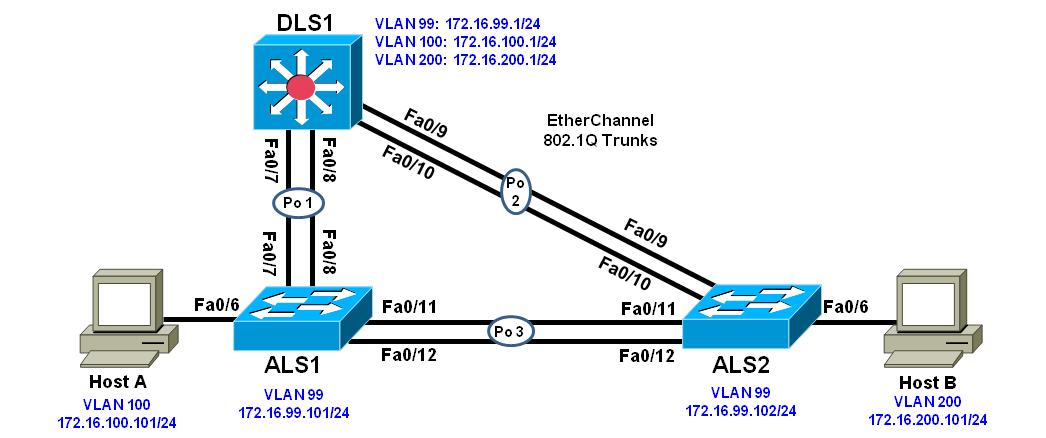
CCNPv7.1 SWITCH

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

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)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)
* 2 PC’s with Windows OS. One of the PCs should be equipped with Wireshark Application
* 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#

* 1. 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

* + 1. 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 }**

1. Configure Cisco IOS IP SLA
   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**

* 1. 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**

* 1. 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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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.

1. Switch Port Analyzer (SPAN) Feature

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

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

* 1. Configure Remote SPAN (RSPAN).

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

DLS1(config)# **vlan 300**

DLS1(config-vlan)# **name REMOTE\_SPAN**

DLS1(config-vlan)# **remote-span**

Use the **show vlan remote-span** command to verify the vlan 300 is configured correctly and is designated as the remote-span vlan. Ensure that the VLAN propagates across the VTP Domain

with show vlan brief command. Use the **show interface trunk** command to ensure the RSPAN VLAN is allowed on the trunks. The RSPAN VLAN should not be a DATA VLAN. Its purpose is strictly for carrying the monitored traffic across trunk links from one switch to another.

Verify the output on DLS1.

DLS1# **show vlan brief | include active**

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

99 Management active

100 Finance active

200 Engineering active

300 REMOTE\_SPAN active

666 NATIVE\_DO\_NOT\_USE active

DLS1#

Verify the output on ALS1.

ALS1# **show vlan brief | include active**

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

99 Management active

100 Finance active Fa0/6

200 Engineering active

300 REMOTE\_SPAN active

666 NATIVE\_DO\_NOT\_USE active

ALS1#

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

ALS1(config)# **monitor session 1 source interface Fa0/6**

ALS1(config)# **monitor session 1 destination remote vlan 300**

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

ALS1# **show monitor**

Session 1

---------

Type : Remote Source Session

Source Ports :

Both : Fa0/6

Dest RSPAN VLAN : 300

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

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

Configure ALS2 for the remote span session.

ALS2(config)# **monitor session 10 source remote vlan 300**

ALS2(config)# **monitor session 10 destination interface Fa0/6**

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

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

ALS2# **show monitor**

Session 10

----------

Type : Remote Destination Session

Source RSPAN VLAN : 300

Destination Ports : Fa0/6

Encapsulation : Native

Ingress : Disabled

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

ALS2# **show interface f0/6**

FastEthernet0/6 is up, line protocol is down (monitoring)

Hardware is Fast Ethernet, address is 5017.ff84.0a86 (bia 5017.ff84.0a86)

<output omitted>

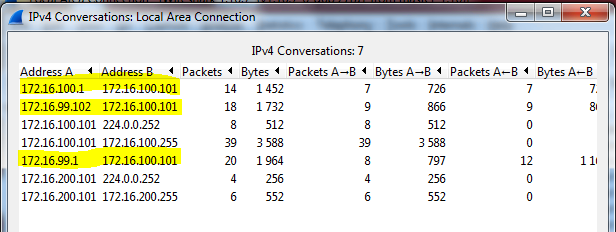
* 1. Test RSPAN operation

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

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

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

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



* 1. End of Lab

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