Troubleshoot Network Time Protocol (NTP) Issues on vEdge

Contents

Introduction

This document describes how to troubleshoot Network Time Protocol (NTP) issues with **show ntp** commands and packet capture tools on vEdge platforms.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software versions or vEdge models.

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.

Example Symptoms of NTP Issues

Loss of NTP synchonization to a vEdge can manifest in a few different ways, for example:

- Incorrect time in **show clock** output on the device.
- Certificates seen as invalid due to an incorrect time outside the validity range.

- Incorrect timestamps on logs.

NTP Show Commands

To begin isolation of NTP problems, you must understand the use of and output from two main commands:

- show ntp associations
- show ntp peer

Further details of specific commands can be found in the SD-WAN Command Reference.

Show NTP Associations

```
vedge1# show ntp associations

                                                                    LAST
IDX  ASSOCID  STATUS  CONF  REACHABILITY  AUTH  CONDITION  EVENT      COUNT
-------------------------------------------------------------------------------
1    56368    8011    yes   no            none  reject     mobilize   1
2    56369    911a    yes   yes           none  falsetick  sys_peer   1
3    56370    9124    yes   yes           none  falsetick  reachable  2
```

IDX	local index number
ASSOCID	association ID
STATUS	peer status word (in hexadecimal)
CONF	configuration (persistent or ephemeral)
REACHABILITY	reachability (yes or no)
AUTH	authentication (ok, yes, bad, or none)
CONDITION	selection status
EVENT	last event for this peer
COUNT	event count

Show NTP Peer

```
vedge1# show ntp peer | tab

INDEX  REMOTE          REFID     ST  TYPE  WHEN  POLL  REACH  DELAY    OFFSET   JITTER
-------------------------------------------------------------------------------------
1      192.168.18.201  .STEP.    16  u     37    1024  0      0.000    0.000    0.000
2      x10.88.244.1    LOCAL(1)  2   u     7     64    377    108.481  140.642  20.278
3      x172.18.108.15  .GPS.     1   u     66    64    377    130.407  -24883.  55.334
```

INDEX	local index number
REMOTE	NTP server address
REFID	Current source of synchonization from the peer

ST	stratum NTP uses the concept of a stratum in order to describe how far away (in NTP hops) a machine is from an authoritative time source. For example, a stratum 1 time server has a radio or atomic clock directly attached to it. It sends its time to a stratum 2 time server through NTP, and so on up to stratum 16. A machine that runs NTP automatically chooses the machine with the lowest stratum number with which it can communicate and uses NTP as its time source.
TYPE	type
WHEN	The time since the last NTP packet was received from a peer is reported in seconds. This value must be lower than the poll interval.
POLL	poll interval (seconds)
REACH	reach, as specified by octal value based on last 8 connections 377 (1 1 1 1 1 1 1 1) - Last 8 were all OK 376 (1 1 1 1 1 1 1 0) - Last connection bad .... 177 (0 1 1 1 1 1 1 1) - Oldest connection was bad, all since good and so on
DELAY	The round-trip delay to peer is reported in milliseconds. In order to set the clock more accurately, this delay is taken into account when the clock time is set.
OFFSET	offset (in milliseconds) Offset is the clock time difference between the peers or between the primary and client. This value is the correction that is applied to a client clock in order to synchronize it. A positive value indicates the server clock is higher. A negative value indicates the client clock is higher.
JITTER	jitter (in milliseconds)

Troubleshoot NTP with vManage and Packet Capture Tools

Verify Egress with Simulate Flows on vManage

1. Choose the Network Device dashboard via **Monitor > Network**
2. Choose the applicable vEdge.
3. Click the **Troubleshooting** option, followed by **Simulate Flows**.
4. Specify source VPN and interface from drop-downs, set destination IP, and set application as ntp.
5. Click **Simulate.**

This gives the expected forwarding behavior for NTP traffic from the vEdge.

Collect TCPDump from vEdge

When NTP traffic traverses the control plane of the vEdge, it can be captured via TCPdump. The match condition would need to use the standard UDP port 123 to filter for NTP traffic specifically.

tcpdump vpn 0 options "dst port 123"

```
vedge1# tcpdump interface ge0/0 options "dst port 123"
tcpdump -p -i ge0_0 -s 128 dst port 123 in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
19:05:44.364567 IP 192.168.19.55.ntp > 10.88.244.1.ntp: NTPv4, Client, length 48
19:05:44.454385 IP 10.88.244.1.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:05:45.364579 IP 192.168.19.55.ntp > 172.18.108.15.ntp: NTPv4, Client, length 48
19:05:45.373547 IP 172.18.108.15.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:06:52.364470 IP 192.168.19.55.ntp > 10.88.244.1.ntp: NTPv4, Client, length 48
19:06:52.549536 IP 10.88.244.1.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
19:06:54.364486 IP 192.168.19.55.ntp > 172.18.108.15.ntp: NTPv4, Client, length 48
19:06:54.375065 IP 172.18.108.15.ntp > 192.168.19.55.ntp: NTPv4, Server, length 48
```

Add the verbose flag **-v** to decode the timestamps from within the NTP packets.

tcpdump vpn 0 options "dst port 123 -v"

```
vedge1# tcpdump interface ge0/0 options "dst port 123 -n -v"
tcpdump -p -i ge0_0 -s 128 dst port 123 -n -v in VPN 0
tcpdump: listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
19:10:13.364515 IP (tos 0xb8, ttl 64, id 62640, offset 0, flags [DF], proto UDP (17), length 76)
    192.168.19.55.123 > 192.168.18.201.123: NTPv4, length 48
        Client, Leap indicator: clock unsynchronized (192), Stratum 3 (secondary reference), poll 6 (64s
        Root Delay: 0.103881, Root dispersion: 1.073425, Reference-ID: 10.88.244.1
          Reference Timestamp:  3889015198.468340729 (2023/03/28 17:59:58)
          Originator Timestamp: 3889019320.559000091 (2023/03/28 19:08:40)
          Receive Timestamp:    3889019348.377538353 (2023/03/28 19:09:08)
          Transmit Timestamp:   3889019413.364485614 (2023/03/28 19:10:13)
            Originator - Receive Timestamp:  +27.818538262
            Originator - Transmit Timestamp: +92.805485523
19:10:13.365092 IP (tos 0xc0, ttl 255, id 7977, offset 0, flags [none], proto UDP (17), length 76)
    192.168.18.201.123 > 192.168.19.55.123: NTPv4, length 48
        Server, Leap indicator:  (0), Stratum 8 (secondary reference), poll 6 (64s), precision -10
        Root Delay: 0.000000, Root dispersion: 0.002166, Reference-ID: 127.127.1.1
          Reference Timestamp:  3889019384.881000144 (2023/03/28 19:09:44)
          Originator Timestamp: 3889019413.364485614 (2023/03/28 19:10:13)
```

```
Receive Timestamp:    3889019385.557000091 (2023/03/28 19:09:45)
Transmit Timestamp:   3889019385.557000091 (2023/03/28 19:09:45)
  Originator - Receive Timestamp:  -27.807485523
  Originator - Transmit Timestamp: -27.807485523
```

Perform Wireshark Capture from vManage

If packet captures have been enabled from vManage, NTP traffic can also be captured this way directly to a file readable by Wireshark.

1. Choose the Network Device dashboard via **Monitor > Network**
2. Choose the applicable vEdge.
3. Click the **Troubleshooting** option, followed by **Packet Capture**.
4. Choose VPN 0 and the outside interface from the drop-down menus.
5. Click **Traffic Filter**. Here you can specify destination port 123 and if desired, a specific destination server.

> **Note**: Filter by IP address only captures packets in one direction, as the IP filter is by source or destination. Because the destination layer 4 port is 123 in both directions, filter by the port only to capture bidirectional traffic.

---

6. Click **Start**.

vManage now communicates with the vEdge to gather a packet capture for either 5 minutes or until the 5MB buffer fills up, whichever comes first. Upon completion, that capture can be downloaded for review.

Common NTP Issues

NTP Packets Not Received

Packet captures show outbound packets sent to the configured server(s), but no replies received.

```
vedge1# tcpdump interface ge0/0 options "dst 192.168.18.201 && dst port 123 -n"
tcpdump -p -i ge0_0 -s 128 dst 192.168.18.201 && dst port 123 -n in VPN 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
14:24:49.364507 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
14:25:55.364534 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
14:27:00.364521 IP 192.168.19.55.123 > 192.168.18.201.123: NTPv4, Client, length 48
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

Once you confirm NTP packets are not received, you can:

- Check if NTP is configured correctly.
- If traffic traverses a tunnel in VPN 0, make sure **allow-service ntp** or **allow-service all** is enabled under the tunnel-interface.
- Check if NTP is blocked by an access-list or intermediary device.

- Check for routing issues between the NTP source and destination.

Loss of Synchonization

Loss of synchonization can ocur if the dispersion and/or delay value for a server goes very high. High values indicate that the packets take too long to get to the client from the server/peer in reference to the root of the clock. So, the local machine cannot trust the accuracy of the time present in the packet, because it does not know how long it took for the packet to arrive.

If there is a congested link in the path which causes buffering, packets are be delayed as they come to the NTP client.

If you experience a loss of synchonization, you must check the links:

- Is there congestion/oversubscription in the path?
- Are there dropped packets observed?
- Is there encryption involved?

The reach value in **show ntp peer** can indicate loss of NTP traffic. If the value is less than 377, packets are received intermittently and the client goes out of sync.

Clock on the Device Has Been Set Manually

The clock values learned from NTP can be overridden via the **clock set** command. When this happens, offset values for all peers increase significantly.

```
vedge1# show ntp peer | tab

INDEX  REMOTE           REFID     ST  TYPE  WHEN  POLL  REACH  DELAY    OFFSET   JITTER
-------------------------------------------------------------------------------------
1      x10.88.244.1     LOCAL(1)  2   u     40    64    1      293.339  -539686  88.035
2      x172.18.108.15   .GPS.     1   u     39    64    1      30.408   -539686  8.768
3      x192.168.18.201  LOCAL(1)  8   u     38    64    1      5.743    -539686  2.435
```

Verbose captures also show that the reference timestamps and originator timestamps do not align.

```
vedge1# tcpdump interface ge0/0 options "src 192.168.18.201 && dst port 123 -n -v"
tcpdump -p -i ge0_0 -s 128 src 192.168.18.201 && dst port 123 -n -v in VPN 0
tcpdump: listening on ge0_0, link-type EN10MB (Ethernet), capture size 128 bytes
00:01:28.156796 IP (tos 0xc0, ttl 255, id 8542, offset 0, flags [none], proto UDP (17), length 76)
    192.168.18.201.123 > 192.168.19.55.123: NTPv4, length 48
        Server, Leap indicator:  (0), Stratum 8 (secondary reference), poll 6 (64s), precision -10
        Root Delay: 0.000000, Root dispersion: 0.002365, Reference-ID: 127.127.1.1
          Reference Timestamp:  3889091263.881000144 (2023/03/29 15:07:43)
          Originator Timestamp: 133810392.155976055 (2040/05/05 00:01:28)
          Receive Timestamp:    3889091277.586000096 (2023/03/29 15:07:57)
          Transmit Timestamp:   3889091277.586000096 (2023/03/29 15:07:57)
            Originator - Receive Timestamp:  -539686410.569975959
            Originator - Transmit Timestamp: -539686410.569975959
^C
1 packet captured
1 packet received by filter
```

```
0 packets dropped by kernel
```

To force the vEdge to resume preference for NTP as its time source, delete, commit, re-add, and re-commit the configuration under **system ntp**.

References and Related Information

- Troubleshoot and Debug NTP Issues (Cisco IOS devices)
- Cisco SD-WAN Command Reference
- Verifying NTP Status with the show ntp associations Command