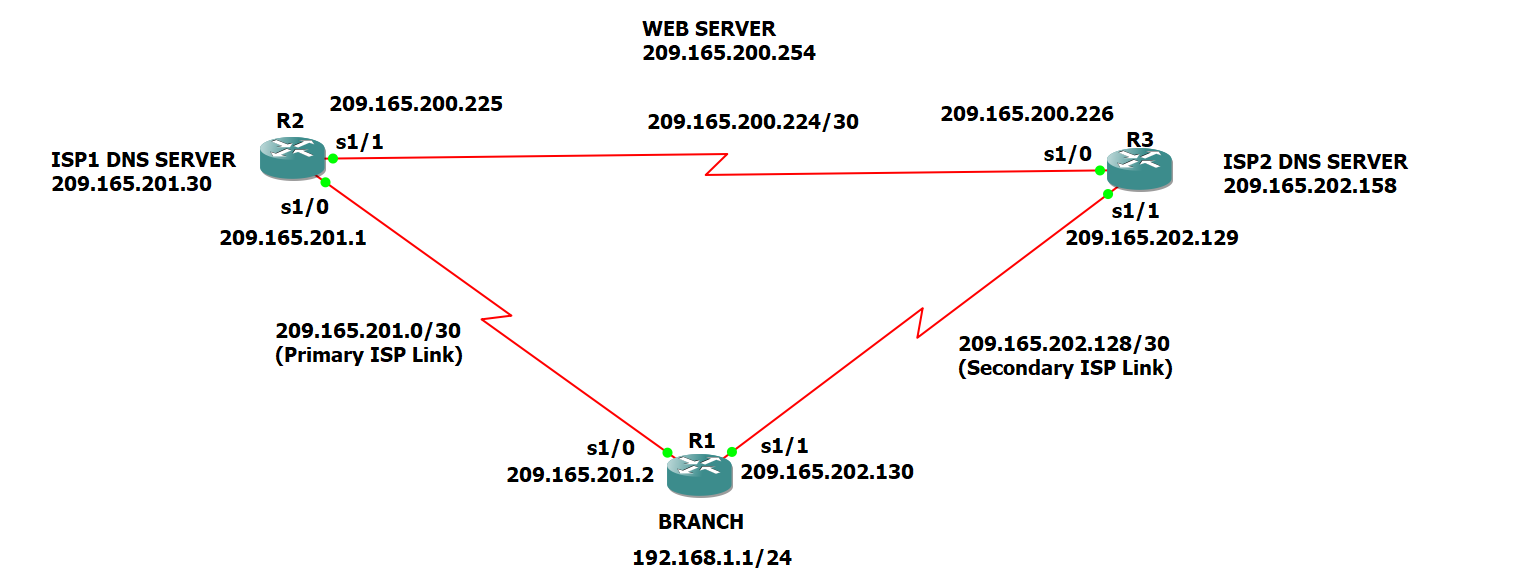
**Practical 1**

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

**Topology:-**

****

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

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

Router R1 Console

Conf t

hostname R1

interface Loopback 0

description R1 LAN

ip address 192.168.1.1 255.255.255.0

interface Serial1/0

description R1 🡪 ISP1

ip address 209.165.201.2 255.255.255.252

clock rate 128000

bandwidth 128

no shutdown

interface Serial1/1

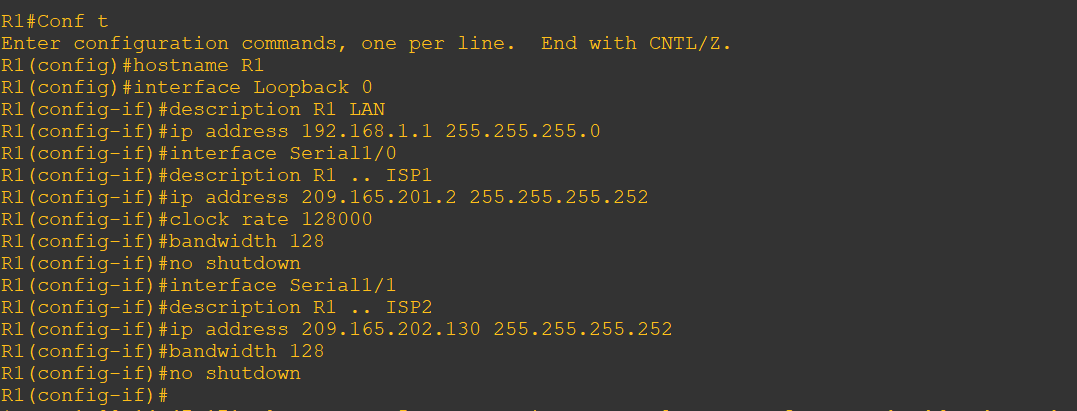
description R1 🡪 ISP2

ip address 209.165.202.130 255.255.255.252

bandwidth 128

no shutdown

exit



**Router R2 Console (hostname ISP1)**

Conf t

hostname ISP1

interface Loopback0

description Simulated Internet Web Server

ip address 209.165.200.254 255.255.255.255

interface Loopback1

description ISP1 DNS Server

ip address 209.165.201.30 255.255.255.255

interface Serial1/0

description ISP1 🡪 R1

ip address 209.165.201.1 255.255.255.252

bandwidth 128

no shutdown

interface Serial1/1

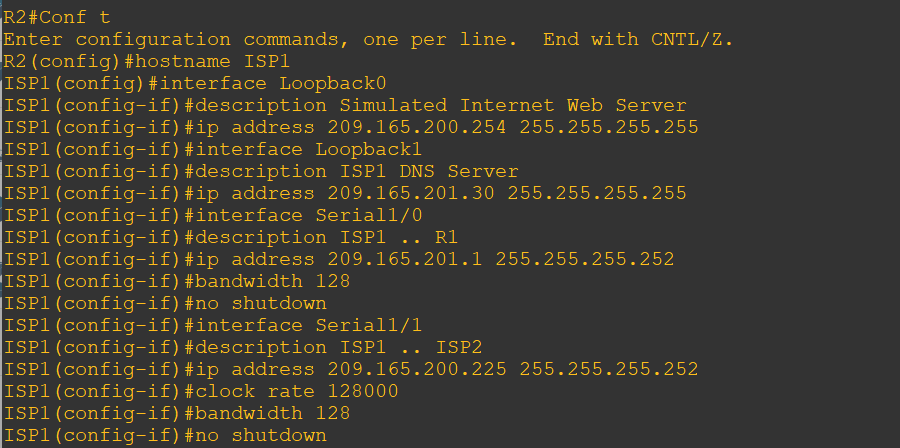
description ISP1 🡪 ISP2

ip address 209.165.200.225 255.255.255.252

clock rate 128000

bandwidth 128

no shutdown



**Router R3 Console (hostname ISP2)**

conf t

hostname ISP2

interface Loopback0

description Simulated Internet Web Server

ip address 209.165.200.254 255.255.255.255

interface Loopback1

description ISP2 DNS Server

ip address 209.165.202.158 255.255.255.255

interface Serial1/1

description ISP2 🡪 R1

ip address 209.165.202.129 255.255.255.252

clock rate 128000

bandwidth 128

no shutdown

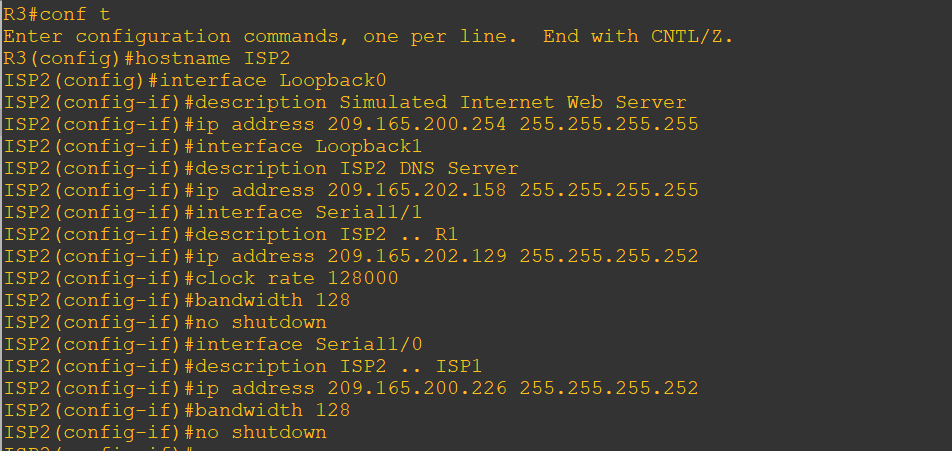
interface Serial1/0

description ISP2 🡪 ISP1

ip address 209.165.200.226 255.255.255.252

bandwidth 128

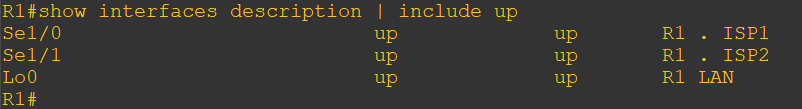
no shutdown



b) Verify the configuration by using the show interfaces description command. The output from router R1 is shown below.

**Router R1 Console**

show interfaces description | include up



All three interfaces should be active. Troubleshoot if necessary.

**Step 2:- Configure static routing.**

The current routing policy in the topology is as follows:

1) Router R1 establishes connectivity to the Internet through ISP1 using a default static route.

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

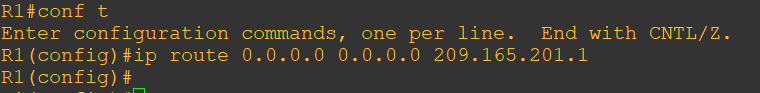
3) ISP1 and ISP2 both have static routes back to the ISP LAN.

a) Implement the routing policies on the respective routers.

**Router R1 Console**

conf t

ip route 0.0.0.0 0.0.0.0 209.165.201.1



**Router R2 Console (hostname ISP1)**

conf t

router eigrp 1

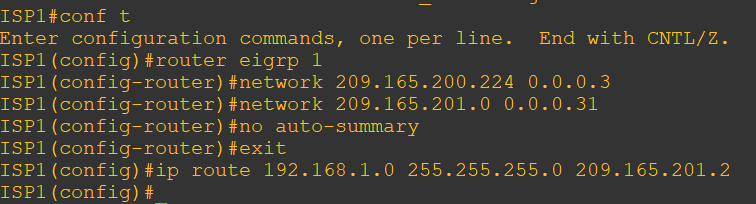
network 209.165.200.224 0.0.0.3

network 209.165.201.0 0.0.0.31

no auto-summary

exit

ip route 192.168.1.0 255.255.255.0 209.165.201.2



**Router R3 Console (hostname ISP2)**

conf t

router eigrp 1

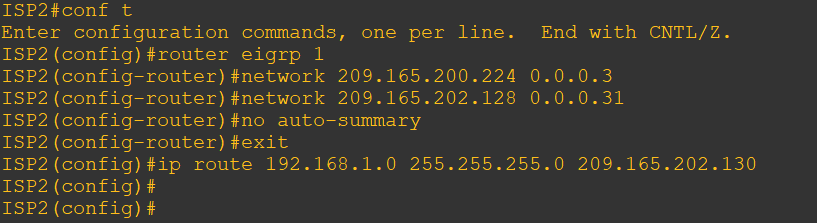
network 209.165.200.224 0.0.0.3

network 209.165.202.128 0.0.0.31

no auto-summary

exit

ip route 192.168.1.0 255.255.255.0 209.165.202.130



b) The Cisco IOS IP SLA feature enables an administrator to monitor network performance between Cisco devices (switches or routers) or from a Cisco device to a remote IP device. IP SLA probes continuously check the reachability of a specific destination, such as a provider edge router interface, the DNS server of the ISP, or any other specific destination, and can conditionally announce a default route only if the connectivity is verified.

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

**Router R1 Console**

tclsh

foreach address {

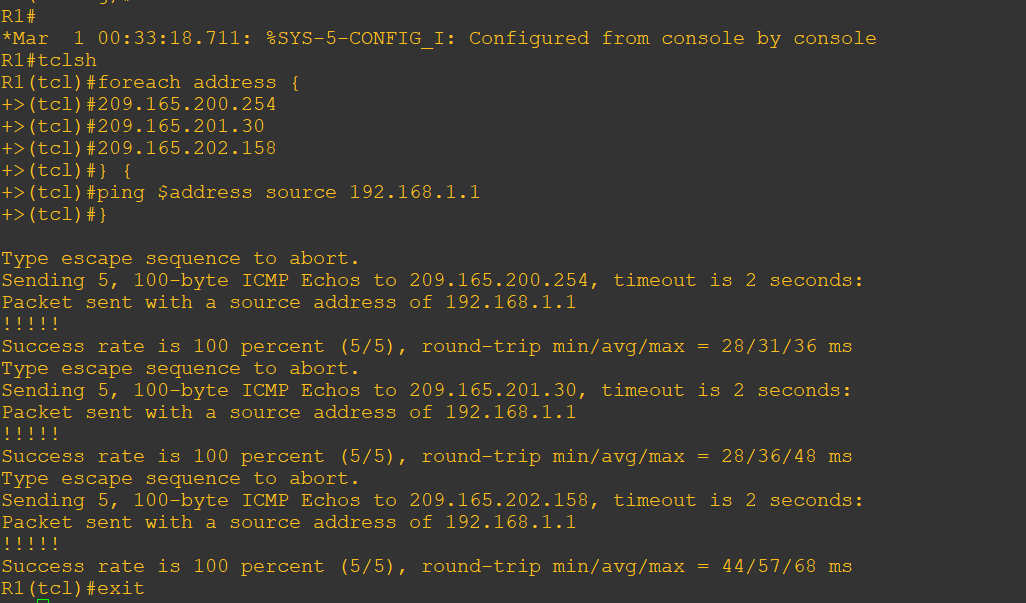
209.165.200.254

209.165.201.30

209.165.202.158

} { ping $address source 192.168.1.1 }

exit



c) Trace the path taken to the web server, ISP1 DNS server, and ISP2 DNS server

**Router R1 Console**

tclsh

foreach address {

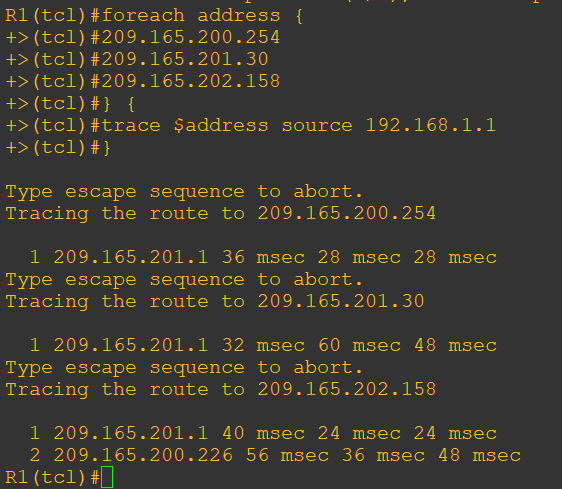
209.165.200.254

209.165.201.30

209.165.202.158

} { ping $address source 192.168.1.1 }

exit



**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 monitor command.

**Router R1 Console**

conf t

ip sla monitor 11

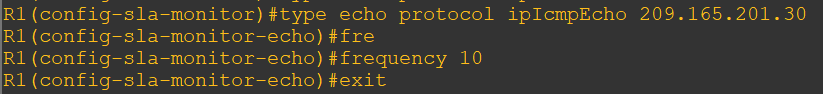
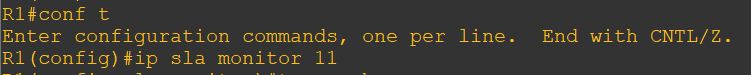
type echo protocol ipIcmpEcho 209.165.201.30

frequency 10

exit

ip sla monitor schedule 11 life forever start-time now

exit

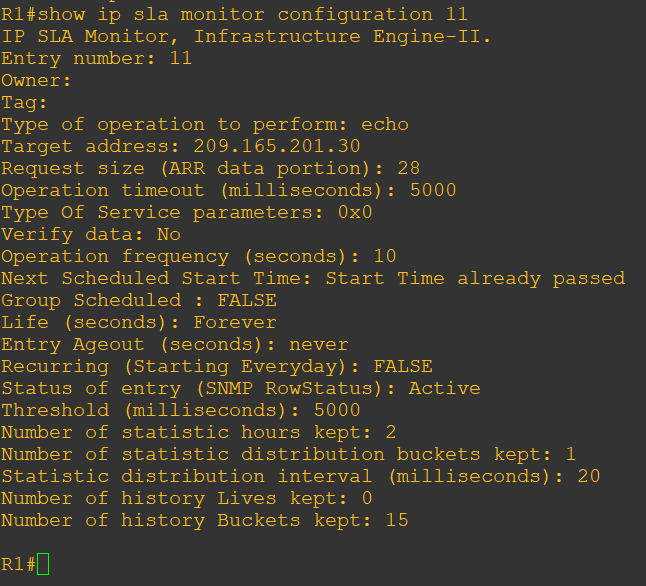


The operation number of 11 is only locally significant to the router. The frequency 10 command schedules the connectivity test to repeat every 10 seconds. The probe is scheduled to start now and to run forever.

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

**Router R1 Console**

show ip sla monitor configuration 11

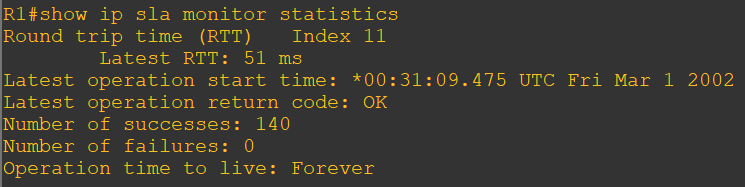


The output lists the details of the configuration of operation 11. The operation is an ICMP echo to 209.165.201.30, with a frequency of 10 seconds, and it has already started (the start time has already passed).

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

**Router R1 Console**

show ip sla monitor statistics



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

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

**Router R1 Console**

conf t

ip sla monitor 22

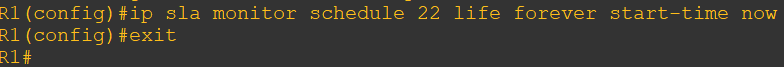
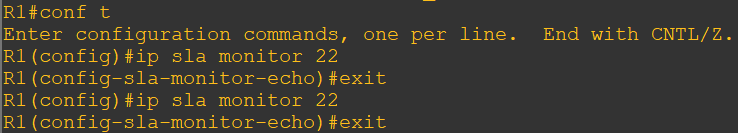
type echo protocol ipIcmpEcho 209.165.201.30

frequency 10

exit

ip sla monitor schedule 22 life forever start-time now

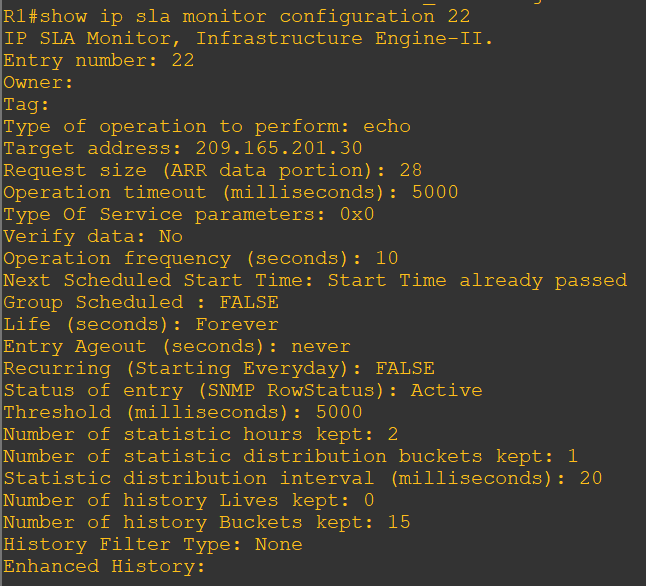
exit



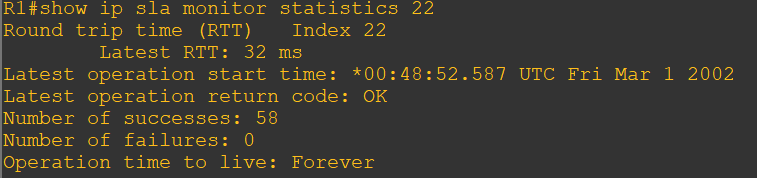
e) Verify the new probe using the **show ip sla monitor configuration** and **show ip sla monitor statistics** commands.

**Router R1 Console**

show ip sla monitor configuration 22



show ip sla monitor statistics 22



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

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

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

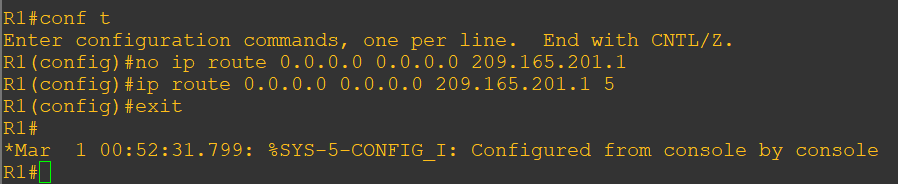
a) On R1, remove the current default route and replace it with a floating static route having an administrative distance of 5.

**Router R1 Console**

no ip route 0.0.0.0 0.0.0.0 209.165.201.1

ip route 0.0.0.0 0.0.0.0 209.165.201.1 5

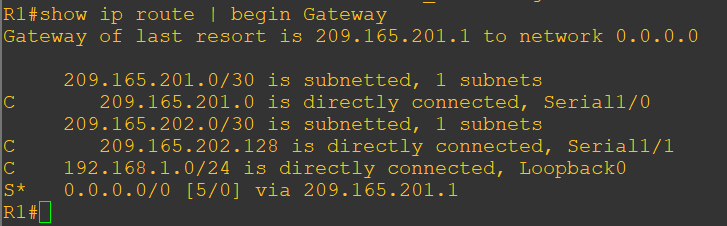
exit



b) Verify the routing table.

**Router R1 Console**

show ip route | begin Gateway

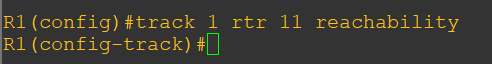


Notice that the default static route is now using the route with the administrative distance of 5. The first tracking object is tied to IP SLA object 11.

c) From global configuration mode on R1, use the track 1 rtr 11 reachability reachability command to enter the config-track subconfiguration mode.

**Router R1 Console**

track 1 rtr 11 reachability

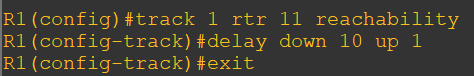


d) Specify the level of sensitivity to changes of tracked objects to 10 seconds of down delay and 1 second of up delay using the **delay down 10 up 1** command. The delay helps to alleviate the effect of flapping objects—objects that are going down and up rapidly. In this situation, if the DNS server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

delay down 10 up 1

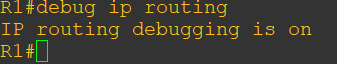
exit

exit



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

debug ip routing

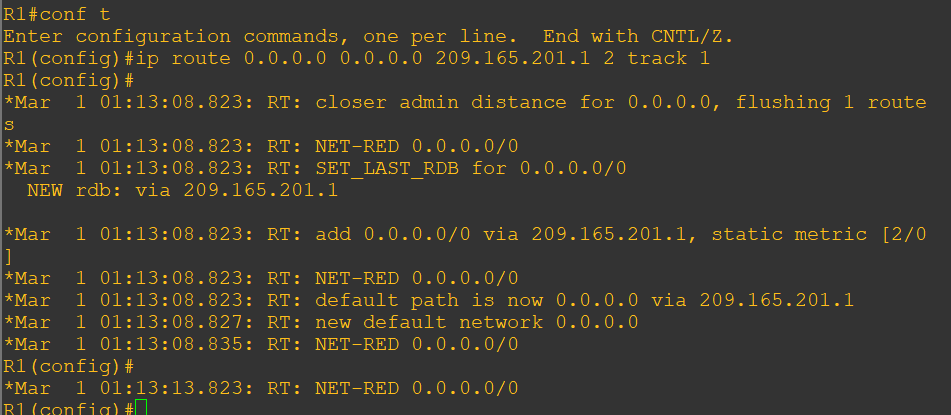


f) Configure the floating static route that will be implemented when tracking object 1 is active. Use the ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1 command to create a floating static default route via 209.165.201.1 (ISP1). Notice that this command references the tracking object number 1, which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

conf t

ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1

exit



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

g. 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.

conf t

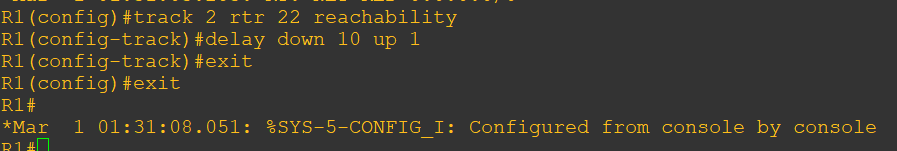
track 2 rtr 22 reachability

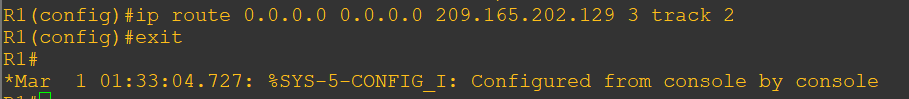
delay down 10 up 1

exit

ip route 0.0.0.0 0.0.0.0 209.165.202.129 3 track 2

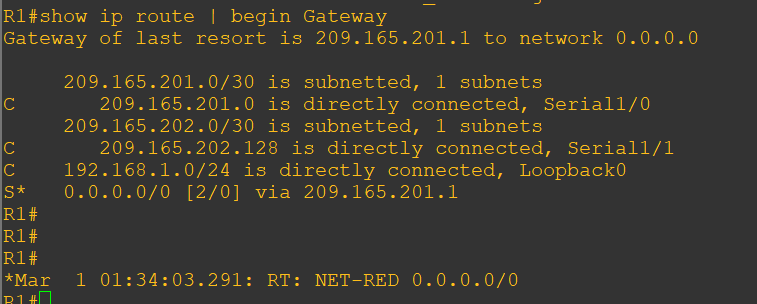
exit





h. Verify the routing table again.

show ip route | begin Gateway



Step 5: Verify IP SLA operation.

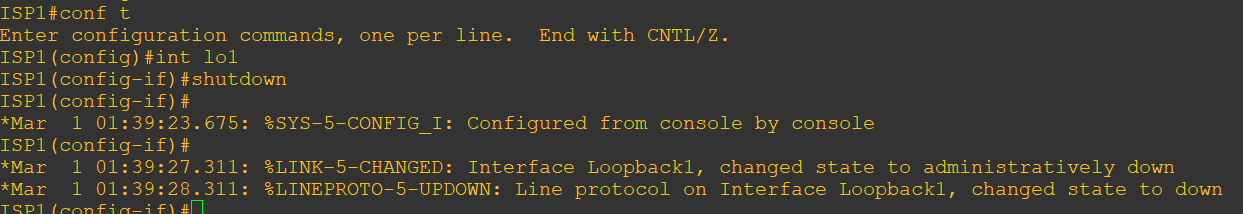
a) On ISP1, disable the loopback interface 1.

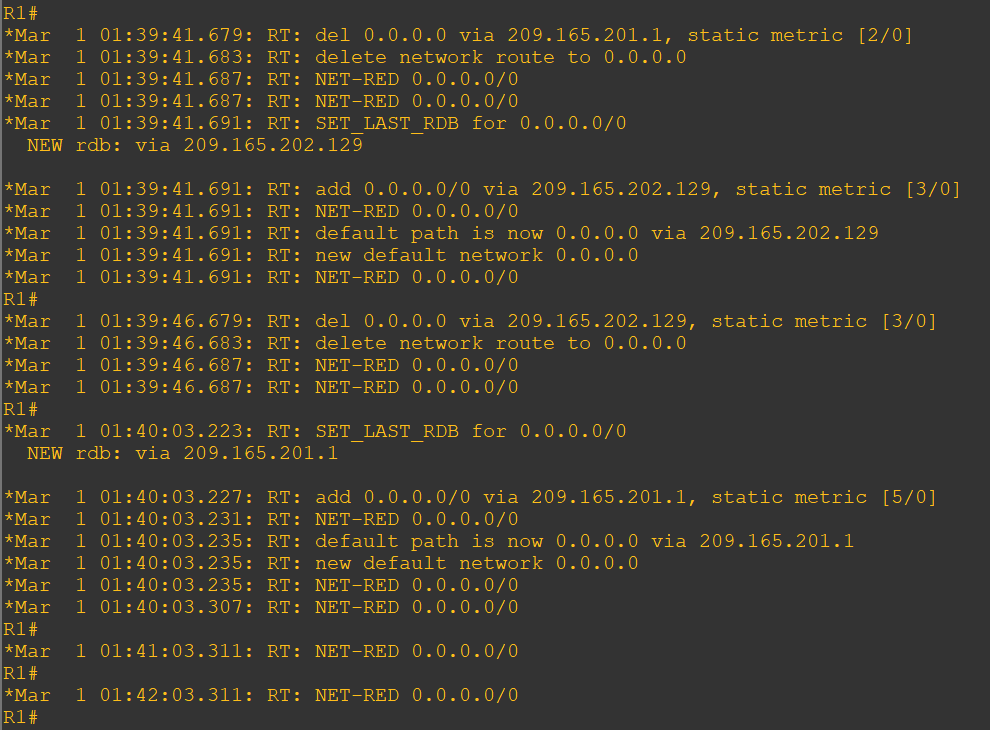
**ISP1 R2 Console**

conf t

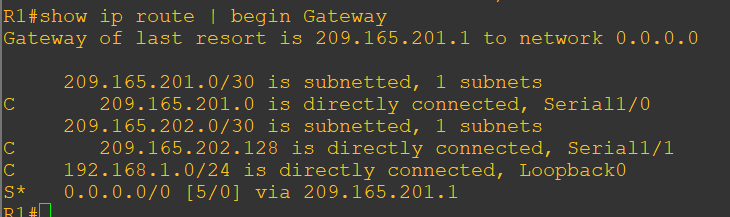
int lo1

shutdown





c. On R1, verify the routing table.



d. Verify the IP SLA statistics

