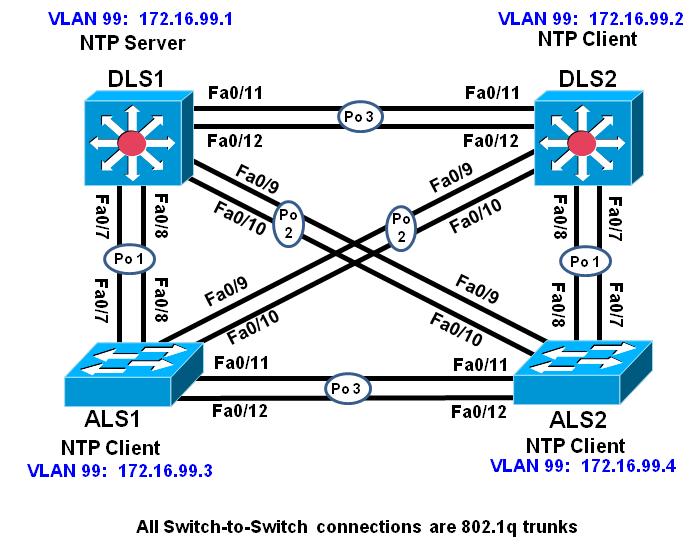
CCNPv7.1 SWITCH

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

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 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

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.

1. 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** |

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

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

* 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.

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. 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

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. 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**

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?

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

* 1. 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**

\*00:24:31.647 UTC Mon Mar 1 1993

1. 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**.**

1. Verify that the system clock has been updated.

DLS1# **show clock**

14:45:33.755 UTC Wed Jul 29 2015

1. 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

1. 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.

* 1. 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**

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 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.

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

* 1. 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.**

1. Secure NTP Operation using Access-Lists and Authentication
   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.

1. 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**

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.

1. Repeat these commands on ALS1 and ALS2. Verify that the device clocks are synchronized using the appropriate show command.
   1. 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 rendered to the requesting device.

* 1. 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#

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

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

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#

* 1. End of Lab.

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