Verify NTP Status with the Show NTP Associations Command

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Understand the Show NTP Associations Command

- Examples of Reach Field Values
- Differences When Configured as Primary
- What Does a Pound Sign (#) Indicate?

Related Information

Introduction

This document describes how to run the **show ntp associations** command output to determine if NTP works properly.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Conventions

Refer toCisco Technical Tips Conventionsfor more information on document conventions.

Background Information

Network Time Protocol (NTP) synchronizes clocks across network devices so routers, switches, servers, and other systems use a consistent time source. Accurate time is important for log correlation, certificate validation, security event analysis, scheduled operations, and troubleshooting across multiple devices.

NTP uses a hierarchical time model based on stratum levels. A lower stratum value represents a device that is closer to an authoritative time source. For example, a stratum 1 server is directly connected to a primary reference clock, while a stratum 2 device synchronizes to a stratum 1 server. Cisco devices can synchronize to external NTP servers or, if configured, can provide time to other devices.

On Cisco IOS and Cisco IOS XE devices, the show ntp associations command displays information on configured and learned NTP peers. The output includes peer-selection status, reachability, stratum, poll interval, delay, offset, and dispersion information. These fields help determine whether the device can communicate with its NTP peers and whether a peer is selected as the synchronization source.

The reach field helps identify whether recent NTP responses were received from a peer. The offset field shows the calculated time difference between the local device and the NTP peer. The delay and dispersion fields provide additional information about network delay and time accuracy.

Run **show ntp associations** together with **show ntp status** to verify if the local device is synchronized and which peer is used as the synchronization source. The **show ntp status** command provides the overall NTP state of the device, while **show ntp associations** provides per-peer details that help validate or troubleshoot NTP operation.

Understand the Show NTP Associations Command

First, examine the output of the **show ntp associations** command. Then, describe in detail, the information the command presents.

This is an example output and an explanation of certain output fields.

<#root>

```
Router#
```

```
show ntp associations
```

```
address            ref clock         st      when    poll   reach   delay   offset    disp
~172.31.32.2       172.31.32.1       5       29      1024   377     4.2     -8.59     1.6
+~192.168.13.33    192.168.1.111     3       69      128    377     4.1     3.48      2.3
*~192.168.13.57    192.168.1.111     3       32      128    377     7.9     11.18     3.6
* primary (synced), # primary (unsynced), + selected, - candidate, ~ configured
```

The poll field shows the polling interval, in seconds, between NTP packets. On many Cisco IOS platforms, the interval can increase as the association stabilizes, up to the platform default maximum, commonly 1024 seconds. Actual behavior can vary by platform, release, and configuration.

The offset field shows the calculated time difference, in milliseconds, between the local device and the NTP peer. As NTP disciplines the local clock, the offset typically trends closer to zero, but it can fluctuate because of network delay variation and clock stability.

If an asterisk (*) appears next to a peer, that peer is the selected synchronization source. Confirm the overall synchronization state by running the **show ntp status** command.

Examples of Reach Field Values

The reach field is a circular 8-bit reachability buffer displayed in octal format. It records whether the router received responses for the last 8 Network Time Protocol (NTP) poll attempts to a peer.

Each bit represents one poll interval:

- 1 means the router received a response from the NTP peer.
- 0 means the router did not receive a response from the NTP peer.

A reach value of 377 means the router received responses for the last 8 NTP polls. In binary, octal 377 represents 11111111. Lower values indicate one or more recent NTP responses were missed. For example, if one response is lost, the reach value changes as the missed response moves through the circular buffer across subsequent poll intervals.

A stable NTP association commonly shows a reach value of 377. However, a value other than 377 does not always mean that NTP is failing. Lower values can appear during initial convergence, after a reload, after a peer is newly configured, or when there is intermittent packet loss. Use the reach field together with other fields, such as when, poll, delay, offset, and disp, and confirm the overall synchronization state with the **show ntp status** command.

In general:

- 377 means the last 8 NTP responses were received.
- A non-zero value lower than 377 means some responses were received, however, one or more recent responses were missed.
- 0 means no responses were received during the last 8 NTP poll attempts. In this case, check IP reachability, routing, access control lists, firewalls, User Datagram Protocol (UDP) port 123, NTP authentication, and the NTP server status.

This table provides explanations for possible reach field values with the loss of an NTP response packet, starting from 377, one NTP response is lost, and all subsequent NTP responses are received:



Note: This table assumes the reach value starts at 377, one NTP response is missed, and all subsequent responses are received. The missed response is represented by a 0 bit, which shifts left with each subsequent successful poll until it ages out of the 8-bit reachability buffer.

Reach Field Value (Reported/Binary)	Explanation
377 = 1 1 1 1 1 1 1 1	Time 0: Last eight responses from server were received.
376 = 1 1 1 1 1 1 1 0	Time 1: Last NTP response was NOT received (lost in network).
375 = 1 1 1 1 1 1 0 1	Time 2: Last NTP response was received; missed response shifts left.
373 = 1 1 1 1 1 0 1 1	Time 3: Last NTP response was received; missed response continues to age.
367 = 1 1 1 1 0 1 1 1	Time 4: Last NTP response was received; missed response continues to age.
357 = 1 1 1 0 1 1 1 1	Time 5: Last NTP response was received; missed response continues to age.
337 = 1 1 0 1 1 1 1 1	Time 6: Last NTP response was received; missed response continues to age.
277 = 1 0 1 1 1 1 1 1	Time 7: Last NTP response was received; missed response continues to age.
177 = 0 1 1 1 1 1 1 1	Time 8: Last NTP response was received; missed response is now the oldest tracked result

377 = 1 1 1 1 1 1 1 1	Time 9: Last NTP response was received; missed response aged out; last eight responses were received

---

The logic can be explained as:

- The reach value is shown in octal.
- It represents the last 8 NTP poll results.
- A bit value of 1 means a response was received.
- A bit value of 0 means a response was missed.
- The rightmost bit represents the most recent poll result.
- As new polls occur, the previous results shift left.
- After eight successful polls, the missed response ages out and the value returns to 377.

Each new NTP poll shifts the previous reach value left by one bit, drops the oldest result, and adds the latest result on the right as 1 for a received response or 0 for a lost response.

For example, if another response is lost after the reach value is 375, the next reach value is 372. This is because the previous results shift left, and the newest lost response is added as 0 on the right.

Differences When Configured as Primary

When a router is configured to use its local clock as an NTP source with the **ntp master** command, the **show ntp associations** output can show the local clock association. For example:

```
<#root>

address             ref clock      st    when   poll   reach   delay    offset    disp

*~127.127.7.1       127.127.7.1    6     20     64     377     0.0      0.00      0.0

* primary (synced), # primary (unsynced), + selected, - candidate, ~ configured
```

In this output, 127.127.7.1 represents the router local clock. The asterisk (*) indicates the local clock is selected as the synchronization source, and the tilde (~) indicates the the association is configured.

The stratum value shown in the output can be one less than the value configured with the **ntp master** command. For example, if the router is configured with **ntp master 7**, the local clock association can appear with stratum 6 in the **show ntp associations** output.

Since the router is polling its own internal clock, the local clock association is not unreachable in the same

way that a remote NTP peer can become unreachable. In this mode, the poll interval commonly remains at 64 seconds instead of increasing to a longer interval, such as 1024 seconds.

Platform and software behavior can vary, by running the **show ntp status** with **show ntp associations** to confirm the synchronization state and the selected clock source.

What Does a Pound Sign (#) Indicate?

A pound sign (#) displayed next to a configured peer in the **show ntp associations** command output indicates the peer is selected as the primary synchronization candidate, but the router is not synchronized to that peer.

In this condition, NTP request and response packets can still be exchanged between the router and the peer, but the clocks do not synchronize successfully.

To investigate why the router is not synchronized, run these commands:

- **show ntp associations detail**
- **show ntp status**

The **show ntp associations** detail command provides additional information on the peer association; including reachability, synchronization state, validity, and possible rejection reasons. The show ntp status command shows the overall NTP state of the router, including whether the router is synchronized, the selected reference clock, and the local stratum.

If more detailed troubleshooting is required, run NTP debug commands carefully, especially on production devices. One possible reason for the pound sign (#) is the NTP client clock differs from the NTP server clock by more than 4000 seconds. On Cisco routers, a time difference greater than 4000 seconds can be considered out of range and can prevent the router from synchronizing to the server.

This behavior does not apply when an NTP peer is configured first on a Cisco router or immediately after a reload. In those cases, the NTP client, which is the Cisco router, can update its clock to match the NTP server clock even when the time difference is larger than 4000 seconds.

NTP uses Coordinated Universal Time (UTC), also referred to as Greenwich Mean Time (GMT), in protocol messages. The configured local time zone affects only how the time is displayed on the router. If the displayed local time appears incorrect, verify the time zone configuration on the client router.

If the client clock is too far from the NTP server clock and synchronization does not occur, manually set the client clock to within a few minutes of the NTP server clock, then verify NTP synchronization again by

running **show ntp status** and **show ntp associations** commands.

Related Information

- Network Time Protocol (NTP) Issues Troubleshooting and Debugging Guide
- Technical Support & Documentation - Cisco Systems