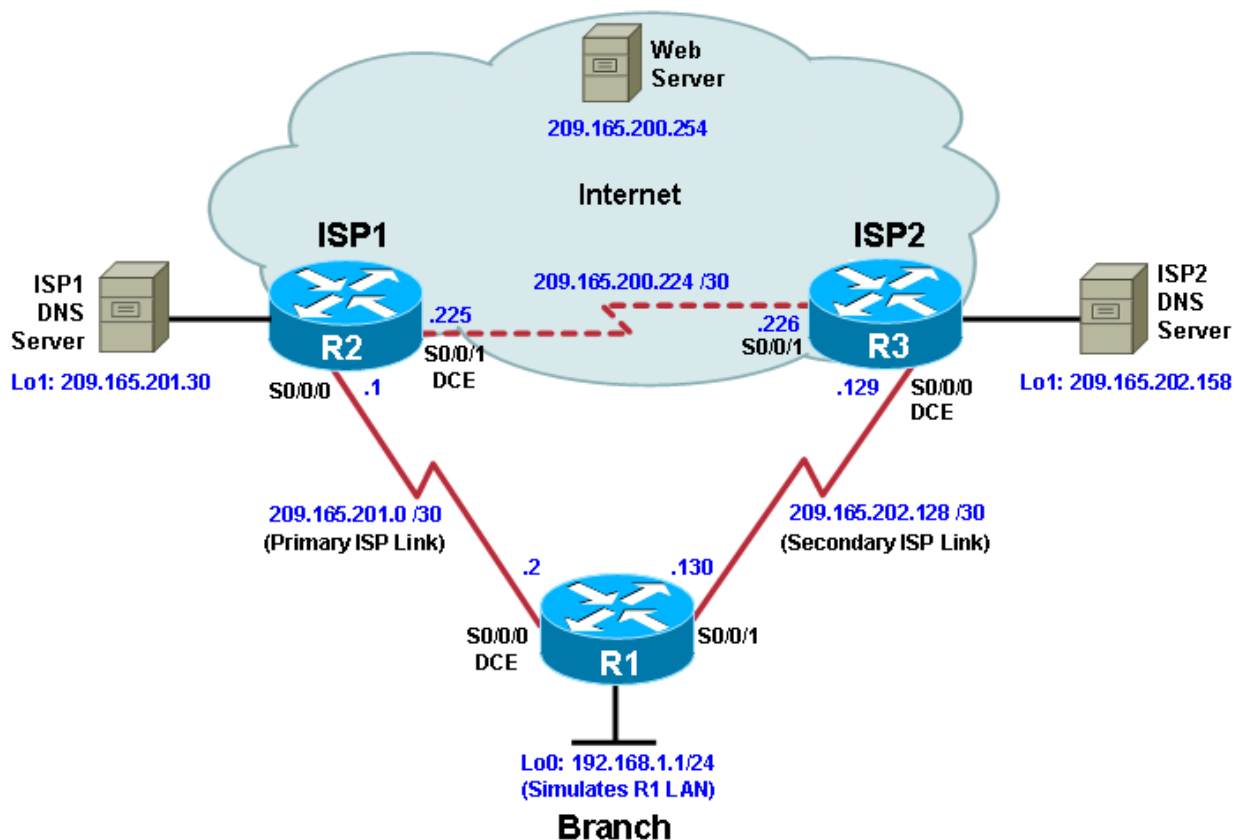# Practical No: 1

Aim: Configure IP SLA Tracking and Path Control

Topology

Objectives

Configure and verify the IP SLA feature.

Test the IP SLA tracking feature.

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

Background

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

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

to a backup ISP.

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

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

Required Resources

3 routers (Cisco IOS Release 15.2 or comparable)

Serial and Ethernet cables

Step 1: Configure loopbacks and assign addresses.

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

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

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

Router R1

hostname R1

interface Loopback 0

 description R1 LAN

 ip address 192.168.1.1 255.255.255.0

interface Serial0/0/0

 description R1 --> ISP1

 ip address 209.165.201.2 255.255.255.252

 clock rate 128000

 bandwidth 128

no shutdown

interface Serial0/0/1

 description R1 --> ISP2

 ip address 209.165.202.130 255.255.255.252

 bandwidth 128

 no shutdown

Router ISP1 (R2)

hostname ISP1

interface Loopback0

 description Simulated Internet Web Server

 ip address 209.165.200.254 255.255.255.255

interface Loopback1

 description ISP1 DNS Server

 ip address 209.165.201.30 255.255.255.255

interface Serial0/0/0

 description ISP1 --> R1

 ip address 209.165.201.1 255.255.255.252

 bandwidth 128

 no shutdown

interface Serial0/0/1

 description ISP1 --> ISP2

ip address 209.165.200.225 255.255.255.252

 clock rate 128000

 bandwidth 128

 no shutdown

Router ISP2 (R3)

hostname ISP2

interface Loopback0

 description Simulated Internet Web Server

 ip address 209.165.200.254 255.255.255.255

interface Loopback1

 description ISP2 DNS Server

 ip address 209.165.202.158 255.255.255.255

interface Serial0/0/0

 description ISP2 --> R1

 ip address 209.165.202.129 255.255.255.252

 clock rate 128000

 bandwidth 128

 no shutdown

interface Serial0/0/1

 description ISP2 --> ISP1

 ip address 209.165.200.226 255.255.255.252

 bandwidth 128

no shutdown

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

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

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

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

Lo0   up   up   R1 LAN

R1#

All three interfaces should be active. Troubleshoot if necessary.

Step 2: Configure static routing.

The current routing policy in the topology is as follows:

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

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

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

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

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

Router R1

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

R1(config)#

Router ISP1 (R2)

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

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

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

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

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

ISP1(config)#

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

ISP1(config)#

Router ISP2 (R3)

ISP2(config)# router eigrp 1

ISP2(config-router)# network 209.165.200.224 0.0.0.3

ISP2(config-router)# network 209.165.202.128 0.0.0.31

ISP2(config-router)# no auto-summary

ISP2(config-router)# exit

ISP2(config)#

ISP2(config)# ip route 192.168.1.0 255.255.255.0 209.165.202.130

ISP2(config)#

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

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

Before implementing the Cisco IOS SLA feature, you must verify reachability to the Internet servers. From router R1, ping the web server, ISP1 DNS server, and ISP2 DNS server to verify connectivity. You can copy the following Tcl script and paste it into R1.

foreach address {

209.165.200.254

209.165.201.30

209.165.202.158

} {

ping $address source 192.168.1.1

}

All pings should be successful. Troubleshoot if necessary.

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

foreach address {

209.165.200.254

209.165.201.30

209.165.202.158

} {

trace $address source 192.168.1.1

}

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.

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

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

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

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

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

R1(config)#

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

R1(config)#

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

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

R1# **show ip sla configuration 11**

IP SLAs Infrastructure Engine-III

Entry number: 11

Owner:

Tag:

Operation timeout (milliseconds): 5000

==Type of operation to perform: icmp-echo==

==Target address==/Source address: ==209.165.201.30==/0.0.0.0

Type Of Service parameter: 0x0

Request size (ARR data portion): 28

Verify data: No

Vrf Name:

Schedule:

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

==Next Scheduled Start Time: Start Time already passed==

Group Scheduled : FALSE

Randomly Scheduled : FALSE

==Life (seconds): Forever==

Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE

Status of entry (SNMP RowStatus): Active

Threshold (milliseconds): 5000

Distribution Statistics:

Number of statistic hours kept: 2

Number of statistic distribution buckets kept: 1

Statistic distribution interval (milliseconds): 20

Enhanced History:

History Statistics:

Number of history Lives kept: 0

Number of history Buckets kept: 15

History Filter Type: None

R1#

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

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

R1# **show ip sla statistics**

IPSLAs Latest Operation Statistics

IPSLA operation id: 11

Latest RTT: 8 milliseconds

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

Latest operation return code: OK

Number of successes: 51

Number of failures: 0

Operation time to live: Forever

R1#

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

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

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

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

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

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

R1(config)#

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

R1(config)# **end**

R1#

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

R1# **show ip sla configuration 22**

IP SLAs Infrastructure Engine-III

Entry number: 22

Owner:

Tag:

Operation timeout (milliseconds): 5000

Type of operation to perform: icmp-echo

Target address/Source address: 209.165.202.158/0.0.0.0

Type Of Service parameter: 0x0

Request size (ARR data portion): 28

Verify data: No

Vrf Name:

Schedule:

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

Next Scheduled Start Time: Start Time already passed

Group Scheduled : FALSE

Randomly Scheduled : FALSE

Life (seconds): Forever

Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE

Status of entry (SNMP RowStatus): Active

Threshold (milliseconds): 5000

Distribution Statistics:

Number of statistic hours kept: 2

Number of statistic distribution buckets kept: 1

Statistic distribution interval (milliseconds): 20

Enhanced History:

History Statistics:

Number of history Lives kept: 0

Number of history Buckets kept: 15

History Filter Type: None

R1# show ip sla configuration 22

IP SLAs, Infrastructure Engine-II.

Entry number: 22

Owner:

Tag:

Type of operation to perform: icmp-echo

Target address/Source address: 209.165.201.158/0.0.0.0

Type Of Service parameter: 0x0

Request size (ARR data portion): 28

Operation timeout (milliseconds): 5000

Verify data: No

Vrf Name:

Schedule:

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

Next Scheduled Start Time: ==Start Time already passed==

Group Scheduled : FALSE

Randomly Scheduled : FALSE

Life (seconds): ==Forever==

Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE

Status of entry (SNMP RowStatus): Active

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

Distribution Statistics:

Number of statistic hours kept: 2

Number of statistic distribution buckets kept: 1

Statistic distribution interval (milliseconds): 20

History Statistics:

Number of history Lives kept: 0

Number of history Buckets kept: 15

History Filter Type: None

Enhanced History:

R1#

R1# **show ip sla statistics 22**

IPSLAs Latest Operation Statistics

==IPSLA operation id: 22==

Latest RTT: 16 milliseconds

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

Number of failures: 0

R1#

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

Step 4: Configure tracking options.

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

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

R1(config)# no ip route 0.0.0.0 0.0.0.0 209.165.201.1

R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.1 5

R1(config)# exit

Verify the routing table.

R1# show ip route | begin Gateway

Gateway of last resort is 209.165.201.1 to network 0.0.0.0

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

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

C   192.168.1.0/24 is directly connected, Loopback0

L   192.168.1.1/32 is directly connected, Loopback0

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

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

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

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

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

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

R1#

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

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

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

   R1(config-track)#

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

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

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

   R1(config)#

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

   R1# **debug ip routing**

   IP routing debugging is on

   R1#

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

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

   R1(config)#

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

     via 209.165.201.1   0 1048578

Jan 10 10:45:39.119: RT: <mark>closer admin distance for 0.0.0.0,</mark> <mark>flushing 1 routes</mark>

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

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

  via 209.165.201.1 0 1048578

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

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

  via 209.165.201.1 0 1048578

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

R1(config)#

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

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

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

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

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

R1(config)#

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

R1(config)#

Verify the routing table again.

R1#show ip route | begin Gateway

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

C   192.168.1.0/24 is directly connected, Loopback0

L   192.168.1.1/32 is directly connected, Loopback0

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

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

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

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

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

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

R1#

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

Step 5: Verify IP SLA operation.

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

Disable the DNS loopback interface on ISP1 (R2).

Observe the output of the **debug** command on R1.

Verify the static route entries in the routing table and the IP SLA statistics of R1.

Re-enable the loopback interface on ISP1 (R2) and again observe the operation of the IP SLA tracking feature.

On ISP1, disable the loopback interface 1.

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

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

ISP1(config-if)#

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

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

changed state to down

ISP1(config-if)#

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

R1#

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

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

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

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

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

   via 209.165.202.129   0 1048578

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

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

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

   via 209.165.201.1   0 1048578

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

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

   via 209.165.202.129   0 1048578

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

   via 209.165.201.1   0 1048578

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

R1#

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

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

On R1, verify the routing table.

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

<mark>Gateway of last resort is 209.165.202.129 to network 0.0.0.0</mark>

<mark>S*   0.0.0.0/0 [3/0] via 209.165.202.129</mark>

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

C   192.168.1.0/24 is directly connected, Loopback0

L   192.168.1.1/32 is directly connected, Loopback0

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

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

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

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

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

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

R1#

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

Verify the IP SLA statistics.

R1# **show ip sla statistics**

IPSLAs Latest Operation Statistics

IPSLA operation id: 11

      Latest RTT: NoConnection/Busy/Timeout

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

<mark>Latest operation return code: Timeout</mark>

Number of successes: 173

<mark>Number of failures: 45</mark>

Operation time to live: Forever

IPSLA operation id: 22

Latest RTT: 8 milliseconds

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

Latest operation return code: OK

Number of successes: 218

Number of failures: 0

Operation time to live: Forever

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

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

R1# **trace 209.165.200.254 source 192.168.1.1**

Type escape sequence to abort.

Tracing the route to 209.165.200.254

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

  1 209.165.202.129 4 msec * *

R1#

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

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

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

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

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

ISP1(config-if)#

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

R1#

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

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

  via 209.165.201.1 0 1048578

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

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

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

  via 209.165.202.129 0 1048578

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

Jan 10 11:06:20.551: RT: u

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

  via 209.165.202.129 0 1048578

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

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

  via 209.165.201.1 0 1048578

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

R1#

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

Again examine the IP SLA statistics.

R1# **show ip sla statistics**

IPSLAs Latest Operation Statistics

IPSLA operation id: 11

      Latest RTT: 8 milliseconds

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

<mark>Latest operation return code: OK</mark>

<mark>Number of successes: 182</mark>

Number of failures: 75

Operation time to live: Forever

IPSLA operation id: 22

      Latest RTT: 16 milliseconds

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

Latest operation return code: OK

Number of successes: 257

Number of failures: 0

Operation time to live: Forever

R1#

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

Verify the routing table.

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

Gateway of last resort is 209.165.201.1 to network 0.0.0.0

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

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

C   192.168.1.0/24 is directly connected, Loopback0

L   192.168.1.1/32 is directly connected, Loopback0

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

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

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

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

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

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

R1#