Diplomado de Profundización CISCO CCNP
Paso 7 - 4to Trabajo Colaborativo

Presentado por:
PABLO FELIPE REYES - 1061784581
ALVARO ELIU MELO - 93409341
MARILIN VELASCO VELEZ - 1061541075

Presentado a:
GERARDO GRANADOS ACUÑA
Grupo colaborativo:
208014-1

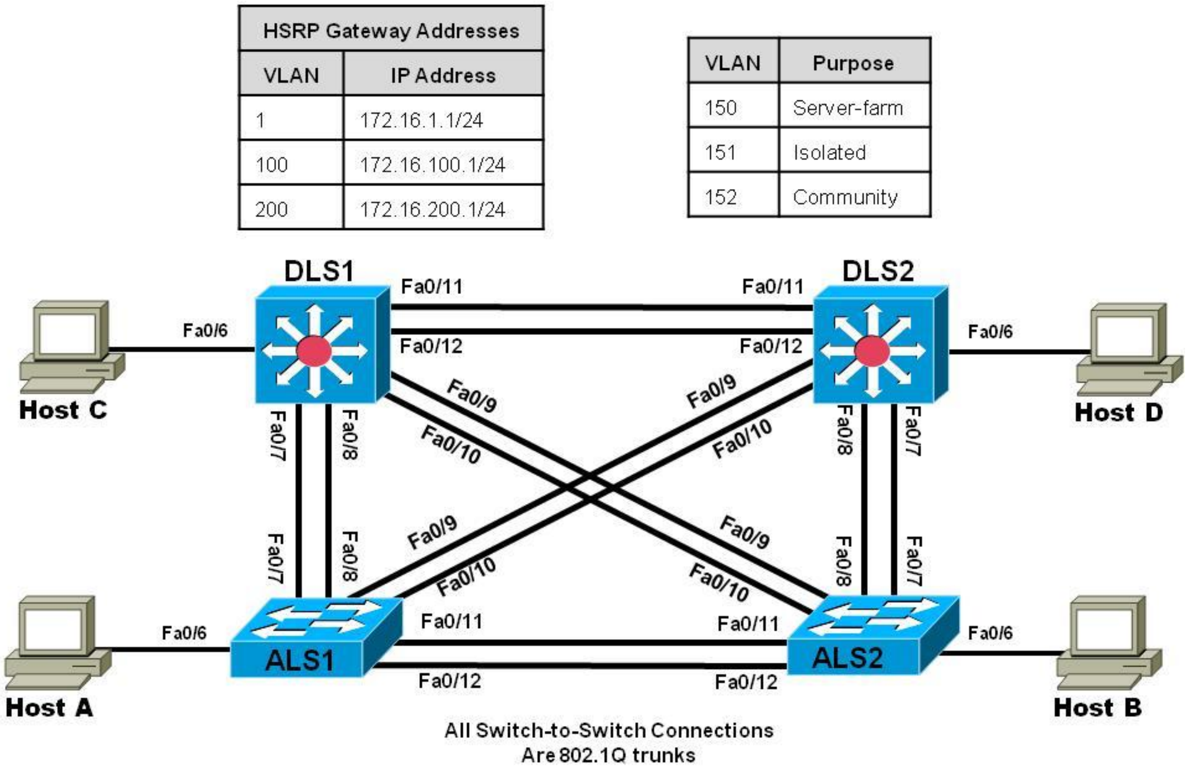
Universidad Nacional Abierta y a Distancia

Noviembre 2017

CCNPv7.1 SWITCH

Chapter 10 Lab 10-2, Securing VLANs

Topology



HSRP Gateway Addresses	
VLAN	IP Address
1	172.16.1.1/24
100	172.16.100.1/24
200	172.16.200.1/24

VLAN	Purpose
150	Server-farm
151	Isolated
152	Community

All Switch-to-Switch Connections
Are 802.1Q trunks

Prepare the switches for the lab

The instructions in this lab assume that the switches are running using the final configuration from Lab 10-1 "Securing Layer 2 Switches".

Part 1: Configure private VLANs.

Private VLANs are an option when you have multiple devices in the same broadcast domain, but need to prevent them from communicating from each other. A good example is in a server farm where the servers do not need to receive other server's broadcast traffic.

In a sense, private VLANs allow you to sub-divide the layer 2 broadcast domain. You are able to associate a primary VLAN with multiple secondary VLANs, while using the same IP address space for all of the devices.

Secondary VLANs are defined as one of two types; either COMMUNITY or ISOLATED. A secondary community VLAN allows the hosts within the VLAN to communicate with one another and the primary VLAN. A secondary isolated VLAN does not allow hosts to communicate with others in the same isolated VLAN. They can only communicate with the primary VLAN.

A primary VLAN can have multiple secondary community VLANs associated with it, but only one secondary isolated VLAN.

Step 1: Configure VTP

VTP version 2 does not support PVLANs, so any switches that must host a PVLAN port have to be in transparent mode and the PVLANs have to be manually configured. VTP version 3 does support PVLANs, so the configuration only has to be done in one place.

a. Convert all switches to VTP version 3, and configure a VTP password of cisco123. Configure all four switches. An example of DLS1 configuration follows:

```
DLS1(config)# vtp version 3
Aug  4 12:39:11.944: %SW_VLAN-6-OLD_CONFIG_FILE_READ: Old version 2 VLAN
configuration file detected and read OK.  Version 3
    files will be written in the future.
DLS1(config)# vtp password cisco123
Setting device VTP password to cisco123
DLS1(config)# exit
```

b. Configure DLS1 to be the primary switch for VLANs.

```
DLS1# vtp primary vlan
This system is becoming primary server for feature vlan
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
DLS1#
Aug  4 12:40:44.680: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: e840.406f.7280 has
become the primary server for the VLAN VTP feature
DLS1#
```

Step 2: Configure the Primary Private VLAN

a. Based on the topology diagram, VLAN 150 will be used as the VLAN for the new server farm. On VTP server DLS1, add VLAN 150, name the VLAN **server-farm** and exit vlan config mode. This allows VLAN 150 to be propagated to the other switches in the network. In addition, configure DLS1 as the root bridge for VLANs 150, 151, and 152.

```
DLS1(config)# vlan 150
DLS1(config-vlan)# name SERVER-FARM
DLS1(config-vlan)# exit
DLS1(config)# spanning-tree vlan 150-152 root primary
```

b. Once this is complete, verify that VLAN 150 is preset in the database on DLS2.

Step 2: Configure interface VLAN 150 at DLS1 and DLS2:

```
DLS1(config)# interface vlan 150
DLS1(config-if)# ip address 172.16.150.1 255.255.255.0

DLS2(config)# interface vlan 150
DLS2(config-if)# ip add 172.16.150.2 255.255.255.0
```

Step 3: Create the PVLANs on the VTP server

a. Configure the new PVLANs on DLS1. Secondary PVLAN 151 is an isolated VLAN, while secondary PVLAN 152 is used as a community PVLAN. Configure these new PVLANs and associate them with primary VLAN 150.

```
DLS1(config)# vlan 151
DLS1(config-vlan)# private-vlan isolated
```

```
DLS1(config-vlan)# exit
DLS1(config)# vlan 152
DLS1(config-vlan)# private-vlan community
DLS1(config-vlan)# exit
DLS1(config)# vlan 150
DLS1(config-vlan)# private-vlan primary
DLS1(config-vlan)# private-vlan association 151,152
DLS1(config-vlan)# exit
DLS1(config)#
```

b. Verify the PVLANs propagate to the other switches.

```
DLS2# show vlan brief  | include active
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
99   Management                       active
100  STAFF                            active
150  SERVER-FARM                      active
151  VLAN0151                         active
152  VLAN0152                         active
200  STUDENTS                         active
666  NATIVE_DO_NOT_USE                active
```

c. Verify the creation of the secondary PVLANs and their association with the primary VLAN using the **show vlan private-vlan** command. Note that no ports are currently associated with these VLANs. This is expected behavior.

```
DLS1#show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------
-
150     151       isolated
150     152       community

DLS2# show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------
150     151       isolated
150     152       community
```

Step 4: Configure support for routing of PVLANs

The **private-vlan mapping** interface configuration command permits PVLAN traffic to be switched through Layer 3. Normally you would include all the secondary VLANs to allow for HSRP to work, but for this example we will not include a mapping VLAN 151 on DLS2 so we can demonstrate the isolation of VLAN 151. Configure these commands for interface VLAN 150 on DLS1 and DLS2.

```
DLS1(config)# interface vlan 150
DLS1(config-if)# private-vlan mapping 151-152
DLS1(config-if)# end

DLS2(config)# interface vlan 150
```

```
DLS2(config-if)# private-vlan mapping 152
DLS2(config-if)# end
```

Will hosts assigned to ports on private VLAN 151 be able to communicate directly with each other?

No, En una VLAN aislada todos los puertos pueden comunicarse solo con puertos de la VLAN primaria

Step 5: Configure host access to PVLANs

a. On DLS1, configure interface FastEthernet 0/6 so it is in private-vlan host mode and has association to VLAN 150:

```
DLS1(config)# interface fastethernet 0/6
DLS1(config-if)# switchport mode private-vlan host
DLS1(config-if)# switchport private-vlan host-association 150 152
DLS1(config-if)# exit
```

b. Use the **show vlan private-vlan** command and note that the ports configured are currently associated with these VLANs.

```
DLS1#show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- -----------------------------------------
-
150     151       isolated
150     152       community         Fa0/6
```

c. On DLS2, configure the Fast Ethernet ports that are associated with the server farm private VLANs. Fast Ethernet port 0/6 is used for the secondary isolated PVLAN 151, and ports 0/18–0/20 are used for the secondary community VLAN 152. The **switchport mode private-vlan host command sets the mode on the interface and the switchport private-vlan host-association** *primary-vlan-id secondary-vlan-id* command assigns the appropriate VLANs to the interface. The following commands configure the PVLANs on DLS2.

```
DLS2(config)# interface fastethernet 0/6
DLS2(config-if)# switchport mode private-vlan host
DLS2(config-if)# switchport private-vlan host-association 150 151
DLS2(config-if)# exit
DLS2(config)# interface range fa0/18 - 20
DLS2(config-if-range)# switchport mode private-vlan host
DLS2(config-if-range)# switchport private-vlan host-association 150 152
```

As servers are added to Fast Ethernet 0/18–20, will these servers be allowed to hear broadcasts from each other? Explain.

Si, porque los servidores estarán en la misma VLAN

d. Use the **show vlan private-vlan** command and note that the ports configured are currently associated with these VLANs.

```
DLS2# show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- -----------------------------------------
150     151       isolated          Fa0/6
150     152       community         Fa0/18, Fa0/19, Fa0/20
```

e. Configure HOST C on DLS1 interface f0/6 with the IP address 172.16.150.50/24. Use 172.16.150.1 as the default gateway address.

f. Configure HOST D on DLS2 interface f0/6 with the IP address 172.16.150.150/24. Use 172.16.150.1 as the default gateway address.

Step 6: Verify PVLANs are working

a. From HOST C, try to ping the following addresses - they should all work: 172.16.150.1 (DLS1), 172.16.150.2 (DLS2), 172.16.99.5 (ALS1).

b. From HOST C, try to ping HOST D (172.16.150.150). This should NOT work.

c. From HOST D, try to ping the following addresses - they should all work: 172.16.150.1 (DLS1), 172.16.99.5 (ALS1).

d. From HOST D, try to ping 172.16.150.2 (DLS2). This should NOT work.

Part 3: RACLs.

You can use router access control lists (RACLs) to separate the student and staff VLANs. In this lab scenario, write an ACL that allows the staff VLAN (100) to access the student VLAN (200), and deny student VLAN access to the staff VLAN.

Step 1: Write an extended IP access list

Write an ACL that meets the requirement and assign the access list to the appropriate VLAN interfaces on DLS1 and DLS2 using the **ip access-group** *acl-num* {**in** | **out**} command.

```
DLS1(config)# access-list 100 permit tcp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255
established
DLS1(config)# access-list 100 permit icmp 172.16.200.0 0.0.0.255 172.16.100.0
0.0.0.255 echo-reply
DLS1(config)# access-list 100 deny ip 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255
DLS1(config)# access-list 100 permit ip any any
DLS1(config)# interface vlan 200
DLS1(config-if)# ip access-group 100 in
DLS1(config-if)# exit

DLS2(config)# access-list 100 permit tcp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255
established
DLS2(config)# access-list 100 permit icmp 172.16.200.0 0.0.0.255 172.16.100.0
0.0.0.255 echo-reply
DLS2(config)# access-list 100 deny ip 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255
DLS2(config)# access-list 100 permit ip any any
DLS2(config)# interface vlan 200
DLS2(config-if)# ip access-group 100 in
DLS2(config-if)# exit
```

e. Check the configuration using the **show ip access-list** and **show ip interface vlan *vlan-id*** commands.

```
DLS1# show access-lists
Extended IP access list 100
    10 permit tcp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 established
    20 permit icmp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 echo-reply
    30 deny ip 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255
    40 permit ip any any

DLS1# show ip interface vlan 100
Vlan100 is up, line protocol is up
  Internet address is 172.16.100.3/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.2
  Outgoing access list is not set
  Inbound  access list is 100
  <output omitted>
```

f. After the access list has been applied verify the configuration in one of the following ways. Option 1 using real hosts is preferred.

Option 1:

Lab 10-1 finished with ALS1 F0/6 assigned to VLAN 200. Change this assignment to VLAN 100. Host A should be connected to ALS1 F0/6 and assigned the IP address 172.16.100.50/24 with default gateway 172.16.100.1 from Lab 10-1. If not, set Host A up with those parameters.

Host B should be connected to ALS2 F0/6 from Lab 10-1 as well, but its last configuration in that lab was to use DHCP, so assign a static IP address   Connect host PC-B to ALS2 port Fa0/6 in student VLAN 200 and assign it IP address 172.16.200.50/24 with default gateway 172.16.200.1.

Ping the staff host from the student host. This ping should fail. Then ping the student host from the staff host. This ping should succeed.

Option 2: On ALS1 set up a simulated host in VLAN 100 and one in VLAN 200 by creating a VLAN 100 and 200 interface on the switch. Give the VLAN 100 interface an IP address in VLAN 100. Give the VLAN 200 interface an IP address in VLAN 200. The following is a sample configuration on ALS1.

```
ALS1(config)# int vlan 100
ALS1(config-if)# ip address 172.16.100.100 255.255.255.0

ALS1(config)# int vlan 200
ALS1(config-if)# ip address 172.16.200.200 255.255.255.0
```

Ping the interface of the gateway for the staff VLAN (172.16.100.1) with a source of staff VLAN 100 (172.16.100.100) and then ping with a source of student VLAN 200. The pings from the student VLAN should fail.

```
ALS1# ping 172.16.100.1 source vl100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.100.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.100.100
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/205/1007 ms

ALS1# ping 172.16.100.1 source vl200
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.100.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.200.200
.U.U.
Success rate is 0 percent (0/5)
```

What does a U signify in the output of the **ping** command?

El símbolo U significa inalcanzable, es decir cuando el ping se estaba enrutando existe un router que desconoce la ruta destino.

Part 4: Configure VACLs.

Configure the network so that the temporary staff host cannot access the rest of the staff VLAN, yet still be able to use the default gateway of the staff subnet to connect to the rest of the network and the ISP. You can accomplish this task by using a VLAN ACL (VACL).

For this scenario, Host C (DLS1 Fast Ethernet 0/6) will act as a temporary staff PC, therefore the VACL must be placed on DLS1.

Step 1: Configure DLS1 F0/6 and Host C

a. Change the configuration of DLS1 F0/6 so that the interface is associated with VLAN 100. To keep things tidy, also remove the private vlan mapping on the interface as well:

```
DLS1(config)#interface f0/6
DLS1(config-if)#switchport mode access
DLS1(config-if)#switchport access vlan 100
DLS1(config-if)#no switchport private-vlan host-association 150 152
DLS1(config-if)#exit
```

b. Change the configuration of HOST C so that it is using the IP address 172.16.100.150/24 with the default gateway set as 172.16.100.1

Step 2: Configure and apply the VACL

a. Configure an access list on DLS1 called temp-host using the **ip access-list extended** *name* command. This list defines the traffic between the host and the rest of the network. Then define the traffic using the **permit ip host** *ip-address subnet wildcard-mask* command. Note that you must be explicit about what traffic to match -- this isn't a traffic *filtering* ACL, it is a traffic *matching* ACL. If you were to leave the second line of the example below out, pings would work.

```
DLS1(config)# ip access-list extended temp-host
DLS1(config-ext-nacl)# permit ip host 172.16.100.150 172.16.100.0 0.0.0.255
DLS1(config-ext-nacl)# permit icmp host 172.16.100.150 172.16.100.0 0.0.0.255
DLS1(config-ext-nacl)# exit
```

b. The VACL is defined using a VLAN access map. Access maps are evaluated in a numbered sequence. To set up an access map, use the **vlan access-map** *map-name seq#* command. The following configuration defines an access map named block-temp, which uses the **match** statement to match the traffic defined in the access list and denies that traffic. You also need to add a line to the access map that allows all other traffic. If this line is not added, an implicit deny catches all other traffic and denies it.

```
DLS1(config)# vlan access-map block-temp 10
DLS1(config-access-map)# match ip address temp-host
DLS1(config-access-map)# action drop
DLS1(config-access-map)# vlan access-map block-temp 20
```

```
DLS1(config-access-map)# action forward
DLS1(config-access-map)# exit
```

c. Define which VLANs the access map should be applied to using the **vlan filter** *map-name* **vlan-list** *vlan-ID* command.

```
DLS1(config)# vlan filter block-temp vlan-list 100
```

d. Verify the VACL configuration using the **show vlan access-map** command on DLS1.

```
DLS1# show vlan access-map

Vlan access-map "block-temp"  10
  Match clauses:
    ip  address: temp-host
  Action:
    drop
Vlan access-map "block-temp"  20
  Match clauses:
  Action:
    forward
```

Step 3: Test the VACL

a. From HOST C, try to ping to HOST A on ALS1 (172.16.100.50). The ping should fail.

b. From HOST C, try to ping the default gateway (172.16.100.1). The ping should fail.

c. From HOST C, try to ping Host D (172.16.200.50). The ping should succeed.

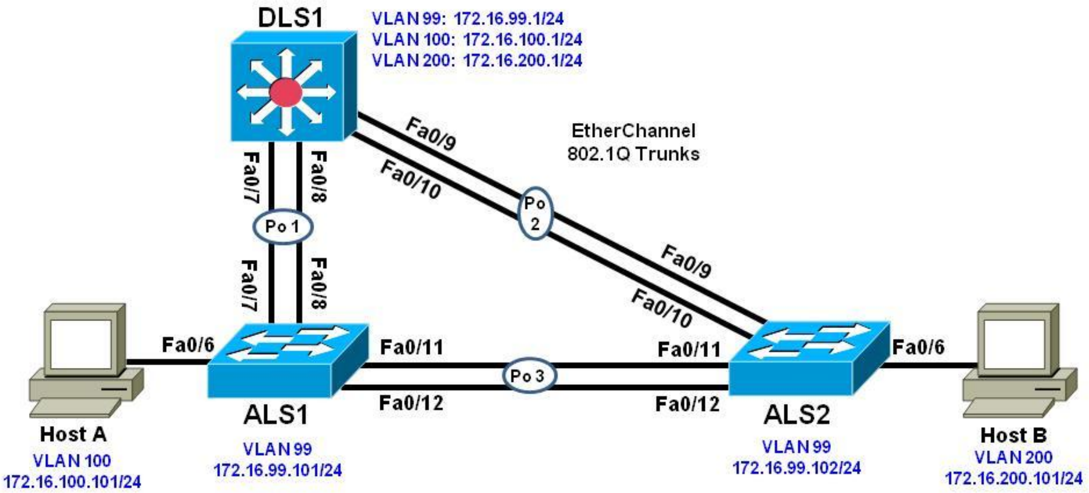
Step 4: End of Lab

Do not save your configurations. The equipment will be reset for the next lab.

CCNPv7.1 SWITCH

Chapter 8 Lab 8-1, IP Service Level Agreements and Remote SPAN in a Campus Environment.

Topology



Part 5: Prepare for the Lab

Step 1: Prepare the switches for the lab

Use the **reset.tcl** script you created in Lab 1 “Preparing the Switch” to set your switches up for this lab. Then load the file BASE.CFG into the running-config with the command **copy flash:BASE.CFG running-config**. An example from DLS1:

```
DLS1# tclsh reset.tcl
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Reloading the switch in 1 minute, type reload cancel to halt

Proceed with reload? [confirm]

*Mar  7 18:41:40.403: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
*Mar  7 18:41:41.141: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload command.
<switch reloads - output omitted>

Would you like to enter the initial configuration dialog? [yes/no]: n
Switch> en
```

```
*Mar  1 00:01:30.915: %LINK-5-CHANGED: Interface Vlan1, changed state to
administratively down
Switch# copy BASE.CFG running-config
Destination filename [running-config]?
184 bytes copied in 0.310 secs (594 bytes/sec)
DLS1#
```

Step 2:   Configure basic switch parameters.

Configure an IP address on the management VLAN according to the diagram. VLAN 1 is the default management VLAN, but following best practice, we will use a different VLAN. In this case, VLAN 99.

Enter basic configuration commands on each switch according to the diagram.

DLS1 example:

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# interface vlan 99
DLS1(config-if)# ip address 172.16.99.1 255.255.255.0
DLS1(config-if)# no shutdown
```

The interface VLAN 99 will not come up immediately, because the broadcast domain it is associated with (VLAN 99) doesn't exist on the switch. We will fix that in a few moments.

(Optional) On each switch, create an enable secret password and configure the VTY lines to allow remote access from other network devices.

DLS1 example:

```
DLS1(config)# enable secret class
DLS1(config)# line vty 0 15
DLS1(config-line)# password cisco
DLS1(config-line)# login
```

Note: The passwords configured here are required for NETLAB compatibility only and are NOT recommended for use in a live environment.

Note(2): For purely lab environment purposes, it is possible to configure the VTY lines so that they accept any Telnet connection immediately, without asking for a password, and place the user into the privileged EXEC mode directly. The configuration would be similar to the following example for DLS1:

```
DLS1(config)# enable secret class
DLS1(config)# line vty 0 15
DLS1(config-line)# no login
DLS1(config-line)# privilege level 15
```

Note: The %PKI-6-AUTOSAVE message tells you that your BASE.CFG has been saved as the startup-config, so a simple reload will revert the switch back to BASE configuration

a. Configure default gateways on ALS1 and ALS2. These are access layer switches operating as Layer 2 devices and need a default gateway to send traffic from their management interface to other networks. Configure both ALS1 and ALS2. An example from ALS1 is shown:

```
ALS1(config)# ip default-gateway 172.16.99.1
```

Step 3: Configure host PCs.

Configure PCs Host A and Host B with the IP address and subnet mask shown in the topology. Host A is in VLAN 100 with a default gateway of 172.16.100.1. Host B is in VLAN 200 with a default gateway of 172.16.200.1.

Step 4: Configure trunks and EtherChannels between switches.

Configure trunking according to the diagram. LACP is used for EtherChannel negotiation for these trunks. Examples from DLS1 and ALS1 are shown. Configure all the switches with the channel groups shown in the topology:

Configure the trunks and EtherChannel from DLS1 to ALS1 and ALS2.

```
DLS1(config)# vlan 666
DLS1(config-vlan)# name NATIVE_DO_NOT_USE
DLS1(config-vlan)# exit
DLS1(config)# int ran f0/7-10
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport trunk native vlan 666
DLS1(config-if-range)# switchport nonegotiate
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# exit
DLS1(config)# int ran f0/7-8
DLS1(config-if-range)# channel-group 1 mode active
DLS1(config-if-range)# description EtherChannel to ALS1
DLS1(config-if-range)# no shut
DLS1(config-if-range)# exit
DLS1(config)# int ran f0/9-10
DLS1(config-if-range)# channel-group 2 mode active
DLS1(config-if-range)# description EtherChannel to ALS2
DLS1(config-if-range)# no shut
DLS1(config-if-range)# exit
```

Configure the trunks and EtherChannel between ALS1 and ALS2.

```
ALS1(config)# interface range fastEthernet 0/11 - 12
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# channel-group 3 mode active
ALS1(config-if-range)# no shut
```

Step 5: Configure VTP on ALS1 and ALS2.

Change the VTP mode of ALS1 and ALS2 to client.

```
ALS1(config)# vtp mode client
Setting device to VTP CLIENT mode.

ALS2(config)# vtp mode client
Setting device to VTP CLIENT mode.
```

Step 6: Configure VTP on DLS1.

Create the VTP domain on DLS1, and create VLANs 100 and 200 for the domain.

```
DLS1(config)# vtp domain SWPOD
DLS1(config)# vtp version 2

DLS1(config)# vlan 99
```

```
DLS1(config-vlan)# name Management
DLS1(config-vlan)# vlan 100
DLS1(config-vlan)# name Finance
DLS1(config-vlan)# vlan 200
DLS1(config-vlan)# name Engineering
DLS1(config-vlan)# exit
DLS1(config)#
```

Step 7: Configure access ports.

Configure the host ports for the appropriate VLANs according to the diagram.

```
ALS1(config)# interface fastEthernet 0/6
ALS1(config-if)# switchport mode access
ALS1(config-if)# switchport access vlan 100
ALS1(config-if)# no shut

ALS2(config)# interface fastEthernet 0/6
ALS2(config-if)# switchport mode access
ALS2(config-if)# switchport access vlan 200
ALS1(config-if)# no shut
```

Step 8: Configure VLAN interfaces and enable routing.

On DLS1, create the SVIs for VLANs 100 and 200. Note that the corresponding Layer 2 VLANs must be configured for the Layer 3 SVIs to activate. This was done in Step 6.

```
DLS1(config)# interface vlan 100
DLS1(config-if)# ip address 172.16.100.1 255.255.255.0
DLS1(config-if)# interface vlan 200
DLS1(config-if)# ip address 172.16.200.1 255.255.255.0
```

The **ip routing** command is also needed to allow the DLS1 switch to act as a Layer 3 device to route between these VLANs. Because the VLANs are all considered directly connected, a routing protocol is not needed at this time. The default configuration on 3560 switches is **no ip routing**.

```
DLS1(config)# ip routing
```

Verify the configuration using the **show ip route** command on DLS1.

```
DLS1# show ip route | begin Gateway
Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C        172.16.99.0/24 is directly connected, Vlan99
L        172.16.99.1/32 is directly connected, Vlan99
C        172.16.100.0/24 is directly connected, Vlan100
L        172.16.100.1/32 is directly connected, Vlan100
C        172.16.200.0/24 is directly connected, Vlan200
L        172.16.200.1/32 is directly connected, Vlan200
DLS1#
```

Run the following Tcl script on DLS1 to verify full connectivity. If these pings are not successful, troubleshoot.

```
DLS1# tclsh

foreach address {
172.16.99.1
172.16.99.101
172.16.99.102
172.16.100.1
172.16.200.1
172.16.100.101
172.16.200.101
} {
ping $address }
```

Part 6: Configure Cisco IOS IP SLA

Step 1: Configure Cisco IOS IP SLA responders.

IP SLA responders are Cisco IOS devices that support the IP SLA control protocol. An IP SLA responder uses the Cisco IOS IP SLA Control Protocol for notification configuration and on which port to listen and respond. Some operations, such as ICMP echo, do not require a dedicated IP SLA responder.

Use the **ip sla responder** command on ALS1 and ALS2 to enable sending and receiving IP SLAs control packets.

Note: This command replaces the ip sla monitor responder command. All commands that used to begin with “ip sla monitor” now begin with “ip sla” (without “monitor”). Configure this on both ALS1 and ALS2. An example from ALS1:

```
ALS1(config)# ip sla responder
```

Configure ALS1 and ALS2 as IP SLA responders for UDP jitter using the **ip sla responder udp-echo ipaddress** command. Specify the IP address of DLS1 VLAN 1 to act as the destination IP address for the reflected UDP traffic on both ALS1 and ALS2. Configure this on both ALS1 and ALS2. An example from ALS1:

```
ALS1(config)# ip sla responder udp-echo ipaddress 172.16.99.1 port 5000
```

Step 2: Configure the Cisco IOS IP SLA source to measure network performance.

IP SLA uses generated traffic to measure network performance between two networking devices.

On DLS1, create an IP SLA operation and enter IP SLA configuration mode with the **ip sla** *operation-number* command.

```
DLS1(config)# ip sla 1
DLS1(config-ip-sla)#
```

Configure an IP SLA ICMP echo operation using the icmp-echo command in IP SLA configuration mode. The IP SLA ICMP echo operation does not require a dedicated Cisco IOS IP SLA responder (the destination device can be a non-Cisco device, such as a PC). By default, the ICMP operation repeats every 60 seconds. On DLS1, for ICMP echo operation 1, specify the IP address of Host A as the target. For ICMP echo operation 2, specify the IP address of Host B as the target.

```
DLS1(config-ip-sla)# icmp-echo 172.16.100.101
DLS1(config-ip-sla-echo)# exit

DLS1(config)# ip sla 2
DLS1(config-ip-sla)# icmp-echo 172.16.200.101
DLS1(config-ip-sla-echo)# exit
```

Jitter means inter-packet delay variance. UDP-based voice traffic associated with IP phone and PC softphone applications at the access layer require strict adherence to delay and jitter thresholds. To configure an IP SLA UDP jitter operation, use the udp-jitter command in IP SLA configuration mode. By default, the UDP jitter operation repeats every 60 seconds. For UDP jitter operation 3, specify the destination IP address of the ALS1 VLAN 99 interface as the target. For operation 4, specify the destination IP address of the ALS2 VLAN 99 interface as the target. The IP SLA communication port is 5000 for both operations.

```
DLS1(config)# ip sla 3
DLS1(config-ip-sla)# udp-jitter 172.16.99.101 5000
DLS1(config-ip-sla-jitter)# exit

DLS1(config)# ip sla 4
DLS1(config-ip-sla)# udp-jitter 172.16.99.102 5000
DLS1(config-ip-sla-jitter)# exit
```

Schedule the IP SLAs operations to run indefinitely beginning immediately using the ip sla schedule global configuration mode command.

```
DLS1(config)# ip sla schedule 1 life forever start-time now
DLS1(config)# ip sla schedule 2 life forever start-time now
DLS1(config)# ip sla schedule 3 life forever start-time now
DLS1(config)# ip sla schedule 4 life forever start-time now
```

Step 3: Monitor IP SLAs operations.

View the IP SLA configuration for IP SLA 1 on DLS1. The output for IP SLA 2 is similar.

```
DLS1# show ip sla configuration 1
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 172.16.100.101/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 60  (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
```

What type of operation is being performed with IP SLA 1?

ICMP echo request

View the IP SLA configuration for IP SLA 3 on DLS1. The output for IP SLA 4 is similar.

```
DLS1# show ip sla configuration 3
```

```
IP SLAs Infrastructure Engine-III
Entry number: 2
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 172.16.200.101/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 60  (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
```

What type of operation is being performed with IP SLA 3?

UDP jitter

Display global information about Cisco IOS IP SLAs on DLS1.

```
DLS1# show ip sla application

IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, video, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 9359471
Estimated system max number of entries: 6855

Estimated number of configurable operations: 6817
Number of Entries configured  : 4
Number of active Entries      : 4
Number of pending Entries     : 0
Number of inactive Entries    : 0
```

```
Time of last change in whole IP SLAs: 13:54:00.025 CDT Fri Jul 31 2015
```

Display information about Cisco IOS IP SLA responders on ALS1. The ALS2 output is similar.

```
ALS1# show ip sla responder
General IP SLA Responder on Control port 1967
General IP SLA Responder is: Enabled
Number of control message received: 26 Number of errors: 0
Recent sources:
        172.16.99.1 [14:17:28.775 CDT Fri Jul 31 2015]
        172.16.99.1 [14:16:28.780 CDT Fri Jul 31 2015]
        172.16.99.1 [14:15:28.776 CDT Fri Jul 31 2015]
        172.16.99.1 [14:14:28.781 CDT Fri Jul 31 2015]
        172.16.99.1 [14:13:28.777 CDT Fri Jul 31 2015]
Recent error sources:

        Permanent Port IP SLA Responder
Permanent Port IP SLA Responder is: Enabled

udpEcho Responder:
  IP Address            Port
  172.16.99.1           5000
```

Display IP SLA statistics on DLS1 for IP SLA 1. The IP SLA 2 output is similar.

```
DLS1# show ip sla statistics 1

IPSLAs Latest Operation Statistics

IPSLA operation id: 1
        Latest RTT: 1 milliseconds
Latest operation start time: 14:17:00 CDT Fri Jul 31 2015
Latest operation return code: OK
Number of successes: 26
Number of failures: 0
Operation time to live: Forever
```

From this output, you can see that the latest round-trip time (RTT) for SLA operation Index 1 (icmp-echo) is 1 millisecond (ms). The number of packets sent successfully from DLS1 to PC Host A was 26, and there were no failures.

Display IP SLA statistics on DLS1 for IP SLA 3. The IP SLA 4 output is similar.

```
DLS1# show ip sla statistics 3

IPSLAs Latest Operation Statistics

IPSLA operation id: 3
Type of operation: udp-jitter
        Latest RTT: 3 milliseconds
Latest operation start time: 14:18:01 CDT Fri Jul 31 2015
Latest operation return code: OK
RTT Values:
        Number Of RTT: 10               RTT Min/Avg/Max: 3/3/5 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 0
        Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 9
        Number of DS Jitter Samples: 9
        Source to Destination Jitter Min/Avg/Max: 0/1/1 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/1/1 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 27
Number of failures: 0
Operation time to live: Forever
```

From this output, you can see that the latest RTT for SLA operation Index 3 (udp-jitter) is 3 ms. Jitter time from source to destination and from destination to source is averaging 1 ms, which is acceptable for voice applications. The number of packets sent successfully from DLS1 to ALS1 was 27, and there were no failures.

Disable interface VLAN 99 on ALS1 using the **shutdown** command.

```
ALS1(config)# interface vlan 99
ALS1(config-if)# shutdown
```

Allow a few minutes to pass and then issue the **show ip sla statistics 3** command on DLS1. The output should look similar to the following.

```
DLS1# show ip sla statistics 3

IPSLAs Latest Operation Statistics

IPSLA operation id: 3
Type of operation: udp-jitter
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 14:22:01 CDT Fri Jul 31 2015
Latest operation return code: No connection
RTT Values:
        Number Of RTT: 0                RTT Min/Avg/Max: 0/0/0 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 0
        Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 0
        Number of DS Jitter Samples: 0
        Source to Destination Jitter Min/Avg/Max: 0/0/0 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/0/0 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
```

```
                Source to Destination Inter Loss Period Length Min/Max: 0/0
                Loss Destination to Source: 0
                Destination to Source Loss Periods Number: 0
                Destination to Source Loss Period Length Min/Max: 0/0
                Destination to Source Inter Loss Period Length Min/Max: 0/0
                Out Of Sequence: 0      Tail Drop: 0
                Packet Late Arrival: 0  Packet Skipped: 0
        Voice Score Values:
                Calculated Planning Impairment Factor (ICPIF): 0
                Mean Opinion Score (MOS): 0
        Number of successes: 29
        Number of failures: 2
        Operation time to live: Forever
```

If there is a connectivity problem between IP SLA source DLS1 and responder ALS1 or ALS2, the communication to the responder will be lost and statistics will cease to be collected, except for the number of failed tests.

Note: 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.

Re-enable ALS1's interface vlan 99 before continuing.

Part 7: Switch Port Analyzer (SPAN) Feature

SPAN is tool that allows for monitoring and troubleshooting a network. There are different variations of the SPAN tool. There is local SPAN, Remote Span, and VLAN span. Local Span allows an administrator to monitor traffic from a source and have it sent to a destination port on the same switch running a protocol analyzer on the same switch. The source and destination port used to create the monitor session must be on the same switch. Remote SPAN allows the source and destination ports to be on different switches. In order for this to work, it uses a vlan configured only for remote span functionality. The source port then places the transmitted or received data onto the remote span vlan. The remote span vlan is carried across trunks. The receiving switch takes the data sourced from the remote vlan and sends it to the destination port running the protocol analyzer.

In this lab, we will demonstrate the use of remote SPAN (RSPAN). VLAN 300 will be created and used as the remote span VLAN. We will set up a monitoring session for the host connected to port fa0/6 on switch ALS1. Ultimately, the destination port will be the host connected to fa0/6 of ALS2. The ALS2 host is collect the transmit and receive data using Wireshark.

Step 1: Configure Remote SPAN (RSPAN).

Create the RSPAN VLAN on DLS1 using the VLAN 300 command from global configuration mode.

```
DLS1(config)# vlan 300
DLS1(config-vlan)# name REMOTE_SPAN
DLS1(config-vlan)# remote-span
```

Use the **show vlan remote-span** command to verify the vlan 300 is configured correctly and is designated as the remote-span vlan. Ensure that the VLAN propagates across the VTP Domain with show vlan brief command. Use the **show interface trunk** command to ensure the RSPAN VLAN is allowed on the trunks. The RSPAN VLAN should not be a DATA VLAN. Its purpose is strictly for carrying the monitored traffic across trunk links from one switch to another.

Verify the output on DLS1.

```
DLS1# show vlan brief | include active
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
99   Management                       active
100  Finance                          active
200  Engineering                      active
300  REMOTE_SPAN                      active
666  NATIVE_DO_NOT_USE                active
DLS1#
```

Verify the output on ALS1.

```
ALS1# show vlan brief | include active
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
99   Management                       active
100  Finance                          active    Fa0/6
200  Engineering                      active
300  REMOTE_SPAN                      active
666  NATIVE_DO_NOT_USE                active
ALS1#
```

Now configure the monitor session on ALS1 with a source interface of fa0/6 and a destination of remote vlan 300. Because the captured traffic must traverse the local switch to a remote switch, we must use the remote VLAN as the destination.

```
ALS1(config)# monitor session 1 source interface Fa0/6
ALS1(config)# monitor session 1 destination remote vlan 300
```

Verify the configuration using the **show monitor** command.

```
ALS1# show monitor
Session 1
---------
Type                   : Remote Source Session
Source Ports           :
    Both               : Fa0/6
Dest RSPAN VLAN        : 300
```

Move to the ALS2 switch and configure it to collect the desired traffic. The source port on ALS2 will be the remote span vlan 300 and the destination port will be the Engineering client connected to port fa0/6.

It is important to note that the PC-B host should be running a protocol analyzer to view the contents of the captured traffic and perform traffic analysis. Both transmit and receive traffic of the source port will be captured. The configuration can be modified to only capture transmit or receive traffic if necessary.

Configure ALS2 for the remote span session.

```
ALS2(config)# monitor session 10 source remote vlan 300
ALS2(config)# monitor session 10 destination interface Fa0/6
```

Our configuration shows the use of a different session number than the one used on ALS1. The session numbers do not have to match from device to device.

Verify the configuration using the show monitor command. The source port should show VLAN 300 and the destination port should be interface fa0/6.

```
ALS2# show monitor
Session 10
----------
Type                   : Remote Destination Session
Source RSPAN VLAN      : 300
Destination Ports      : Fa0/6
    Encapsulation      : Native
          Ingress      : Disabled
```

Use the **show interfaces fa0/6** to command to view the status of the interface. Notice from the output the line protocol is down. When a port is used as a destination in monitoring session, it cannot be used to transmit and receive regular network traffic.

```
ALS2# show interface f0/6
FastEthernet0/6 is up, line protocol is down (monitoring)
  Hardware is Fast Ethernet, address is 5017.ff84.0a86 (bia 5017.ff84.0a86)
<output omitted>
```

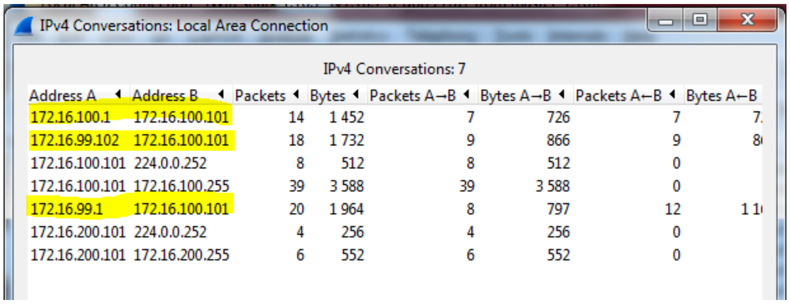
Step 2:   Test RSPAN operation

On PC-B, turn on Wireshark and capture all interface traffic.

In order to test the RSPAN configuration implemented on ALS1 and ALS2, we need to generate traffic from the source host, PC-A.

- Initiate a **ping** from PC-A to the **172.16.99.102** address
- Open a web browser. Browse to the following url: http://172.16.99.1
- From ALS2, initiate a **ping** to PC-A, **172.16.100.101**.
- From DLS1, initiate a **ping** to PC-A, **172.16.100.101**.

In the Wireshark application that is running on PC-B, select the STOP button then use the Statistics > Converstion List > IPv4 menu to view the IPv4 conversations contained in the capture. You will see that 172.16.200.101 (the address of PC-B) is not involved in any conversations except for traffic to 224.0.0.252 and 172.16.200.255.



IPv4 Conversations: 7

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B
172.16.100.1	172.16.100.101	14	1 452	7	726	7	7.
172.16.99.102	172.16.100.101	18	1 732	9	866	9	8
172.16.100.101	224.0.0.252	8	512	8	512	0	
172.16.100.101	172.16.100.255	39	3 588	39	3 588	0	
172.16.99.1	172.16.100.101	20	1 964	8	797	12	1 1
172.16.200.101	224.0.0.252	4	256	4	256	0	
172.16.200.101	172.16.200.255	6	552	6	552	0	

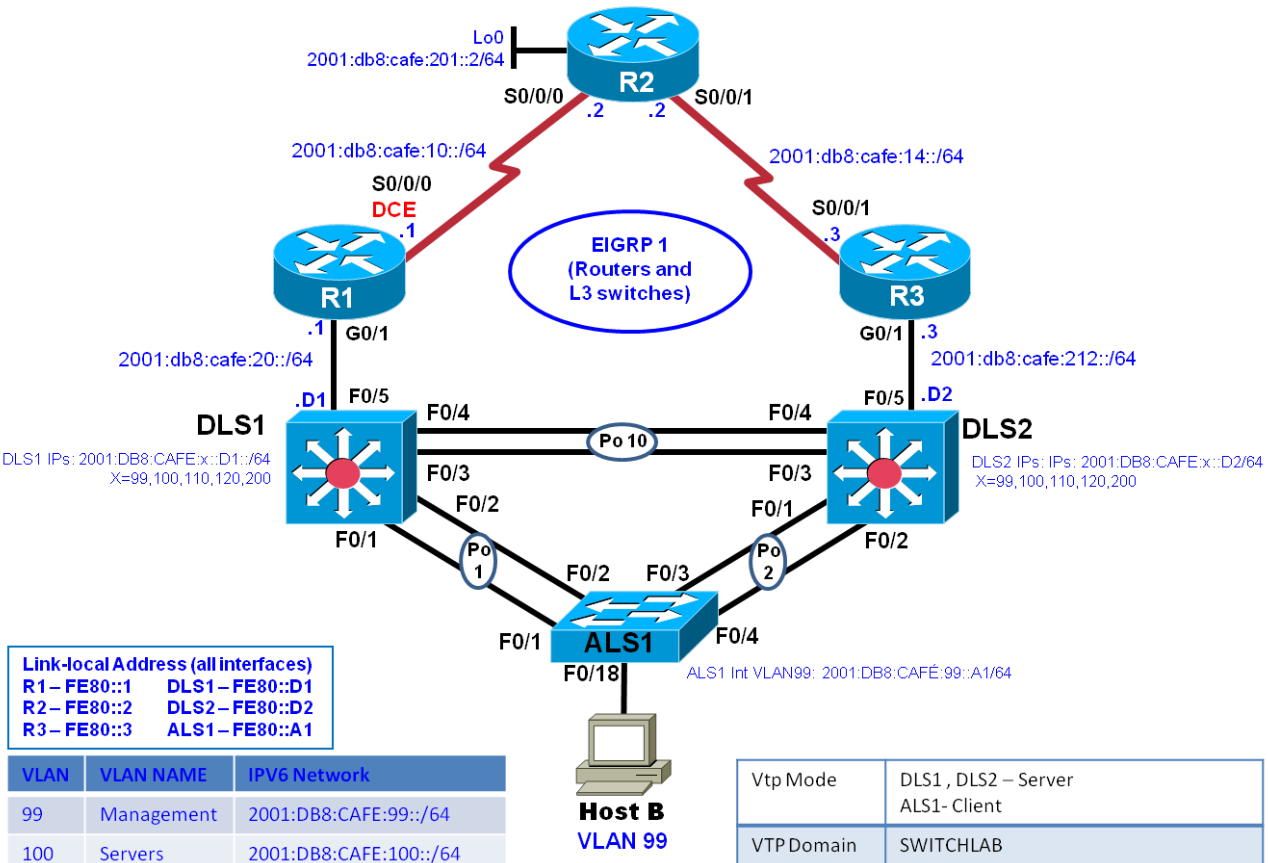
Step 3: End of Lab

Do not save your configurations. The equipment will be reset for the next lab.

CCNPv7.1 SWITCH

Chapter 6 Lab 6-2, Hot Standby Router Protocol for IPV6

Topology



Link-local Address (all interfaces)	
R1 – FE80::1	DLS1 – FE80::D1
R2 – FE80::2	DLS2 – FE80::D2
R3 – FE80::3	ALS1 – FE80::A1

VLAN	VLAN NAME	IPV6 Network
99	Management	2001:DB8:CAFE:99::/64
100	Servers	2001:DB8:CAFE:100::/64
110	Guest	2001:DB8:CAFE:110::/64
120	Office	2001:DB8:CAFÉ:120::/64
200	Voice	2001:DB8:CAFÉ:200::/64

Vtp Mode	DLS1 , DLS2 – Server ALS1- Client
VTP Domain	SWITCHLAB
PVRST+	DLS1 Root for VLANs 99, 110, 120 DLS2 Active for VLANs 100, 200
HSRPv6	DLS1 Active for VLANs 99, 110, 120 DLS2 Active for VLANs 100, 200

Objective

- Configure inter-VLAN routing with HSRP for IPV6 to provide redundant, fault-tolerant routing to the internal network.
- Configure HSRP object tracking
- Adjust HSRP times for optimization.

Background

Hot Standby Router Protocol (HSRP) version 2 is a Cisco-proprietary redundancy protocol for establishing a fault-tolerant default gateway. It is described in RFC 2281. HSRP provides a transparent failover mechanism to the end stations on the network. This provides users at the access layer with uninterrupted service to the network if the primary gateway becomes inaccessible. The Virtual Router Redundancy Protocol (VRRP) is a standards-based alternative to HSRP and is defined in RFC 3768. The two technologies are similar but not compatible. This lab focuses on HSRP.

Note: This lab uses Cisco ISR G2 routers running Cisco IOS 15.4(3) images with IP Base and Security packages enabled, and Cisco Catalyst 3560 and 2960 switches running Cisco IOS 15.0(2) IP Services and LAN Base images, respectively. The switches have Fast Ethernet interfaces, so the routing metrics for all Ethernet links in the labs are calculated based on 100 Mb/s, although the routers have Gigabit Ethernet interfaces. The 3560 and 2960 switches are configured with the SDM templates “dual-ipv4-and-ipv6 routing” and “lanbase-routing”, respectively. 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. Catalyst 3650 switches (running any Cisco IOS XE release) and Catalyst 2960-Plus switches (running any Cisco IOS image) can be used in place of the Catalyst 3560 switches and the Catalyst 2960 switches.

Note(2): This lab's topology is based on the NETLAB Multi-Purpose Academy Pod (MAP). If your classroom is using the standard Cuatro Switch Pod, the PC names may be different than displayed here. Consult with your instructor.

Required Resources

- 1 switches (Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-IPSERVICESK9-M image or comparable)
- Ethernet and console cables
- 1 PC

Implement HSRP for IPv6

Step 1: Prepare the switches for the lab

Use the **`reset.tcl`** script you created in Lab 1 “Preparing the Switch” to set your switches up for this lab. Then load the file BASE.CFG into the running-config with the command **`copy flash:BASE.CFG running-config`**. An example from DLS1:

```
DLS1# tclsh reset.tcl
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Reloading the switch in 1 minute, type reload cancel to halt

Proceed with reload? [confirm]

*Mar  7 18:41:40.403: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

```
*Mar  7 18:41:41.141: %SYS-5-RELOAD: Reload requested by console. Reload Reason: 
Reload command.
<switch reloads - output omitted>

Would you like to enter the initial configuration dialog? [yes/no]: n
Switch> en
*Mar  1 00:01:30.915: %LINK-5-CHANGED: Interface Vlan1, changed state to 
administratively down
Switch# copy BASE.CFG running-config
Destination filename [running-config]?
184 bytes copied in 0.310 secs (594 bytes/sec)
```

Step 2: Configure basic switch parameters.

Configure an IP address on the management VLAN according to the diagram. VLAN 1 is the default management VLAN, but following best practice, we will use a different VLAN. In this case, VLAN 99.

Enter basic configuration commands on each switch according to the diagram. Each interface should be configured with a global unicast address and a *statically assigned* link-local address. Please refer to the table on the topology diagram for the address information.

DLS1 example:

```
DLS1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)# interface vlan 99
DLS1(config-if)# ipv6 address 2001:DB8:CAFE:99::D1/64
DLS1(config-if)# ipv6 address fe80::d1 link-local
DLS1(config-if)# no shutdown
```

The interface VLAN 99 will not come up immediately, because the layer 2 instance of the vlan has not yet been defined. This issue will be remedied in subsequent steps.

(Optional) On each switch, create an enable secret password and configure the VTY lines to allow remote access from other network devices.

DLS1 example:

```
DLS1(config)# enable secret class
DLS1(config)# line vty 0 15
DLS1(config-line)# password cisco
DLS1(config-line)# login
```

Note: The passwords configured here are required for NETLAB compatibility only and are NOT recommended for use in a live environment.

Note(2): For purely lab environment purposes, it is possible to configure the VTY lines so that they accept any Telnet connection immediately, without asking for a password, and place the user into the privileged EXEC mode directly. The configuration would be similar to the following example for DLS1:

```
DLS1(config)# enable secret class
DLS1(config)# line vty 0 15
DLS1(config-line)# no login
DLS1(config-line)# privilege level 15
```

Step 3: Configure trunks and EtherChannels between switches.

EtherChannel is used for the trunks because it allows you to utilize both Fast Ethernet interfaces that are available between each device, thereby doubling the bandwidth.

Note: It is good practice to shut down the interfaces on both sides of the link before a port channel is created and then re-enable them after the port channel is configured; recall that BASE.CFG shut all interfaces down.

d. Configure trunks and EtherChannels from DLS1, DLS2, and ALS1 according to the diagram. Use PaGP as the negotiation protocol for EtherChannel configurations. ***Refer to diagram for port channel numbers*.

```
DLS1(config)# interface range fastEthernet 0/1-2
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# channel-group 1 mode desirable
DLS1(config-if-range)# no shut
Creating a port-channel interface Port-channel 1
```

e. Verify trunking and EtherChannel configurations between all switches with the appropriate trunking and EtherChannel verification commands.

Step 4: Configure VTP on all switches according to the VTP information on the diagram.

a. A sample configuration is provided for you.

```
DLS2(config)# vtp mode server
Setting device to VTP Server mode for VLANS
```

NOTE: Switches default to vtp mode server. However, remember the base configuration modifies this setting to vtp mode transparent.

Repeat similar configurations on ALS1.

b. Verify the VTP changes.

Step 5: Configure VTP on DLS1.

a. Create the VTP domain on VTP server DLS1 and create VLANs 99, 100, 110, 120, 200, for the domain.

NOTE: Switches default to vtp mode server. However, remember the base configuration modifies this setting to vtp mode transparent.

```
DLS1(config)# vtp domain SWITCHLAB
DLS1(config)# vtp version 2
DLS1(config)# vtp mode server
Setting device to VTP Server mode for VLANS

DLS1(config)# vlan 99
DLS1(config-vlan)# name Management
DLS1(config-vlan)# vlan 100
DLS1(config-vlan)# name Servers
DLS1(config-vlan)# vlan 110
DLS1(config-vlan)# name Guest
```

```
DLS1(config-vlan)# vlan 120
DLS1(config-vlan)# name office
DLS1(config-vlan)# vlan 200
DLS1(config-vlan)# name Voice
```

b. Verify that VLANs propagated to the other switches in the network.

Step 6: Configure HSRPv6 interfaces and enable IPV6 routing with EIGRP.

HSRP provides redundancy in the network. Traffic can be load-balanced by using the **`standby`** *`group`* **`priority`** *`priority`* command. The **`ipv6 unicast-routing`** command is used on DLS1 and DLS2 to activate ipv6 routing capabilities on these Layer 3 switches.

Each route processor can route between the various SVIs configured on its switch. In addition to the real IP address assigned to each distribution switch SVI, assign a third IP address in each subnet to be used as a virtual gateway address. HSRP negotiates and determines which switch accepts information forwarded to the virtual gateway IP address.

The **`standby`** command configures the IP address of the virtual gateway, sets the priority for each VLAN, and configures the router for preemption. Preemption allows the router with the higher priority to become the active router after a network failure has been resolved. HSRP version 2 must be implemented for support of IPv6. This is accomplised by using the **`standby version 2`** command on every interface required.

The **`standby x ipv6 autoconfig`** command, where x is the assigned HSRP group number, is used to assign the group an automatically generated virtual ipv6 address.

DLS1 is configured to be the active router for VLANs 99, 110, and 120 with a configured priority of 110, and the standby router for VLANs 100 and 200 with the default priority of 100.

DLS2 is configured to be the active router for VLANs 100 and 200 with a *configured* priority of 110, and the standby router for VLANs 99, 110, and 120 with a default priority of 100.

Note: It is recommended that the HSRP group number be mapped to VLAN number.

```
DLS1(config)# ipv6 unicast-routing
DLS1(config)# ipv6 router eigrp 1
DLS1(config-router)# no shutdown
DLS1(config-router)# router-id 1.1.1.1
DLS1(config-router)# exit
DLS1(config)# interface FastEthernet0/5
DLS1(config-if)# no switchport
DLS1(config-if)# ipv6 address FE80::D1 link-local
DLS1(config-if)# ipv6 address 2001:DB8:CAFE:20::D1/64
DLS1(config-if)# ipv6 eigrp 1
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# interface vlan 99
DLS1(config-if)# standby version 2
DLS1(config-if)# standby 99 ipv6 autoconfig
DLS1(config-if)# standby 99 priority 110
DLS1(config-if)# standby 99 preempt
DLS1(config-if)# ipv6 eigrp 1
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# interface vlan 100
DLS1(config-if)# ipv6 address 2001:DB8:CAFE:100::D1/64
DLS1(config-if)# ipv6 address FE80::D1 link-local
```

```
DLS1(config-if)# standby version 2
DLS1(config-if)# standby 100 ipv6 autoconfig
DLS1(config-if)# standby 100 preempt
DLS1(config-if)# ipv6 eigrp 1
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# interface vlan 110
DLS1(config-if)# ipv6 address 2001:DB8:CAFE:110::D1/64
DLS1(config-if)# ipv6 address FE80::D1 link-local
DLS1(config-if)# standby version 2
DLS1(config-if)# standby 110 ipv6 autoconfig
DLS1(config-if)# standby 110 priority 110
DLS1(config-if)# standby 110 preempt
DLS1(config-if)# ipv6 eigrp 1
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# interface vlan 120
DLS1(config-if)# ipv6 address 2001:DB8:CAFE:120::D1/64
DLS1(config-if)# ipv6 address FE80::D1 link-local
DLS1(config-if)# standby version 2
DLS1(config-if)# standby 120 ipv6 autoconfig
DLS1(config-if)# standby 120 priority 110
DLS1(config-if)# standby 120 preempt
DLS1(config-if)# ipv6 eigrp 1
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# interface vlan 200
DLS1(config-if)# ipv6 address 2001:DB8:CAFE:200::D1/64
DLS1(config-if)# ipv6 address FE80::D1 link-local
DLS1(config-if)# standby version 2
DLS1(config-if)# standby 200 ipv6 autoconfig
DLS1(config-if)# standby 200 preempt
DLS1(config-if)# ipv6 eigrp 1
DLS1(config-if)# no shutdown
```

```
DLS2(config)# ipv6 unicast-routing
DLS2(config)# ipv6 router eigrp 1
DLS2(config-router)# router-id 2.2.2.2
DLS2(config-router)# no shutdown
DLS2(config-router)# exit
DLS2(config)# interface FastEthernet0/5
DLS2(config-if)# no switchport
DLS2(config-if)# ipv6 address FE80::d2 link-local
DLS2(config-if)# ipv6 address 2001:DB8:CAFE:212::D2/64
DLS2(config-if)# ipv6 eigrp 1
DLS2(config-if)# no shutdown
DLS2(config-if)# exit
DLS2(config)# interface vlan 99
DLS2(config-if)# ipv6 address fe80::d2 link-local
DLS2(config-if)# standby version 2
DLS2(config-if)# standby 99 ipv6 autoconfig
DLS2(config-if)# standby 99 preempt
DLS2(config-if)# ipv6 eigrp 1
DLS2(config-if)# no shutdown
DLS2(config-if)# exit
```

```
DLS2(config)# interface vlan 100
DLS2(config-if)# ipv6 address 2001:DB8:CAFE:100::D2/64
DLS2(config-if)# ipv6 address FE80::D2 link-local
DLS2(config-if)# standby version 2
DLS2(config-if)# standby 100 ipv6 autoconfig
DLS1(config-if)# standby 100 priority 110
DLS2(config-if)# standby 100 preempt
DLS2(config-if)# ipv6 eigrp 1
DLS2(config-if)# no shutdown
DLS2(config-if)# exit
DLS2(config)# interface vlan 110
DLS2(config-if)# ipv6 address 2001:DB8:CAFE:110::D2/64
DLS2(config-if)# ipv6 address FE80::D2 link-local
DLS2(config-if)# standby version 2
DLS2(config-if)# standby 110 ipv6 autoconfig
DLS2(config-if)# standby 110 preempt
DLS2(config-if)# ipv6 eigrp 1
DLS2(config-if)# no shutdown
DLS2(config-if)# exit
DLS2(config)# interface vlan 120
DLS2(config-if)# ipv6 address 2001:DB8:CAFE:120::D2/64
DLS2(config-if)# ipv6 address FE80::D2 link-local
DLS2(config-if)# standby version 2
DLS2(config-if)# standby 120 ipv6 autoconfig
DLS2(config-if)# standby 120 preempt
DLS2(config-if)# ipv6 eigrp 1
DLS2(config-if)# no shutdown
DLS2(config-if)# exit
DLS2(config)# interface vlan 200
DLS2(config-if)# ipv6 address 2001:DB8:CAFE:200::D2/64
DLS2(config-if)# ipv6 address FE80::D2 link-local
DLS2(config-if)# standby version 2
DLS2(config-if)# standby 200 ipv6 autoconfig
DLS1(config-if)# standby 200 priority 110
DLS2(config-if)# standby 200 preempt
DLS2(config-if)# ipv6 eigrp 1
DLS2(config-if)# no shutdown
```

Step 7: Verify the HSRP configuration.

f. Issue the **show standby** command on both DLS1 and DLS2. Notice that the command to view HSRPv6 configuration is the same command used in implementing HSRPv4.

```
DLS1# sh standby
Vlan99 - Group 99 (version 2)
  State is Active
    4 state changes, last state change 00:05:05
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:63 (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.0063
    Local virtual MAC address is 0005.73a0.0063 (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.776 secs
  Preemption enabled
  Active router is local
  Standby router is FE80::D2, priority 100 (expires in 10.336 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl99-99" (default)
Vlan100 - Group 100 (version 2)
  State is Standby
    3 state changes, last state change 00:04:45
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:64 (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.0064
    Local virtual MAC address is 0005.73a0.0064 (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.080 secs
  Preemption enabled
  Active router is FE80::D2, priority 110 (expires in 10.672 sec)
    MAC address is e840.406f.6e43
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl100-100" (default)
Vlan110 - Group 110 (version 2)
  State is Active
    4 state changes, last state change 00:04:59
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:6E (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.006e
    Local virtual MAC address is 0005.73a0.006e (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.448 secs
  Preemption enabled
  Active router is local
  Standby router is FE80::D2, priority 100 (expires in 9.184 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl110-110" (default)
Vlan120 - Group 100 (version 2)
  State is Active
    4 state changes, last state change 00:05:00
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:64 (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.0064
    Local virtual MAC address is 0005.73a0.0064 (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.512 secs
  Preemption enabled
  Active router is local
  Standby router is FE80::D2, priority 100 (expires in 9.840 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl120-100" (default)
Vlan200 - Group 100 (version 2)
  State is Standby
    3 state changes, last state change 00:04:45
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:64 (conf auto EUI64)
  Active virtual MAC address is 0005.73a0.0064
    Local virtual MAC address is 0005.73a0.0064 (v2 IPv6 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.352 secs
  Preemption enabled
  Active router is FE80::D2, priority 110 (expires in 9.856 sec)
    MAC address is e840.406f.6e46
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl200-100" (default)
DLS1#
```

g. Issue the **show standby brief** command on both DLS1 and DLS2.

```
DLS1# sh stand bri
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl99        99   110 P Active  local           FE80::D2        FE80::5:73FF:FEA0:63
Vl100       100  100 P Standby FE80::D2        local           FE80::5:73FF:FEA0:64
Vl110       110  110 P Active  local           FE80::D2        FE80::5:73FF:FEA0:6E
Vl120       100  110 P Active  local           FE80::D2        FE80::5:73FF:FEA0:64
Vl200       100  100 P Standby FE80::D2        local           FE80::5:73FF:FEA0:64
DLS1#
DLS2# sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl99        99   100 P Standby FE80::D1        local           FE80::5:73FF:FEA0:63
Vl100       100  110 P Active  local           FE80::D1        FE80::5:73FF:FEA0:64
Vl110       110  100 P Standby FE80::D1        local           FE80::5:73FF:FEA0:6E
Vl120       100  100 P Standby FE80::D1        local           FE80::5:73FF:FEA0:64
Vl200       100  110 P Active  local           FE80::D1        FE80::5:73FF:FEA0:64
DLS2#
```

Referencing the above output, notice that the virtual IPv6 address for each HSRP group was automatically generated using EUI-64 format and that the address is a link-local address. This happened as a result of the **`standby x ipv6 autoconfig`** command being entered on the interface.

Part 2: Configure Interface Tracking.

Step 1: Configure routers R1, R2, and R3.

a. Configure EIGRP version 6 routing between R1, R2, and R3. Use the global unicast addresses and link-local addresses shown in the topology.

b. Manually set the router-id on these devices. Use the chart listed below.

R1	11.11.11.11
R2	12.12.12.12
R3	3.3.3.3

e. Verify connectivity throughout the network. If for some reason you do not have full connectivity, stop and troubleshoot routing before continuing with the next step in the lab.

Step 2: Configure interface tracking with HSRPv6.

Interface tracking is used to monitor interfaces that affect HSRP operation. If DLS1 is the active router for VLANs 99,110 and 120 forwarding to destination address 2001:db8:café:201::2 (located at router R2) and the connection between DLS1 and R1 is lost, DLS1 would have to reroute traffic over to DLS2. DLS2 would then forward traffic to the specified destination.

In order to prevent this from happening, we will tell HSRP to track the interface connected to R1. If that interface goes down, we will decrement the priority assigned to the interface by enough to cause DLS2 to take over as the active router.

If no decrement value is configured as a part of the interface tracking configuration, the default decrement is 10. The default can be used as long as the standby forwarder has a priority that is within 10 of the active forwarder.

```
DLS1(config-if)# standby 99 track ?
  <1-1000>            Tracked object number
  Async               Async interface
  Auto-Template       Auto-Template interface
  BVI                 Bridge-Group Virtual Interface
  CTunnel             CTunnel interface
  Dialer              Dialer interface
  FastEthernet        FastEthernet IEEE 802.3
  Filter              Filter interface
  Filtergroup         Filter Group interface
  GigabitEthernet     GigabitEthernet IEEE 802.3z
  GroupVI             Group Virtual interface
  Lex                 Lex interface
  Loopback            Loopback interface
  Port-channel        Ethernet Channel of interfaces
  Portgroup           Portgroup interface
  Pos-channel         POS Channel of interfaces
  Tunnel              Tunnel interface
  Vif                 PGM Multicast Host interface
  Virtual-TokenRing   Virtual TokenRing
  Vlan                Catalyst Vlans
  fcpa                Fiber Channel

DLS1(config-if)# standby 99 track fastEthernet 0/5 ?
  <1-255>  Decrement value
  <cr>

DLS1(config)# interface vlan 99
DLS1(config-if)# standby 99 track fastEthernet 0/5 30

DLS1(config)# interface vlan 110
DLS1(config-if)# standby 110 track fastEthernet 0/5 30

DLS1(config)# interface vlan 120
DLS1(config-if)# standby 120 track fastEthernet 0/5 30
```

NOTE: Repeat on DLS2 to track interface F0/5 for SVIs 100 and 200. Use a decrement value of 30.

Step 3: Test HSRPv6 tracked interfaces.

Configure interface F0/18 on ALS1 as an access port in VLAN 99.

Manually configure Host B with an IPv6 address with the 2001:db8:3115:99::/64 prefix

On Host B, start an extended ping using the command **`ping 2001:db8:café:201::2 –t`**

While the ping is running, move to DLS1 and shut down interface fa0/5. You should see an immediate HSRP state change. The goal of HSRP operation is to provide end user(s) (Host B) with automatic backup default-gateway services. As a result of the HSRP state change, clients experience minimal disruption and require no reconfiguration.

The following is from Host B (VLAN 99) to the R2 IPv6 loopback address.

```
C:\>ping 2001:db8:café:201::2 -t

Output omitted

DLS1(config)# interface fastEthernet 0/5
DLS1(config-if-range)# shutdown
```

Output to the console at DLS1 should reflect DLS2 becoming the active router for VLANs 99, 110 and 120.

Step 4: Verify that DLS2 is acting as the backup default gateway for VLANs 99, 110 and 120.

DLS2 is now the active HSRP router for all VLANs and the standby router is DLS1.

```
DLS1# sh stand bri
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl99        99   80  P Standby FE80::D2        local           FE80::5:73FF:FEA0:63
Vl100       100  100 P Standby FE80::D2        local           FE80::5:73FF:FEA0:64
Vl110       110  80  P Standby FE80::D2        local           FE80::5:73FF:FEA0:6E
Vl120       100  110 P Active  local           FE80::D2        FE80::5:73FF:FEA0:64
Vl200       100  100 P Standby FE80::D2        local           FE80::5:73FF:FEA0:64

DLS2# sh stand bri
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl99        99   100 P Active  local           FE80::D1        FE80::5:73FF:FEA0:63
Vl100       100  110 P Active  local           FE80::D1        FE80::5:73FF:FEA0:64
Vl110       110  100 P Active  local           FE80::D1        FE80::5:73FF:FEA0:6E
Vl120       100  100 P Standby FE80::D1        local           FE80::5:73FF:FEA0:64
Vl200       100  110 P Active  local           FE80::D1        FE80::5:73FF:FEA0:64
```

Repeat this process by bringing up the DLS1 interface connecting to R1. Shut down the DLS2 interface connecting to R3. Use the **show standby brief** command to see the results.

Note: Since DLS1 and DLS2 have links to the Internet, failure of either switch will cause HSRP to redirect packets to the other switch. The functioning switch will take over as the default gateway to provide virtually uninterrupted connectivity for hosts at the access layer.

CHALLENGE: Optimize HSRPv6 by adjusting the hello and hold timers used in HSRP communication with the hello time adjusted to 50 milliseconds and hold time adjusted to 250 milliseconds on all HSRP groups**.**

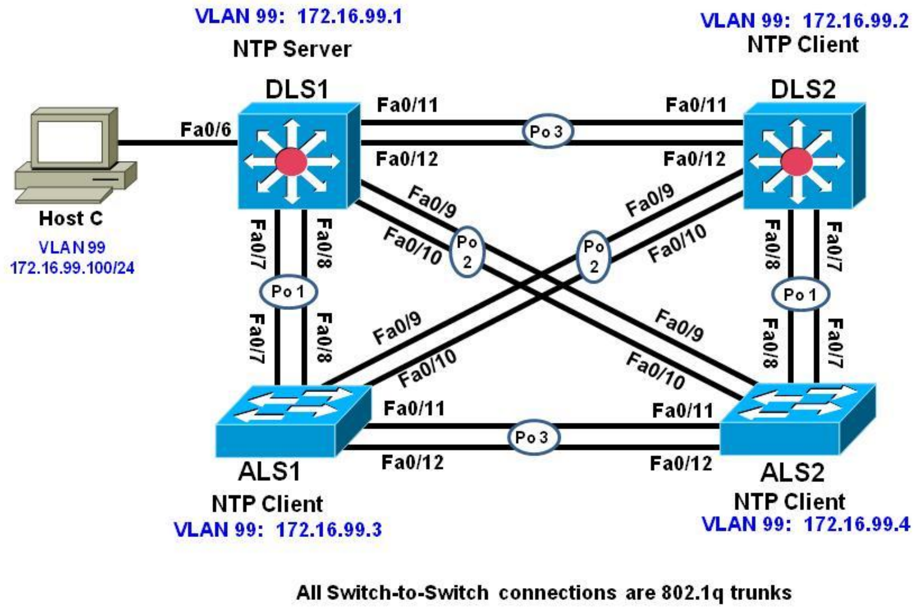
Step 5: End of Lab

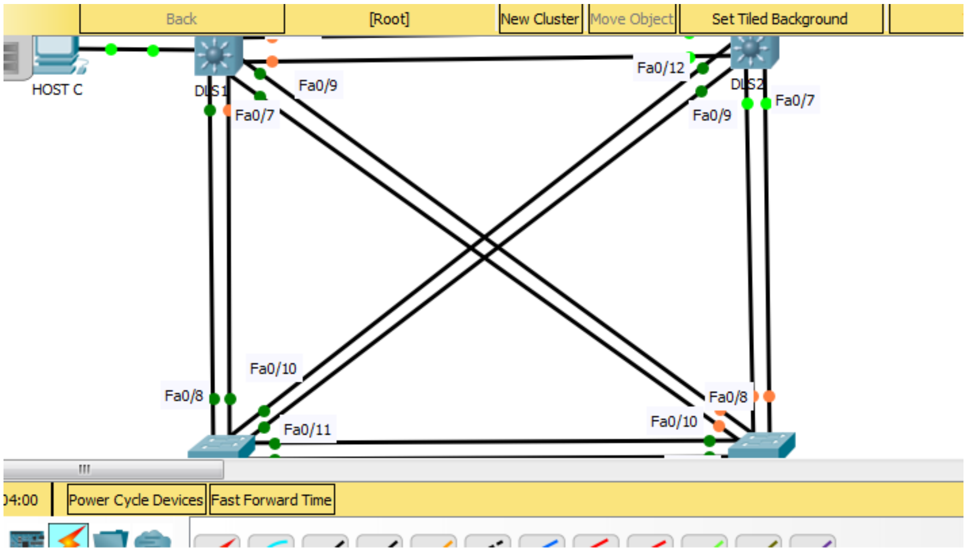
Do not save your configurations. The equipment will be reset for the next lab.

CCNPv7.1 SWITCH

Lab 7-2 Configure Campus Network Devices to support Simple Network Management Protocol (SNMPv3)

Topology





Objective

- Configure an SNMP View
- Configure SNMP version 2c
- Configure SNMP version 3
- Verify SNMP operation

Background

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between an agent and a management server. SNMP enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth. SNMP management workstations can ask (*get*) for the value of a specific *object identifier* (*OID*) from the *management information base* (*MIB*) maintained by SNMP agents. The Manager can also configure (*set*) specific variable values in an OID. Additionally, the agent can send notifications (*traps or informs*) when an event occurs or threshold is reached (simply put, an *inform* is a trap that must be acknowledged by the manager). Like any powerful tool, SNMP can be dangerous if not used properly, and securing the protocol and its uses are critical.

There are three SNMP versions. SNMPv3 is considered the most secure because it offers authentication and encryption, where SNMP versions 1 and 2 offer neither. SNMP access can also be limited using an access control list.

In this lab you will configure SNMP v3 on the distribution layer switches and SNMP v2c on the access layer switches. The network should still be configured and operating based on the configurations that you applied in Lab 7-1 Synchronizing NTP in the campus network. All SNMP communications will be carried on the Management VLAN (VLAN 99), and agent access will be restricted to the IP address of the Network management Server (HOST C).

Note: This lab uses Cisco Catalyst 3560 and 2960 switches running Cisco IOS 15.0(2) IP Services and LAN Base images, respectively. The 3560 and 2960 switches are configured with the SDM templates “dual-ipv4-and-ipv6 routing” and “lanbase-routing”, respectively. Depending on the switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab. Catalyst 3650 switches (running any Cisco IOS XE release) and Catalyst 2960-Plus switches (running any supported Cisco IOS image) can be used in place of the Catalyst 3560 switches and the Catalyst 2960 switches.

Required Resources

- 2 switches (Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-IPSERVICESK9-M image or comparable)
- Ethernet and console cables
- 1 PC (Windows Host with a Static IP) with Network Monitoring software (the free version of ManageEngine MIB Browser is used in this lab

Part 10: Prepare for the Lab

This lab uses the existing configurations from **Lab 7-1 Synchronizing NTP in the Campus Network**. The NTP functionality and security is not critical to perform this lab. However, you will need L2 trunking configured.

Step 1: Configure host access for Host C

Configure DLS1 interface F0/6 for access to VLAN 99 and configure Host C with the IP address 172.16.99.100/24 with a default gateway of 172.16.99.1. Verify Host C can ping all four switch management interfaces.

Part 11: Configure general SNMP parameters

In this part you will configure general SNMP parameters that will be used by all four switches.

Step 1: Configure general SNMP information

Configure general values to identify the device, it's location, and a point of contact. **Configure this with appropriate values on all four switches**:

```
DLS1(config)# snmp-server location DLS1 Rack 1
```

```
DLS1(config)# snmp-server contact Student
DLS1(config)# snmp-server chassis-id Cisco 3560v2 SN FTX2222222
```

Step 2: Configure access-lists for SNMP.

Configure an access list on each switch. This ACL will be used to specify exactly where SNMP get and set messages should be coming from. In this lab, the 172.16.99.0/24 network is the management network. **Configure this ACL on all four switches**:

```
DLS1(config)# ip access-list standard NMS-SERVERS
DLS1(config-std-nacl)# permit 172.16.99.0 0.0.0.255
DLS1(config-std-nacl)# exit
```

Step 3: Configure an SNMP view.

Access to the MIB is open access by default, and any authorized user can read or change the value of any OID in the MIB. Besides the ACL, you should also configure SNMP VIEWs. A view specifically allows or disallows access to certain parts of the MIB, which can provide both security and help control CPU utilization by limiting large SNMP polls.

The MIB is large and there are many different branches and variables, so how the views are configured really depends on how the NMS is implemented versus other SNMP access to the system. Views should be created and configured to contain those variables required by the different entities that might use SNMP to access your devices.

The output below is a basic view configuration that follows Cisco's guidance for OID access located at http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/configuration/12-4t/nm-snmp-cfg-snmp-support.html. The commands specify the "root" of the MIB tree and then further specifies sub-branches that are excluded. **Configure this view on all four switches.**

```
DLS1(config)#snmp-server view NMS-LIMIT iso included
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.21 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.22 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.35 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.3 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.6.3.15 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.6.3.16 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.6.3.18 excluded
```

The OID values in the above configuration correspond to the following:

Note: iso in the text below refers to the root of the MIB tree

1.3.6.1.2.1.4.21 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(ip-4).(ipRouteTable-21).

1.3.6.1.2.1.4.21 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(ip-4).(ipNetToMediaTable-22).

1.3.6.1.2.1.4.21 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(ip-4).(ipNetToPhysicalTable-35).

1.3.6.1.2.1.3 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(atTable-3)

1.3.6.1.6.3.15 is (iso-1).(org-3).(dod-6).(internet-1).(snmpv2-6).(snmpModules-3).(snmpUsmMIB-15)

1.3.6.1.6.3.16 is (iso-1).(org-3).(dod-6).(internet-1).(snmpv2-6).(snmpModules-3).(snmpVacMMIB-16)

1.3.6.1.6.3.18 is (iso-1).(org-3).(dod-6).(internet-1).(snmpv2-6).(snmpModules-3).(snmpCommunityMIB-18)

The NMS-LIMIT view above will protect some of the SNMP credentials from accidental exposure (nsmpUsmMIB, snmpVacmMIB, snmpCommunityMIB) and deny access to the Routing Table (ipRouteTable), the ARP table (atTable), and the deprecated ipNetToMediaTable and ipNetToPhysicalTable OIDs.

Part 12: Configure DLS1 and DLS2 for SNMPv3

Step 1: Configure SNMP groups.

SNMP groups are a construct that allows for users and views to be associated with one another.

Included as a part of the group configuration for SNMPv3 is the security model (no auth, auth, or priv), optional associated read, write, and inform views, and optional access-list controlling source addresses in the group.

In the output below, a group called **ccnp-switch3** is created to use SNMPv3, the security features implemented by the group, the read view of NMS-LIMIT and is restricted by the ACL NMS-SERVERS. Configure this on both DLS1 and DLS2. An example from DLS1:

```
DLS1(config)# snmp-server group ccnp-switch3 v3 priv read NMS-LIMIT access
NMS-SERVERS
```

Step 2: Configure SNMP users.

Configure users on DLS1 and DLS2. They will use an **SNMPv3 user** who is a part of the group **ccnp-switch3**. They will authenticate using **SHA** with **password cisco123**, and will encrypt using **AES 128** with a **password** of **cisco123.** Configure this on both DLS1 and DLS2. An example from DLS1:

```
DLS1(config)# snmp-server user student ccnp-switch3 v3 auth sha cisco123 priv
aes 128 cisco123
```

Note: This command will **not** show in the running configuration after it is entered.

After configuring the user, you should see this SYSLOG message:

```
Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...
```

Step 3: Configure SNMP trap receiver

Configure the NMS server traps will be sent to. As a part of this command, specific traps or sets of traps to send can be specified. If no traps are specified, this receiver will be forwarded all traps that are enabled. This particular configuration needs to be coordinated with the network management system and network monitoring requirements for the organization.

Configure 172.16.99.100 as a trap receiver for DLS1 and DLS2 For simplicity, do not configure any trap limits. Configure this on both DLS1 and DLS2. An example from DLS1:

```
DLS1(config)# snmp-server host 172.16.99.100 traps version 3 priv student
```

Step 4: Configure Interface Index Persistence.

Network monitoring systems record throughput and other interface statistics using SNMP polling. Each interface is referenced by its unique index number, which is dynamically assigned by the IOS upon boot. The index of each interface can be determined with the command **show snmp mib ifmib ifindex**. The dynamic assignment aspect of this can be problematic for documentation. Therefore, it is a good idea to instruct the system to keep a persistent list of interfaces rather than a dynamic one. The use of this command creates a file stored in NVRAM. Configure this on both DLS1 and DLS2. An example from DLS1:

```
DLS1(config)# snmp-server ifindex persist
```

Step 5: Enable SNMP Trap Sending

This final command actually enables the forwarding of traps to the configured trap receivers. As a part of this command, traps can be limited (as they can be in the snmp-server host command). Once again this will need to be coordinated with the network management system and network monitoring requirements for the organization. Configure this on both DLS1 and DLS2. An example from DLS1:

```
DLS1(config)# snmp-server enable traps
```

Step 6: Verify SNMP configuration.

To very quickly verify that traps are being sent, issue the command debug snmp packets and then enter configuration mode. You should see debug output indicating a packet was sent:

```
DLS1# debug snmp packets
SNMP packet debugging is on
DLS1#
DLS1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#
Jul 30 18:27:05.274: SNMP: Queuing packet to 172.16.99.100
Jul 30 18:27:05.274: SNMP: V2 Trap, reqid 1, errstat 0, erridx 0
 sysUpTime.0 = 37646
 snmpTrapOID.0 = ciscoConfigManMIB.2.0.1
 ccmHistoryEventEntry.3.7 = 1
 ccmHistoryEventEntry.4.7 = 2
 ccmHistoryEventEntry.5.7 = 3
DLS1(config)# end
DLS1# undebug all
```

Use the **show snmp** command to view configuration information for SNMP:

```
DLS1# show snmp
Chassis: Cisco 3560v2 SN FTX2222222
Contact: Student
Location: DLS1 Rack 1
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
1 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    1 Trap PDUs
SNMP global trap: enabled

SNMP logging: enabled
    Logging to 172.16.99.100.162, 0/10, 1 sent, 0 dropped.
SNMP agent enabled
DLS1#
```

Use the **show snmp view** command:

```
DLS1# show snmp view
cac_view pimMIB - included read-only active
cac_view msdpMIB - included read-only active
cac_view ip - included read-only active
cac_view ospf - included read-only active
cac_view bgp - included read-only active
cac_view dot1dBridge - included read-only active
cac_view ipMRouteStdMIB - included read-only active
cac_view igmpStdMIB - included read-only active
cac_view ipForward - included read-only active
cac_view ipTrafficStats - included read-only active
cac_view ospfTrap - included read-only active
cac_view sysUpTime.0 - included read-only active
cac_view ciscoPingMIB - included read-only active
cac_view ciscoStpExtensionsMIB - included read-only active
cac_view ciscoIpSecFlowMonitorMIB - included read-only active
cac_view ciscoPimMIB - included read-only active
cac_view ciscoMgmt.187 - included read-only active
cac_view ciscoEigrpMIB - included read-only active
cac_view ciscoCefMIB - included read-only active
cac_view ciscoIpMRouteMIB - included read-only active
cac_view ciscoIPsecMIB - included read-only active
cac_view cospf - included read-only active
cac_view ciscoExperiment.101 - included read-only active
cac_view ciscoIetfIsisMIB - included read-only active
cac_view ifIndex - included read-only active
cac_view ifDescr - included read-only active
cac_view ifType - included read-only active
cac_view ifAdminStatus - included read-only active
cac_view ifOperStatus - included read-only active
cac_view snmpTraps.3 - included read-only active
cac_view snmpTraps.4 - included read-only active
cac_view snmpTrapOID.0 - included read-only active
cac_view snmpMIB.1.4.3.0 - included read-only active
cac_view lifEntry.20 - included read-only active
cac_view cciDescriptionEntry.1 - included read-only active
NMS-LIMIT iso - included nonvolatile active
NMS-LIMIT at - excluded nonvolatile active
NMS-LIMIT snmpUsmMIB - excluded nonvolatile active
NMS-LIMIT snmpVacmMIB - excluded nonvolatile active
NMS-LIMIT snmpCommunityMIB - excluded nonvolatile active
NMS-LIMIT ip.21 - excluded nonvolatile active
NMS-LIMIT ip.22 - excluded nonvolatile active
NMS-LIMIT ip.35 - excluded nonvolatile active
v1default iso - included permanent active
v1default internet - included permanent active
v1default snmpUsmMIB - excluded permanent active
v1default snmpVacmMIB - excluded permanent active
v1default snmpCommunityMIB - excluded permanent active
v1default ciscoMgmt.252 - excluded permanent active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
FFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F iso - included volatile active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
FFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F iso.2.840.10036 - included
volatile active
```

Verify SNMP groups.

```
DLS1# show snmp group
groupname: ccnp-switch3                     security model:v3 priv
contextname: <no context specified>         storage-type: nonvolatile
readview : NMS-LIMIT                        writeview: <no writeview
specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active      access-list: NMS-SERVERS

DLS1#
```

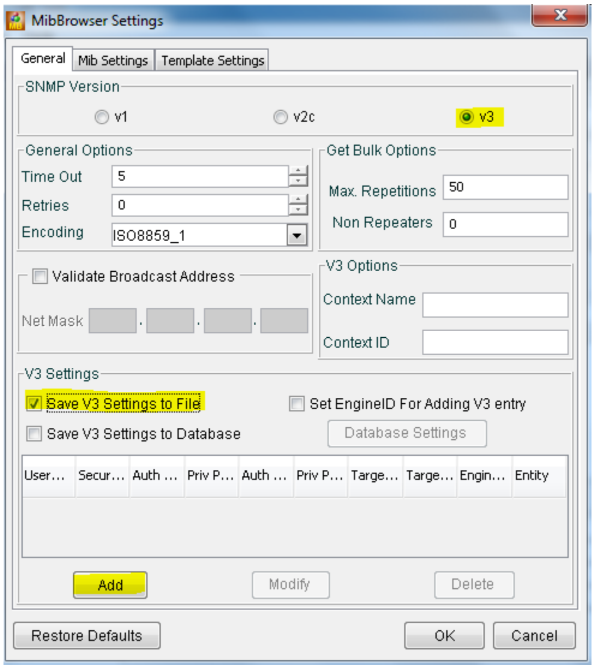
Verify SNMPv3 users:

```
DLS1#show snmp user
User name: student
Engine ID: 800000090300E840406F7283
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ccnp-switch3
```

Step 7: Configure MIBBrowser software

This lab uses the free tool "MIBBrowser" from ManageEngine for verification. Other tools that will listen for traps at are acceptable substitutes as well.

On the MIBBrowser file menu, select **Edit** and **Settings**. Select **the SNMP version 3** radio button, select “**Save V3 Settings** to file and then click **ADD**.



MibBrowser Settings

General | Mib Settings | Template Settings

SNMP Version: ○ v1 ○ v2c ● v3

General Options

Time Out	5
Retries	0
Encoding	ISO8859_1

Get Bulk Options

Max. Repetitions	50
Non Repeaters	0

□ Validate Broadcast Address

Net Mask

V3 Options

Context Name

Context ID

V3 Settings

☑ Save V3 Settings to File

□ Set EngineID For Adding V3 entry

□ Save V3 Settings to Database

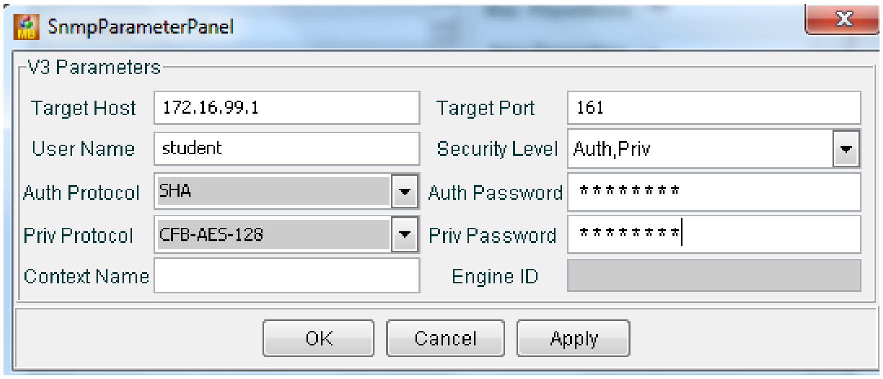
Database Settings

User…	Secur…	Auth …	Priv P…	Auth …	Priv P…	Targe…	Targe…	Engin…	Entity

Add | Modify | Delete

Restore Defaults | OK | Cancel

On the **SnmpParameterPanel**, fill in the values for the SNMPv3 user:



SnmpParameterPanel

V3 Parameters

Target Host	172.16.99.1	Target Port	161
User Name	student	Security Level	Auth,Priv
Auth Protocol	SHA	Auth Password	********
Priv Protocol	CFB-AES-128	Priv Password	********
Context Name		Engine ID	

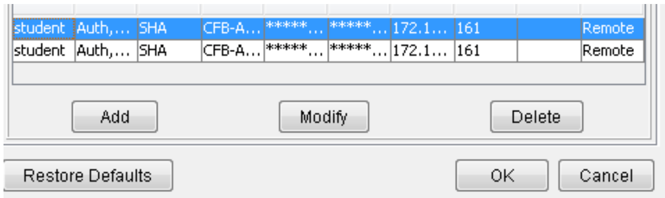
OK | Cancel | Apply

- Target Host: **IP Address of DLS1 (172.16.99.1)**

- User Name: **student**
- Security Level: **Auth,Priv**
- Auth Protocol: **SHA**
- Auth Password: **cisco123**
- Priv Protocol: **CFB-AES-128**
- Priv Password: **cisco123**

Once the values are entered, then, click **ok**. Click **Add again** and **add DLS2 (172.16.99.2)** with the same values.

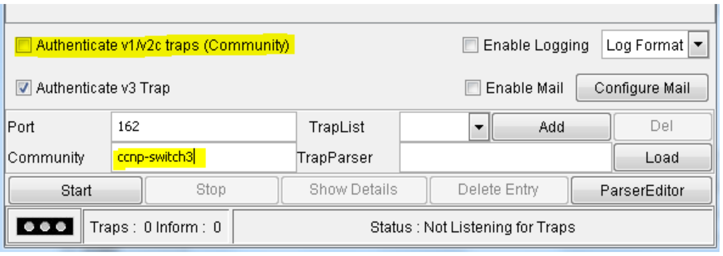
Once values are added for both devices, select DLS1's entry and click **OK**.



student	Auth,...	SHA	CFB-A...	*****...	*****...	172.1...	161		Remote
student	Auth,...	SHA	CFB-A...	*****...	*****...	172.1...	161		Remote

Step 8: Verify SNMP TRAP Operation

Run MibBrowser. Select **View** and then **Trap Viewer** from the File Menu. The TrapViewer window will open. Uncheck the "**Authenticate v1/v2c traps (Community).** Click into the Community field and change **'public' to 'ccnp-switch3'** and click the **add** button.



□ Authenticate v1/v2c traps (Community)

☑ Authenticate v3 Trap

□ Enable Logging

□ Enable Mail

Port 162

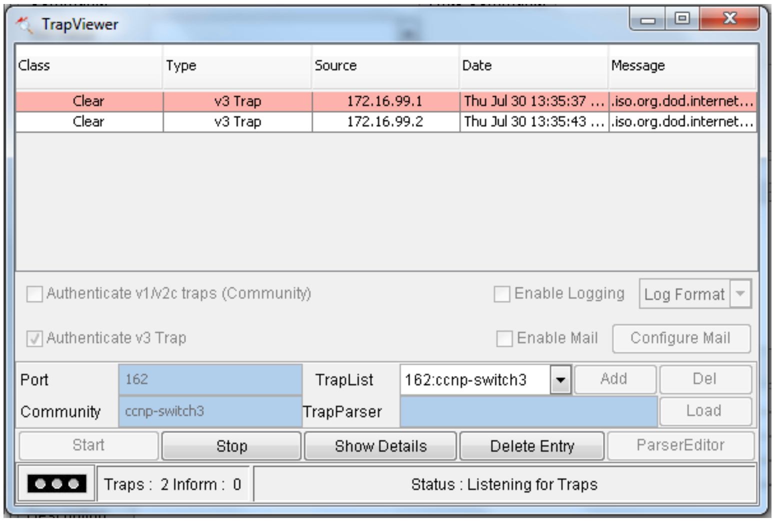
Community ccnp-switch3

Traps : 0 Inform : 0

Status : Not Listening for Traps

Finally, click Start. TrapViewer is now listening for traps.

Go to the command prompt at DLS1 and DLS2 and enter configuration mode. You should see at least two SNMPv3 traps collected in the TrapViewer. This validates that traps are being sent to the designated host.



Class	Type	Source	Date	Message
Clear	v3 Trap	172.16.99.1	Thu Jul 30 13:35:37 ...	.iso.org.dod.internet...
Clear	v3 Trap	172.16.99.2	Thu Jul 30 13:35:43 ...	.iso.org.dod.internet...

□ Authenticate v1/v2c traps (Community)   □ Enable Logging

☑ Authenticate v3 Trap   □ Enable Mail

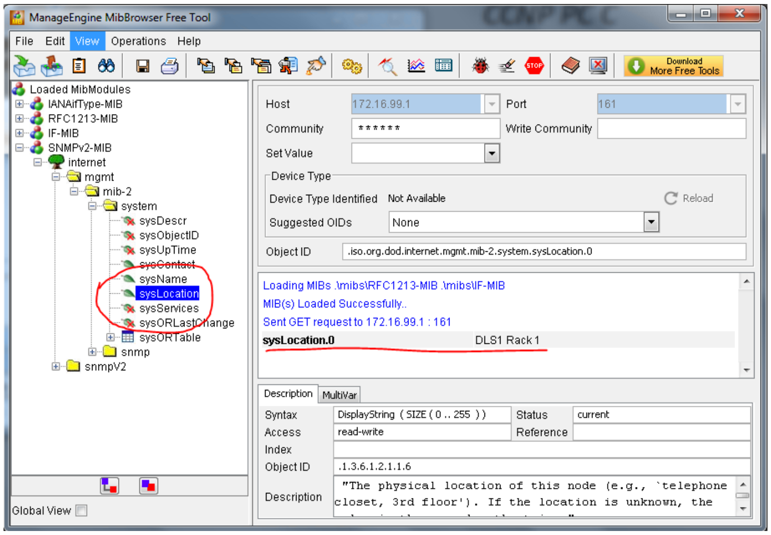
Port 162   TrapList 162:ccnp-switch3

Community ccnp-switch3   TrapParser

Traps : 2 Inform : 0   Status : Listening for Traps

Step 9:   Verify SNMP GET Operation

Move the TrapViewer window out of the way (do not close it) and click on the main MibBrowser window. Under the "Loaded MibModules" category, expand SNMPv2-MIB, internet, mgmt, mib-2, and system and then select sysLocation. Right click and select GET. You should see the system location information you configured previously appear in the center window.



Host 172.16.99.1   Port 161

Community ******   Write Community

Set Value

Device Type

Device Type Identified   Not Available

Suggested OIDs   None

Object ID   .iso.org.dod.internet.mgmt.mib-2.system.sysLocation.0

```
Loading MIBs .\mibs\RFC1213-MIB .\mibs\IF-MIB
MIB(s) Loaded Successfully..
Sent GET request to 172.16.99.1 : 161
sysLocation.0                          DLS1 Rack 1
```

Syntax   DisplayString (SIZE (0 .. 255))   Status   current

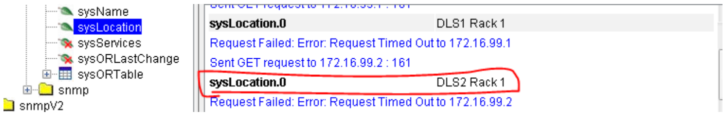
Access   read-write   Reference

Index

Object ID   .1.3.6.1.2.1.1.6

Description   "The physical location of this node (e.g., `telephone closet, 3rd floor'). If the location is unknown, the

Click on Edit, then Settings. Select the second SNMPv3 entry and click OK, then repeat the above steps to verify SNMPv3 is working with DLS2.



```
sysLocation.0                          DLS1 Rack 1
Request Failed: Error: Request Timed Out to 172.16.99.1
Sent GET request to 172.16.99.2 : 161
sysLocation.0                          DLS2 Rack 1
Request Failed: Error: Request Timed Out to 172.16.99.2
```

Part 13: Configure ALS1 and ALS2 for SNMPv2c

Step 1: Configure SNMP Community String.

SNMPv2c using a community-string based authentication. Access can be limited further by using an access list. Create a read-only community named ccnp-switch2 that is limited by the NMS-SERVERS ACL and restricted to the view NMS-VIEW that was created earlier. Configure this on both ALS1 and ALS2. An example from ALS1:

```
ALS1(config)# snmp-server community ccnp-switch2 view NMS-LIMIT ro NMS-
SERVERS
```

Step 2: Configure SNMP trap receiver

Configure the NMS server traps will be sent to. As a part of this command, specific traps or sets of traps to send can be specified. If no traps are specified, this receiver will be forwarded all traps that are enabled. This particular configuration needs to be coordinated with the network management system and network monitoring requirements for the organization.

Configure 172.16.99.100 as a trap receiver using SNMPv2c and the community ccnp-switch2. Configure this on both ALS1 and ALS2. An example from ALS1:

```
ALS1(config)# snmp-server host 172.16.99.100 version 2c ccnp-switch2
```

Step 3: Configure Interface Index Persistence.

Network monitoring systems record throughput and other interface statistics using SNMP polling. Each interface is referenced by its unique index number, which is dynamically assigned by the IOS upon boot. The index of each interface can be determined with the command **show snmp mib ifmib ifindex**. The dynamic assignment aspect of this can be problematic for documentation. Therefore, it is a good idea to instruct the system to keep a persistent list of interfaces, rather than a dynamic one. The use of this command creates a file stored in NVRAM. Configure this on both ALS1 and ALS2. An example from ALS1:

```
ALS1(config)# snmp-server ifindex persist
```

Step 4: Enable SNMP Trap Sending

This final command actually enables the forwarding of traps to the configured trap receivers. As a part of this command, traps can be limited (as they can be in the snmp-server host command). Once again this will need to be coordinated with the network management system and network monitoring requirements for the organization. Configure this on both ALS1 and ALS2. An example from ALS1:

```
ALS1(config)# snmp-server enable traps
```

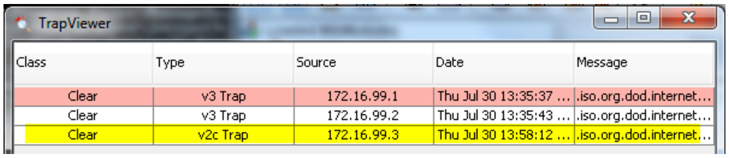
Step 5: Verify SNMP configuration.

To very quickly verify that traps are being sent, issue the command debug snmp packets and then enter configuration mode. You should see debug output indicating a packet was sent:

```
ALS1# debug snmp packets
SNMP packet debugging is on
```

```
ALS1#
ALS1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#
Jul 30 18:57:17.770: SNMP: Queuing packet to 172.16.99.100
Jul 30 18:57:17.770: SNMP: V2 Trap, reqid 1, errstat 0, erridx 0
 sysUpTime.0 = 878054
 snmpTrapOID.0 = ciscoConfigManMIB.2.0.1
 ccmHistoryEventEntry.3.5 = 1
 ccmHistoryEventEntry.4.5 = 2
 ccmHistoryEventEntry.5.5 = 3
ALS1(config)# end
ALS1# undebug all
```

At this point, look at the TrapViewer window and you should see a v2c trap was received.



Class	Type	Source	Date	Message
Clear	v3 Trap	172.16.99.1	Thu Jul 30 13:35:37 ...	.iso.org.dod.internet...
Clear	v3 Trap	172.16.99.2	Thu Jul 30 13:35:43 ...	.iso.org.dod.internet...
Clear	v2c Trap	172.16.99.3	Thu Jul 30 13:58:12 ...	.iso.org.dod.internet...

Use the **show snmp** command to view configuration information for SNMP:

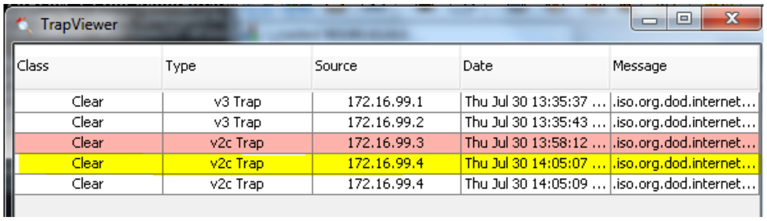
```
ALS1# show snmp
Chassis: Cisco 2960 SN FTX4444444
Contact: Student
Location: ALS1 Rack 1
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
1 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    1 Trap PDUs
SNMP global trap: enabled

SNMP logging: enabled
    Logging to 172.16.99.100.162, 0/10, 1 sent, 0 dropped.
SNMP agent enabled
ALS1#
```

Use the **show snmp community** command (community will be repeated for each VLAN, noted by the @[vlan #]):

```
ALS1# show snmp community

Community name: ccnp-switch2
Community Index: ccnp-switch2
Community SecurityName: ccnp-switch2
storage-type: nonvolatile        active access-list: NMS-SERVERS


Community name: ccnp-switch2@1
Community Index: ccnp-switch2@1
Community SecurityName: ccnp-switch2
storage-type: read-only  active access-list: NMS-SERVERS


Community name: ccnp-switch2@1002
Community Index: ccnp-switch2@1002
Community SecurityName: ccnp-switch2
storage-type: read-only  active access-list: NMS-SERVERS


Community name: ccnp-switch2@1003
Community Index: ccnp-switch2@1003
Community SecurityName: ccnp-switch2
storage-type: read-only  active access-list: NMS-SERVERS


Community name: ccnp-switch2@1004
Community Index: ccnp-switch2@1004
Community SecurityName: ccnp-switch2
storage-type: read-only  active access-list: NMS-SERVERS


Community name: ccnp-switch2@1005
Community Index: ccnp-switch2@1005
Community SecurityName: ccnp-switch2
storage-type: read-only  active access-list: NMS-SERVERS


Community name: ccnp-switch2@99
Community Index: ccnp-switch2@99
Community SecurityName: ccnp-switch2
storage-type: read-only  active access-list: NMS-SERVERS


ALS1#
```

Step 6: Verify SNMP TRAP Operation

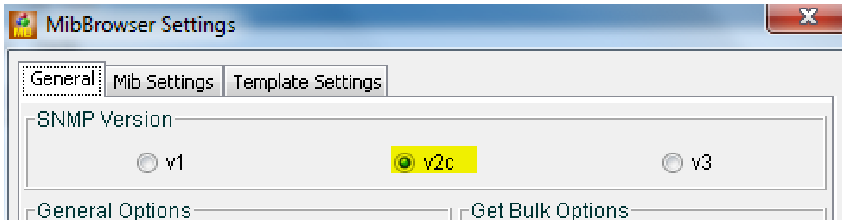
MibBrowser's TrapViewer should still be open and listening for traps, and you should have already seen a trap from ALS1. Go into configuration mode on ALS2 and verify a trap is received.



Class	Type	Source	Date	Message
Clear	v3 Trap	172.16.99.1	Thu Jul 30 13:35:37 ...	.iso.org.dod.internet...
Clear	v3 Trap	172.16.99.2	Thu Jul 30 13:35:43 ...	.iso.org.dod.internet...
Clear	v2c Trap	172.16.99.3	Thu Jul 30 13:58:12 ...	.iso.org.dod.internet...
Clear	v2c Trap	172.16.99.4	Thu Jul 30 14:05:07 ...	.iso.org.dod.internet...
Clear	v2c Trap	172.16.99.4	Thu Jul 30 14:05:09 ...	.iso.org.dod.internet...

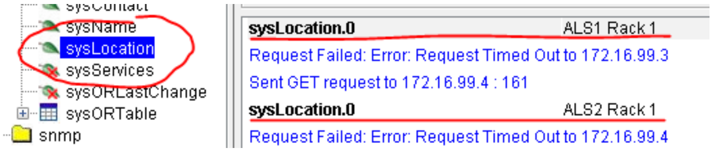
Step 7: Verify SNMP GET Operation

Next to verify GET operations in SNMPv2c are working, go back to the Settings screen (edit>settings) and change the radio button selection from **v3** to **v2** and click OK**.**



SNMP Version: ○ v1 ● v2c ○ v3

Once you click OK you will be returned to the main screen. Here the host settings fields will be available for editing . In the Host field, type **172.16.99.3** (ALS1), and in the Community field, type **ccnp-switch2**. Under the "Loaded MibModules" category, expand SNMPv2-MIB, internet, mgmt, mib-2, and system and then select sysLocation. Right click and select GET. You should see the system location information you configured previously appear in the center window. Repeat this process for ALS2 (172.16.99.4) to verify SNMPvc is configured correctly on this device.



```
sysLocation.0                              ALS1 Rack 1
Request Failed: Error: Request Timed Out to 172.16.99.3
Sent GET request to 172.16.99.4 : 161
sysLocation.0                              ALS2 Rack 1
Request Failed: Error: Request Timed Out to 172.16.99.4
```

Step 8: End of Lab

Do not save your configurations. The equipment will be reset for the next lab.