排除vEdge上的网络时间协议(NTP)问题

目录

简介

本文档介绍如何在vEdge平台上使用show ntp命令和数据包捕获工具解决网络时间协议(NTP)问题.

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定软件版本或vEdge型号。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

NTP问题的示例症状

NTP同步到vEdge的丢失可能表现为几种不同的方式，例如：

- 设备上的show clock输出中的时间不正确。
- 证书被视为无效，因为有效范围外的时间不正确。
- 日志上的时间戳不正确。

NTP Show命令

要开始隔离NTP问题，您必须了解两个主要命令的用法和输出：

- show ntp associations
- show ntp peer

有关特定命令的详细信息，请参阅SD-WAN命令参考。

显示NTP关联

```
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	本地索引号
关联	关联Id
状态	对等体状态字（十六进制）
会议	配置（持久或短暂）
可达性	可达性（是或否）
AUTH	authentication（ok、yes、bad或none）
条件	选择状态
事件	此对等体的最后一个事件
计数	event count（事件计数）

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
```

索引	本地索引号
远程	NTP服务器地址
REFID	从对等体同步的当前源
ST	层 NTP使用层的概念来描述机器距离权威时间源的距离（在NTP跳数中）。例如，第1层时钟服务器有无线电或原子时钟直接与它连接。它通过NTP将其时间发送到第2层时间服务器，以此类推，一直到第16层。运行NTP的计算机会自动选择具有最低层数的计算机进行通信，并使用NTP作为其时间源。
类型	类型
时间	自从对等设备收到最后一个NTP数据包以来的时间以秒为单位报告。该值必须小于轮询间隔。
投票	轮询间隔（秒）
覆盖范围	reach（按基于前8个连接的八进制值指定） 377(1 1 1 1 1 1 1 1) — 最后8个均正常 376(1 1 1 1 1 1 1 0) — 最后一个连接错误 .... 177(0 1 1 1 1 1 1 1) — 最早的连接是坏的，所有连接都是良好的 等等
延迟	对等体的往返延迟以毫秒为单位。为了更准确地设置时钟，在设置时钟时间时会考虑此延迟。
偏移	偏移（以毫秒为单位） Offset是对等设备之间或主设备和客户端之间的时钟时间差。此值是应用于客户端时钟以便进行同步的更正。正值表示服务器时钟较高。负值表示客户端时钟较高。
抖动	抖动（以毫秒为单位）

使用vManage和数据包捕获工具排除NTP故障

在vManage上使用模拟流验证出口

1. 通过Monitor > Network选择网络设备控制面板
2. 选择适用的vEdge。
3. 单击Troubleshooting选项，然后单击Simulate Flows。
4. 从下拉列表指定源VPN和接口，设置目标IP，并将应用设置为ntp。
5. 单击Simulate。

这会为来自vEdge的NTP流量提供预期的转发行为。

从vEdge收集TCPDump

当NTP流量通过vEdge的控制平面时，可以通过TCPdump捕获该流量。 匹配条件需要使用标准UDP端口123专门过滤NTP流量。

tcpdump vpn 0选项“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
```

添加详细标志-v以从NTP数据包中解码时间戳。

tcpdump vpn 0选项“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 (64
        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
```

从vManage执行Wireshark捕获

如果已从vManage启用数据包捕获，也可以通过这种方式将NTP流量直接捕获到Wireshark可读取的文件。

1. 通过Monitor > Network选择网络设备控制面板
2. 选择适用的vEdge。
3. 单击Troubleshooting选项，然后单击Packet Capture。
4. 从下拉菜单中选择VPN 0和外部接口。
5. 点击流量过滤器。您可以在此处指定目标端口123，如果需要，还可以指定特定目标服务器。

> 注意：按IP地址过滤只捕获一个方向的数据包，因为IP过滤器按源或目标进行过滤。 由于目标第4层端口在两个方向上都是123，因此仅按端口过滤以捕获双向流量。

6. 单击开始。

vManage现在与vEdge通信，以收集数据包捕获5分钟或直到5MB缓冲区满为止（以先到者为准）。完成后，可以下载该捕获以供查看。

常见NTP问题

未收到NTP数据包

数据包捕获显示发送到已配置服务器的出站数据包，但未收到回复。

```
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
```

确认未收到NTP数据包后，您可以：

- 检查NTP是否配置正确。
- 如果流量流经VPN 0中的隧道，请确保在隧道接口下启用allow-service ntp或allow-service all。
- 检查访问列表或中间设备是否阻止了NTP。
- 检查NTP源和目标之间的路由问题。

同步丢失

如果服务器的分散和/或延迟值非常高，则可能会发生同步丢失。 高值表示从服务器/对等设备到达客户端所用的时间太长（参考时钟的根）。 因此，本地计算机无法信任数据包中当前时间的准确性，因为它不知道数据包到达所需的时间。

如果路径中存在导致缓冲的拥塞链路，则数据包在到达NTP客户端时会延迟。

如果遇到同步丢失的情况，您必须检查以下链接：

- 路径中是否存在拥塞/超订用？
- 是否观察到丢弃的数据包？
- 是否涉及加密？

show ntp peer中的到达值可能表示NTP流量丢失。 如果该值小于377，则间歇接收数据包，并且客户端不同步。

设备上的时钟已手动设置

通过clock set命令可以覆盖从NTP获取的时钟值。 发生这种情况时，所有对等体的偏移值都会显着增加。

```
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
```

详细捕获还显示参考时间戳和发起方时间戳不一致。

```
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
```

要强制vEdge恢复将NTP用作其时间源的首选项，请删除、提交、重新添加和重新提交系统ntp下的配置。

参考和相关信息

- 排查和调试NTP问题（Cisco IOS设备）
- Cisco SD-WAN命令参考
- 用 show ntp associations 命令认证 NTP 状态

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。