CCNPv7 SWITCH

Chapter 7 Lab 7-1, Synchronizing Campus Network Devices using Network Time Protocol (NTP) **Instructor Version**

Topology

Objective

* Configure network to synchronize time using the Network Time Protocol.
* Secure NTP using MD5 authentication and access-lists
* Verify NTP Operation
* NTP cez NAT z internetu?vyzadovalo by to router s VRF a NAT

Background

NTP is designed to synchronize the time on a network of devices. NTP runs over the 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 is 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-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 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-ipservicesK9-M image or comparable)
* Ethernet and console cables
* 4 PC’s connected to the topology according to the diagram.

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 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** |

1. Configure default gateways on the access layer switches ALS1 and ALS2. The distribution layer switches will not use a default gateway because they act as Layer 3 devices. The access layer switches act as Layer 2 devices and need a default gateway to send management VLAN traffic off of the local subnet for the management VLAN.

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

ALS2(config)# **ip default-gateway 172.16.99.2**

Step 4: 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 reenable them after the port channel is configured.

1. 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. The native vlan has been changed to vlan 666 and the switchport has been set to nonegotiate. 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 trunk native vlan 666**

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

1. 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. The native vlan has been changed to vlan 666 and the switchport has been set to nonegotiate. 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 trunk native vlan 666**

ALS1(config-if-range)# **switchport nonegotiate**

ALS1(config-if-range)# **channel-group 1 mode desirable**

ALS1(config-if-range)# **no shut**

1. 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

1. 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?

The EtherChannel negotiation in use is PagP

Step 5: Configure VTP on DLS2, ALS1 and ALS2.

1. Change the VTP mode of ALS1 and ALS2 to client and VTP modes of DLS2 to *server*.

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

Setting device to VTP CLIENT mode for VLANS.

**ALS2(config)# vtp mode client**

Setting device to VTP CLIENT mode for VLANS.

Set DLS2 to server mode**.**

**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.

1. Verify the VTP changes with the show vtp status command.

**ALS1# 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 : 0017.95d1.8b80

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 : 255

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

Step 6: Configure VTP on DLS1.

1. 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 NTP**

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**

DLS1(config-vlan)# **vlan 666**

DLS1(config-vlan)# **name NATIVE\_DO\_NOT\_USE**

Step 7: Configure access ports.

1. 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.

DLS1(config)# **interface fastEthernet 0/6**

DLS1(config-if)# **switchport mode access**

DLS1(config-if)# **switchport access vlan 99**

DLS1(config-if)# **spanning-tree portfast**

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

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**

ALS1(config)# **interface fastEthernet 0/6**

ALS1(config-if)# **switchport mode access**

ALS1(config-if)# **switchport access vlan 10**

ALS1(config-if)# **spanning-tree portfast**

DALS1(config-if)# **no shutdown**

ALS2(config)# **interface fastEthernet 0/6**

ALS2(config-if)# **switchport mode access**

ALS2(config-if)# **switchport access vlan 20**

ALS2(config-if)# **spanning-tree portfast**

ALS2(config-if)# **no shutdown**

1. Ping from the host on VLAN 10 to the host on VLAN 40. The ping should fail.

Are these results expected at this point? Why?

Yes, it is expected that the pings will fail because no SVIs have been created on DLS1 and DLS2, except for VLAN 1. Therefore, there is no default gateway for the hosts.

**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).

Step 8: Configure SVIs for L3 interfaces and enable routing.

**DLS1(config)# ip routing**

**DLS1(config)# interface loopback 1**

**DLS1(config-if)# ip address 200.200.200.1 255.255.255.0**

**DLS1(config-if)# exit**

Note: The purpose of this loopback interface is to be used as the source for NTP.

DLS1(config)# **interface vlan 10**

DLS1(config-if)# **ip address 172.16.10.1 255.255.255.0**

**DLS1(config-if)# exit**

DLS1(config)# **interface vlan 20**

DLS1(config-if)# **ip address 172.16.20.1 255.255.255.0**

DLS1(config)# **interface vlan 30**

DLS1(config-if)# **ip address 172.16.30.1 255.255.255.0**

DLS1(config)# **interface vlan 40**

DLS1(config-if)# **ip address 172.16.40.1 255.255.255.0**

DLS2(config)# **ip routing**

DLS2(config)# **interface vlan 10**

DLS2(config-if)# **ip address 172.16.10.2 255.255.255.0**

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)# **exit**

DLS2(config)# **interface vlan 30**

DLS2(config-if)# **ip address 172.16.30.2 255.255.255.0**

DLS2(config)# **interface vlan 40**

DLS2(config-if)# **ip address 172.16.40.2 255.255.255.0**

DLS2(config)# **ip route 200.200.200.0 255.255.255.0 172.16.99.1**

NOTE: This static route is used to route to R1’s loopback interface. R1’s loopback interface will be used as the NTP source for synchronization purposes in subsequent steps in the lab.

Step 9: Configure the system clock .

1. 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**

**\*02:27:16.911 UTC Mon Mar 1 1993**

1. 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.*

DLS1# **clock set ?**

**hh:mm:ss Current Time**

DLS1# **clock set 1:06:15 ?**

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

**MONTH Month of the year**

DLS1# **clock set 1:06:15 8 September ?**

**<1993-2035> Year**

DLS1# **clock set 1:06:15 8 September 2014**

**\*Sep 8 01:06:15.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 02:32:45 UTC Mon Mar 1 1993 to 01:06:15 UTC Mon Sep 8 2014, configured from console by console.**

1. Verify that the system clock has been updated.

DLS1# **show clock**

**01:06:32.070 UTC Mon Sep 8 2014DLS1#sh clock**

**\*02:27:16.911 UTC Mon Mar 1 1993**

1. The default timezone is UTC. Change the default timezone to EDT -5. The -5 is the difference in hours from UTC. Use clock timezone zone hours-offset command in ***global configuration***.

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

**WORD name of time zone**

DLS1(config)# **clock timezone EDT ?**

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

DLS1(config)# **clock timezone EDT -5 ?**

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

**<cr>**

DLS1(config)# **clock timezone EDT -5**

Sep 8 01:13:45.191: %SYS-6-CLOCKUPDATE: System clock has been updated from 01:13:45 UTC Mon Sep 8 2014 to 20:13:45 EDT Sun Sep 7 2014, configured from console by console.

1. Enable daylight savings time. The command **clock summer-time EDT recurring** command will allow the automatic switch to daylight saving time.

DLS1(config)# **clock summer-time ?**

**WORD name of time zone in summer**

DLS1(config)# **clock summer-time EDT ?**

**date Configure absolute summer time**

**recurring Configure recurring summer time**

DLS1(config)# **clock summer-time EDT recurring**

Sep 8 01:14:10.516: %SYS-6-CLOCKUPDATE: System clock has been updated from 20:14:10 EDT Sun Sep 7 2014 to 21:14:10 EDT Sun Sep 7 2014, configured from console by console.]

NOTE: This command used without parameters defaults to United States rules.

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

DLS1# **show clock detail**

21:14:31.395 EDT Sun Sep 7 2014

Time source is user configuration

Summer time starts 02:00:00 EDT Sun Mar 9 2014

Summer time ends 02:00:00 EDT Sun Nov 2 2014

The clock setting should reflect the local time.

Setting the clocks manually is not viewed as an accurate method of keeping track of 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.

Step 10: 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.

1. 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**

It is recommended that more than one device be designated as NTP server. If multiple devices are configured as ntp servers, the **ntp server 200.200.200.1 prefer** command can be used to designate one as preferred over another. In this lab scenario, only one device will be used as an NTP time source.

1. 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 200.200.200.1**

DLS2(config)# **clock timezone EDT -5**

Mar 1 00:48:25.968: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:48:25 UTC Mon Mar 1 1993 to 20:48:25 EDT Sun Feb 28 1993, configured from console by console.

DLS2(config)# **clock summer-time ?**

WORD name of time zone in summer

DLS2(config)# **clock summer-time EDT recurring**

Mar 1 00:54:36.589: %SYS-6-CLOCKUPDATE: System clock has been updated from 20:54:36 EDT Sun Feb 28 1993 to 20:54:36 EDT Sun Feb 28 1993, configured from console by console.

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

Step 11: 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 200.200.200.1

nominal freq is 119.2092 Hz, actual freq is 119.2101 Hz, precision is 2\*\*17

reference time is AF3CE6C4.CD93512C (14:47:16.803 EDT Mon Mar 1 1993)

clock offset is -4.5084 msec, root delay is 2.03 msec

root dispersion is 7944.53 msec, peer dispersion is 2.14 msec

loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000007161 s/s

system poll interval is 64, last update was 2 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.**

**Step 12: Secure NTP Operation using Access-Lists and Authentication**

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. Use the show ntp associations command to view the IP address of the internal NTP server.

NTP operation can also 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 unathenticated requests. For this reason, access lists should be used in conjunction with NTP authenciation to restrict NTP access.

1. **Configure NTP authentication on NTP server.**

DLS1(config)# **ntp authenticate**

DLS1(config)# **ntp authentication-key 1 md5 P@55word**

DLS1(config)# **ntp trusted-key 1**

1. **Configure NTP authentication on NTP clients (DLS2, ALS1, ALS2).**

DLS2(config)# **ntp authentication-key 1 md5 P@55word**

DLS2(config)# **ntp authenticate**

DLS2(config)# **ntp trusted-key 1**

**! Pridane**

DLS2(config)# **ntp server 200.200.200.1 key 1**

Use the **show ntp status** command to verify that clock is still synchronized. If the clock shows unsynchronized, the client has not successfully authenticated.

DLS2# **show ntp status**

Clock is synchronized, stratum 11, reference is 200.200.200.1

nominal freq is 119.2092 Hz, actual freq is 119.2106 Hz, precision is 2\*\*17

reference time is D7C2D495.6AD26EF6 (12:24:05.417 EDT Tue Sep 16 2014)

clock offset is -0.0479 msec, root delay is 1.63 msec

root dispersion is 5.83 msec, peer dispersion is 2.48 msec

loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000011269 s/s

system poll interval is 128, last update was 35 sec ago.

DLS2#

* + 1. Repeat this commands on ALS1 and ALS2. Verify that the device clocks are synchronized using the appropriate show command.

1. **Control NTP Access using Access-Lists**

View the output for the **show ntp associations**. 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# **sh 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 0.241

\* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

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(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 ?**

<1-99> Standard IP access list

<1300-1999> Standard IP access list (expanded range)

WORD Named access list

DLS1(config)# **ntp access-group peer 1**

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 serve-only 2**

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

**Step 13: 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 D7BD8B98.3BCA053A (11:11:20.233 EDT Fri Sep 12 2014)

clock offset is 0.0000 msec, root delay is 0.00 msec

root dispersion is 7937.58 msec, peer dispersion is 7937.50 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 12 16 1 0.000 0.000 7937.5

\* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

DLS1# **show clock detail**

11:11:38.268 EDT Fri Sep 12 2014

Time source is NTP

Summer time starts 02:00:00 EDT Sun Mar 9 2014

Summer time ends 02:00:00 EDT Sun Nov 2 201

Compare the output on DLS2 to ALS1 and ALS2 devices.

DLS2# **show ntp status**

Clock is synchronized, stratum 11, reference is 200.200.200.1

nominal freq is 119.2092 Hz, actual freq is 119.2096 Hz, precision is 2\*\*17

reference time is D7BDB443.388A60FB (15:04:51.220 EDT Fri Sep 12 2014)

clock offset is -10.7549 msec, root delay is 1.42 msec

root dispersion is 16.67 msec, peer dispersion is 3.42 msec

loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000002674 s/s

system poll interval is 64, last update was 204 sec ago.

DLS2# **show ntp associations**

address ref clock st when poll reach delay offset disp

\*~200.200.200.1 127.127.1.1 10 18 64 377 1.414 -10.754 3.427

\* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

DLS2# **show clock detail**

15:08:32.977 EDT Fri Sep 12 2014

Time source is NTP

Summer time starts 02:00:00 EDT Sun Mar 9 2014

Summer time ends 02:00:00 EDT Sun Nov 2 2014

ALS1# **show ntp status**

Clock is synchronized, stratum 11, reference is 200.200.200.1

nominal freq is 119.2092 Hz, actual freq is 119.2097 Hz, precision is 2\*\*17

reference time is D7BDB481.693FE416 (18:05:53.411 UTC Fri Sep 12 2014)

clock offset is -12.9590 msec, root delay is 1.59 msec

root dispersion is 20.49 msec, peer dispersion is 4.45 msec

loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000004084 s/s

system poll interval is 64, last update was 369 sec ago.

ALS1# **show ntp associations**

address ref clock st when poll reach delay offset disp

\*~200.200.200.1 127.127.1.1 10 49 64 377 1.590 -12.959 4.455

\* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

ALS1# **show clock detail**

18:12:11.276 UTC Fri Sep 12 2014

Time s

ALS2# **show ntp status**

Clock is synchronized, stratum 11, reference is 200.200.200.1

nominal freq is 119.2092 Hz, actual freq is 119.2098 Hz, precision is 2\*\*17

reference time is D7BDB418.17E9DD27 (18:04:08.093 UTC Fri Sep 12 2014)

clock offset is -16.3063 msec, root delay is 1.50 msec

root dispersion is 24.85 msec, peer dispersion is 4.54 msec

loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000004397 s/s

system poll interval is 64, last update was 428 sec ago.

ALS2# **show clock detail**

18:11:22.236 UTC Fri Sep 12 2014

Time source is NTP

**Step 14. Review the requirements in the next lab before proceeding with erasing of your device configurations and removal of the VLAN database.**