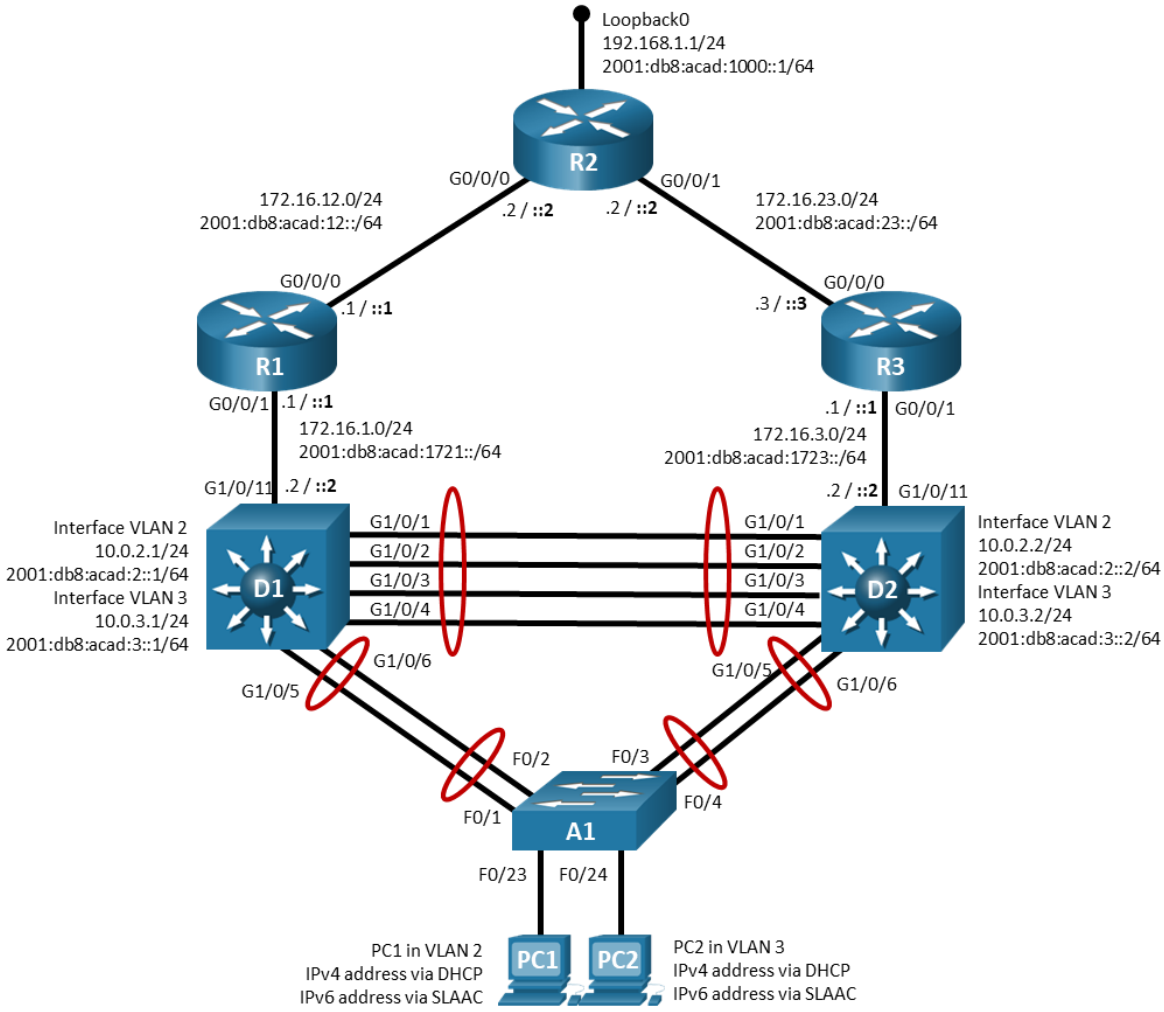
Lab - Implement IP SLA

Topology



Addressing Table

Device	Interface	IPv4 Address/Mask	IPv6 Address/Prefix	IPv6 Link Local
R1	G0/0/0	172.16.12.1/24	2001:db8:acad:12::1/64	fe80::1:1
	G0/0/1	172.16.1.1/24	2001:db8:acad:1721::1/64	fe80::1:2
R2	G0/0/0	172.16.12.2/24	2001:db8:acad:12::2/64	fe80::2:1
	G0/0/1	172.16.24.2/24	2001:db8:acad:23::2/64	fe80::2:2
	Loopback 0	192.168.1.1/24	2001:db8:acad:1000::1/64	fe80::2:3
R3	G0/0/0	172.16.23.3/24	2001:db8:acad:23::3/64	fe80::3:1

Device	Interface	IPv4 Address/Mask	IPv6 Address/Prefix	IPv6 Link Local
	G0/0/1	172.16.3.1/24	2001:db8:acad:1723::1/64	fe80::3:2
D1	G1/0/11	172.16.1.2/24	2001:db8:acad:1721::2/64	fe80::d1:1
	VLAN 2	10.0.2.1/24	2001:db8:acad:2::1/64	fe80::d1:2
	VLAN 3	10.0.3.1/24	2001:db8:acad:3::1/64	fe80::d1:3
D2	G1/0/11	172.16.3.2/24	2001:db8:acad:23::3/64	fe80::d2:1
	VLAN 2	10.0.2.2/24	2001:db8:acad:2::2/64	fe80::d2:2
	VLAN 3	10.0.3.2/24	2001:db8:acad:3::2/64	fe80::d2:3
A1	VLAN 2	10.0.2.3/24	2001:db8:acad:2::3/64	fe80::a1:1
PC 1	NIC	DHCP	SLAAC	EUI-64
PC 2	NIC	DHCP	SLAAC	EUI-64

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Observe IP SLA Operations

Part 3: Configure and Observe HSRP IP SLA Tracking

Background / Scenario

Cisco IP service level agreements (SLAs) allow users to monitor network performance between Cisco devices (switches or routers), or from a Cisco device to a remote IP device. Cisco IP SLAs can be applied to VoIP and video applications as well as monitoring end-to-end IP network performance.

Note: This lab is an exercise in deploying and verifying IP SLAs and does not necessarily reflect networking best practices. The IP SLA itself is an additional task that must be performed by the switch CPU. A large number of intensive SLAs could create a significant burden on the CPU, possibly interfering with other switch functions and having detrimental impact on the overall device performance. Therefore, you should carefully evaluate the benefits of running IP SLAs. The CPU load should be monitored after the SLAs are deployed to verify that they do not stress the device's CPU above safe limits.

Note: The routers used with CCNP hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 3650s with Cisco IOS XE Release 16.9.4 (universalk9 image) and Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Note: The default Switch Database Manager (SDM) template on a Catalyst 2960 does not support IPv6. You must change the default SDM template to the dual-ipv4-and-ipv6 default template using the **sdm prefer dual-ipv4-and-ipv6 default** global configuration command. Changing the template will require a reboot.

Required Resources

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 2 Switches (Cisco 3650 with Cisco IOS XE Release 16.9.4 universal image or comparable)

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PC (Choice of operating system with a terminal emulation program installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructions

Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing

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

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 switch.

a. Console into each switch, enter global configuration mode, and apply the basic settings. The startup configurations for each device are provided below.

Router R1

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, Implement IP SLA #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
 exit
interface g0/0/0
 ip address 172.16.12.1 255.255.255.0
 ipv6 address fe80::1:1 link-local
 ipv6 address 2001:db8:acad:12::1/64
 no shutdown
 exit
interface g0/0/1
 ip address 172.16.1.1 255.255.255.0
 ipv6 address fe80::1:2 link-local
 ipv6 address 2001:db8:acad:1721::1/64
 no shutdown
```

```
 exit
router ospf 4
 router-id 1.1.1.4
 network 172.16.0.0 0.0.255.255 area 0
 exit
ipv6 router ospf 6
 router-id 1.1.1.6
 exit
interface g0/0/0
 ipv6 ospf 6 area 0
 exit
interface g0/0/1
 ipv6 ospf 6 area 0
 exit
end
```

Router R2

```
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, Implement IP SLA #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
 exit
interface g0/0/1
 ip address 172.16.23.2 255.255.255.0
 ipv6 address fe80::2:1 link-local
 ipv6 address 2001:db8:acad:23::2/64
 no shutdown
 exit
interface g0/0/0
 ip address 172.16.12.2 255.255.255.0
 ipv6 address fe80::2:2 link-local
 ipv6 address 2001:db8:acad:12::2/64
 no shutdown
 exit
interface loopback 0
 ip address 192.168.1.1 255.255.255.0
```

```
 ipv6 address fe80::2:3 link-local
 ipv6 address 2001:db8:acad:1000::1/64
 ip ospf network point-to-point
 ipv6 ospf network point-to-point
 no shutdown
 exit
router ospf 4
 router-id 2.2.2.4
 network 172.16.0.0 0.0.255.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
 exit
ipv6 router ospf 6
 router-id 2.2.2.6
 exit
interface g0/0/0
 ipv6  ospf 6 area 0
 exit
interface g0/0/1
 ipv6  ospf 6 area 0
 exit
interface Loopback 0
 ipv6  ospf 6 area 0
 exit
end
```

Router R3

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, Implement IP SLA #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
 exit
interface g0/0/0
 ip address 172.16.23.3 255.255.255.0
 ipv6 address fe80::3:1 link-local
 ipv6 address 2001:db8:acad:23::3/64
 no shutdown
```

```
 exit
interface g0/0/1
 ip address 172.16.3.1 255.255.255.0
 ipv6 address fe80::3:2 link-local
 ipv6 address 2001:db8:acad:1723::1/64
 no shutdown
 exit
router ospf 4
 router-id 3.3.3.4
 network 172.16.0.0 0.0.255.255 area 0
 exit
ipv6 router ospf 6
 router-id 3.3.3.6
 exit
interface g0/0/0
 ipv6 ospf 6 area 0
 exit
interface g0/0/1
 ipv6 ospf 6 area 0
 exit
end
```

Switch D1

```
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, Implement IP SLA #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
 exit
interface range g1/0/1-24, g1/1/1-4, g0/0
 shutdown
 exit
interface range g1/0/1-6
 switchport mode trunk
 no shutdown
 exit
```

```
interface range g1/0/1-4
 channel-group 12 mode active
 exit
interface range g1/0/5-6
 channel-group 1 mode active
 exit
interface g1/0/11
 no switchport
 ip address 172.16.1.2 255.255.255.0
 ipv6 address fe80::d1:1 link-local
 ipv6 address 2001:db8:acad:1721::2/64
 no shutdown
 exit
vlan 2
 name SECOND_VLAN
 exit
vlan 3
 name THIRD_VLAN
 exit
spanning-tree vlan 2 root primary
spanning-tree vlan 3 root secondary
interface vlan 2
 ip address 10.0.2.1 255.255.255.0
 ipv6 address fe80::d1:2 link-local
 ipv6 address 2001:db8:acad:2::1/64
 no shutdown
 exit
interface vlan 3
 ip address 10.0.3.1 255.255.255.0
 ipv6 address fe80::d1:3 link-local
 ipv6 address 2001:db8:acad:3::1/64
 no shutdown
 exit
interface vlan 2
 standby version 2
 standby 2 ip 10.0.2.254
 standby 2 priority 150
 standby 2 preempt
 standby 26 ipv6 autoconfig
 standby 26 priority 150
 standby 26 preempt
 exit
interface vlan 3
 standby version 2
 standby 3 ip 10.0.3.254
```

```
 standby 3 preempt
 standby 36 ipv6 autoconfig
 standby 36 preempt
 exit
router ospf 4
 router-id 0.13.1.4
 network 172.16.1.0 0.0.0.255 area 0
 network 10.0.0.0 0.0.255.255 area 0
 passive-interface vlan 2
 passive-interface vlan 3
 exit
ipv6 router ospf 6
 router-id 0.13.1.6
 passive-interface vlan 2
 passive-interface vlan 3
 exit
interface g1/0/11
 ipv6 ospf 6 area 0
 exit
interface vlan 2
 ipv6 ospf 6 area 0
 exit
interface vlan 3
 ipv6 ospf 6 area 0
 exit
ip dhcp excluded-address 10.0.2.1 10.0.2.5
ip dhcp excluded-address 10.0.2.128 10.0.2.254
ip dhcp pool SECOND_VLAN_DHCP_POOL
 network 10.0.2.0 255.255.255.0
 default-router 10.0.2.254
 exit
ip dhcp excluded-address 10.0.3.1 10.0.3.128
ip dhcp excluded-address 10.0.3.254
ip dhcp pool THIRD_VLAN_DHCP_POOL
 network 10.0.3.0 255.255.255.0
 default-router 10.0.3.254
 exit
end
```

Switch D2

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, Implement IP SLA #
line con 0
```

```
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
 exit
interface range g1/0/1-24, g1/1/1-4, g0/0
 shutdown
 exit
interface range g1/0/1-6
 switchport mode trunk
 no shutdown
 exit
interface range g1/0/1-4
 channel-group 12 mode active
 exit
interface range g1/0/5-6
 channel-group 2 mode active
 exit
interface g1/0/11
 no switchport
 ip address 172.16.3.2 255.255.255.0
 ipv6 address fe80::d2:1 link-local
 ipv6 address 2001:db8:acad:1723::2/64
 no shutdown
 exit
vlan 2
 name SECOND_VLAN
 exit
vlan 3
 name THIRD_VLAN
 exit
spanning-tree vlan 2 root secondary
spanning-tree vlan 3 root primary
interface vlan 2
 ip address 10.0.2.2 255.255.255.0
 ipv6 address fe80::d2:2 link-local
 ipv6 address 2001:db8:acad:2::2/64
 no shutdown
 exit
interface vlan 3
```

```
 ip address 10.0.3.2 255.255.255.0
 ipv6 address fe80::d2:3 link-local
 ipv6 address 2001:db8:acad:3::2/64
 no shutdown
 exit
interface vlan 2
 standby version 2
 standby 2 ip 10.0.2.254
 standby 2 preempt
 standby 26 ipv6 autoconfig
 standby 26 preempt
 exit
interface vlan 3
 standby version 2
 standby 3 ip 10.0.3.254
 standby 3 priority 150
 standby 3 preempt
 standby 36 ipv6 autoconfig
 standby 36 priority 150
 standby 36 preempt
 exit
router ospf 4
 router-id 0.13.2.4
 network 172.16.3.0 0.0.0.255 area 0
 network 10.0.0.0 0.0.255.255 area 0
 passive-interface vlan 2
 passive-interface vlan 3
 exit
ipv6 router ospf 6
 router-id 0.13.2.6
 passive-interface vlan 2
 passive-interface vlan 3
 exit
interface g1/0/11
 ipv6 ospf 6 area 0
 exit
interface vlan 2
 ipv6 ospf 6 area 0
 exit
interface vlan 3
 ipv6 ospf 6 area 0
 exit
ip dhcp excluded-address 10.0.2.1 10.0.2.128
ip dhcp excluded-address 10.0.2.254
ip dhcp pool SECOND_VLAN_DHCP_POOL
```

```
 network 10.0.2.0 255.255.255.0
 default-router 10.0.2.254
 exit
ip dhcp excluded-address 10.0.3.1 10.0.3.5
ip dhcp excluded-address 10.0.3.128 10.0.3.254
ip dhcp pool THIRD_VLAN_DHCP_POOL
 network 10.0.3.0 255.255.255.0
 default-router 10.0.3.254
 exit
end
```

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, Implement IP SLA #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 logging synchronous
 login
 exit
interface range f0/1-24, g0/1-2
 shutdown
 exit
interface range f0/1-4
 switchport mode trunk
 no shutdown
 exit
interface range f0/1-2
 channel-group 1 mode active
 exit
interface range f0/3-4
 channel-group 2 mode active
 exit
vlan 2
 name SECOND_VLAN
 exit
vlan 3
 name THIRD_VLAN
 exit
interface f0/23
```

```
 switchport mode access
 switchport access vlan 2
 spanning-tree portfast
 no shutdown
 exit
interface f0/24
 switchport mode access
 switchport access vlan 3
 spanning-tree portfast
 no shutdown
 exit
interface vlan 2
 ip address 10.0.2.3 255.255.255.0
 ipv6 address fe80::a1:1 link-local
 ipv6 address 2001:db8:acad:2::3/64
 no shutdown
 exit
ip default-gateway 10.0.2.254
end
```

b. Set the clock on each switch to UTC time.

c. Save the running configuration to startup-config.

Step 3: Configure the PCs for network connectivity.

Configure PC1 and PC2 for DHCP and SLAAC.

Part 2: Configure and Observe IP SLA Operations

In Part 2 you will configure and observe IP SLA operations. The SLA itself is simply a testing mechanism. Our example will test for simple reachability with an ICMP echo, but SLAs can do a lot more with many other protocols.

For now, all you will do is configure and schedule the IP SLAs and then query their status. This way you see the SLA operation separate from any application it might be used for.

Step 1: Create IP SLAs on switch D1.

a. Create IP SLA 4 using the command **ip sla 4**. The number 4 is locally significant and could be any number between 1 and 2147483647.

```
D1(config)# ip sla 4
```

b. Configure IP SLA 4 to send an icmp-echo to the IPv4 address 192.168.1.1 and set the frequency for the ping to be every 15 seconds.

```
D1(config-ip-sla)# icmp-echo 192.168.1.1
D1(config-ip-sla-echo)# frequency 15
D1(config-ip-sla-echo)# exit
```

c. Create IP SLA 6.

```
D1(config)# ip sla 6
```

d. Configure IP SLA 6 to send an icmp-echo to the IPv4 address 2001:db8:acad:1000::1 and set the frequency for the ping to be every 15 seconds.

```
D1(config-ip-sla)# icmp-echo 2001:db8:acad:1000::1
D1(config-ip-sla-echo)# frequency 15
D1(config-ip-sla-echo)# exit
```

e. Use the **ip sla schedule** command to configure both SLA 4 and SLA 6 with a life of forever and to start immediately.

```
D1(config)# ip sla schedule 4 life forever start-time now
D1(config)# ip sla schedule 6 life forever start-time now
```

Step 2: Observe IP SLA operation.

a. Issue the command **show ip sla summary** to see a summarized status of the SLAs now that you have scheduled them.

```
D1# show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return      Last
                                                       Code        Run
---------------------------------------------------------------------
*4           icmp-echo   192.168.1.1       RTT=2       OK          12 seconds ago



*6           icmp-echo   2001:DB8:ACAD:100 RTT=1       OK          12 seconds ago
                         0::1
```

b. To test and see what response the SLAs give in a failure, issue the **shutdown** command on R1 interface G0/0/0, then issue the **show ip sla summary** command again.

```
D1# show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return      Last
                                                       Code        Run
---------------------------------------------------------------------
*4           icmp-echo   192.168.1.1       -           Timeout     8 seconds ago



*6           icmp-echo   2001:DB8:ACAD:100 -           Timeout     8 seconds ago
                         0::1
```

c. Issue the command **show ip sla configuration 4** to see details on IP SLA 4.

```
D1# show ip sla configuration 4
```

```
IP SLAs Infrastructure Engine-III
Entry number: 4
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 192.168.1.1/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Data pattern: 0xABCDABCD
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 15  (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
```

d. Issue the command **show ip sla statistics 4** to examine statistical information on this IP SLA.

```
D1# show ip sla statistics 4
IPSLAs Latest Operation Statistics

IPSLA operation id: 4
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 19:04:46 UTC Fri Feb 7 2020
Latest operation return code: Timeout
Number of successes: 14
Number of failures: 7
Operation time to live: Forever
```

e. Issue the **no shutdown** command on R1 interface G0/0/0.

f. Configure the same IP SLAs on Switch D2. Verify them in the same manner, issuing the **shutdown** command on R3 interface G0/0/0. When you have verified that SLA is tracking reachability to R2 interface Loopback 0, issue the **no shutdown** command on R3 interface G0/0/0.

Part 3: Configure and Observe HSRP IP SLA Tracking

In this part, we will put the IP SLAs that you created into use, and you can see how they work. In this case, our network is operational and HSRP is providing first-hop redundancy. HSRP will react to a directly connected interface that is failing or coming online, as you saw in the tracking section of the HSRP lab. But what if there is an indirect link failure that makes the active HSRP router less desirable? The IP SLA will allow us to handle this scenario. For this example, we will treat R2 interface Loopback 0 as a critical entity on the internet, like a DNS server. The organizational policy is that if that DNS server is not reachable from the gateway, the gateway should not be used.

Step 1: Verify HSRPv2 is operational.

a. Verify that HSRP is active and operating on Switch D1 with the **show standby brief** command.

```
D1# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl2         2    150 P Active  local           10.0.2.2        10.0.2.254
Vl2         26   150 P Active  local           FE80::D2:2      FE80::5:73FF:FEA0:1A
Vl3         3    100 P Standby 10.0.3.2        local           10.0.3.254
Vl3         36   100 P Standby FE80::D2:3      local           FE80::5:73FF:FEA0:24
```

As you can see from the output, switch D1 is the active virtual router for VLAN 2 and the standby for VLAN 3 for both IPv4 and IPv6.

b. From PC1, start a continuous ping to 192.168.1.1.

c. On D1, issue the **shutdown** command on interface VLAN 2. You should see that HSRP fails over to D2 as the Active Virtual Router for VLAN 2, and the pings continue to succeed. When verified, issue the **no shutdown** command on switch D1 interface VLAN 2.

d. From PC2, start a continuous ping to 192.168.1.1.

e. On D2, issue the **shutdown** command on interface VLAN 3. You should see that HSRP fails over to D1 as the Active Virtual Router for VLAN 3, and the pings continue to succeed. When verified, issue the **no shutdown** command on switch D2 interface VLAN 3.

f. Now issue the **shutdown** command on R1 interface G0/0/0 and R3 interface G0/0/0. Note that there is no impact on either D1 or D2 regarding HSRP, and the pings start failing. Stop the continuous pings on PC1 and PC2 and issue the **no shutdown** command on R1 interface G0/0/0 and R3 interface G0/0/0.

Step 2: Reconfigure HSRP to use the IP SLA.

a. Create a track object using the command **track [number] ip sla [sla number]**.

```
D1(config)# track 4 ip sla 4
```

b. Set the delay timers. These are used to help manage changes on flapping links. In this case, R2 interface Loopback 0 is known to D1 and D2 via OSPF, so the delay needs to take OSPF timers into account. The command is setting the SLA up so that it will wait a period of time after the first failed SLA to make sure it is actually down, and it will wait a period of time after it appears to be returned to operation to be sure it is actually operating.

```
D1(config-track)# delay down 45 up 20
D1(config-track)# exit
```

c. Configure track 6 to pay attention to IP SLA 6 with the same delay values.

```
D1(config)# track 6 ip sla 6
D1(config-track)# delay down 45 up 20
```

```
D1(config-track)# exit
```

d. Now that the IP SLAs are being tracked, we must associate the status of the track with the HSRP group. This is done on the VLAN interface using the **standby [group] track [track number]** command. As a part of that command, add a decrement value, which will drop the interface's HSRP priority should the IP SLA fail.

```
D1(config)# interface vlan 2
D1(config-if)# standby 2 track 4 decrement 60
D1(config-if)# standby 26 track 4 decrement 60
D1(config-if)# exit
D1(config)# interface vlan 3
D1(config-if)# standby 3 track 4 decrement 60
D1(config-if)# standby 36 track 4 decrement 60
D1(config-if)# exit
```

e. Repeat the same commands on D2 so that HSRP is tracking IP SLAs there as well.

```
D2(config)# track 4 ip sla 4
D2(config-track)# delay down 45 up 20
D2(config-track)# exit
D2(config)# track 6 ip sla 6
D2(config-track)# delay down 45 up 20
D2(config-track)# exit
D2(config)# interface vlan 2
D2(config-if)# standby 2 track 4 decrement 60
D2(config-if)# standby 26 track 4 decrement 60
D2(config-if)# exit
D2(config)# interface vlan 3
D2(config-if)# standby 3 track 4 decrement 60
D2(config-if)# standby 36 track 4 decrement 60
D2(config-if)# exit
```

Step 3: Observe and validate HSRPv2 operation with IP SLAs.

a. On PC1, start a continuous ping to 192.168.1.1.

b. On R1, shutdown interface G0/0/0.

c. After about 45 seconds, you should see that HSRP fails over for VLAN 2 from switch D1 to switch D2, and pings from PC1 work again.

d. Issue the **no shutdown** command on R1 interface G0/0/0.

e. Switch D1 takes over again as the Active Virtual Router for VLAN 2, and the host is still able to ping 192.168.1.1.

f. Stop the continuous ping running on PC1.

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.