

**ACTIVIDAD COLABORATIVA 4 – ADMINISTRACIÓN, SEGURIDAD Y ESTABILIDAD EN
REDES CONMUTADAS**

NOMBRES

JONNY ZUÑIGA
JUAN DAVID BELTRAN
JOAO ALBERTINI PASCUAZA
CRISTIAN ARLEY BERNAL
JULIO EDUARDO GARRIDO MEJIA

TUTOR: GERARDO GRANADOS ACUÑA

GRUPO: 208014A_363

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
DIPLOMADO DE PROFUNDIZACION CISCO CCNP
NOVIEMBRE
2017**

TABLA DE CONTENIDO

INTRODUCCION.....	3
OBJETIVO.....	4
DESARROLLO DE LOS LABORATORIOS	5
CCNPv7.1_SWITCH_Lab6-1_FHRP_HSRP_VRRP_STUDENT.....	5
CCNPv7.1_SWITCH_Lab6-2_HSRPv6_STUDENT	55
CCNPv7.1_SWITCH_Lab6-3_GLBP_STUDENT	71
CCNPv7.1_SWITCH_Lab7-1_NTP_STUDENT.....	100
CCNPv7.1_SWITCH_Lab7-2_SNMP_STUDENT	118
CCNPv7.1_SWITCH_Lab8-1_IP_SLA_SPAN_STUDENT	140
CCNPv7.1_SWITCH_Lab 10-1_Securing_Layer2_STUDENT	154
CCNPv7.1_SWITCH_Lab 10-2_Securing VLANs_STUDENT	182
CONCLUSIONES.....	192
REFERENCIAS BIBLIOGRAFICAS.....	193

INTRODUCCION

En el siguiente informe se da a conocer la importancia del curso como forma de aprendizaje acerca del proceso de enrutamiento y configuración avanzado usando Switch para segmentar la red a través de VLAN para enviar paquetes a la red de destino a través de equipos estos conectados en la red LAN, pasando por capa 2 y capa 3.

Por medio de un componente práctico (laboratorio) se hace uso de Packet Tracer como herramienta de simulación de redes bajo el uso de tecnología CISCO, desarrollando la habilidad de configurar y administrar equipos de enrutamiento avanzado e implementando protocolos; VLAN – IP ROUTE

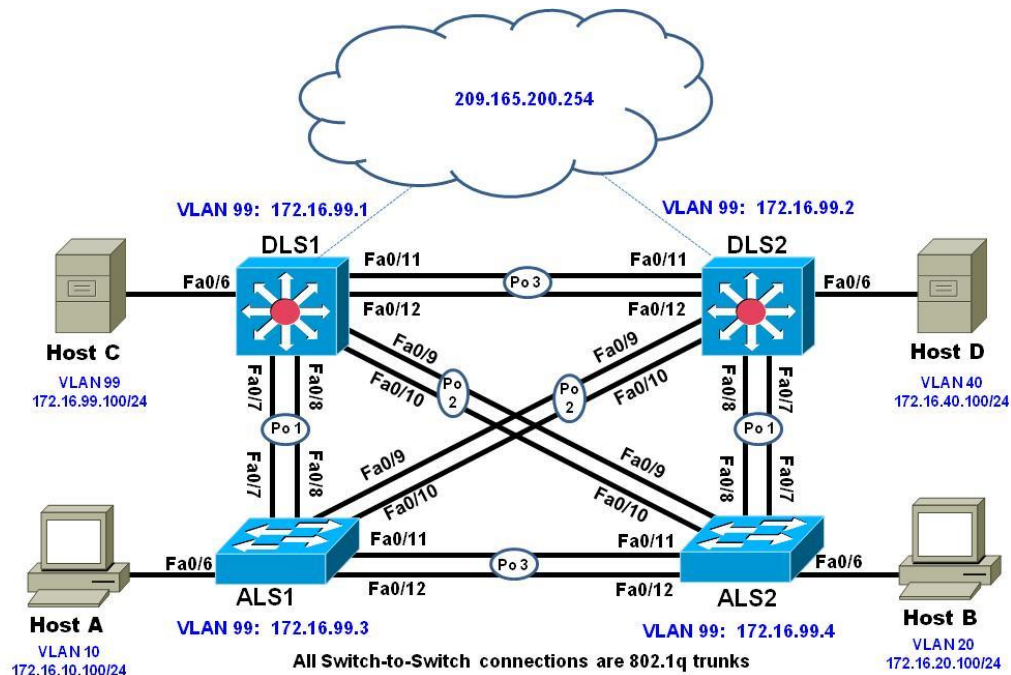
OBJETIVO

- Diseñar, instalar, configurar y administrar redes conmutadas
- Aprender a configurar y administrar los protocolos STP y LACP VTP
- Resolver problemas de red relacionados con; Administración, Seguridad y Escalabilidad en redes conmutadas
- Aprender a realizar resolución de problemas en problemas de enrutamiento avanzados

DESARROLLO DE LOS LABORATORIOS

CCNPv7.1_SWITCH_Lab6-1_FHRP_HSRP_VRRP_STUDENT

Topology



Gateway Addresses	
VLAN	Address
10	172.16.10.524
20	172.16.20.5/24
30	172.16.30.5/24
40	172.16.40.5/24
99	172.16.99.5/24

Objectives

- Configure inter-VLAN routing with HSRP and load balancing
- Configure HSRP authentication
- Configure HSRP interface tracking
- Configure VRRP
- Configure VRRP object tracking

Hot Standby Router Protocol (HSRP) 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 will offer configuration experience with both of the protocols in a phased approach.

Some of the configurations in this lab will be used in subsequent labs. Please read carefully before clearing your devices.

Note: This lab uses the Cisco WS-C2960-24TT-L switch with the Cisco IOS image c2960-lanbasek9-mz.150-2.SE6.bin and the Catalyst 3560V2-24PS switch with the Cisco IOS image c3560-ipservicesk9-mz.150-2.SE6.bin. Other switches and Cisco IOS Software versions can be used if they have comparable capabilities and features. 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.

Required Resources

- 2 switches (Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable)
- 2 switches (Cisco 3560v2 with the Cisco IOS Release 15.0(2)SE6 C3560-IPSERVICESK9-M image or comparable)
- Ethernet and console cables
- 4 PC's with Windows OS

1 Prepare for the Lab

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)
```

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.

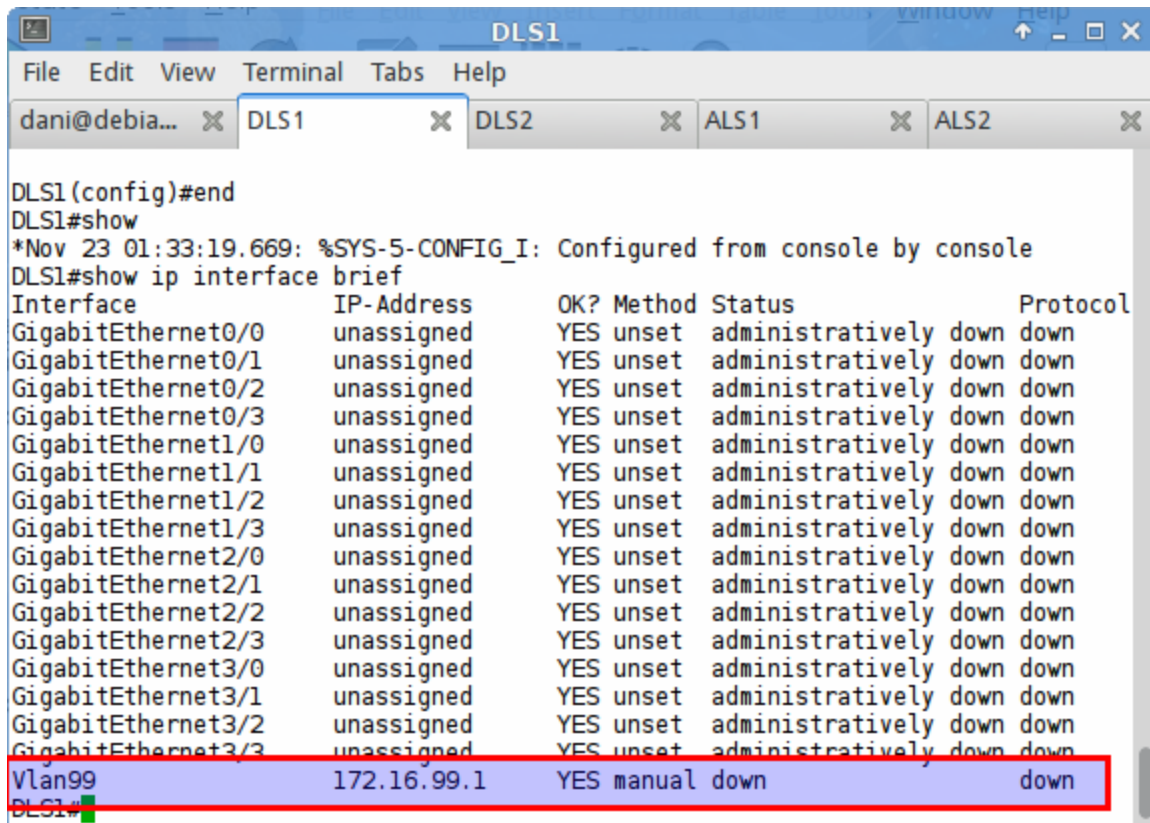
Enter basic configuration commands on each switch according to the diagram.

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 Layer 2 instance of the VLAN does not yet exist. This issue will be remedied in subsequent step

A continuación se muestra la que la configuración ingresada en el switch (DLS1 por ejemplo), ya ha tomado lugar. La correspondiente configuración se establece en los otros switches:



```
DLS1(config)#end
DLS1#show
*Nov 23 01:33:19.669: %SYS-5-CONFIG_I: Configured from console by console
DLS1#show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0       unassigned      YES unset  administratively down  down
GigabitEthernet0/1       unassigned      YES unset  administratively down  down
GigabitEthernet0/2       unassigned      YES unset  administratively down  down
GigabitEthernet0/3       unassigned      YES unset  administratively down  down
GigabitEthernet1/0       unassigned      YES unset  administratively down  down
GigabitEthernet1/1       unassigned      YES unset  administratively down  down
GigabitEthernet1/2       unassigned      YES unset  administratively down  down
GigabitEthernet1/3       unassigned      YES unset  administratively down  down
GigabitEthernet2/0       unassigned      YES unset  administratively down  down
GigabitEthernet2/1       unassigned      YES unset  administratively down  down
GigabitEthernet2/2       unassigned      YES unset  administratively down  down
GigabitEthernet2/3       unassigned      YES unset  administratively down  down
GigabitEthernet3/0       unassigned      YES unset  administratively down  down
GigabitEthernet3/1       unassigned      YES unset  administratively down  down
GigabitEthernet3/2       unassigned      YES unset  administratively down  down
GigabitEthernet3/3       unassigned      YES unset  administratively down  down
Vlan99                   172.16.99.1     YES manual down             down
```

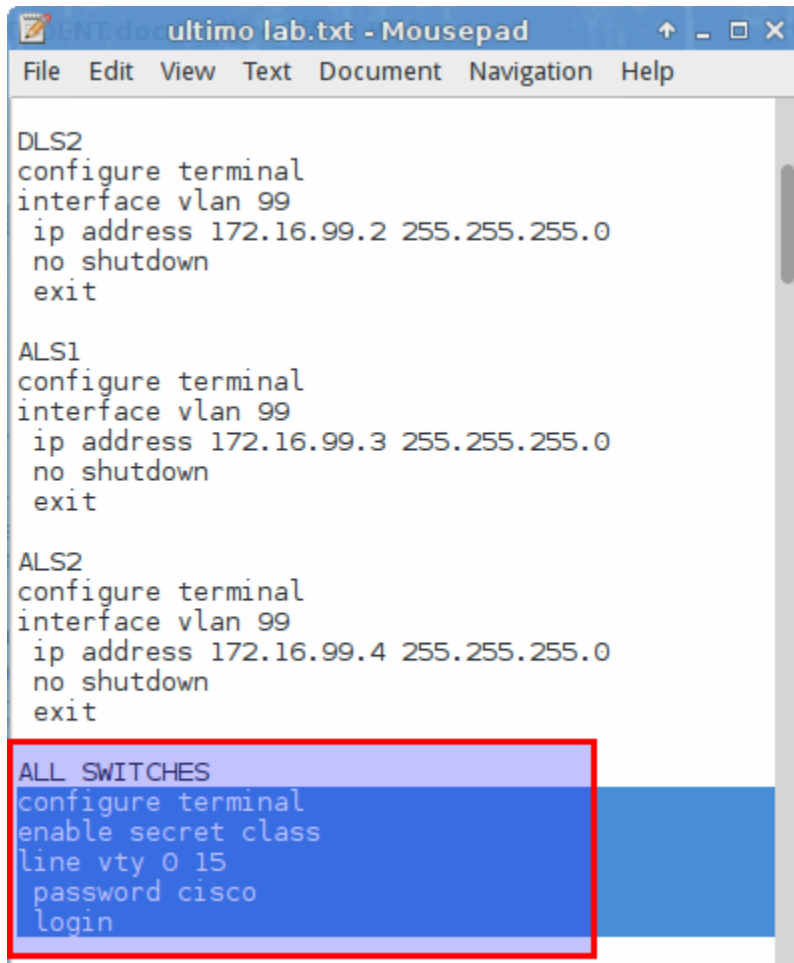
(Optional) On each switch, create an enable secret password and configure the VTY lines to allow remote access from other network devices.

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.

En la siguiente imagen puede apreciarse la configuración que será establecida en el switch:



```
DLS2
configure terminal
interface vlan 99
ip address 172.16.99.2 255.255.255.0
no shutdown
exit

ALS1
configure terminal
interface vlan 99
ip address 172.16.99.3 255.255.255.0
no shutdown
exit

ALS2
configure terminal
interface vlan 99
ip address 172.16.99.4 255.255.255.0
no shutdown
exit

ALL SWITCHES
configure terminal
enable secret class
line vty 0 15
password cisco
login
```

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:

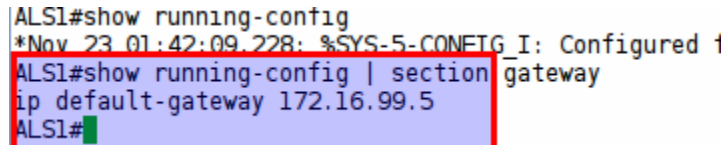
```
DLS1(config)# enable secret class
DLS1(config)# line vty 0 15
DLS1(config-line)# no login
DLS1(config-line)# privilege level 15
```

- a The access layer switches (ALS1 and ALS2) are Layer 2 devices and need a default gateway to send traffic outside of the local subnet. The distribution layer switches will not use a default gateway because they

are Layer 3 devices. Configure default gateways on the access layer switches. ***The HSRP virtual IP address 172.16.99.5 will be configured in subsequent steps.*

```
ALS1(config)# ip default-gateway 172.16.99.5
```

En la siguiente imagen puede verse que se ha configurado la puerta de enlace para ALS1:



```
ALS1#show running-config
*Nov 23 01:42:09.228: %SYS-5-CONFIG I: Configured 1
ALS1#show running-config | section gateway
ip default-gateway 172.16.99.5
ALS1#
```

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.

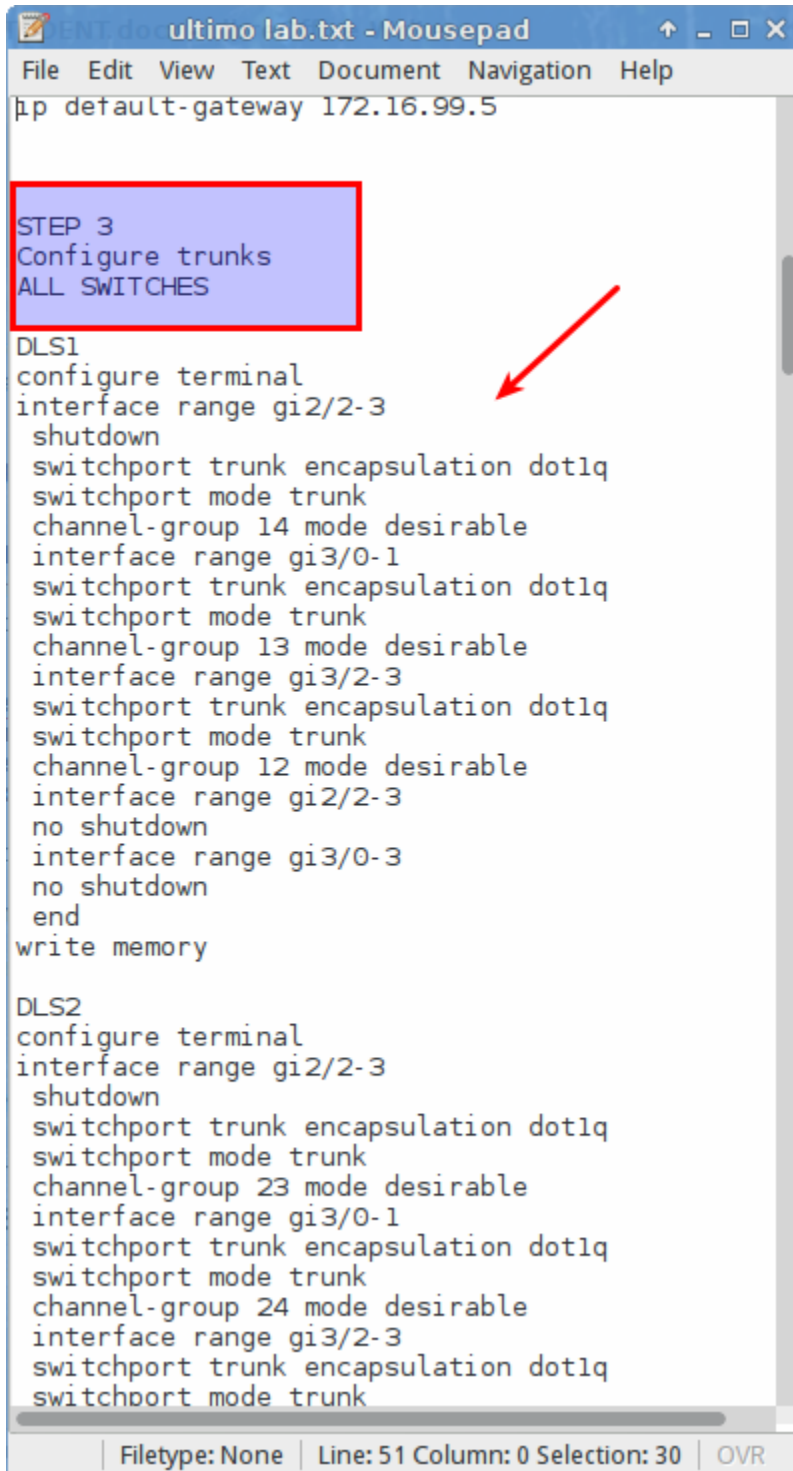
Note: It is good practice to shut down the interfaces on both sides of the link before a port channel is created and then re-enable them after the port channel is configured.

- a Configure trunks and EtherChannels from DLS1 and DLS2 to the other three switches according to the diagram. The **switchport trunk encapsulation {isl | dot1q}** command is used because these switches also support ISL encapsulation. A sample configuration is provided. Not all of the commands listed below will be used on all devices. Repeat and reference chapter 2 labs if you still are having difficulty with implementing trunking between devices.

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

Note: Repeat configurations on the other three switches.

En esta imagen puede verse la configuración que se ingresará a los switches:



```
File Edit View Text Document Navigation Help
ip default-gateway 172.16.99.5

STEP 3
Configure trunks
ALL SWITCHES

DLS1
configure terminal
interface range gi2/2-3
shutdown
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 14 mode desirable
interface range gi3/0-1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 13 mode desirable
interface range gi3/2-3
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 12 mode desirable
interface range gi2/2-3
no shutdown
interface range gi3/0-3
no shutdown
end
write memory

DLS2
configure terminal
interface range gi2/2-3
shutdown
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 23 mode desirable
interface range gi3/0-1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 24 mode desirable
interface range gi3/2-3
switchport trunk encapsulation dot1q
switchport mode trunk
```

Filetype: None | Line: 51 Column: 0 Selection: 30 | OVR

- a. Verify trunking between DLS1, ALS1, and ALS2 using the **show interface trunk** command on all switches.

A continuación, se muestra que se han configurado adecuadamente los enlaces troncales:

The image displays three terminal windows, each representing a different switch in a network. Each window has a title bar with the switch name (DLS1, DLS2, or ALS2) and a menu bar with options like File, Edit, View, Terminal, Tabs, and Help. Below the menu bar is a toolbar with various icons. The terminal content shows the user 'dani@debia...' and the switch prompt. The command 'show interfaces trunk' is entered, and the output is displayed as a table with columns: Port, Mode, Encapsulation, Status, and Native vlan.

DLS1 Terminal:

```
DLS1#
DLS1#
DLS1#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Po12	on	802.1q	trunking	1
Po13	on	802.1q	trunking	1
Po14	on	802.1q	trunking	1

DLS2 Terminal:

```
DLS2#
DLS2#
DLS2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Po12	on	802.1q	trunking	1
Po24	on	802.1q	trunking	1
Po23	on	802.1q	trunking	1

ALS2 Terminal:

```
el24, changed state to up
ALS2#
ALS2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Po34	on	802.1q	trunking	1
Po24	on	802.1q	trunking	1
Po14	on	802.1q	trunking	1

```

ALS1#
ALS1#
ALS1#show interfaces trunk

Port      Mode          Encapsulation  Status        Native vlan
-----
Po34      on            802.1q         trunking      1
Po13      on            802.1q         trunking      1
Po23      on            802.1q         trunking      1

```

b. Verify the EtherChannel configuration

Se emite el comando “show etherchannel summary” para comprobar el estado de la agregación de enlaces, en este caso en DLS1, como se aprecia en la imagen:

```

DLS1#show etherchannel summary

H - Hot-standby (LACP only)
R - Layer3
S - Layer2
U - in use      N - not in use, no aggregation
f - failed to allocate aggregator

M - not in use, minimum links not met
m - not in use, port not aggregated due to minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

A - formed by Auto LAG

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----
12     Po12(SU)      PAgP        Gi3/2(P)   Gi3/3(P)
13     Po13(SU)      PAgP        Gi3/0(P)   Gi3/1(P)
14     Po14(SU)      PAgP        Gi2/2(P)   Gi2/3(P)

```

c. Which EtherChannel negotiation protocol is in use here?

El protocolo que se está usando para agregación de enlaces es PAgP_____

Step 4: Configure VTP on DLS2, ALS1 and ALS2.

- b Change the VTP mode of ALS1 and ALS2 to *client* and VTP mode of DLS2 to *server*. A sample configuration is provided.

```
ALS1(config)# vtp mode client
```

Setting device to VTP CLIENT mode for VLANs.

- d. Verify the VTP changes.

Se muestra aquí la configuración que se estableció, en este caso el ejemplo es ALS2:

```
ALS2#
ALS2#
ALS2#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 1
VTP Domain Name          :
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0031.3661.b100
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision    : 0
MD5 digest                : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                          : 0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC

ALS2#
```

Step 5: Configure VTP on DLS1 and create VLANs.

- c Create the VTP domain on VTP server DLS1 and create VLANs 10, 20, 30, 40 and 99 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 SWLAB
```

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

```
DLS1(config)# vtp mode server
```

Setting device to VTP Server mode for VLANs

```
DLS1(config)# vlan 10
```

```

DLS1(config-vlan) # name Finance
DLS1(config-vlan) # vlan 20
DLS1(config-vlan) # name Engineering
DLS1(config-vlan) # vlan 30
DLS1(config-vlan) # name Server-Farm1
DLS1(config-vlan) # vlan 40
DLS1(config-vlan) # name Server-Farm2
DLS1(config-vlan) # vlan 99
DLS1(config-vlan) # name Management

```

Verify VLAN propagation across the SWLAB domain.

En la siguiente imagen puede verse la configuración que tomó DLS1 en cuanto a VTP:

```

DLS1#
DLS1#
DLS1#
DLS1#
DLS1#
DLS1#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : SWLAB
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 0031.3605.5500
Configuration last modified by 0.0.0.0 at 11-23-17 02:04:06
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 10
Configuration Revision   : 5
MD5 digest               : 0x38 0x03 0x7C 0xD0 0xD4 0x05 0xE1 0x59
                        : 0x8D 0x5B 0xB1 0xD2 0x67 0x9E 0x6B 0xF6
DLS1#

```

Y lo que recibió para VLANs:

```

DLS1
File Edit View Terminal Tabs Help
dani@debia... x DLS1 x DLS2 x ALS1 x ALS2 x
Configuration Revision: 5
MD5 digest: 0x38 0x03 0x7C 0xD0 0xD4 0x05 0xE1 0x59
              0x8D 0x5B 0xB1 0xD2 0x67 0x9E 0x6B 0xF6
DLS1#
*Nov 23 02:04:39.233: %LINK-3-UPDOWN: Interface Vlan99, changed state to up
*Nov 23 02:04:40.233: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
DLS1#show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
              Gi1/0, Gi1/1, Gi1/2, Gi1/3
              Gi2/0, Gi2/1
10   Finance                 active
20   Engineering             active
30   Server-Farm1            active
40   Server-Farm2            active
99   Management               active
1002 fddi-default             act/unsup
1003 trcrf-default          act/unsup
1004 fddinet-default         act/unsup
1005 trbrf-default          act/unsup
DLS1#

```

Step 6: Configure access ports.

- d Configure the host ports of all four switches. The following commands configure the switch port mode as access, place the port in the proper VLANs, and turn on spanning-tree PortFast for the ports. A sample configuration is provided for you.

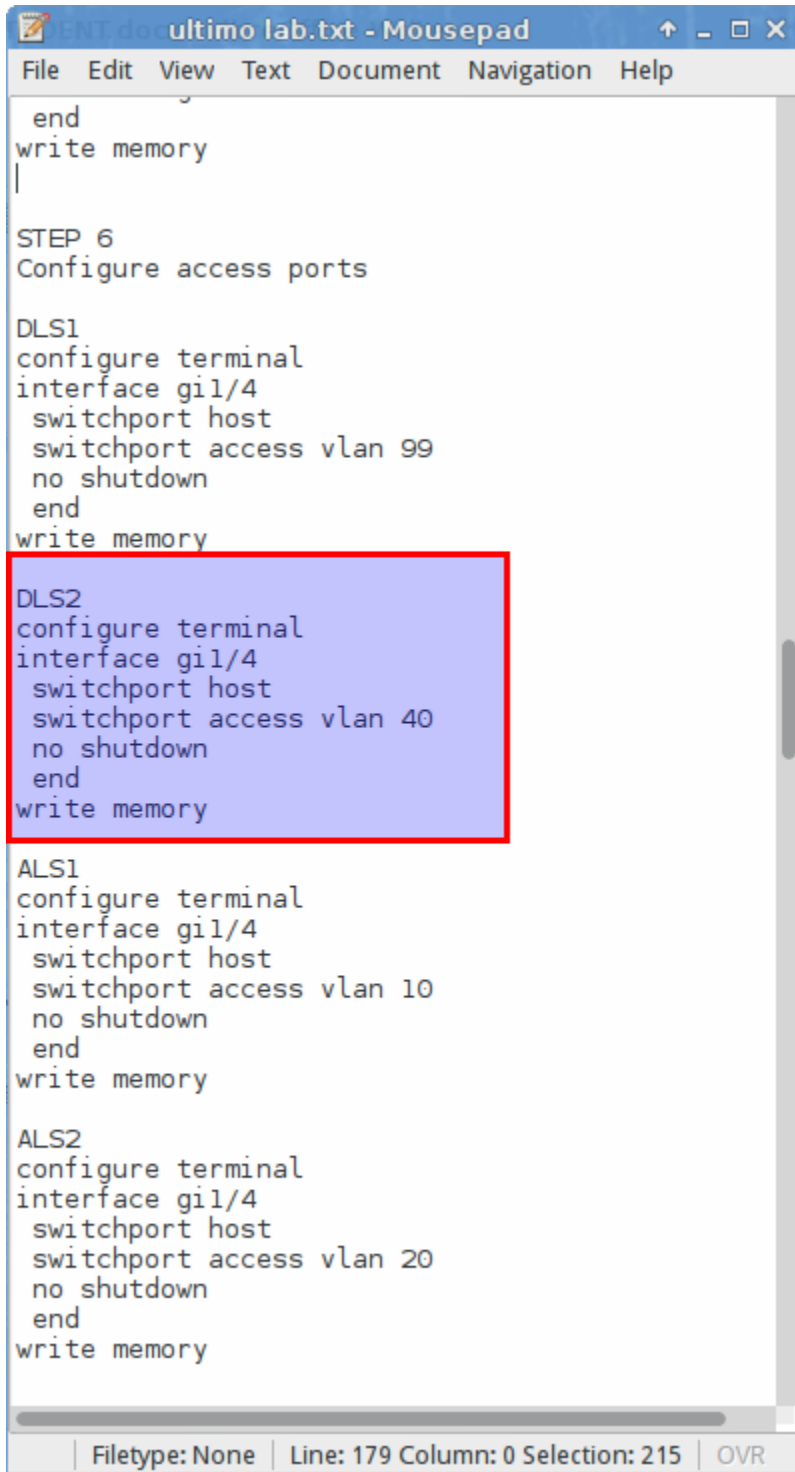
```

DLS2(config)# interface fastEthernet 0/6
DLS2(config-if)# switchport mode access
DLS2(config-if)# switchport access vlan 40
DLS2(config-if)# spanning-tree portfast
DLS2(config-if)# no shutdown

```

Note: The **switchport host** command can be used to configure individual access ports. This command automatically activates access mode, PortFast, and removes all associations of the physical switch port with the port-channel interfaces (if there are any).

En la siguiente imagen puede verse la configuración que se ingresó al puerto Gi1/3 en los switches, tomando en cuenta el switch DLS2:



```
end
write memory

STEP 6
Configure access ports

DLS1
configure terminal
interface gil/4
  switchport host
  switchport access vlan 99
  no shutdown
end
write memory

DLS2
configure terminal
interface gil/4
  switchport host
  switchport access vlan 40
  no shutdown
end
write memory

ALS1
configure terminal
interface gil/4
  switchport host
  switchport access vlan 10
  no shutdown
end
write memory

ALS2
configure terminal
interface gil/4
  switchport host
  switchport access vlan 20
  no shutdown
end
write memory
```

Filetype: None | Line: 179 Column: 0 Selection: 215 | OVR

- e Configure PC's with the IP addresses shown in the topology diagram. Use the address ending in .5 as the gateway address for the respective VLANs.

- e. Ping from the Host A (VLAN 10) to Host D (VLAN 40). The ping should fail.

Are these results expected at this point? Why?

El ping falla por que no existe un gateway asociado a los hosts para que sus paquetes puedan salir a otras redes. Además no está configurado un enrutamiento en los switches que permita a los paquetes ser trasladados de una red a otra.

Step 7: Configure HSRP interfaces and enable routing.

HSRP provides redundancy in the network. The traffic can be load-balanced by using the **standby group priority** command. The **ip routing** command is used on DLS1 and DLS2 to activate 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 group, 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. Notice that HSRP is not used in the command syntax to implement HSRP.

In the following configurations, the priority for VLANs 10, 20, and 99 is 150 on DLS1, making it the active router for those VLANs. VLANs 30 and 40 have the default priority of 100 on DLS1, making DLS1 the standby router for these VLANs. DLS2 is configured to be the active router for VLANs 30 and 40 with a priority of 150, and the standby router for VLANs 10, 20, and 99 with a default priority of 100.

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

```
DLS1(config)# ip routing
DLS1(config)# interface loopback 200
DLS1(config-if)# ip address 209.165.200.254 255.255.255.0
*NOTE: This loopback is used only for the purpose of testing HSRP
state changes. Both DLS1 and DLS2 will have this loopback configured.
```

```
DLS1(config)# interface vlan 99
DLS1(config-if)# ip address 172.16.99.1 255.255.255.0
DLS1(config-if)# standby 99 ip 172.16.99.5
DLS1(config-if)# standby 99 preempt
DLS1(config-if)# standby 99 priority 110
DLS1(config-if)# exit
```

```
DLS1(config)# interface vlan 10
DLS1(config-if)# ip address 172.16.10.1 255.255.255.0
DLS1(config-if)# standby 10 ip 172.16.10.5
DLS1(config-if)# standby 10 preempt
DLS1(config-if)# standby 10 priority 110
DLS1(config-if)# exit
```

```

DLS1(config)# interface vlan 20
DLS1(config-if)# ip address 172.16.20.1 255.255.255.0
DLS1(config-if)# standby 20 ip 172.16.20.5
DLS1(config-if)# standby 20 preempt
DLS1(config-if)# standby 20 priority 110
DLS1(config-if)# exit

DLS1(config)# interface vlan 30
DLS1(config-if)# ip address 172.16.30.1 255.255.255.0
DLS1(config-if)# standby 30 ip 172.16.30.5
DLS1(config-if)# standby 30 preempt
DLS1(config-if)# exit
*NOTE: When the priority command is not present on the L3 interface,
the HSRP priority value defaults to 100.

DLS1(config)# interface vlan 40
DLS1(config-if)# ip address 172.16.40.1 255.255.255.0
DLS1(config-if)# standby 40 ip 172.16.40.5
DLS1(config-if)# standby 40 preempt

DLS2(config)# ip routing

DLS1(config)# interface loopback 200
DLS1(config-if)# ip address 209.165.200.254 255.255.255.0
*NOTE: This loopback is used only for the purpose of testing HSRP
state changes. Both DLS1 and DLS2 will have this loopback configured.

DLS2(config)# interface vlan 99
DLS2(config-if)# ip address 172.16.99.2 255.255.255.0
DLS2(config-if)# standby 99 ip 172.16.99.5
DLS2(config-if)# standby 99 preempt
DLS2(config-if)# exit

DLS2(config)# interface vlan 10
DLS2(config-if)# ip address 172.16.10.2 255.255.255.0
DLS2(config-if)# standby 10 ip 172.16.10.5
DLS2(config-if)# standby 10 preempt
DLS2(config-if)# exit

DLS2(config)# interface vlan 20
DLS2(config-if)# ip address 172.16.20.2 255.255.255.0
DLS2(config-if)# standby 20 ip 172.16.20.5
DLS2(config-if)# standby 20 preempt
DLS2(config-if)# exit

DLS2(config)# interface vlan 30
DLS2(config-if)# ip address 172.16.30.2 255.255.255.0
DLS2(config-if)# standby 30 ip 172.16.30.5
DLS2(config-if)# standby 30 preempt
DLS2(config-if)# standby 30 priority 110
DLS2(config-if)# exit

```

```

DLS2(config)# interface vlan 40
DLS2(config-if)# ip address 172.16.40.2 255.255.255.0
DLS2(config-if)# standby 40 ip 172.16.40.5
DLS2(config-if)# standby 40 preempt
DLS2(config-if)# standby 40 priority 110

```

A continuación se muestra la configuración que será ingresada en los switches:

```

end
write memory|

STEP 7
Configure HSRP and Routing

DLS1
configure terminal
interface loopback 200
ip address 209.165.200.254 255.255.255.0
interface vlan 99
ip address 172.16.99.1 255.255.255.0
standby 99 ip 172.16.99.5
standby preempt
standby 99 priority 110
interface vlan 10
ip address 172.16.10.1 255.255.255.0
standby 10 ip 172.16.10.5
standby 10 preempt
standby 10 priority 110
interface vlan 20
ip address 172.16.20.1 255.255.255.0
standby 20 ip 172.16.20.5
standby 20 preempt
standby 20 priority 110
interface vlan 30
ip address 172.16.30.1 255.255.255.0
standby 30 ip 172.16.30.5
standby 30 preempt
interface vlan 40
ip address 172.16.40.1 255.255.255.0
standby 40 ip 172.16.40.5
standby 40 preempt
end
write memory

DLS2
ip routing
interface loopback 200
ip address 209.165.200.254 255.255.255.0
interface vlan 99
ip address 172.16.99.2 255.255.255.0
standby 99 ip 172.16.99.5

```

Filetype: None | Line: 218 Column: 12 | OVR

From Host A (VLAN 10) ping the HSRP virtual gateway address of 172.16.10.5.

```
C:\>ping 172.16.10.5
```

```
Pinging 172.16.10.5 with 32 bytes of data:
```

```
Reply from 172.16.10.5: bytes=32 time=1ms TTL=127
Reply from 172.16.10.5: bytes=32 time<1ms TTL=127
Reply from 172.16.10.5: bytes=32 time=1ms TTL=127
Reply from 172.16.10.5: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 172.16.10.5:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Now, start a continuous ping using the `-t` option to the loopback interface 209.165.200.254. The following is from Host A (VLAN 10) to the address 209.165.200.254. This continuous ping will be used to analyze the loss of connectivity experienced as result HSRP failover demonstration in coming in future steps.

```
C:\>ping 209.165.200.254 -t
```

```
Pinging 209.165.200.254 with 32 bytes of data:
```

```
Reply from 209.165.200.254: bytes=32 time=1ms TTL=127
Reply from 209.165.200.254: bytes=32 time<1ms TTL=127
Reply from 209.165.200.254: bytes=32 time=1ms TTL=127
Reply from 209.165.200.254: bytes=32 time<1ms TTL=127
<output omitted>
```

Aquí se puede ver la salida del comando ping en la estación cliente:

```

HostA> ping 172.16.10.1
84 bytes from 172.16.10.1 icmp_seq=1 ttl=255 time=3.815 ms
84 bytes from 172.16.10.1 icmp_seq=2 ttl=255 time=4.005 ms
^C
HostA> ping 172.16.10.5
84 bytes from 172.16.10.5 icmp_seq=1 ttl=255 time=2.178 ms
84 bytes from 172.16.10.5 icmp_seq=2 ttl=255 time=3.537 ms
84 bytes from 172.16.10.5 icmp_seq=3 ttl=255 time=3.916 ms
^C
HostA> ping 209.165.200.254
84 bytes from 209.165.200.254 icmp_seq=1 ttl=255 time=2.974 ms
84 bytes from 209.165.200.254 icmp_seq=2 ttl=255 time=4.400 ms
84 bytes from 209.165.200.254 icmp_seq=3 ttl=255 time=3.665 ms
84 bytes from 209.165.200.254 icmp_seq=4 ttl=255 time=2.500 ms
84 bytes from 209.165.200.254 icmp_seq=5 ttl=255 time=2.928 ms
HostA>

```

Step 8: Verify the HSRP configuration.

In the output below, the last two digits (XX) in the MAC address (0000.0c07.acXX) correspond with the HSRP group number. The MAC address is 0000.0c07.ac0a. The last two hexadecimal digits are 0a. These equate to decimal # 10. Our HSRP configuration is group 10.

- a Issue the **show standby** command on both DLS1 and DLS2.

```

DLS1# show standby
Vlan10 - Group 10
  State is Active
    2 state changes, last state change 00:01:36
  Virtual IP address is 172.16.10.5
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.560 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.10.2, priority 100 (expires in 10.704 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Vl10-10" (default)
Vlan20 - Group 20
  State is Active
    2 state changes, last state change 00:01:27

```

Note that both the active priority and configured priority are shown.
We configured the priority for this group at 150

```
Virtual IP address is 172.16.20.5
Active virtual MAC address is 0000.0c07.ac14
  Local virtual MAC address is 0000.0c07.ac14 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.192 secs
Preemption enabled
Active router is local
Standby router is 172.16.20.2, priority 100 (expires in 8.784 sec)
Priority 150 (configured 150)
Group name is "hsrp-Vl20-20" (default)
Vlan30 - Group 30
  State is Standby
    1 state change, last state change 00:01:10
  Virtual IP address is 172.16.30.5
  Active virtual MAC address is 0000.0c07.ac1e
    Local virtual MAC address is 0000.0c07.ac1e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.160 secs
  Preemption enabled
  Active router is 172.16.30.2, priority 150 (expires in 9.392 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl30-30" (default)
Vlan40 - Group 40
  State is Standby
    1 state change, last state change 00:01:37
  Virtual IP address is 172.16.40.5
  Active virtual MAC address is 0000.0c07.ac28
    Local virtual MAC address is 0000.0c07.ac28 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.624 secs
  Preemption enabled
  Active router is 172.16.40.2, priority 150 (expires in 7.920 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl40-40" (default)
Vlan99 - Group 99
  State is Active
    2 state changes, last state change 00:10:23
  Virtual IP address is 172.16.99.5
  Active virtual MAC address is 0000.0c07.ac63
    Local virtual MAC address is 0000.0c07.ac63 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.416 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.99.2, priority 100 (expires in 9.216 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Vl99-99" (default)
DLS1#
```

```
DLS2# show standby
```

Vlan10 - Group 10
State is Standby
1 state change, last state change 00:05:09
Virtual IP address is 172.16.10.5
Active virtual MAC address is 0000.0c07.ac0a
Local virtual MAC address is 0000.0c07.ac0a (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.488 secs
Preemption enabled
Active router is 172.16.10.1, priority 150 (expires in 8.624 sec)
Standby router is local
Priority 100 (default 100)
Group name is "hsrp-Vl10-10" (default)

Vlan20 - Group 20
State is Standby
1 state change, last state change 00:05:03
Virtual IP address is 172.16.20.5
Active virtual MAC address is 0000.0c07.ac14
Local virtual MAC address is 0000.0c07.ac14 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.336 secs
Preemption enabled
Active router is 172.16.20.1, priority 150 (expires in 8.640 sec)
Standby router is local
Priority 100 (default 100)
Group name is "hsrp-Vl20-20" (default)

Vlan30 - Group 30
State is Active
2 state changes, last state change 00:05:26
Virtual IP address is 172.16.30.5
Active virtual MAC address is 0000.0c07.ac1e
Local virtual MAC address is 0000.0c07.ac1e (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.416 secs
Preemption enabled
Active router is local
Standby router is 172.16.30.1, priority 100 (expires in 9.120 sec)
Priority 150 (configured 150)
Group name is "hsrp-Vl30-30" (default)

Vlan40 - Group 40
State is Active
2 state changes, last state change 00:12:58
Virtual IP address is 172.16.40.5
Active virtual MAC address is 0000.0c07.ac28
Local virtual MAC address is 0000.0c07.ac28 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.592 secs
Preemption enabled
Active router is local
Standby router is 172.16.40.1, priority 100 (expires in 8.800 sec)
Priority 150 (configured 150)
Group name is "hsrp-Vl40-40" (default)

```

Vlan99 - Group 99
  State is Standby
    1 state change, last state change 00:05:29
  Virtual IP address is 172.16.99.5
  Active virtual MAC address is 0000.0c07.ac63
    Local virtual MAC address is 0000.0c07.ac63 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.112 secs
  Preemption enabled
  Active router is 172.16.99.1, priority 150 (expires in 11.408 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl99-99" (default)
DLS2#

```

- b 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
Vl10      10   150 P Active  local   172.16.10.2
172.16.10.5
Vl20      20   150 P Active  local   172.16.20.2
172.16.20.5
Vl30      30   100 P Standby 172.16.30.2  local
172.16.30.5
Vl40      40   100  Standby 172.16.40.2  local
172.16.40.5
Vl99      99   150 P Active  local   172.16.99.2
172.16.99.5

```

```

DLS2# sh stand bri
                P indicates configured to preempt.
                |
Interface  Grp  Pri P State  Active  Standby  Virtual
IP
Vl10      10   100 P Standby 172.16.10.1  local
172.16.10.5
Vl20      20   100 P Standby 172.16.20.1  local
172.16.20.5
Vl30      30   150 P Active  local   172.16.30.1
172.16.30.5
Vl40      40   150 P Active  local   172.16.40.1
172.16.40.5
Vl99      99   100 P Standby 172.16.99.1  local
172.16.99.5

```

Ahora se presenta la salida del comando "show standby brief" en los switchces de distribución:


```

DLS1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DLS1(config)#ip routi
DLS1(config)#ip routin
DLS1(config)#ip routing
DLS1(config)#show standby brief
^
% Invalid input detected at '^' marker.

DLS1(config)#end
DLS1#show standb
*Nov 23 03:19:21.698: %SYS-5-CONFIG_I: Configured from console by console
DLS1#show standby brief
                P indicates configured to preempt.
                |
Interface    Grp  Pri P State    Active        Standby        Virtual IP
Vl10         10   110 P Active   local         172.16.10.2    172.16.10.5
Vl20         20   110 P Active   local         172.16.20.2    172.16.20.5
Vl30         30   100 P Standby  172.16.30.2   local          172.16.30.5
Vl40         40   100 P Standby  172.16.40.2   local          172.16.40.5
Vl99         99   110 Active    local         172.16.99.2    172.16.99.5
DLS1#

```

```
DLS2#
DLS2#
DLS2#conf g
% Invalid input detected at '^' marker.

DLS2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DLS2(config)#ip routing
DLS2(config)#ip routing
DLS2(config)#end
DLS2#show standb
*Nov 23 03:19:33.499: %SYS-5-CONFIG_I: Configured from console by console
DLS2#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State      Active        Standby        Virtual IP
Vl10       10   100  P Standby    172.16.10.1   local          172.16.10.5
Vl20       20   100  P Standby    172.16.20.1   local          172.16.20.5
Vl30       30   110  P Active     local         172.16.30.1   172.16.30.5
Vl40       40   110  P Active     local         172.16.40.1   172.16.40.5
Vl99       99   100  Standby    172.16.99.1   local          172.16.99.5
DLS2#
```

Which router is the active router for VLANs 10, 20, and 99? Which is the active router for 30 and 40?

Para las VLANs 10, 20 y 99, el router activo es DLS1. Para las VLANs 30 y 40 el router activo es DLS2.

What is the default hello time for each VLAN? What is the default hold time?

El hello time por defecto es 3 segundos, el hold time es de 10 segundos

How is the active HSRP router selected?

El router con mayor prioridad es el elegido.

- f. Use the **show ip route** command to verify routing on both DLS1 and DLS2.

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

172.16.0.0/16 is variably subnetted, 10 subnets, 2 masks

```

C      172.16.10.0/24 is directly connected, Vlan10
L      172.16.10.1/32 is directly connected, Vlan10
C      172.16.20.0/24 is directly connected, Vlan20
L      172.16.20.1/32 is directly connected, Vlan20
C      172.16.30.0/24 is directly connected, Vlan30
L      172.16.30.1/32 is directly connected, Vlan30
C      172.16.40.0/24 is directly connected, Vlan40
L      172.16.40.1/32 is directly connected, Vlan40
C      172.16.99.0/24 is directly connected, Vlan99
L      172.16.99.1/32 is directly connected, Vlan99
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.200.0/24 is directly connected, Loopback200
L      209.165.200.254/32 is directly connected, Loopback200
DLS1#

```

Aquí se muestra la tabla de enrutamiento de DLS1:

```

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

      172.16.0.0/16 is variably subnetted, 10 subnets, 2 masks
C      172.16.10.0/24 is directly connected, Vlan10
L      172.16.10.1/32 is directly connected, Vlan10
C      172.16.20.0/24 is directly connected, Vlan20
L      172.16.20.1/32 is directly connected, Vlan20
C      172.16.30.0/24 is directly connected, Vlan30
L      172.16.30.1/32 is directly connected, Vlan30
C      172.16.40.0/24 is directly connected, Vlan40
L      172.16.40.1/32 is directly connected, Vlan40
C      172.16.99.0/24 is directly connected, Vlan99
L      172.16.99.1/32 is directly connected, Vlan99
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.200.0/24 is directly connected, Loopback200
L      209.165.200.254/32 is directly connected, Loopback200
DLS1#

```

Step 9: Verify connectivity between VLANs.

Verify connectivity between VLANs using the **ping** command with a **-t** option from Host D (VLAN 40) to the other hosts and servers on the network. Keep the ping running to evaluate loss of connectivity that will occur in Step 11.

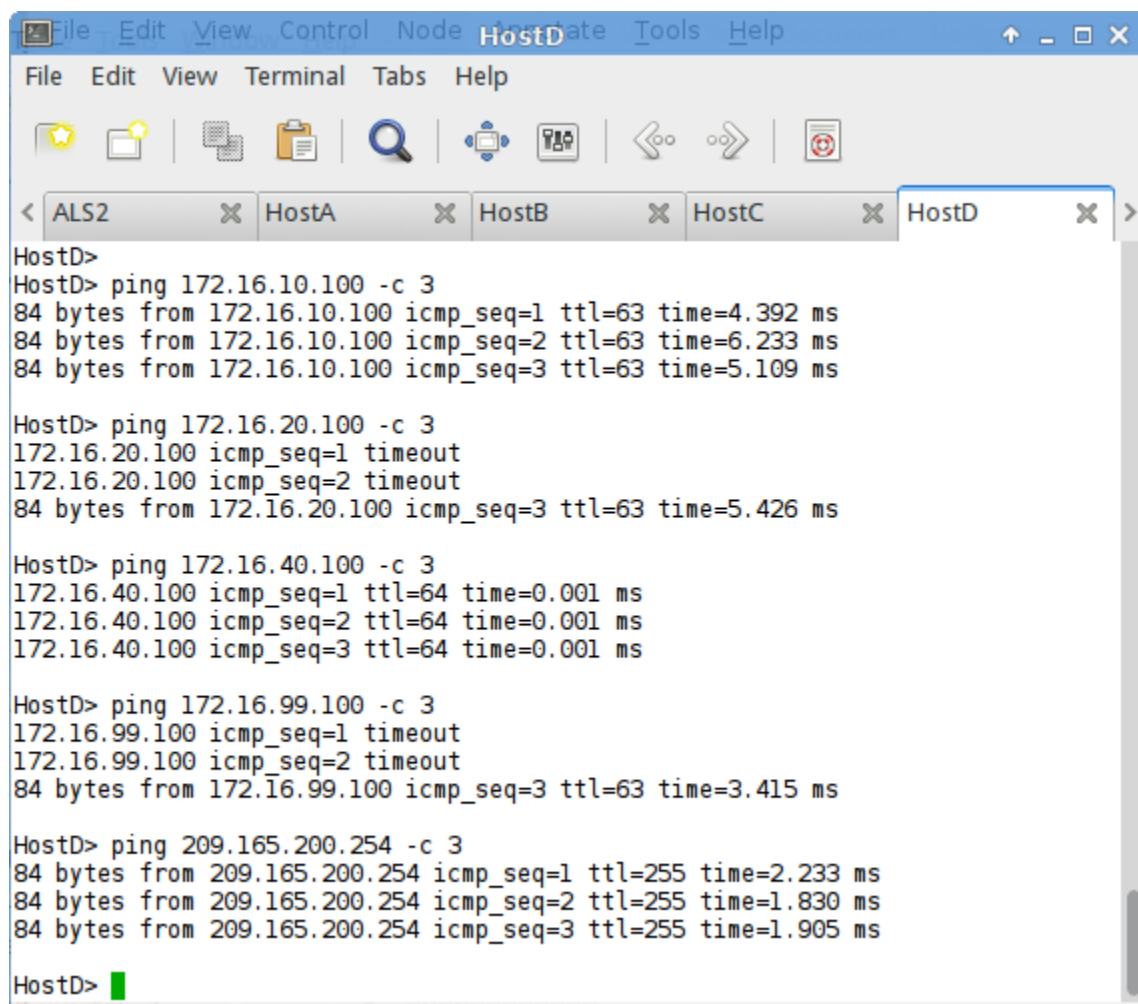
The following is from the Host D(VLAN 40) to the 209.165.200.254 address.

```
C:\>ping 209.165.200.254 -t
```

Pinging 209.165.200.254 with 32 bytes of data:

```
Reply from 209.165.200.254: bytes=32 time=1ms TTL=127
Reply from 209.165.200.254: bytes=32 time<1ms TTL=127
Reply from 209.165.200.254: bytes=32 time=1ms TTL=127
Reply from 209.165.200.254: bytes=32 time<1ms TTL=127
<output omitted>
```

Aquí se presenta la prueba de conectividad desde el HostD hacia los demás hosts:



```
File Edit View Control Node HostD State Tools Help
File Edit View Terminal Tabs Help
< ALS2 HostA HostB HostC HostD >
HostD>
HostD> ping 172.16.10.100 -c 3
84 bytes from 172.16.10.100 icmp_seq=1 ttl=63 time=4.392 ms
84 bytes from 172.16.10.100 icmp_seq=2 ttl=63 time=6.233 ms
84 bytes from 172.16.10.100 icmp_seq=3 ttl=63 time=5.109 ms

HostD> ping 172.16.20.100 -c 3
172.16.20.100 icmp_seq=1 timeout
172.16.20.100 icmp_seq=2 timeout
84 bytes from 172.16.20.100 icmp_seq=3 ttl=63 time=5.426 ms

HostD> ping 172.16.40.100 -c 3
172.16.40.100 icmp_seq=1 ttl=64 time=0.001 ms
172.16.40.100 icmp_seq=2 ttl=64 time=0.001 ms
172.16.40.100 icmp_seq=3 ttl=64 time=0.001 ms

HostD> ping 172.16.99.100 -c 3
172.16.99.100 icmp_seq=1 timeout
172.16.99.100 icmp_seq=2 timeout
84 bytes from 172.16.99.100 icmp_seq=3 ttl=63 time=3.415 ms

HostD> ping 209.165.200.254 -c 3
84 bytes from 209.165.200.254 icmp_seq=1 ttl=255 time=2.233 ms
84 bytes from 209.165.200.254 icmp_seq=2 ttl=255 time=1.830 ms
84 bytes from 209.165.200.254 icmp_seq=3 ttl=255 time=1.905 ms

HostD>
```

Step 10: Verify HSRP functionally.

- a. Verify HSRP by disconnecting the trunks to DLS2. You can simulate this using the **shutdown** command on those interfaces.

```
DLS2(config)# interface range fastEthernet 0/7 - 12
```

```
DLS2(config-if-range)# shutdown
```

Output to the console at DLS1 should reflect DLS1 becoming the active router for VLANs 30 and 40.

- g. Verify that DLS1 is acting as the backup default gateway for VLANs 30 and 40 using the **show standby brief** command. DLS1 is now the active HSRP router for all VLANs and the standby router is unknown.

```
DLS1# sh stand bri
```

```

                P indicates configured to preempt.
                |
Interface      Grp  Pri P State   Active           Standby           Virtual
IP
Vl10           10   150 P Active  local           unknown
172.16.10.5
Vl20           20   150 P Active  local           unknown
172.16.20.5
Vl30           30   100 P Active  local           unknown
172.16.30.5
Vl40           40   100   Active  local           unknown
172.16.40.5
Vl99           99   150 P Active  local           unknown
172.16.99.5
```

Aquí se aprecia el cambio de topología y el registro de acciones con el resultado sobre HSRP en DLS1:

```

C 172.16.30.0/24 is directly connected, Vlan30
L 172.16.30.1/32 is directly connected, Vlan30
C 172.16.40.0/24 is directly connected, Vlan40
L 172.16.40.1/32 is directly connected, Vlan40
C 172.16.99.0/24 is directly connected, Vlan99
L 172.16.99.1/32 is directly connected, Vlan99
C 209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
L 209.165.200.0/24 is directly connected, Loopback200
L 209.165.200.254/32 is directly connected, Loopback200
DLS1#
DLS1#
DLS1#show stand
*Nov 23 03:33:45.745: %HSRP-5-STATECHANGE: Vlan40 Grp 40 state Standby -> Activ
e
DLS1#show standby bre
*Nov 23 03:33:47.501: %HSRP-5-STATECHANGE: Vlan30 Grp 30 state Standby -> Activ
e
DLS1#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State  Active        Standby        Virtual IP
Vl10       10   110  P Active local        unknown       172.16.10.5
Vl20       20   110  P Active local        unknown       172.16.20.5
Vl30       30   100  P Active local        unknown       172.16.30.5
Vl40       40   100  P Active local        unknown       172.16.40.5
Vl99       99   110   Active local        unknown       172.16.99.5
DLS1#

```

Repeat this process by bringing up the DLS2 trunks and shutting down the DLS1 interfaces. Use the **show standby brief** command to see the results.

Note: If both 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.

Go back to Host A and Host D. The ping to 209.165.200.254 should still be running. Evaluate the loss of connectivity the hosts experienced during the HSRP state change. The users should experience minimal service disruption as a result of the HSRP state change.

Step 11: Apply HSRP authentication using MD5.

Now that we have successfully implemented default gateway redundancy in our network, we should think about securing the HSRP communication between member devices. HSRP authentication prevents rogue routers on the network from joining the HSRP group. Without authentication a rogue router could join the group and claim the active role. The attacker would then be able to capture all the traffic forwarded to attacker's device. HSRP authentication can be configured using plain text or MD5. MD5 is the preferred method. Using MD5 key, a hash is calculated on HSRP messages.

```
DLS1(config)# int vlan 10
DLS1(config-if)# standby 10 authentication ?

WORD   Plain text authentication string (8 chars max)
md5     Use MD5 authentication
text    Plain text authentication
```

```
DLS1(config-if)# standby 10 authentication md5 ?
key-chain Set key chain
key-string Set key string
```

With MD5 authentication, you can choose between a configuration using the key string or a key chain. Key chains offer more options and security because you can have lifetime parameters associated with the different keys. For simplicity, we will configure HSRP authentication using the key string option.

```
DLS1(config-if)# standby 10 authentication md5 key-string ?
0       Specifies an UNENCRYPTED key string will follow
7       Specifies a HIDDEN key string will follow
WORD    Key string (64 chars max)
```

```
DLS1(config-if)# standby 10 authentication md5 key-string cisco123
```

```
*Mar  1 22:22:34.315: %HSRP-4-BADAUTH: Bad authentication from
172.16.10.2, group 10, remote state Active
```

```
Building configuration...
Compressed configuration from 5405 bytes to 2494 bytes[OK]
*Nov 23 03:37:42.205: %SYS-5-CONFIG_I: Configured from console by console
*Nov 23 03:37:43.205: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updat
ed on disk. Please wait...
*Nov 23 03:37:43.236: %HSRP-4-BADAUTH: Bad authentication from 172.16.10.2, gro
up 10, remote state Standby
DLS1#
DLS1#
*Nov 23 03:37:43.862: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to
disk successfully.
DLS1#
```

Notice as soon as this command was entered on DLS1 that we received a “bad authentication” message display to the console screen. HSRP authentication is not yet configured on DLS2 therefore we expect for the HSRP process to be disrupted. The output of the **show standby brief** command below confirms that DLS2 is no longer the standby router for group 10. The standby router shows *unknown*.

```
DLS1# sh stand bri
```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl10	10	110	P	Active	local	unknown	
Vl20	20	110	P	Active	local	172.16.20.2	

Vl30	30	100	P	Standby	172.16.30.2	local
172.16.30.5						
Vl40	40	100		Standby	172.16.40.2	local
172.16.40.5						
Vl99	99	110	P	Active	local	172.16.99.2
172.16.99.5						

Ahora se muestran los pasos anteriores en DLS1:

```
DLS1#show standby brief
P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual IP
Vl10 10 110 P Active local unknown 172.16.10.5
Vl20 20 110 P Active local 172.16.20.2 172.16.20.5
Vl30 30 100 P Standby 172.16.30.2 local 172.16.30.5
Vl40 40 100 P Standby 172.16.40.2 local 172.16.40.5
Vl99 99 110 Active local 172.16.99.2 172.16.99.5
DLS1#
```

Now configure HSRP authentication for interface VLAN 10 on DLS2.

```
DLS2(config-if)# standby 10 authentication md5 key-string cisco123
```

```
*Mar 1 22:24:04.165: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active ->
Speak
```

```
*Mar 1 22:24:14.349: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak ->
Standby
```

Refer to the above output. Once the HSRP authentication with the correct key string were added to DLS2, the HSRP state changed.

Verify the HSRP status of VLAN 10 on DLS1 and DLS2. DLS1 should be the active router for VLAN 10 while DLS2 is the standby.

```
DLS1# sh stand bri
```

```
P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual IP
Vl10 10 110 P Active local 172.16.10.2 172.16.10.5
Vl20 20 110 P Active local 172.16.20.2 172.16.20.5
Vl30 30 100 P Standby 172.16.30.2 local 172.16.30.5
Vl40 40 100 Standby 172.16.40.2 local 172.16.40.5
Vl99 99 110 P Active local 172.16.99.2 172.16.99.5
```

```
DLS1#show standby brief
P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual IP
Vl10 10 110 P Active local 172.16.10.2 172.16.10.5
Vl20 20 110 P Active local 172.16.20.2 172.16.20.5
Vl30 30 100 P Standby 172.16.30.2 local 172.16.30.5
Vl40 40 100 P Standby 172.16.40.2 local 172.16.40.5
Vl99 99 110 Active local 172.16.99.2 172.16.99.5
DLS1#
```

Continue configuring HSRP authentication on the remaining HSRP groups used in this lab scenario.

CHALLENGE:

On one of the groups, implement HSRP authentication using a key chain instead of a key string.

Step 12: Configure HSRP interface tracking.

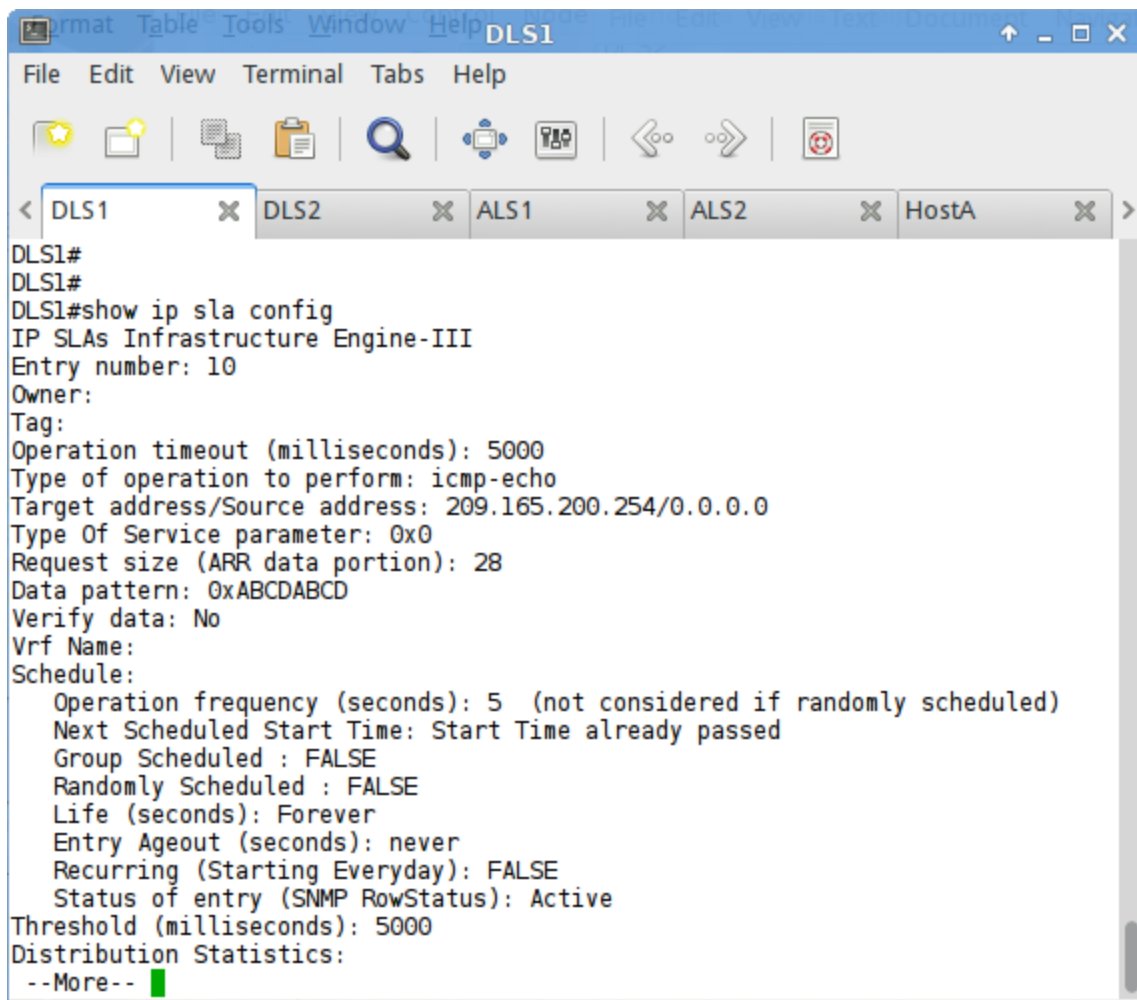
Interface tracking enables the priority of a standby group router to be automatically adjusted, based on the availability of the router interfaces. When a tracked interface becomes unavailable, the HSRP priority of the router is decreased. When properly configured, the HSRP tracking features ensures that a router with an unavailable key interface will relinquish the active router role.

Refer to the network topology, we will track availability to the 209.165.200.254 destination. Loopback 200 is configured with this address and is used for testing HSRP interface tracking concepts.

HSRP can perform object and interface tracking. Configure an IP SLA reachability test on DLS1. Also create an object that tracks this SLA test. HSRP will then be configured to track this object and decrease the priority by a value that will cause an HSRP state change.

```
DLS1# conf t
DLS1(config)# ip sla 10
DLS1(config-ip-sla)# icmp-echo 209.165.200.254
DLS1(config-ip-sla-echo)# frequency 5
DLS1(config-ip-sla-echo)# ip sla schedule 10 life forever start-time now
DLS1(config)# track 100 ip sla 10
DLS1(config)# int vlan 10
DLS1(config-if)# standby 10 track 100 decrement 70
DLS1(config-if)# exit
```

Verify SLA configuration using the **show ip sla configuration** and the **show ip sla statistics** command



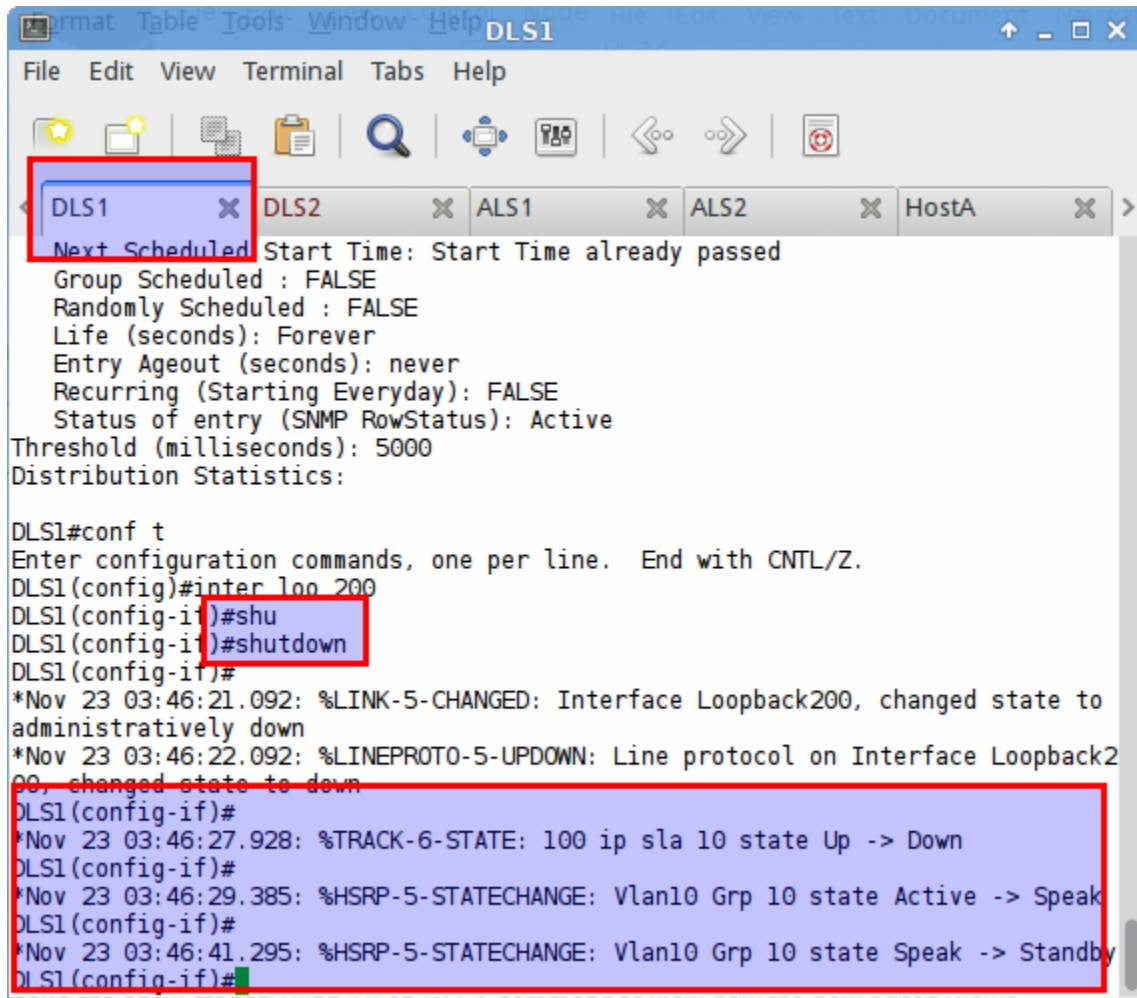
```
termat Table Tools Window Help DLS1
File Edit View Terminal Tabs Help
DLS1#
DLS1#
DLS1#show ip sla config
IP SLAs Infrastructure Engine-III
Entry number: 10
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 209.165.200.254/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Data pattern: 0xABCDABCD
Verify data: No
Vrf Name:
Schedule:
  Operation frequency (seconds): 5 (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:
--More--
```

Verify HSRP tracking configuration using the **show standby** command.

To test the HSRP tracked object, shut down the loopback 200 interface. Notice the messages displayed to console screen concerning the tracked object 10. More significantly, notice the HSRP state change that happened as a result of the failure of the SLA test.

```
DLS1(config)# int lo 200
DLS1(config-if)# shut
*Mar 1 23:29:32.072: %TRACKING-5-STATE: 1 interface Lo200 line-protocol
Up->Down
*Mar 1 23:29:34.077: %LINK-5-CHANGED: Interface Loopback200, changed
state to administratively down
*Mar 1 23:29:35.084: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Loopback200, changed state to down
*Mar 1 23:29:43.707: %TRACKING-5-STATE: 100 ip sla 10 state Up->Down
*Mar 1 23:29:46.207: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active ->
Speak
*Mar 1 23:29:57.691: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak ->
Standby
```

Puede verse aquí como la configuración del tracking, al recibir un cambio en el objeto hace que el estado de HSRP también se adecúe a este comportamiento:

A screenshot of a Cisco IOS terminal window titled 'DLS1'. The window shows the configuration of HSRP on interface Loopback200. The configuration includes setting the group to 10, the virtual IP to 172.16.10.2, and the priority to 110. A track object 100 is configured to track the state of interface Loopback200. The terminal output shows the state of the HSRP group changing from Active to Standby when the tracked interface goes down. The terminal text is as follows:

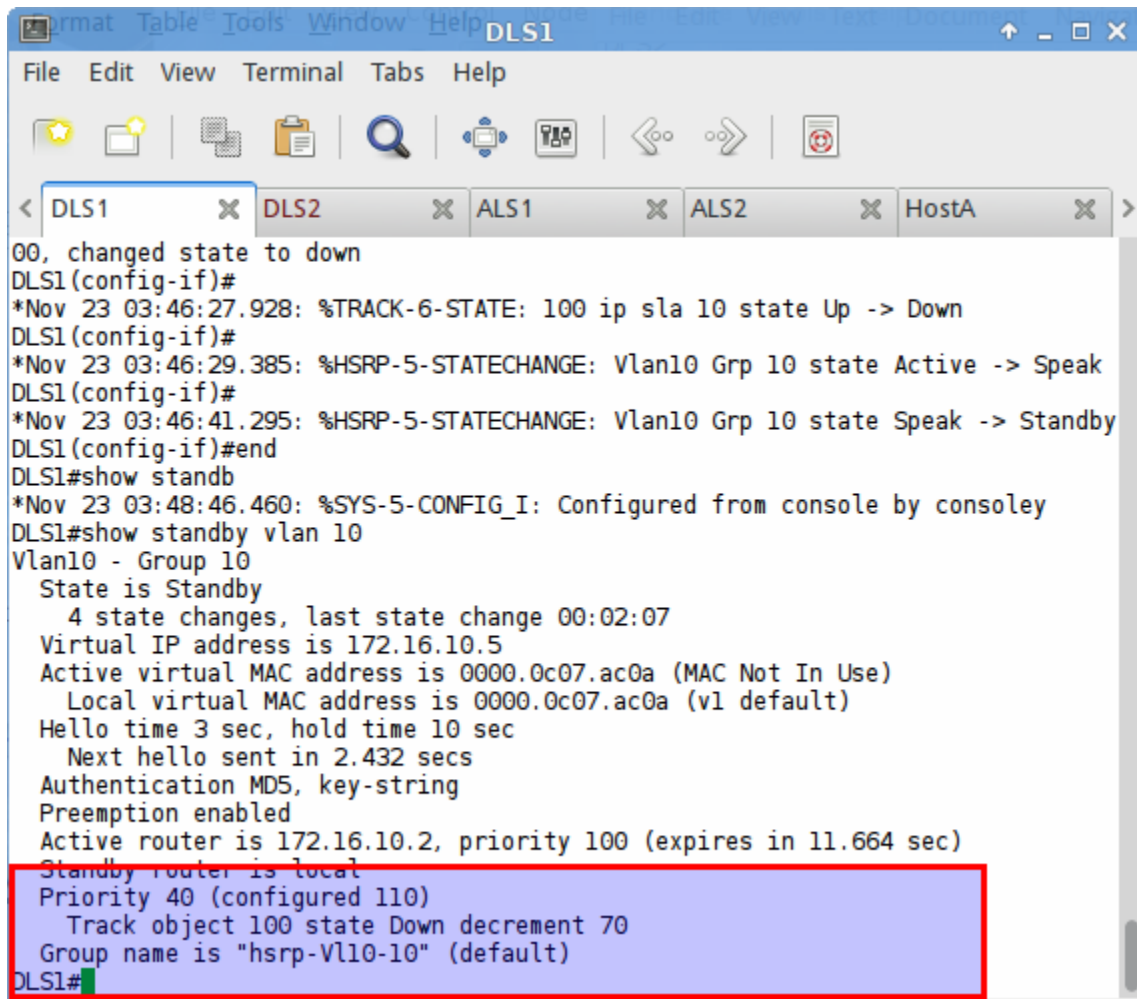
```
DLS1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DLS1(config)#inter loo 200
DLS1(config-if)#shu
DLS1(config-if)#shutdown
DLS1(config-if)#
*Nov 23 03:46:21.092: %LINK-5-CHANGED: Interface Loopback200, changed state to
administratively down
*Nov 23 03:46:22.092: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2
00, changed state to down
DLS1(config-if)#
*Nov 23 03:46:27.928: %TRACK-6-STATE: 100 ip sla 10 state Up -> Down
DLS1(config-if)#
*Nov 23 03:46:29.385: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active -> Speak
DLS1(config-if)#
*Nov 23 03:46:41.295: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
DLS1(config-if)#
```

Issue the show standby vlan 10 on DLS1 command to view how the new priority value.

```
DLS1# sh stand vlan 10
Vlan10 - Group 10
  State is Standby
    4 state changes, last state change 01:33:49
  Virtual IP address is 172.16.10.5
  Active virtual MAC address is 0000.0c07.ac0a
  Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.752 secs
  Authentication MD5, key-string
  Preemption enabled
  Active router is 172.16.10.2, priority 100 (expires in 9.488 sec)
  Standby router is local
  Priority 80 (configured 110)
  Track object 100 state Down decrement 30
```

Group name is "hsrp-Vl10-10" (default)

Ahora se ve el nuevo valor que recibió la configuración en HSRP:



```
DLS1
File Edit View Terminal Tabs Help
DLS1
DLS1(config-if)#
*Nov 23 03:46:27.928: %TRACK-6-STATE: 100 ip sla 10 state Up -> Down
DLS1(config-if)#
*Nov 23 03:46:29.385: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active -> Speak
DLS1(config-if)#
*Nov 23 03:46:41.295: %HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
DLS1(config-if)#end
DLS1#show standby
*Nov 23 03:48:46.460: %SYS-5-CONFIG_I: Configured from console by consoley
DLS1#show standby vlan 10
Vlan10 - Group 10
  State is Standby
    4 state changes, last state change 00:02:07
  Virtual IP address is 172.16.10.5
  Active virtual MAC address is 0000.0c07.ac0a (MAC Not In Use)
  Local virtual MAC address is 0000.0c07.ac0a (vl default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.432 secs
  Authentication MD5, key-string
  Preemption enabled
  Active router is 172.16.10.2, priority 100 (expires in 11.664 sec)
  Standby router is local
  Priority 40 (configured 110)
  Track object 100 state Down decrement 70
  Group name is "hsrp-Vl10-10" (default)
DLS1#
```

Part 1: Implement VRRP.

Background: Your company is merging with another company that does not have all Cisco devices deployed in their campus network. As a result, you need to change your first hop redundancy protocols from a proprietary solution to an industry standard solution. In preparation for the next phase of this lab, remove all HSRP configurations. Issuing the command `no standby [group #]` on the switched virtual interface (SVI) will remove all HSRP commands configured on that SVI.

In the next phase of this lab, we will use the Virtual Router Redundancy Protocol (VRRP). VRRP is an industry standard protocol that has many similarities to HSRP. HSRP elects an active and standby router to participate in the HSRP process, while VRRP elects a Master and Backup. Although referred to by different names, the operational concepts of the VRRP master and backup are similar to the HSRP active and standby respectively.

Both HSRP and VRRP operation requires the use of a virtual router IP address, but VRRP can use an address assigned to an interface on the device. In this case, the device automatically assumes the master role and ignores the priority value in its role election process. Recall that preemption in HSRP must be explicitly

configured. VRRP uses preempt by default. The next lab will demonstrate the commands necessary to run VRRP in a campus switched network.

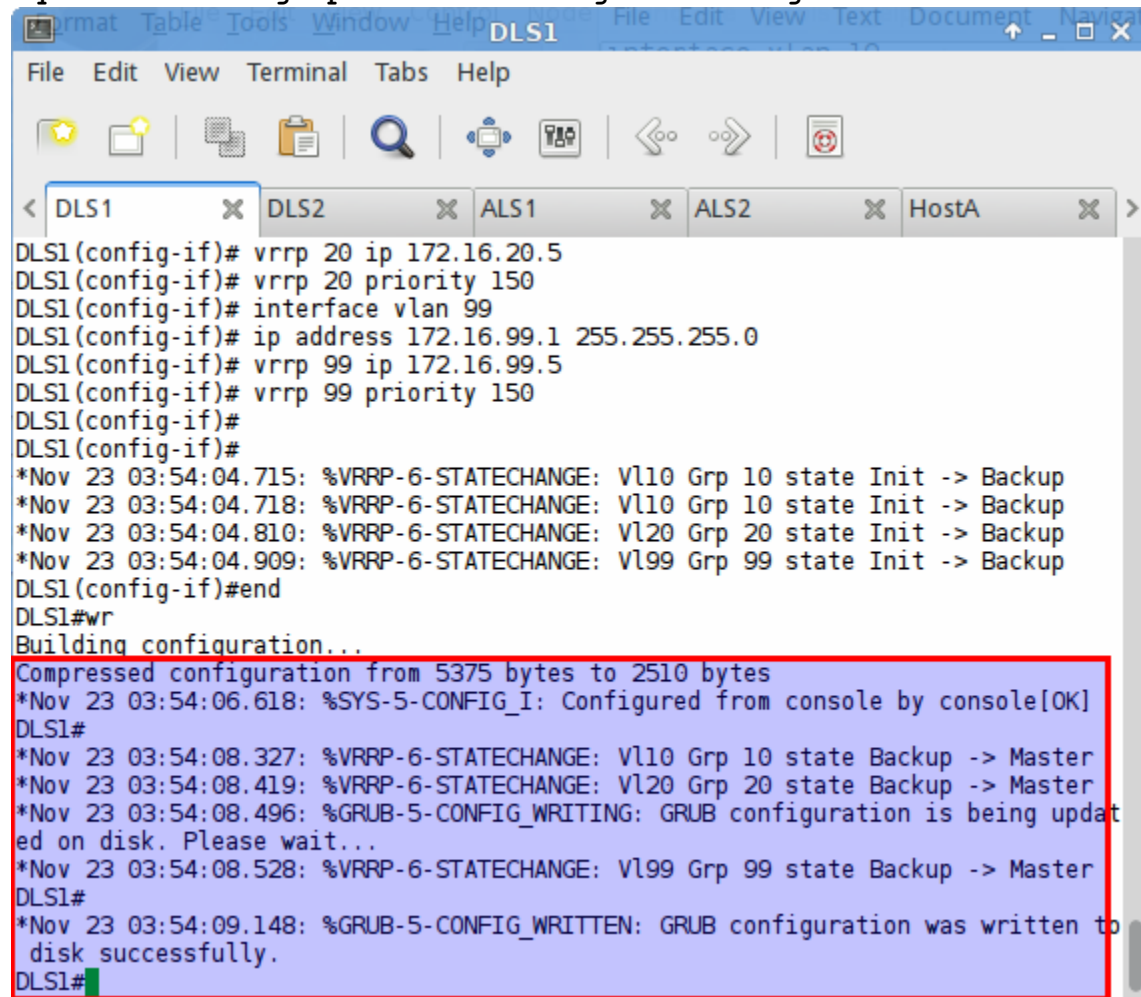
Step 1: Implement VRRP on DLS1 and DLS2.

Assign the VRRP protocol to the switched virtual interfaces. DLS1 will be the master for VLANs 10, 20, and 99. DLS2 will be the master for VLANs 30 and 40. The priority values *default* to 100, with a higher priority being preferred.

NOTE: The IP address shown in the example below has previously been configured in earlier steps of the lab. It is displayed here to show a complete configuration.

```
DLS1(config)# interface Vlan10
DLS1(config-if)# ip address 172.16.10.1 255.255.255.0
DLS1(config-if)# vrrp 10 ip 172.16.10.5
DLS1(config-if)# vrrp 10 priority 150
```

Aquí se ve un ejemplo de la configuración ingresada en DLS1:



```
DLS1
File Edit View Terminal Tabs Help
DLS1
DLS1(config-if)# vrrp 20 ip 172.16.20.5
DLS1(config-if)# vrrp 20 priority 150
DLS1(config-if)# interface vlan 99
DLS1(config-if)# ip address 172.16.99.1 255.255.255.0
DLS1(config-if)# vrrp 99 ip 172.16.99.5
DLS1(config-if)# vrrp 99 priority 150
DLS1(config-if)#
DLS1(config-if)#
*Nov 23 03:54:04.715: %VRRP-6-STATECHANGE: Vl10 Grp 10 state Init -> Backup
*Nov 23 03:54:04.718: %VRRP-6-STATECHANGE: Vl10 Grp 10 state Init -> Backup
*Nov 23 03:54:04.810: %VRRP-6-STATECHANGE: Vl20 Grp 20 state Init -> Backup
*Nov 23 03:54:04.909: %VRRP-6-STATECHANGE: Vl99 Grp 99 state Init -> Backup
DLS1(config-if)#end
DLS1#wr
Building configuration...
Compressed configuration from 5375 bytes to 2510 bytes
*Nov 23 03:54:06.618: %SYS-5-CONFIG_I: Configured from console by console[OK]
DLS1#
*Nov 23 03:54:08.327: %VRRP-6-STATECHANGE: Vl10 Grp 10 state Backup -> Master
*Nov 23 03:54:08.419: %VRRP-6-STATECHANGE: Vl20 Grp 20 state Backup -> Master
*Nov 23 03:54:08.496: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Nov 23 03:54:08.528: %VRRP-6-STATECHANGE: Vl99 Grp 99 state Backup -> Master
DLS1#
*Nov 23 03:54:09.148: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
DLS1#
```

*Only use the **vrrp x priority** command on the interfaces in which you desire this switch to be the master forwarder.

Repeat these commands as necessary to implement VRRP on all SVIs on DLS1 and DLS2 switches.

Verify VRRP operation using the following show commands: **show vrrp**. Ensure DLS1 is the master for VLANs 10, 20 and 99 and backup for VLANs 30 and 40, and DLS2 is the master for VLANs 30 and 40 and backup for VLANs 10, 20, and 99.

DLS1# **show vrrp**

Vlan10 - Group 10

State is Master

Virtual IP address is 172.16.10.5

Virtual MAC address is 0000.5e00.010a

Advertisement interval is 1.000 sec

Preemption enabled

Priority is 150

Master Router is 172.16.10.1 (local), priority is 150

Master Advertisement interval is 1.000 sec

Master Down interval is 3.414 sec

Vlan20 - Group 20

State is Master

Virtual IP address is 172.16.20.5

Virtual MAC address is 0000.5e00.0114

Advertisement interval is 1.000 sec

Preemption enabled

Priority is 150

Master Router is 172.16.20.1 (local), priority is 150

Master Advertisement interval is 1.000 sec

Master Down interval is 3.414 sec

Vlan30 - Group 30

State is Backup

Virtual IP address is 172.16.30.5

Virtual MAC address is 0000.5e00.011e

Advertisement interval is 1.000 sec

Preemption enabled

Priority is 100

Master Router is 172.16.30.2, priority is 150

Master Advertisement interval is 1.000 sec

Master Down interval is 3.609 sec (expires in 3.475 sec)

Vlan40 - Group 40

State is Backup

Virtual IP address is 172.16.40.5

Virtual MAC address is 0000.5e00.0128

Advertisement interval is 1.000 sec

Preemption enabled

Priority is 100

Master Router is 172.16.40.2, priority is 150

Master Advertisement interval is 1.000 sec

Master Down interval is 3.609 sec (expires in 2.930 sec)

Vlan99 - Group 99

```
State is Master
Virtual IP address is 172.16.99.5
Virtual MAC address is 0000.5e00.0163
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 150
Master Router is 172.16.99.1 (local), priority is 150
Master Advertisement interval is 1.000 sec
Master Down interval is 3.414 sec
```

View the **show vrrp** output on DLS2.

DLS2# **sh vrrp**

Vlan10 - Group 10

```
State is Backup
Virtual IP address is 172.16.10.5
Virtual MAC address is 0000.5e00.010a
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Master Router is 172.16.10.1, priority is 150
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec (expires in 3.097 sec)
```

Vlan20 - Group 20

```
State is Backup
Virtual IP address is 172.16.20.5
Virtual MAC address is 0000.5e00.0114
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
Master Router is 172.16.20.1, priority is 150
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec (expires in 2.736 sec)
```

Vlan30 - Group 30

```
State is Master
Virtual IP address is 172.16.30.5
Virtual MAC address is 0000.5e00.011e
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 150
Master Router is 172.16.30.2 (local), priority is 150
Master Advertisement interval is 1.000 sec
Master Down interval is 3.414 sec
```

Vlan40 - Group 40

```
State is Master
Virtual IP address is 172.16.40.5
```


Virtual MAC address is 0000.5e00.0128
 Advertisement interval is 1.000 sec
 Preemption enabled
 Priority is 150
 Master Router is 172.16.40.2 (local), priority is 150
 Master Advertisement interval is 1.000 sec
 Master Down interval is 3.414 sec

Vlan99 - Group 99
 State is Backup
 Virtual IP address is 172.16.99.5
 Virtual MAC address is 0000.5e00.0163
 Advertisement interval is 1.000 sec
 Preemption enabled
 Priority is 100
 Master Router is 172.16.99.1, priority is 150
 Master Advertisement interval is 1.000 sec
 Master Down interval is 3.609 sec (expires in 3.206 sec)

You can also use the **show vrrp brief** command to view a summary of the VRRP configuration.

DLS1# **show vrrp brief**

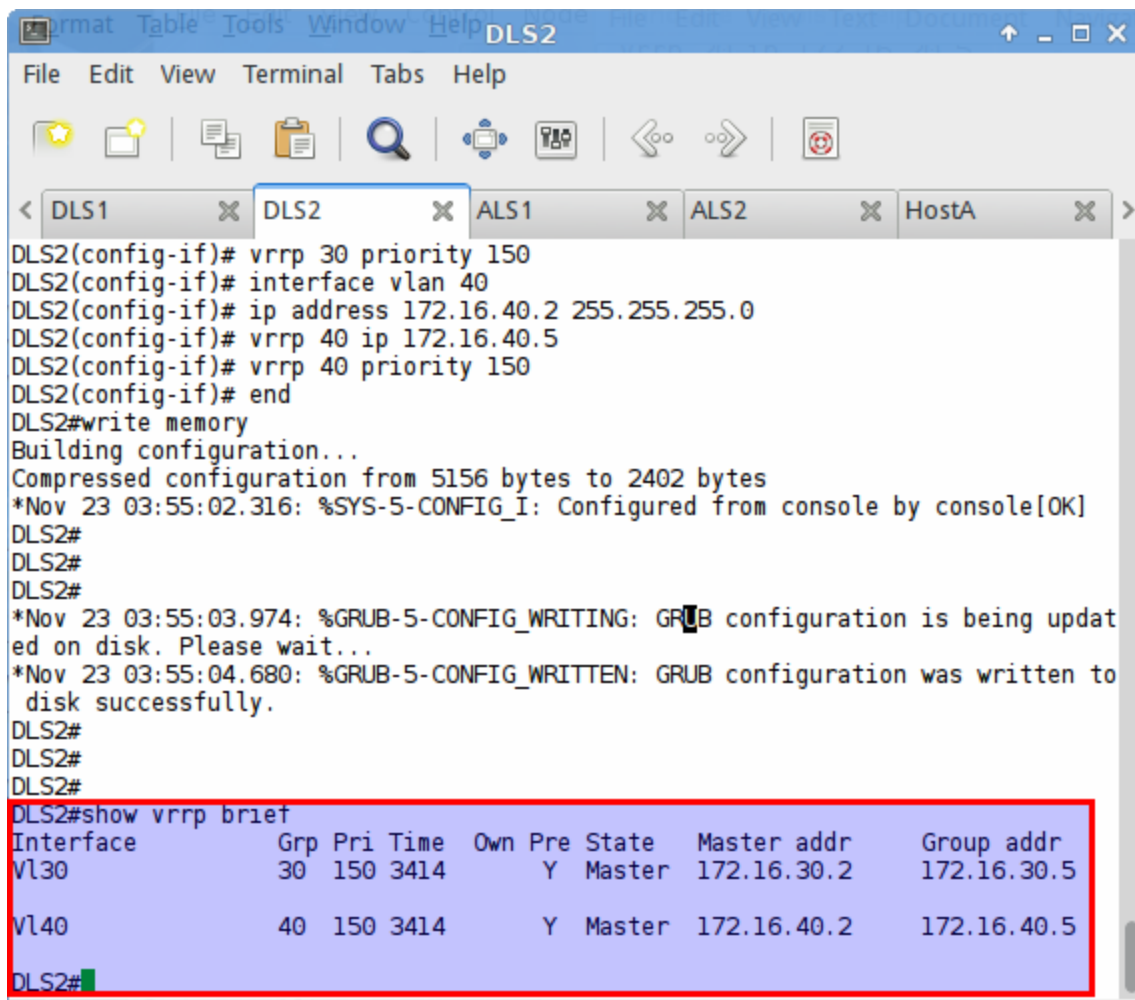
Interface addr	Grp	Pri	Time	Own	Pre	State	Master addr	Group
Vl10 172.16.10.5	10	150	3414		Y	Master	172.16.10.1	
Vl20 172.16.20.5	20	150	3414		Y	Master	172.16.20.1	
Vl30 172.16.30.5	30	100	3609		Y	Backup	172.16.30.2	
Vl40 172.16.40.5	40	100	3609		Y	Backup	172.16.40.2	
Vl99 172.16.99.5	99	150	3414		Y	Master	172.16.99.1	

DLS2# **show vrrp brief**

Interface addr	Grp	Pri	Time	Own	Pre	State	Master addr	Group
Vl10 172.16.10.5	10	100	3609		Y	Backup	172.16.10.1	
Vl20 172.16.20.5	20	100	3609		Y	Backup	172.16.20.1	
Vl30 172.16.30.5	30	150	3414		Y	Master	172.16.30.2	
Vl40 172.16.40.5	40	150	3414		Y	Master	172.16.40.2	
Vl99 172.16.99.5	99	100	3609		Y	Backup	172.16.99.1	

Ahora, se muestra el comando `"show vrrp brief"` en DLS1 y DLS2:

```
ermat Table Tools Window Help DLS1
File Edit View Terminal Tabs Help
[Icons]
< DLS1 x DLS2 x ALS1 x ALS2 x HostA x >
*Nov 23 03:54:04.715: %VRRP-6-STATECHANGE: Vl10 Grp 10 state Init -> Backup
*Nov 23 03:54:04.718: %VRRP-6-STATECHANGE: Vl10 Grp 10 state Init -> Backup
*Nov 23 03:54:04.810: %VRRP-6-STATECHANGE: Vl20 Grp 20 state Init -> Backup
*Nov 23 03:54:04.909: %VRRP-6-STATECHANGE: Vl99 Grp 99 state Init -> Backup
DLS1(config-if)#end
DLS1#wr
Building configuration...
Compressed configuration from 5375 bytes to 2510 bytes
*Nov 23 03:54:06.618: %SYS-5-CONFIG_I: Configured from console by console[OK]
DLS1#
*Nov 23 03:54:08.327: %VRRP-6-STATECHANGE: Vl10 Grp 10 state Backup -> Master
*Nov 23 03:54:08.419: %VRRP-6-STATECHANGE: Vl20 Grp 20 state Backup -> Master
*Nov 23 03:54:08.496: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Nov 23 03:54:08.528: %VRRP-6-STATECHANGE: Vl99 Grp 99 state Backup -> Master
DLS1#
*Nov 23 03:54:09.148: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
DLS1#show vrrp brief
Interface      Grp Pri Time  Own Pre State  Master addr  Group addr
Vl10           10  150 3414      Y Master 172.16.10.1  172.16.10.5
Vl20           20  150 3414      Y Master 172.16.20.1  172.16.20.5
Vl99           99  150 3414      Y Master 172.16.99.1  172.16.99.5
DLS1#
```

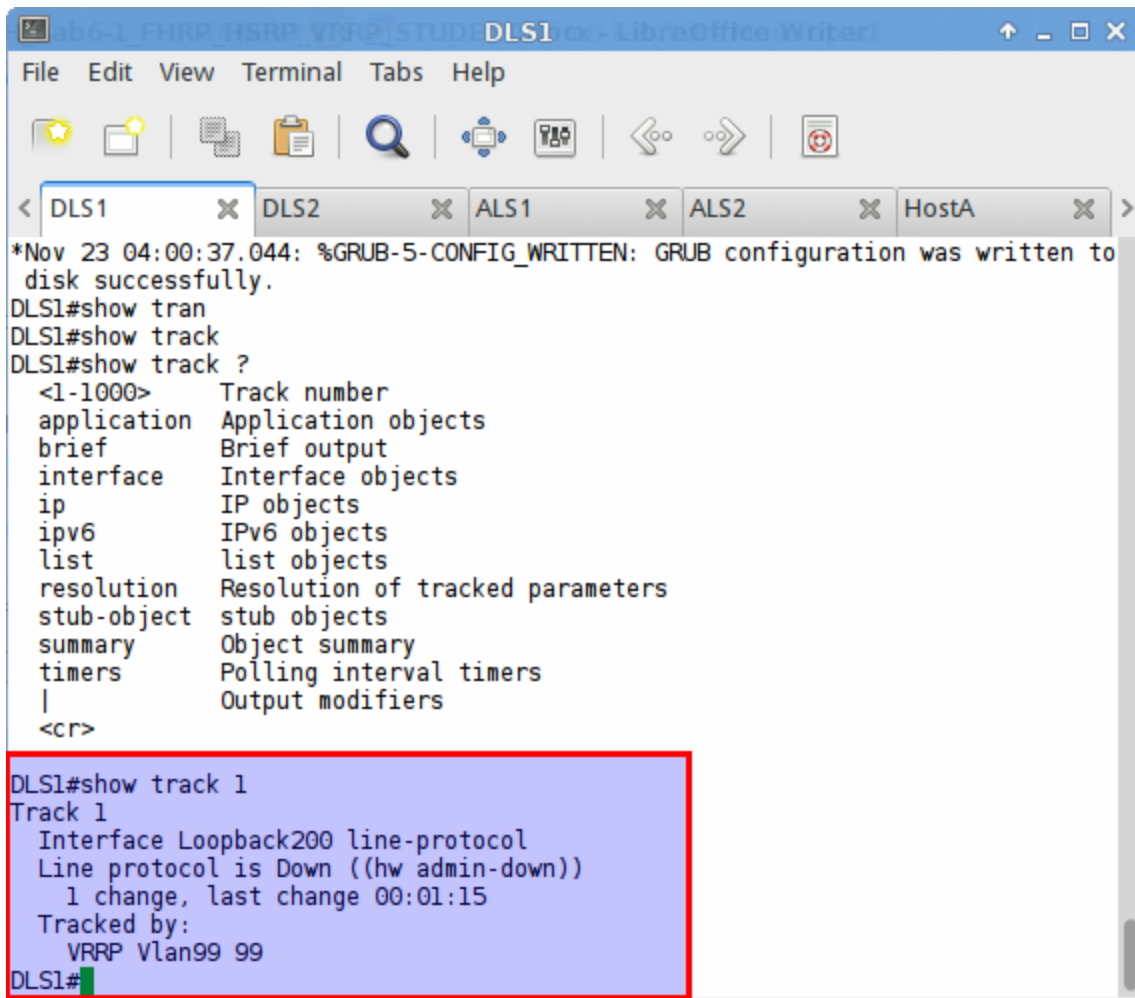


```
DLS2
DLS2(config-if)# vrrp 30 priority 150
DLS2(config-if)# interface vlan 40
DLS2(config-if)# ip address 172.16.40.2 255.255.255.0
DLS2(config-if)# vrrp 40 ip 172.16.40.5
DLS2(config-if)# vrrp 40 priority 150
DLS2(config-if)# end
DLS2#write memory
Building configuration...
Compressed configuration from 5156 bytes to 2402 bytes
*Nov 23 03:55:02.316: %SYS-5-CONFIG_I: Configured from console by console[OK]
DLS2#
DLS2#
DLS2#
*Nov 23 03:55:03.974: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Nov 23 03:55:04.680: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
DLS2#
DLS2#
DLS2#
DLS2#show vrrp brief
Interface          Grp Pri Time   Own Pre State   Master addr   Group addr
Vl30                30  150 3414      Y Master 172.16.30.2   172.16.30.5
Vl40                40  150 3414      Y Master 172.16.40.2   172.16.40.5
DLS2#
```

Step 2: Configure VRRP tracking.

As you may recall from earlier, HSRP can perform interface tracking and object tracking. VRRP can only perform object tracking. As with the HSRP scenario, we are simulating connectivity to the 209.165.200.254 address in the cloud. Create an object that tracks the line protocol status of the interface loopback 200 with this address. Once the object is created, configure VRRP to track the object and to decrease the priority to a value that would cause a state change between the Master and Backup devices. Recall that we configured the priority values to 150 on the Master devices. The Backup devices priority defaults to 100. To cause the state change, we would need to decrease the priority by at least 60. A sample configuration is provided for you below.

```
DLS1(config)# track 1 int loop 200 line-protocol
DLS1(config-track)# int vlan 99
DLS1(config-if)# vrrp 99 track 1 decrement 60
```



```
*Nov 23 04:00:37.044: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to
disk successfully.
DLS1#show tran
DLS1#show track
DLS1#show track ?
<1-1000> Track number
application Application objects
brief Brief output
interface Interface objects
ip IP objects
ipv6 IPv6 objects
list list objects
resolution Resolution of tracked parameters
stub-object stub objects
summary Object summary
timers Polling interval timers
| Output modifiers
<cr>

DLS1#show track 1
Track 1
Interface Loopback200 line-protocol
Line protocol is Down ((hw admin-down))
  1 change, last change 00:01:15
Tracked by:
  VRRP Vlan99 99
DLS1#
```

CHALLENGE:

Step 3: Alternative option for VRRP configuration

Remove the VRRP commands from the interfaces and implement VRRP using the IP addresses assigned to the SVIs.

NOTE: The IP addresses shown in the examples below have previously been configured in earlier steps of the lab. They are displayed here to show a complete configuration.

- On DLS1, configure VRRP using the IP addresses assigned to interfaces VLAN 10 as the virtual router IP. A sample configuration is provided for you below.

- Do not configure the VRRP priority.

```
DLS1(config)# interface Vlan10
DLS1(config-if)# ip address 172.16.10.1 255.255.255.0
DLS1(config-if)# vrrp 10 ip 172.16.10.1
```

- On DLS2, use the IP address assigned to interfaces VLAN 30.

```
DLS2(config)# interface Vlan30
```

```
DLS2(config-if) # ip address 172.16.30.2 255.255.255.0
DLS2(config-if) # vrrp 10 ip 172.16.30.2
```

- Observe VRRP results. DLS1 should automatically become the Master for VLAN 10 and Backup for VLAN 30.
- DLS2 should become the Master for VLAN 30 and become the backup for VLAN 10.

Step 3: End of Lab

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

Device Configurations:

Below are the final configurations for each switch.

DLS1:

```
DLS1# show run | exclude !
Building configuration...

Current configuration : 3392 bytes
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname DLS1
boot-start-marker
boot-end-marker
enable secret 5 $1$iH7y$KmmPyHeHJXQezv2wRIctX/
no aaa new-model
system mtu routing 1500
ip routing
no ip domain-lookup
ip domain-name CCNP.NET
key chain HSRP-CHAIN
  key 1
    key-string cisco456
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
track 1 interface Loopback200 line-protocol
track 100 ip sla 10
interface Loopback200
  ip address 209.165.200.254 255.255.255.0
interface Port-channel1
  switchport trunk encapsulation dot1q
  switchport mode trunk
interface Port-channel2
  switchport trunk encapsulation dot1q
  switchport mode trunk
interface Port-channel3
  switchport trunk encapsulation dot1q
```

```
    switchport mode trunk
interface FastEthernet0/1
    shutdown
interface FastEthernet0/2
    shutdown
interface FastEthernet0/3
    shutdown
interface FastEthernet0/4
    shutdown
interface FastEthernet0/5
    shutdown
interface FastEthernet0/6
    switchport access vlan 99
    switchport mode access
    spanning-tree portfast
interface FastEthernet0/7
    switchport trunk encapsulation dot1q
    switchport mode trunk
    channel-group 1 mode desirable
interface FastEthernet0/8
    switchport trunk encapsulation dot1q
    switchport mode trunk
    channel-group 1 mode desirable
interface FastEthernet0/9
    switchport trunk encapsulation dot1q
    switchport mode trunk
    channel-group 2 mode desirable
interface FastEthernet0/10
    switchport trunk encapsulation dot1q
    switchport mode trunk
    channel-group 2 mode desirable
interface FastEthernet0/11
    switchport trunk encapsulation dot1q
    switchport mode trunk
    channel-group 3 mode desirable
interface FastEthernet0/12
    switchport trunk encapsulation dot1q
    switchport mode trunk
    channel-group 3 mode desirable
interface FastEthernet0/13
    shutdown
interface FastEthernet0/14
    shutdown
interface FastEthernet0/15
    shutdown
interface FastEthernet0/16
    shutdown
interface FastEthernet0/17
    shutdown
interface FastEthernet0/18
    shutdown
interface FastEthernet0/19
    shutdown
interface FastEthernet0/20
    shutdown
interface FastEthernet0/21
    shutdown
```

```

interface FastEthernet0/22
 shutdown
interface FastEthernet0/23
 shutdown
interface FastEthernet0/24
 shutdown
interface GigabitEthernet0/1
 shutdown
interface GigabitEthernet0/2
 shutdown
interface Vlan1
 no ip address
 shutdown
interface Vlan10
 ip address 172.16.10.1 255.255.255.0
 vrrp 10 ip 172.16.10.5
 vrrp 10 priority 150
interface Vlan20
 ip address 172.16.20.1 255.255.255.0
 vrrp 20 ip 172.16.20.5
 vrrp 20 priority 150
interface Vlan30
 ip address 172.16.30.1 255.255.255.0
 vrrp 30 ip 172.16.30.5
interface Vlan40
 ip address 172.16.40.1 255.255.255.0
 vrrp 40 ip 172.16.40.5
interface Vlan99
 ip address 172.16.99.1 255.255.255.0
 vrrp 99 ip 172.16.99.5
 vrrp 99 priority 150
 vrrp 99 track 1 decrement 60
ip http server
ip http secure-server
ip sla 10
 icmp-echo 209.165.200.254
 frequency 5
ip sla schedule 10 life forever start-time now
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
end

DLS1#

```

DLS2:

```

DLS2# show run | exclude !
Building configuration...

```



```
Current configuration : 3175 bytes
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname DLS2
boot-start-marker
boot-end-marker
enable secret 5 $1$FN15$.TMOHwkzsahidv1ZImuBP0
no aaa new-model
system mtu routing 1500
ip routing
no ip domain-lookup
ip domain-name CCNP.NET
key chain HSRP-CHAIN
  key 1
    key-string cisco456
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
interface Loopback200
  ip address 209.165.200.254 255.255.255.0
interface Port-channel1
  switchport trunk encapsulation dot1q
  switchport mode trunk
interface Port-channel2
  switchport trunk encapsulation dot1q
  switchport mode trunk
interface Port-channel3
  switchport trunk encapsulation dot1q
  switchport mode trunk
interface FastEthernet0/1
  shutdown
interface FastEthernet0/2
  shutdown
interface FastEthernet0/3
  shutdown
interface FastEthernet0/4
  shutdown
interface FastEthernet0/5
  shutdown
interface FastEthernet0/6
  switchport access vlan 40
  switchport mode access
  spanning-tree portfast
interface FastEthernet0/7
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 1 mode desirable
interface FastEthernet0/8
  switchport trunk encapsulation dot1q
  switchport mode trunk
  channel-group 1 mode desirable
interface FastEthernet0/9
  switchport trunk encapsulation dot1q
  switchport mode trunk
```

```

    channel-group 2 mode desirable
interface FastEthernet0/10
    switchport trunk encapsulation dot1q
    switchport mode trunk
    channel-group 2 mode desirable
interface FastEthernet0/11
    switchport trunk encapsulation dot1q
    switchport mode trunk
    channel-group 3 mode desirable
interface FastEthernet0/12
    switchport trunk encapsulation dot1q
    switchport mode trunk
    channel-group 3 mode desirable
interface FastEthernet0/13
    shutdown
interface FastEthernet0/14
    shutdown
interface FastEthernet0/15
    shutdown
interface FastEthernet0/16
    shutdown
interface FastEthernet0/17
    shutdown
interface FastEthernet0/18
    shutdown
interface FastEthernet0/19
    shutdown
interface FastEthernet0/20
    shutdown
interface FastEthernet0/21
    shutdown
interface FastEthernet0/22
    shutdown
interface FastEthernet0/23
    shutdown
interface FastEthernet0/24
    shutdown
interface GigabitEthernet0/1
    shutdown
interface GigabitEthernet0/2
    shutdown
interface Vlan1
    no ip address
    shutdown
interface Vlan10
    ip address 172.16.10.2 255.255.255.0
    vrrp 10 ip 172.16.10.5
interface Vlan20
    ip address 172.16.20.2 255.255.255.0
    vrrp 20 ip 172.16.20.5
interface Vlan30
    ip address 172.16.30.2 255.255.255.0
    vrrp 30 ip 172.16.30.5
    vrrp 30 priority 150
interface Vlan40
    ip address 172.16.40.2 255.255.255.0
    vrrp 40 ip 172.16.40.5

```

```

    vrrp 40 priority 150
interface Vlan99
    ip address 172.16.99.2 255.255.255.0
    vrrp 99 ip 172.16.99.5
ip http server
ip http secure-server
line con 0
    exec-timeout 0 0
    logging synchronous
line vty 0 4
    password cisco
    login
line vty 5 15
    password cisco
    login
end

DLS2#

```

ALS1:

```

ALS1# show run | exclude !
Building configuration...

Current configuration : 2302 bytes
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname ALS1
boot-start-marker
boot-end-marker
enable secret 5 $1$XhgA$UgBJw/pOfDf.5XeSWE3Sw0
no aaa new-model
system mtu routing 1500
no ip domain-lookup
ip domain-name CCNP.NET
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
interface Port-channel1
    switchport mode trunk
interface Port-channel2
    switchport mode trunk
interface Port-channel3
    switchport mode trunk
interface FastEthernet0/1
    shutdown
interface FastEthernet0/2
    shutdown
interface FastEthernet0/3
    shutdown
interface FastEthernet0/4
    shutdown
interface FastEthernet0/5

```

```

shutdown
interface FastEthernet0/6
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
interface FastEthernet0/7
  switchport mode trunk
  channel-group 1 mode desirable
interface FastEthernet0/8
  switchport mode trunk
  channel-group 1 mode desirable
interface FastEthernet0/9
  switchport mode trunk
  channel-group 2 mode desirable
interface FastEthernet0/10
  switchport mode trunk
  channel-group 2 mode desirable
interface FastEthernet0/11
  switchport mode trunk
  channel-group 3 mode desirable
interface FastEthernet0/12
  switchport mode trunk
  channel-group 3 mode desirable
interface FastEthernet0/13
  shutdown
interface FastEthernet0/14
  shutdown
interface FastEthernet0/15
  shutdown
interface FastEthernet0/16
  shutdown
interface FastEthernet0/17
  shutdown
interface FastEthernet0/18
  shutdown
interface FastEthernet0/19
  shutdown
interface FastEthernet0/20
  shutdown
interface FastEthernet0/21
  shutdown
interface FastEthernet0/22
  shutdown
interface FastEthernet0/23
  shutdown
interface FastEthernet0/24
  shutdown
interface GigabitEthernet0/1
  shutdown
interface GigabitEthernet0/2
  shutdown
interface Vlan1
  no ip address
interface Vlan99
  ip address 172.16.99.3 255.255.255.0
  ip default-gateway 172.16.99.5
  ip http server

```

```
ip http secure-server
line con 0
  exec-timeout 0 0
  logging synchronous
line vty 0 4
  password cisco
  login
line vty 5 15
  password cisco
  login
end
```

ALS1#

ALS2:

```
ALS2# show run | exclude !
Building configuration...
```

```
Current configuration : 2312 bytes
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname ALS2
boot-start-marker
boot-end-marker
enable secret 5 $1$p6PN$sW8CgvvOPVCkyhezwxB720
no aaa new-model
system mtu routing 1500
no ip domain-lookup
ip domain-name CCNP.NET
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
interface Port-channel1
  switchport mode trunk
interface Port-channel2
  switchport mode trunk
interface Port-channel3
  switchport mode trunk
interface FastEthernet0/1
  shutdown
interface FastEthernet0/2
  shutdown
interface FastEthernet0/3
  shutdown
interface FastEthernet0/4
  shutdown
interface FastEthernet0/5
  shutdown
interface FastEthernet0/6
  switchport access vlan 20
  switchport mode access
  spanning-tree portfast
```

```

interface FastEthernet0/7
  switchport mode trunk
  channel-group 1 mode desirable
interface FastEthernet0/8
  switchport mode trunk
  channel-group 1 mode desirable
interface FastEthernet0/9
  switchport mode trunk
  channel-group 2 mode desirable
interface FastEthernet0/10
  switchport mode trunk
  channel-group 2 mode desirable
interface FastEthernet0/11
  switchport mode trunk
  channel-group 3 mode desirable
interface FastEthernet0/12
  switchport mode trunk
  channel-group 3 mode desirable
interface FastEthernet0/13
  shutdown
interface FastEthernet0/14
  shutdown
interface FastEthernet0/15
  shutdown
interface FastEthernet0/16
  shutdown
interface FastEthernet0/17
  shutdown
interface FastEthernet0/18
  shutdown
interface FastEthernet0/19
  shutdown
interface FastEthernet0/20
  shutdown
interface FastEthernet0/21
  shutdown
interface FastEthernet0/22
  shutdown
interface FastEthernet0/23
  shutdown
interface FastEthernet0/24
  shutdown
interface GigabitEthernet0/1
  shutdown
interface GigabitEthernet0/2
  shutdown
interface Vlan1
  no ip address
  shutdown
interface Vlan99
  ip address 172.16.99.4 255.255.255.0
ip default-gateway 172.16.99.5
ip http server
ip http secure-server
line con 0
  exec-timeout 0 0
  logging synchronous

```

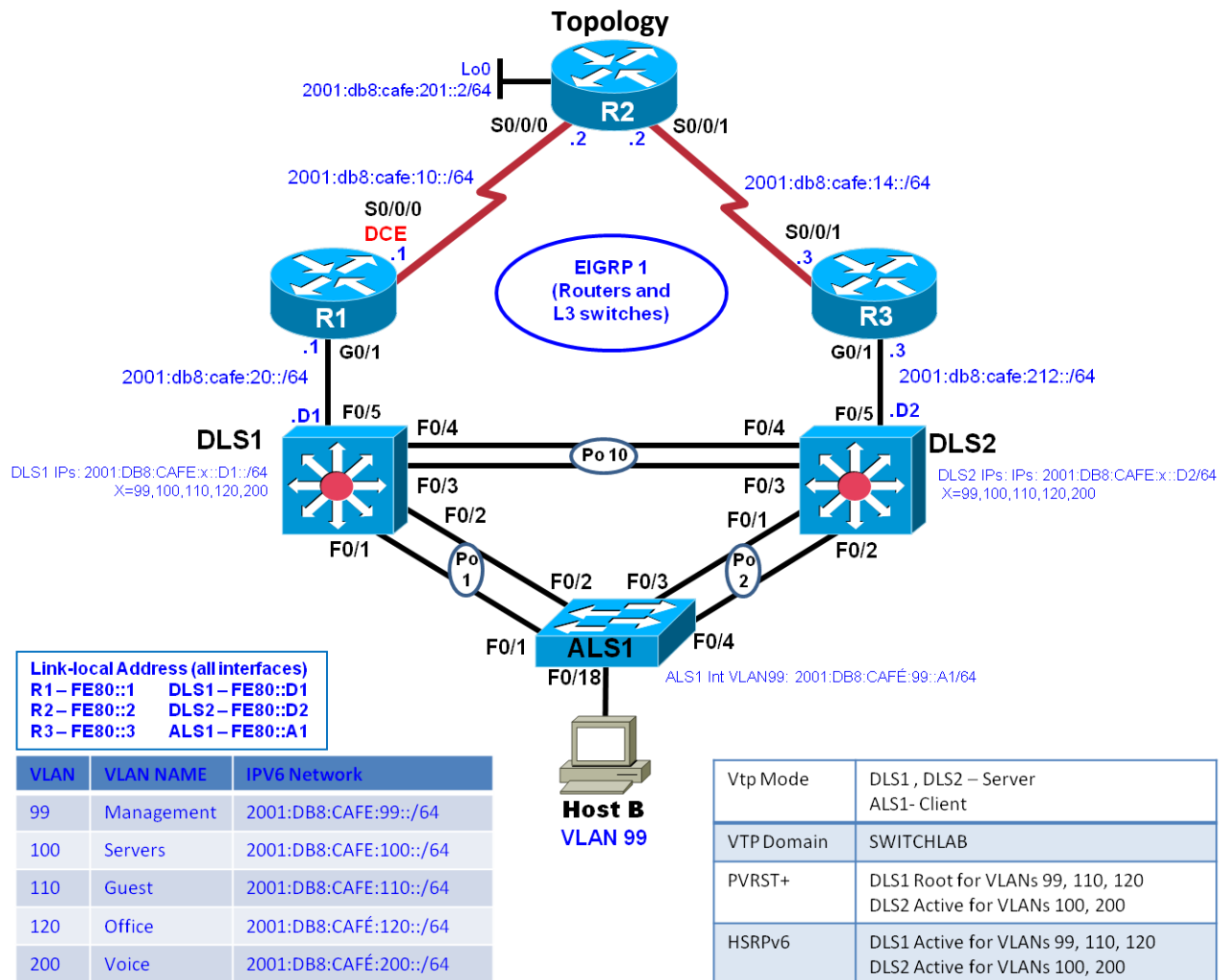
```

line vty 0 4
  password cisco
  login
line vty 5 15
  password cisco
  login
end

```

ALS2#

CCNPv7.1_SWITCH_Lab6-2_HSRPv6_STUDENT



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

Part 1: 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
ESTE COMANDO NO LO EJECUTA EL PKT V.7
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
```

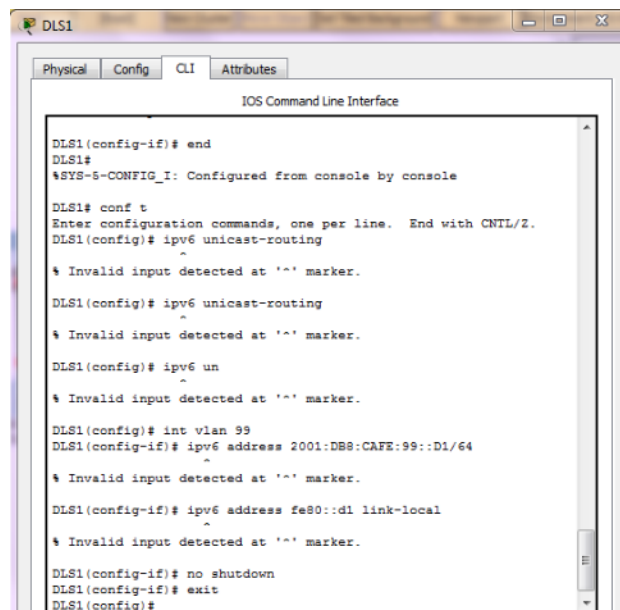
NO LO EJECUTA EL PKT

V.7

```
DLS1(config-if)# ipv6 address fe80::d1 link-local
```

NO LO EJECUTA EL PKT V.7

```
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.

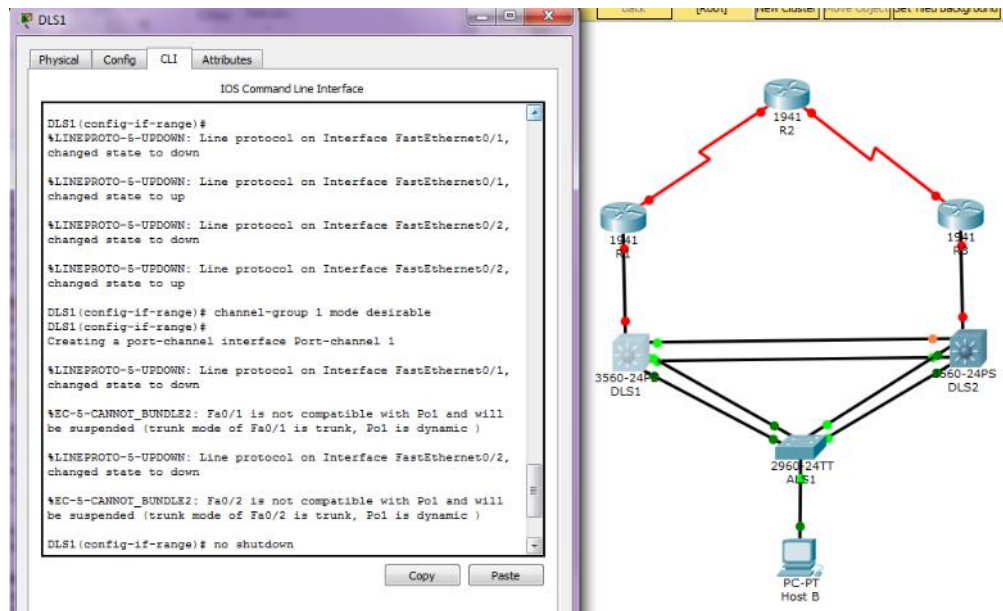
EtherChannel is used for the trunks because it allows you to utilize both Fast Ethernet interfaces that are available between each device, thereby doubling the bandwidth.

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.

- a. 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
```

- b. 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 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.

- Verify the VTP changes.

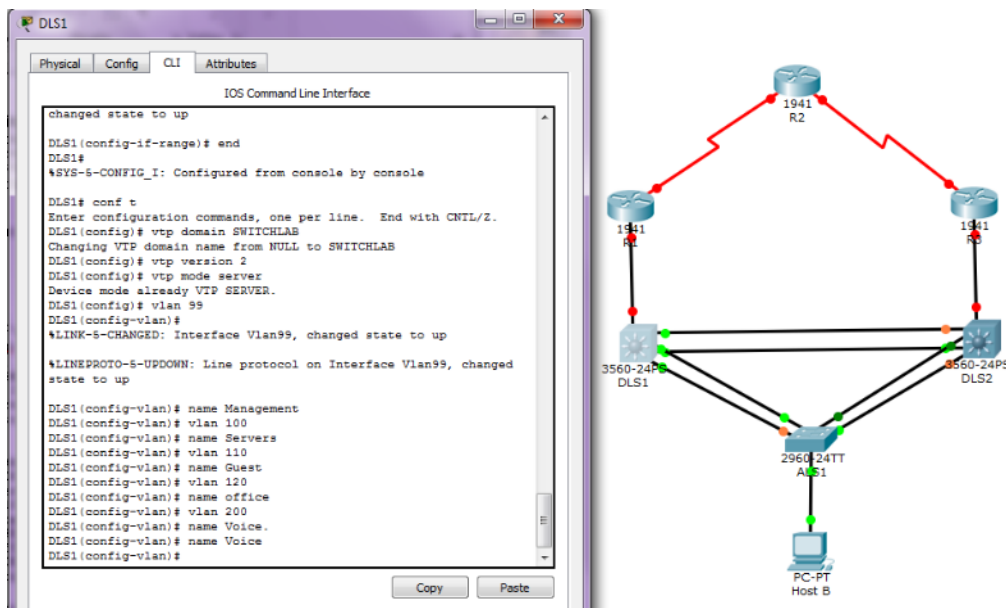
Step 5: Configure VTP on DLS1.

- 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 accomplished 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
```

V.7

ESTE COMANDO NO LO EJECUTA EL PKT

```

DLS1(config)# ipv6 router eigrp 1 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 NO LO EJECUTA PKT
V.7
DLS1(config-if)# ipv6 address 2001:DB8:CAFE:20::D1/64 NO LO EJECUTA PKT
V.7
DLS1(config-if)# ipv6 eigrp 1 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 NO LO EJECUTA
PKT V.7
DLS1(config-if)# ipv6 address FE80::D1 link-local NO LO EJECUTA PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 NO LO EJECUTA
PKT V.7
DLS1(config-if)# ipv6 address FE80::D1 link-local NO LO EJECUTA PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 NO LO EJECUTA
PKT V.7

```

```

DLS1(config-if)# ipv6 address FE80::D1 link-local NO LO EJECUTA PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 NO LO EJECUTA
PKT V.7
DLS1(config-if)# ipv6 address FE80::D1 link-local NO LO EJECUTA PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
DLS1(config-if)# no shutdown

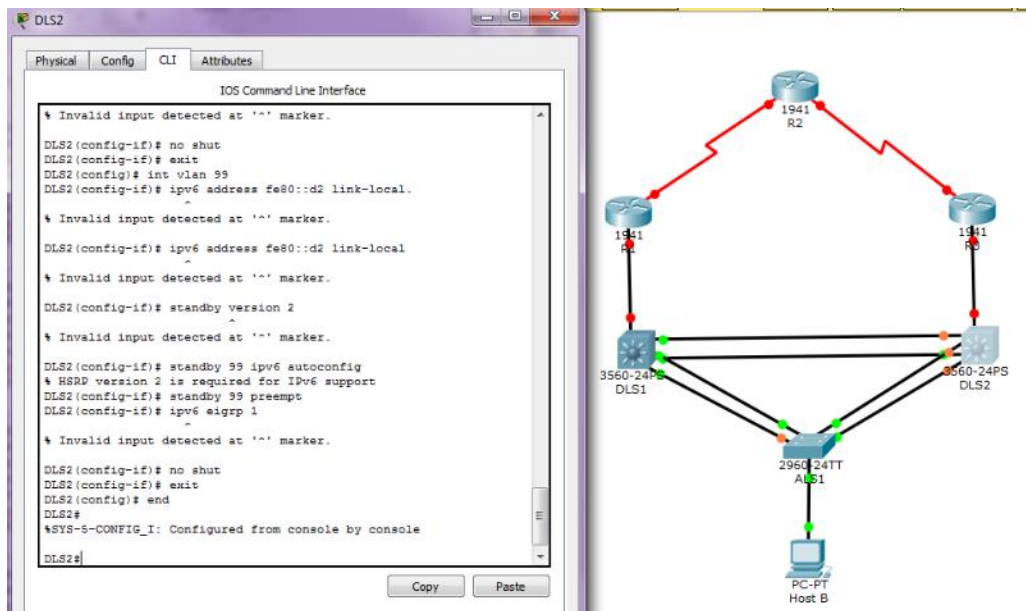
DLS2(config)# ipv6 unicast-routing ESTE COMANDO NO LO EJECUTA EL PKT
V.7
DLS2(config)# ipv6 router eigrp 1 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
DLS2(config-router)# router-id 2.2.2.2
DLS2(config-router)# no shutdown
DLS2(config-router)# exit
DLS2(config)# interface FastEthernet0/5
DLS2(config-if)# no switchport
DLS2(config-if)# ipv6 address FE80::d2 link-local NO LO EJECUTA PKT
V.7
DLS2(config-if)# ipv6 address 2001:DB8:CAFE:212::D2/64 NO LO EJECUTA
PKT V.7
DLS2(config-if)# ipv6 eigrp 1 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
DLS2(config-if)# no shutdown
DLS2(config-if)# exit
DLS2(config)# interface vlan 99
DLS2(config-if)# ipv6 address fe80::d2 link-local NO LO EJECUTA PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 NO LO EJECUTA
PKT V.7

```

```

DLS2(config-if)# ipv6 address FE80::D2 link-local NO LO EJECUTA PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 NO LO EJECUTA
PKT V.7
DLS2(config-if)# ipv6 address FE80::D2 link-local NO LO EJECUTA PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 NO LO EJECUTA
PKT V.7
DLS2(config-if)# ipv6 address FE80::D2 link-local NO LO EJECUTA PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
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 NO LO EJECUTA
PKT V.7
DLS2(config-if)# ipv6 address FE80::D2 link-local NO LO EJECUTA PKT
V.7
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 ESTE COMANDO NO LO EJECUTA EL PKT
V.7
DLS2(config-if)# no shutdown

```

Step 7: Verify the HSRP configuration.

- 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**

ESTE COMANDO NO MUESTRA NADA EN EL PKT

V.7

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#

```

- b. Issue the `show standby brief` command on both DLS1 and DLS2.**

```
DLS1# sh stand bri
```

ESTE COMANDO NO MUESTRA NADA EN EL PKT V.7

```

P indicates configured to preempt.
|
Interface  Grp  Pri P State  Active      Standby      Virtual IP
Vl199      99   110 P Active  local       FE80::D2     FE80::5:73FF:FEA0:63
Vl1100     100  100 P Standby FE80::D2     local        FE80::5:73FF:FEA0:64
Vl1110     110  110 P Active  local       FE80::D2     FE80::5:73FF:FEA0:6E
Vl1120     100  110 P Active  local       FE80::D2     FE80::5:73FF:FEA0:64
Vl1200     100  100 P Standby FE80::D2     local        FE80::5:73FF:FEA0:64
DLS1#

```

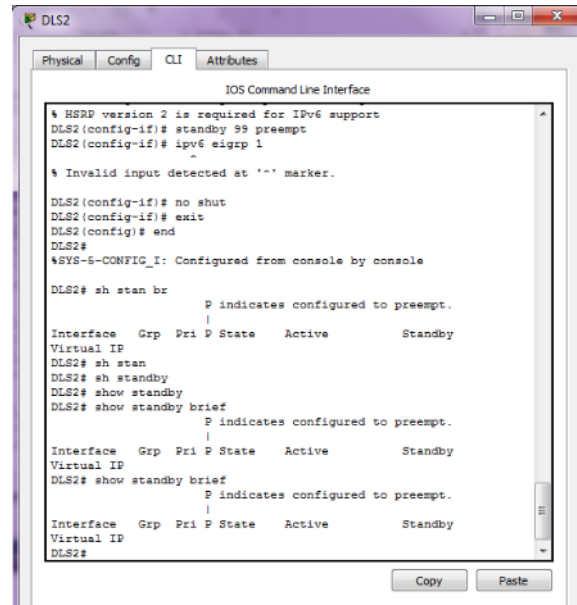
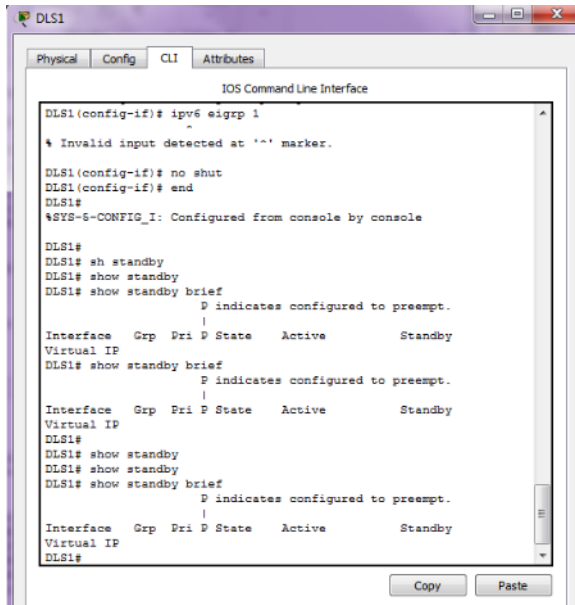
DLS2# **sh standby brief**

ESTE COMANDO NO MUESTRA NADA EN EL PKT V.7

```

P indicates configured to preempt.
|
Interface  Grp  Pri P State  Active      Standby      Virtual IP
Vl199      99   100 P Standby FE80::D1     local        FE80::5:73FF:FEA0:63
Vl1100     100  110 P Active  local       FE80::D1     FE80::5:73FF:FEA0:64
Vl1110     110  100 P Standby FE80::D1     local        FE80::5:73FF:FEA0:6E
Vl1120     100  100 P Standby FE80::D1     local        FE80::5:73FF:FEA0:64
Vl1200     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.

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

- 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 ?
```

PKT V.7

<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 Vlan
fcpa	Fiber Channel

```
DLS1(config-if)# standby 99 track fastEthernet 0/5 ? NO MUESTRA NADA  
EN PKT
```

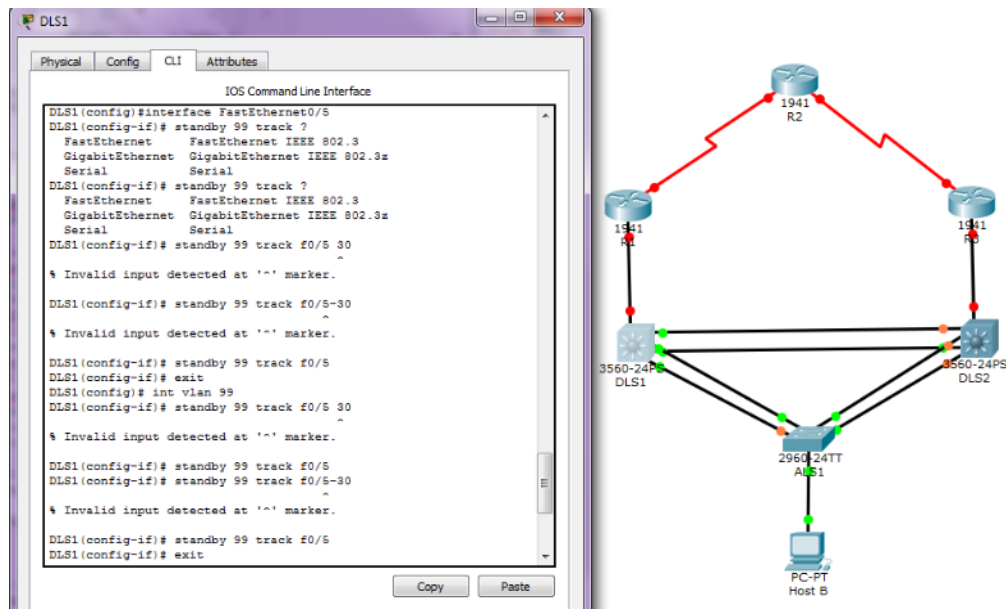
```
<1-255> Decrement value  
<cr>
```

```
DLS1(config)# interface vlan 99  
DLS1(config-if)# standby 99 track fastEthernet 0/5 30 NO MUESTRA NADA  
EN PKT
```

```
DLS1(config)# interface vlan 110  
DLS1(config-if)# standby 110 track fastEthernet 0/5 30 NO MUESTRA NADA  
EN PKT
```

```
DLS1(config)# interface vlan 120  
DLS1(config-if)# standby 120 track fastEthernet 0/5 30 NO MUESTRA NADA  
EN PKT
```

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-

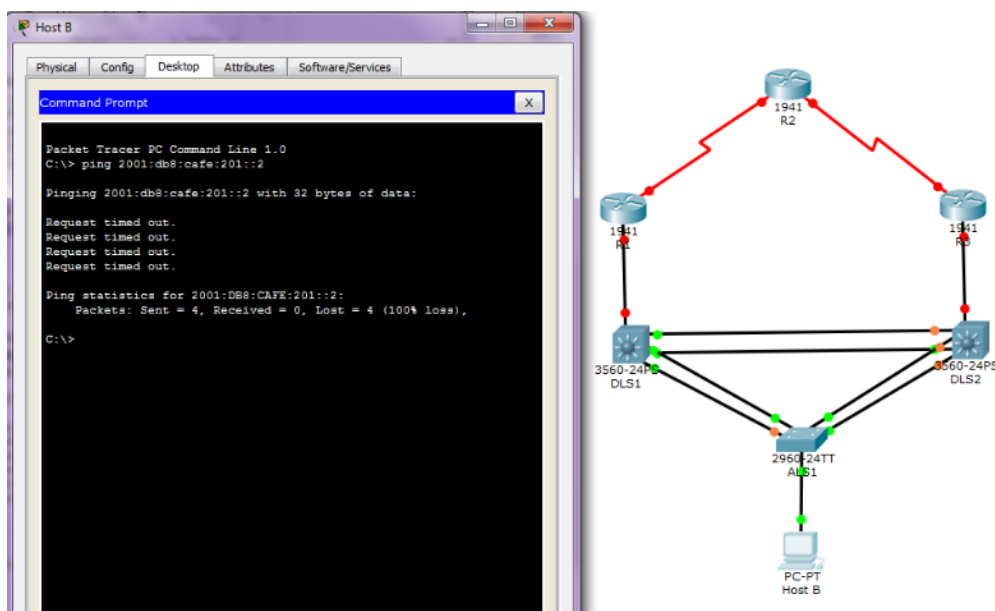
gateway services. As a result of the HSRP state change, clients experience minimal disruption and require no reconfiguration.

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

C:\>ping 2001:db8:café:201::2 -t

NO REALIZA PING EN PKT

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

ESTE COMANDO NO MUESTRA NADA EN PKT

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

ESTE COMANDO NO MUESTRA NADA EN PKT

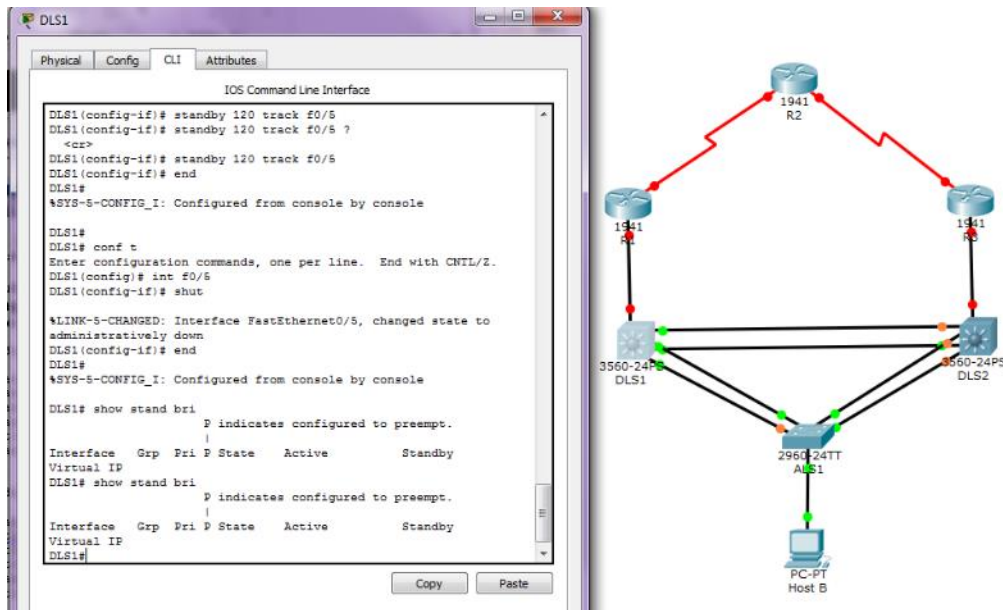
P indicates configured to preempt.

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

V1200 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.

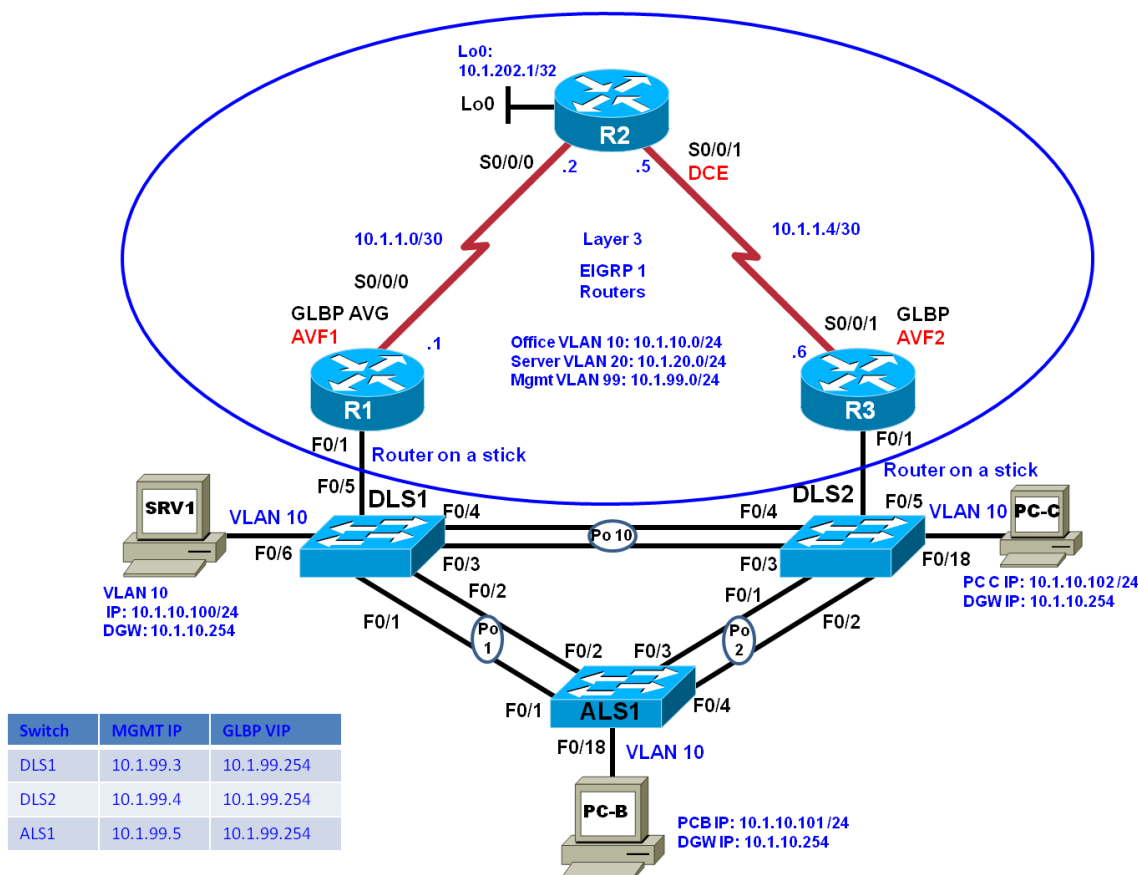
CHALLENGE: Optimize HSRPv6 by adjusting the hello and hold timers used in HSRP communication with the hello time adjusted to 50 milliseconds and hold time adjusted to 250 milliseconds on all HSRP groups.

Step 5: End of Lab

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

CCNPv7.1_SWITCH_Lab6-3_GLBP_STUDENT

Topology



Objectives

- Configure trunking, VTP, and inter-VLAN routing using router-on-a stick
- Configure GLBP
- Configure GLBP priorities
- Configure GLBP object tracking.

Background

Although HSRP and VRRP provide gateway resiliency for the standby members of the redundancy group, the upstream bandwidth is not used while the device is in standby mode. Only the active router for HSRP and the master for VRRP groups forward traffic for the virtual MAC. Resources associated with the standby router are not fully utilized. Some load balancing can be accomplished with these protocols through the creation of multiple groups and through the assignment of multiple default gateways, but this configuration creates an administrative burden. Previous labs provided you with experience configuring HSRP and VRRP to act as First Hop Redundancy Protocols. Gateway Load Balancing Protocol (GLBP) performs a similar function in redundancy, but offers the capability to load balance over multiple gateways.

GLBP is a Cisco-proprietary solution created to enable automatic selection and simultaneous use of multiple available gateways in addition to automatic failover between those gateways. Multiple routers share the load of frames that, from a client perspective, are sent to a single default gateway address.

Like HSRP and VRRP, an election occurs, but rather than a single active router winning the election, GLBP elects an Active Virtual Gateway (AVG). The AVG assigns virtual MAC addresses to each of the routers in the GLBP group (called Active Virtual Forwarders or AVFs). These virtual MAC addresses are then provided to hosts in an algorithmic manner in response to ARP requests from hosts for the default gateway.

GLBP allows for simultaneous forwarding from routers participating in a GLBP group. GLBP can support up to 4 routers in a group. GLBP also offers authentication and object tracking.

In this lab, you will set the network up by configuring trunking, VTP, VLANs, router-on-a-stick and EIGRP routing. Once the network is set up, you will configure and verify GLBP.

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 3560 switches are being used only as layer 2 devices in this lab topology. 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 release).

Note(2): The 3 switches in this topology are only being used to support layer-2 functions, so 3 Cisco 2960 switches are acceptable for this lab. All Inter-VLAN routing will be facilitated by implementing a router-on-a-stick on R1 and R3.

Note(3): 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

- 2 Cisco 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-IPSERVICESK9-M image or comparable
- 1 Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable
- Three routers (This lab uses Cisco ISR G2 routers running Cisco IOS 15.4(3) images with IP Base and Security packages enabled, or comparable)
- Ethernet and console cables
- 3 PC's with Windows OS

Step 6: 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>

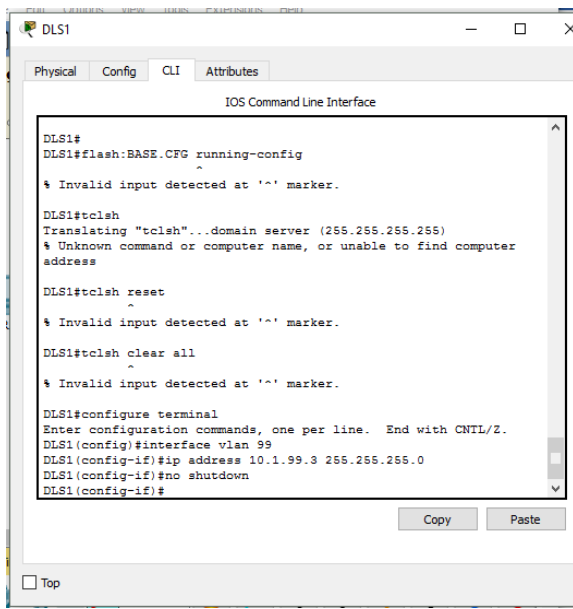
Would you like to enter the initial configuration dialog? [yes/no]: n
Switch> en
*Mar  1 00:01:30.915: %LINK-5-CHANGED: Interface Vlan1, changed state to
administratively down
Switch# copy BASE.CFG running-config
Destination filename [running-config]?
184 bytes copied in 0.310 secs (594 bytes/sec)
DLS1#
```

Step 7: Configure basic switch parameters.

On each switch, 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 lab, VLAN 99 will be used as the management VLAN.

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 10.1.99.3 255.255.255.0
DLS1(config-if)# no shutdown
```



The interface VLAN 99 will not come up immediately, because the Layer 2 instance of the VLAN does not yet exist. 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.

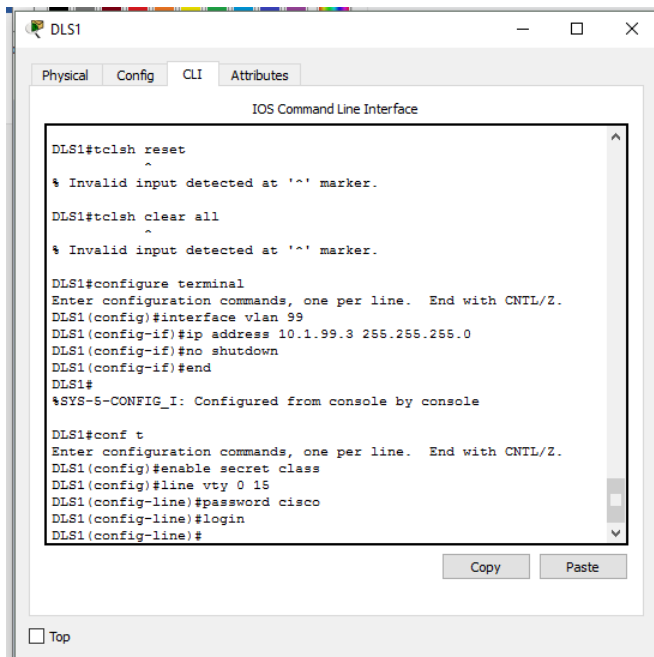
DLS1 example:

```
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 8: 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.

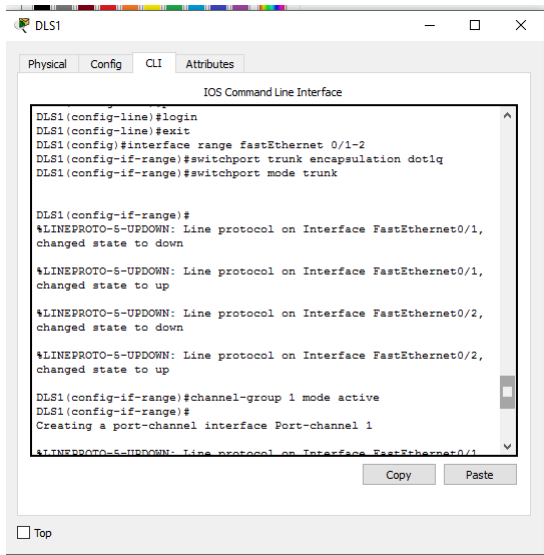
Configure trunks and EtherChannels from DLS1, DLS2, and ALS1 according to the diagram. Use LACP as the negotiation protocol for EtherChannel configurations. Remember that BASE.CFG has all interfaces shut down, so don't forget to issue the **no shutdown** command.

Refer to diagram for port channel numbers.

Note: The **switchport trunk encapsulation dot1q** command is required on Cisco 3560 switches. It is not required on Cisco 2960 switches.

```

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 active
DLS1(config-if-range)# no shut
Creating a port-channel interface Port-channel 1
  
```



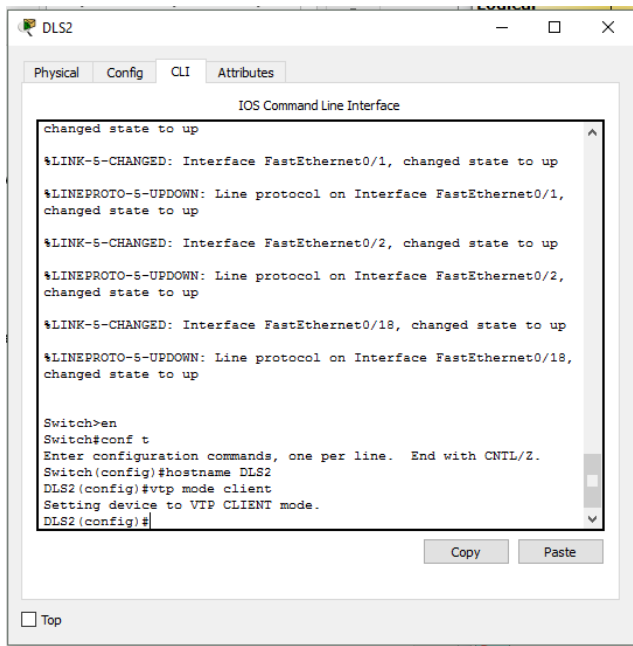
Verify trunking and EtherChannel configurations between all switches with the appropriate trunking and EtherChannel verification commands. Refer back to Chapter 3 labs as necessary.

Step 9: Configure VTP Client mode on DLS2 and ALS1.

A sample configuration is provided for you.

```
DLS2(config)# vtp mode client
```

Setting device to VTP client mode for VLANs



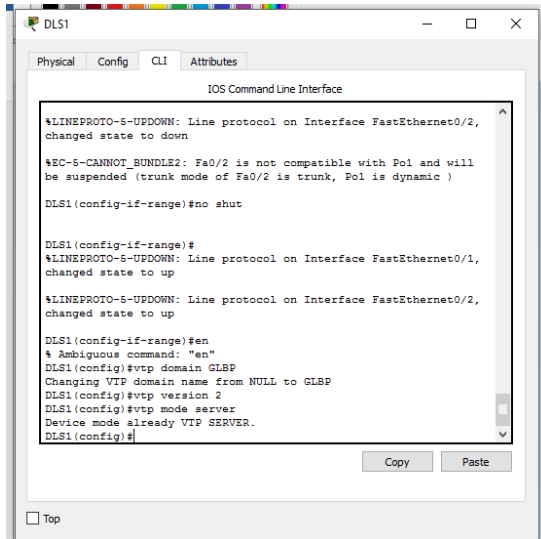
Note: Switches default to vtp mode server. However, remember the base configuration modifies this setting to vtp mode transparent.

Step 10: Configure VTP and VLANs on DLS1.

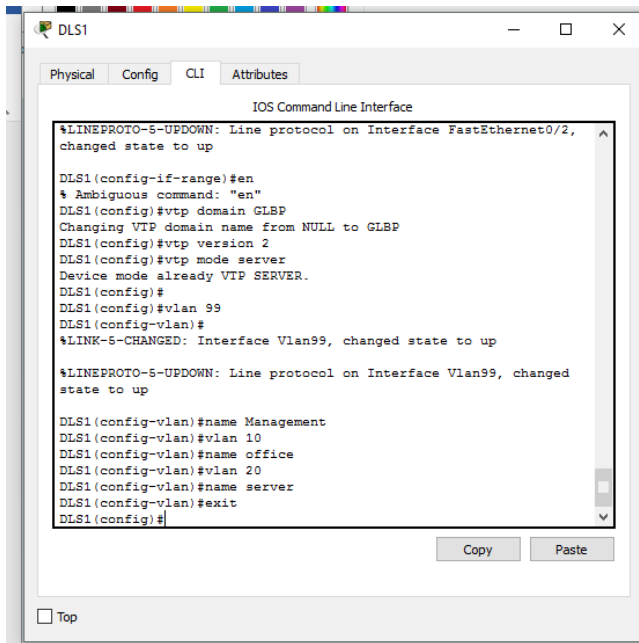
Create the VTP domain on VTP server DLS1 and create VLANs 10, 20, and 99 for the domain.

NOTE: Switches default to **vtp mode server**. Recall that the base configuration modifies this setting to **vtp mode transparent**.

```
DLS1(config)# vtp domain GLBP
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 10
DLS1(config-vlan)# name Office
DLS1(config-vlan)# vlan 20
DLS1(config-vlan)# name Server
DLS1(config-vlan)# exit
```



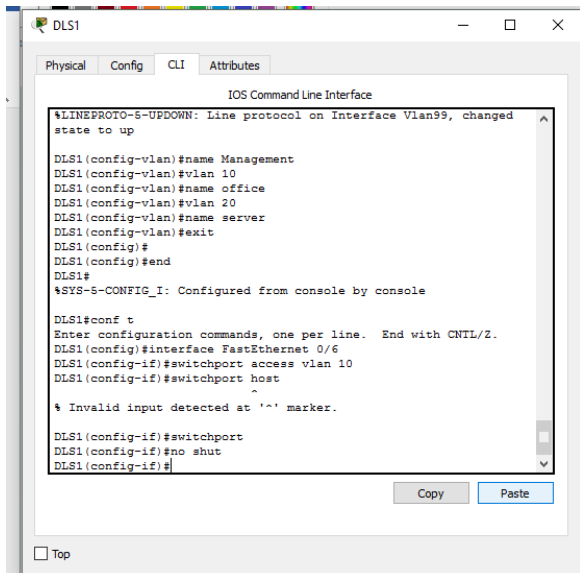
Verify that VLANs propagated to the other switches in the network.

Step 11: Configure switch access ports.

As the diagram illustrates, there are PCs connected to DLS1 fa0/6, DLS2 fa0/18, and ALS1 fa0/18. All PCs connected to the lab topology will statically access VLAN 10. Additionally, configure spanning-tree portfast on these switchports. The simplest way to do all of this is to use the **switchport host** macro. Also, don't forget to issue the **no shutdown** command.

```
DLS1(config)# interface FastEthernet 0/6
DLS1(config-if)# switchport access vlan 10
DLS1(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

DLS1(config-if)# no shutdown
```



Repeat this configuration for interface fa0/18 on DLS2 and ALS1, and then verify the switchports on DLS1, DLS2 and ALS1 are members of VLAN 10.

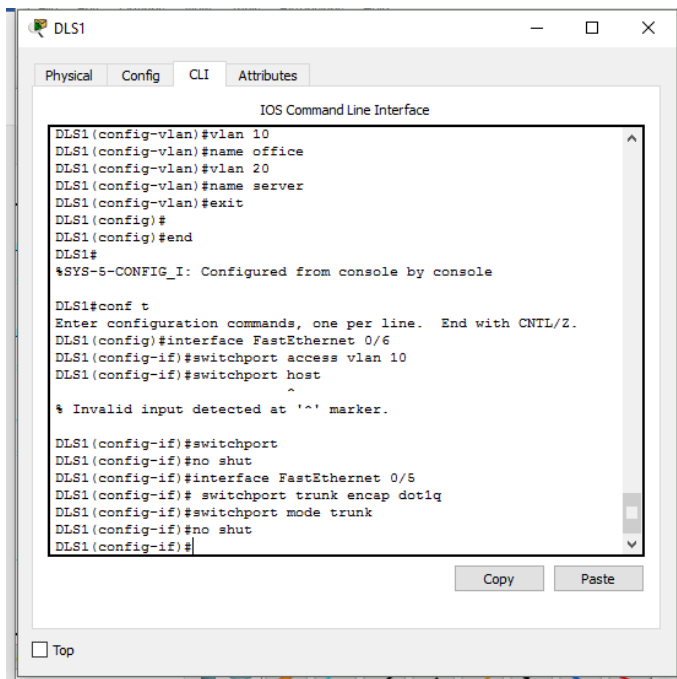
Step 12: Configure DLS1 and DLS2 trunking to the R1 and R3 router.

Configure DLS1 and DLS2 interface fa0/5 for trunking with the R1 and R3 router Gigabit Ethernet interface, according to the topology diagram. An example from DLS1:

```

DLS1(config)# interface FastEthernet 0/5
DLS1(config)# switchport trunk encap dot1q
DLS1(config)# switchport mode trunk
DLS1(config)# no shutdown

```

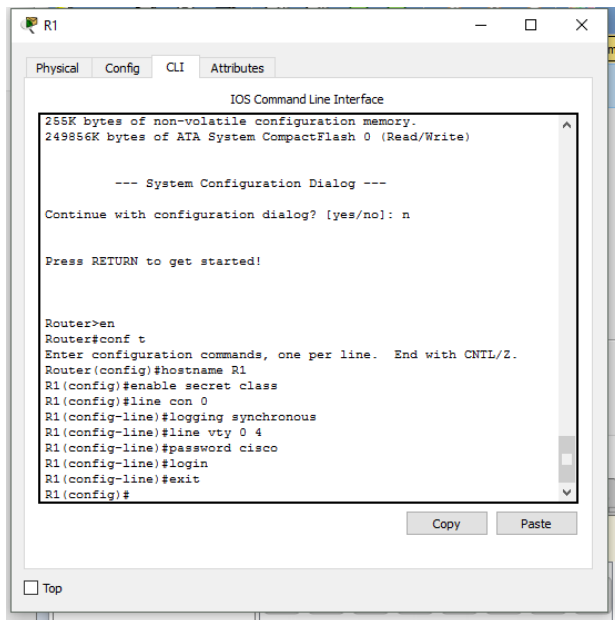


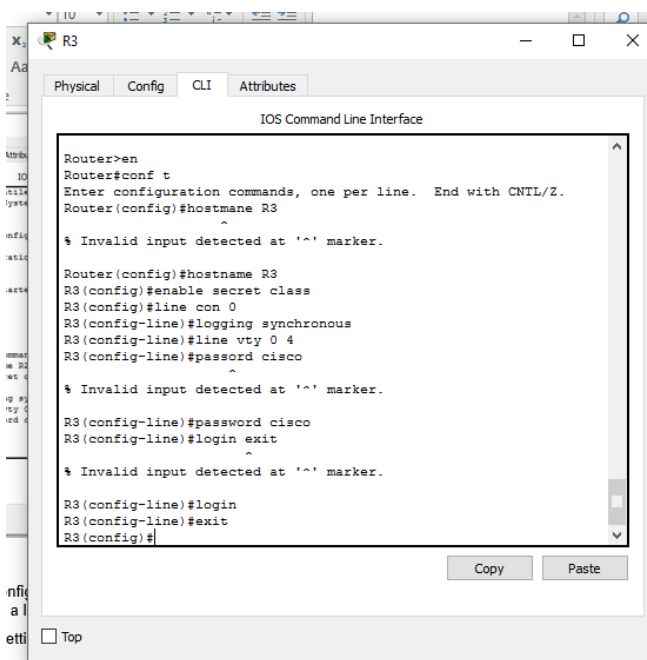
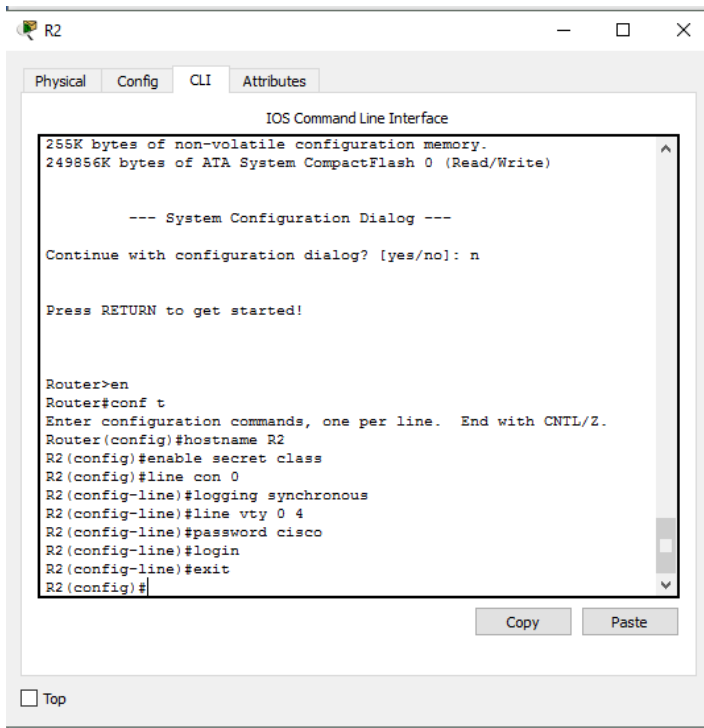
Note: The `switchport trunk encapsulation dot1q` command is required on Cisco 3560 switches. It is not required on Cisco 2960 switches.

Step 13: Configure basic settings on R1, R2, and R3.

Configure basic settings on all three routers. An example for R1 follows:

```
Router> enable
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line con 0
R1(config-line)# logging synchronous
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

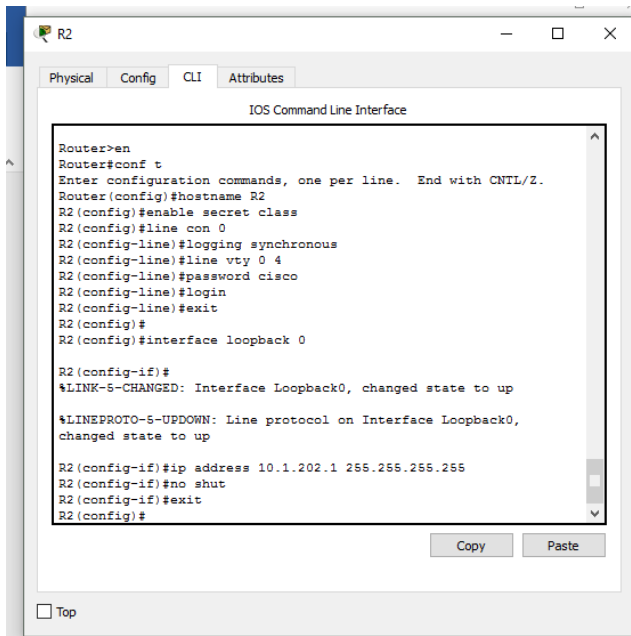




Note: The passwords configured here are required for NETLAB compatibility only and are NOT recommended for use in a live environment.

In addition to the basic settings on R2, configure interface Loopback 0 with the IP address 10.1.202.1/32

```
R2(config)# interface loopback 0
R2(config-if)# ip address 10.1.202.1 255.255.255.255
R2(config-if)# no shut
R2(config-if)# exit
```



Step 14: Configure the R1 and R3 Gigabit Ethernet interfaces for VLAN trunking.

Create a sub-interface for each VLAN. Enable each sub-interface with the proper trunking protocol, and configure it for a particular VLAN with the **encapsulation** command. Assign an IP address to each sub-interface from the table below. Hosts on the VLAN will use this address as their default gateway.

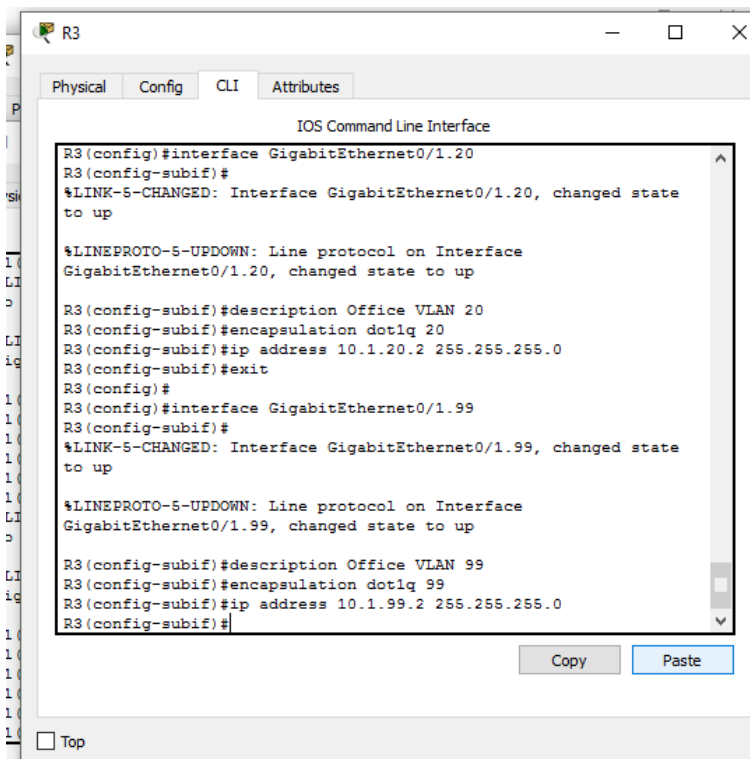
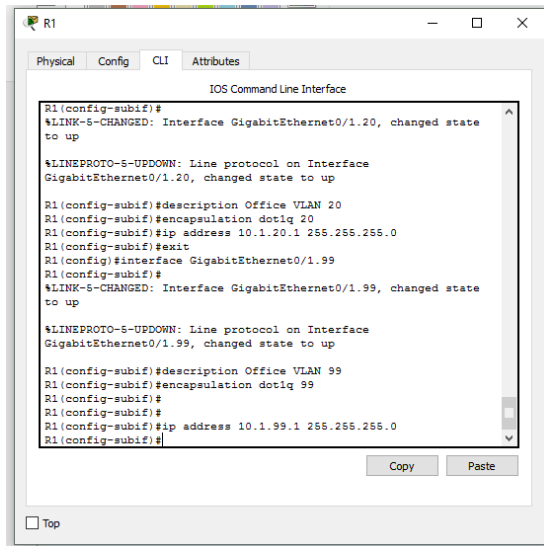
VLAN	R1	R3
99	10.1.99.1/24	10.1.99.2/24
10	10.1.10.1/24	10.1.10.2/24
20	10.1.20.1/24	10.1.20.2/24

The following is a sample configuration for the Gigabit Ethernet 0/1 interface:

```

R1(config)# interface GigabitEthernet0/1
R1(config-if)# no shut
R1(config)# interface GigabitEthernet0/1.10
R1(config-subif)# description Office VLAN 10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 10.1.10.1 255.255.255.0
R1(config)# interface GigabitEthernet0/1.20
R1(config-subif)# description Server VLAN 20
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# ip address 10.1.20.1 255.255.255.0
R1(config)# interface GigabitEthernet0/1.99
R1(config-subif)# description Management VLAN 99
R1(config-subif)# encapsulation dot1q 99
R1(config-subif)# ip address 10.1.99.1 255.255.255.0

```

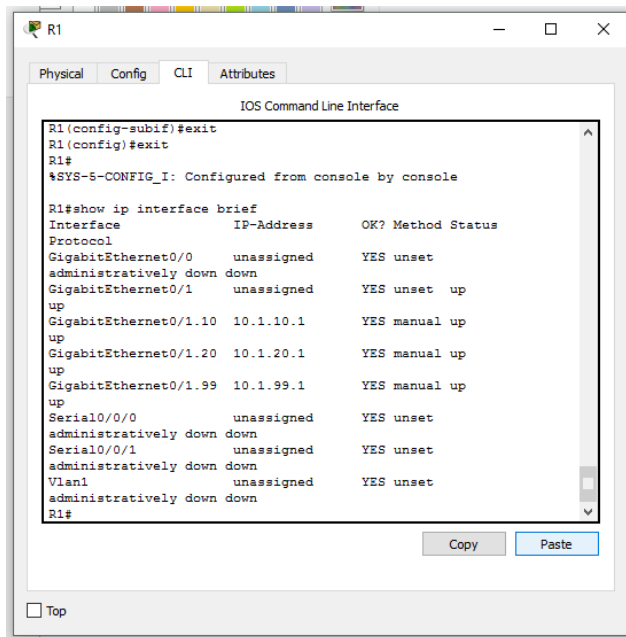


Now, move to the R3 router to repeat similar configurations. In order for the R3 router to provide load balancing and redundancy VLAN 10, 20 and 99 networks, R3 must be configured to logically participate in the network. Create a sub-interface for each VLAN. Enable each sub-interface with the respective trunking protocol, and configure it for a particular VLAN with the **encapsulation** command. Assign an IP address to each sub-interface from the table above. Hosts on the VLAN can use this address as their default gateway.

Use the **show ip interface brief** command to verify the interface configuration and status.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/1.10	10.1.10.1	YES	manual	up	up
GigabitEthernet0/1.20	10.1.20.1	YES	manual	up	up
GigabitEthernet0/1.99	10.1.99.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down
Serial0/1/0	unassigned	YES	unset	administratively down	down
Serial0/1/1	unassigned	YES	unset	administratively down	down



Use the **show vlans** command on the R1 and R3 router to verify inter-vlan routing configurations. The following is a sample output from router R1. Verify configurations on router R3.

R1# **show vlans**

Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/1

This is configured as native Vlan for the following interface(s) :
GigabitEthernet0/1 Native-vlan Tx-type: Untagged

Protocols Configured:	Address:	Received:	Transmitted:
GigabitEthernet0/1 (1)			
Other		0	19
17 packets, 5572 bytes input			
19 packets, 1856 bytes output			

Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/1.10

Protocols Configured:	Address:	Received:	Transmitted:

```

GigabitEthernet0/1.10 (10)
    IP          10.1.10.1          0          0
    Other              0          2

    0 packets, 0 bytes input
    2 packets, 92 bytes output

Virtual LAN ID: 20 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface: GigabitEthernet0/1.20

    Protocols Configured: Address:          Received:          Transmitted:

GigabitEthernet0/1.20 (20)
    IP          10.1.20.1          0          0
    Other              0          1

    0 packets, 0 bytes input
    1 packets, 46 bytes output

Virtual LAN ID: 99 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interface: GigabitEthernet0/1.99

    Protocols Configured: Address:          Received:          Transmitted:

GigabitEthernet0/1.99 (99)
    IP          10.1.99.1          0          0
    Other              0          1

    0 packets, 0 bytes input
    1 packets, 46 bytes output

```

Step 15: Configure EIGRP routing in AS 1 for use with GLBP interface tracking.

Configure R1 serial interface s0/0/0 as shown in the topology diagram. Also configure EIGRP AS 1 for the 10.0.0.0 network. Below is an example of the configuration:

```

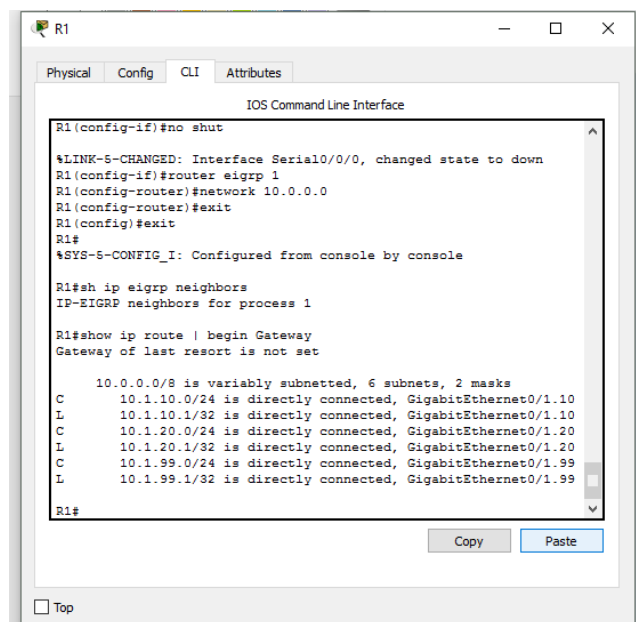
R1(config)# int s0/0/0
R1(config-if)# ip add 10.1.1.1 255.255.255.252
R1(config-if)# no shut

R1(config)# router eigrp 1
R1(config-router)# network 10.0.0.0

```


Gateway of last resort is not set

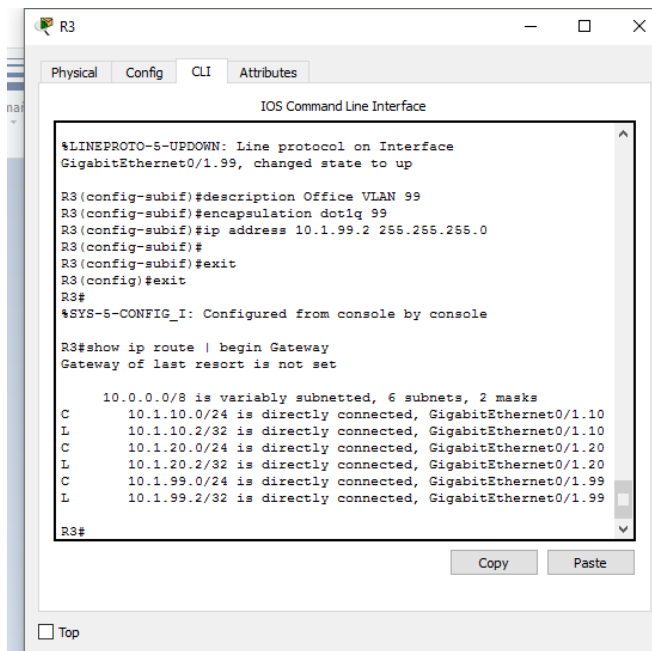
```
10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0
D    10.1.1.4/30
      [90/2172416] via 10.1.99.2, 00:04:15, GigabitEthernet0/1.99
      [90/2172416] via 10.1.20.2, 00:04:15, GigabitEthernet0/1.20
      [90/2172416] via 10.1.10.2, 00:04:15, GigabitEthernet0/1.10
C    10.1.10.0/24 is directly connected, GigabitEthernet0/1.10
L    10.1.10.1/32 is directly connected, GigabitEthernet0/1.10
C    10.1.20.0/24 is directly connected, GigabitEthernet0/1.20
L    10.1.20.1/32 is directly connected, GigabitEthernet0/1.20
C    10.1.99.0/24 is directly connected, GigabitEthernet0/1.99
L    10.1.99.1/32 is directly connected, GigabitEthernet0/1.99
D    10.1.202.1/32 [90/2297856] via 10.1.1.2, 00:04:15, Serial0/0/0
```



R3# show ip route | begin Gateway

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
D    10.1.1.0/30
      [90/2172416] via 10.1.99.1, 00:05:09, GigabitEthernet0/1.99
      [90/2172416] via 10.1.20.1, 00:05:09, GigabitEthernet0/1.20
      [90/2172416] via 10.1.10.1, 00:05:09, GigabitEthernet0/1.10
C    10.1.1.4/30 is directly connected, Serial0/0/1
L    10.1.1.6/32 is directly connected, Serial0/0/1
C    10.1.10.0/24 is directly connected, GigabitEthernet0/1.10
L    10.1.10.2/32 is directly connected, GigabitEthernet0/1.10
C    10.1.20.0/24 is directly connected, GigabitEthernet0/1.20
L    10.1.20.2/32 is directly connected, GigabitEthernet0/1.20
C    10.1.99.0/24 is directly connected, GigabitEthernet0/1.99
L    10.1.99.2/32 is directly connected, GigabitEthernet0/1.99
D    10.1.202.1/32 [90/2297856] via 10.1.1.5, 00:05:09, Serial0/0/1
```



From R1 and R3, ensure that you can ping the 10.1.202.1 destination address.

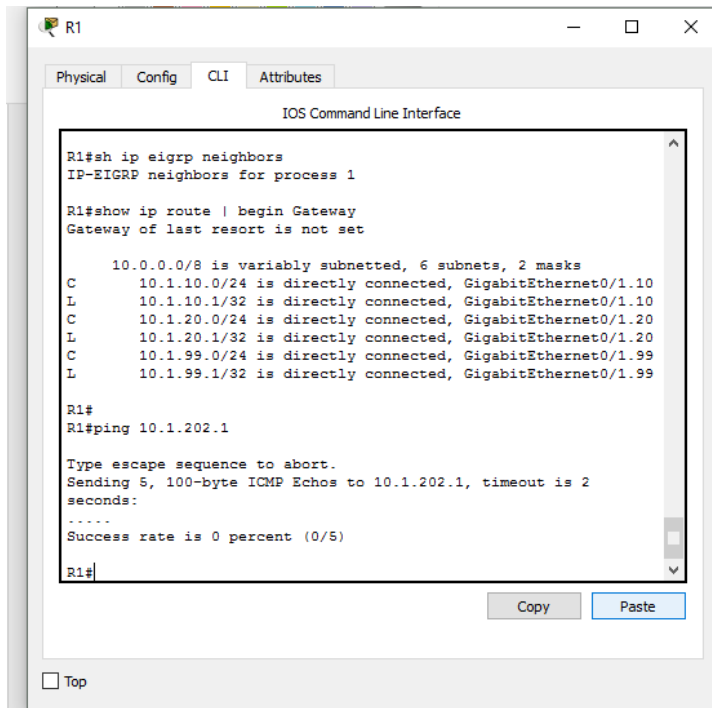
R1# **ping 10.1.202.1**

Type escape sequence to abort.

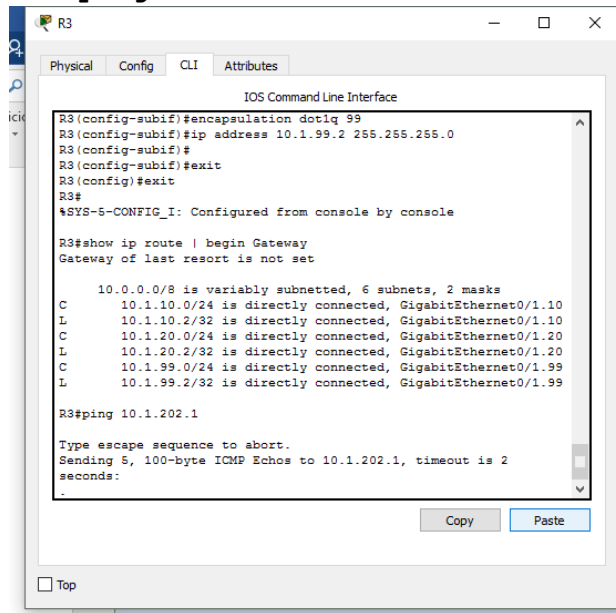
Sending 5, 100-byte ICMP Echos to 10.1.202.1, timeout is 2 seconds:

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms



R3# ping 10.1.202.1



Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.202.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Step 16: Configure the routers for GLBP operation.

In this step you will configure a single GLBP group consisting of two members (R1 and R3). A GLBP group can have as many as four members. A single member will be elected as the AVG, and then routers will be designated as AVFs and their virtual MAC address will be distributed to hosts by the AVG in response to ARP requests.

AVG election is based on highest GLBP priority. In case of a tie, the highest assigned IP address is used. The **glbp <grp #> priority** interface configuration command can be used to modify the priority from the default of 100 in order to influence the election of the AVG. Should the AVG lose its role, the backup router with highest priority will assume the role. If you desire for the original AVG router to reassume its role once it comes back up, the **glbp <grp #> preempt** command must be configured.

The AVF is responsible for forwarding packets that are sent to the virtual MAC address assigned to that gateway by the AVG. Forward preemption is used with the AVFs and allows another AVF to assume responsibility for forwarding packets for an AVF that has lost its role or been disconnected. While AVG preemption must be manually configured, AVF preemption is enabled by default.

However, the AVFs use a weighting value rather than a priority value. Weighting thresholds are defined in conjunction with interface tracking. This functionality will be demonstrated later in the lab.

In this lab R1 will act as AVG and AVF1 and R3 will act as the AVF2. R1's GLBP priority will be modified to ensure its election as AVG.

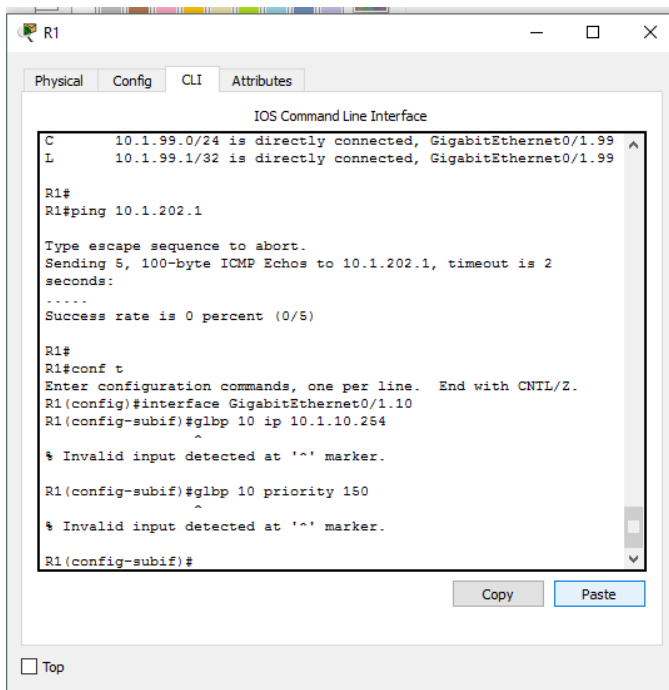
The standby address for each VLAN will be the host address 254; VLAN 10 will use 10.1.10.254, VLAN 20 will use 10.1.20.254.

The following is a sample GLBP configuration on R1.

```

R1(config)# interface GigabitEthernet0/1.10
R1(config-subif)# glbp 10 ip 10.1.10.254
R1(config-subif)# glbp 10 priority 150
R1(config-subif)# glbp 10 preempt
R1(config-subif)# exit
R1(config)# interface GigabitEthernet0/1.20
R1(config-subif)# glbp 20 ip 10.1.20.254
R1(config-subif)# glbp 20 priority 150
R1(config-subif)# glbp 20 preempt
R1(config-subif)# exit
R1(config)# interface GigabitEthernet0/1.99
R1(config-subif)# glbp 99 ip 10.1.99.254
R1(config-subif)# glbp 99 priority 150
R1(config-subif)# glbp 99 preempt

```



Except for the priority command, the same commands are used on the sub-interfaces on R3.

As a result of our configuration, we should see R1 router with the AVG role. Issue the **show glbp** command for GLBP configuration analysis. Before examining the output, it might be useful to take note of the MAC address of R1 and R3's G0/1 interfaces.

```

R1# sho int g0/1 | i bia
    Hardware is CN Gigabit Ethernet, address is acf2.c523.7a09 (bia
acf2.c523.7a09)
R1#

R3# show int g0/1 | i bia
    Hardware is CN Gigabit Ethernet, address is acf2.c518.0651 (bia
acf2.c518.0651)
R3#

```

R1# **show glbp**

GigabitEthernet0/1.10 - Group 10

State is Active

1 state change, last state change 00:01:28

Virtual IP address is 10.1.10.254

Hello time 3 sec, hold time 10 sec

Next hello sent in 2.272 secs

Redirect time 600 sec, forwarder timeout 14400 sec

Preemption enabled, min delay 0 sec

Active is local

Standby is 10.1.10.2, priority 100 (expires in 7.840 sec)

Priority 150 (configured)

Weighting 100 (default 100), thresholds: lower 1, upper 100

Load balancing: round-robin

Group members:

acf2.c518.0651 (10.1.10.2)

acf2.c523.7a09 (10.1.10.1) local

There are 2 forwarders (1 active)

Forwarder 1

State is Active

1 state change, last state change 00:00:46

MAC address is 0007.b400.0a01 (default)

Owner ID is acf2.c523.7a09

Redirection enabled

Preemption enabled, min delay 30 sec

Active is local, weighting 100

Forwarder 2

State is Listen

MAC address is 0007.b400.0a02 (learnt)

Owner ID is acf2.c518.0651

Redirection enabled, 597.856 sec remaining (maximum 600 sec)

Time to live: 14397.856 sec (maximum 14400 sec)

Preemption enabled, min delay 30 sec

Active is 10.1.10.2 (primary), weighting 100 (expires in 8.384

sec)

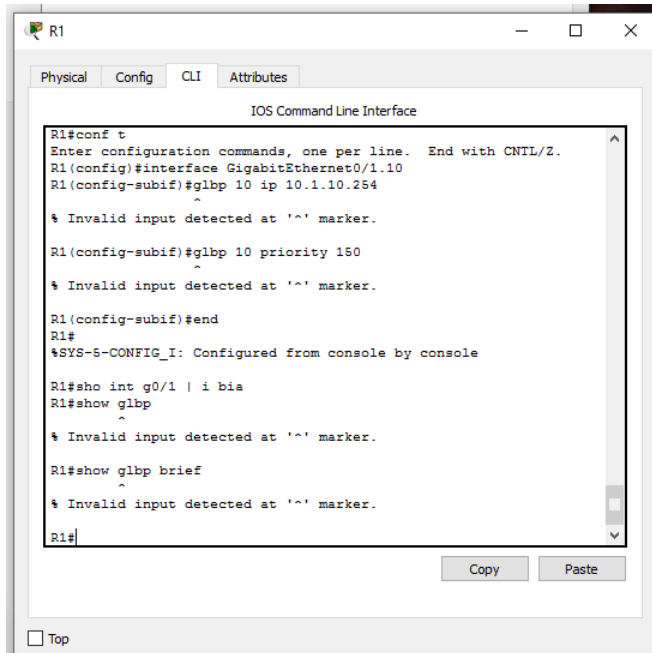
<output omitted>

The **show glbp brief** command can also be used to view a brief synopsis of GLBP operation.

R1# **show glbp brief**

	Interface	Grp	Fwd	Pri	State	Address	Active router	
	Standby router							
Line 1 ->	Gi0/1.10	10	-	150	Active	10.1.10.254	local	
Line 2 ->	10.1.10.2							
Line 3 ->	Gi0/1.10	10	1	-	Active	0007.b400.0a01	local	-
	Gi0/1.10	10	2	-	Listen	0007.b400.0a02	10.1.10.2	-
	Gi0/1.20	20	-	150	Active	10.1.20.254	local	
	10.1.20.2							
	Gi0/1.20	20	1	-	Active	0007.b400.1401	local	-

Gi0/1.20	20	2	-	Listen	0007.b400.1402	10.1.20.2	-
Gi0/1.99	99	-	150	Active	10.1.99.254	local	
10.1.99.2							
Gi0/1.99	99	1	-	Active	0007.b400.6301	local	-
Gi0/1.99	99	2	-	Listen	0007.b400.6302	10.1.99.2	-



The **first line** in the GLBP output shows the role of the AVG for group 10. The priority has been set to 150 for this group and the state shows R1 as the active AVG. The virtual IP address is 10.1.10.254. The standby AVG is 10.1.10.2 which is the R3 router.

Notice the **next two lines** also pertain to GLBP group 10. These lines detail information about the AVF. There are two forwarders in this group. The virtual MAC addresses are **0007.b400.0a01** and **0007.b400.0a02**.

The last hexet is **0a01**. The first two hex characters, **0a** equal 10 in decimal, which corresponds to the group number. The last two digits (**01**) correspond to one of the four MAC addresses (01-04) that can be used in GLBP operation.

The second line in the GLBP output displays information about the AVF. Line 2 shows that R1 is forwarding packets for the MAC address ending in 01. Line 3 of the output shows that R1 is listening or in standby AVF mode for the MAC address ending in 02.

Continue the analysis on the remaining lines of output for GLBP.

Which router is the active forwarder MAC Address 0007.b400.6302 for GLBP group 99?

What MAC address is the active forwarder for GLBP group 99 listening?

Step 17: Verify PCs can reach R2 L0 using the GLBP gateway

Configure the PCs with the IP Addresses shown in the topology diagram. The PCs used in this lab scenario were given access earlier to VLAN 10. The gateway address is set to the GLBP virtual address 10.1.10.254.

This is the IPCONFIG output from SRV1 connected to DLS1 F0/6.

```
Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::a940:91fe:38dd:da0c%10
IPv4 Address. . . . . : 10.1.10.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.10.254
```

This is the IPCONFIG output from PC-B connected to ALS1 F0/18.

```
Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::ee:d834:9d99:45e8%11
IPv4 Address. . . . . : 10.1.10.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.10.254
```

This is the IPCONFIG output from PC-C connected to DLS2 F0/18.

```
Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::a4d3:c82d:93c4:f2e6%11
IPv4 Address. . . . . : 10.1.10.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.10.254
```

Verify that SRV1, PC-B, and PC-C can ping their default gateway. Upon successful ping of the gateway, view the **arp** cache on each PC using the **arp -a**.

Output from SRV1

```
C:\Users\student>ping -n 3 10.1.10.254
```

```
Pinging 10.1.10.254 with 32 bytes of data:
Reply from 10.1.10.254: bytes=32 time=1ms TTL=255
Reply from 10.1.10.254: bytes=32 time=1ms TTL=255
Reply from 10.1.10.254: bytes=32 time=1ms TTL=255
```

```
Ping statistics for 10.1.10.254:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\Users\student>arp -a
```

```

Interface: 10.1.10.100 --- 0xa
  Internet Address      Physical Address      Type
  10.1.10.101           00-0c-29-80-cb-b6     dynamic
  10.1.10.102           00-0c-29-6a-07-e6     dynamic
  10.1.10.254           00-07-b4-00-0a-02     dynamic
  10.1.10.255           ff-ff-ff-ff-ff-ff     static
  169.254.69.232        00-0c-29-80-cb-b6     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

```

The output of the arp cache reveals the 10.1.10.254 associated with GLBP virtual MAC address 00-07-b4-00-0a-02. The first address to be issued to the first client request was the 00-07-b4-00-0a-02 MAC address.

NOTE: The MAC addresses and other output you receive will vary. The important thing to note is that each router is listening for one MAC address either ending in 01 or 02 and that the AVG alternated these MAC addresses in the ARP replies as part of the *default* round robin algorithm.

Now, move to PC-B and ping the default gateway address 10.1.10.254. View the arp cache using the `arp -a` command.

What MAC Address has been issued to the PC-B client?

OUTPUT from PC-B

```

C:\Users\student>ping -n 3 10.1.10.254

Pinging 10.1.10.254 with 32 bytes of data:
Reply from 10.1.10.254: bytes=32 time=2ms TTL=255
Reply from 10.1.10.254: bytes=32 time=1ms TTL=255
Reply from 10.1.10.254: bytes=32 time=1ms TTL=255

Ping statistics for 10.1.10.254:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\student>arp -a

Interface: 10.1.10.101 --- 0xb
  Internet Address      Physical Address      Type
  10.1.10.100           00-0c-29-15-ab-9d     dynamic
  10.1.10.102           00-0c-29-6a-07-e6     dynamic
  10.1.10.254           00-07-b4-00-0a-01     dynamic
  10.1.10.255           ff-ff-ff-ff-ff-ff     static
  11.0.0.5              00-0c-29-6a-07-e6     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

```

Repeat these steps PC-C.

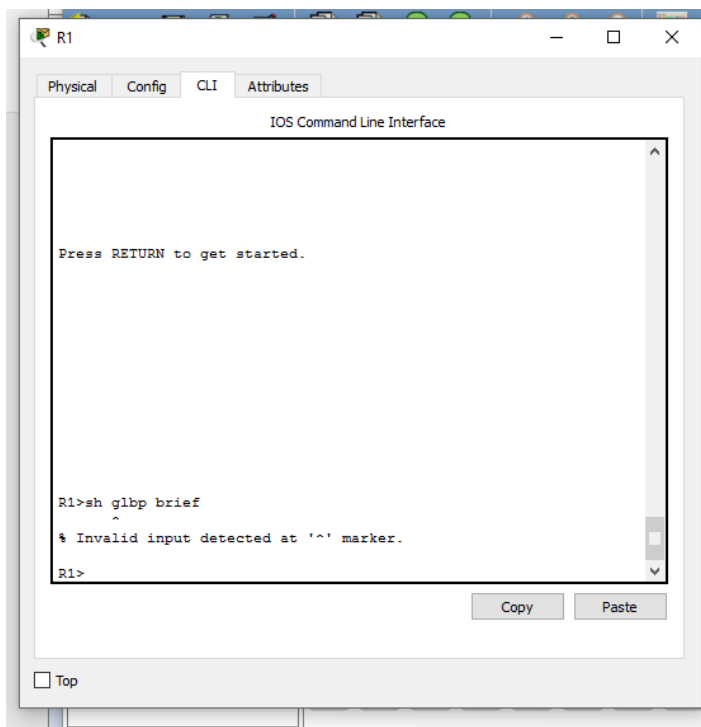
What virtual MAC address is being used by PC-C?

Move to R1 router and issue the **show glbp brief** command. Notice how the MAC addresses correlate to the MAC address issued to the VLAN 10 clients.

```
R1>sh glbp brief
```

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Gi0/1.10	10	-	150	Active	10.1.10.254	local	10.1.10.2
Gi0/1.10	10	1	-	Active	0007.b400.0a01	local	-
Gi0/1.10	10	2	-	Listen	0007.b400.0a02	10.1.10.2	-
Gi0/1.20	20	-	150	Active	10.1.20.254	local	10.1.20.2
Gi0/1.20	20	1	-	Active	0007.b400.1401	local	-
Gi0/1.20	20	2	-	Listen	0007.b400.1402	10.1.20.2	-
Gi0/1.99	99	-	150	Active	10.1.99.254	local	10.1.99.2
Gi0/1.99	99	1	-	Active	0007.b400.6301	local	-
Gi0/1.99	99	2	-	Listen	0007.b400.6302	10.1.99.2	-

R1>



The highlighted line above in the **show glbp brief** output shows that R1 is the active forwarder for the MAC address **0007.b400.0a01** and the standby for the MAC address **0007.b400.0a02**.

Move to the R3 router and issue the **show glbp brief** command. Notice how the MAC addresses correlate to the MAC address issued to the VLAN 10 clients.

```
R3>show glbp brief
```

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Gi0/1.10	10	-	100	Standby	10.1.10.254	10.1.10.1	local
Gi0/1.10	10	1	-	Listen	0007.b400.0a01	10.1.10.1	-
Gi0/1.10	10	2	-	Active	0007.b400.0a02	local	-
Gi0/1.20	20	-	100	Standby	10.1.20.254	10.1.20.1	local
Gi0/1.20	20	1	-	Listen	0007.b400.1401	10.1.20.1	-
Gi0/1.20	20	2	-	Active	0007.b400.1402	local	-
Gi0/1.99	99	-	100	Standby	10.1.99.254	10.1.99.1	local
Gi0/1.99	99	1	-	Listen	0007.b400.6301	10.1.99.1	-
Gi0/1.99	99	2	-	Active	0007.b400.6302	local	-

```
R3>
```

The highlighted line above in the **show glbp brief** output shows that R3 is the active forwarder for the MAC address **0007.b400.0a02** and the standby for the MAC address **0007.b400.0a01**. With PC-C being issued the MAC address **0007.b400.0a02**, this demonstrates GLBP's ability to offer simultaneous forwarding and load balancing from the R1 and R3 routing devices participating in GLBP.

The GLBP behavior demonstrated is based on the GLBP default load-balancing algorithm of round-robin. As clients send ARP requests to resolve the MAC address of the default gateway, the AVG reply to each client contains the MAC address of the next possible router in a round-robin fashion.

Load balancing options with GLBP are weighted, host dependent and round robin (default). The load balancing algorithm can be changed using the interface configuration command **glbp group load-balancing[host-dependent | round-robin | weighted]**

Step 18: Configure GLBP interface tracking.

If R1's interface s0/0/0 goes down, clients using R1 as an AVF will not be able to reach the destinations located off of the R2 router. Similarly, if R3's serial interface s0/0/1 goes down, clients using R3 as an AVF will not be able to reach the destinations located off of the R2 router.

GLBP interface tracking uses a weighting mechanism which is different than HSRP or VRRP. With GLBP, two thresholds are defined: one lower threshold that applies when the router loses weight and one upper threshold that applies when the router regains weight. The weighting mechanism offers more flexibility with upper and lower thresholds defined over its counterparts HSRP and VRRP which only allow a single threshold to be defined. If the router priority (or weight) falls below the threshold, the router loses its active state. As soon as the router weight (or priority) exceeds the upper threshold, the router regains its active state.

Because R1's s0/0/0 interface and R3's s0/0/1 interface affect GLBP forwarding operations, we will need to configure tracking on these interfaces. Tracking with GLBP uses objects. The first step is to track the line protocol status of R1's serial interface s0/0/0. On R1, issue the following command:


```
R1(config)# track 15 interface s0/0/0 line-protocol
```

On R1, enter in sub-interface configuration mode for VLAN 10 and configure the weighting mechanism and associate it with the track object number 15.

Consider the example configuration below.

In the first command, R1's g0/1.10 is configured with a **glbp weight** of 110 and lower threshold of 85 and an upper threshold of 105. When the weight falls below the specified lower threshold, the R1 AVF is forced to relinquish its role for the ACTIVE MAC address assigned to it.

In the second command, GLBP weighting is associated with the line protocol status of s0/0/0. If the line protocol state changes, the weight configured for 110 will be decreased by 30 resulting in a weight of 80. R1 would then lose its AVF role until the weight exceeds the upper defined threshold of 105.

```
R1(config)# interface gi0/1.10
R1(config-subif)# glbp 10 weighting 110 lower 85 upper 105
R1(config-subif)# glbp 10 weighting track 15 decrement 30
```

For testing purposes, on a PC that is using R1 as an AVF, start a continuous ping to the destination address 10.1.202.1. This will be useful to demonstrate the automatic failover of one AVF to the other when the tracked object decrements the GLBP weight.

In this lab scenario, SRV1 uses R1 as its default gateway.

Output from SRV1

```
ping 10.1.202.1 -t
```

On R1, shut down the interface s0/0/0.

```
R1(config)# int s0/0/0
R1(config-if)# shutdown
```

Notice the console messages listed below.

```
*Jul 29 12:53:45.263: %TRACK-6-STATE: 15 interface Se0/0/0 line-protocol Up -> Down
*Jul 29 12:53:45.263: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.2 (Serial0/0/0)
is down: interface down
*Jul 29 12:53:47.263: %LINK-5-CHANGED: Interface Serial0/0/0, changed state to
administratively down
*Jul 29 12:53:48.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
*Jul 29 12:54:19.835: %GLBP-6-FWDSTATECHANGE: GigabitEthernet0/1.10 Grp 10 Fwd 1 state
Active -> Listen
```

We see state change of the tracked interface and then the GLBP state of AVF 2 go from an active state to listen.

After the GLBP state change occurs, notice the ping output from the PC. The ping should continue without fail. GLBP failed over automatically to the R3 device and the client experienced no disruption in service.

View the output of the **show glbp** command. Output has been omitted here to only show the output for group 10 since this was the only group in which we applied interface tracking.

```
R1# show glbp
GigabitEthernet0/1.10 - Group 10
  State is Active
    1 state change, last state change 18:04:27
  Virtual IP address is 10.1.10.254
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.288 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 10.1.10.2, priority 100 (expires in 9.376 sec)
  Priority 150 (configured)
  Weighting 80, low (configured 110), thresholds: lower 85, upper 105
  Track object 15 state Down decrement 30
  Load balancing: round-robin
  Group members:
    acf2.c518.0651 (10.1.10.2)
    acf2.c523.7a09 (10.1.10.1) local
  There are 2 forwarders (0 active)
  Forwarder 1
    State is Listen
      2 state changes, last state change 00:05:52
      MAC address is 0007.b400.0a01 (default)
      Owner ID is acf2.c523.7a09
      Redirection enabled
      Preemption enabled, min delay 30 sec
      Active is 10.1.10.2 (secondary), weighting 100 (expires in 10.592
sec)
    Client selection count: 13
  Forwarder 2
    State is Listen
      MAC address is 0007.b400.0a02 (learnt)
      Owner ID is acf2.c518.0651
      Redirection enabled, 599.392 sec remaining (maximum 600 sec)
      Time to live: 14399.392 sec (maximum 14400 sec)
      Preemption enabled, min delay 30 sec
      Active is 10.1.10.2 (primary), weighting 100 (expires in 10.368
sec)
    Client selection count: 13
    <output omitted>
```

The first part of the GLBP output deals with R1's role as an AVG. The AVG role has not been affected by the configuration we applied above. The highlighted portion shows the impact of the interface tracking and weighting mechanism configurations. The weighting mechanism only affects the forwarder role in GLBP.

Notice that R1 is no longer the forwarder for the MAC address 0007.b400.0a01. R1 shows the forwarder roles for both MAC addresses in the listen state.

It is important to note that similar configurations should be applied on R1 for GLBP groups 20 and 99 for consistency of operations. R3 would need to be configured to track the serial interface s0/0/1 and have the weighting mechanism applied as appropriate. To limit the length and time required to perform this lab, these steps have been omitted.

Activate R1 serial interface s0/0/0 using the no shutdown command.

On R1, shutdown the interface s0/0/0.

```
R1(config)# int s0/0/0
R1(config-if)# no shut
```

Use the **show glbp** command to ensure R1 resumed its AVF role.

Step 19: Configure GLBP authentication.

GLBP authentication is important to ensure that no rogue device is allowed join your GLBP group and adversely affect GLBP operations by initiating attacks such as Man-in-the-Middle, etc. GLBP supports two options for authentication: plain text authentication and MD5 authentication. MD5 authentication offers greater security. Using MD5 authentication, a coordinated secret key is used to generate a keyed MD5 hash, which is then included in GLBP packets sent back and forth. A keyed hash of an incoming packet is generated and if the hash within the incoming packet does not match the generated hash the packet is ignored.

Configure the R1 and R3 routers sub-interfaces to support MD5 authentication using the following command:
glbp <0-1023> Group Number authentication md5 key-string cisco123

```
R1(config)# interface GigabitEthernet0/1.10
R1(config-subif)# glbp 10 authentication md5 key-string cisco123

R1(config)# interface GigabitEthernet0/1.20
R1(config-subif)# glbp 20 authentication md5 key-string cisco123

R1(config)# interface GigabitEthernet0/1.99
R1(config-subif)# glbp 99 authentication md5 key-string cisco123
```

NOTE: The cisco123 is used as the shared key password in this lab scenario.

When you added the commands for GLBP authentication to the R1 router, a GLBP state change occurred because only one router was configured with authentication. Now move to R3 router and add glbp authentication to each sub-interface **using the same command with the respective glbp group number and the same key-string shown above.**

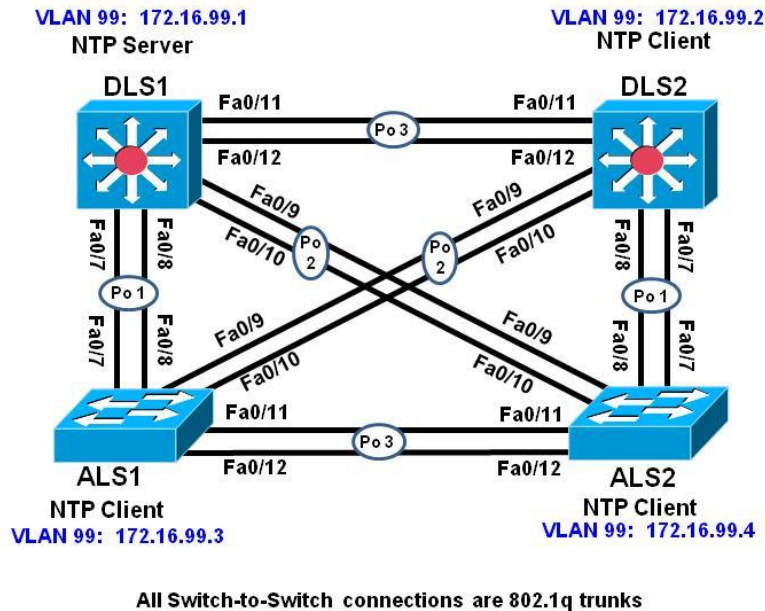
Verify the GLBP operation. Ensure that the R1 is still the AVG and both routers are participating as AVFs for each configured GLBP group. If there is a problem, check the GLBP authentication configuration for errors.

Step 13: End of Lab

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

CCNPv7.1_SWITCH_Lab7-1_NTP_STUDENT

Topology



Objective

- Configure network to synchronize time using the Network Time Protocol.
- Secure NTP using MD5 authentication and access-lists
- Verify NTP Operation

Background

NTP is designed to synchronize the time on network devices. NTP runs over UDP, using port 123 as both the source and destination, which in turn runs over IP. NTP is used to synchronize timekeeping among a set of distributed time servers and clients. A set of nodes on a network is identified and configured with NTP and the nodes form a synchronization subnet, sometimes referred to as an overlay network. While multiple masters (primary servers) may exist, there is no requirement for an election protocol. DLS1 is designated as the authoritative time source in the lab environment. All other devices (DLS2, ALS1, and ALS2) should synchronize to DLS1. NTP is subject to network attacks therefore, we will control the access to the DLS1 switch using NTP authentication and access-lists. The current version is NTP version 4 and is backwards compatible with earlier versions.

Note: This lab uses the Cisco WS-C2960-24TT-L switch with the Cisco IOS image c2960-lanbasek9-mz.150-2.SE6.bin and the Catalyst 3560V2-24PS switch with the Cisco IOS image c3560-ipervicesk9-mz.150-2.SE6.bin. Other switches and Cisco IOS Software versions can be used if they have comparable capabilities and features. 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.

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 Prepare for the Lab

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#
```

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.

- a. 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)# vlan 99
```

```
DLS1(config-vlan)# name Management
```

```
DLS1(config-vlan)# exit
```

```
DLS1(config)# interface vlan 99
```

```
DLS1(config-if)# ip address 172.16.99.1 255.255.255.0
```

```
DLS1(config-if)# no shutdown
```

(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
```

- b. Configure DLS2, ALS1, and ALS2 to use DLS1 as their default gateway.

```
DLS2(config)# ip default-gateway 172.16.99.2
```

Step 1: 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. In the BASE configuration, all interfaces are shut down, so you must remember to issue the **no shutdown** command.

- a. Configure trunks and EtherChannels from DLS1 and DLS2 to the other three switches according to the diagram. The **switchport trunk encapsulation {isl | dot1q}** command is used because these switches also support ISL encapsulation. A sample configuration has been provided to assist you with the trunking and etherchannel configurations.

```
DLS1(config)# interface range fastEthernet 0/7 - 8
```

```
DLS1(config-if-range)# switchport trunk encapsulation dot1q
```

```
DLS1(config-if-range)# switchport mode trunk
```

```
DLS1(config-if-range)# switchport nonegotiate
```

```
DLS1(config-if-range)# channel-group 1 mode desirable
```

```
DLS1(config-if-range)# no shut
```

Creating a port-channel interface Port-channel 1

- b. Configure the trunks and EtherChannel from ALS1 and ALS2 to the other switches. Notice that no encapsulation type is needed because the 2960 supports only 802.1q trunks. A sample configuration has been provided to assist you with the trunking and etherchannel configurations.

```
ALS1(config)# interface range fastEthernet 0/7 - 8
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# switchport nonegotiate
ALS1(config-if-range)# channel-group 1 mode desirable
ALS1(config-if-range)# no shut
```

- a. Verify trunking between DLS1, ALS1, and ALS2 using the **show interface trunk** command on all switches.

```
DLS1# show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Po1	on	802.1q	trunking	1
Po2	on	802.1q	trunking	1
Po3	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Po1	1-4094
Po2	1-4094
Po3	1-4094

Port	Vlans allowed and active in management domain
Po1	1
Po2	1
Po3	1

Port	Vlans in spanning tree forwarding state and not pruned
Po1	1
Po2	1
Po3	1

- b. Issue the **show etherchannel summary** command on each switch to verify the EtherChannels. In the following sample output from ALS1, notice the three EtherChannels on the access and distribution layer switches.

```
ALS1# show etherchannel summary
```

```
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby  (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

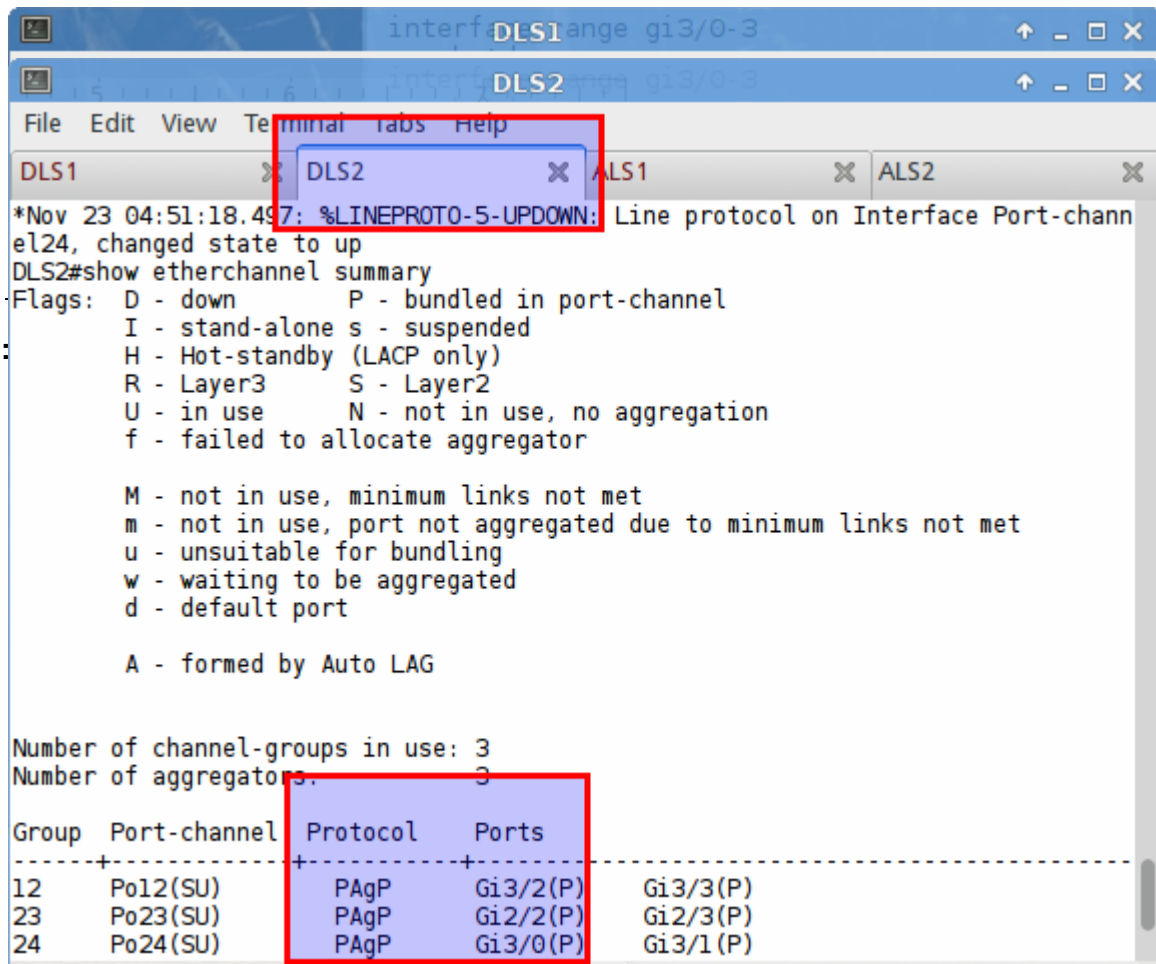
Number of channel-groups in use: 3
 Number of aggregators: 3

Group	Port-channel	Protocol	Ports	
1	Po1 (SU)	PAgP	Fa0/7 (P)	Fa0/8 (P)
2	Po2 (SU)	PAgP	Fa0/9 (P)	Fa0/10 (P)
3	Po3 (SU)	PAgP	Fa0/11 (P)	Fa0/12 (P)

Which EtherChannel negotiation protocol is in use here?

El protocolo de negociación de agregación de enlaces es PagP

Step 2:



tem clock .

- a The system clock can be set using a variety of methods. The system clock can be manually set, the time can be derived from an NTP source or from a subset of NTP (SNTP). It is important that all of your devices have accurate timestamps for use in systems reporting and for tracking validity of X.509 certificates used in Public Key Infrastructure and for event correlation in attack identification.

DLS1# **show clock**
 *00:24:31.647 UTC Mon Mar 1 1993

- b DLS1# The show clock command displays what time is currently set on the device.

On DLS1, manually reconfigure the system clock using the **clock set** command from *privileged exec mode of operation*.

Note that the time you set should be the Coordinated Universal Time value.

```
DLS1# clock set ?
```

```
hh:mm:ss Current Time
```

```
DLS1# clock set 14:45:00 ?
```

```
<1-31> Day of the month
```

```
MONTH Month of the year
```

```
DLS1# clock set 14:45:00 29 ?
```

```
MONTH Month of the year
```

```
DLS1# clock set 14:45:00 29 July ?
```

```
<1993-2035> Year
```

```
DLS1# clock set 14:45:00 29 July 2015
```

```
DLS1#
```

```
*Jul 29 14:45:00.000: %SYS-6-CLOCKUPDATE: System clock has been  
updated from 00:03:21 UTC Mon Mar 1 1993 to 14:45:00 UTC Wed Jul 29  
2015, configured from console by console.
```

- c Verify that the system clock has been updated.

```
DLS1# show clock
```

```
14:45:33.755 UTC Wed Jul 29 2015
```

- d The default timezone is UTC. Change the default timezone to your current timezone and your standard time offset. For this example the system will be set for US Central Standard Time (CST) with a 6 hour negative offset. The -6 is the difference in hours from UTC for US Central Standard Time. Use clock timezone zone hours-offset command in *global configuration*.

```
DLS1# conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
DLS1(config)# clock timezone ?
```

```
WORD name of time zone
```

```
DLS1(config)# clock timezone CST ?
```

```
<-23 - 23> Hours offset from UTC
```

```
DLS1(config)# clock timezone CST -6 ?
```

```
<0-59> Minutes offset from UTC
```

```
<cr>
```

```
DLS1(config)# clock timezone CST -6
```

```
DLS1(config)#
```

```
Jul 29 14:46:26.620: %SYS-6-CLOCKUPDATE: System clock has been updated
from 14:46:26 UTC Wed Jul 29 2015 to 08:46:26 CST Wed Jul 29 2015,
configured from console by console
```

- e The command **clock summer-time** command can be used to automatically switch between standard time and daylight saving time. If you do not use this command, the system will default to using daylight savings rules for the United States.

```
DLS1(config)# clock summer-time ?
WORD    name of time zone in summer
```

```
DLS1(config)# clock summer-time CDT ?
date          Configure absolute summer time
recurring     Configure recurring summer time
```

```
DLS1(config)# clock summer-time CDT recurring ?
<1-4>         Week number to start
first         First week of the month
last          Last week of the month
<cr>
```

```
DLS1(config)# clock summer-time CDT recurring
```

```
DLS1(config)#
```

```
Jul 29 14:47:20.249: %SYS-6-CLOCKUPDATE: System clock has been updated
from 08:47:20 CST Wed Jul 29 2015 to 09:47:20 CDT Wed Jul 29 2015,
configured from console by console]
```

Verify clock settings using the **show clock** command with the keyword **detail**.

```
DLS1# show clock detail
09:48:11.679 CDT Wed Jul 29 2015
Time source is user configuration
Summer time starts 02:00:00 CST Sun Mar 8 2015
Summer time ends 02:00:00 CDT Sun Nov 1 2015
```

The clock setting should reflect the current local time, adjusted for daylight savings as appropriate.

Setting the clocks manually is not considered an accurate method of tracking time and events in networks. It is also not a scalable solution to manually configure time on all network devices. The Network Time Protocol (NTP) allows the network device to poll an authoritative time source for synchronization.

En las imágenes que se presentan a continuación se muestra la configuración de la zona horaria en COT a -5 horas de UTC, y luego el ajuste del reloj:

```
DLS1(config)#clock timezone COT -5
DLS1(config)#
Nov 23 00:07:07.694: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:07:07 UTC Thu Nov 23 2017 to 19:07:07 COT Wed Nov 22 2017, configured from console by console.
DLS1(config)#exit
DLS1#clock set 00:05:10 23 NOVEMBER 2017
Nov 23 00:07:34.113: %SYS-5-CONFIG_I: Configured from console by console
DLS1#clock set 00:05:10 23 NOVEMBER 2017
DLS1#
Nov 23 05:05:10.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 19:07:36 COT Wed Nov 22 2017 to 00:05:10 COT Thu Nov 23 2017, configured from console by console.
DLS1#
```

```
DLS1#show clock
00:05:49.109 COT Thu Nov 23 2017
DLS1#
DLS1#
DLS1#show clock detail
00:06:19.523 COT Thu Nov 23 2017
Time source is user configuration
DLS1#
```

Step 3: Configure NTP.

NTP is used to make sure all network devices in the campus are synchronized. Time accuracy can be derived from three different external sources: Atomic clock, GPS receiver, and accurate time source. NTP synchronizes using UDP port 123. All of the devices must be configured with NTP.

- Configure DLS1 as the authoritative time source in the campus network by using the **ntp master** command.

```
DLS1(config)# ntp master ?
<1-15> Stratum number
<cr>
```

This command should only be used if you do not have a reliable external reference clock. We will use **ntp master stratum_number** command in global configuration mode. The stratum number should be configured with a high number in the event that there is more reliable NTP source available. A machine running NTP automatically chooses the machine with the lowest stratum number that is configured to communicate with using NTP as its time source. The lower the stratum number the more trustworthy the accuracy of the time source.

```
DLS1(config)# ntp master 10
```

Aquí se muestra la configuración establecida en DLS1:

```
DLS1(config)#ntp master 10
DLS1(config)#exit
```

- Configure DLS2, ALS1, and ALS2 to synchronize to DLS1 using the **ntp server A.B.C.D** (IP address of peer) command. NTP synchronization should always refer to the most stable interface. Loopback

interfaces are considered always up interfaces and therefore, the best choice for NTP synchronization. Also, the local time zone should be configured on each local device. Also, configure these devices with the same time zone and summer time configuration as on DLS1.

```
DLS2(config)# ntp server ?
A.B.C.D      IP address of peer
WORD         Hostname of peer
X:X:X:X::X   IPv6 address of peer
ip           Use IP for DNS resolution
ipv6         Use IPv6 for DNS resolution
vrf          VPN Routing/Forwarding Information
```

```
DLS2(config)# ntp server 172.16.99.1
```

```
DLS2(config)# clock timezone CST -6
```

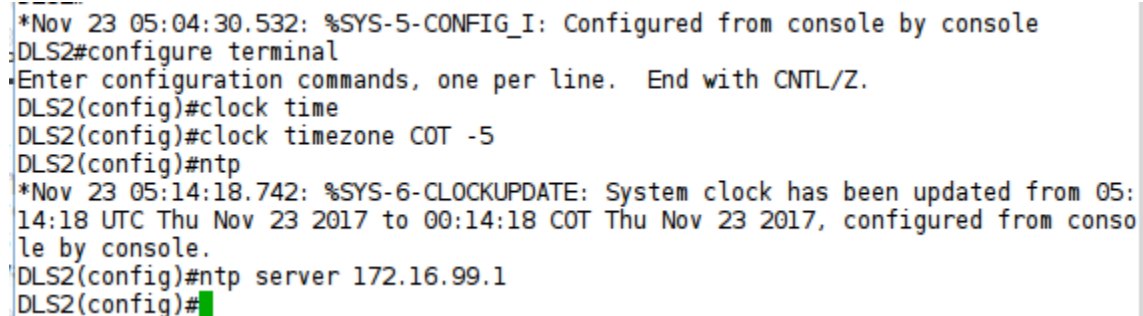
```
*Jul 29 14:50:38.980: %SYS-6-CLOCKUPDATE: System clock has been
updated from 14:50:38 UTC Wed Jul 29 2015 to 08:50:38 CST Wed Jul 29
2015, configured from console by console.
```

```
DLS2(config)# clock summer-time CDT recurring
```

```
DLS2(config)#
```

```
Jul 29 14:50:54.247: %SYS-6-CLOCKUPDATE: System clock has been updated
from 08:50:54 CST Wed Jul 29 2015 to 09:50:54 CDT Wed Jul 29 2015,
configured from console by console.
```

Aquí se puede apreciar la configuración que se estableció en DLS2 por ejemplo:



```
*Nov 23 05:04:30.532: %SYS-5-CONFIG_I: Configured from console by console
DLS2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DLS2(config)#clock time
DLS2(config)#clock timezone COT -5
DLS2(config)#ntp
*Nov 23 05:14:18.742: %SYS-6-CLOCKUPDATE: System clock has been updated from 05:
14:18 UTC Thu Nov 23 2017 to 00:14:18 COT Thu Nov 23 2017, configured from conso
le by console.
DLS2(config)#ntp server 172.16.99.1
DLS2(config)#
```

NOTE: Ensure that these commands are repeated on ALS1 and ALS2.

Step 4: Verify NTP .

On DLS2, ALS1, and ALS2, use the **show ntp status** command to verify if these device clocks have synchronized to DLS1.

```
DLS2# show ntp status
```

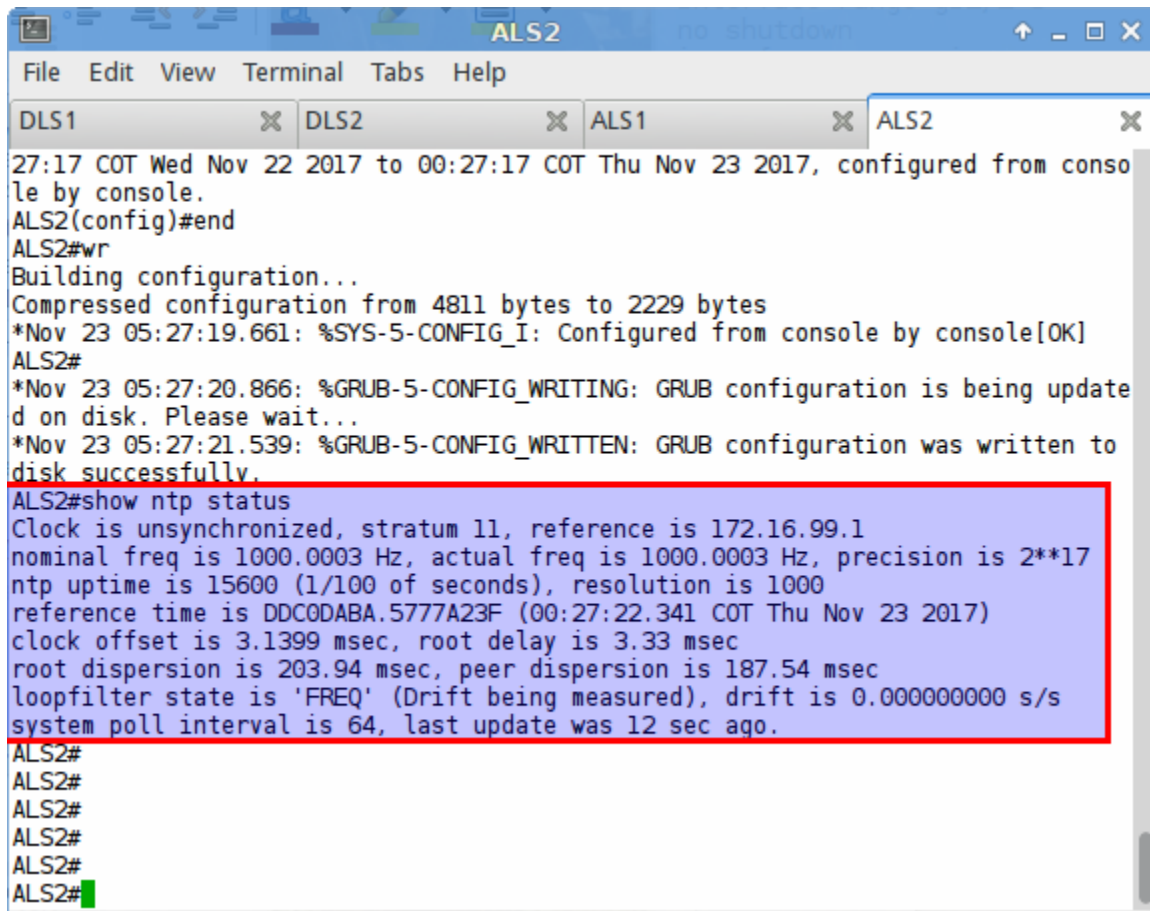
```
Clock is synchronized, stratum 11, reference is 172.16.99.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**17
reference time is D96366D1.B4DD4BA4 (09:50:57.706 CDT Wed Jul 29 2015)
clock offset is -0.2067 msec, root delay is 2.03 msec
root dispersion is 195.31 msec, peer dispersion is 1.55 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000002 s/s
system poll interval is 64, last update was 165 sec ago
```

Outputs for ALS1 and ALS2 should be similar to the output displayed above for DLS2.

The stratum will be +1 from the stratum value used on the master in the network. In this lab scenario, we use ntp master 10. This indicates a stratum of $10 + 1 = 11$. The stratum 11 is indicated in the show output.

NOTE: NTP may take up to 5 minutes to synchronize.

Aquí se puede apreciar el cambio que entregó NTP server a sus clientes:



```
File Edit View Terminal Tabs Help
DLS1 x DLS2 x ALS1 x ALS2 x
27:17 COT Wed Nov 22 2017 to 00:27:17 COT Thu Nov 23 2017, configured from console by console.
ALS2(config)#end
ALS2#wr
Building configuration...
Compressed configuration from 4811 bytes to 2229 bytes
*Nov 23 05:27:19.661: %SYS-5-CONFIG_I: Configured from console by console[OK]
ALS2#
*Nov 23 05:27:20.866: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Nov 23 05:27:21.539: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
ALS2#show ntp status
Clock is unsynchronized, stratum 11, reference is 172.16.99.1
nominal freq is 1000.0003 Hz, actual freq is 1000.0003 Hz, precision is 2**17
ntp uptime is 15600 (1/100 of seconds), resolution is 1000
reference time is DDC0DABA.5777A23F (00:27:22.341 COT Thu Nov 23 2017)
clock offset is 3.1399 msec, root delay is 3.33 msec
root dispersion is 203.94 msec, peer dispersion is 187.54 msec
loopfilter state is 'FREQ' (Drift being measured), drift is 0.000000000 s/s
system poll interval is 64, last update was 12 sec ago.
ALS2#
ALS2#
ALS2#
ALS2#
ALS2#
ALS2#
```

Part 2: Secure NTP Operation using Access-Lists and Authentication

Step 1: Secure NTP Operation using Access-Lists and Authentication

NTP operation can be secured using MD5 authentication. Authentication is enabled with the **ntp authenticate** command. The authentication keys are defined with **ntp authentication-key** command. The number specifies a unique NTP key. Valid keys are identified using the **ntp-trusted-key** command. It is important to note that NTP does not authenticate clients. NTP authenticates the source. Devices can still respond to unauthenticated requests. For this reason, access lists should be used in conjunction with NTP authentication to restrict NTP access.

- a. Configure NTP authentication on DLS1 and DLS2.

```
DLS1(config)# ntp authenticate
DLS1(config)# ntp authentication-key 1 md5 P@55word
DLS1(config)# ntp trusted-key 1
```

```

DLS1#
DLS1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DLS1(config)#ntp authenticate
DLS1(config)#ntp authentication-key 1 md5 P@55word
DLS1(config)#ntp trusted-key 1
DLS1(config)#

```

Use the **show ntp status** command to verify that clock is still synchronized (note that it could take 5 minutes to resynchronize). The system clock is not reset, just the NTP relationship). If the clock shows unsynchronized, the client has not successfully authenticated.

```
DLS2# show ntp status
```

```

Clock is synchronized, stratum 11, reference is 172.16.99.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**17
reference time is D9636A49.B36724F9 (10:05:45.700 CDT Wed Jul 29 2015)
clock offset is -0.3060 msec, root delay is 2.50 msec
root dispersion is 68.07 msec, peer dispersion is 0.10 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000003 s/s
system poll interval is 128, last update was 12 sec ago.

```

- b. Repeat these commands on ALS1 and ALS2. Verify that the device clocks are synchronized using the appropriate show command.

Aquí se muestra que DLS2 ha realizado la sincronización después de autenticarse:

```

DLS2#show run
DLS2#show running-config | se
Nov 23 05:42:28.867: %SYS-5-CONFIG_I: Configured from console by console
DLS2#show running-config | section ntp
ntp authentication-key 1 md5 12292542471C03162E 7
ntp authenticate
ntp trusted-key 1
ntp update-calendar
ntp server 172.16.99.1
DLS2#show ntp status
Clock is synchronized, stratum 11, reference is 172.16.99.1
nominal freq is 1000.0003 Hz, actual freq is 999.5003 Hz, precision is 2**16
ntp uptime is 196700 (1/100 of seconds), resolution is 1001
reference time is DDC0DE3D.CA694169 (00:42:21.790 COT Thu Nov 23 2017)
clock offset is 7.5149 msec, root delay is 3.29 msec
root dispersion is 7946.34 msec, peer dispersion is 7937.51 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000499999 s/s
system poll interval is 64, last update was 62 sec ago.
DLS2#

```

Step 2: Control NTP Access using Access-Lists

Time Servers can provide synchronization services in all directions to other devices in your network. A rogue NTP server to come in and falsify time on your network. Also, a rogue device could send a large number of bogus synchronization requests to your server preventing it from servicing legitimate devices. Configure an access-list so that polling can only come from members of the 172.16.0.0/16 network. NTP masters must allow "peer" access to source with IP address 127.127.x.1. This IP address is the internal server address

created by the NTP master command. The local router synchronizes using this IP. View the output for the **show ntp associations** command. If your device is configured as NTP master, then you must allow access to source IP of 127.127.x.1. This is because 127.127.x.1 is the internal server that is created by the **ntp master** command. The value of the third octet varies between platforms.

```
DLS1# show ntp associations
```

```
address          ref clock      st   when   poll reach  delay  offset  disp
*~127.127.1.1    .LOCL.        9    12     16   377   0.000   0.000  0.226
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
DLS1#
```

Use the following commands to ensure that only devices on the 172.16.0.0/16 network are able to poll or send requests to the NTP server. The **ntp access-group peer** command allows the devices to synchronize itself to remote systems that pass the access-list. Time synchronization and control queries are allowed.

```
DLS1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
DLS1(config)# access-list 1 permit 127.127.1.1
DLS1(config)# access-list 2 permit 172.16.0.0 0.0.255.255
DLS1(config)#
DLS1(config)# ntp access-group ?
peer          Provide full access
query-only    Allow only control queries
serve         Provide server and query access
serve-only    Provide only server access

DLS1(config)# ntp access-group peer 1
DLS1(config)# ntp access-group serve-only 2
DLS1(config)# end
DLS1#
```

This command references the source address listed in **access-list 2** to determine if NTP services will be rendered to the requesting device.

Aquí se puede ver la configuración de la ACL para NTP en DLS1:


```

DLS1#show ntp associations
  address      ref clock      st  when  poll reach  delay  offset  disp
*~127.127.1.1  .LOCL.             9    0    16   377  0.000   0.000  0.246
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
DLS1#access-list 1 permit 127.127.1.1
^
% Invalid input detected at '^' marker.

DLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#accessli
DLS1(config)#access-list 1 permit 127.127.1.1
DLS1(config)#access-list 2 permit 172.16.0.0 0.0.255.255
DLS1(config)#ntp access-group peer 1
DLS1(config)#ntp access-group serve-only 2
DLS1(config)#

```

Step 3: Verify NTP on all devices.

Use the **show ntp associations**, **show ntp status**, **show clock detail** commands to verify synchronization and configurations across the campus network.

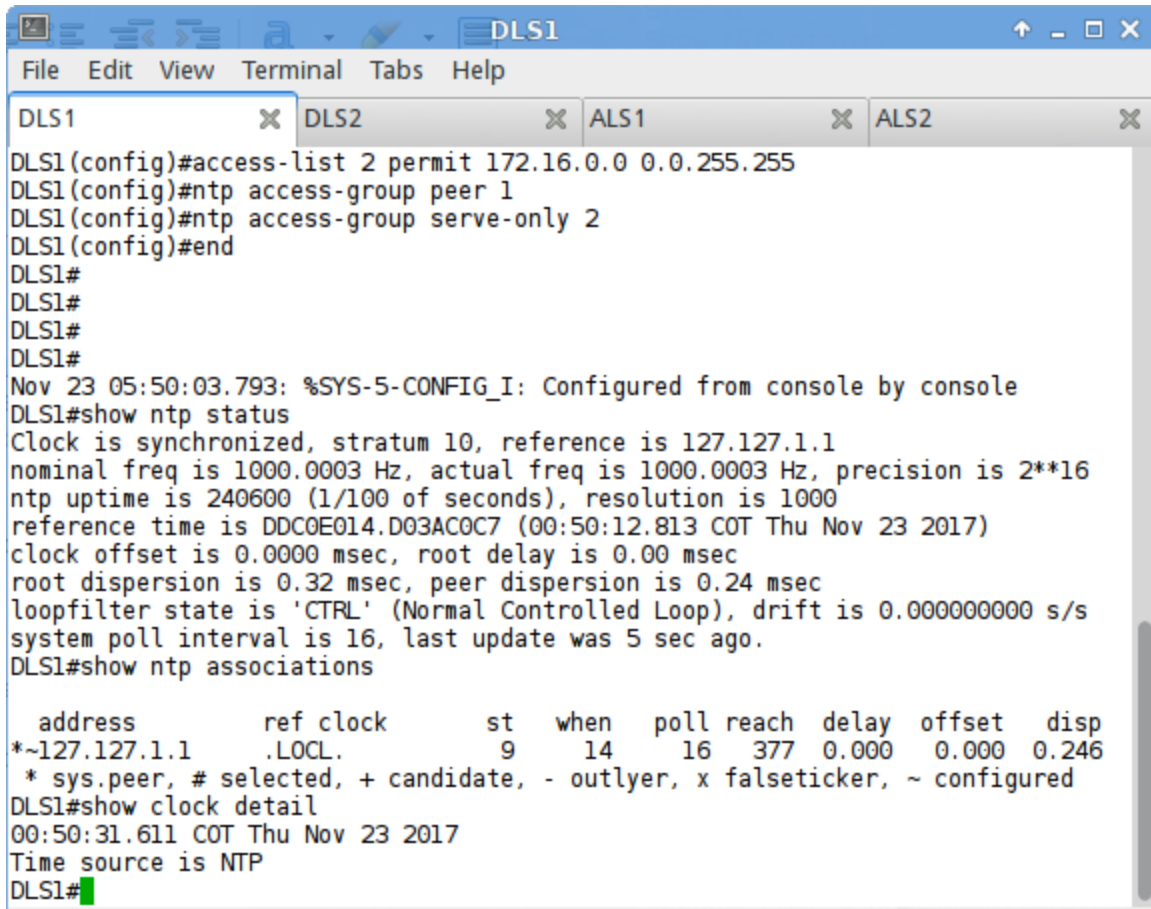
```

DLS1# show ntp status
Clock is synchronized, stratum 10, reference is 127.127.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**17
reference time is D963700D.38FAF326 (10:30:21.222 CDT Wed Jul 29 2015)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.48 msec, peer dispersion is 0.25 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 15 sec ago.

DLS1# show ntp associations

  address      ref clock      st  when  poll reach  delay  offset  disp
*~127.127.1.1  .LOCL.             9    0    16   377  0.000   0.000  0.244
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
DLS1#
DLS1# show clock detail
10:31:16.453 CDT Wed Jul 29 2015
Time source is NTP
Summer time starts 02:00:00 CST Sun Mar 8 2015
Summer time ends 02:00:00 CDT Sun Nov 1 2015

```



```
DLS1
DLS1(config)#access-list 2 permit 172.16.0.0 0.0.255.255
DLS1(config)#ntp access-group peer 1
DLS1(config)#ntp access-group serve-only 2
DLS1(config)#end
DLS1#
DLS1#
DLS1#
DLS1#
Nov 23 05:50:03.793: %SYS-5-CONFIG_I: Configured from console by console
DLS1#show ntp status
Clock is synchronized, stratum 10, reference is 127.127.1.1
nominal freq is 1000.0003 Hz, actual freq is 1000.0003 Hz, precision is 2**16
ntp uptime is 240600 (1/100 of seconds), resolution is 1000
reference time is DDC0E014.D03AC0C7 (00:50:12.813 COT Thu Nov 23 2017)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.32 msec, peer dispersion is 0.24 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 5 sec ago.
DLS1#show ntp associations

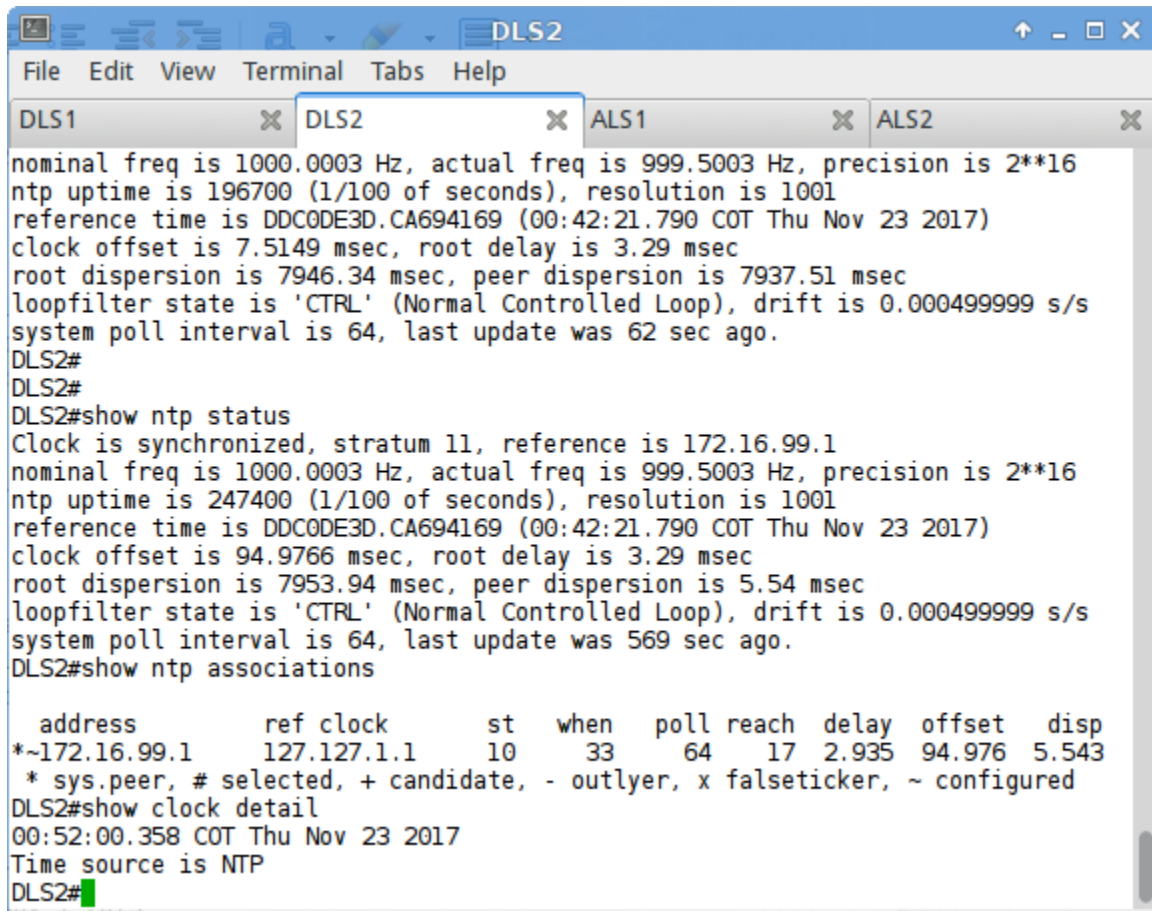
address          ref clock      st  when  poll reach delay offset disp
*~127.127.1.1    .LOCL.         9   14    16   377  0.000  0.000  0.246
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
DLS1#show clock detail
00:50:31.611 COT Thu Nov 23 2017
Time source is NTP
DLS1#
```

Compare the output on DLS2 to ALS1 and ALS2 devices.

```
DLS2# show ntp status
Clock is synchronized, stratum 11, reference is 172.16.99.1
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**17
reference time is D9636FBE.B4569C10 (10:29:02.704 CDT Wed Jul 29 2015)
clock offset is 0.3609 msec, root delay is 1.99 msec
root dispersion is 7.82 msec, peer dispersion is 3.64 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000003 s/s
system poll interval is 128, last update was 170 sec ago.
DLS2#
DLS2# show ntp associations

address          ref clock      st  when  poll reach delay offset disp
*~172.16.99.1    127.127.1.1    10  176   128  376  1.990  0.360  3.642
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
DLS2#
DLS2# show clock detail
10:32:02.545 CDT Wed Jul 29 2015
Time source is NTP
Summer time starts 02:00:00 CST Sun Mar 8 2015
```

Summer time ends 02:00:00 CDT Sun Nov 1 2015



```
DLS2
File Edit View Terminal Tabs Help
DLS1 x DLS2 x ALS1 x ALS2 x
nominal freq is 1000.0003 Hz, actual freq is 999.5003 Hz, precision is 2**16
ntp uptime is 196700 (1/100 of seconds), resolution is 1001
reference time is DDCODE3D.CA694169 (00:42:21.790 COT Thu Nov 23 2017)
clock offset is 7.5149 msec, root delay is 3.29 msec
root dispersion is 7946.34 msec, peer dispersion is 7937.51 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000499999 s/s
system poll interval is 64, last update was 62 sec ago.
DLS2#
DLS2#
DLS2#show ntp status
Clock is synchronized, stratum 11, reference is 172.16.99.1
nominal freq is 1000.0003 Hz, actual freq is 999.5003 Hz, precision is 2**16
ntp uptime is 247400 (1/100 of seconds), resolution is 1001
reference time is DDCODE3D.CA694169 (00:42:21.790 COT Thu Nov 23 2017)
clock offset is 94.9766 msec, root delay is 3.29 msec
root dispersion is 7953.94 msec, peer dispersion is 5.54 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000499999 s/s
system poll interval is 64, last update was 569 sec ago.
DLS2#show ntp associations

  address          ref clock      st  when  poll reach  delay  offset  disp
*~172.16.99.1      127.127.1.1    10   33    64   17  2.935  94.976  5.543
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
DLS2#show clock detail
00:52:00.358 COT Thu Nov 23 2017
Time source is NTP
DLS2#
```

ALS1# **show ntp status**

```
Clock is synchronized, stratum 11, reference is 172.16.99.1
nominal freq is 119.2092 Hz, actual freq is 119.2093 Hz, precision is 2**17
reference time is D9636FCD.C3C21CD9 (10:29:17.764 CDT Wed Jul 29 2015)
clock offset is -2.6199 msec, root delay is 2.16 msec
root dispersion is 13.73 msec, peer dispersion is 67.34 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000145 s/s
system poll interval is 64, last update was 225 sec ago.
```

ALS1#

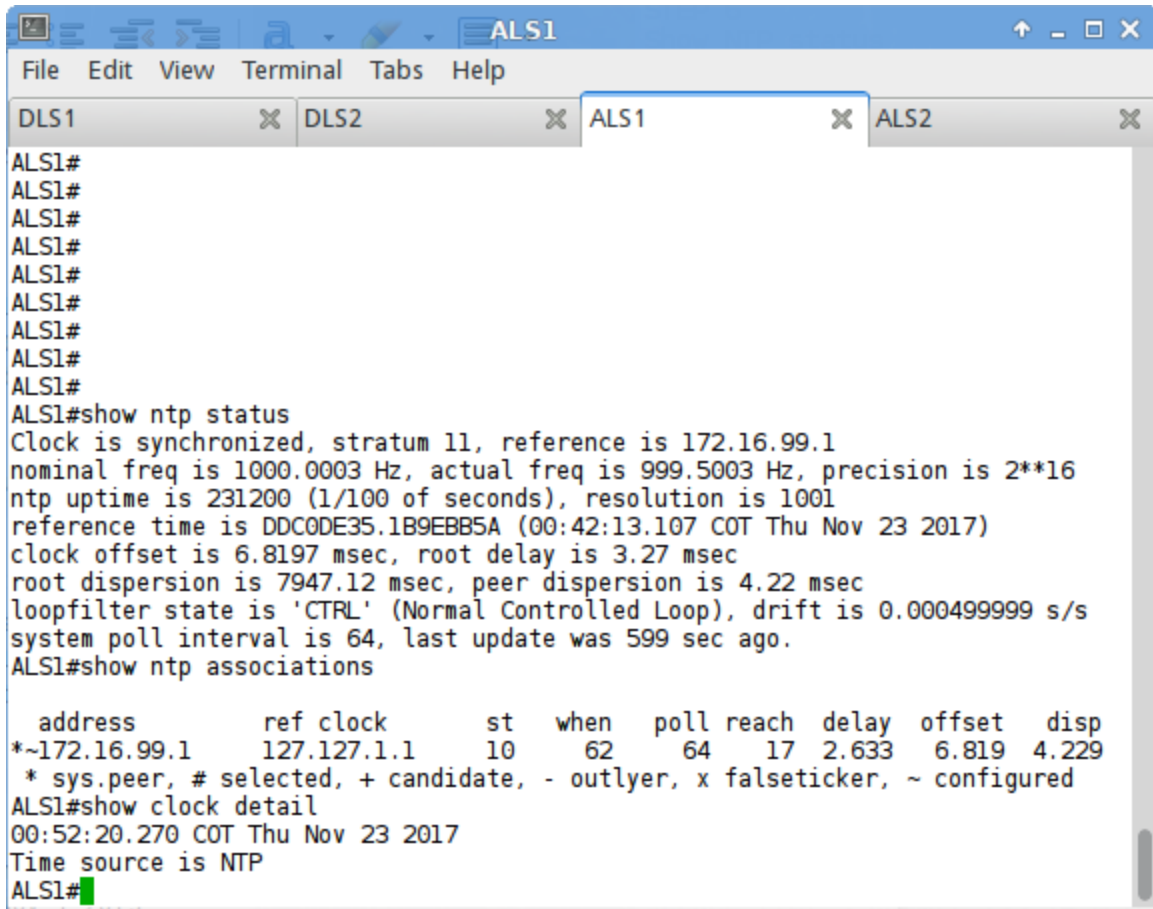
ALS1# **show ntp associations**

```
  address          ref clock      st  when  poll reach  delay  offset  disp
*~172.16.99.1      127.127.1.1    10  229    64  370  2.165  -2.619  67.347
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

ALS1#

ALS1# **show clock detail**

```
10:33:12.625 CDT Wed Jul 29 2015
Time source is NTP
Summer time starts 02:00:00 CST Sun Mar 8 2015
Summer time ends 02:00:00 CDT Sun Nov 1 2015
```



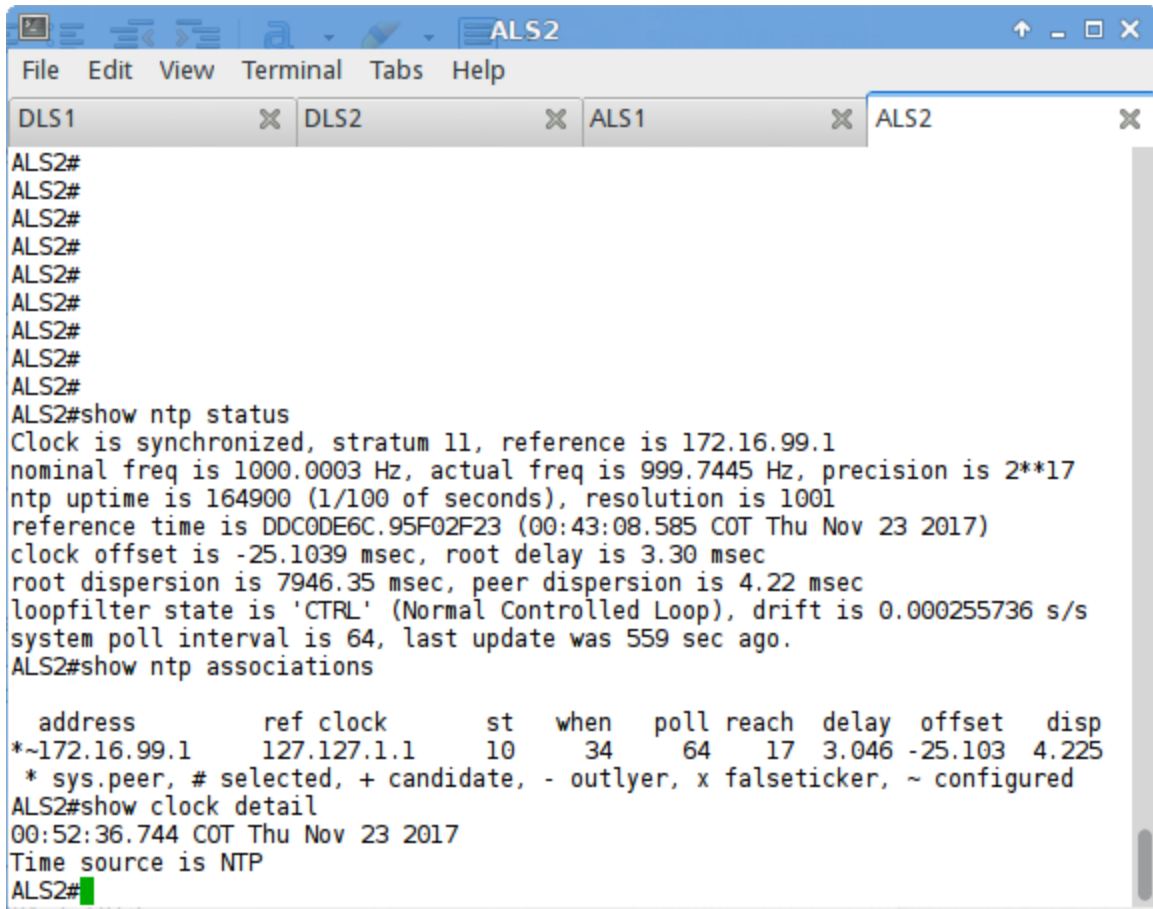
The screenshot shows a terminal window with a blue title bar labeled 'ALS1'. The menu bar includes 'File', 'Edit', 'View', 'Terminal', 'Tabs', and 'Help'. There are four tabs at the top: 'DLS1', 'DLS2', 'ALS1' (which is active), and 'ALS2'. The terminal content shows the user at the 'ALS1#' prompt. They enter 'show ntp status', which displays the following information: 'Clock is synchronized, stratum 11, reference is 172.16.99.1', 'nominal freq is 1000.0003 Hz, actual freq is 999.5003 Hz, precision is 2**16', 'ntp uptime is 231200 (1/100 of seconds), resolution is 1001', 'reference time is DDCODE35.1B9EBB5A (00:42:13.107 COT Thu Nov 23 2017)', 'clock offset is 6.8197 msec, root delay is 3.27 msec', 'root dispersion is 7947.12 msec, peer dispersion is 4.22 msec', 'loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000499999 s/s', and 'system poll interval is 64, last update was 599 sec ago.' Then, they enter 'show ntp associations', which shows a table of associations. The table has columns: 'address', 'ref clock', 'st', 'when', 'poll', 'reach', 'delay', 'offset', and 'disp'. The first entry is '*~172.16.99.1 127.127.1.1 10 62 64 17 2.633 6.819 4.229'. Below the table is a legend: '* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured'. Finally, they enter 'show clock detail', which shows '00:52:20.270 COT Thu Nov 23 2017' and 'Time source is NTP'. The prompt 'ALS1#' is visible at the bottom.

```
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#show ntp status
Clock is synchronized, stratum 11, reference is 172.16.99.1
nominal freq is 1000.0003 Hz, actual freq is 999.5003 Hz, precision is 2**16
ntp uptime is 231200 (1/100 of seconds), resolution is 1001
reference time is DDCODE35.1B9EBB5A (00:42:13.107 COT Thu Nov 23 2017)
clock offset is 6.8197 msec, root delay is 3.27 msec
root dispersion is 7947.12 msec, peer dispersion is 4.22 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000499999 s/s
system poll interval is 64, last update was 599 sec ago.
ALS1#show ntp associations

  address      ref clock      st   when   poll reach  delay  offset  disp
*~172.16.99.1  127.127.1.1    10    62     64   17  2.633   6.819  4.229
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
ALS1#show clock detail
00:52:20.270 COT Thu Nov 23 2017
Time source is NTP
ALS1#
```

```
ALS2# show ntp status
Clock is synchronized, stratum 11, reference is 172.16.99.1
nominal freq is 119.2092 Hz, actual freq is 119.2093 Hz, precision is 2**17
reference time is D9636E71.F02399BE (10:23:29.938 CDT Wed Jul 29 2015)
clock offset is -5.3988 msec, root delay is 1.81 msec
root dispersion is 18.57 msec, peer dispersion is 195.04 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000103 s/s
system poll interval is 64, last update was 624 sec ago.
ALS2#
ALS2# show ntp associations

  address      ref clock      st   when   poll reach  delay  offset  disp
*~172.16.99.1  127.127.1.1    10   306     64   360  1.811  -5.398 195.04
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
ALS2#
ALS2# show clock detail
10:34:04.084 CDT Wed Jul 29 2015
Time source is NTP
Summer time starts 02:00:00 CST Sun Mar 8 2015
Summer time ends 02:00:00 CDT Sun Nov 1 2015
```



```
ALS2#
ALS2#
ALS2#
ALS2#
ALS2#
ALS2#
ALS2#
ALS2#
ALS2#show ntp status
Clock is synchronized, stratum 11, reference is 172.16.99.1
nominal freq is 1000.0003 Hz, actual freq is 999.7445 Hz, precision is 2**17
ntp uptime is 164900 (1/100 of seconds), resolution is 1001
reference time is DDC0DE6C.95F02F23 (00:43:08.585 COT Thu Nov 23 2017)
clock offset is -25.1039 msec, root delay is 3.30 msec
root dispersion is 7946.35 msec, peer dispersion is 4.22 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000255736 s/s
system poll interval is 64, last update was 559 sec ago.
ALS2#show ntp associations

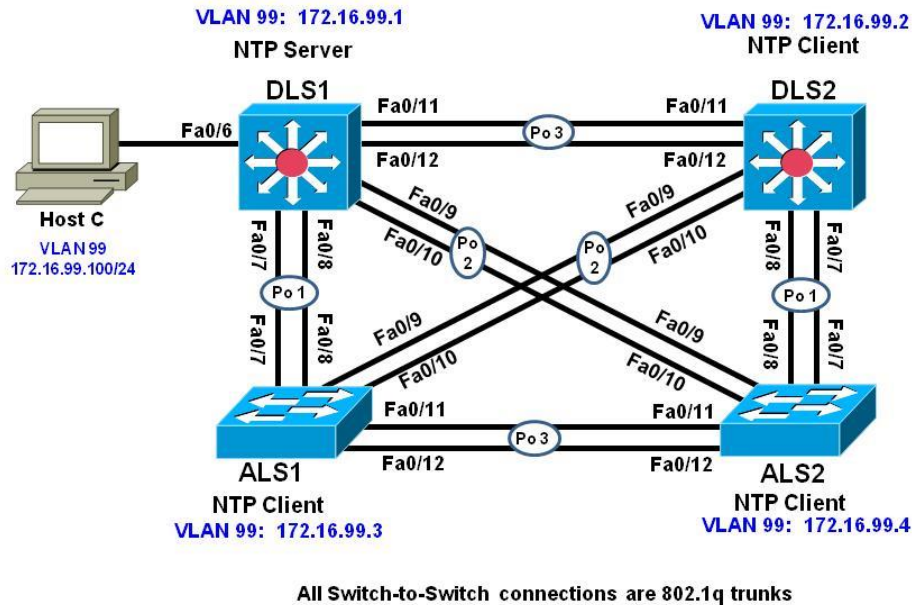
   address          ref clock       st   when  poll reach  delay  offset  disp
*~172.16.99.1      127.127.1.1     10    34    64    17  3.046 -25.103  4.225
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
ALS2#show clock detail
00:52:36.744 COT Thu Nov 23 2017
Time source is NTP
ALS2#
```

Step 4: End of Lab.

Save your configurations. The equipment should be in the correct end state from this lab for Lab 7-2, SNMP.

CCNPv7.1_SWITCH_Lab7-2_SNMP_STUDENT

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 2: 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.

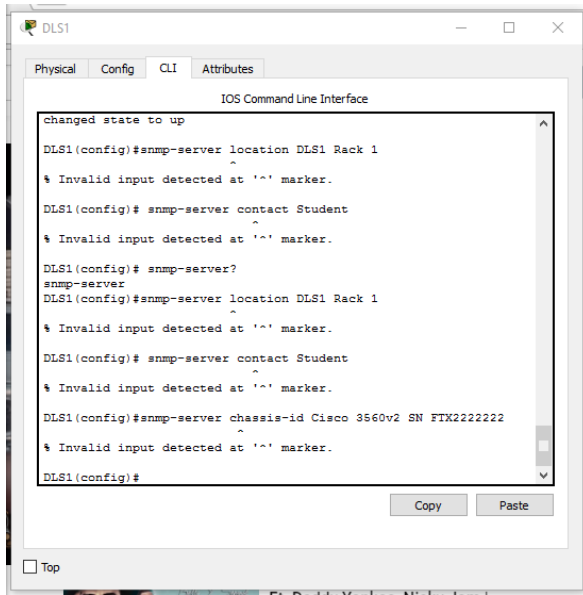
Part 3: Configure general SNMP parameters

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
```

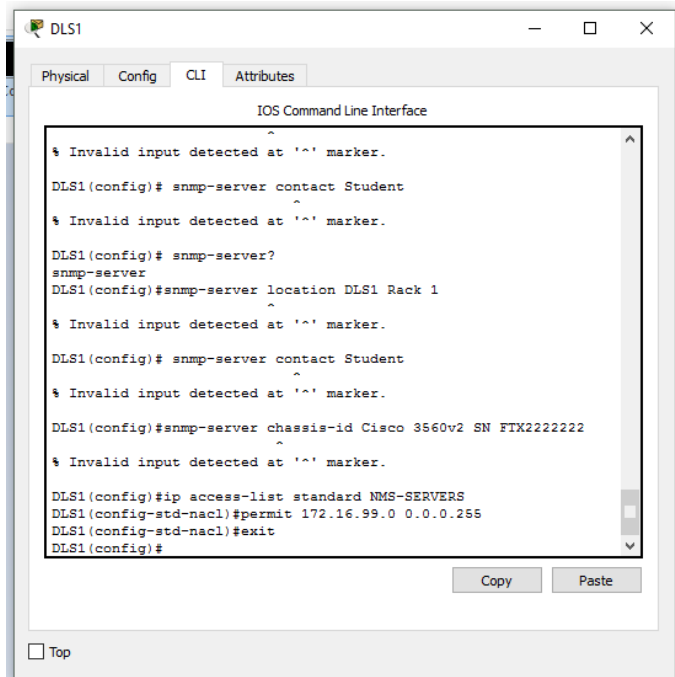


Step 2: Configure access-lists for SNMP.

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.

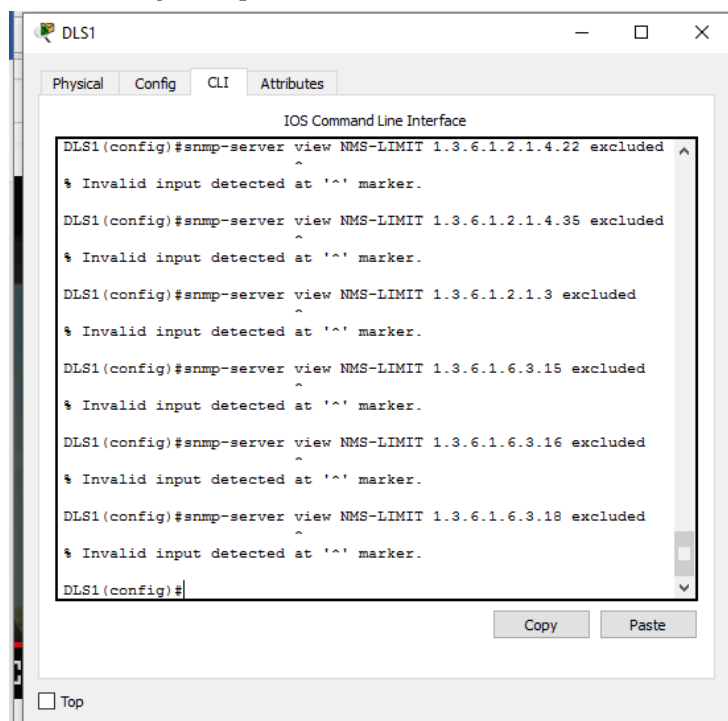
Access to the MIB is open access by default, and any authorized user can read or change the value of any OID in the MIB. Besides the ACL, you should also configure SNMP VIEWS. A view specifically allows or disallows access to certain parts of the MIB, which can provide both security and help control 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 4: Configure DLS1 and DLS2 for SNMPv3

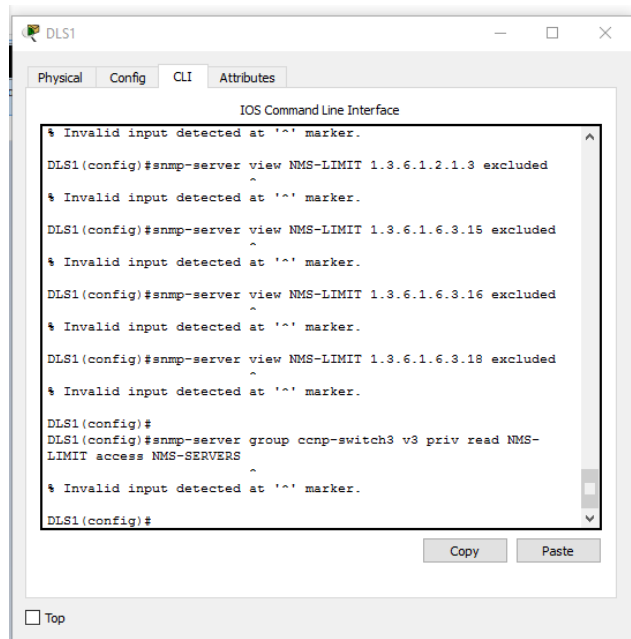
Step 1: Configure SNMP groups.

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:

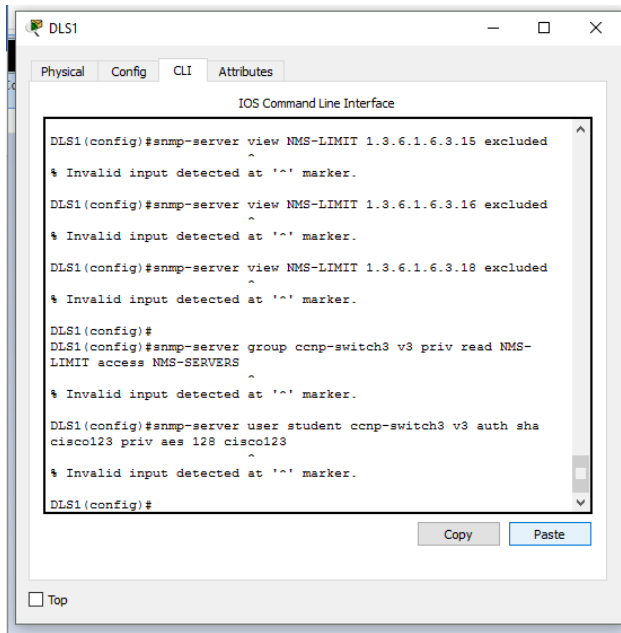
```
DLS1(config)# snmp-server group ccnp-switch3 v3 priv read NMS-LIMIT access NMS-SERVERS
```



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:

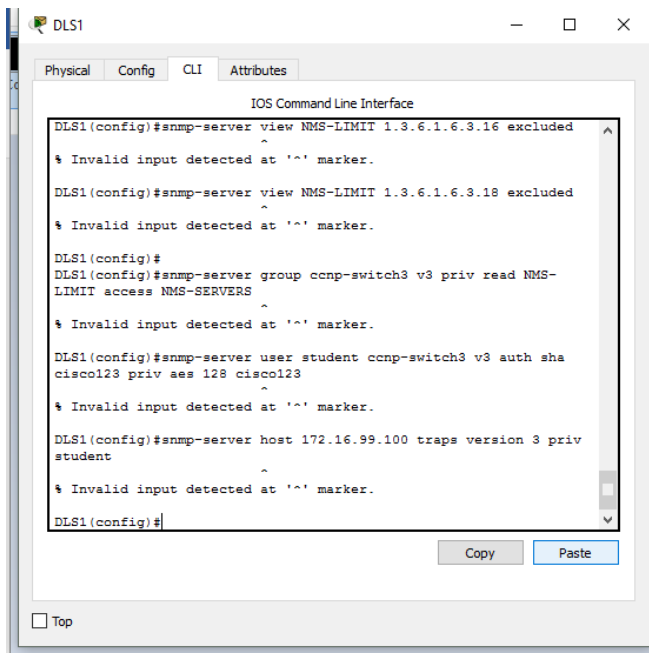
```
Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...
```

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:

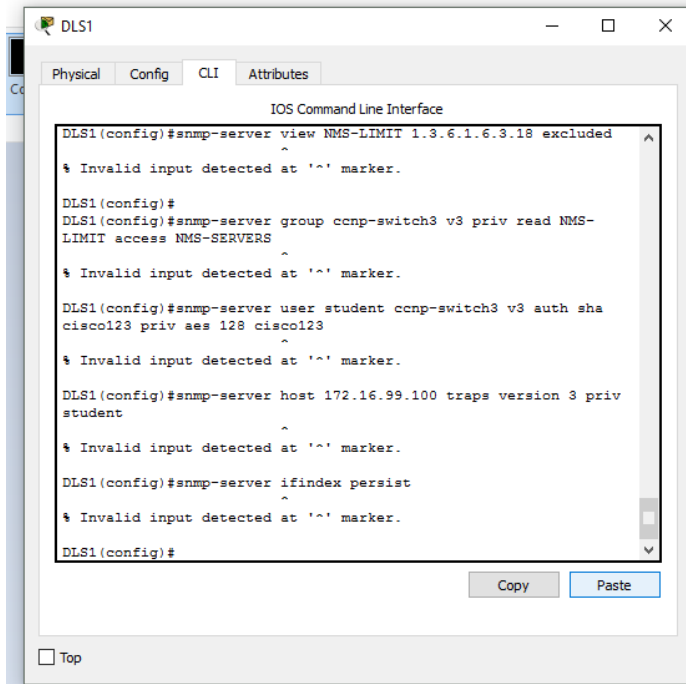
```
DLS1(config)# snmp-server host 172.16.99.100 traps version 3 priv student
```



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:

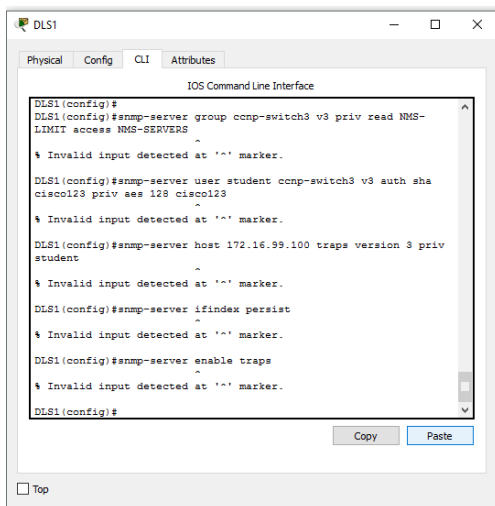
```
DLS1(config)# snmp-server ifindex persist
```



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
```



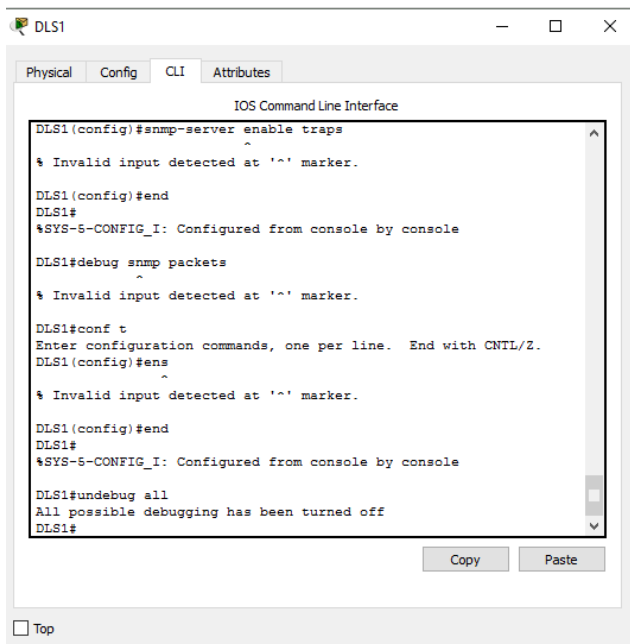
Step 6: Verify SNMP configuration.

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

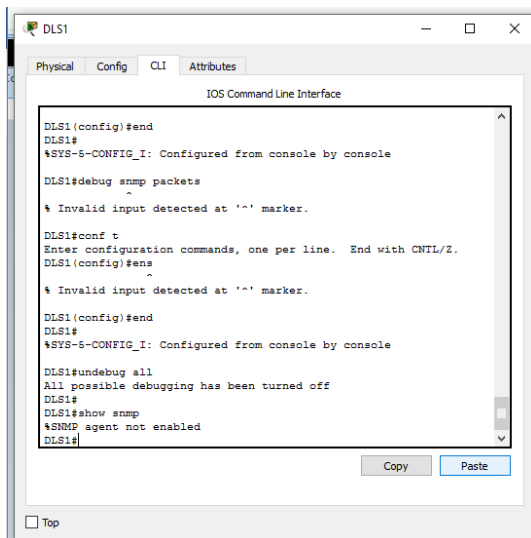
```

```

    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:

```

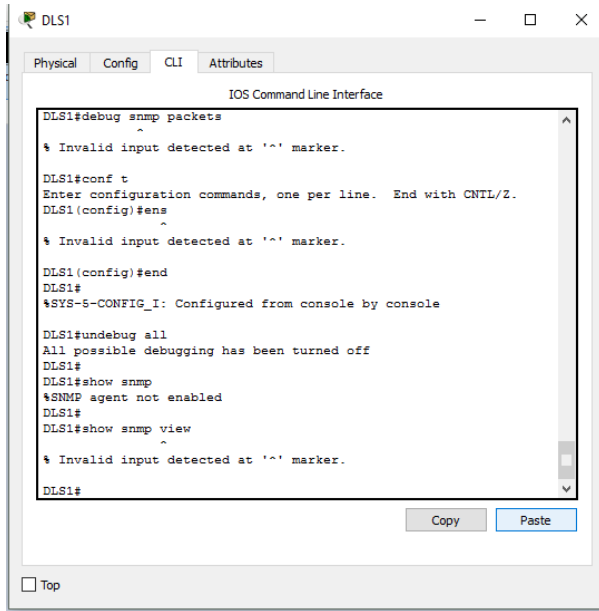
DLS1# show snmp view
cac_view pimMIB - included read-only active
cac_view msdpMIB - included read-only active
cac_view ip - included read-only active
cac_view ospf - included read-only active
cac_view bgp - included read-only active
cac_view dot1dBridge - included read-only active
cac_view ipMRRouteStdMIB - 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 ciscoIetfIisisMIB - 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
vldefault iso - included permanent active
vldefault internet - included permanent active
vldefault snmpUsmMIB - excluded permanent active
vldefault snmpVacmMIB - excluded permanent active
vldefault snmpCommunityMIB - excluded permanent active
vldefault ciscoMgmt.252 - excluded permanent active
*tv.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.F
FFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF0F iso - included volatile active
*tv.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.F
FFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF0F iso.2.840.10036 - included
volatile active

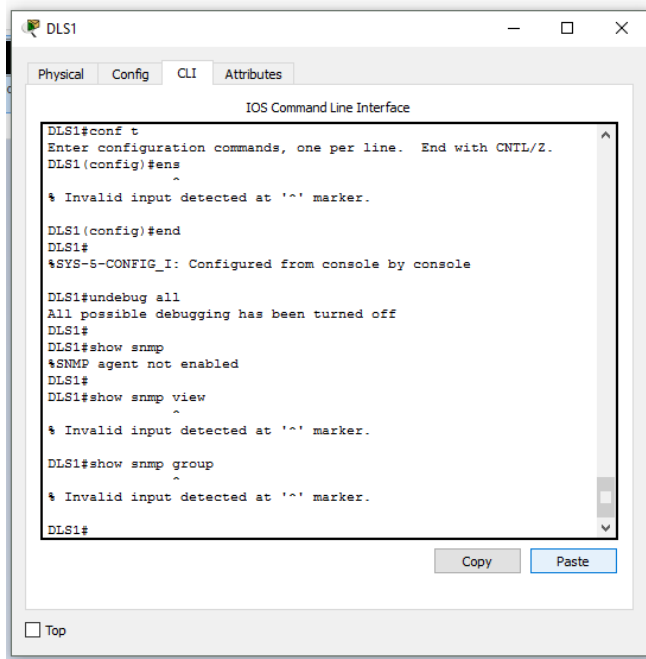
```

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**

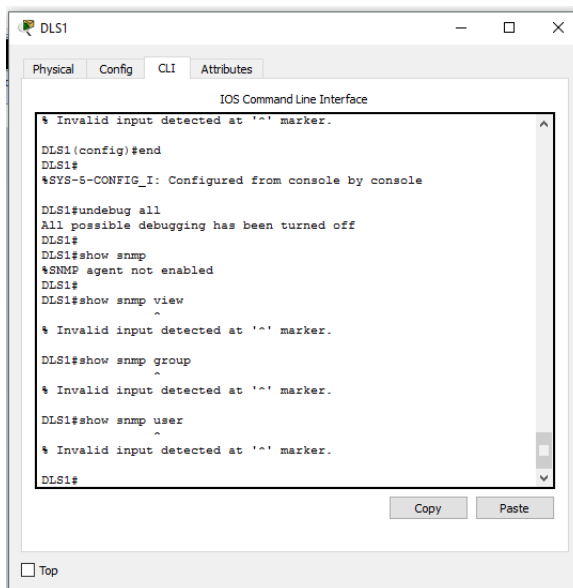
Engine ID: 800000090300E840406F7283

storage-type: nonvolatile active

Authentication Protocol: SHA

Privacy Protocol: AES128

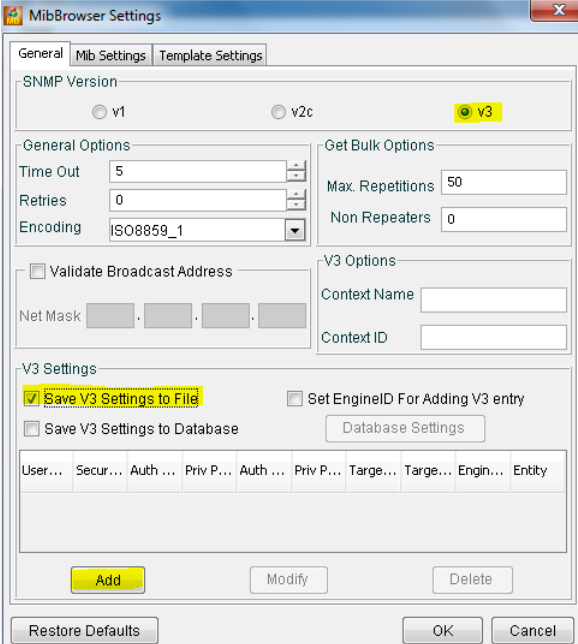
Group-name: ccnp-switch3



Step 7: Configure MIBBrowser software

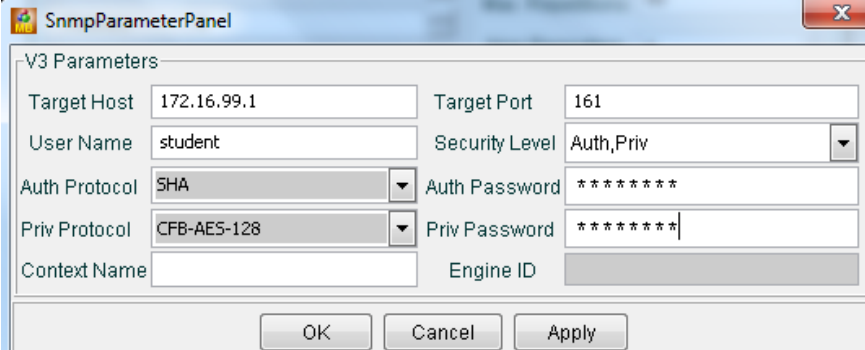
This lab uses the free tool "MIBBrowser" from ManageEngine for verification. Other tools that will listen for traps at are acceptable substitutes as well.

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**.



The MibBrowser Settings dialog box is shown with the 'Mib Settings' tab selected. The 'SNMP Version' section has the 'v3' radio button selected. The 'General Options' section includes 'Time Out' (5), 'Retries' (0), and 'Encoding' (ISO8859_1). The 'Get Bulk Options' section includes 'Max. Repetitions' (50) and 'Non Repeaters' (0). The 'V3 Options' section includes 'Context Name' and 'Context ID' fields. The 'V3 Settings' section has the 'Save V3 Settings to File' checkbox checked. Below this is a table with columns: User..., Secur..., Auth..., Priv P..., Auth..., Priv P..., Targe..., Targe..., Engin..., and Entity. At the bottom are buttons for 'Add', 'Modify', 'Delete', 'Restore Defaults', 'OK', and 'Cancel'.

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



The SnmParameterPanel dialog box is shown with the 'V3 Parameters' section. The 'Target Host' is 172.16.99.1, 'Target Port' is 161, 'User Name' is student, 'Security Level' is Auth,Priv, 'Auth Protocol' is SHA, 'Auth Password' is *****, 'Priv Protocol' is CFB-AES-128, 'Priv Password' is *****, 'Context Name' is empty, and 'Engine ID' is empty. At the bottom are buttons for 'OK', 'Cancel', and '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)
 ☐ Enable Logging
 Log Format ▼

☒ Authenticate v3 Trap
 ☐ Enable Mail
 Configure Mail

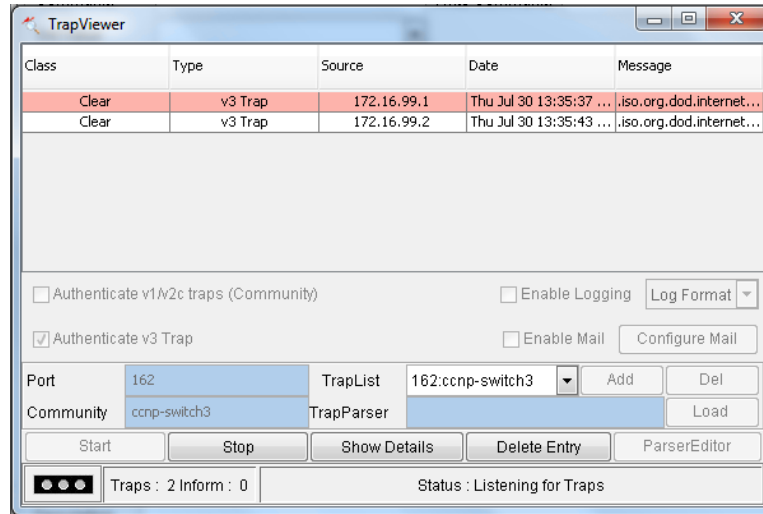
Port: 162
 TrapList: ▼
 Add
 Del

Community: ccnp-switch3
 TrapParser:
 Load

Traps : 0 Inform : 0
 Status : Not Listening for Traps

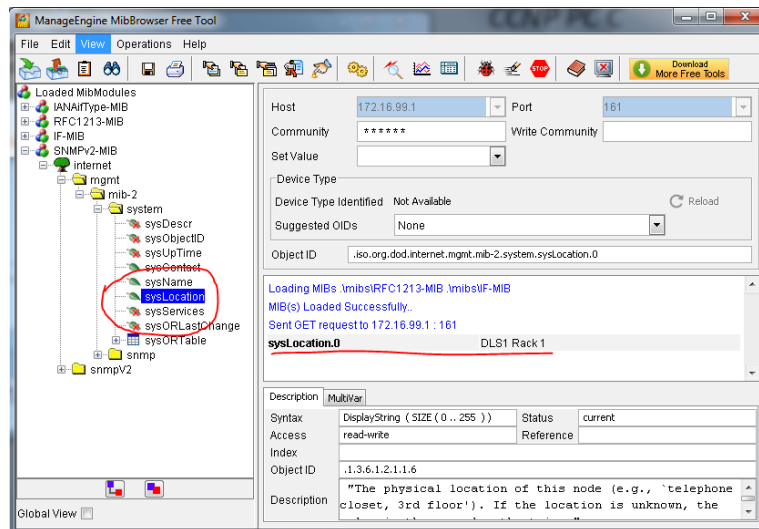
Finally, click Start. TrapViewer is now listening for traps.

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.

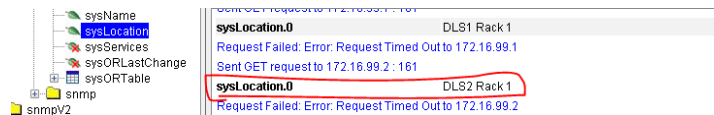


Step 9: Verify SNMP GET Operation

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.



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.

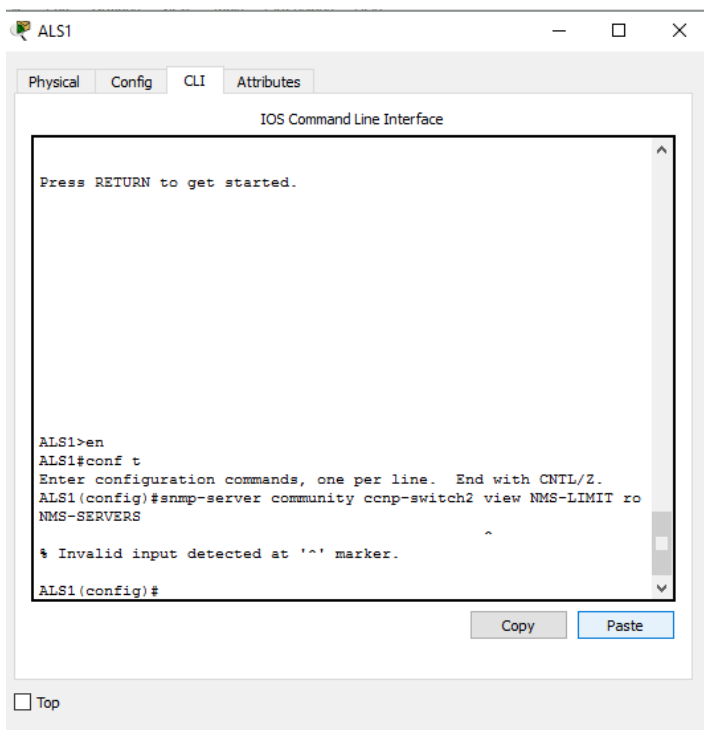


Part 5: Configure ALS1 and ALS2 for SNMPv2c

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
```

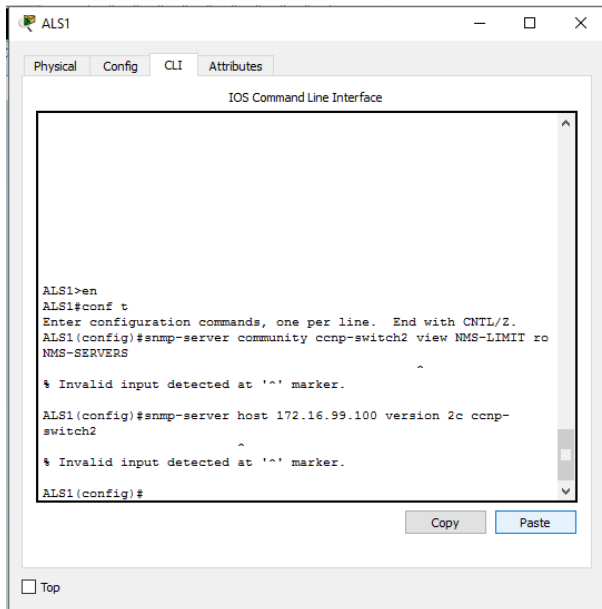


Step 2: Configure SNMP trap receiver

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:

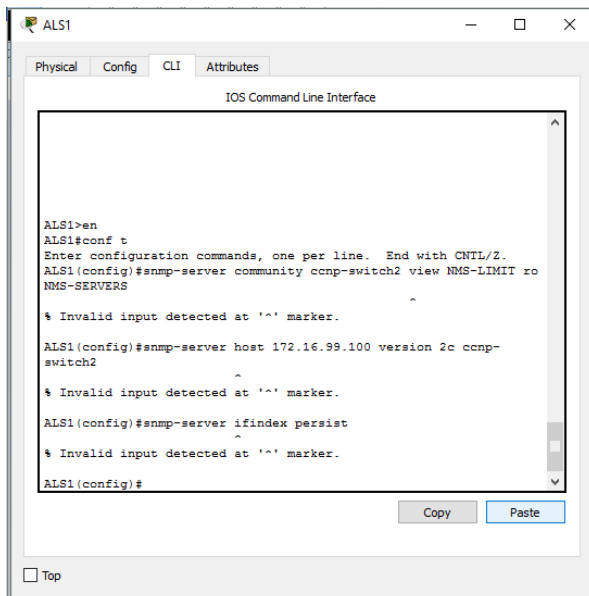
```
ALS1(config)# snmp-server host 172.16.99.100 version 2c ccnp-switch2
```



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

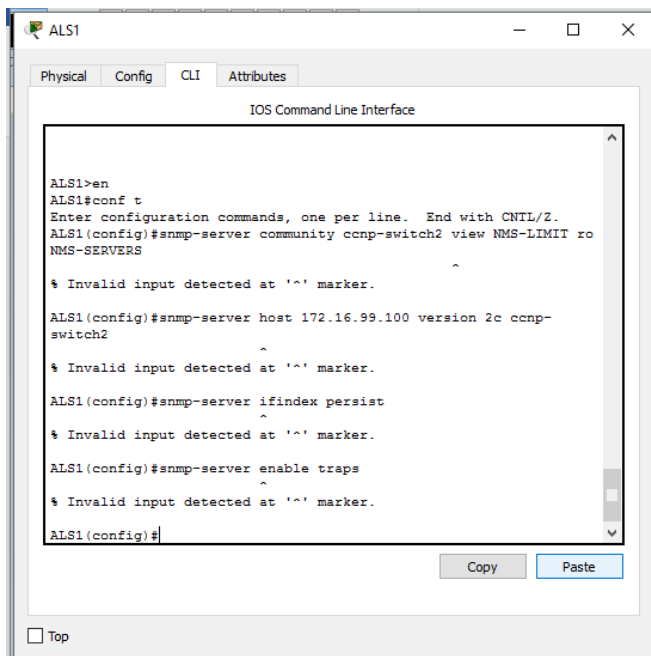
This final command actually enables the forwarding of traps to the configured trap receivers. As a part of this command, traps can be limited (as they can be in the snmp-server host command). Once again this will need to be coordinated with the network management system and network monitoring requirements 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.

TrapViewer				
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...

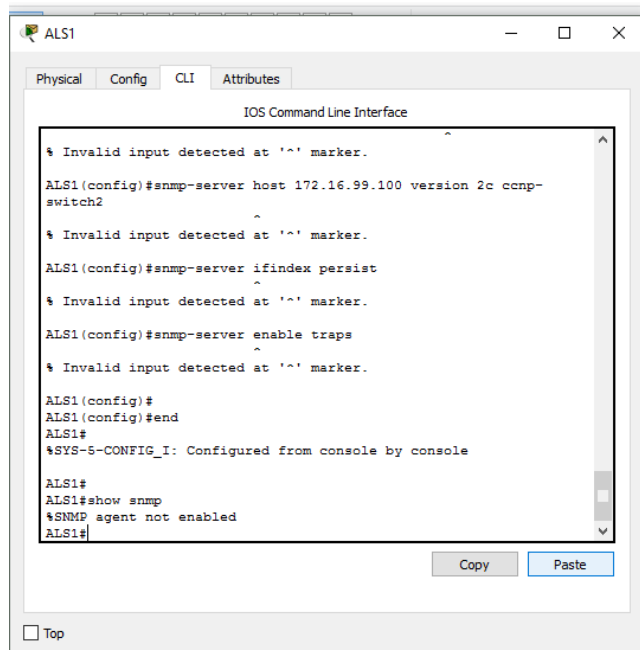
Use the **show snmp** command to view configuration information for SNMP:

```

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
```

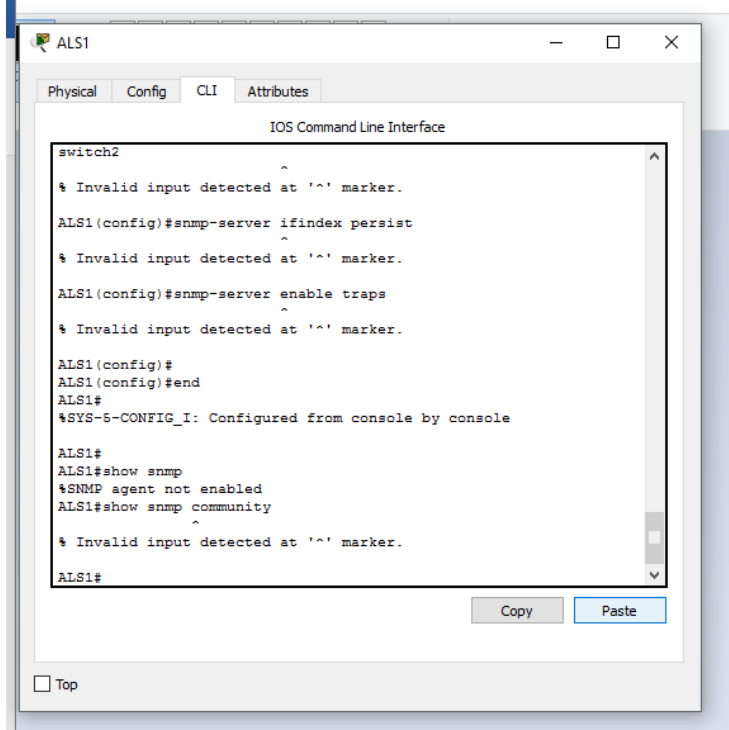
```
Community name: ccnp-switch2@1004
```

```
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#



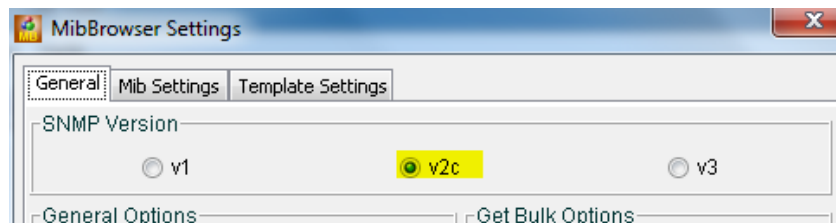
Step 6: Verify SNMP TRAP Operation

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.

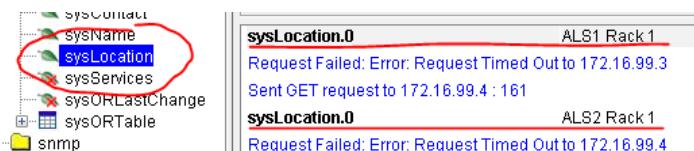
Class	Type	Source	Date	Message
Clear	v3 Trap	172.16.99.1	Thu Jul 30 13:35:37 ...	iso.org.dod.internet...
Clear	v3 Trap	172.16.99.2	Thu Jul 30 13:35:43 ...	iso.org.dod.internet...
Clear	v2c Trap	172.16.99.3	Thu Jul 30 13:58:12 ...	iso.org.dod.internet...
Clear	v2c Trap	172.16.99.4	Thu Jul 30 14:05:07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



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 SNMPv2c is configured correctly on this device.

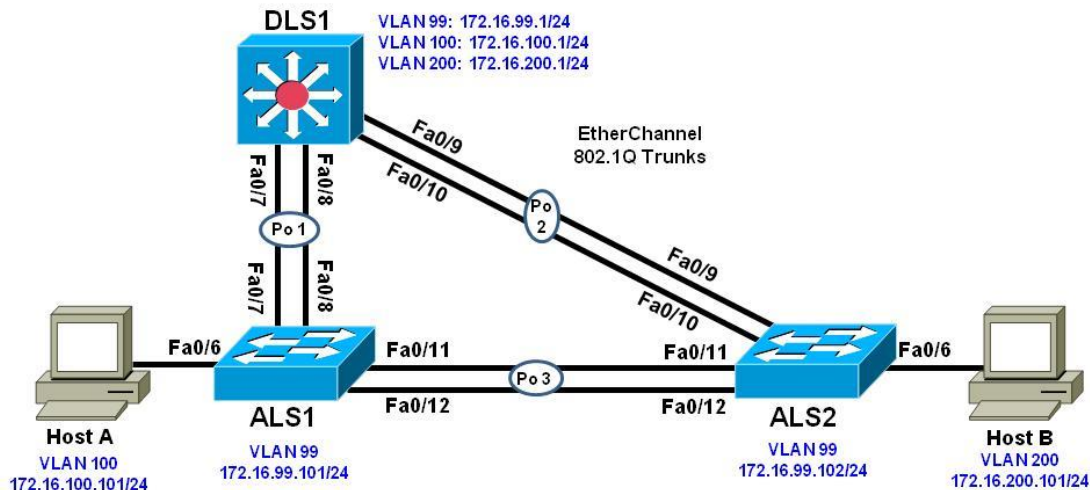


Step 8: End of Lab

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

CCNPv7.1_SWITCH_Lab8-1_IP_SLA_SPAN_STUDENT

Topology



Objectives

- Configure trunking, VTP, and SVIs.
- Implement IP SLAs to monitor various network performance characteristics.
- Implement Remote SPAN

Background

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

The SPAN feature allows you to instruct a switch to send copies of packets seen on one port, multiple ports, or an entire VLAN to another port on the same switch. Moreover, the Remote SPAN (RSPAN) feature takes the SPAN feature beyond a single switch to a network, allowing you to remotely capture traffic on different switches in the network. This is extremely useful in campus networks where a sniffer may not be located at the desired traffic capture point. In addition, this allows you to permanently place a sniffer in the campus network to SPAN traffic as necessary or when troubleshooting situations arise.

In this lab, you configure trunking, VTP, and SVIs. You configure IP SLA monitors to test ICMP echo network performance between DLS1 and each host. You also configure IP SLA monitors to measure jitter between DLS1 and the access layer switches ALS1 and ALS2. Finally, you will set up an RSPAN and capture traffic.

Note: This lab uses the Cisco WS-C2960-24TT-L switch with the Cisco IOS image c2960-lanbasek9-mz.150-2.SE6.bin and the Catalyst 3560V2-24PS switch with the Cisco IOS image c3560-ipservicesk9-mz.150-2.SE6.bin. Other switches and Cisco IOS Software versions can be used if they have comparable capabilities and features. 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.

Required Resources

- 2 switches (Cisco 2960 with the Cisco IOS Release 15.0(2)SE6C2960-LANBASEK9-M image or comparable)
- 1 switches (Cisco 3560 with the Cisco IOS Release 15.0(2)SE6C3560-IPSERVICESK9-M image or comparable)
- 2 PC's with Windows OS. One of the PCs should be equipped with Wireshark Application

- Ethernet and console cables

Part 6: 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 7: 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?

SLA de IP puede recopilar historial y capturar estadísticas. De forma predeterminada, el historial de una operación de SLA de IP, cuando el tipo de operación es eco de ruta ICMP, se crea una entrada para cada salto a lo largo de la ruta que la operación necesita para llegar a su destino. _____

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?

SLA de IP Las operaciones de conexión de Protocolo de control de transmisión (TCP) admiten direcciones IPv4 e IPv6. _____

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 8: 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 switchrunning 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` 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>
```

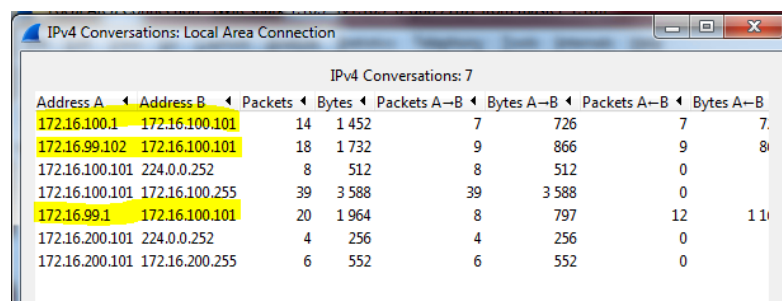
Step 2: Test RSPAN operation

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 > Conversation 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.



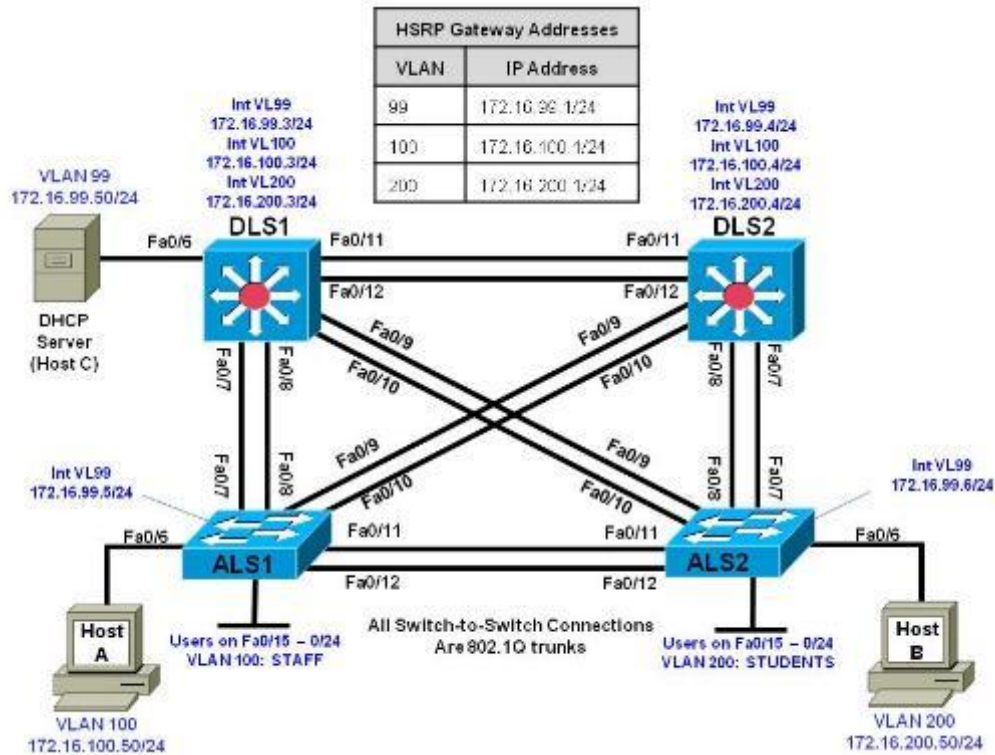
Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets B→A	Bytes B→A
172.16.100.1	172.16.100.101	14	1 452	7	726	7	726
172.16.99.102	172.16.100.101	18	1 732	9	866	9	866
172.16.100.101	224.0.0.252	8	512	8	512	0	0
172.16.100.101	172.16.100.255	39	3 588	39	3 588	0	0
172.16.99.1	172.16.100.101	20	1 964	8	797	12	1 167
172.16.200.101	224.0.0.252	4	256	4	256	0	0
172.16.200.101	172.16.200.255	6	552	6	552	0	0

Step 3: End of Lab

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

CCNPv7.1_SWITCH_Lab 10-1_Securing_Layer2_STUDENT

Topology



Objectives

- Prepare the Network.
- Implement Layer 2 network security features.
- Prevent DHCP spoofing attacks.
- Prevent unauthorized access to the network using AAA.

Background

A fellow network engineer that you have known and trusted for many years has invited you to lunch this week. At lunch, he brings up the subject of network security and how two of his former co-workers had been arrested for using different Layer 2 attack techniques to gather data from other users in the office for their own personal gain in their careers and finances. The story shocks you because you have always known your friend to be very cautious with security on his network. His story makes you realize that your business network has been cautious with external threats, Layer 3–7 security, firewalls at the borders, and so on, but insufficient at Layer 2 security and protection inside the local network.

When you get back to the office, you meet with your boss to discuss your concerns. After reviewing the company's security policies, you begin to work on a Layer 2 security policy.

First, you establish which network threats you are concerned about and then put together an action plan to mitigate these threats. While researching these threats, you learn about other potential threats to Layer 2 switches that might not be malicious but could threaten network stability. You decide to include these threats in the policies as well.

Other security measures need to be put in place to further secure the network, but you begin with configuring the switches against a few specific types of attacks, including MAC flood attacks, DHCP spoofing attacks, and unauthorized access to the local network. You plan to test the configurations in a lab environment before placing them into production.

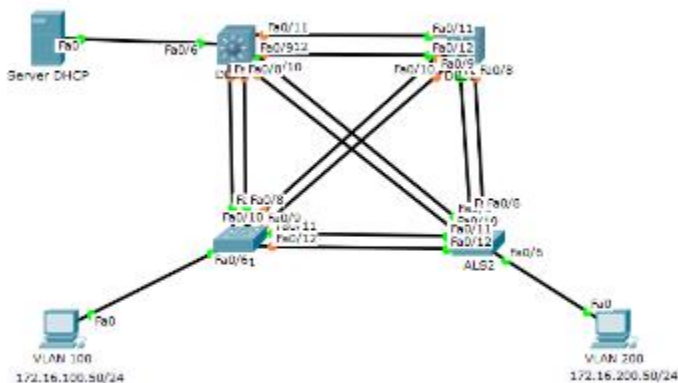
Note: This lab uses Cisco Catalyst 3560 and 2960 switches running Cisco IOS 15.0(2) IP Services and LAN Base images, respectively. The 3560 and 2960 switches are configured with the SDM templates “dual-ipv4-and-ipv6 routing” and “lanbase-routing”, respectively. Depending on the switch model and Cisco 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.

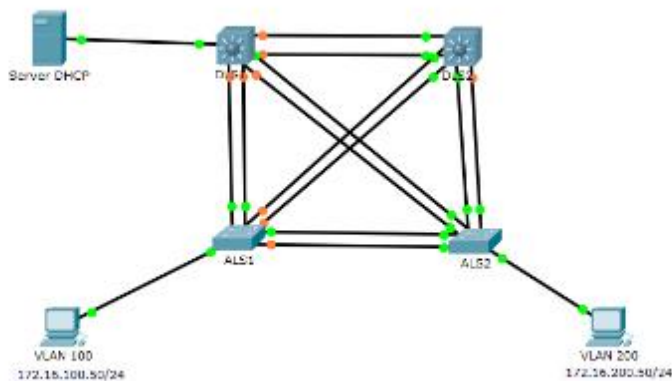
Note: This lab uses the Cisco WS-C2960-24TT-L switch with the Cisco IOS image c2960-lanbasek9-mz.150-2.SE6.bin and the Catalyst 3560V2-24PS switch with the Cisco IOS image c3560-ipservicesk9-mz.150-2.SE6.bin. Other switches and Cisco IOS Software versions can be used if they have comparable capabilities and features. 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.

Required Resources

- 2 switches (Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable).
- 1 switches (Cisco 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-IPSERVICESK9-M image or comparable).
- 3 PC's with Windows OS. One of the PCs should be equipped Wireshark, WinRadius, and Tftpd32 software.
- Ethernet and console cables

Part 9: 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`.

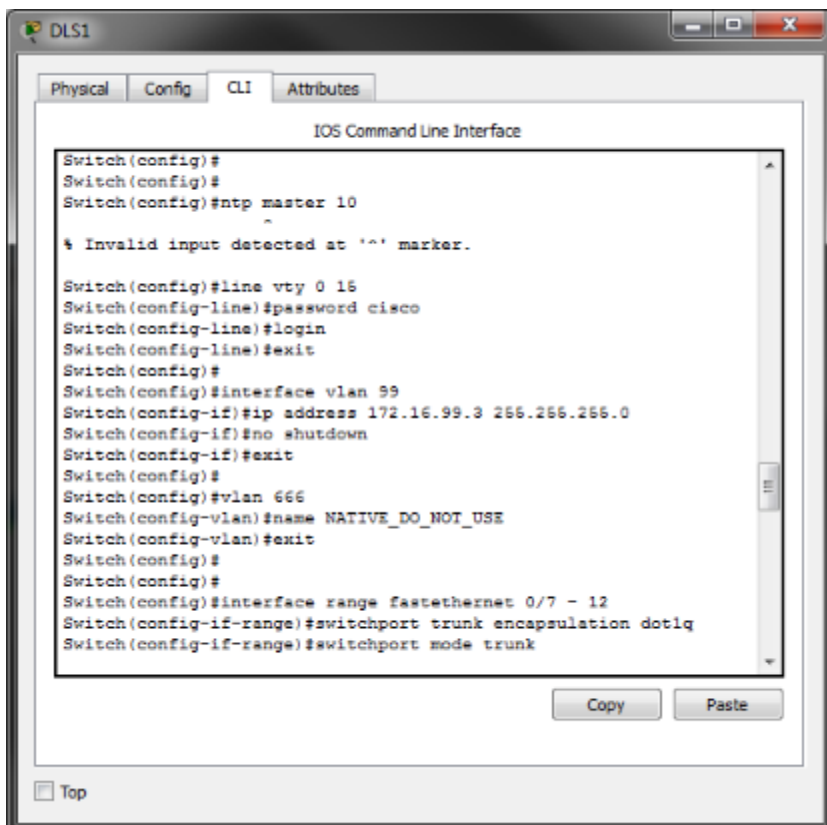
Step 2: Configure basic switch parameters.

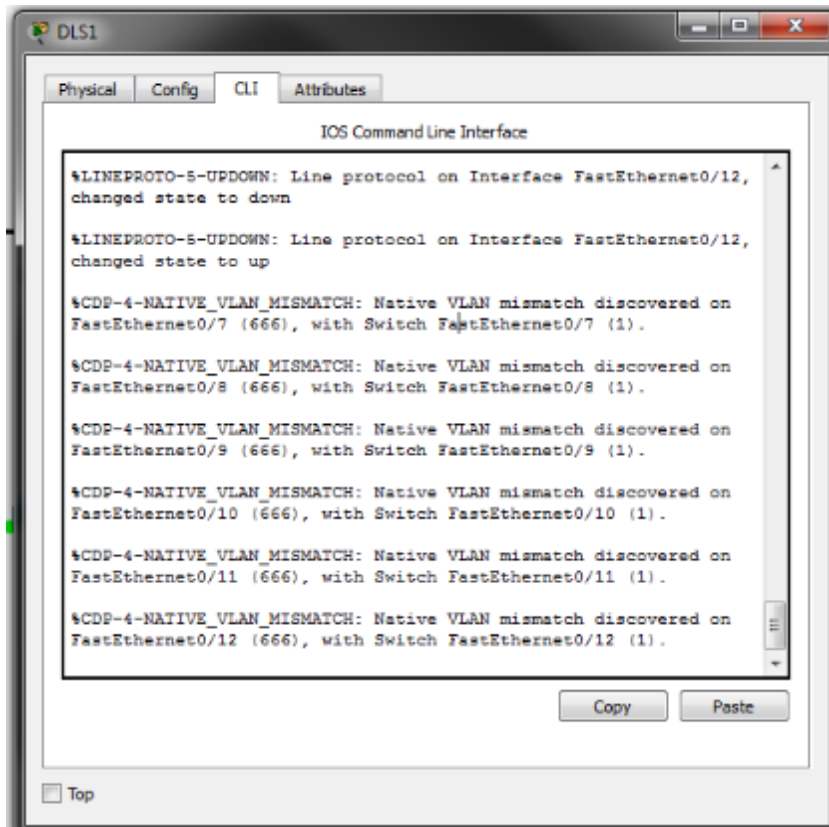
- Loading `BASE.CFG` should have set the hostname, IP domain name, and shut down all of the interfaces on each switch.
- Configure enable secret, and VTY passwords. As with previous labs, if NETLAB compatibility is required, use `class` as the enable secret and `cisco` as the VTY password.
- Configure interface VLAN 99 on each switch with the management IP address shown in the topology diagram.
- Configure the access layer switches (ALS1 and ALS2) to use a default gateway IP address of 172.16.99.1.
- Configure basic (unauthenticated) NTP in the network. Use DLS1 as the NTP master and have DLS2, ALS1, and ALS2 synchronize to 172.16.99.3.
- Configure 802.1q trunking between the switches according to the diagram (Note that there are no EtherChannels in this topology). Create and then use VLAN 666 as the native VLAN for all trunks. Also turn off switchport negotiation on all trunks.

Configure all four switches. An example of DLS1 and ALS1 configuration follows:

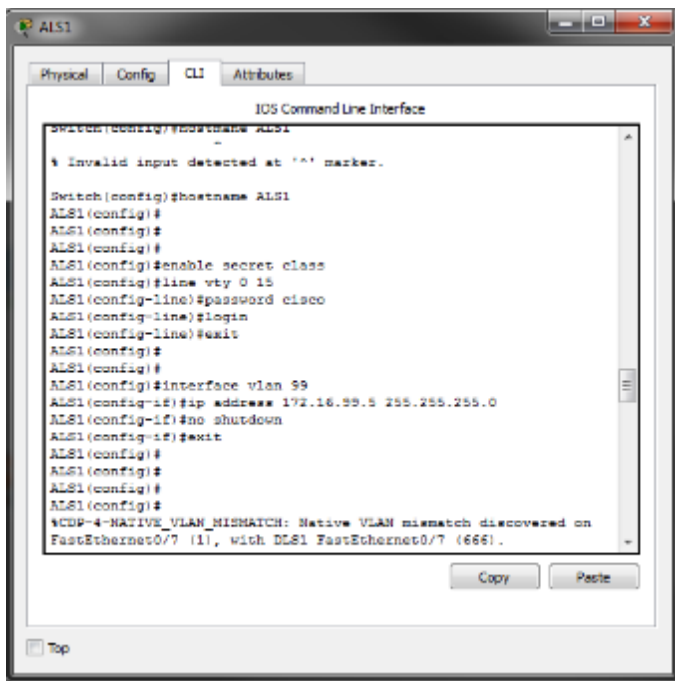
```
DLS1# clock set 14:55:00 3 August 2015
DLS1# config t
DLS1(config)# clock timezone CST -6
DLS1(config)# clock summer-time CDT recurring
DLS1(config)# ntp master 10
DLS1(config)# enable secret class
DLS1(config)# enable secret class
DLS1(config)# line vty 0 15
DLS1(config-line)# password cisco
DLS1(config-line)# login
DLS1(config-line)# exit
```

```
DLS1(config)# interface vlan 99
DLS1(config-if)# ip address 172.16.99.3 255.255.255.0
DLS1(config-if)# no shutdown
DLS1(config-if)# exit
DLS1(config)# vlan 666
DLS1(config-vlan)# name NATIVE_DO_NOT_USE
DLS1(config-vlan)# exit
DLS1(config)# interface range fastethernet 0/7 - 12
DLS1(config-if-range)# switchport trunk encapsulation dot1q
DLS1(config-if-range)# switchport mode trunk
DLS1(config-if-range)# switchport trunk native vlan 666
DLS1(config-if-range)# switchport nonegotiate
DLS1(config-if-range)# no shut
DLS1(config-if-range)# exit
```



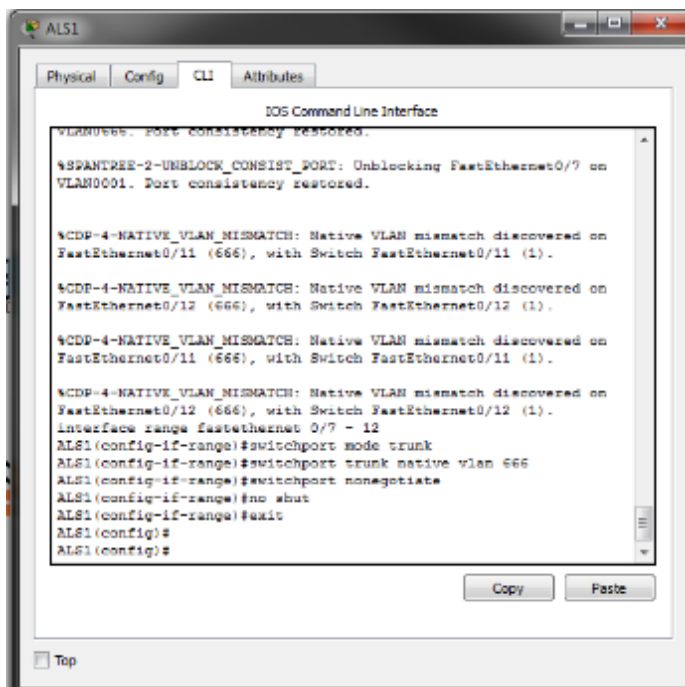


```
ALS1(config)# enable secret class
ALS1(config)# line vty 0 15
ALS1(config-line)# password cisco
ALS1(config-line)# login
ALS1(config-line)# exit
ALS1(config)# interface vlan 99
ALS1(config-if)# ip address 172.16.99.5 255.255.255.0
ALS1(config-if)# no shutdown
ALS1(config-if)# exit
ALS1(config)# ip default-gateway 172.16.99.1
ALS1(config)# ntp server 172.16.99.3
ALS1(config)# clock timezone CST -6
ALS1(config)# clock summer-time CDT recurring
ALS1(config)# vlan 666
ALS1(config-vlan)# name NATIVE_DO_NOT_USE
ALS1(config-vlan)# exit
ALS1(config)# interface range fastethernet 0/7 - 12
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# switchport trunk native vlan 666
ALS1(config-if-range)# switchport nonegotiate
ALS1(config-if-range)# no shut
ALS1(config-if-range)# exit
```



```
Switch(config)#hostname ALS1
Switch(config)#
% Invalid input detected at '^' marker.

Switch(config)#hostname ALS1
ALS1(config)#
ALS1(config)#
ALS1(config)#enable secret class
ALS1(config)#line vty 0 15
ALS1(config-line)#password cisco
ALS1(config-line)#login
ALS1(config-line)#exit
ALS1(config)#
ALS1(config)#
ALS1(config)#interface vlan 99
ALS1(config-if)#ip address 192.16.99.5 255.255.255.0
ALS1(config-if)#no shutdown
ALS1(config-if)#exit
ALS1(config)#
ALS1(config)#
ALS1(config)#
ALS1(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/7 (1), with DLS1 FastEthernet0/7 (666).
```



```
VLAN0066: Port consistency restored.
%SPANTRIE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/7 on
VLAN0001. Port consistency restored.

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/11 (666), with Switch FastEthernet0/11 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/12 (666), with Switch FastEthernet0/12 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/11 (666), with Switch FastEthernet0/11 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/12 (666), with Switch FastEthernet0/12 (1).
interface range fastEthernet 0/7 - 12
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#switchport trunk native vlan 666
ALS1(config-if-range)#switchport nonegotiate
ALS1(config-if-range)#no shut
ALS1(config-if-range)#exit
ALS1(config)#
ALS1(config)#
```

- g. Verify trunking and spanning-tree operations using the **show interfaces trunk** and **show spanning-tree** commands. Which switch is the root bridge?

ALS1

- h. For ALS1 and ALS2, which trunks have a role of designated (Desg), Alternate (Altn), and Root?

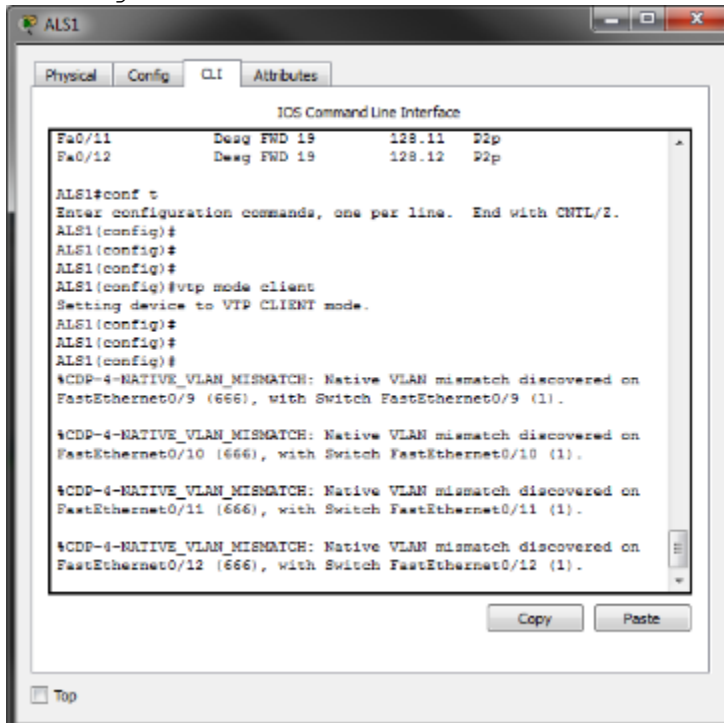
Para la vlan 666 ALS1 es root

Step 3: Configure VTP on DLS2, ALS1, and ALS2.

- i. Change the VTP mode of ALS1 and ALS2 to client. An example from ALS1:

```
ALS1(config)# vtp mode client
```

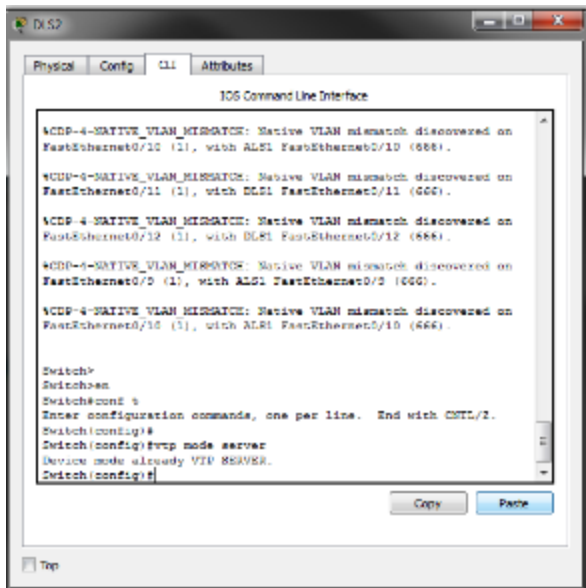
Setting device to VTP CLIENT mode.



- j. Change the VTP mode of DLS2 to server with no further configuration:

```
DLS2(config)# vtp mode server
```

Setting device to VTP SERVER mode.

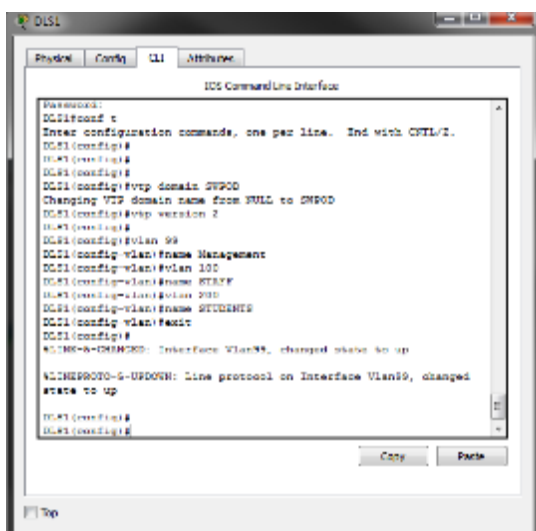


Step 3: Configure VTP on DLS1.

Create the VTP domain on DLS1, and create VLANs 99, 100, and 200 for the domain.

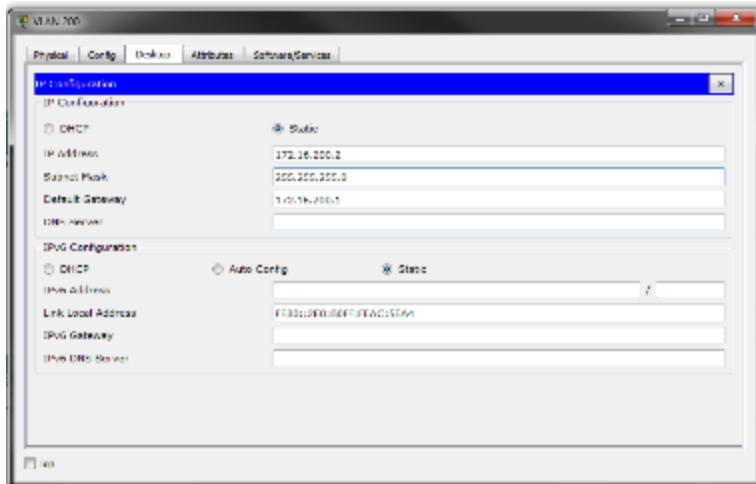
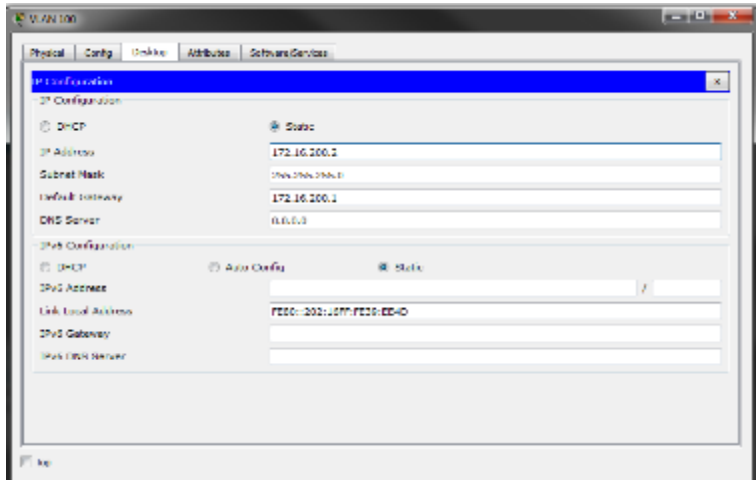
```
DLS1(config)# vtp domain SWPOD
DLS1(config)# vtp version 2

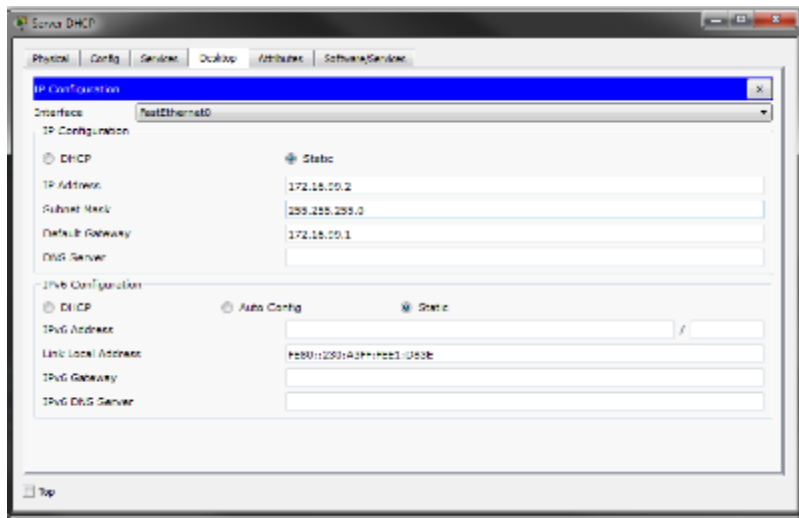
DLS1(config)# vlan 99
DLS1(config-vlan)# name Management
DLS1(config-vlan)# vlan 100
DLS1(config-vlan)# name STAFF
DLS1(config-vlan)# vlan 200
DLS1(config-vlan)# name STUDENTS
DLS1(config-vlan)# exit
DLS1(config)#
```



Step 4: Configure host PCs.

Configure PCs Host A, B, and C 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. Host C is in VLAN 99 with a default gateway of 172.16.99.1.





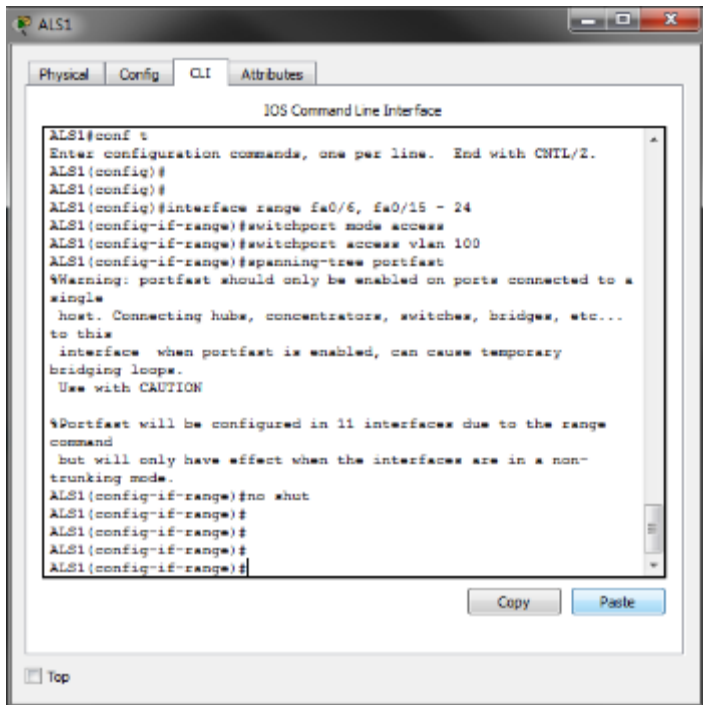
Step 5: Configure access ports.

Configure the host ports for the appropriate VLANs according to the diagram. Configure this on DLS1, ALS1, and ALS2. An example from ALS1 is below (all ports on ALS1 should be in VLAN 100, all ports on ALS2 should be in VLAN 200):

```
ALS1(config)# interface range fa0/6, fa0/15 - 24
ALS1(config-if-range)# switchport mode access
ALS1(config-if-range)# switchport access vlan 100
ALS1(config-if-range)# spanning-tree portfast
ALS1(config-if-range)# no shut
```

%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 10 interfaces due to the range command but will only have effect when the interfaces are in a non-trunking mode.

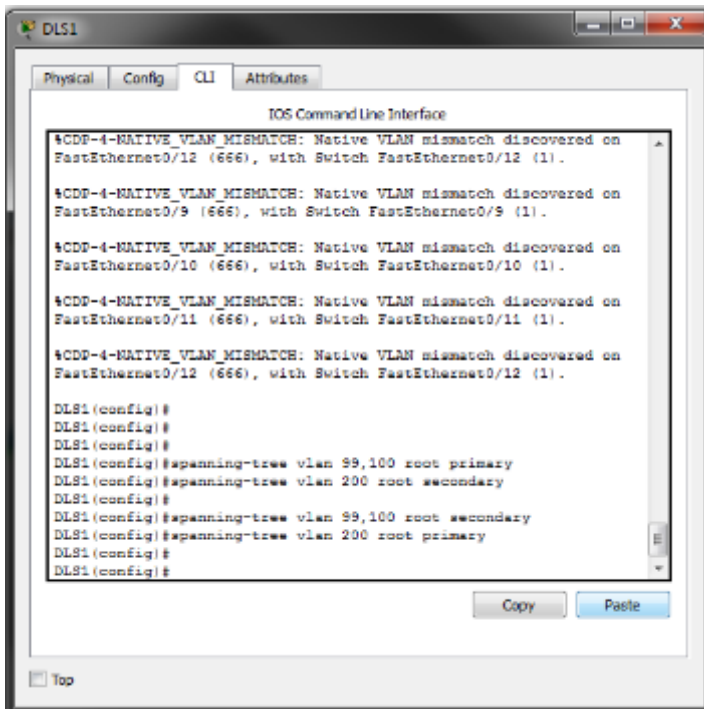


Step 6: Configure Spanning-Tree Root switches

Configure DLS1 to be the primary root for VLANs 99 and 100 and secondary root for VLAN 200. Configure DLS2 to be the primary root for VLAN 200 and the secondary root for VLANs 99 and 100.

```
DLS1(config)# spanning-tree vlan 99,100 root primary
DLS1(config)# spanning-tree vlan 200 root secondary
```

```
DLS2(config)# spanning-tree vlan 99,100 root secondary
DLS2(config)# spanning-tree vlan 200 root primary
```

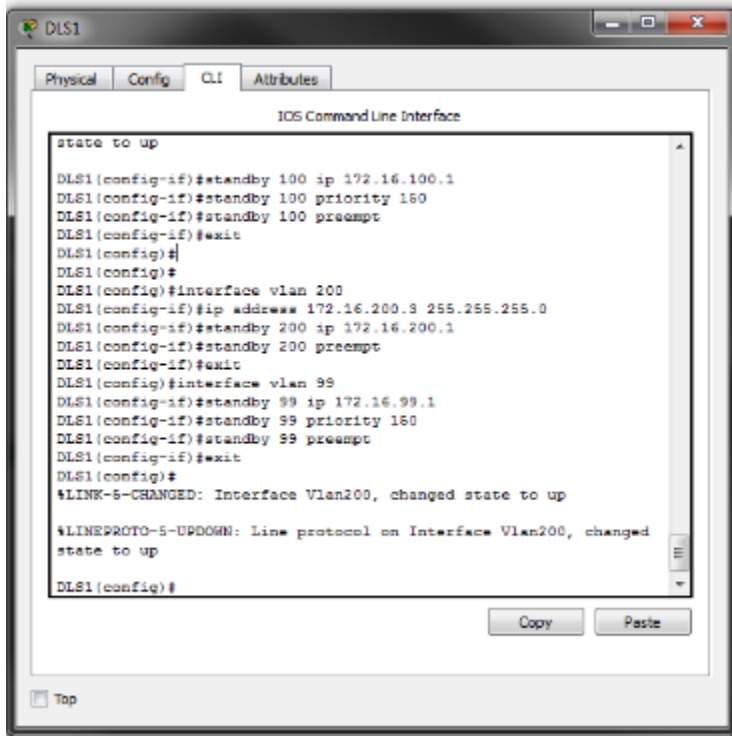


Step 7: Configure Routing and HSRP on DLS1 and DLS2.

On the DLS switches, create the SVIs for VLANs 100 and 200 using the addresses specified in the topology diagram. Further, configure HSRP with preemption on all three networks. Configure DLS1 with a priority of 150 for VLAN 99 and 100, and DLS2 with a priority of 150 for VLAN 200. Configure this on DLS1 and DLS2. An example from DLS1 is below:

```

DLS1(config)# ip routing
DLS1(config)# interface vlan 100
DLS1(config-if)# ip address 172.16.100.3 255.255.255.0
DLS1(config-if)# standby 100 ip 172.16.100.1
DLS1(config-if)# standby 100 priority 150
DLS1(config-if)# standby 100 preempt
DLS1(config-if)# exit
DLS1(config)# interface vlan 200
DLS1(config-if)# ip address 172.16.200.3 255.255.255.0
DLS1(config-if)# standby 200 ip 172.16.200.1
DLS1(config-if)# standby 200 preempt
DLS1(config-if)# exit
DLS1(config)# interface vlan 99
DLS1(config-if)# standby 99 ip 172.16.99.1
DLS1(config-if)# standby 99 priority 150
DLS1(config-if)# standby 99 preempt
DLS1(config-if)# exit
  
```



Verify the configuration using the **show vlan brief**, **show vtp status**, **show standby brief**, and **show ip route** command on DLS1. Output from DLS1 is shown here.

DLS1# show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2
100	staff	active	
200	Student	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

How many VLANs are active in the VTP domain?

_____tres vlan_____

DLS1# **show vtp status**

VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : SWLAB
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : e840.406f.7280
Configuration last modified by 0.0.0.0 at 8-3-15 14:56:12
Local updater ID is 172.16.99.3 on interface Vl99 (lowest numbered VLAN interface found)

Feature VLAN:

VTP Operating Mode : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 9
Configuration Revision : 3
MD5 digest : 0xE2 0x62 0xBC 0xCE 0x16 0xF3 0xBC
0x0C
0x6D 0x84 0x63 0xF2 0x38 0x55 0xB9
0xB7

DLS1# **show standby brief**

P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual
IP
Vl99 99 150 Active local 172.16.99.4
172.16.99.1
Vl100 100 150 P Active local 172.16.100.4
172.16.100.1
Vl200 200 100 P Standby 172.16.200.4 local
172.16.200.1

What is the active router for VLANs 1 and 100? **DLS1** What is the active router for VLAN 200? **DLS2**

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 172.16.99.3/32 is directly connected, Vlan99
C 172.16.100.0/24 is directly connected, Vlan100
L 172.16.100.3/32 is directly connected, Vlan100
C 172.16.200.0/24 is directly connected, Vlan200
L 172.16.200.3/32 is directly connected, Vlan200

What would be the effect on virtual interface VLAN 100 if VLAN 100 had not been created?

Pues no abria ningun efecto si la vlan no se crea porq no habria trafico atraves de ella

Part 2: Implement Layer 2 network security features.

Specify verification methods and mitigation techniques for attack types.

Complete the following table with the appropriate verification methods and mitigation approaches for the attack types specified in the left column.

Step 8: Storm Prevention

When packets flood the local area network, a traffic storm occurs. This could degrade network performance. Storm control features help to protect against such an attack. Storm control is typically implemented at the access layer switch ports to mitigate the effects of a traffic storm before propagating to the network. Storm control can also be implemented on trunk interfaces, including port-channel interfaces, to protect distribution-layer devices from traffic saturation, which could have a much broader impact on the network.

Storm control can detect and mitigate storms of broadcast, unicast, or multicast traffic. As a part of the configuration, you must specify what qualifies as a storm; either a rising and falling threshold based on the percentage of an interface's bandwidth used (the storm is recognized when X% of the interface bandwidth is used, and seen to be abated when Y% of the interface bandwidth is used), or based on rising and falling thresholds measured in either bits-per-second (bps) or packets-per-second (pps).

Storm Control Command Options			
storm-control [unicast broadcast multicast] level	0-100 <i>Rising Threshold</i>	0-100 <i>Falling Threshold</i>	<i>Omit Falling and Rising is the high/low mark</i>
	bps	0-10,000,000,000 [k m g] <i>Rising Threshold</i>	0-10,000,000,000 [k m g] <i>Falling Threshold</i>
	pps	0-10,000,000,000 [k m g] <i>Rising Threshold</i>	0-10,000,000,000 [k m g] <i>Falling Threshold</i>

To accurately configure these levels, you must know the amount of these traffic types flowing in your network during peak hours.

When a traffic storm is detected and storm control is configured, the default response is to silently filter the traffic. Storm control can optionally be configured to either shutdown the interface receiving the traffic storm or to send an SNMP trap to the NMS.

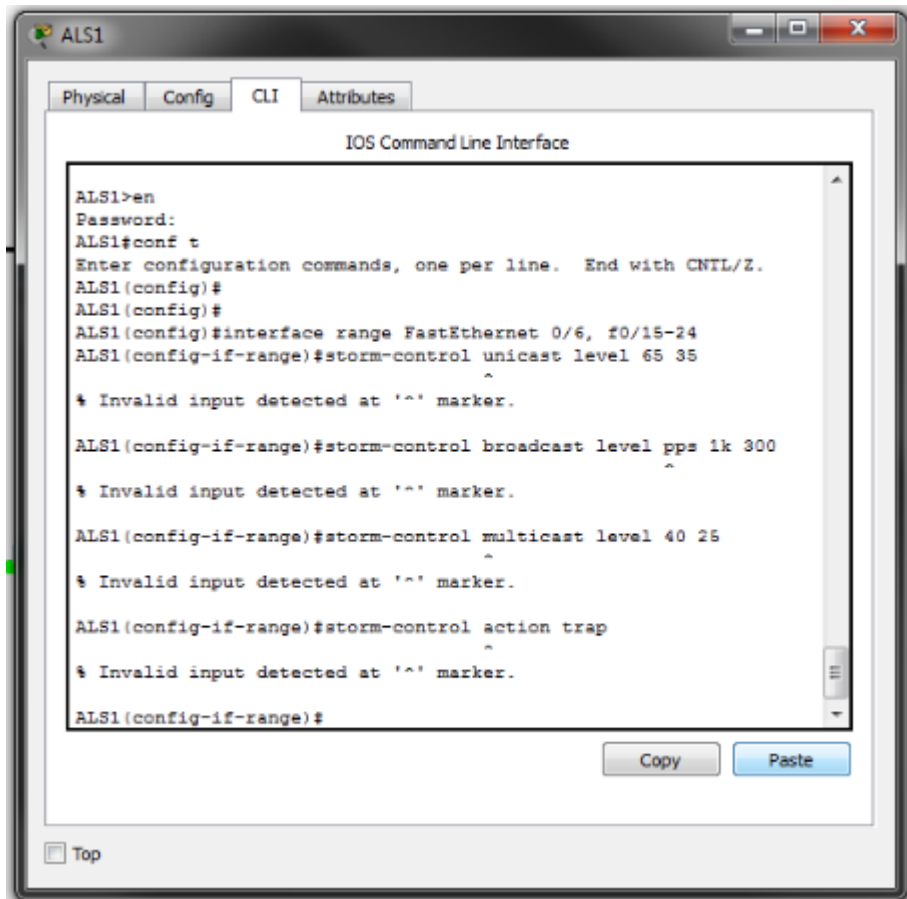
- a. Enable broadcast storm control on ports 0/6 and 0/15 - 0/24 on ALS1 with the parameters listed below. If any storm is detected, an SNMP trap will be sent.
 - 1) Unicast storms will be noted at 65% bandwidth usage, and abated at 35% bandwidth
 - 2) Broadcast storms will be noted at 1000 pps and abated at 300pps
 - 3) Multicast storms will be noted at 40% bandwidth usage and abated at 25% bandwidth

```
ALS1(config)# interface range FastEthernet 0/6, f0/15-24
ALS1(config-if-range)# storm-control unicast level 65 35
ALS1(config-if-range)# storm-control broadcast level pps 1k 300
```

```

ALS1(config-if-range)# storm-control multicast level 40 25
ALS1(config-if-range)# storm-control action trap

```



- b. Verify the configuration with the **show storm-control** command. The output below is showing the information for just f0/6; leaving the interface designation off would show configuration information for all storm-control configured interfaces.

```

ALS1# show storm-control f0/6 unicast
Interface  Filter State  Upper      Lower      Current
-----
Fa0/6      Forwarding     65.00%     35.00%     0.00%
ALS1# show storm-control f0/6 broadcast
Interface  Filter State  Upper      Lower      Current
-----
Fa0/6      Forwarding     1k pps     300 pps     0 pps
ALS1# show storm-control f0/6 multicast
Interface  Filter State  Upper      Lower      Current
-----
Fa0/6      Forwarding     40.00%     25.00%     0.00%
ALS1#

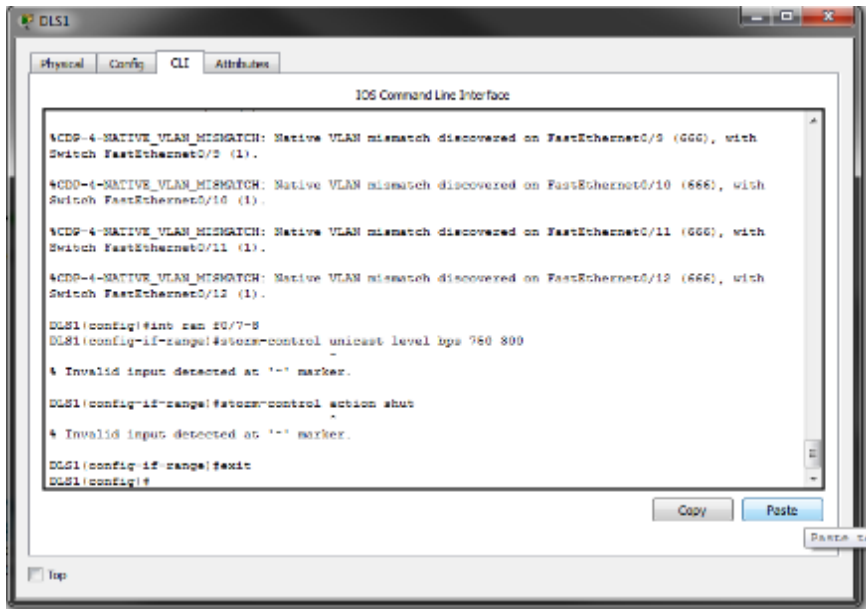
```

Step 9: Demonstrate Storm Control Operation

To demonstrate the effects of storm control, configure unicast storm control on DLS1 interfaces F0/7 and F0/8 with purposely low numbers and then generate traffic from ALS1 that will cause the threshold to be exceeded.

- a. At DLS1, configure F0/7 and F0/8 with the following:

```
DLS1(config)#int ran f0/7-8
DLS1(config-if-range)#storm-control unicast level bps 750 300
DLS1(config-if-range)#storm-control action shut
DLS1(config-if-range)#exit
```



- b. At ALS1, issue the command **ping 172.16.99.3 repeat 1000**.
- c. Within a few seconds you will see a SYSLOG message on DLS1 indicating that a storm had been detected and the interfaces shut down.

```
Aug  3 15:44:38.333: %PM-4-ERR_DISABLE: storm-control error detected
on Fa0/7, putting Fa0/7 in err-disable state
```

```
Aug  3 15:44:38.358: %STORM_CONTROL-3-SHUTDOWN: A packet storm was
detected on Fa0/7. The interface has been disabled.
```

```
Aug  3 15:44:39.339: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/7, changed state to down
```

```
Aug  3 15:44:40.363: %LINK-3-UPDOWN: Interface FastEthernet0/7,
changed state to down
```

```
Aug  3 15:45:09.572: %PM-4-ERR_DISABLE: storm-control error detected
on Fa0/8, putting Fa0/8 in err-disable state
```

```
Aug  3 15:45:09.597: %STORM_CONTROL-3-SHUTDOWN: A packet storm was
detected on Fa0/8. The interface has been disabled.
```

```
Aug  3 15:45:10.579: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/8, changed state to down
```

```
Aug  3 15:45:11.602: %LINK-3-UPDOWN: Interface FastEthernet0/8,
changed state to down
```

- d. Reset the storm control configuration on DLS1 F0/7 and F0/8. Because the interfaces are now shutdown due to an ERR-DISABLE, you have to manually reset them by issuing the shutdown and no shutdown commands. While you do this, remove the storm control from the interfaces.

```
DLS1(config)#int ran f0/7-8
DLS1(config-if-range)#shutdown
DLS1(config-if-range)#no storm-control unicast level bps 750 300
```

```
DLS1(config-if-range) #no storm-control action shut
DLS1(config-if-range) #no shutdown
DLS1(config-if-range) #exit
```

Step 10: Configure Basic Port Security.

To protect against MAC flooding or spoofing attacks, configure port security on the VLAN 100 and 200 access ports. Because the two VLANs serve different purposes—one for staff and one for students—configure the ports to meet the different requirements.

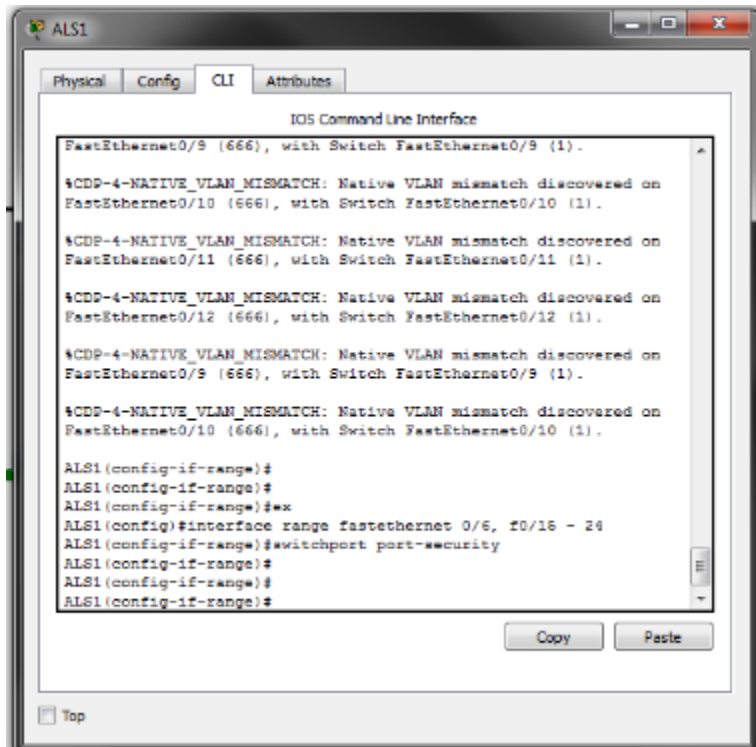
The student VLAN must allow MAC addresses assigned to a port to change, because most of the students use laptops and move around within the network. Set up port security so that only one MAC address is allowed on a port at a given time. This type of configuration does not work on ports that need to service IP phones with PCs attached or PC's running virtual machines. In this case, there would be two allowed MAC addresses. To enable security on a port, you must first issue the **switchport port-security command by itself**.

The staff MAC addresses do not change often, because the staff uses desktop workstations provided by the IT department. In this case, you can configure the staff VLAN so that the MAC address learned on a port is added to the configuration on the switch as if the MAC address were configured using the **switchport port-security mac-address** command. This feature, which is called sticky learning, is available on some switch platforms. It combines the features of dynamically learned and statically configured addresses. The staff ports also allow for a maximum of two MAC addresses to be dynamically learned per port.

- a. Enter the configuration for the student access ports on ALS2. To enable basic port security, issue the **switchport port-security command**.

Note: By default, issuing the **switchport port-security** command by itself sets the maximum number of MAC addresses to 1, and the violation mode to shutdown. It is not necessary to specify the maximum number of addresses, unless it is greater than 1.

```
ALS2(config)# interface range fastethernet 0/6, f0/15 - 24
ALS2(config-if-range)# switchport port-security
```



- b. Verify the configuration for ALS2 using the **show port-security interface** command.

```
ALS2# show port-security interface f0/6
```

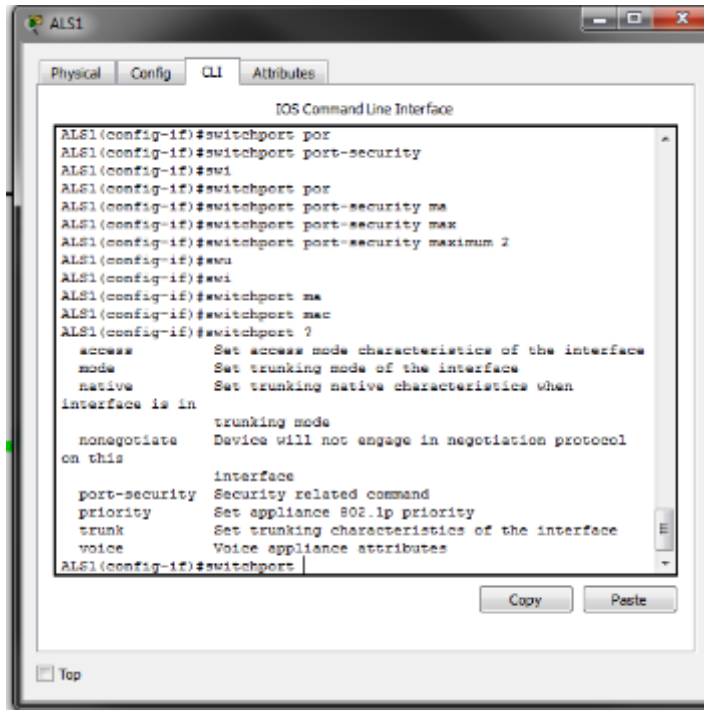
```
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type               : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses    : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses     : 0
Last Source Address:Vlan : 000c.2911.a33a:200
Security Violation Count : 0
```

Step 11: Configure Additional Port Security Parameters.

- a. Enter the configuration of the staff ports on ALS1. First, enable port security with the **switchport port-security** command. Use the **switchport port-security maximum #_of_MAC_addresses** command to change the maximum number of MAC addresses to 2, and use the **switchport port-security mac-address sticky** command to allow the two dynamically learned addresses to be added to the running configuration.

```
ALS1(config)# interface range fastethernet f0/6, f0/15 - 24
ALS1(config-if-range)# switchport port-security
ALS1(config-if-range)# switchport port-security maximum 2
```

```
ALS1(config-if-range) # switchport port-security mac-address sticky
```



This time two MAC addresses are allowed. Both will be dynamically learned and then added to the running configuration.

- b. Verify the configuration using the **show port-security interface** command.

```
ALS1#sho port-security int f0/6  
Port Security           : Enabled  
Port Status             : Secure-up  
Violation Mode          : Shutdown  
Aging Time              : 0 mins  
Aging Type              : Absolute  
SecureStatic Address Aging : Disabled  
Maximum MAC Addresses   : 2  
Total MAC Addresses     : 1  
Configured MAC Addresses : 0  
Sticky MAC Addresses    : 1  
Last Source Address:Vlan : 000c.2915.ab9d:100  
Security Violation Count : 0
```

Step 12: Configure Error Disabled Port Automatic Recovery

Once a violation occurs on a port, the port will transition to an error disabled state. The only way to clear a port that has been error disabled is to perform a **shutdown** command and then a **no shutdown** on the interface. This method, of course, requires manual intervention by an administrator.

Error disabled ports can be configured to automatically recover from port security violations with the use of the **errdisable recovery cause** command. An interval can be configured so that after a specified time the port will automatically clear the violation.

The command to verify the error disable configuration is the **show errdisable recovery**.

Configure the switch to automatically recover an error disabled port caused from a port security violation. Notice there are many different options for which you can configure error disable recovery. However, we will configure it only for port-security violation.

```

ALS1(config)# errdisable recovery cause ?
all                Enable timer to recover from all error causes
arp-inspection      Enable timer to recover from arp inspection error
                   disable state
bpduguard          Enable timer to recover from BPDU Guard error
channel-misconfig (STP) Enable timer to recover from channel misconfig error
dhcp-rate-limit     Enable timer to recover from dhcp-rate-limit error
dtp-flap            Enable timer to recover from dtp-flap error
gbic-invalid        Enable timer to recover from invalid GBIC error
inline-power        Enable timer to recover from inline-power error
link-flap           Enable timer to recover from link-flap error
loopback            Enable timer to recover from loopback error
mac-limit           Enable timer to recover from mac limit disable state
pagp-flap           Enable timer to recover from pagp-flap error
port-mode-failure   Enable timer to recover from port mode change
                   failure
pppoe-ia-rate-limit Enable timer to recover from PPPoE IA rate-limit
                   error
psecure-violation   Enable timer to recover from psecure violation error
psp                 Enable timer to recover from psp
security-violation  Enable timer to recover from 802.1x violation error
sfp-config-mismatch Enable timer to recover from SFP config mismatch
                   error
small-frame         Enable timer to recover from small frame error
storm-control        Enable timer to recover from storm-control error
udld                Enable timer to recover from udld error
vmpps               Enable timer to recover from vmpps shutdown error

```

```

ALS1(config)# errdisable recover cause psecure-violation

```

Configure the recovery interval for 30 seconds. If no recovery interval is specified, the recovery time defaults to 300 seconds.

```

ALS1(config)# errdisable recovery interval ?
<30-86400> timer-interval (sec)
ALS1(config)# errdisable recovery interval 30

```

Use the **show errdisable recovery** command to view the configuration.

```

ALS1# show errdisable recovery
ErrDisable Reason      Timer Status
-----

```

arp-inspection	Disabled
bpduguard	Disabled
channel-misconfig (STP)	Disabled
dhcp-rate-limit	Disabled
dtp-flap	Disabled
gbic-invalid	Disabled
inline-power	Disabled
link-flap	Disabled
mac-limit	Disabled
loopback	Disabled
pagp-flap	Disabled
port-mode-failure	Disabled
pppoe-ia-rate-limit	Disabled
psecure-violation	Enabled
security-violation	Disabled
sfp-config-mismatch	Disabled
small-frame	Disabled
storm-control	Disabled
udld	Disabled
vmps	Disabled
psp	Disabled

Timer interval: 30 seconds

Interfaces that will be enabled at the next timeout:

Part 10: Configure IPv4 DHCP snooping

DHCP spoofing is a type of attack primarily where an unauthorized device assigns IP addressing and configuration information to hosts on the network.

IPv4 DHCP servers reply to DHCPDISCOVER frames. These frames are generally BROADCAST, which means they are seen all over the network. The attacker replies to a DHCP request, claiming to have valid gateway and DNS information. A valid DHCP server might also reply to the request, but if the attacker's reply reaches the requestor first, the invalid information from the attacker is used. This can lead to a denial of service or traffic interception.

The process we will use to see this work is to first verify that the DHCP DISCOVER is broadcast everywhere, and then enable DHCP snooping to see this being stopped.

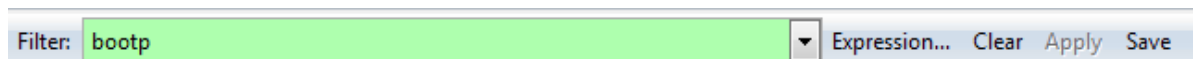
To do this, we will use Tftpd32's DHCP server function.

Step 1: Verify DHCP Broadcast Operation

On Host C, configure the DHCP server settings in Tftpd32 to support DHCP for VLAN 200. The screenshot details the settings:



- On DLS1, issue the `ip helper-address 172.16.99.50` command under interface VLAN 200.
- Reassign interface f0/6 on ALS1 to VLAN 200.
- On Host A, run Wireshark and have it collect on its ethernet interface. In the filter bar, type **bootp** and press enter (this filters the output to show only packets related to DHCP).



- On Host B, reconfigure the network interface to use DHCP. You should see that Host B receives an IP address and other DHCP information.

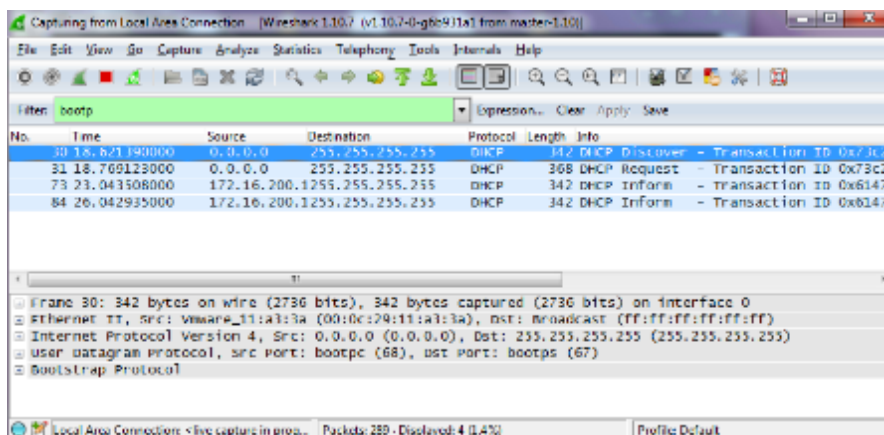
Ethernet adapter Local Area Connection:

```

Connection-specific DNS Suffix . : GOOD-DHCP.SRV
Link-local IPv6 Address . . . . . : fe80::b8ee:7ffd:e885:8423%10
IPv4 Address. . . . . : 172.16.200.150
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.200.1

```

- Return to Host A and you should see the DHCP traffic in the capture window.



If Host A were an attacker, it could craft DHCP server OFFER messages or other DHCP server messages to respond to Host B's DHCP request.

To help protect the network from such an attack, you can use DHCP snooping.

Step 2: Configure DHCP Snooping

DHCP snooping is a Cisco Catalyst feature that determines which switch ports are allowed to respond to DHCP requests. Ports are identified as trusted or untrusted. Trusted ports permit all DHCP messages, while untrusted ports permit (ingress) DHCP requests only. Trusted ports can host a DHCP server or can be an uplink toward a DHCP server. If a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is disabled. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as a DHCP OFFER, DHCP ACK, or DHCP NAK.

Configuring DHCP Snooping on a single switch is very simple. There are additional considerations when configuring DHCP Snooping at the access layer of a multi-layer enterprise network. By default switches that pass DHCP requests on to another switch will insert option-82 information, which can be used for various management functions.

When a switch receives a DHCP frame that has option-82 information on an untrusted interface, the frame will be dropped. The `ip dhcp relay information trust-all` command is one way to work around this default behavior. It is not necessary to enable DHCP snooping on the distribution layer switches, although this would allow DLS1 and DLS2 to trust ALS1 and ALS2 as relay agents.

- a. Configure DLS1 and DLS2 to trust relayed DHCP requests (Option 82 preset with giaddr field equal to 0.0.0.0). Configure this on DLS1 and DLS2. An example from DLS1 is below:

```
DLS1(config)# ip dhcp relay information trust-all
```

- b. Configure ALS1 and ALS2 to trust DHCP information on the trunk ports only, and limit the rate that requests are received on the access ports. Configuring DHCP snooping on the access layer switches involves the following steps:
 - Turn snooping on globally using the `ip dhcp snooping` command.
 - Configure the trusted interfaces with the `ip dhcp snooping trust` command. By default, all ports are considered untrusted unless statically configured to be trusted. * Very Important *: The topology used for this lab is not using EtherChannels. Remember that when an EtherChannel is created, the virtual port channel interface is used by the switch to pass traffic; the physical interfaces (and importantly their configuration) is not referenced by the switch. Therefore, if this topology was using EtherChannels, the `ip dhcp snooping trust` command would need to be applied to the Port Channel interfaces and not to the physical interfaces that make up the bundle.
 - Configure a DHCP request rate limit on the user access ports to limit the number of DHCP requests that are allowed per second. This is configured using the `ip dhcp snooping limit rate rate_in_pps`. This command prevents DHCP starvation attacks by limiting the rate of the DHCP requests on untrusted ports.
 - Configure the VLANs that will use DHCP snooping. In this scenario, DHCP snooping will be used on both the student and staff VLANs.

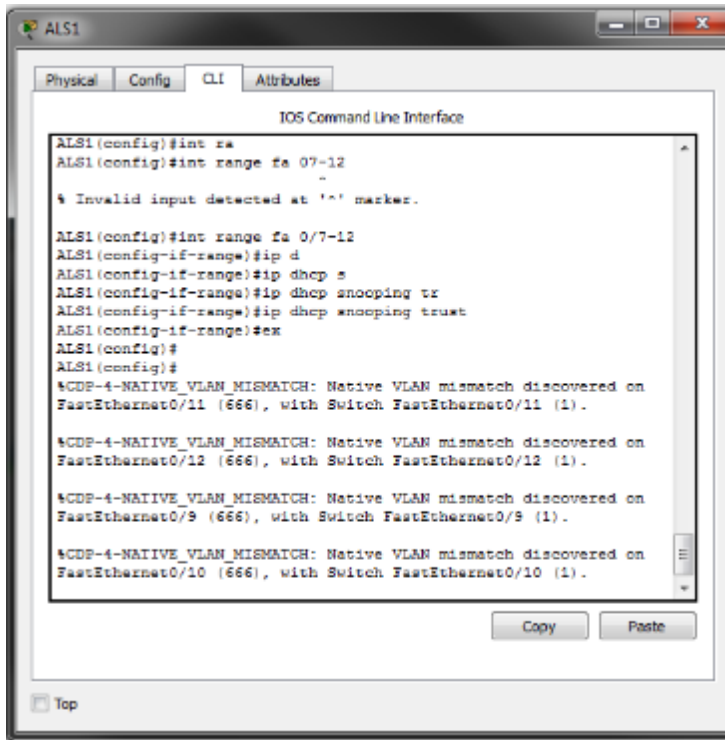
Configure this on ALS1 and ALS2. An example from ALS1 is below:

```
ALS1(config)# ip dhcp snooping
ALS1(config)# interface range fastethernet 0/7 - 12
ALS1(config-if-range)# ip dhcp snooping trust
ALS1(config-if-range)# exit
```

```

ALS1(config)# interface range fastethernet 0/6, f0/15 - 24
ALS1(config-if-range)# ip dhcp snooping limit rate 20
ALS1(config-if-range)# exit
ALS1(config)# ip dhcp snooping vlan 100,200

```



- c. Verify the configurations on ALS1 and ALS2 using the **show ip dhcp snooping** command.

```

ALS2# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
100,200
DHCP snooping is operational on following VLANs:
100,200
DHCP snooping is configured on the following L3 Interfaces:

```

```

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: 5017.ff84.0a80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

```

Interface	Trusted	Allow option	Rate limit (pps)
FastEthernet0/6	no	no	20
Custom circuit-ids:			
FastEthernet0/7	yes	yes	unlimited

```

Custom circuit-ids:
FastEthernet0/8          yes          yes          unlimited
Custom circuit-ids:
Interface                Trusted    Allow option  Rate limit (pps)
-----
FastEthernet0/9          yes          yes          unlimited
Custom circuit-ids:
FastEthernet0/10         yes          yes          unlimited
Custom circuit-ids:
FastEthernet0/11         yes          yes          unlimited
Custom circuit-ids:
FastEthernet0/12         yes          yes          unlimited
Custom circuit-ids:
<...OUTPUT OMITTED...>

```

Step 3: Verify IPv4 DHCP Snooping Operation

To verify DHCP Snooping is working, re-run the test conducted to observe DHCP operation without DHCP snooping configured. Ensure WIRESHARK is still running on HOST_A. Issue the `ipconfig /renew` command on HOST_B. In this case, the DHCPDISCOVER should NOT be seen at HOST_A.

Once validated, change ALS1 f0/6 back to VLAN 100 and make sure HOSTA and HOSTB have valid static IP addresses assigned.

Will DHCP replies be allowed to ingress access ports assigned to VLAN 200?

No Habra replicas de informacion

How many DHCP packets will be allowed on Fast Ethernet 0/16 per second?

3

Part 11: Configure AAA

AAA stands for Authentication, Authorization, and Accounting. The authentication portion of AAA is concerned with the user being positively identified. Authentication is configured by defining a list of authentication methods and applying that list to specific interfaces. If lists are not defined, a default list is used.

To demonstrate this we will use AAA to validate users attempting to log into the VTY lines of our network devices. The AAA server will be a radius server on Host C (172.16.99.50) connected to DLS1's F0/6 . There are many different radius server alternatives, but for this lab the program WinRadius is used.

Step 1: Configure Switches to use AAA to secure VTY line access

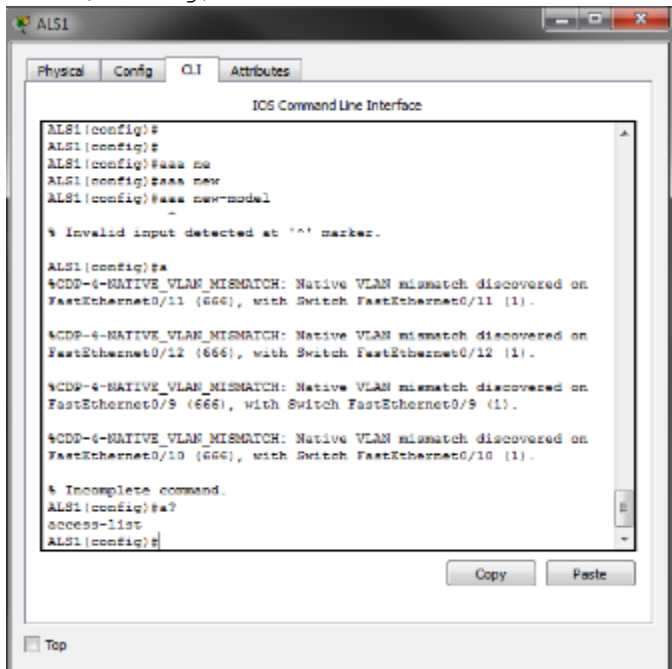
As it stands, all of the switches should have a statically assigned password of cisco on the VTY lines. This is not a scalable configuration. It requires a single known password, and manual modification of each switch individually as well as controlled dissemination of that single known password. Using centralized authentication is a much simpler method, where each user uses their own unique username and password.

Ensure that Host C has connectivity to the gateway and all four switches.

Make the following configuration changes to all four switches:

- Issue the `aaa new-model` global configuration command to enable AAA

```
ALS1(config)# aaa new-model
```



AAA no funciona en packet en esos switch

- b. Configure a local user named lastditch with a privilege level of 15 and a password of \$cisco123&

```
ALS1(config)# username lastditch privilege 15 password $cisco123&
```

- c. Configure the radius server to use authentication port 1812, accounting port 1813 and the shared key WinRadius

```
ALS1(config)# radius server RADIUS
```

```
ALS1(config-radius-server)# address ipv4 172.16.99.50 auth-port 1812  
acct-port 1813
```

```
ALS1(config-radius-server)# key WinRadius
```

```
ALS1(config-radius-server)# exit
```

- d. Configure the AAA authentication method REMOTE-CONTROL to use the radius server and to fallback to the local database

```
ALS1(config)# aaa authentication login REMOTE-CONTROL group radius  
local
```

- e. Configure the VTY lines to use the REMOTE-CONTROL authentication method

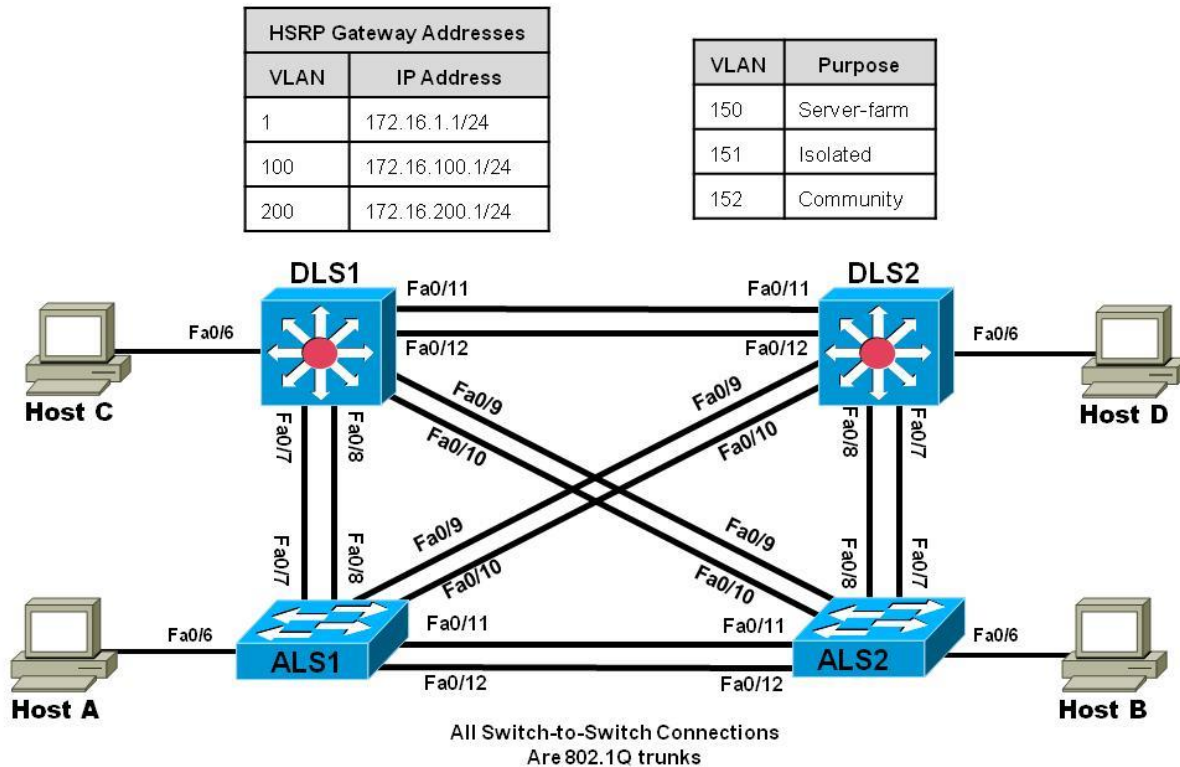
```
ALS1(config)# line vty 0 4
```

```
ALS1(config-line)# login authentication REMOTE-CONTROL
```

```
ALS1(config-line)# exit
```

CCNPv7.1_SWITCH_Lab 10-2_Securing VLANs_STUDENT

Topology



Objectives

- Secure the server farm using private VLANs.
- Secure the staff VLAN from the student VLAN.
- Secure the staff VLAN when temporary staff personnel are used.

Background

In this lab, you will configure the network to protect the VLANs using router ACLs, VLAN ACLs, and private VLANs. First, you will secure the new server farm (Host C) by using private VLANs. Service providers use private VLANs to separate different customers' traffic while utilizing the same parent VLAN for all server traffic. The private VLANs provide traffic isolation between devices, even though they might exist on the same VLAN.

You will then secure the staff VLAN from the student VLAN by using a RACL, which prevents traffic from the student VLAN from reaching the staff VLAN. This allows the student traffic to utilize the network and Internet services while keeping the students from accessing any of the staff resources.

Lastly, you will configure a VACL that allows a host on the staff network to be set up to use the VLAN for access but keeps the host isolated from the rest of the staff machines. This machine is used by temporary staff employees.

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)
- 4 PCs
- Ethernet and console cables

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 12: 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

- c. 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

- d. 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)#

```

- e. 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

- f. 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?

Al volver un servidor VTP DLS1, se agrega la VLAN 150 y asigna un nombre a la granja de servidores VLAN . Esto permite que la VLAN 150 se propague a los otros conmutadores en la red. Además, configure DLS1 como puente raíz para las VLAN 150, 151 y 152.

Step 5: Configure host access to PVLANS

- g. 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
```

- h. 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

- i. 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.

Al estar dentro del rango de la VLAN , proporciona que conectividad a los diferentes host de la red en donde estos pueden comunicarse y en enviar información._____

- j. 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

- k. 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.
- l. 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

- m. 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).
- n. From HOST C, try to ping HOST D (172.16.150.150). This should NOT work.
- o. From HOST D, try to ping the following addresses - they should all work: 172.16.150.1 (DLS1), 172.16.99.5 (ALS1).
- p. From HOST D, try to ping 172.16.150.2 (DLS2). This should NOT work.

Part 14: 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
```

- q. 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>

```

- r. 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 resto de comandos no se déjá ejecutar para poder hacer ping de extreme a extreme y estos obtengan conectividad en la red. _____

Part 15: 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

- s. 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

```

- t. 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

- u. 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
```

- v. 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
```

- w. 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
```

- x. 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

- y. From HOST C, try to ping to HOST A on ALS1 (172.16.100.50). The ping should fail.
- z. From HOST C, try to ping the default gateway (172.16.100.1). The ping should fail.
- aa. 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.

CONCLUSIONES

Aprender a configurar dispositivos de red avanzados en entorno IOS para aplicar a la solución de problemas en infraestructura tecnológica.

Gracias a la práctica se pudo observar y aprender cómo se configura una red a través de switching basado en protocolos avanzados de capa 2 pasando por capa 3 otorgando conectividad entre los hosts de la red.

Adquirir habilidades de gestión de redes orientadas hacia el mundo profesional y corporativo, además necesarios para planificar, implementar, asegurar, mantener y solucionar problemas de redes convergentes.

Entender el funcionamiento de un sistema de enrutamiento avanzado y su importancia a la hora de implementarlo en una red de datos.

Configurar y administrar dispositivos de Networking mediante el estudio y la práctica de ejercicios, basados en protocolos de enrutamiento avanzado.

Entender el enrutamiento inter-VLAN como una mayor velocidad del tráfico de red, ya que al no usarse toda la capacidad de la red, el router permite una comunicación de las subredes que pasan a través de sus interfaces, hay menos retardo debido a la distancia física ya que hay menos cables.

Adquirir el conocimiento para poder configurar los switches Cisco, y familiarizarse con los menús del mismo y sus comandos principales como avanzados.

Capacidad de configurar Inter-VLANs y enlaces troncales en una red de área local a través de switches 2960 - 3560 de Cisco.

REFERENCIAS BIBLIOGRAFICAS

Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH

<https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

First Hop Redundancy Protocols

<https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

Network Management

<https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

Switching Features and Technologies

<https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

High Availability

<https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>

Campus Network Security

<https://1drv.ms/b/s!AmIJYei-NT1lInWR0hoMxgBNv1CJ>