Practical no 6

**Aim - Control Routing Updates**

**Instructions**

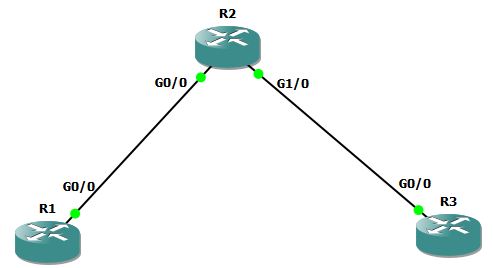
Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings and interface addressing on

routers.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.



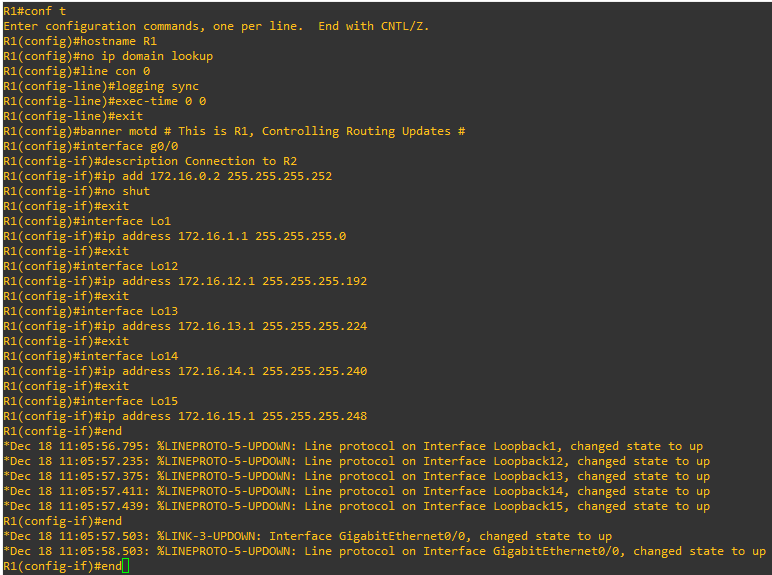
Step 2: Configure basic settings for each device.

a. Console into each device, enter global configuration mode, and apply the basic settings. The startup

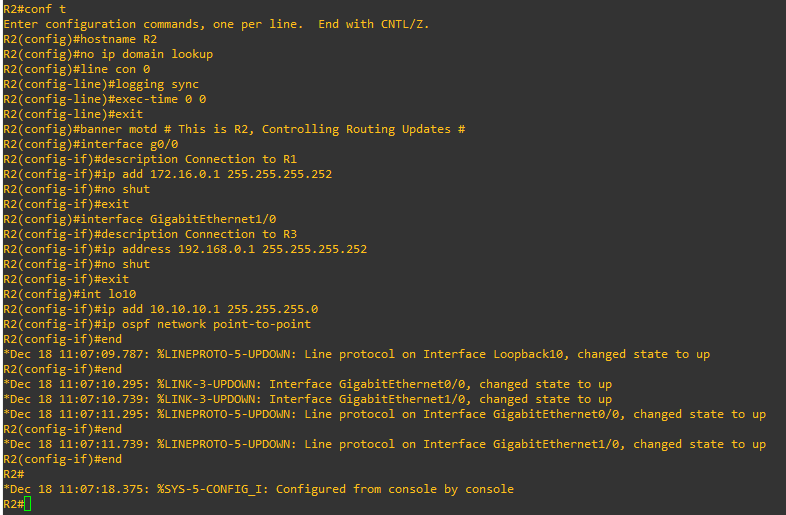
configurations for each device are provided below. Make sure to run config terminal before configuring

in each router

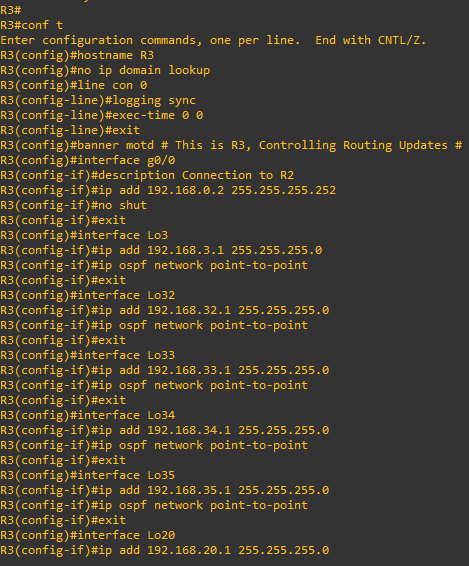
**Router R1**

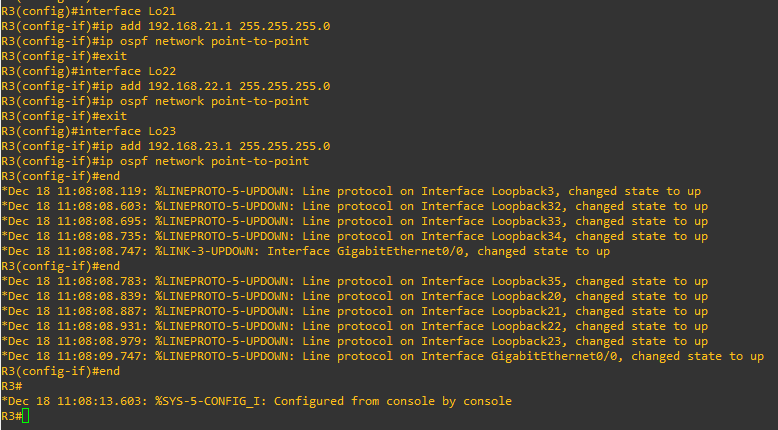


**Router R2**



**Router R3**



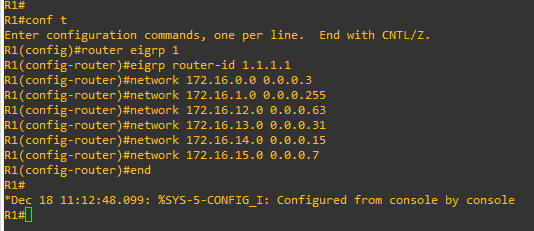


**Part 2: Configure Routing and Redistribution**

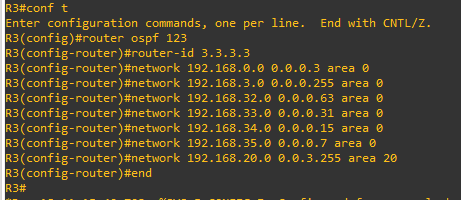
**Step 1: Configure Routing.**

a. On R1, advertise the connected networks using EIGRP in autonomous system 1. Assign R1 the router ID

of 1.1.1.1.

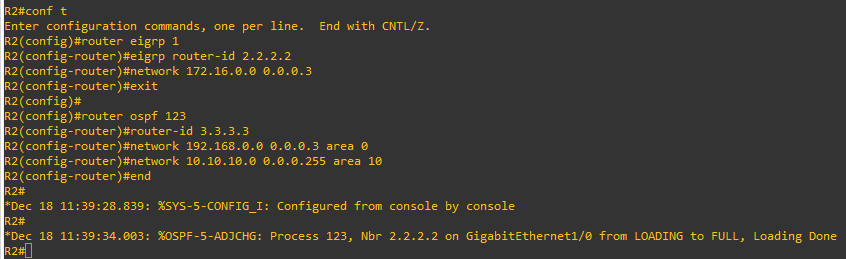


b. On R3, advertise the connected networks using OSPF process ID 123 for area 0 and area 20.



c. On R2, configure EIGRP and redistribute the OSPF networks into EIGRP AS 1. Then configure OSPF

and redistribute and summarize the EIGRP networks into OSPF.



**Step 2: Verify EIGRP and OSPF routing**

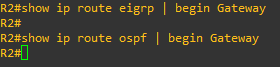
a. Verify the EIGRP routing table entries on R1. No routes are displayed because R1 is directly connected to all of the EIGRP routes.



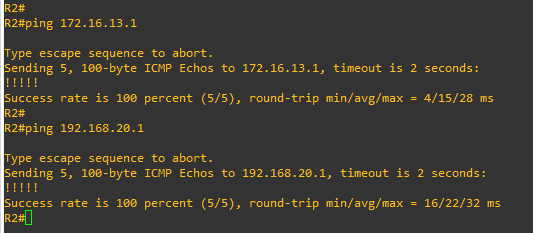
b. Verify the OSPF routing table entries on R3. R3 has an inter-area route entry for the OSPF area 10 network.



c. Verify the EIGRP and OSPF routing table entries on R2. R2 has entries for all of the EIGRP networks and the OSPF networks including the Area 20 networks

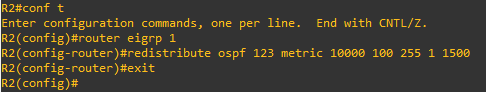


d. Verify connectivity to an EIGRP and OSPF network using the ping command as shown. R2 has connectivity to the EIGRP and OSPF networks.

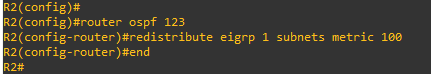


**Step 3: Configure Redistribution on R2**

a. On R2, redistribute the OSPF routes in EIGRP. Routes redistributed into EIGRP require that a metric be assigned.



b. On R2, redistribute the EIGRP routes in OSPF. Routes redistributed into OSPF are automatically assigned a metric of 20. In our example, you are assigning a higher cost metric of 100 to redistributed routes.



Step 4: Verify Redistribution

A .On R2, verify the EIGRP and OSPF routing table. Notice how the R2 routing table has not change.



B . On R1, verify the EIGRP routing table. Originally the R1 routing table displayed no entries as R1 was

directly connected to all EIGRP networks. However, R1 now knows about the external routes redistributed from the R2 OSPF routing domain. The highlighted entries identify all of the OSPF routes.



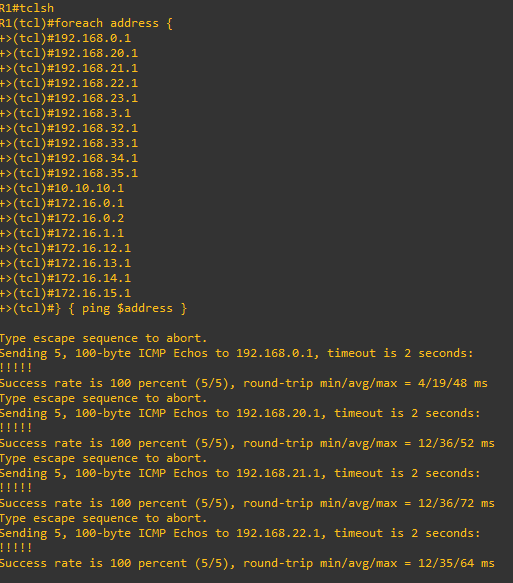
C . Verify the EIGRP routing table on R3. Previously, R3 only had the Area 10 network in its routing table. R3

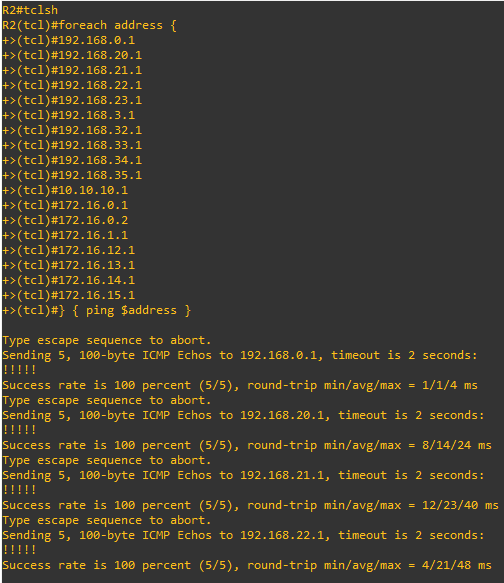
now knows about the external EIGRP routes redistributed by R2. Also notice that the redistribution command assigned a metric of 100.

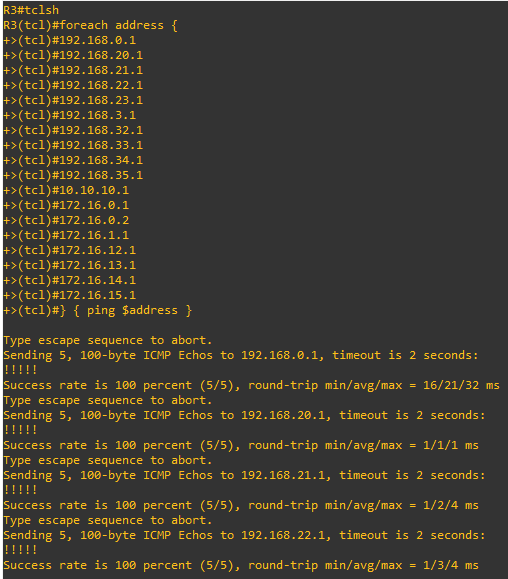


D . From all routers, verify connectivity to all configured destinations using the following TCL script. All pings

should be successful. Troubleshoot if necessary.



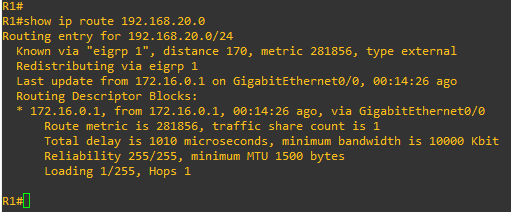




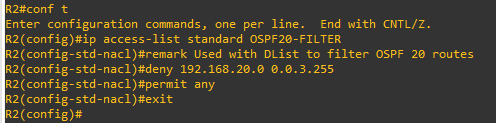
**Part 3: Filter Redistributed Routes using a Distribute List and ACL.**

Step 1: Configure an ACL and distribute list on R2

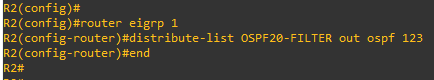
A . On R1, verify the routing table entry for the 192.168.20.0/22 route. R1 displays the entry for the 192.169.20.0 network.



B . You will filter the Area 20 networks from being advertised into the EIGRP domain. Although a distribute list could be implemented on the receiving router (i.e., R1), it is usually best to filter routes from the redistributing router. Therefore, on R2, create a standard named ACL called OSPF20-FILTER that denies the 192.168.20.0/22 route. The ACL must also permit all other routes otherwise, no OSPF routes would be redistributed into EIGRP.

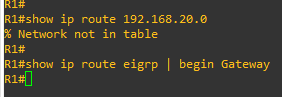


C . Next configure a distribute list under the EIGRP process to filter routes propagated to R1 using the pre- configured ACL.



Step 2: Verify the configuration

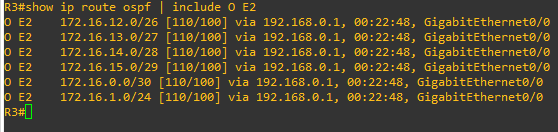
A . On R1, verify if the 192.168.20.0 route is now missing from the R1 routing table. The output confirms that the 192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/24, 192.168.23.0/24 (192.168.20.0/22) routes are no longer in the routing table of R1.



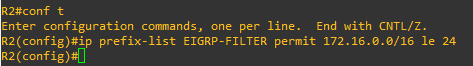
**Part 4: Filter Redistributed Routes using a Distribute List and Prefix List**

Step 1: Filter redistributed routes using a distribute list and prefix list.

A . On R3, verify the routing table entry for the routes learned externally identified with the O E2 source entry. The output displays route entries for the EIGRP networks connected to R1.



B . Configure R2 with a prefix list identifying which networks to advertise to R3. Specifically, only the networks with the first two octets being 172.16 (i.e., 172.16.0.0/16) with a subnet mask of /24 or less will be advertised.



C . Configure a distribute list under the OSPF process to filter routes propagated to R3 using the pre- configured prefix list.



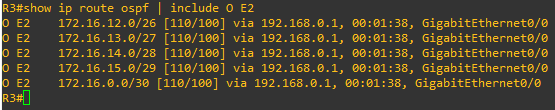
D . On R3, verify which EIGRP redistributed routes have been learned from R2. Notice how only the 172.16.1.0/24 route is listed because all other routes have subnet masks greater than /24.



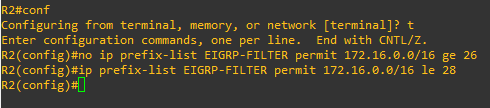
E . To observe how a prefix list can be used to filter routes, remove the previously configured prefix list and change the prefix list on R2 advertise only EIGRP networks with subnet masks of /26 or greater.



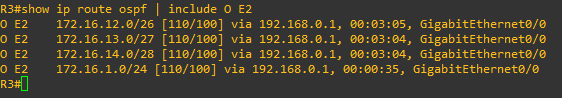
F . Verify the change on R3 as shown. Now only the 172.16.1.0/24 route is not listed as all other routes have subnet masks greater than or equal to /26.



G . Now change the prefix list on R2 to advertise only networks with subnet masks of /28 or less.



h. Verify the output on R3 as shown. Notice how the 172.16.0.0/30 and 172.16.15.0/29 are no longer advertised as their subnet masks are greater than /28.



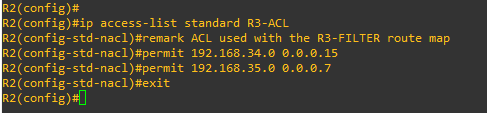
**Part 5: Filter Redistributed Routes using a Route Map.**

Step 1: Filter redistributed routes using a route map

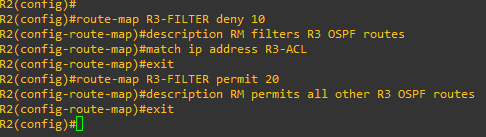
A .On R1, display the current routing table.



B . Route maps can be used to filter redistributed traffic in multiple ways. In this step, you will filter and deny the R3 Lo 34 and Lo 35 networks (i.e., 192.168.34.0/28 and 192.168.35.0/29) from being redistributed into the EIGRP routing domain. All other networks connected to R1 will be redistributed. On R2, create a standard named ACL called R3-ACL that identifies the R3 Lo 34 and Lo 35 networks (i.e., 192.168.34.0/28 and 192.168.35.0/29) as shown.



C . Configure a route map with a statement that denies traffic based on a match with the named ACL. Then add a permit statement without a match statement to provide an explicit “permit all”.



D . Apply this route map to EIGRP by reentering the redistribute command using the route-map keyword.



E . Verify that the two R3 networks are filtered out in the R1 routing table. Notice that the 192.168.34.0/28 and 192.168.35.0/29 networks are no longer in the R1 routing table.



**Step 2: Filter redistributed routes and set attributes using a route map.**

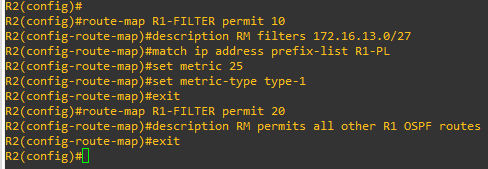
A . On R3, verify the routing table entry for the routes learned externally identified with the 0 E2 source entry. The 172.16.13.0/27 route will be configured with additional attributes.



b. Although an ACL could be used, this example will use a prefix list. Configure a prefix list identifying the route to be filtered**.**



C . Configure a route map matching the identified route in the prefix list and assign the OSPF metric cost of 25 and change the metric type to External Type 1. Then add a permit statement without a match statement acting as an explicit “permit all”.



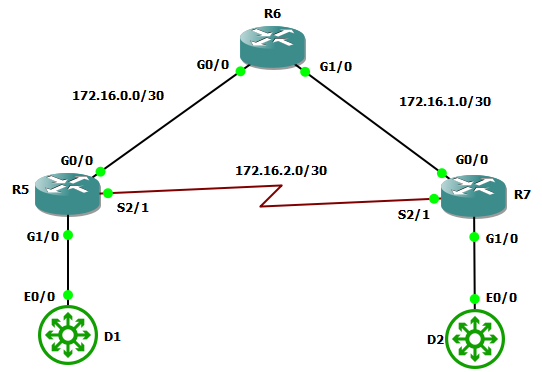
D . Apply this route map to OSPF by reentering the redistribute command using the route-map keyword.



E . Verify that the two R3 networks are filtered out in the R1 routing table. Notice that only the 172.16.13.0/27 route is an OSPF External Type 1 route (i.e., O E1) with a cost metric of 26 (i.e., the assigned metric cost of 25 plus the cost of 1 for the R2 to R3 link).



**B. Path Control Using PBR (Policy Based Routing)**



**NOTE : R1=R5 , R2=R6, R3=R7**

Part 1: Build the Network and Configure Basic Device Settings

Step 1: Cable the network as shown in the topology.

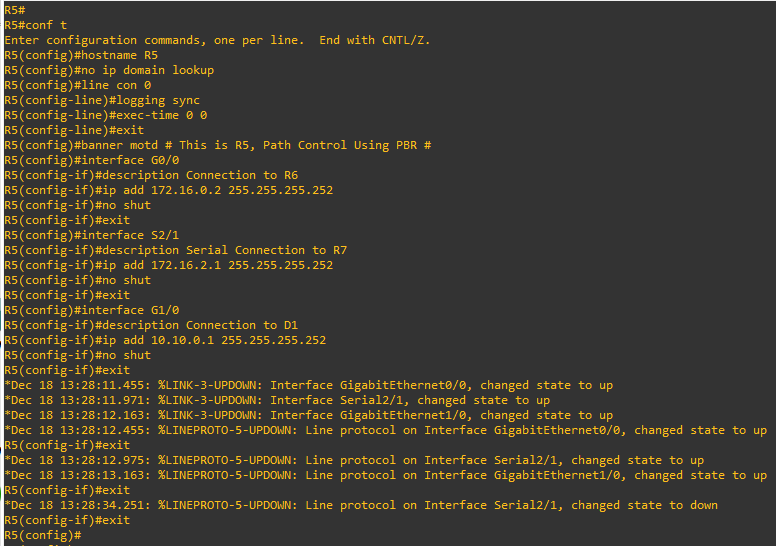
Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each device.

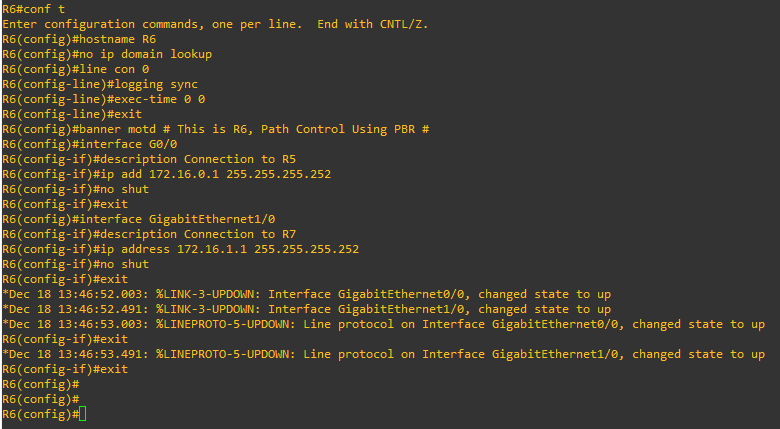
a. Console into each device, enter global configuration mode, and apply the basic settings. The startup

configurations for each device are provided below.

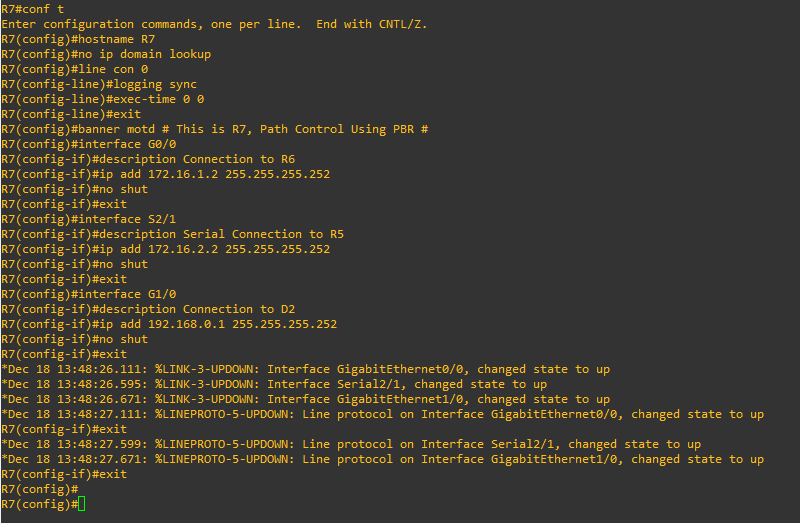
**Router R5**



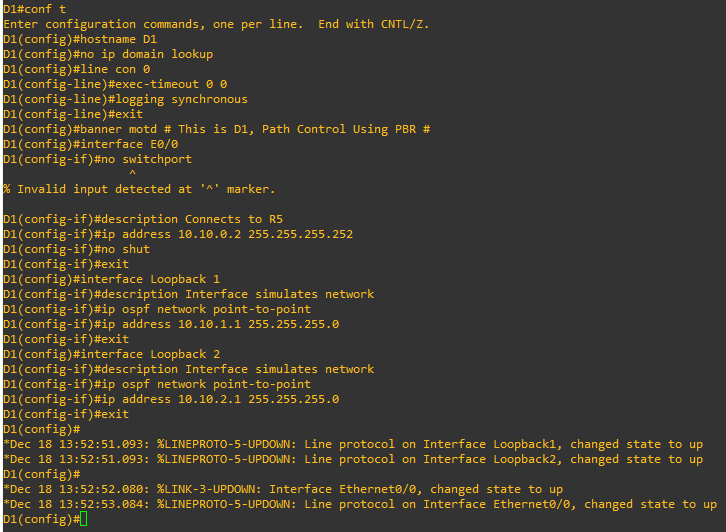
**Router R6**



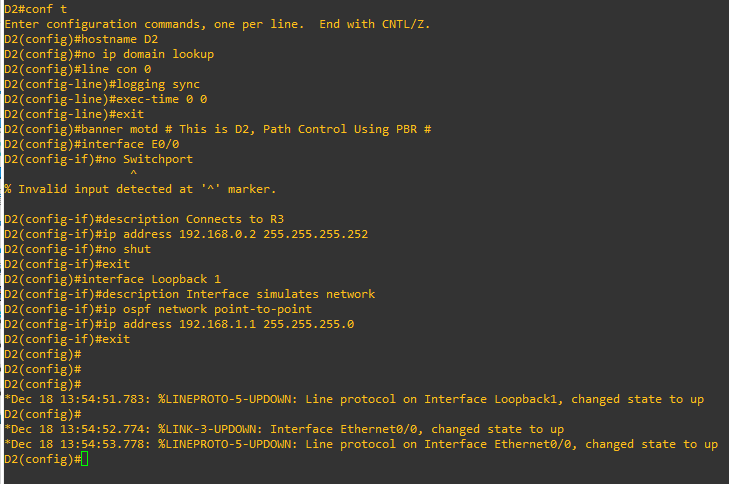
**Router R7**



**Switch D1**



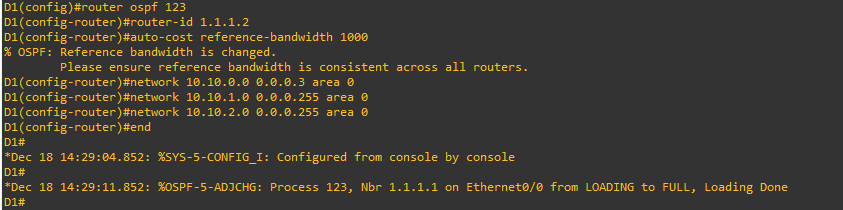
**Switch D2**



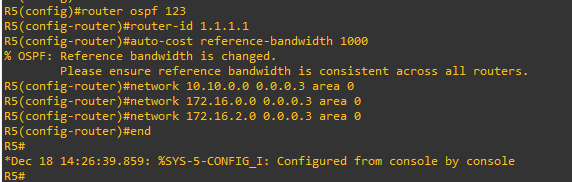
**Part 2: Configure and Verify Routing**

Step 1: Configure Routing.

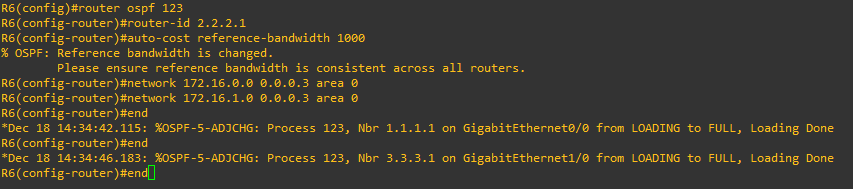
A . On D1, advertise the connected networks using OSPF process ID 123. Also assign D1 the router ID of1.1.1.2 and set the reference bandwidth to recognize Gigabit Ethernet interfaces.



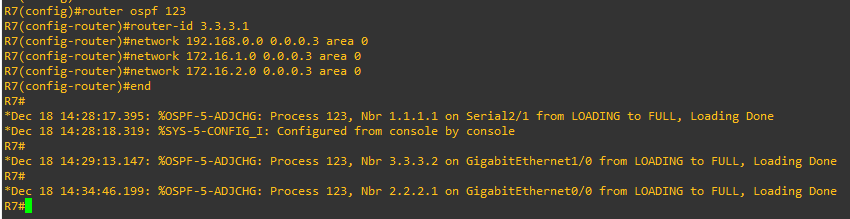
B . On R1, advertise the connected networks using OSPF process ID 123. Also assign R1 the router ID of 1.1.1.1 and set the reference bandwidth to recognize Gigabit Ethernet interfaces.



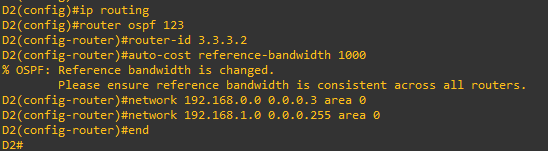
C . On R2, advertise the connected networks using OSPF process ID 123. Also assign R2 the router ID of 2.2.2.1 and set the reference bandwidth to recognize Gigabit Ethernet interfaces.



D . On R3, advertise the connected networks using OSPF process ID 123. Also assign R3 the router ID of 3.3.3.1 and set the reference bandwidth to recognize Gigabit Ethernet interfaces.



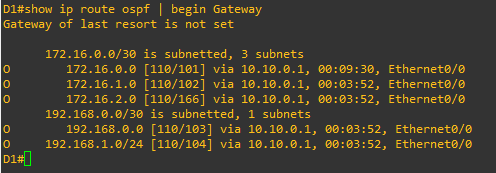
E . On D2, advertise the connected networks using OSPF process ID 123. Also assign D2 the router ID of 3.3.3.2 and set the reference bandwidth to recognize Gigabit Ethernet interfaces.

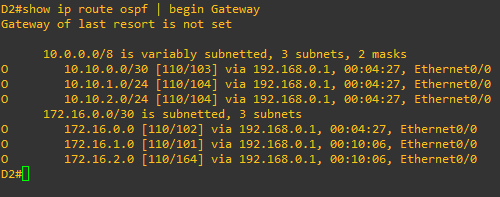




**Step 2: Verify OSPF routing**

a. Before configuring PBR, verify the current routing table on all devices. All routing tables look accurate.











Step 3: Verify end-to-end connectivity and path taken

1. From any device, verify connectivity to all configured destinations using the following TCL script. All pings should be successful. Troubleshoot if necessary.

tclsh

foreach address {

10.10.0.1

10.10.0.2

10.10.1.1

10.10.2.1

172.16.0.1

172.16.0.2

172.16.1.1

172.16.1.2

172.16.2.1

172.16.2.2

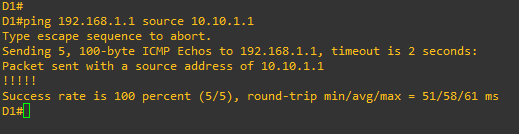
192.168.0.1

192.168.0.2

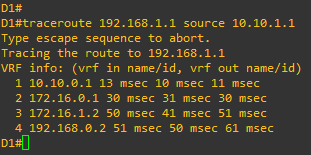
192.168.1.1

} { ping $address }

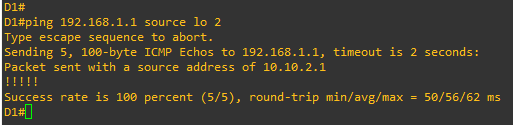
b. On D1, ping the D2 Loopback interface 192.168.1.1 address from the Lo1 interface as shown. The pingsshould be successful.



c. Next, identify the path taken to D2 Lo1 interface using the traceroute command as shown. Notice that the path taken for the packets sourced from the D1 Lo1 LAN is going through R1 --> R2 --> R3 --> D2.



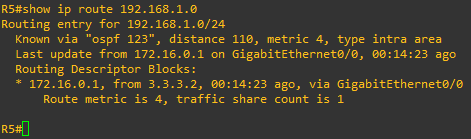
d. Now ping and traceroute the D2 Lo1 interface from the D1 Loopback 2 interface as shown. It is also taking the same path.



e . Display the OSPF routes in the routing table of R1. R1 forwards all packets destined to the 192.168.1.0/24 network out of its G0/0/0 interface to R2.



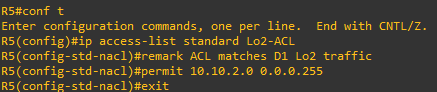
F . Display how R1 learned about the 192.168.1.0 network. R1 learned of the network from R2 (i.e., 172.16.0.1) who originally learned it from D2 (i.e., 3.3.3.2).



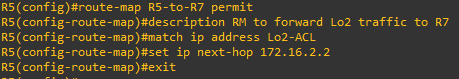
**Part 3: Configure PBR to Provide Path Co3ntrol**

Step 1: Configure PBR on R1.

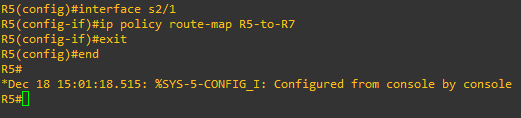
a. On R1, create a standard named ACL called Lo2-ACL to identify the D1 Loopback 2 (i.e., 10.10.2.0/24) LAN.



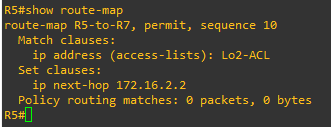
b. Create a route map called R1-to-R3 that matches Lo2-ACL and sets the next-hop interface to the R3 serial 0/1/0 interface.



c. Apply the R1-to-R3 route map to the G0/0/1 interface using the ip policy route-map command.



d. On R1, display the policy and matches using the show route-map command.

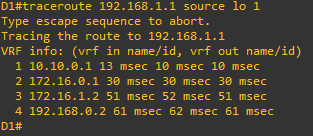


e. On R1, verify that the R1-to-R3 route map has been applied to the G0/0/1 interface.

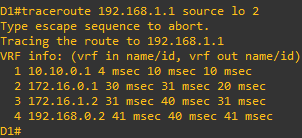


**Step 2: Test the policy.**

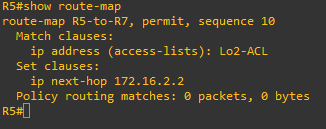
a. From D1, test the policy with the traceroute command, using D1 Lo1 interface as the source network.



b. Now test the policy with the traceroute command, using D1 Lo2 interface as the source network. Now the path taken for the packet sourced from D1 Lo 2 LAN is R1 --> R3 --> D2, as expected.

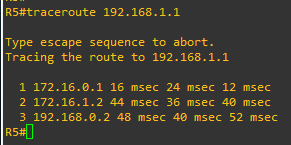


c. On R1, display the policy and matches using the show route-map command.

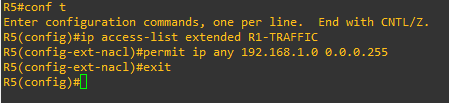


**Part 4: Configure Local PBR to Provide Path Control**

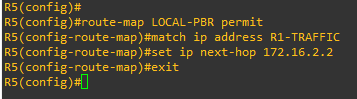
a. Verify the path that R1 currently takes without local PBR configured. R1 sends traffic to R2 then R3 and finally D2 as expected.



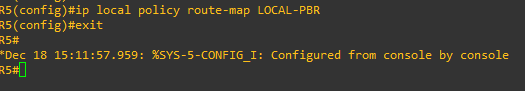
b. On R1, create a named extended ACL called R1-TRAFFIC which matches all IP generated packets from R1 and destined to the D2 192.162.1.0/24 network.



c. On R1, create a route map called LOCAL-PBR that permits traffic matching the R1-TRAFFIC ACL and redirects it to the R3 172.16.2.2 interface.

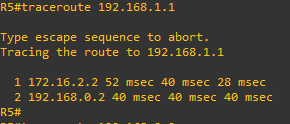


d. Create a local PBR policy that matches the LOCAL-PBR route map.

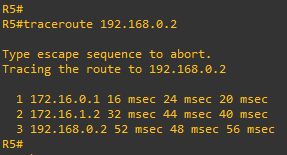


Step 2: Test Local PBR on R1.

a. Verify the path taken by R1 to reach the 192.168.1.0/24 LAN. The traffic generated by R1 and going to 192.168.1.0/24 is now policy routed directly to R3 (i.e., 172.16.2.2).



b. Verify the path taken by R1 to reach other networks. The traffic takes the normal OSPF generated path and is not policy routed.



c. Verify the route-map counters. The local PBR policy has matched packets.

