Nexus에서 Network Time Protocol을 서버 및 클라이언트로 구성

목차

소개

이 문서에서는 NTP(Network Time Protocol) 서버 및 클라이언트 역할을 하는 Nexus 9000 플랫폼의 간단한 구성 및 검증에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

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

사용되는 구성 요소

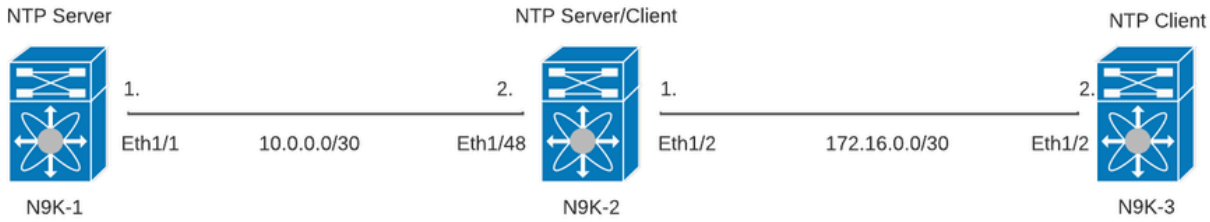
이 문서의 정보는 NXOS 버전 10.2(5)를 사용하는 Cisco Nexus 9000을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

NTP는 여러 네트워크 디바이스에서 시스템 로그 및 기타 시간별 이벤트를 수신할 때 이벤트의 상관관계를 분석하기 위해 네트워크 내에서 디바이스 집합의 시간을 동기화하는 데 사용되는 네트워킹 프로토콜입니다.

네트워크 다이어그램



설정

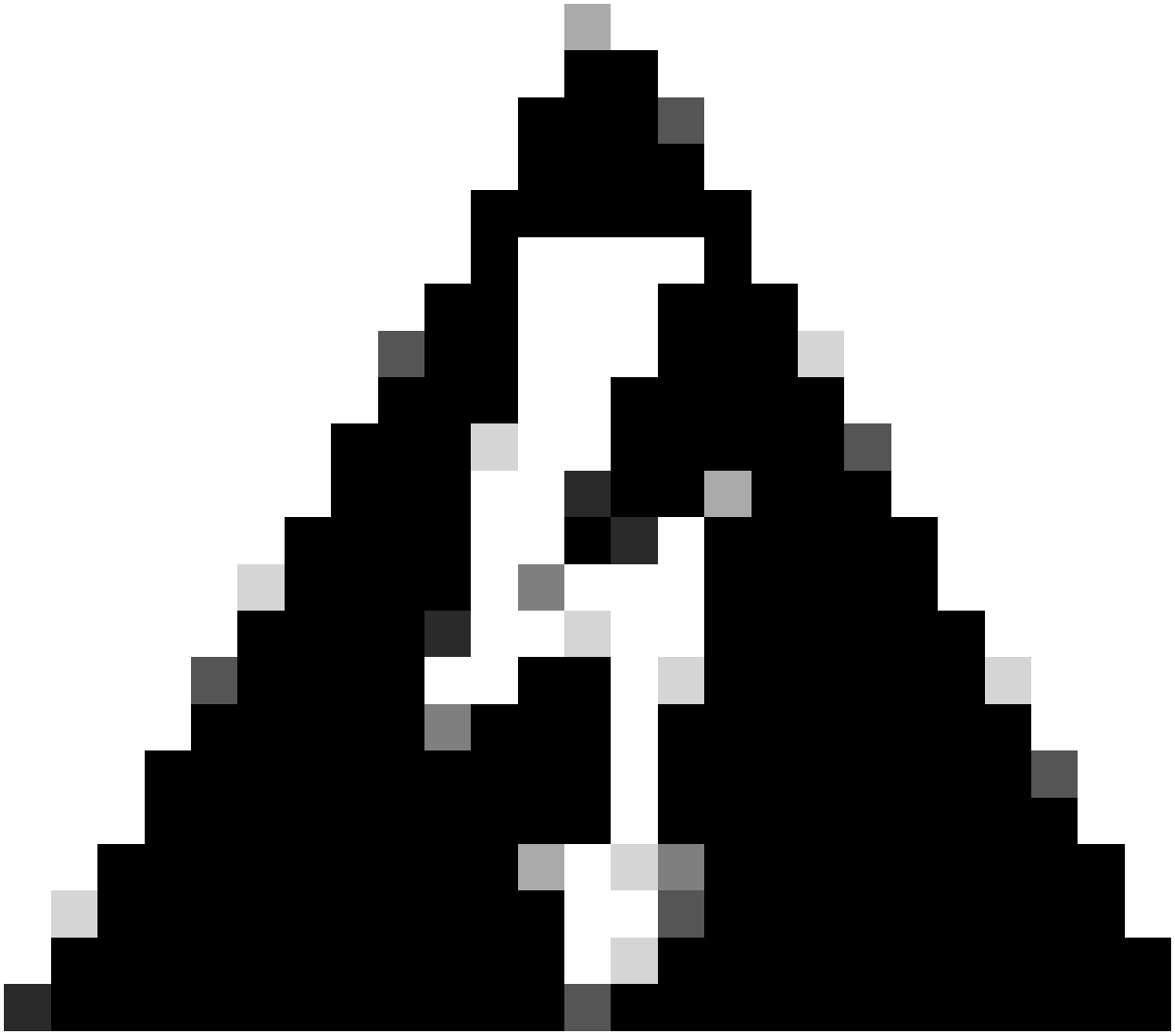
1단계. NTP를 활성화합니다.

```
feature ntp
```

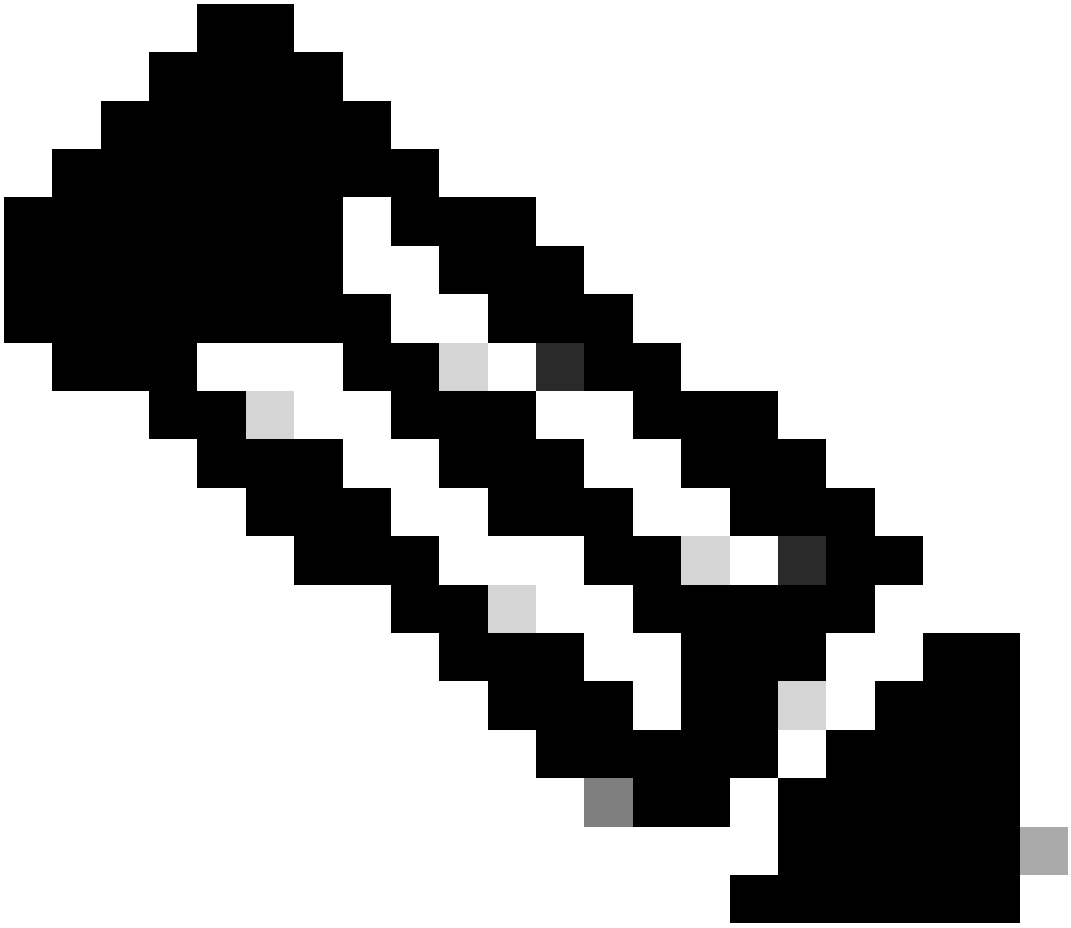
2단계. 클록 프로토콜을 NTP로 설정합니다.

```
clock protocol ntp
```

3단계. Nexus를 NTP 클라이언트 및 서버로 정의합니다.



경고: 이 프로토콜은 서버에서 클라이언트로 패킷이 교환된 후에도 동기화하는 데 몇 분 정도 걸릴 수 있습니다.



참고: 계층 개념은 NTP에서 시스템과 권한 있는 시간 소스 간의 거리(NTP 홉)를 나타내기 위해 사용합니다. 이 값은 "ntp master <stratum>" 명령을 사용하여 Nexus에서 NTP 서버를 활성화할 때 구성할 수 있습니다.

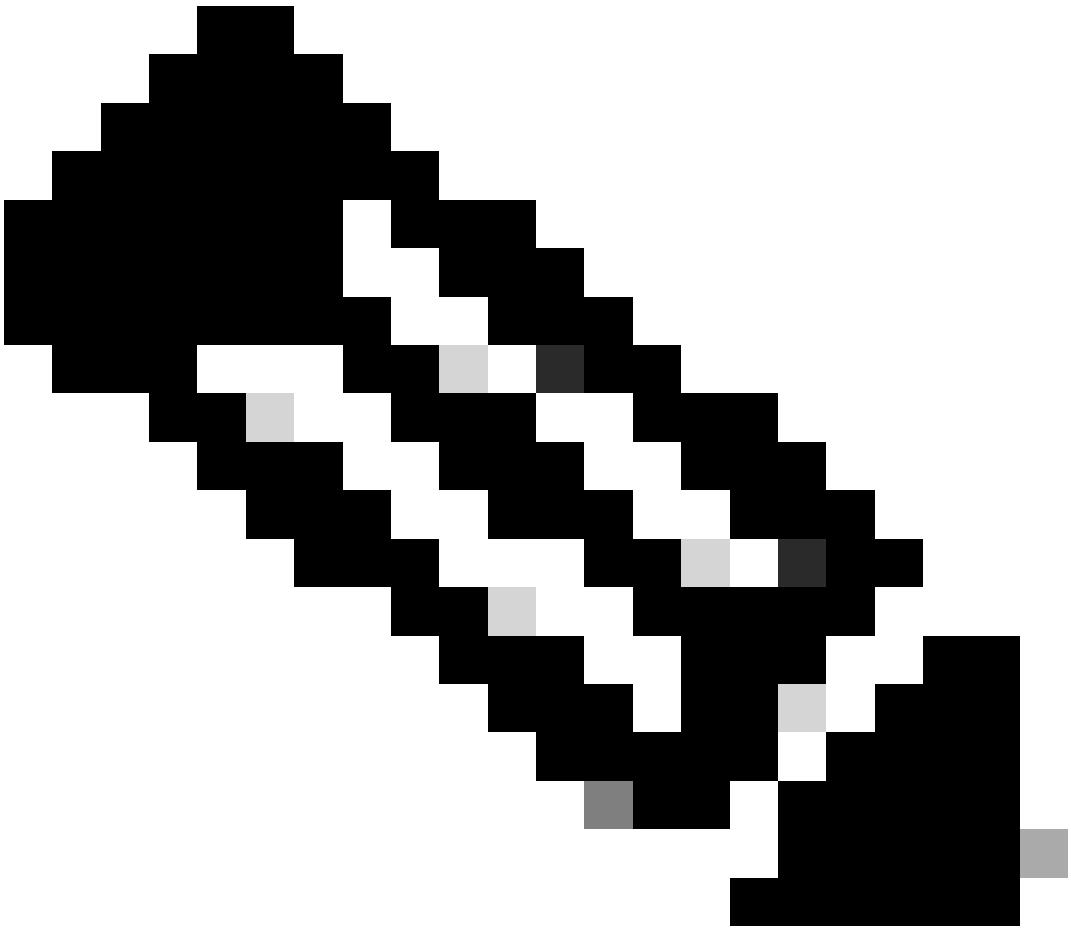
```
N9K-1# show running-config ntp
ntp source 10.0.0.1
ntp master 1
```

```
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
```

다음을 확인합니다.



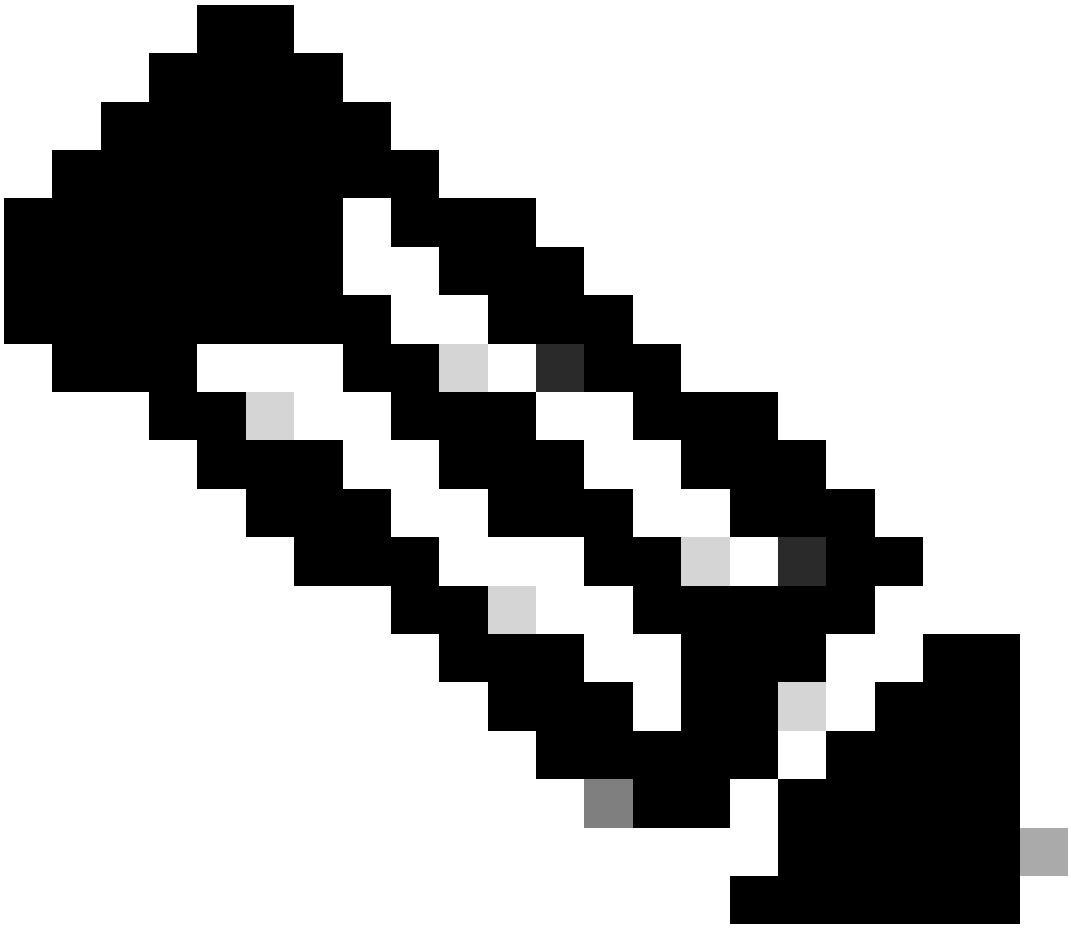
참고: 예를 들어, NTP 서버 및 클라이언트 역할을 동시에 실행 중이므로 N9K-2에만 확인이 집중됩니다.

---

1. 클럭이 NTP 프로토콜로 구성되었는지 확인합니다.

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

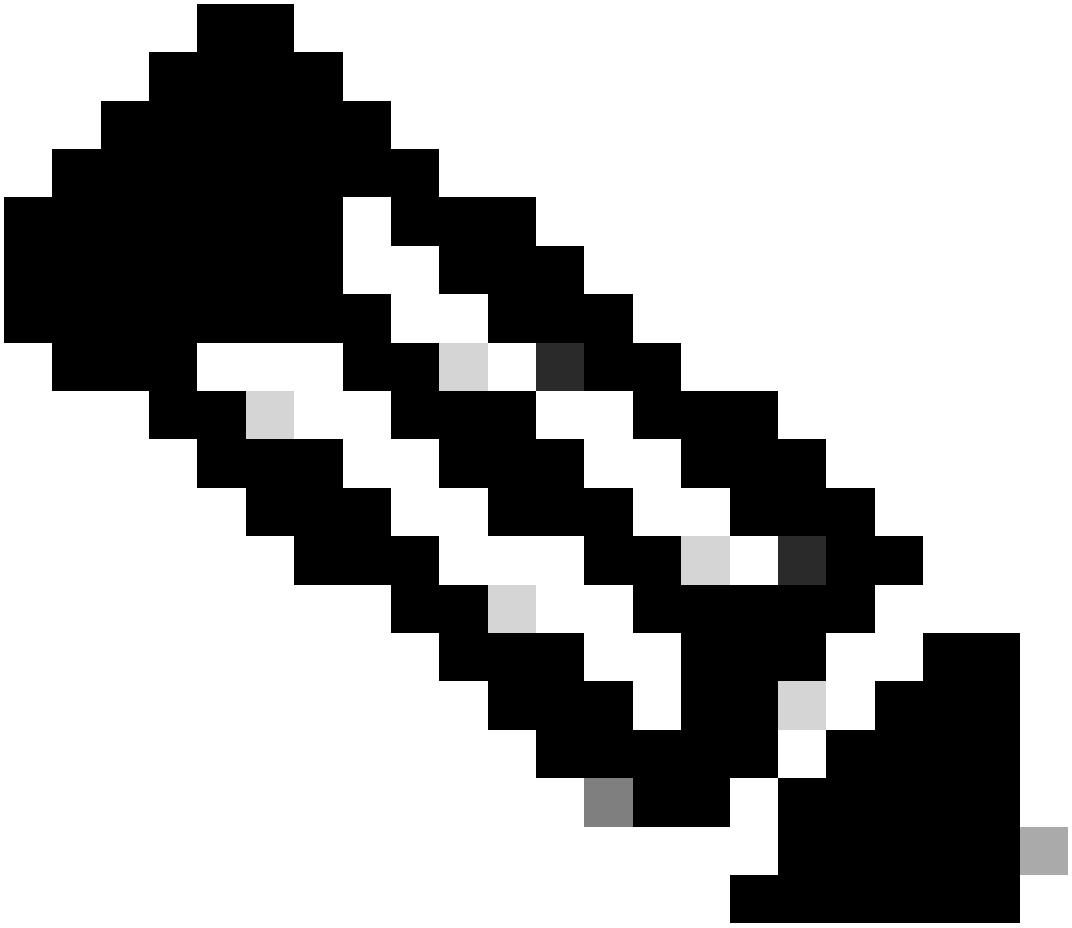
2. NTP 서버 및 Nexus IP가 나열되는지 확인합니다.



참고: IP 주소가 127.127.1.0인 항목은 Nexus가 자신과 동기화되었음을 나타내는 로컬 IP이며, 로컬에서 생성된 참조 클록 소스를 NTP 서버 역할의 일부로 나타냅니다.

```
N9K-2# show ntp peers
-------------------------------------------------
  Peer IP Address               Serv/Peer
-------------------------------------------------
  10.0.0.1                      Server (configured)
  127.127.1.0                   Server (configured)    <<<
```

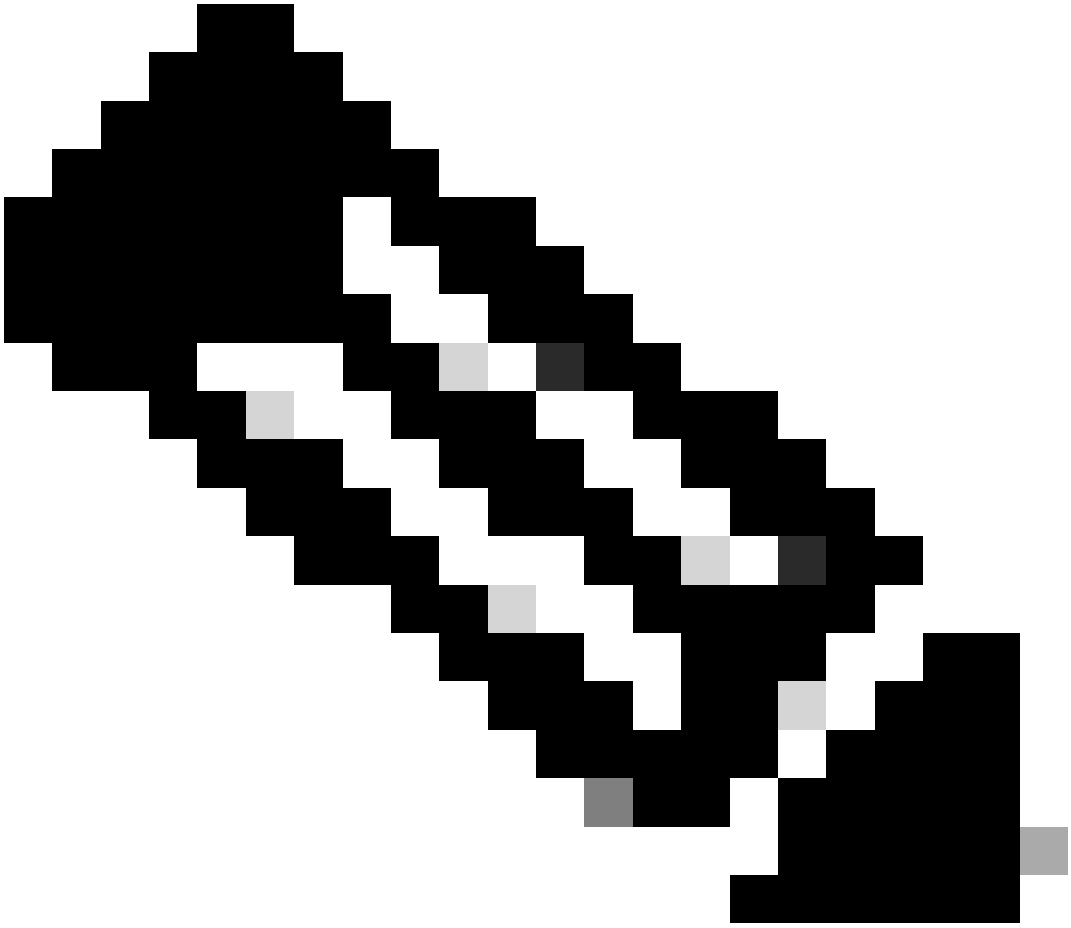
3. 구성된 NTP 서버가 동기화하도록 선택되었는지 확인합니다.



참고: 계층(st)이 16이면 서버가 현재 신뢰할 수 있는 시간 소스에 동기화되지 않았으며 동기화하도록 선택하지 않았음을 나타냅니다. Cisco NX-OS Release 10.1(1)부터는 13 이하 계층만 동기화할 수 있습니다.

```
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. NTP 패킷이 수신되어 서버로 전송되는지 확인합니다.



참고: "show ntp statistics peer ipaddr <ntp-server>" 명령은 NTP 클라이언트에만 작동합니다. 카운터에 기본값이 아닌 값이 있는 경우 "clear ntp statistics all-peers" 명령을 사용하여 이를 지울 수 있습니다.

```
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
```

양방향 NTP 패킷 흐름에 대한 패킷 캡처의 예:

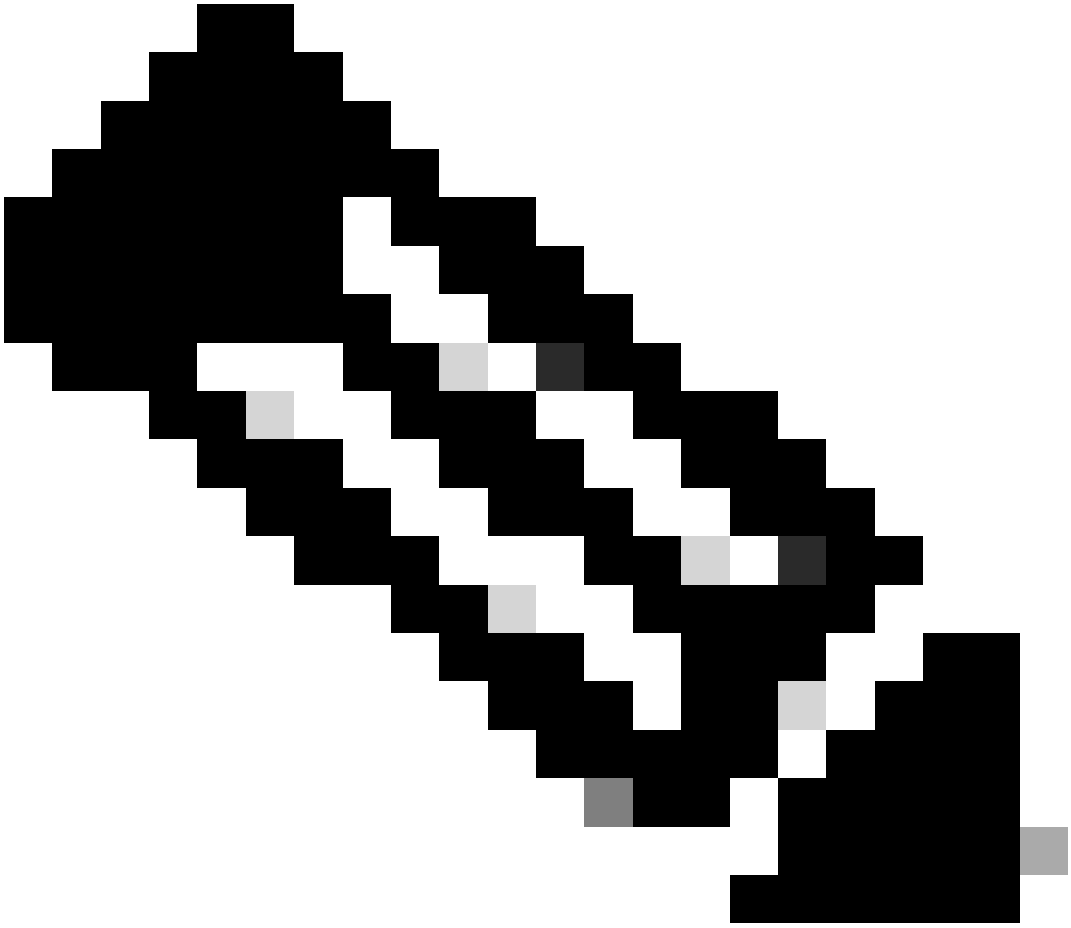
```
N9K-2# ethanalyzer local interface inband display-filter ntp limit-captured-frames 0
Capturing on 'ps-inb'
    4 2024-01-01 03:23:47.900233043   172.16.0.2 → 172.16.0.1   NTP 90 NTP Version 4, client
2     5 2024-01-01 03:23:47.900863464   172.16.0.1 → 172.16.0.2   NTP 90 NTP Version 4, server
    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. 구성된 NTP 서버를 참조로 사용하여 Nexus에서 NTP 클라이언트로 보낸 패킷을 확인하여 패킷을 확인합니다.

```
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. ELAM을 실행하여 패킷이 COPP(감독자) 리디렉션 ACL의 통계에 올바르게 할당되었는지 확인합니다.



참고: NTP 트래픽은 sup_hit 플래그가 설정되어 있으므로 CPU에 펀팅해야 합니다.

```
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-insel6)# reset
N9K-2(TAH-elam-insel6)# 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-insel6)# start
N9K-2(TAH-elam-insel6)# 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-insel6)#  show system internal access-list sup-redirect-stats | i 2753
    2753                            copp-system-p-acl-ntp    462        <<<<< correct ACL assigned
```

관련 정보

[Cisco Nexus 9000 Series NX-OS System Management 컨피그레이션 가이드, 릴리스 10.2(x)]

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.