping
Protocol [ip]:
Target IP address: 192.168.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.32.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.32.1
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)

Reply to request 0 (32 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (172.16.1.2)
    (192.168.1.6)
    (192.168.1.5)
```

```
 Record route:
    (172.16.1.2)
    (192.168.1.6)
    (192.168.1.5)
    (192.168.1.1)
    (192.168.1.2) <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
 End of list

Reply to request 1 (48 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (172.16.1.2)
    (192.168.1.6)
    (192.168.1.5)
    (192.168.1.1)
    (192.168.1.2) <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
 End of list

Reply to request 2 (40 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (172.16.1.2)
    (192.168.1.6)
    (192.168.1.5)
    (192.168.1.1)
    (192.168.1.2) <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
```

```
    (192.168.1.6)
    (192.168.1.5)
    (192.168.1.1)
    (192.168.1.2) <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
 End of list

Reply to request 3 (44 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (172.16.1.2)
    (192.168.1.6)
    (192.168.1.5)
    (192.168.1.1)
    (192.168.1.2) <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
 End of list

Reply to request 4 (20 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (172.16.1.2)
    (192.168.1.6)
    (192.168.1.5)
    (192.168.1.1)
    (192.168.1.2) <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
 End of list
```

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

```
SanJose1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SanJose1(config)#route-map PRIMARY_T1_MED_OUT permit 10
SanJose1(config-route-map)#set Metric 50
SanJose1(config-route-map)#exit
SanJose1(config)#router bgp 64512
SanJose1(config-router)#neighbor 192.168.1.5 route-map PRIMARY_T1_MED_OUT out
SanJose1(config-router)#end
SanJose1#
*Apr 13 01:18:09.471: %SYS-5-CONFIG_I: Configured from console by console
```

```
SanJose2#
SanJose2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
SanJose2(config-router)#$2.168.1.1 route-map SECONDARY_T1_MED_OUT out
SanJose2(config-router)#$2.168.1.1 route-map SECONDARY_T1_MED_OUT out
SanJose2(config-router)#end
SanJose2#
*Apr 13 01:18:24.083: %SYS-5-CONFIG_I: Configured from console by console
```

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

```
*Apr 13 01:08:13.791: %SYS-5-CONFIG_I: Configured from console by console
SanJose1#clear ip bgp * soft
SanJose1#show ip bgp
BGP table version is 6, local router ID is 172.16.64.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 * i 172.16.0.0       172.16.32.1              0    100      0 i
 *>                   172.16.1.2         2169856         32768 i
 *>  192.168.100.0    192.168.1.5              0    150      0 200 i
```

```
*Apr 13 01:18:24.083: %SYS-5-CONFIG_I: Configured from console by console
SanJose2#clear ip bgp * soft
SanJose2#show ip bgp
BGP table version is 5, local router ID is 172.16.32.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  172.16.0.0       0.0.0.0                  0         32768 i
 * i                  172.16.64.1        2169856    100      0 i
 *   192.168.100.0    192.168.1.1              0    125      0 200 i
 *>i                  172.16.64.1              0    150      0 200 i
```

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

```
SanJose2#ping
Protocol [ip]:
Target IP address: 192.168.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.32.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.32.1

Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)

Reply to request 0 (68 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
   (172.16.1.2)
   (192.168.1.6)
   (192.168.1.5)
   (192.168.1.5)
   (172.16.1.1)
   (172.16.1.2) <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
 End of list

Reply to request 1 (56 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
   (172.16.1.2)
   (192.168.1.6)
   (192.168.1.5)
   (192.168.1.5)
   (172.16.1.1)
   (172.16.1.2) <*>
   (0.0.0.0)
   (0.0.0.0)

 Total option bytes= 40, padded length=40
 Record route:
   (172.16.1.2)
   (192.168.1.6)
   (192.168.1.5)
   (192.168.1.5)
   (172.16.1.1)
   (172.16.1.2) <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
 End of list

Success rate is 100 percent (5/5), round-trip min/avg/max = 52/64/72 ms
```

```
ISP#show ip bgp
BGP table version is 13, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *   172.16.0.0       192.168.1.2              75             0 64512 i
 *>                   192.168.1.6              50             0 64512 i
 *>  192.168.100.0    0.0.0.0                   0         32768 i
```

Step 10: Establish a default route.

a.Configure ISP to inject a default route to both SanJose1 and SanJose2 using BGP using the **default-originate** command.

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#router bgp 200
ISP(config-router)#neighbor 192.168.1.6 default-originate
```

b. Verify that both routers have received the default route by examining the routing tables on SanJose1 and SanJose2.

```
SanJose1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.5 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 192.168.1.5, 00:00:11
      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
D        172.16.0.0/16 [90/2169856] via 172.16.1.2, 00:42:54, Serial2/1
C        172.16.1.0/24 is directly connected, Serial2/1
L        172.16.1.1/32 is directly connected, Serial2/1
D        172.16.32.0/24 [90/2297856] via 172.16.1.2, 00:50:57, Serial2/1
C        172.16.64.0/24 is directly connected, Loopback0
L        172.16.64.1/32 is directly connected, Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.4/30 is directly connected, Serial2/0
L        192.168.1.6/32 is directly connected, Serial2/0
B     192.168.100.0/24 [20/0] via 192.168.1.5, 00:15:12
SanJose1#
```

```
SanJose2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.64.1 to network 0.0.0.0

B*    0.0.0.0/0 [200/0] via 172.16.64.1, 00:00:25
      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
S        172.16.0.0/16 is directly connected, Null0
C        172.16.1.0/24 is directly connected, Serial2/1
L        172.16.1.2/32 is directly connected, Serial2/1
C        172.16.32.0/24 is directly connected, Loopback0
L        172.16.32.1/32 is directly connected, Loopback0
D        172.16.64.0/24 [90/2297856] via 172.16.1.1, 00:51:11, Serial2/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial2/0
L        192.168.1.2/32 is directly connected, Serial2/0
```

c. The preferred default route is by way of SanJose1 because of the higher local preference attribute configured on SanJose1 earlier and using the traceroute command verify that packets to 10.0.0.1 is using the default route through SanJose1.

```
SanJose2#how ip bgp
         ^
% Invalid input detected at '^' marker.

SanJose2#show ip bgp
BGP table version is 7, local router ID is 172.16.32.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0          172.16.64.1              0    150      0 200 i
 *                    192.168.1.1                   125      0 200 i
 *>  172.16.0.0       0.0.0.0                  0         32768 i
 * i                  172.16.64.1        2169856    100      0 i
 *   192.168.100.0    192.168.1.1              0    125      0 200 i
 *>i                  172.16.64.1              0    150      0 200 i
SanJose2#traceroute 10.0.0.1
Type escape sequence to abort.
Tracing the route to 10.0.0.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 20 msec 28 msec 32 msec
  2 192.168.1.5 [AS 200] 68 msec 56 msec 48 msec
```

d. 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
Type escape sequence to abort.
Tracing the route to 10.0.0.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 20 msec 28 msec 32 msec
  2 192.168.1.5 [AS 200] 68 msec 56 msec 48 msec
```

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

```
SanJose1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.32.1 to network 0.0.0.0

B*    0.0.0.0/0 [200/0] via 172.16.32.1, 00:00:43
      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
D        172.16.0.0/16 [90/2169856] via 172.16.1.2, 00:47:03, Serial2/1
C        172.16.1.0/24 is directly connected, Serial2/1
L        172.16.1.1/32 is directly connected, Serial2/1
D        172.16.32.0/24 [90/2297856] via 172.16.1.2, 00:55:06, Serial2/1
C        172.16.64.0/24 is directly connected, Loopback0
L        172.16.64.1/32 is directly connected, Loopback0
B     192.168.100.0/24 [200/0] via 172.16.32.1, 00:00:43
```

```
SanJose2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 192.168.1.1, 00:00:31
      172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
S        172.16.0.0/16 is directly connected, Null0
C        172.16.1.0/24 is directly connected, Serial2/1
L        172.16.1.2/32 is directly connected, Serial2/1
C        172.16.32.0/24 is directly connected, Loopback0
L        172.16.32.1/32 is directly connected, Loopback0
D        172.16.64.0/24 [90/2297856] via 172.16.1.1, 00:54:54, Serial2/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial2/0
L        192.168.1.2/32 is directly connected, Serial2/0
B     192.168.100.0/24 [20/0] via 192.168.1.1, 00:00:31
SanJose2#
```

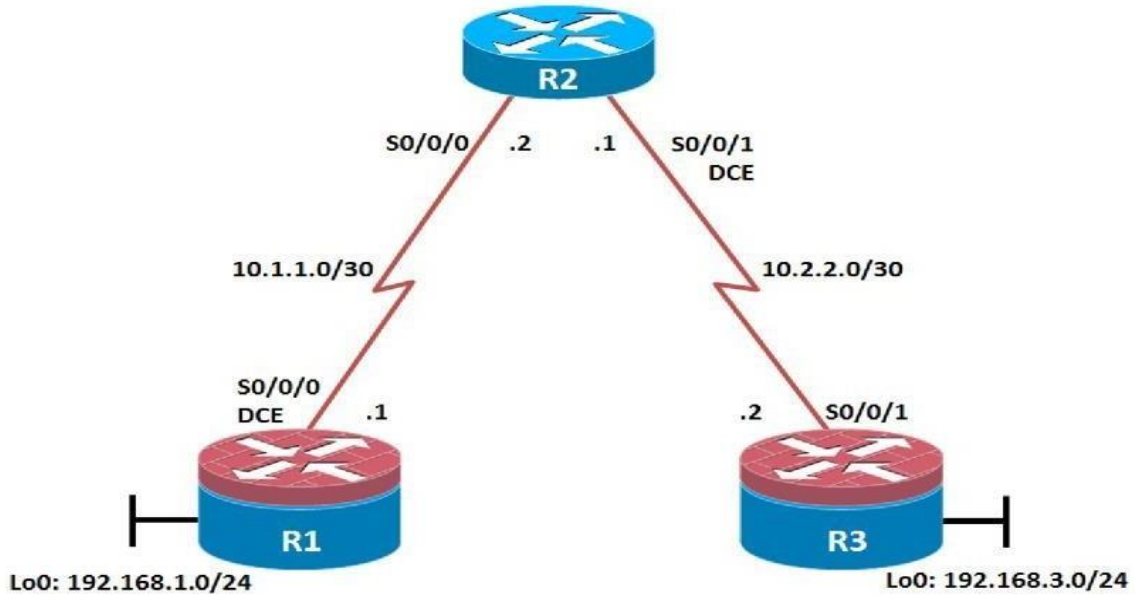
f. Verify the new path using the traceroute command to 10.0.0.1 from SanJose1. Notice the default route is now through SanJose2.

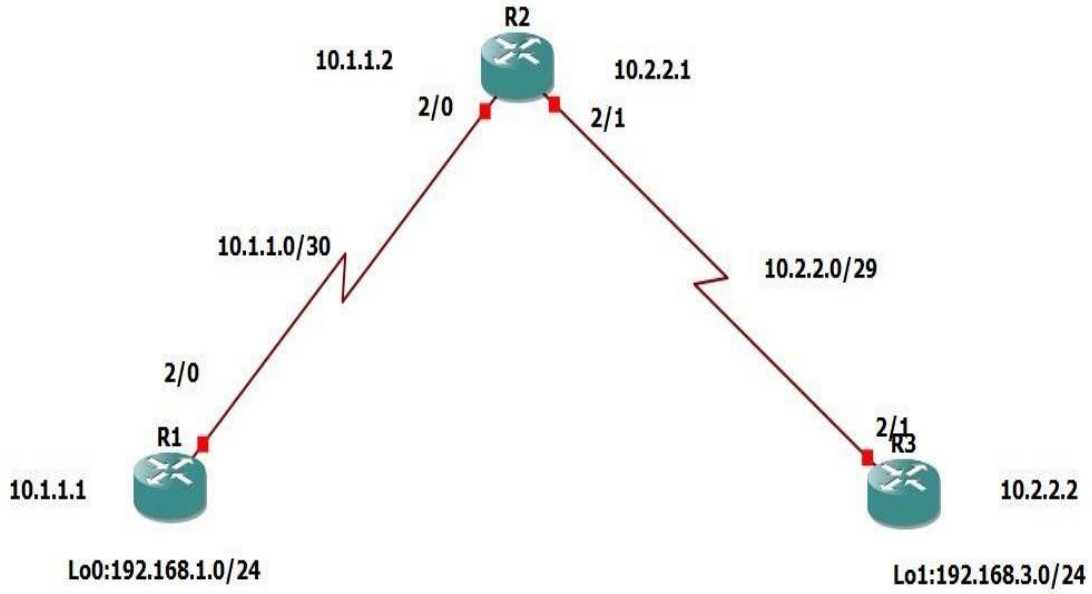
```
SanJose1#trace 10.0.0.1
Type escape sequence to abort.
Tracing the route to 10.0.0.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.2 40 msec 48 msec 44 msec
  2 192.168.1.1 [AS 200] 80 msec 60 msec 80 msec
SanJose1#
```

Practical 4

Secure the Management Plane

Topology





Objectives

Secure management access.

Configure enhanced username password security.

Enable AAA RADIUS authentication.

Enable secure remote management.

Background

The management plane of any infrastructure device should be protected as much as possible. Controlling access to routers and enabling reporting on routers are critical to network security and should be part of a comprehensive security policy. **Required Resources**

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

Step 1: Configure loopbacks and assign addresses.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1
R1(config)#interface Loopback 0
R1(config-if)#d
*Apr 18 19:29:06.099: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#description R1 LAN
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface serial 2/0
R1(config-if)#description R1-->R2
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clockrate 128000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Apr 18 19:31:12.431: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
R1(config)#
*Apr 18 19:31:13.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R1(config)#
*Apr 18 19:31:39.759: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
R1(config)#
*Apr 18 19:33:19.759: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname R2
R2(config)#interface serial 2/0
R2(config-if)#description R2-->R1
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Apr 18 19:33:13.615: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
R2(config)#
*Apr 18 19:33:14.623: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R2(config)#interface serial 2/1
R2(config-if)#description R2-->R3
R2(config-if)#ip address 10.2.2.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Apr 18 19:34:19.135: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
R2(config)#
*Apr 18 19:34:20.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
R2(config)#
*Apr 18 19:34:49.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to down
R2(config)#
*Apr 18 19:36:49.851: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
```

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#hostname R3
R3(config)#interface Loopback 0
R3(config-if)#desc
*Apr 18 19:34:56.279: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R3(config-if)#description R3 LAN
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface serial 2/1
R3(config-if)#description R3-->R2
R3(config-if)#ip address 10.2.2.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
*Apr 18 19:36:31.943: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
R3(config-if)#exit
*Apr 18 19:36:32.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
R3(config-if)#exit
```

Step 2: Configure static routes.

a.On R1, configure a default static route to ISP.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
R1(config)#end
```

b. On R3, configure a default static route to ISP

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

c. On R2, configure two static routes.

```
*Apr 18 19:36:49.851: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
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
R2(config)#
```

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

```
*Apr 18 19:41:20.907: %SYS-5-CONFIG_I: Configured from console by console
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 = 1/2/8 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 = 20/23/24 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 = 8/12/20 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/20 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/45/52 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/44/44 ms
```

Step 3: Secure management access.

a.On R1, use the security passwords command to set a minimum password length of 10 characters and configure the enable secret encrypted password on both routers.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#security passwords min-length 10
R1(config)#enable secret class12345
```

b. Configure a console password and enable login for routers.

```
R1(config)#line console 0
R1(config-line)#password cisconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
```

c. 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
```

d. 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
R1#
*Apr 18 19:50:59.399: %SYS-5-CONFIG_I: Configured from console by console
```

e. Enter privileged EXEC mode and issue the show run command.

```
R1#show run
Building configuration...

Current configuration : 2269 bytes
!
! Last configuration change at 19:50:59 UTC Tue Apr 18 2023
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
enable secret 5 $1$5uTL$KHNkBKuUeh19q.n8GtQ1w.
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
```

```
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/5
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/6
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/7
 no ip address
 shutdown
 serial restart-delay 0
!
interface Ethernet4/0
 no ip address
 shutdown
 duplex full
!
interface Ethernet4/1
 no ip address
 shutdown
 duplex full
!
interface Ethernet4/2
 no ip address
 shutdown
 duplex full
!
interface Ethernet4/3
 no ip address
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
```

```
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 privilege level 15
 password cisconpass
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 no exec
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 password ciscovtypass
 login
!
!
end
```

f. Use the service password-encryption command to encrypt the line console and vty passwords and Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner using the banner motd command.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# service password-encryption
R1(config)#banner motd $Unauthorized access strictly prohibited!$
R1(config)#exit
R1#
*Apr 18 20:11:58.351: %SYS-5-CONFIG_I: Configured from console by console
```

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

```
R3(config)#security passwords min-length 10
R3(config)#enable secret class12345
R3(config)#line console 0
R3(config-line)#password cisconpass
R3(config-line)#exec-timeout 5 0
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password ciscovtypass
R3(config-line)#exec-timeout 5 0
R3(config-line)#login
R3(config-line)#exit
R3(config)#line aux 0
R3(config-line)#no exec
R3(config-line)#end
R3#
*Apr 18 20:17:05.587: %SYS-5-CONFIG_I: Configured from console by console
R3#show run
Building configuration...

Current configuration : 2250 bytes
!
! Last configuration change at 20:17:05 UTC Tue Apr 18 2023
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
enable secret 5 $1$l40e$Qbt2dx6gpCK5gawkVEUNg/
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
!
!
```

```
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 description R3 LAN
 ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet1/0
 no ip address
 shutdown
 negotiation auto
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
```

```
interface Ethernet4/2
 no ip address
 shutdown
 duplex full
!
interface Ethernet4/3
 no ip address
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.2.2.1
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 privilege level 15
 password cisconpass
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 no exec
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 password ciscovtypass
 login
!
!
end
```

```
R3(config)#service password-encryption
R3(config)#show run
           ^
% Invalid input detected at '^' marker.

R3(config)#end
R3#conf t
*Apr 18 20:18:54.867: %SYS-5-CONFIG_I: Configured from console by console
R3#show run
Building configuration...

Current configuration : 2308 bytes
!
! Last configuration change at 20:18:54 UTC Tue Apr 18 2023
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
enable secret 5 $1$l40e$Qbt2dx6gpCK5gawkVEUNg/
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!
!
no ip domain lookup
no ipv6 cef
!
!
multilink bundle-name authenticated
```

```
 no ip address
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.2.2.1
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 privilege level 15
 password 7 02050D48080901314D5D1A
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 no exec
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 password 7 14141B180F0B3C3F3D38322631
 login
!
!
end
```

Step 4: Configure enhanced username password security.

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

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username JR-ADMIN secret class12345
R1(config)#username ADMIN secret class54321
```

b. Set the console line to use the locally defined login accounts and Set the vty lines to use the locally defined login accounts.

```
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#end
R1#
*Apr 18 20:25:47.851: %SYS-5-CONFIG_I: Configured from console by console
```

c. Repeat the steps 4a & 4b on R3.

```
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username JR-ADMIN secret class12345
R3(config)#username ADMIN secret class54321
R3(config)#line console 0
R3(config-line)#login local
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#end
R3#
*Apr 18 20:28:20.575: %SYS-5-CONFIG_I: Configured from console by console
```

d. 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


User Access Verification

Username: ADMIN
Password:
% Login invalid

Username: ADMIN
Password:
R3>exit

[Connection to 10.2.2.2 closed by foreign host]
```

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

a. Always have local database accounts created before enabling AAA. Since we created two local database accounts in the previous step, then we can proceed and enable AAA on R1 and Configure the specifics for the first RADIUS server located at 192.168.1.101.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model
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
```

b. Configure the specifics for the second RADIUS server located at 192.168.1.102 and Assign both RADIUS servers to a server group.

```
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
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
```

c.Enable the default AAA authentication login to attempt to validate against the server group and Enable the default AAA authentication Telnet login to attempt to validate against the server group.

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

d. 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
R1(config)#exit
R1#
*Apr 18 20:53:43.891: %SYS-5-CONFIG_I: Configured from console by console
```

e.Repeat steps 5a to 5d on R3.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#aaa new-model
R3(config)#radius server RADIUS-1
R3(config-radius-server)#address ipv4 192.168.1.101
R3(config-radius-server)#key RADIUS-1-pa55w0rd
R3(config-radius-server)#exit
R3(config)#radius server RADIUS-1
R3(config-radius-server)#address ipv4 192.168.1.102
R3(config-radius-server)#key RADIUS-2-pa55w0rd
R3(config-radius-server)#exit
R3(config)#radius server RADIUS-2
R3(config-radius-server)#address ipv4 192.168.1.102
%Server already exists with same address port combination.
R3(config-radius-server)#exit
Warning: Address not yet configured.
R3(config)#radius server RADIUS-1
R3(config-radius-server)#address ipv4 192.168.1.101
R3(config-radius-server)#key RADIUS-1-pa55w0rd
R3(config-radius-server)#exit
R3(config)#radius server RADIUS-2
R3(config-radius-server)#address ipv4 192.168.1.102
R3(config-radius-server)#key RADIUS-2-pa55w0rd
R3(config-radius-server)#exit
R3(config)#aaa group server radius RADIUS-GROUP
R3(config-sg-radius)#server name RADIUS-1
R3(config-sg-radius)#server name RADIUS-2
R3(config-sg-radius)#EXIT
R3(config)#aaa authentication login default group RADIUS-GROUP local
R3(config)#$ication login TELNET-LOGIN group RADIUS-GROUP local-case
R3(config)#line vty 0 4
R3(config-line)#login authentication TELNET-LOGIN
R3(config-line)#exit
```

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

```
R1#
*Apr 18 20:53:43.891: %SYS-5-CONFIG_I: Configured from console by console
R1#telnet 10.2.2.2
Trying 10.2.2.2 ... Open

User Access Verification

Username: admin
Password:

% Authentication failed

Username:
Username:

[Connection to 10.2.2.2 closed by foreign host]
R1#telnet 10.2.2.2
Trying 10.2.2.2 ... Open

User Access Verification

Username: ADMIN
Password:

R3>
R3>
R3>
R3>
R3>
R3>
R3>exit
```

Step 6: Enabling secure remote management using SSH.

a. configure the domain name and The router uses the RSA key pair for authentication and encryption of transmitted SSH data.

```
[Connection to 10.2.2.2 closed by foreign host]
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name ccnasecurity.com
R1(config)#crypto key zeroize rsa
% No Signature Keys found in configuration.

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

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Apr 18 20:57:55.455: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

b.Configure SSH version 2 on R1 and Configure the vty lines to use only SSH connections.

```
R1(config)#
*Apr 18 20:57:55.455: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#ip ssh version 2
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#end
R1#
*Apr 18 20:58:58.531: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

c. 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 AAAAB3NzaC1yc2EAAAADAQABAAAAgQC1BHA1sXhOfyjxFJ1/lHW1XPif5faoXYaE3b7Gow/z
4xyB2Vp+DC1jPzU04CDkNbg5XGhMVTIbnHiL6Eig5Sq1RWeyA0HEueSJg24wFaPqwm4dTOe5xbxGDCTh
iRexe9hS+1EHvcGo1gNC11AMfq6d4M0/16MxXJYEzaJ1yM7ogQ==
```

d.Repeat steps 6a to 6c on R3.

```
R3(config)#ip domain-name ccnasecurity.com
R3(config)#crypto key zeroize rsa
% No Signature Keys found in configuration.

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

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R3(config)#
*Apr 18 21:04:20.251: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#ip ssh version 2
R3(config)#line vty 0 4
R3(config-line)#transport input ssh
R3(config-line)#end
R3#
*Apr 18 21:04:49.155: %SYS-5-CONFIG_I: Configured from console by console
R3#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 AAAAB3NzaC1yc2EAAAADAQABAAAAgQDouIbAepILqT/m5wmeToQEBN3OUoOTtiSd7CCMK1s9
CFW41UIG+X+bnMvetQ4OU01CQrnBfpT8WjB7ExWvtcRpBVLneCcU3M81pWIYyD3rVtyq2urGPXUARYV1
KCRZ4scKO7svl91yspgFhY/p4tBKjE2AT0MY9lmeGoImtPYS5w==
R3#
*Apr 18 21:06:01.235: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.101:1645,1646 is not responding.
*Apr 18 21:06:01.235: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.101:1645,1646 is being marked alive.
R3#
*Apr 18 21:06:21.331: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.102:1645,1646 is not responding.
*Apr 18 21:06:21.331: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.102:1645,1646 is being marked alive.
R3#
```

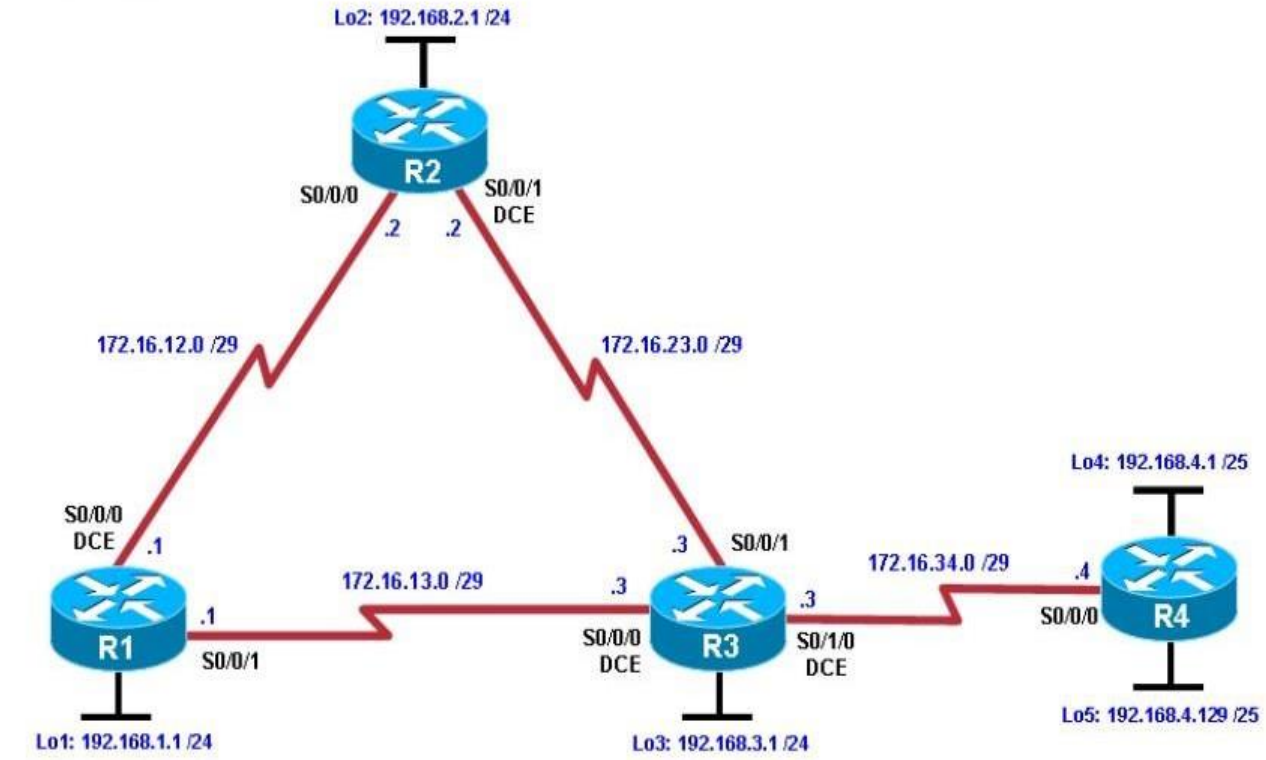
e. Although a user can SSH from a host using the SSH option of TeraTerm of PuTTY, a router can also SSH to another SSH enabled device. SSH to R3 from R1.

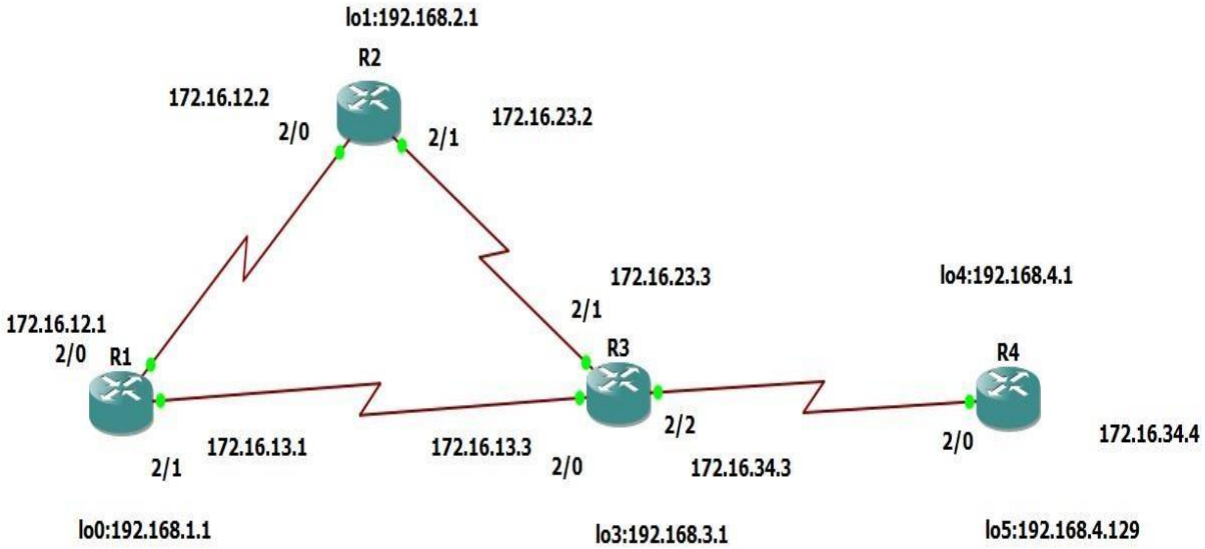
```
R1#ssh -l ADMIN 10.2.2.2
               ^
% Invalid input detected at '^' marker.

R1#ssh -l ADMIN 10.2.2.2
               ^
% Invalid input detected at '^' marker.

R1#ssh -l ADMIN 10.2.2.2
Password:
R3>
R3>
R3>en
Password:
% Access denied

R3>enable
Password:
% Access denied

R3>exit

[Connection to 10.2.2.2 closed by foreign host]
R1#
```

Practical 5

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.

Background

You want to experiment with policy-based routing (PBR) to see how it is implemented and to study how it could be of value to your organization. To this end, you have interconnected and configured a test network with four routers. All routers are exchanging routing information using EIGRP.

Required Resources

- 4 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Services or comparable)
- Serial and console cables

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 router hostname and interface addresses

a. 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.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1
R1(config)#!
R1(config)#interface Lo1
R1(config-if)#
*Apr 14 00:53:36.891: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R1(config-if)#description R1 LAN
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#!
R1(config-if)#interface serial 2/0
R1(config-if)#description R1 --> R2
R1(config-if)#ip address 172.16.12.1 255.255.255.248
R1(config-if)#clock rate 128000
R1(config-if)#bandwidth 128
R1(config-if)#no shutdown
R1(config-if)#!
*Apr 14 00:55:29.059: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
R1(config-if)#!
R1(config-if)#
*Apr 14 00:55:30.067: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R1(config-if)#interface serial 2/1
R1(config-if)#description R1 --> R3
R1(config-if)#ip address 1
*Apr 14 00:55:54.515: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to down
R1(config-if)#ip address 172.16.13.1 255.255.255.248
R1(config-if)#bandwidth 64
R1(config-if)#no shutdown
R1(config-if)#!
R1(config-if)#en
*Apr 14 00:56:23.535: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
R1(config-if)#end
*Apr 14 00:56:24.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
R1(config-if)#end
R1#
*Apr 14 00:56:27.471: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname R2
R2(config)#!
R2(config)#interface Lo2
R2(config-if)#
*Apr 14 00:57:10.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state to up
R2(config-if)#description R2 LAN
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#!
R2(config-if)#interface serial 2/0
R2(config-if)#description R2 --> R1
R2(config-if)#ip address 172.16.12.2 255.255.255.248
R2(config-if)#bandwidth 128
R2(config-if)#no shutdown
R2(config-if)#
*Apr 14 01:01:03.391: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
R2(config-if)#
*Apr 14 01:01:04.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R2(config-if)#interface serial 2/1
R2(config-if)#description R2 --> R3
R2(config-if)#ip address 172.16.23.2 255.255.255.248
R2(config-if)#clock rate 128000
R2(config-if)#bandwidth 128
R2(config-if)#no shutdown
R2(config-if)#!
R2(config-if)#
*Apr 14 01:02:48.431: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
R2(config-if)#en
*Apr 14 01:02:49.435: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to upd
R2(config-if)#end
R2#
*Apr 14 01:02:53.595: %SYS-5-CONFIG_I: Configured from console by console
R2#
*Apr 14 01:03:14.467: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to down
R2#
*Apr 14 01:06:54.463: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
```

```
R3(config)#!
R3(config)#interface Lo3
R3(config-if)#
*Apr 14 01:03:45.631: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback3, changed state to up
R3(config-if)#description R3 LAN
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#!
R3(config-if)#interface serial 2/0
R3(config-if)#description R3 --> R1
R3(config-if)#ip address 172.16.13.3 255.255.255.248
R3(config-if)#clock rate 64000
R3(config-if)#bandwidth 64
R3(config-if)#no shutdown
R3(config-if)#!
R3(config-if)#in
*Apr 14 01:05:32.883: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
R3(config-if)#ine
*Apr 14 01:05:33.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R3(config-if)#interface serial 2/1
R3(config-if)#description R3 --> R2
R3(config-if)#ip address 172.16.23.3 255.255.255.248
R3(config-if)#bandwidth 128
R3(config-if)#no shutdown
R3(config-if)#!
R3(config-if)#
*Apr 14 01:06:53.383: %LINK-3-UPDOWN: Interface Serial2/1, changed state to up
R3(config-if)#int
*Apr 14 01:06:54.391: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1, changed state to up
R3(config-if)#interface serial 2/2
R3(config-if)#description R3 --> R4
R3(config-if)#ip address 172.16.34.3 255.255.255.248
R3(config-if)#clock rate 64000
R3(config-if)#bandwidth 64
R3(config-if)#no shutdown
R3(config-if)#
*Apr 14 01:07:46.403: %LINK-3-UPDOWN: Interface Serial2/2, changed state to up
R3(config-if)#
```

```
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#hostname R4
R4(config)#!
R4(config)#interface Lo4
R4(config-if)#
*Apr 14 01:08:26.087: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
R4(config-if)#description R4 LAN A
R4(config-if)#ip address 192.168.4.1 255.255.255.128
R4(config-if)#!
R4(config-if)#interface Lo5
R4(config-if)#
*Apr 14 01:09:06.963: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
R4(config-if)#description R4 LAN B
R4(config-if)#ip address 192.168.4.129 255.255.255.128
R4(config-if)#!
R4(config-if)#interface serial 2/0
R4(config-if)#description R4 --> R3
R4(config-if)#ip address 172.16.34.4 255.255.255.248
R4(config-if)#bandwidth 64
R4(config-if)#no shutdown
R4(config-if)#!
R4(config-if)#e
*Apr 14 01:10:40.943: %LINK-3-UPDOWN: Interface Serial2/0, changed state to up
R4(config-if)#end
*Apr 14 01:10:41.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
R4(config-if)#end
R4#
*Apr 14 01:10:44.055: %SYS-5-CONFIG_I: Configured from console by console
```

b. Verify the configuration with the show ip interface brief, show protocols, and show interfaces description commands.

```
R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
GigabitEthernet1/0     unassigned      YES unset  administratively down down
Serial2/0              172.16.13.3     YES manual up                    up
Serial2/1              172.16.23.3     YES manual up                    up
Serial2/2              172.16.34.3     YES manual up                    up
Serial2/3              unassigned      YES unset  administratively down down
Serial3/0              unassigned      YES unset  administratively down down
Serial3/1              unassigned      YES unset  administratively down down
Serial3/2              unassigned      YES unset  administratively down down
Serial3/3              unassigned      YES unset  administratively down down
Serial3/4              unassigned      YES unset  administratively down down
Serial3/5              unassigned      YES unset  administratively down down
Serial3/6              unassigned      YES unset  administratively down down
Serial3/7              unassigned      YES unset  administratively down down
Ethernet4/0            unassigned      YES unset  administratively down down
Ethernet4/1            unassigned      YES unset  administratively down down
Ethernet4/2            unassigned      YES unset  administratively down down
Ethernet4/3            unassigned      YES unset  administratively down down
Loopback3              192.168.3.1     YES manual up                    up
R3#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is administratively down, line protocol is down
GigabitEthernet1/0 is administratively down, line protocol is down
Serial2/0 is up, line protocol is up
  Internet address is 172.16.13.3/29
Serial2/1 is up, line protocol is up
  Internet address is 172.16.23.3/29
Serial2/2 is up, line protocol is up
  Internet address is 172.16.34.3/29
Serial2/3 is administratively down, line protocol is down
Serial3/0 is administratively down, line protocol is down
Serial3/1 is administratively down, line protocol is down
Serial3/2 is administratively down, line protocol is down
Serial3/3 is administratively down, line protocol is down
```

```
Serial3/3 is administratively down, line protocol is down
Serial3/4 is administratively down, line protocol is down
Serial3/5 is administratively down, line protocol is down
Serial3/6 is administratively down, line protocol is down
Serial3/7 is administratively down, line protocol is down
Ethernet4/0 is administratively down, line protocol is down
Ethernet4/1 is administratively down, line protocol is down
Ethernet4/2 is administratively down, line protocol is down
Ethernet4/3 is administratively down, line protocol is down
Loopback3 is up, line protocol is up
  Internet address is 192.168.3.1/24
R3#show interfaces description
Interface                      Status         Protocol Description
Fa0/0                          admin down     down
Gi1/0                          admin down     down
Se2/0                          up             up       R3 --> R1
Se2/1                          up             up       R3 --> R2
Se2/2                          up             up       R3 --> R4
Se2/3                          admin down     down
Se3/0                          admin down     down
Se3/1                          admin down     down
Se3/2                          admin down     down
Se3/3                          admin down     down
Se3/4                          admin down     down
Se3/5                          admin down     down
Se3/6                          admin down     down
Se3/7                          admin down     down
Et4/0                          admin down     down
Et4/1                          admin down     down
Et4/2                          admin down     down
Et4/3                          admin down     down
Lo3                            up             up       R3 LAN
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

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.

```
R1(config)#router eigrp 1
R1(config-router)#network 192.168.1.0
R1(config-router)#network 172.16.12.0 0.0.0.7
R1(config-router)#network 172.16.13.0 0.0.0.7
R1(config-router)#no auto-summary
R1(config-router)#
*Apr 14 01:13:46.699: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.12.2 (Serial2/0) is up: new adjacency
R1(config-router)#
*Apr 14 01:15:18.647: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.13.3 (Serial2/1) is up: new adjacency
R1(config-router)#end
R1#
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router eigrp 1
R2(config-router)#network 192.168.2.0
R2(config-router)#network 172.16.12.0 0.0.0.7
R2(config-router)#
*Apr 14 01:13:46.911: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.12.1 (Serial2/0) is up: new adjacency
R2(config-router)#network 172.16.23.0 0.0.0.7
R2(config-router)#no auto-summary
R2(config-router)#
*Apr 14 01:15:32.523: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.23.3 (Serial2/1) is up: new adjacency
R2(config-router)#end
```

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router eigrp 1
R3(config-router)#network 192.168.3.0
R3(config-router)#network 172.16.13.0 0.0.0.7
```

```
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#router eigrp 1
R4(config-router)#network 192.168.4.0
R4(config-router)#network 172.16.34.0 0.0.0.7
R4(config-router)#np
*Apr 14 01:16:41.611: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.34.3 (Serial2/0) is up: new adjacency
R4(config-router)#no auto-summary
R4(config-router)#end
R4#s
*Apr 14 01:18:26.991: %SYS-5-CONFIG_I: Configured from console by console
```

Step 4: Verify EIGRP connectivity

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

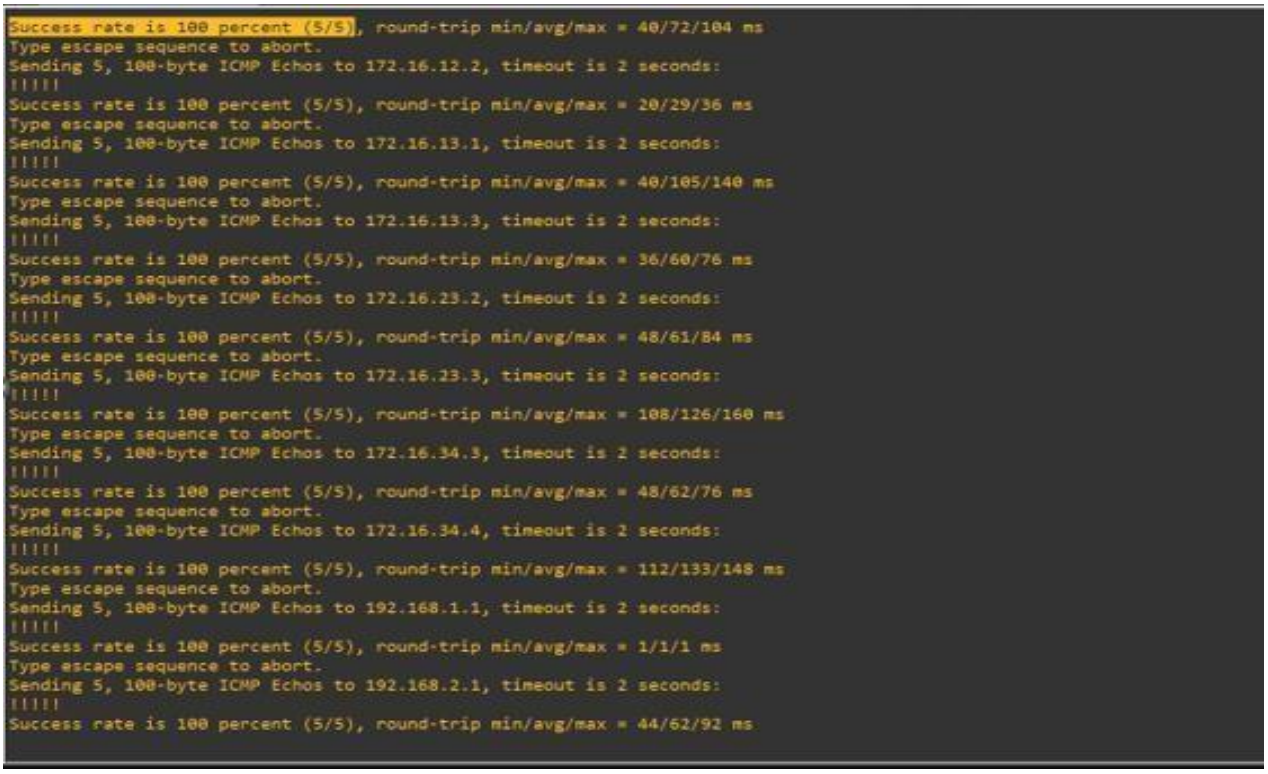
```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   172.16.13.3             Se2/1                    11 00:01:54   54  2340  0  15
0   172.16.12.2             Se2/0                    13 00:03:26   54  1170  0  12
```

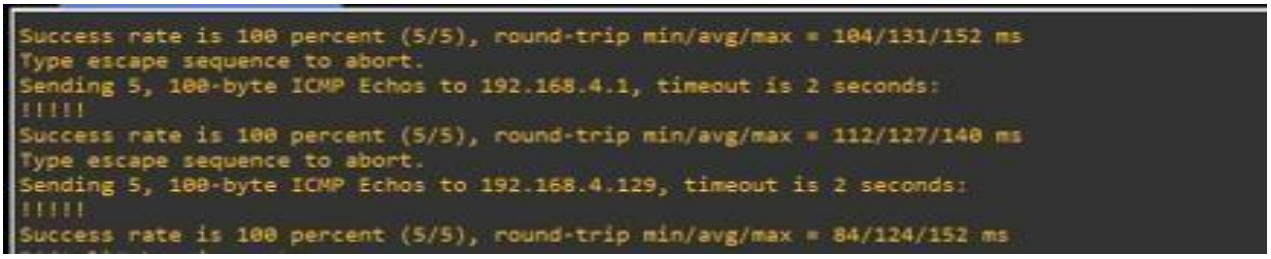
```
R2#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   172.16.23.3             Se2/1                    14 00:02:21   60  1170  0  14
0   172.16.12.1             Se2/0                    14 00:04:06   60  1170  0  13
R2#
```

```
*Apr 14 01:18:26.991: %SYS-5-CONFIG_I: Configured from console by console
R4#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   172.16.34.3             Se2/0                    14 00:01:56   87  2340  0  13
```

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

```
R1#tclsh
R1(tcl)#foreach address {
+>(tcl)#172.16.12.1
+>(tcl)#172.16.12.2
+>(tcl)#172.16.13.1
+>(tcl)#172.16.13.3
+>(tcl)#172.16.23.2
+>(tcl)#172.16.23.3
+>(tcl)#172.16.34.3
+>(tcl)#172.16.34.4
+>(tcl)#192.168.1.1
+>(tcl)#192.168.2.1
+>(tcl)#192.168.3.1
+>(tcl)#192.168.4.1
+>(tcl)#192.168.4.129
+>(tcl)#} { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.1, timeout is 2 seconds:
!!!!!
```





Step 5: Verify the current path.

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

```
R1(tcl)#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C        172.16.12.0/29 is directly connected, Serial2/0
L        172.16.12.1/32 is directly connected, Serial2/0
C        172.16.13.0/29 is directly connected, Serial2/1
L        172.16.13.1/32 is directly connected, Serial2/1
D        172.16.23.0/29 [90/21024000] via 172.16.12.2, 00:05:55, Serial2/0
D        172.16.34.0/29 [90/41024000] via 172.16.13.3, 00:05:45, Serial2/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback1
L        192.168.1.1/32 is directly connected, Loopback1
D     192.168.2.0/24 [90/20640000] via 172.16.12.2, 00:05:55, Serial2/0
D     192.168.3.0/24 [90/21152000] via 172.16.12.2, 00:05:55, Serial2/0
      192.168.4.0/25 is subnetted, 2 subnets
D        192.168.4.0 [90/41152000] via 172.16.13.3, 00:04:45, Serial2/1
D        192.168.4.128 [90/41152000] via 172.16.13.3, 00:04:45, Serial2/1
R1(tcl)#
```

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

```
R4#traceroute 192.168.1.1 source 192.168.4.129
Type escape sequence to abort.
Tracing the route to 192.168.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.34.3 24 msec 32 msec 56 msec
  2 172.16.23.2 112 msec 136 msec 120 msec
  3 172.16.12.1 100 msec 84 msec 88 msec
R4#traceroute 192.168.1.1 source 192.168.4.1
Type escape sequence to abort.
Tracing the route to 192.168.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.34.3 64 msec 100 msec 40 msec
  2 172.16.23.2 140 msec 136 msec 124 msec
  3 172.16.12.1 156 msec 168 msec 124 msec
```

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

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
D        172.16.12.0/29 [90/21024000] via 172.16.23.2, 00:07:12, Serial2/1
C        172.16.13.0/29 is directly connected, Serial2/0
L        172.16.13.3/32 is directly connected, Serial2/0
C        172.16.23.0/29 is directly connected, Serial2/1
L        172.16.23.3/32 is directly connected, Serial2/1
C        172.16.34.0/29 is directly connected, Serial2/2
L        172.16.34.3/32 is directly connected, Serial2/2
D     192.168.1.0/24 [90/21152000] via 172.16.23.2, 00:07:12, Serial2/1
D     192.168.2.0/24 [90/20640000] via 172.16.23.2, 00:07:12, Serial2/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Loopback3
L        192.168.3.1/32 is directly connected, Loopback3
      192.168.4.0/25 is subnetted, 2 subnets
D        192.168.4.0 [90/40640000] via 172.16.34.4, 00:06:02, Serial2/2
D        192.168.4.128 [90/40640000] via 172.16.34.4, 00:06:02, Serial2/2
```

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

```
R3#show interfaces serial 2/0
Serial2/0 is up, line protocol is up
  Hardware is M4T
  Description: R3 --> R1
  Internet address is 172.16.13.3/29
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:00:03, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 48 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     327 packets input, 24486 bytes, 0 no buffer
     Received 134 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     294 packets output, 22537 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

```
R3#show interfaces serial 2/1
Serial2/1 is up, line protocol is up
  Hardware is M4T
  Description: R3 --> R2
  Internet address is 172.16.23.3/29
  MTU 1500 bytes, BW 128 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     308 packets input, 22582 bytes, 0 no buffer
     Received 137 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     290 packets output, 21066 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

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

```
R3#show ip eigrp topology 192.168.1.0
EIGRP-IPv4 Topology Entry for AS(1)/ID(192.168.3.1) for 192.168.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 21152000
  Descriptor Blocks:
  172.16.23.2 (Serial2/1), from 172.16.23.2, Send flag is 0x0
      Composite metric is (21152000/20640000), route is Internal
      Vector metric:
        Minimum bandwidth is 128 Kbit
        Total delay is 45000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
        Originating router is 192.168.1.1
  172.16.13.1 (Serial2/0), from 172.16.13.1, Send flag is 0x0
      Composite metric is (40640000/128256), route is Internal
      Vector metric:
        Minimum bandwidth is 64 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
        Originating router is 192.168.1.1
R3#
```

Step 6: Configure PBR to provide path control.

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

```
R3#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
```

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.

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

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.

```
R3(config)#interface serial 2/2
R3(config-if)#ip policy route-map R3-to-R1
```

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

```
R3#
*Apr 14 01:31:14.859: %SYS-5-CONFIG_I: Configured from console by console
R3#show route-map
route-map R3-to-R1, permit, sequence 10
  Match clauses:
    ip address (access-lists): PBR-ACL
  Set clauses:
    ip next-hop 172.16.13.1
  Policy routing matches: 0 packets, 0 bytes
```

Step 7:Test the policy.

a. 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
R3#
*Apr 14 01:32:18.895: %SYS-5-CONFIG_I: Configured from console by console
```

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

```
R3#
*Apr 14 01:32:18.895: %SYS-5-CONFIG_I: Configured from console by console
R3#debug ip policy ?
  <1-199>  Access list
  dynamic  dynamic PBR
  early    Early PBR
  <cr>

R3#debug ip policy 1
Policy routing debugging is on for access list 1
R3#
```

c. 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
Type escape sequence to abort.
Tracing the route to 192.168.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.34.3 64 msec 100 msec 40 msec
  2 172.16.23.2 140 msec 136 msec 124 msec
  3 172.16.12.1 156 msec 168 msec 124 msec
```

```
R3#
*Apr 14 01:33:16.967: IP: s=192.168.4.1 (Serial2/2), d=192.168.1.1, len 28, policy rejected -- normal forwarding
*Apr 14 01:33:17.039: IP: s=192.168.4.1 (Serial2/2), d=192.168.1.1, len 28, policy rejected -- normal forwarding
*Apr 14 01:33:17.123: IP: s=192.168.4.1 (Serial2/2), d=192.168.1.1, len 28, policy rejected -- normal forwarding
*Apr 14 01:33:17.183: IP: s=192.168.4.1 (Serial2/2), d=192.168.1.1, len 28, FIB policy rejected(no match) - normal forwarding
*Apr 14 01:33:17.323: IP: s=192.168.4.1 (Serial2/2), d=192.168.1.1, len 28, FIB policy rejected(no match) - normal forwarding
*Apr 14 01:33:17.467: IP: s=192.168.4.1 (Serial2/2), d=192.168.1.1
R3#, len 28, FIB policy rejected(no match) - normal forwarding
*Apr 14 01:33:17.575: IP: s=192.168.4.1 (Serial2/2), d=192.168.1.1, len 28, FIB policy rejected(no match) - normal forwarding
*Apr 14 01:33:17.743: IP: s=192.168.4.1 (Serial2/2), d=192.168.1.1, len 28, FIB policy rejected(no match) - normal forwarding
*Apr 14 01:33:17.915: IP: s=192.168.4.1 (Serial2/2), d=192.168.1.1, len 28, FIB policy rejected(no match) - normal forwarding
R3#
```

d. 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
Type escape sequence to abort.
Tracing the route to 192.168.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.34.3 56 msec 60 msec 72 msec
  2 172.16.13.1 136 msec 88 msec 64 msec
R4#
```

```
R3#
*Apr 14 01:35:42.727: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, len 28, policy match
*Apr 14 01:35:42.731: IP: route map R3-to-R1, item 10, permit
*Apr 14 01:35:42.735: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1 (Serial2/0), len 28, policy routed
*Apr 14 01:35:42.735: IP: Serial2/2 to Serial2/0 172.16.13.1
*Apr 14 01:35:42.823: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, len 28, policy match
*Apr 14 01:35:42.827: IP: route map R3-to-R1, item 10, permit
*Apr 14 01:35:42.827: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1 (Serial2/0), len 28, policy routed
*Apr 14 01:35:42.831: IP: Serial2/2 to Serial2/0 172.16.13.1
*Apr 14 01:35:42.875: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, len 28, policy match
*Apr 14 01:35:42.879: IP: route map R3-to-R1, item 10, permit
*Apr 14 01:35:42.879: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1 (Serial2/0), len 28, policy routed
*Apr 14 01:35:42.883: IP: Serial2/2 to Serial2/0 172.16.13.1
*Apr 14 01:35:42.955: IP: s=192
R3#.168.4.129 (Serial2/2), d=192.168.1.1, len 28, FIB policy match
*Apr 14 01:35:42.955: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, len 28, PBR Counted
*Apr 14 01:35:42.959: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, g=172.16.13.1, len 28, FIB policy routed
*Apr 14 01:35:43.095: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, len 28, FIB policy match
*Apr 14 01:35:43.095: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, len 28, PBR Counted
*Apr 14 01:35:43.099: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, g=172.16.13.1, len 28, FIB policy routed
*Apr 14 01:35:43.163: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, len 28, FIB policy match
*Apr 14 01:35:43.163: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, len 28, PBR Counted
*Apr 14 01:35:43.167: IP: s=192.168.4.129 (Serial2/2), d=192.168.1.1, g=172.16.13.1, len 28, FIB policy routed
```

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

```
R3#show route-map
route-map R3-to-R1, permit, sequence 10
  Match clauses:
    ip address (access-lists): PBR-ACL
  Set clauses:
    ip next-hop 172.16.13.1
Nexthop tracking current: 0.0.0.0
172.16.13.1, fib_nh:0,oce:0,status:0

  Policy routing matches: 6 packets, 192 bytes
R3#w
```