

Configure Network Time Protocol on Nexus as Server and Client

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

- [1. Confirm clock is configured with NTP protocol.](#)
- [2. Confirm NTP server and Nexus IP is listed.](#)
- [3. Confirm NTP server configured is selected for sync.](#)
- [4. Verify NTP packets are received and sent to the server.](#)
- [5. Search for the packet sent from Nexus to its NTP client to confirm its using the configured NTP server as reference:](#)
- [6. Run an ELAM to verify if packets are assigned correctly to the statistics of the supervisor \(COPP\) redirect ACLs:](#)

[Related information](#)

Introduction

This document describes a simple configuration and validation for a Nexus 9000 platform to act as both Network Time Protocol (NTP) server and client.

Prerequisites

Requirements

Cisco Recommends that you have have knowledge of these topics:

- Nexus NX-OS Software.
- Network Time Protocol (NTP).

Components Used

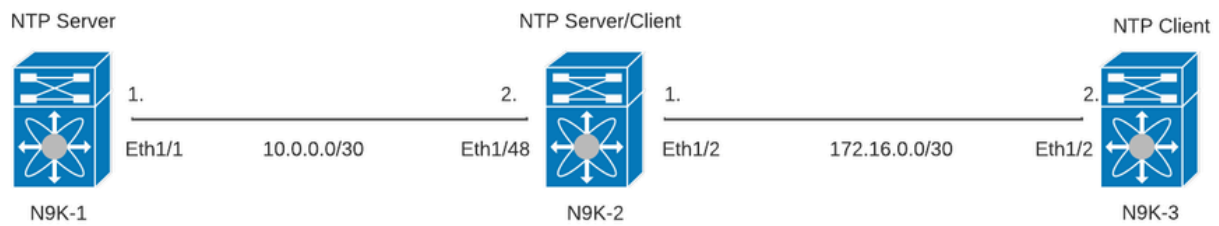
The information in this document is based on Cisco Nexus 9000 with NXOS version 10.2(5).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

NTP is a networking protocol used to synchronize the time of a set of devices within a network to correlate events when you receive system logs and other time-specific events from multiple network devices.

Network Diagram



Configurations

Step 1. Enable NTP.

```
feature ntp
```

Step 2. Set clock protocol to NTP.

```
clock protocol ntp
```

Step 3. Define Nexus as NTP client and server.



Warning: This protocol can take some minutes to sync even after packets are exchanged from server to client.



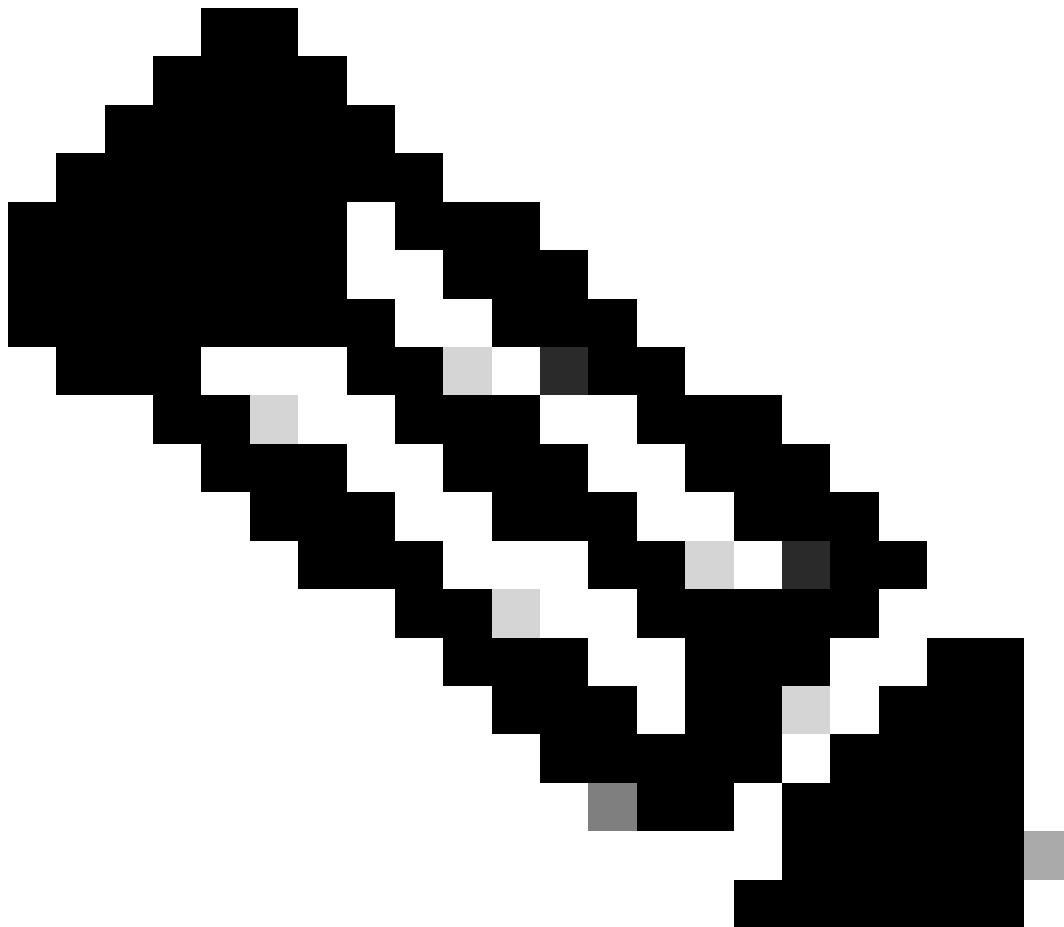
Note: The concept of a stratum is employed by NTP to indicate the distance (in NTP hops) between a machine and an authoritative time source. This value can be configured when enabling the NTP server on a Nexus with the command "ntp master <stratum>".

```
N9K-1# show running-config ntp
ntp source 10.0.0.1
ntp master 1
```

```
N9K-2# show running-config ntp
ntp server 10.0.0.1 use-vrf default
ntp source 10.0.0.2
ntp master 8
```

```
N9K-3# show running-config ntp
ntp server 172.16.0.1 use-vrf default
ntp source 172.16.0.2
```

Verify



Note: For exemplification purposes, verification is only focused on N9K-2, as it is running NTP server and client roles simultaneously.

1. Confirm clock is configured with NTP protocol.

```
N9K-2# show clock
12:32:51.528 UTC Thu Sep 28 2023
Time source is NTP          <<<<<
```

2. Confirm NTP server and Nexus IP is listed.

Note: The entry with IP address 127.127.1.0 is a local IP that indicates the Nexus has synced with itself, representing a locally generated reference clock source as part of the role for an NTP server.

N9K-2# show ntp peers

```
-----  
Peer IP Address          Serv/Peer  
-----  
10.0.0.1                 Server (configured)  
127.127.1.0             Server (configured) <<<
```

3. Confirm NTP server configured is selected for sync.

Note: A stratum (st) of 16 indicates that the server is not currently synchronized to a reliable time source and is never to be selected to synchronize. Beginning with Cisco NX-OS Release 10.1(1), only a stratum of 13 or lower can synchronize.

```
N9K-2# show ntp peer-status
```

```
Total peers : 2
```

```
* - selected for sync, + - peer mode(active),
```

```
- - peer mode(passive), = - polled in client mode
```

remote	local	st	poll	reach	de
=127.127.1.0	10.0.0.2	8	16	0	0.00
*10.0.0.1	10.0.0.2	2	32	377	0.00

4. Verify NTP packets are received and sent to the server.

Note: The command "show ntp statistics peer ipaddr <ntp-server>" only works for NTP clients. If there are non-default values on counters, you can clear them by using the command: "clear ntp statistics all-peers".

```
N9K-2# show ntp statistics peer ipaddr 10.0.0.1
remote host:      10.0.0.1
local interface:  10.0.0.2
time last received: 28s
time until next send: 5s
reachability change: 876s
packets sent:     58      <<<<<<
packets received: 58      <<<<<<
bad authentication: 0
bogus origin:    0
duplicate:       0
bad dispersion:  0
bad reference time: 0
candidate order: 6
```


Example of packet capture for bidirectional NTP packets flow:

```
N9K-2# ethanalyzer local interface inband display-filter ntp limit-captured-frames 0
Capturing on 'ps-inb'
  4 2024-01-01 03:23:47.900233043 172.16.0.2 → 172.16.0.1 NTP 90 NTP Version 4, client
2   5 2024-01-01 03:23:47.900863464 172.16.0.1 → 172.16.0.2 NTP 90 NTP Version 4, server
  6 2024-01-01 03:23:52.926382561 10.0.0.2 → 10.0.0.1 NTP 90 NTP Version 4, client
  4   7 2024-01-01 03:23:52.927169592 10.0.0.1 → 10.0.0.2 NTP 90 NTP Version 4, server
```

5. Search for the packet sent from Nexus to its NTP client to confirm its using the configured NTP server as reference:

```
N9K-2# ethanalyzer local interface inband display-filter ntp limit-captured-frames 0 detail
Capturing on 'ps-inb'
...
<output omitted>
...
Frame 5: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface ps-inb, id 0
  Interface id: 0 (ps-inb)
    Interface name: ps-inb
  Encapsulation type: Ethernet (1)
  Arrival Time: Jan 1, 2024 03:24:35.900699824 UTC
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1704079475.900699824 seconds
  [Time delta from previous captured frame: 0.000643680 seconds]
  [Time delta from previous displayed frame: 0.000643680 seconds]
  [Time since reference or first frame: 10.974237168 seconds]
  Frame Number: 5
  Frame Length: 90 bytes (720 bits)
  Capture Length: 90 bytes (720 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:ntp]
Ethernet II, Src: d4:77:98:2b:4c:87, Dst: f8:0b:cb:e5:d9:fb
  Destination: f8:0b:cb:e5:d9:fb
    Address: f8:0b:cb:e5:d9:fb
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ...0 .... = IG bit: Individual address (unicast)
  Source: d4:77:98:2b:4c:87
    Address: d4:77:98:2b:4c:87
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ...0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.0.1, Dst: 172.16.0.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 76
  Identification: 0xbd85 (48517)
  Flags: 0x0000
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
```

```

Fragment offset: 0
Time to live: 255
Protocol: UDP (17)          <<<<< UDP protocol number
Header checksum: 0xa5f7 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.0.1        <<<<<
Destination: 172.16.0.2  <<<<< NTP Client
User Datagram Protocol, Src Port: 123, Dst Port: 123
Source Port: 123
Destination Port: 123
Length: 56
Checksum: 0x71d5 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]
  [Time since first frame: 0.000643680 seconds]
  [Time since previous frame: 0.000643680 seconds]
Network Time Protocol (NTP Version 4, server)
Flags: 0x24, Leap Indicator: no warning, Version number: NTP Version 4, Mode: server
  00.. .... = Leap Indicator: no warning (0)
  ..10 0... = Version number: NTP Version 4 (4)
  .... .100 = Mode: server (4)
Peer Clock Stratum: secondary reference (3)
Peer Polling Interval: 4 (16 seconds)
Peer Clock Precision: 0.000000 seconds
Root Delay: 0.001083 seconds
Root Dispersion: 0.013611 seconds
Reference ID: 10.0.0.1      <<<<< NTP server
Reference Timestamp: Jan  1, 2024 03:22:32.927228435 UTC
Origin Timestamp: Jan  1, 2024 03:24:35.896950020 UTC
Receive Timestamp: Jan  1, 2024 03:24:35.900271042 UTC
Transmit Timestamp: Jan  1, 2024 03:24:35.900397771 UTC

```

6. Run an ELAM to verify if packets are assigned correctly to the statistics of the supervisor (COPP) redirect ACLs:

Note: NTP traffic must be punted to CPU, so it has the sup_hit flag set.

```
N9K-2# debug platform internal tah elam
N9K-2(TAH-elam)# trigger init
Slot 1: param values: start asic 0, start slice 0, lu-a2d 1, in-select 6, out-select
N9K-2(TAH-elam-inse16)# reset
N9K-2(TAH-elam-inse16)# set outer ipv4 next-protocol 17 packet-len 76 src_ip 10.0.0.1 dst_ip 10.0.0.2
N9K-2(TAH-elam-inse16)# start
N9K-2(TAH-elam-inse16)# report
SUGARBOWL ELAM REPORT SUMMARY
slot - 1, asic - 0, slice - 0
=====

Incoming Interface: Eth1/48
Src Idx : 0xbd, Src BD : 4147
Outgoing Interface Info: dmod 0, dpid 0
Dst Idx : 0x5bf, Dst BD : 4147

Packet Type: IPv4

Dst MAC address: D4:77:98:2B:4C:87
```

Src MAC address: D4:77:98:2B:43:27

Sup hit: 1, Sup Idx: 2753 <<<<< packet punt identifier, use below CLI to resolve its meaning

Dst IPv4 address: 10.0.0.2

Src IPv4 address: 10.0.0.1

Ver = 4, DSCP = 0, Don't Fragment = 0

Proto = 17, TTL = 255, More Fragments = 0

Hdr len = 20, Pkt len = 76, Checksum = 0xae26

L4 Protocol : 17

UDP Dst Port : 123

UDP Src Port : 123

Drop Info:

LUA:

LUB:

LUC:

LUD:

Final Drops:

vntag:

vntag_valid : 0

vntag_vir : 0

vntag_svif : 0

ELAM not triggered yet on slot - 1, asic - 0, slice - 1

```
N9K-2(TAH-elam-inse16)# show system internal access-list sup-redirect-stats | i 2753
2753                                copp-system-p-acl-ntp      462          <<<<< correct ACL assigned
```

Related information

[Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.2\(x\)](#)