

Troubleshoot NTP on IM&P

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[NTP on IM&P Explained](#)

[Requirements for NTP Source](#)

[NTP Status Output Explanation](#)

[NTP Troubleshooting](#)

[NTP CLI Diagnostics](#)

[Verify NTP Communication and Version](#)

Introduction

This document describes how to troubleshoot Network Time Protocol (NTP) synchronization on IM and Presence (IM&P).

Prerequisites

Cisco recommends you have a basic understanding of NTP and the IM&P command line interface (CLI) before you review this document.

Requirements

There are no specific hardware or software requirements for this document.

Components Used

The information in this document is based on IM&P.

Note: Much of this information also applies to other unified communications (UC) platforms; however, the focus of this document is IM&P.

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.

NTP on IM&P Explained

The Cisco Unified Communications Manager (CUCM) Publisher is the NTP source for IM&P. IM&P uses the NTP watchdog to keep the time synchronized with the CUCM Publisher. For IM&P

platforms that are on a virtual machine the NTP Watchdog polls the CUCM Publisher once every 64 seconds by default. If the NTP offset is more than three seconds then the NTP daemon restarts itself.

Note: NTP Watchdog monitors how many times the NTP daemon restarted in the last hour. If more than 10 NTP Daemon restarts occur within an hour, further restarts are briefly postponed.

Requirements for NTP Source

Cisco highly recommends the use of a Stratum 1, Stratum 2, or Stratum 3 NTP server as the CUCM Publisher external NTP reference. Any NTP source for the CUCM publisher **MUST NOT** be higher than stratum 4.

The external NTP servers defined for the CUCM Publisher node **MUST** be NTP v4 to avoid potential compatibility, accuracy, and network jitter problems. NTP version 4 is backward compatible with version 3; however, many issues were observed with attempts to use different NTP versions.

Warning: The use of Windows Time Services as an NTP server is not supported. Often Windows Time Services use Simple Network Time Protocol (SNTP) and CUCM cannot successfully synchronize with SNTP.

Note: All the NTP requirements are clearly noted in the Cisco Collaboration System [SRND](#).

NTP Status Output Explanation

To determine the current status of NTP on IM&P execute the **utils ntp status** command from the CLI of the IM&P server.

```
admin:utils ntp status
ntpd (pid 28589) is running...
```

```
remote          refid          st t when poll reach  delay  offset  jitter
=====
10.0.0.1        192.0.2.0      2  u  40   64   1   0.292  0.041  0.000
```

```
synchronised to NTP server (10.0.0.1) at stratum 3 time server re-starting poll server every 64
s Current time in UTC is : Fri Sep 16 19:41:55 UTC 2016 Current time in America/New_York is :
Fri Sep 16 15:41:55 EDT 2016
```

These are descriptions of the columns seen in the NTP status output

- The **remote** column defines the remote peer where time is synchronised. If set to LOCAL then the local hardware clock is in use.
- The **refid** column defines the remote server time source. If set to .LOCL. then local hardware clock on the remote server is referenced. If set to .INIT. then initialization has not yet

succeeded.

- The **st** column denotes the stratum of the remote NTP peer. When a value of 16 is in the stratum column this means the system uses the internal clock instead of the external NTP source. A system which uses its own clock can be caused by an invalid time provider.
- The **t** column indicates the transmission type in use: (l: local; u: unicast; m: multicast, or b: broadcast).
- The **when** column indicates how many seconds have passed since the remote peer was last polled.
- The **poll** column indicates the poll interval in seconds. The default poll value on IM&P is 64 seconds. However this value can be set anywhere between 64 to 1,024 seconds.
- The **reach** column indicates the trend of reachability tests in octal, where each digit, when converted to binary, represents whether a particular poll was successful (binary 1) or unsuccessful (binary 0). For example, "1" means only one poll has been done thus far and it was successful. "3" (= binary 11) means the last two polls were successful. "7" (= binary 111) means the last three polls were successful. "17" (= binary 1 111) means the last four polls were successful. "15" (= binary 1 101) means the last two polls were successful, the poll prior to that was unsuccessful, and the poll prior to that was successful.
- The **delay** column displays the round trip delay to the remote peer. This is determined by measurement of the time from request to response.
- The **offset** column is the estimated deviation between the local servers clock and the remote servers clock.
- The **jitter** column refers to the variability of delay between poll request. A high jitter value limits the server ability to synchronize NTP accurately.

NTP Troubleshooting

NTP CLI Diagnostics

The commands listed in the examples are executed from the CLI of IM&P. These commands provide a simple way to confirm the NTP peer meets Cisco standards.

Tip: All three of these diagnostic modules run, along with several others, when the **utils diagnose test** command is used

The `ntp_reachability` diagnostic module performs a ping test to all configured NTP peers.

```
admin:utils diagnose module ntp_reachability
```

```
Log file: platform/log/diag2.log
```

```
Starting diagnostic test(s)
=====
test - ntp_reachability : Passed

Diagnostics Completed
```

The `ntp_clock_drift` diagnostic module verifies that the NTP peer drift offset does not exceed 15000 milliseconds.

```
admin:utils diagnose module ntp_clock_drift
```

```
Log file: platform/log/diag3.log
```

```
Starting diagnostic test(s)
=====
test - ntp_clock_drift : Passed
```

```
Diagnostics Completed
```

The `ntp_stratum` diagnostic module verifies the NTP stratum value on the IM&P. This test passes successfully if the NTP stratum on the CUCM Publisher is a value of 5 or less because the CUCM publisher is the external NTP source for IM&P.

```
admin:utils diagnose module ntp_stratum
```

```
Log file: platform/log/diag4.log
```

```
Starting diagnostic test(s)
=====
test - ntp_stratum : Passed
```

```
Diagnostics Completed
```

TIP: If the `ntp_stratum` module fails on your system, review the **Requirements for NTP Source** section of this document

Verify NTP Communication and Version

NTP is a Client\Server protocol which communicates over User Datagram Protocol (UDP) on port 123. To verify NTP communication, and NTP version, you need to perform a packet capture (pcap) on the IM&P sever.

TIP: If you see the IM&P send NTP requests in the pcap; however, there are no NTP responses and a network issue is possibly the cause. Simultaneously gather a pcap on the CUCM server and the IM&P server to confirm the requests sent from IM&P are received on the CUCM side. Confirm CUCM is replies to the requests as well.

The packet captures display one NTP Server response for every NTP Client request. The NTP Client\Server messages displays the NTP version in use. Verify both the client request and server response use NTPv4.

Execute the CLI command **utils network capture port 123** to create a packet capture on port

123. This command is the same for IM&P or CUCM.

IM&P CLI

```
admin:utils network capture port 123
```

```
Executing command with options:
```

```
size=128 count=1000 interface=eth0
```

```
src=dest= port=123
```

```
ip=
```

```
09:44:43.106325 IP imppub.lab.local.46476 > cucmpub.lab.local.ntp: NTPv4, Client, length 48
09:44:43.109866 IP cucmpub.lab.local.ntp > imppub.lab.local.46476: NTPv4, Server, length 48
09:44:43.109931 IP imppub.lab.local.46476 > cucmpub.lab.local.ntp: NTPv4, Client, length 48
09:44:43.112815 IP cucmpub.lab.local.ntp > imppub.lab.local.46476: NTPv4, Server, length 48
09:44:43.112895 IP imppub.lab.local.46476 > cucmpub.lab.local.ntp: NTPv4, Client, length 48
09:44:43.113305 IP cucmpub.lab.local.ntp > imppub.lab.local.46476: NTPv4, Server, length 48
09:44:43.113361 IP imppub.lab.local.46476 > cucmpub.lab.local.ntp: NTPv4, Client, length 48
09:44:43.114157 IP cucmpub.lab.local.ntp > imppub.lab.local.46476: NTPv4, Server, length 48
```

CUCM Publisher CLI

```
admin:utils network capture port 123
```

```
Executing command with options:
```

```
size=128 count=1000 interface=eth0
```

```
src=dest= port=123
```

```
ip=
```

```
09:44:43.106744 IP imppub.lab.local.46476 > cucmpub.lab.local.ntp: NTPv4, Client, length 48
09:44:43.106872 IP cucmpub.lab.local.ntp > imppub.lab.local.46476: NTPv4, Server, length 48
09:44:43.109866 IP imppub.lab.local.46476 > cucmpub.lab.local.ntp: NTPv4, Client, length 48
09:44:43.109914 IP cucmpub.lab.local.ntp > imppub.lab.local.46476: NTPv4, Server, length 48
09:44:43.112637 IP imppub.lab.local.46476 > cucmpub.lab.local.ntp: NTPv4, Client, length 48
09:44:43.112719 IP cucmpub.lab.local.ntp > imppub.lab.local.46476: NTPv4, Server, length 48
09:44:43.113532 IP imppub.lab.local.46476 > cucmpub.lab.local.ntp: NTPv4, Client, length 48
09:44:43.113575 IP cucmpub.lab.local.ntp > imppub.lab.local.46476: NTPv4, Server, length 48
```