



Junos[®] OS

Time Management Administration Guide for Routing Devices



Modified: 2018-04-17

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos® OS Time Management Administration Guide for Routing Devices
Copyright © 2018 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

| | | |
|------------------|--|-----------|
| | About the Documentation | xi |
| | Documentation and Release Notes | xi |
| | Supported Platforms | xi |
| | Using the Examples in This Manual | xii |
| | Merging a Full Example | xii |
| | Merging a Snippet | xiii |
| | Documentation Conventions | xiii |
| | Documentation Feedback | xv |
| | Requesting Technical Support | xvi |
| | Self-Help Online Tools and Resources | xvi |
| | Opening a Case with JTAC | xvi |
| Chapter 1 | Configuring Date and Time | 19 |
| | Setting the Date and Time Locally | 19 |
| | NTP Overview | 20 |
| | Understanding NTP Time Servers | 22 |
| | Synchronizing and Coordinating Time Distribution Using NTP | 23 |
| | Configuring NTP | 23 |
| | Configuring the NTP Boot Server | 24 |
| | Specifying a Source Address for an NTP Server | 24 |
| | Configuring NTP | 26 |
| | Configuring the NTP Time Server and Time Services | 27 |
| | Configuring the Router or Switch to Operate in Client Mode | 28 |
| | Configuring the Router or Switch to Operate in Symmetric Active Mode | 29 |
| | Configuring the Router or Switch to Operate in Broadcast Mode | 29 |
| | Configuring the Router or Switch to Operate in Server Mode | 29 |
| | Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization | 30 |
| | Configuring NTP Authentication Keys | 31 |
| | Configuring the Router or Switch to Listen for Broadcast Messages Using NTP | 32 |
| | Configuring the Router or Switch to Listen for Multicast Messages Using NTP | 32 |
| Chapter 2 | Configuring Time Zones | 35 |
| | Modifying the Default Time Zone for a Router or Switch Running Junos OS | 35 |
| | Updating the IANA Time Zone Database on Junos OS Devices | 36 |
| | Importing and Installing Time Zone Files | 36 |
| | Configuring a Custom Time Zone | 37 |

| | | |
|------------------|--|-----------|
| Chapter 3 | Configuring Network Time Protocols | 39 |
| | Understanding NTP Time Servers | 39 |
| | Configuring NTP Authentication Keys | 40 |
| | Configuring NTP Authentication Keys (QFabric System) | 41 |
| | Configuring the NTP Time Server and Time Services | 42 |
| | Configuring the Switch to Operate in Client Mode | 42 |
| | Configuring the Router or Switch to Operate in Symmetric Active Mode | 43 |
| | Configuring the Router or Switch to Operate in Broadcast Mode | 43 |
| | Configuring the Router or Switch to Operate in Server Mode | 43 |
| | Configuring the NTP Time Server and Time Services (QFabric System) | 45 |
| | Configuring the Switch to Listen for Broadcast Messages Using NTP | 46 |
| | Configuring the Switch to Listen for Multicast Messages Using NTP | 46 |
| | Setting the Date and Time | 47 |
| | Synchronizing and Coordinating Time Distribution Using NTP | 47 |
| | Configuring NTP | 47 |
| | Configuring the NTP Boot Server | 48 |
| | Specifying a Source Address for an NTP Server | 48 |
| | Example: Configuring NTP | 49 |
| | Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization | 52 |
| Chapter 4 | Configuring Precision Time Protocols | 55 |
| | Understanding Transparent Clocks in Precision Time Protocol | 56 |
| | IEEE 1588v2 PTP Boundary Clock Overview | 58 |
| | IEEE 1588v2 PTP Boundary Clock | 58 |
| | Clock Clients | 60 |
| | IEEE 1588v2 Precision Timing Protocol (PTP) | 61 |
| | Understanding the PTP G.8275.2 Enhanced Profile (Telecom Profile) | 63 |
| | Understanding the Precision Time Protocol Enterprise Profile | 65 |
| | Configuring Transparent Clock Mode for Precision Time Protocol | 68 |
| | Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) | 68 |
| | Configuring Precision Time Protocol and Its Options | 68 |
| | Configuring PTP Options | 69 |
| | Configuring Slave Clock Options | 70 |
| | Configuring Master Clock Options | 71 |
| | Configuring Precision Time Protocol Default Profile | 71 |
| | Configuring Precision Time Protocol and its Options | 72 |
| | Configuring PTP Options | 72 |
| | Configuring Slave Clock Options | 73 |
| | Configuring Master Clock Options | 74 |
| | Configuring the Precision Time Protocol Enterprise Profile | 75 |
| | Configuring Precision Time Protocol and its Options | 75 |
| | Configuring PTP Options | 75 |
| | Configuring Slave Clock Options | 76 |
| | Configuring Master Clock Options | 77 |
| | Configuring Precision Time Protocol Clocking | 78 |

| | | |
|------------------|--|------------|
| | Configuring a PTP Master Boundary Clock | 80 |
| | Configuring the PTP Master Boundary Clock Parameters | 80 |
| | Configuring a PTP Master Boundary Clock Interface | 82 |
| | Example: Configuring a PTP Boundary Clock | 83 |
| | Example: Configuring a PTP Boundary Clock With Unicast Negotiation | 86 |
| | Configuring a PTP Slave Clock | 90 |
| | Configuring the PTP Slave Clock Parameters | 90 |
| | Configuring the PTP Slave Clock Interface | 92 |
| | Example: Configuring an Ordinary Slave Clock With Unicast-Negotiation | 93 |
| | Example: Configuring an Ordinary Slave Clock Without Unicast-Negotiation | 96 |
| Chapter 5 | Configuration Statements | 99 |
| | System Management Configuration Statements | 100 |
| | asymmetry | 107 |
| | authentication-key | 108 |
| | authentication-key | 109 |
| | boot-server (NTP) | 110 |
| | boot-server (NTP) | 111 |
| | broadcast | 112 |
| | broadcast | 113 |
| | broadcast-client | 114 |
| | broadcast-client | 114 |
| | clock-client | 115 |
| | clock-mode | 116 |
| | clock-source (PTP Unicast Slave Interface) | 117 |
| | e2e-transparent | 118 |
| | interface (PTP Slave) | 119 |
| | local-priority | 120 |
| | local-ip-address (multicast or unicast mode) | 121 |
| | master | 122 |
| | multicast-client | 123 |
| | multicast-mode (PTP Master and Slave Interfaces) | 124 |
| | ntp | 125 |
| | ntp (QFabric) | 126 |
| | peer (NTP) | 127 |
| | profile-type | 128 |
| | server (NTP) | 130 |
| | slave | 131 |
| | source-address (NTP, RADIUS, System Logging, or TACACS+) | 133 |
| | source-address (NTP, RADIUS, System Logging, or TACACS+) | 134 |
| | system | 135 |
| | time-zone | 136 |
| | transport ipv4 (PTP Unicast Master and Slave Interface) | 138 |
| | trusted-key | 139 |
| | unicast-mode (PTP Slave Interface) | 140 |
| | use-imported-time-zones | 140 |
| Chapter 6 | Operational Commands | 141 |
| | set date | 142 |
| | show ntp associations | 143 |

| | |
|-----------------------------------|-----|
| show ntp status | 145 |
| show ptp clock | 148 |
| show ptp global-information | 151 |
| show ptp master | 154 |
| show ptp slave | 157 |
| show ptp lock-status | 160 |
| show ptp statistics | 163 |

List of Figures

| | | |
|-----------|--|----|
| Chapter 4 | Configuring Precision Time Protocols | 55 |
| | Figure 1: Boundary Clocks in a Network | 59 |

List of Tables

| | | |
|------------------|--|------------|
| | About the Documentation | xi |
| | Table 1: Notice Icons | xiv |
| | Table 2: Text and Syntax Conventions | xiv |
| Chapter 4 | Configuring Precision Time Protocols | 55 |
| | Table 3: Announce, Sync, and Delay Request/ Response Rate Parameters | 64 |
| Chapter 6 | Operational Commands | 141 |
| | Table 4: show ntp associations Output Fields | 143 |
| | Table 5: show ntp status Output Fields | 145 |
| | Table 6: show ptp clock Output Fields | 148 |
| | Table 7: show ptp global-information Output Fields | 151 |
| | Table 8: show ptp master Output Fields | 154 |
| | Table 9: show ptp slave Output Fields | 157 |
| | Table 10: show ptp lock-status Output Fields | 160 |
| | Table 11: show ptp statistics Output Fields | 163 |

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Using the Examples in This Manual on page xii
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xvi

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- M Series
- MX Series
- T Series
- EX Series
- PTX Series
- QFX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {  
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]  
user@host# edit system scripts  
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]  
user@host# load merge relative /var/tmp/ex-script-snippet.conf  
load complete
```

For more information about the **load** command, see [CLI Explorer](#).

Documentation Conventions

[Table 1 on page xiv](#) defines notice icons used in this guide.

Table 1: Notice Icons

| Icon | Meaning | Description |
|--|--------------------|---|
|  | Informational note | Indicates important features or instructions. |
|  | Caution | Indicates a situation that might result in loss of data or hardware damage. |
|  | Warning | Alerts you to the risk of personal injury or death. |
|  | Laser warning | Alerts you to the risk of personal injury from a laser. |
|  | Tip | Indicates helpful information. |
|  | Best practice | Alerts you to a recommended use or implementation. |

Table 2 on page xiv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

| Convention | Description | Examples |
|------------------------------|---|--|
| Bold text like this | Represents text that you type. | To enter configuration mode, type the configure command: user@host> configure |
| Fixed-width text like this | Represents output that appears on the terminal screen. | user@host> show chassis alarms No alarms currently active |
| <i>Italic text like this</i> | <ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. | <ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i> |
| <i>Italic text like this</i> | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i> |

Table 2: Text and Syntax Conventions (continued)

| Convention | Description | Examples |
|--------------------------------|--|---|
| Text like this | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | <ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE. |
| < > (angle brackets) | Encloses optional keywords or variables. | stub <default-metric <i>metric</i>>; |
| (pipe symbol) | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>) |
| # (pound sign) | Indicates a comment specified on the same line as the configuration statement to which it applies. | rsvp { # Required for dynamic MPLS only |
| [] (square brackets) | Encloses a variable for which you can substitute one or more values. | community name members [<i>community-ids</i>] |
| Indentation and braces ({ }) | Identifies a level in the configuration hierarchy. | [edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } } |
| ;(semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |
| GUI Conventions | | |
| Bold text like this | Represents graphical user interface (GUI) items you click or select. | <ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel. |
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections. | In the configuration editor hierarchy, select Protocols>Ospf . |

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <https://www.juniper.net/documentation/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/documentation/feedback/>.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <https://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://www.juniper.net/support/requesting-support.html>.

CHAPTER 1

Configuring Date and Time

- [Setting the Date and Time Locally on page 19](#)
- [NTP Overview on page 20](#)
- [Understanding NTP Time Servers on page 22](#)
- [Synchronizing and Coordinating Time Distribution Using NTP on page 23](#)
- [Configuring NTP on page 26](#)
- [Configuring the NTP Time Server and Time Services on page 27](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)
- [Configuring NTP Authentication Keys on page 31](#)
- [Configuring the Router or Switch to Listen for Broadcast Messages Using NTP on page 32](#)
- [Configuring the Router or Switch to Listen for Multicast Messages Using NTP on page 32](#)

Setting the Date and Time Locally

You can set the date and time on a device running Junos OS by using the **set date** operational mode command:

To enter the date and time locally:

1. From operational mode, manually set the date and time.

Because this is an operational-mode command, there is no need to perform a commit operation.

```
user@host> set date YYYYMMDDhhmm.ss
```

For example:

```
user@host> set date 201307251632
Thu Jul 25 16:32:00 PDT 2013
```

2. Verify the time.

The **show system uptime** command provides the following information: current time, last boot time, protocols start time, last configuration commit time.

```

user@host> show system uptime
Current time: 2013-07-25 16:33:38 PDT
System booted: 2013-07-11 17:14:25 PDT (1w6d 23:19 ago)
Protocols started: 2013-07-11 17:16:35 PDT (1w6d 23:17 ago)
Last configured: 2013-07-23 12:32:42 PDT (2d 04:00 ago) by user
4:33PM up 13 days, 23:19, 1 user, load averages: 0.00, 0.01, 0.00

```

Starting in Junos OS 13.3, you can use the **set date** command from operational mode to instruct the device to retrieve the date and time from a configured NTP server. For example:

- From operational mode, issue the **set date** command and specify **ntp** to retrieve the date and time from a configured NTP server, or specify **ntp ntp-server** to retrieve the date and time from the given NTP server.

```
user@host> set date ntp ntp-server
```

For example:

```

user@host> set date ntp
25 Jun 16:38:28 ntpdate[2314]: step time server 192.0.2.1 offset -0.004182 sec

```

Release History Table

| Release | Description |
|---------|---|
| 13.3 | Starting in Junos OS 13.3, you can use the set date command from operational mode to instruct the device to retrieve the date and time from a configured NTP server. |

Related Documentation

- Time Management Administration Guide for Routing Devices*
- [set date on page 142](#)

NTP Overview

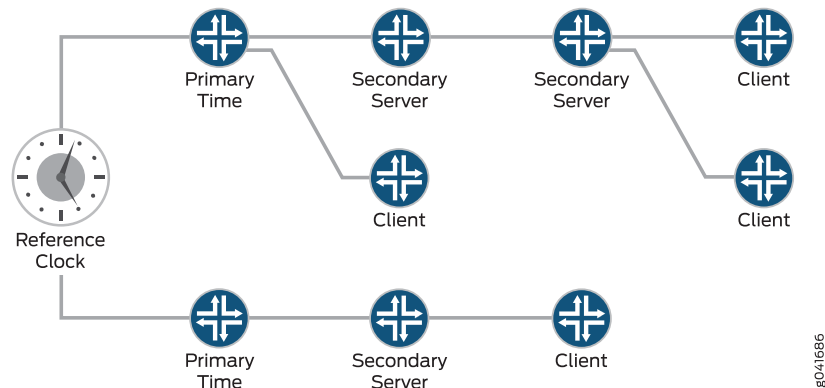
Network Time Protocol (NTP) is a widely used protocol used to synchronize the clocks of routers and other hardware devices on the Internet. Primary NTP servers are synchronized to a reference clock directly traceable to Coordinated Universal Time (UTC). Reference clocks include GPS receivers and telephone modem services, NTP accuracy expectations depend on the environment application requirements, however, NTP can generally maintain time to within tens of milliseconds over the public internet.

NTP is defined in the RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification

Devices running Junos OS can be configured to act as an NTP client, a secondary NTP server, or a primary NTP server. These variations are as follows:

- Primary NTP Server**—Primary NTP servers are synchronized to a reference clock that is directly traceable to UTC. These servers then re-distribute this time data downstream to other Secondary NTP servers or NTP clients.

- **Secondary NTP Server**—Secondary NTP servers are synchronized to a primary or secondary NTP server. These servers then re-distribute this data downstream to other Secondary NTP servers or NTP clients.
- **NTP Client**—NTP clients are synchronized to a primary or secondary NTP server. Clients do not re-distribute this time data to other devices.



NOTE: The NTP subnet includes a number of widely accessible public primary time servers that can be used as a network's primary NTP server. Juniper Networks strongly recommends that you authenticate any primary servers you use.

Each device on your network can be configured to run in one or more of the following NTP modes:

- **Broadcast Mode**—One or more devices is set up to transmit time information to a specified broadcast or multicast address. Other devices listen for time sync packets on these addresses. This mode is less accurate than the client/server mode.
- **Client/Server Mode**—Devices are organized hierarchically across the network in client/server relationships.
- **Symmetric Active (peer) Mode**—Two or more devices are configured as NTP server peers to provide redundancy.

By default, if an NTP client time drifts so that the difference in time from the NTP server exceeds 128 milliseconds, the NTP client is automatically stepped back into synchronization. The NTP client will still synchronize with the server even if the offset between the NTP client and server exceeds the 1000-second threshold. You can manually request that a device synchronize with an NTP server by using the **set date ntp** operational command on the router. On devices running Junos OS that have dual Routing Engines, the backup Routing Engine synchronizes directly with the master Routing Engine.

For more details about the Network Time Protocol, go to the Network Time Foundation website at <http://www.ntp.org>.



NOTE: All Juniper platforms that run Junos OS support the leap second adjustment. By default, if the NTP server is aware of the leap second calculations, then the Junos device will automatically add the 1 second delay. PTP (Precision Time Protocol) is used to detect and propagate leap second synchronization changes throughout all nodes in a network.



NOTE: NTP is required for Common Criteria compliance. For more information on the Common Criteria certification, see [Public Sector Certifications](#).

In Junos operating system (Junos OS) Release 11.2 or later, NTP supports IPv4 VPN routing and forwarding (VRF) requests. This enables an NTP server running on a provider edge (PE) router to respond to NTP requests from a customer edge (CE) router. As a result, a PE router can process any NTP request packet coming from different routing instances. In Junos OS Release 11.4 and later, NTP also supports IPv6 VRF requests.

**Related
Documentation**

- [Synchronizing and Coordinating Time Distribution Using NTP on page 23](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Understanding NTP Time Servers

The IETF defined the Network Time Protocol (NTP) to synchronize the clocks of computer systems connected to each other over a network. Most large networks have an NTP server that ensures that time on all devices is synchronized, regardless of the device location. If you use one or more NTP servers on your network, ensure you include the NTS server addresses in your Junos OS configuration.

When configuring the NTP, you can specify which system on the network is the authoritative time source, or time server, and how time is synchronized between systems on the network. To do this, you configure the router, switch, or security device to operate in one of the following modes:

- Client mode—In this mode, the local router or switch can be synchronized with the remote system, but the remote system can never be synchronized with the local router or switch.
- Symmetric active mode—In this mode, the local router or switch and the remote system can synchronize with each other. You use this mode in a network in which either the local router or switch or the remote system might be a better source of time.



NOTE: Symmetric active mode can be initiated by either the local or the remote system. Only one system needs to be configured to do so. This means that the local system can synchronize with any system that offers symmetric active mode without any configuration whatsoever. However, we strongly encourage you to configure authentication to ensure that the local system synchronizes only with known time servers.

- Broadcast mode—In this mode, the local router or switch sends periodic broadcast messages to a client population at the specified broadcast or multicast address. Normally, you include this statement only when the local router or switch is operating as a transmitter.
- Server mode—In this mode, the local router or switch operates as an NTP server.



NOTE: In NTP server mode, the Junos OS supports authentication as follows:

- If the NTP request from the client comes with an authentication key (such as a key ID and message digest sent with the packet), the request is processed and answered based on the authentication key match.
- If the NTP request from the client comes without any authentication key, the request is processed and answered without authentication.

Related Documentation

- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Synchronizing and Coordinating Time Distribution Using NTP

Using NTP to synchronize and coordinate time distribution in a large network involves these tasks:

1. [Configuring NTP on page 23](#)
2. [Configuring the NTP Boot Server on page 24](#)
3. [Specifying a Source Address for an NTP Server on page 24](#)

Configuring NTP

To configure NTP on the router or switch, include the **ntp** statement at the **[edit system]** hierarchy level:

```
[edit system]
ntp {
  authentication-key number type type value password;
  boot-server (address | hostname);
  broadcast <address> <key key-number> <routing-instance-name routing-instance-name>
    <tll value> <version value> ;
```

```

broadcast-client;
multicast-client <address>;
peer address <key key-number> <version value> <prefer>;
server address <key key-number> <version value> <prefer>;
source-address <source-address> <routing-instance routing-instance-name>;
trusted-key [ key-numbers ];
}

```

Configuring the NTP Boot Server

When you boot the router or switch, it issues an **ntpdate** request, which polls a network server to determine the local date and time. You need to configure a server that the router or switch uses to determine the time when the router or switch boots. If you configure an NTP boot server, then when the router or switch boots, it immediately synchronizes with the boot server even if the NTP process is explicitly disabled or if the time difference between the client and the boot server exceeds the threshold value of 1000 seconds.

To configure the NTP boot server, include the **boot-server** statement at the **[edit system ntp]** hierarchy level:

```

[edit system ntp]
boot-server (address | hostname);

```

Specify the address of the network server. You must specify an IP address or a hostname.

Specifying a Source Address for an NTP Server

For IP version 4 (IPv4), you can specify that if the NTP server configured at the **[edit system ntp]** hierarchy level is contacted on one of the loopback interface addresses, the reply always uses a specific source address. This is useful for controlling which source address NTP will use to access your network when it is either responding to an NTP client request from your network or when it itself is sending NTP requests to your network.



NOTE: The configuration of the source IP address in a routing instance by using the **source-address** statement at the **[edit system ntp source-address source-address]** hierarchy level is supported only for an NTP server. It is not supported for an NTP client

To configure the specific source address that the reply will always use, and the source address that requests initiated by NTP server will use, include the **source-address** statement at the **[edit system ntp]** hierarchy level:

```

[edit system ntp]
source-address source-address;

```

source-address is a valid IP address configured on one of the router or switch interfaces.

Starting in Junos OS 13.3, you can also configure the source address using the **routing-instance** statement at the **[edit system ntp source-address source-address]** hierarchy level:

```


[edit system ntp source-address source-address]
user@host# set routing-instance routing-instance-name


```


For example, the following statement is configured:

```
[edit system ntp source-address source-address]
user@host# set system ntp source-address 12.12.12.12 routing-instance ntp-source-test
```

As a result, while sending NTP message through any interface in the *ntp-source-test* routing instance, the source address 12.12.12.12 is used.

 **NOTE:** The *routing-instance* statement is optional and if not configured, the primary address of the interface will be used.

 **NOTE:** If a firewall filter is applied on the loopback interface, ensure that the *source-address* specified for the NTP server at the *[edit system ntp]* hierarchy level is explicitly included as one of the match criteria in the firewall filter. This enables the Junos OS to accept traffic on the loopback interface from the specified source address.

The following example shows a firewall filter with the source address 10.0.10.100 specified in the *from* statement included at the *[edit firewall filter firewall-filter-name]* hierarchy:

```
[edit firewall filter Loopback-Interface-Firewall-Filter]
term Allow-NTP {
  from {
    source-address {
      172.17.27.46/32; // IP address of the NTP server
      10.0.10.100/32; // Source address specified for the NTP server
    }
  }
  then accept;
}
```

If no *source-address* is configured for the NTP server, include the primary address of the loopback interface in the firewall filter.

Release History Table

| Release | Description |
|---------|---|
| 13.3 | Starting in Junos OS 13.3, you can also configure the source address using the routing-instance statement at the [edit system ntp source-address source-address] hierarchy level: |

Related Documentation

- [NTP Overview on page 20](#)
- [Understanding NTP Time Servers on page 22](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Configuring NTP

The Network Time Protocol (NTP) provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse network. Debugging and troubleshooting are much easier when the timestamps in the log files of all the routers or switches are synchronized, because events that span the network can be correlated with synchronous entries in multiple logs. We recommend using the Network Time Protocol (NTP) to synchronize the system clocks of routers, switches, and other network equipment.

To configure NTP:

1. Configure Junos OS to retrieve the time when it first boots up.

Use the **boot-server** statement with the IP address of your NTP server. If DNS is configured, you can use a domain name instead of an IP address.

```
[edit system ntp]
user@host# set boot-server (name | ip-address)
```

For example, set an IP address of 172.16.1.1 for your NTP server.

```
[edit system ntp]
user@host# set boot-server 172.16.1.1
```

For example, set a domain name. In this example, the domain name is provided by pool.ntp.org.

```
[edit system ntp]
user@host# set boot-server 0.north-america.pool.ntp.org
```

2. (Optional) Configure one or more reference NTP servers to keep the device synchronized with periodic updates.

It is a good practice to do this, as the Junos OS device can remain up for a long time, and therefore the clock can drift.

```
[edit system ntp]
user@host# set server (name | ip-address)
```

For example, set an IP address of 172.16.1.1 for your NTP server.

```
[edit system ntp]
user@host# set server 172.16.1.1
```

For example, set a domain name provided by pool.ntp.org.

```
[edit system ntp]
user@host# set server 0.north-america.pool.ntp.org
```

3. (Optional) Set the local time zone to match the device's location.

Universal Coordinated Time (UTC) is the default. Many administrators prefer to keep all their devices configured to use the UTC time zone. This approach has the benefit of allowing you to easily compare the time stamps of logs and other events across a network of devices in many different time zones.

On the other hand, setting the time zone allows Junos OS to present the time in the correct local format.

```
[edit system ntp]
user@host# set time-zone time-zone
```

For example:

```
[edit system ntp]
user@host# set time-zone America/Los_Angeles
```

4. Verify the configuration.

Check the system uptime. This command provides the current time, when the device was last booted, when the protocols started, and when the device was last configured.

```
user@host> show system uptime
Current time: 2013-07-25 16:33:38 PDT
System booted: 2013-07-11 17:14:25 PDT (1w6d 23:19 ago)
Protocols started: 2013-07-11 17:16:35 PDT (1w6d 23:17 ago)
Last configured: 2013-07-23 12:32:42 PDT (2d 04:00 ago) by user
4:33PM up 13 days, 23:19, 1 user, load averages: 0.00, 0.01, 0.00
```

Check the NTP server status and associations of the clocking sources used by your device.

```
user@host> show ntp associations
```

| remote | refid | st | t | when | poll | reach | delay | offset | jitter |
|-----------------------|-------|----|---|------|------|-------|-------|--------|---------|
| tux.brhewig.co .INIT. | | 16 | - | - | 512 | 0 | 0.000 | 0.000 | 4000.00 |

```
user@host > show ntp status
status=c011 sync_alarm, sync_unspec, 1 event, event_restart,
version="ntpd 4.2.0-a Thu May 30 19:14:15 UTC 2013 (1)",
processor="i386", system="JUNOS13.2-20130530_ib_13_3_psd.1", leap=11,
stratum=16, precision=-18, rootdelay=0.000, rootdispersion=5.130,
peer=0, refid=INIT,
reftime=00000000.00000000 Wed, Feb 6 2036 22:28:16.000, poll=4,
clock=d59d4f2e.1793bce9 Fri, Jul 26 2013 12:40:30.092, state=1,
offset=0.000, frequency=62.303, jitter=0.004, stability=0.000
```

- Related Documentation**
- [Understanding NTP Time Servers on page 22](#)
 - *Time Management Administration Guide for Routing Devices*

Configuring the NTP Time Server and Time Services

When you use NTP, configure the router or switch to operate in one of the following modes:

- Client mode
- Symmetric active mode

- Broadcast mode
- Server mode

The following topics describe how to configure these modes of operation:

1. [Configuring the Router or Switch to Operate in Client Mode on page 28](#)
2. [Configuring the Router or Switch to Operate in Symmetric Active Mode on page 29](#)
3. [Configuring the Router or Switch to Operate in Broadcast Mode on page 29](#)
4. [Configuring the Router or Switch to Operate in Server Mode on page 29](#)

Configuring the Router or Switch to Operate in Client Mode

To configure the local router or switch to operate in client mode, include the **server** statement and other optional statements at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
server address <key key-number> <version value> <routing-instance routing-instance>
  <prefer>;
authentication-key key-number type type value password;
boot-server address;
trusted-key [ key-numbers ];
```

Specify the address of the system acting as the time server. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the time server, include the **key** option. The key corresponds to the key number you specify in the **authentication-key** statement, as described in [“Configuring NTP Authentication Keys” on page 31](#).

By default, the router or switch sends NTP version 4 packets to the time server. To set the NTP version level to 1, 2, or 3, include the **version** option.

If you configure more than one time server, you can mark one server preferred by including the **prefer** option.

For information about how to configure trusted keys, see [“Configuring NTP Authentication Keys” on page 31](#). For information about how to configure an NTP boot server, see [“Configuring the NTP Boot Server” on page 24](#). For information about how to configure the router or switch to operate in server mode, see [“Configuring the Router or Switch to Operate in Server Mode” on page 29](#).

The following example shows how to configure the router or switch to operate in client mode:

```
[edit system ntp]
authentication-key 1 type md5 value "$9$EgfcvX7VY4ZEcwgoHjkP5Q3CuREyv87";
boot-server 10.1.1.1;
server 10.1.1.1 key 1 prefer;
trusted-key 1;
```

Configuring the Router or Switch to Operate in Symmetric Active Mode

To configure the local router or switch to operate in symmetric active mode, include the **peer** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
peer address <key key-number> <version value> <prefer>;
```

Specify the address of the remote system. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the remote system, include the **key** option. The key corresponds to the key number you specify in the **authentication-key** statement, as described in [“Configuring NTP Authentication Keys” on page 31](#).

By default, the router or switch sends NTP version 4 packets to the remote system. To set the NTP version level to 1, 2 or 3, include the **version** option.

If you configure more than one remote system, you can mark one system preferred by including the **prefer** option:

```
peer address <key key-number> <version value> prefer;
```

Configuring the Router or Switch to Operate in Broadcast Mode

To configure the local router or switch to operate in broadcast mode, include the **broadcast** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
broadcast address <key key-number> <version value> <ttl value>;
```

Specify the broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be **224.0.1.1**.

To include an authentication key in all messages sent to the remote system, include the **key** option. The key corresponds to the key number you specify in the **authentication-key** statement, as described in [“Configuring NTP Authentication Keys” on page 31](#).

By default, the router or switch sends NTP version 4 packets to the remote system. To set the NTP version level to 1, 2, or 3, include the **version** option.

Configuring the Router or Switch to Operate in Server Mode

In server mode, the router or switch acts as an NTP server for clients when the clients are configured appropriately. The only prerequisite for “server mode” is that the router or switch must be receiving time from another NTP peer or server. No other configuration is necessary on the router or switch.

To configure the local router or switch to operate as an NTP server, include the following statements at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
authentication-key key-number type type value password;
```

```
server address <key key-number> <version value> <routing-instance routing-instance>  
<prefer>;  
trusted-key [ key-numbers ];
```

Specify the address of the system acting as the time server. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the time server, include the **key** option. The key corresponds to the key number you specify in the **authentication-key** statement, as described in [“Configuring NTP Authentication Keys” on page 31](#).

By default, the router or switch sends NTP version 4 packets to the time server. To set the NTP version level to 1, 2, or 3, include the **version** option.

If you configure more than one time server, you can mark one server preferred by including the **prefer** option.

For information about how to configure trusted keys, see [“Configuring NTP Authentication Keys” on page 31](#). For information about how to configure the router or switch to operate in client mode, see [“Configuring the Router or Switch to Operate in Client Mode” on page 28](#).

The following example shows how to configure the router or switch to operate in server mode:

```
[edit system ntp]  
authentication-key 1 type md5 value "$9$tXERuBEreWx-wtuLNdboaUjH.T3AtOESe";  
server 172.17.27.46 prefer;  
trusted-key 1;
```



NOTE: When a host is added as an NTP server, it resolves to an IP address prior to being added to the configuration. When using a public NTP server, the host might resolve to different IP addresses.

If the resolved IP address becomes unreachable for any reason, the switch cannot access the NTP server. In order to leverage public NTP pool entities, this functionality has been modified so that a host is accepted as a string without DNS resolution.

**Related
Documentation**

- [Understanding NTP Time Servers on page 22](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization

Debugging and troubleshooting are much easier when the timestamps in the log files of all the routers or switches are synchronized, because events that span the network can be correlated with synchronous entries in multiple logs. We strongly recommend using

the Network Time Protocol (NTP) to synchronize the system clocks of routers, switches, and other network equipment.

By default, NTP operates in an entirely unauthenticated manner. If a malicious attempt to influence the accuracy of a router or switch's clock succeeds, it could have negative effects on system logging, make troubleshooting and intrusion detection more difficult, and impede other management functions.

The following sample configuration synchronizes all the routers or switches in the network to a single time source. We recommend using authentication to make sure that the NTP peer is trusted. The **boot-server** statement identifies the server from which the initial time of day and date is obtained when the router boots. The **server** statement identifies the NTP server used for periodic time synchronization. The **authentication-key** statement specifies that an HMAC-Message Digest 5 (MD5) scheme should be used to hash the key value for authentication, which prevents the router or switch from synchronizing with an attacker's host posing as the time server.

```
[edit]
system {
  ntp {
    authentication-key 2 type md5 value "$ABC123"; # SECRET-DATA
    boot-server 10.1.4.1;
    server 10.1.4.2;
  }
}
```

Related Documentation

- [NTP Overview on page 20](#)
- [Understanding NTP Time Servers on page 22](#)
- [show ntp associations on page 143](#)
- [show ntp status on page 145](#)

Configuring NTP Authentication Keys

Time synchronization can be authenticated to ensure that the local router or switch obtains its time services only from known sources. By default, network time synchronization is unauthenticated. The system will synchronize to whatever system appears to have the most accurate time. We strongly encourage you to configure authentication of network time services.

To authenticate other time servers, include the **trusted-key** statement at the **[edit system ntp]** hierarchy level. Only time servers transmitting network time packets that contain one of the specified key numbers and whose key matches the value configured for that key number are eligible to be synchronized to. Other systems can synchronize to the local router without being authenticated.

```
[edit system ntp]
trusted-key [ key-numbers ];
```

Each key can be any 32-bit unsigned integer except 0. Include the **key** option in the **peer**, **server**, or **broadcast** statements to transmit the specified authentication key when transmitting packets. The key is necessary if the remote system has authentication enabled so that it can synchronize to the local system.

To define the authentication keys, include the **authentication-key** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
authentication-key key-number type type value password;
```

number is the key number, **type** is the authentication type (only Message Digest 5 [MD5] is supported), and **password** is the password for this key. The key number, type, and password must match on all systems using that particular key for authentication.

**Related
Documentation**

- [Understanding NTP Time Servers on page 22](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Configuring the Router or Switch to Listen for Broadcast Messages Using NTP

When you are using NTP, you can configure the local router or switch to listen for broadcast messages on the local network to discover other servers on the same subnet by including the **broadcast-client** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
broadcast-client;
```

When the router or switch detects a broadcast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *broadcast client* mode, in which it listens for, and synchronizes to, succeeding broadcast messages.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

**Related
Documentation**

- [Configuring the Router or Switch to Listen for Multicast Messages Using NTP on page 32](#)
- [Configuring the NTP Time Server and Time Services on page 27](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Configuring the Router or Switch to Listen for Multicast Messages Using NTP

When you are using NTP, you can configure the local router or switch to listen for multicast messages on the local network to discover other servers on the same subnet by including the **multicast-client** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
multicast-client <address>;
```


When the router or switch receives a multicast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *multicast client* mode, in which it listens for, and synchronizes to, succeeding multicast messages.

You can specify one or more IP addresses. (You must specify an address, not a hostname.) If you do, the router or switch joins those multicast groups. If you do not specify any addresses, the software uses **224.0.1.1**.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

**Related
Documentation**

- [Configuring the Router or Switch to Listen for Broadcast Messages Using NTP on page 32](#)
- [Configuring the NTP Time Server and Time Services on page 27](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

CHAPTER 2

Configuring Time Zones

- [Modifying the Default Time Zone for a Router or Switch Running Junos OS on page 35](#)
- [Updating the IANA Time Zone Database on Junos OS Devices on page 36](#)

Modifying the Default Time Zone for a Router or Switch Running Junos OS

The default local time zone on a router or a switching device is UTC (Coordinated Universal Time, formerly known as Greenwich Mean Time, or GMT). To modify the local time zone, include the **time-zone** statement at the **[edit system]** hierarchy level:

```
[edit system]
time-zone (GMThour-offset | time-zone);
```

You can use the **GMT *hour-offset*** option to set the time zone relative to UTC (GMT) time. By default, ***hour-offset*** is 0. You can configure this to be a value in the range from -14 to +12.

You can also specify ***time-zone*** as a string such as PDT (Pacific Daylight Time) or WET (Western European Time), or specify the continent and major city.



NOTE: Junos OS complies with the POSIX time-zone standard, which is counter-intuitive to the way time zones are generally indicated relative to UTC. A time zone ahead of UTC (east of the Greenwich meridian) is commonly indicated as GMT +*n*; for example, the Central European Time (CET) zone is indicated as GMT +1. However, this is not true for POSIX time zone designations. POSIX indicates CET as GMT-1. If you include the **set system time-zone GMT+1** statement for a router or a switch in the CET zone, your device time will be set to one hour behind GMT, or two hours behind the actual CET time. For this reason, you might find it easier to use the POSIX time-zone strings, which you can list by entering **set system time-zone ?**.

For the time zone change to take effect for all processes running on the router or switch, you must reboot the router or switch.

The following example shows how to change the current time zone to **America/New_York**:

```
[edit]
user@host# set system time-zone America/New_York
```

```
[edit]
user@host# show
system {
    time-zone America/New_York;
}
```

Starting in Junos OS Release 15.1F6, for the routers with the RE-MX-X6, RE-MX-X8, and RE-PTX-X8 Routing Engines, the date and time zones are synchronized from the admin guest Junos OS to the host OS. Thus, the guest OS and the host OS use the same time zone and there is no difference in the timestamps in system log files of Junos OS and the host OS. This time zone and date synchronization changes the time zone of the host from the default UTC to the configured time zone. However, for the time zone change to take effect for all processes running on the router, reboot the router by using the **request vmhost reboot** command.

- Related Documentation**
- [NTP Overview on page 20](#)
 - [Updating the IANA Time Zone Database on Junos OS Devices on page 36](#)

Updating the IANA Time Zone Database on Junos OS Devices

Junos OS devices use the tz database, also known as the IANA Time Zone Database to manage time zones. This database is periodically updated by IANA to reflect political and time changes. As such, you may need from time to time to update this file to ensure the Junos devices continue to accurately reflect worldwide time zones and daylight savings time intervals.

To update the IANA Time Zone Database, perform the following steps:

1. [Importing and Installing Time Zone Files on page 36](#)
2. [Configuring a Custom Time Zone on page 37](#)

Importing and Installing Time Zone Files

The IANA Time Zone Database is maintained by the Internet Assigned Numbers Authority (IANA), which is a department of the Internet Corporation for Assigned Names and Numbers (ICANN). You can download the latest IANA Time Zone Database file from the following URL: <http://www.iana.org/time-zones>.

The following steps will guide you through one method of installing the file to your device. However, depending on your network access and other preferences, you may need to modify these steps.

1. Log into the Junos device.
2. If you are in the CLI interface, open the shell interface.

```
device@user# start shell
```
3. Create a **tz** directory in the **/var/tmp** and navigate to that directory.

```
# mkdir /var/tmp/tz
# cd /var/tmp/tz
```

4. Using FTP, download the time zone files archive.



NOTE: FTP must be enabled on your device before you can use FTP. FTP is enabled by adding the `ftp` statement into the `[edit system services]` hierarchy.

```
# ftp ftp.iana.org/tz
# bin
# get tzdata-latest.tar.gz
```



NOTE: If needed, you can edit the above untarred files to create or modify the time zones.

5. Select the names of time zone files to compile and feed them to the following script. For example, to generate `northamerica` and `asia` tz files:

```
# /usr/libexec/ui/compile-tz northamerica asia
```

6. Enable the use of the generated tz files using the CLI:

```
[edit]
# set system use-imported-time-zones
[edit]
# set system time-zone ?
```

This should show the newly generated tz files in `/var/db/zoneinfo/`.

7. Set the time zone and commit the configuration:

```
[edit]
# set system time-zone <your-time-zone>
# commit
```

8. Verify that the time zone change has taken effect:

```
[edit]
# run show system uptime
```

See Also

Configuring a Custom Time Zone

To use a custom time zone, follow these steps:

1. Download a time zones archive (from a known or designated source) to the router or switch. Compile the time zone archive using the `zic` time zone compiler, which generates `tz` files.

2. Using the CLI, configure the router or switch to enable the use of the generated tz files as follows:

```
[edit]
user@host# set system use-imported-time-zones
```

3. Display the imported time zones (saved in the directory `/var/db/zoneinfo/`):

```
[edit]
user@host# set system time-zone ?
```

If you do not configure the router to use imported time zones, the Junos OS default time zones are shown (saved in the directory `/usr/share/zoneinfo/`).

**Related
Documentation**

- [Modifying the Default Time Zone for a Router or Switch Running Junos OS on page 35](#)
- [NTP Overview on page 20](#)
- [Understanding NTP Time Servers on page 22](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)
- [use-imported-time-zones on page 140](#)

CHAPTER 3

Configuring Network Time Protocols

- [Understanding NTP Time Servers on page 39](#)
- [Configuring NTP Authentication Keys on page 40](#)
- [Configuring NTP Authentication Keys \(QFabric System\) on page 41](#)
- [Configuring the NTP Time Server and Time Services on page 42](#)
- [Configuring the NTP Time Server and Time Services \(QFabric System\) on page 45](#)
- [Configuring the Switch to Listen for Broadcast Messages Using NTP on page 46](#)
- [Configuring the Switch to Listen for Multicast Messages Using NTP on page 46](#)
- [Setting the Date and Time on page 47](#)
- [Synchronizing and Coordinating Time Distribution Using NTP on page 47](#)
- [Example: Configuring NTP on page 49](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 52](#)

Understanding NTP Time Servers

The IETF defined the Network Time Protocol (NTP) to synchronize the clocks of computer systems connected to each other over a network. Most large networks have an NTP server that ensures that time on all devices is synchronized, regardless of the device location. If you use one or more NTP servers on your network, ensure you include the NTS server addresses in your Junos OS configuration.

When configuring the NTP, you can specify which system on the network is the authoritative time source, or time server, and how time is synchronized between systems on the network. To do this, you configure the router, switch, or security device to operate in one of the following modes:

- **Client mode**—In this mode, the local router or switch can be synchronized with the remote system, but the remote system can never be synchronized with the local router or switch.
- **Symmetric active mode**—In this mode, the local router or switch and the remote system can synchronize with each other. You use this mode in a network in which either the local router or switch or the remote system might be a better source of time.



NOTE: Symmetric active mode can be initiated by either the local or the remote system. Only one system needs to be configured to do so. This means that the local system can synchronize with any system that offers symmetric active mode without any configuration whatsoever. However, we strongly encourage you to configure authentication to ensure that the local system synchronizes only with known time servers.

- Broadcast mode—In this mode, the local router or switch sends periodic broadcast messages to a client population at the specified broadcast or multicast address. Normally, you include this statement only when the local router or switch is operating as a transmitter.
- Server mode—In this mode, the local router or switch operates as an NTP server.



NOTE: In NTP server mode, the Junos OS supports authentication as follows:

- If the NTP request from the client comes with an authentication key (such as a key ID and message digest sent with the packet), the request is processed and answered based on the authentication key match.
- If the NTP request from the client comes without any authentication key, the request is processed and answered without authentication.

**Related
Documentation**

- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Configuring NTP Authentication Keys

Time synchronization can be authenticated to ensure that the switch obtains its time services only from known sources. By default, network time synchronization is unauthenticated. The switch will synchronize to whatever system appears to have the most accurate time. We strongly encourage you to configure authentication of network time services.

To authenticate other time servers, include the **trusted-key** statement at the **[edit system ntp]** hierarchy level. Only time servers that transmit network time packets containing one of the specified key numbers are eligible to be synchronized. Additionally, the key needs to match the value configured for that key number. Other systems can synchronize to the local switch without being authenticated.

```
[edit system ntp]  
trusted-key [ key-numbers ];
```

Each key can be any 32-bit unsigned integer except 0. Include the **key** option in the **peer**, **server**, or **broadcast** statements to transmit the specified authentication key when

transmitting packets. The key is necessary if the remote system has authentication enabled so that it can synchronize to the local system.

To define the authentication keys, include the **authentication-key** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
authentication-key key-number type type value password;
```

number is the key number, **type** is the authentication type (only Message Digest 5 [MD5] is supported), and **password** is the password for this key. The key number, type, and password must match on all systems using that particular key for authentication.

- Related Documentation**
- [Understanding NTP Time Servers on page 22](#)
 - [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)
 - [trusted-key](#)
 - [authentication-key on page 109](#)

Configuring NTP Authentication Keys (QFabric System)

To configure the authentication keys using the CLI:

1. Configure the authentication-key number.

```
[edit system ntp]
user@switch# set authentication-key key-number
```

For example, to specify key 5:

```
user@switch# set authentication-key 5
```

2. Specify the type of authentication you want to use.

```
[edit system ntp]
user@switch# set authentication-key type type
```



NOTE: MD5 is the only authentication type supported.

For example, to specify **MD5**:

```
user@switch# set authentication-key type md5
```

- Related Documentation**
- [NTP Time Server and Time Services Overview \(QFabric System\)](#)
 - [Configuring the NTP Time Server and Time Services \(QFabric System\) on page 45](#)
 - [authentication-key on page 109](#)

Configuring the NTP Time Server and Time Services

When you use NTP, configure the switch to operate in one of the following modes:

- Client mode
- Symmetric active mode
- Broadcast mode
- Server mode

The following topics describe how to configure these modes of operation:

1. [Configuring the Switch to Operate in Client Mode on page 42](#)
2. [Configuring the Router or Switch to Operate in Symmetric Active Mode on page 43](#)
3. [Configuring the Router or Switch to Operate in Broadcast Mode on page 43](#)
4. [Configuring the Router or Switch to Operate in Server Mode on page 43](#)

Configuring the Switch to Operate in Client Mode

To configure the local router or switch to operate in client mode, include the **server** statement and other optional statements at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
server address <key key-number> <version value> <prefer>;
authentication-key key-number type type value password;
boot-server address;
trusted-key [ key-numbers ];
```

Specify the address of the system acting as the time server. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the time server, include the **key** option. The key corresponds to the key number you specify in the **authentication-key** statement, as described in .

By default, the router or switch sends NTP version 4 packets to the time server. To set the NTP version level to 1, 2, or 3, include the **version** option.

If you configure more than one time server, you can mark one server preferred by including the **prefer** option.

The following example shows how to configure the router or switch to operate in client mode:

```
[edit system ntp]
authentication-key 1 type md5 value "$ABC123";
boot-server 10.1.1.1;
server 10.1.1.1 key 1 prefer;
trusted-key 1;
```

See Also • [Configuring NTP Authentication Keys on page 40](#)

- [Synchronizing and Coordinating Time Distribution Using NTP on page 47](#)

Configuring the Router or Switch to Operate in Symmetric Active Mode

To configure the local router or switch to operate in symmetric active mode, include the **peer** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
peer address <key key-number> <version value> <prefer>;
```

Specify the address of the remote system. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the remote system, include the **key** option. The key corresponds to the key number you specify in the **authentication-key** statement.

By default, the router or switch sends NTP version 4 packets to the remote system. To set the NTP version level to 1, 2 or 3, include the **version** option.

If you configure more than one remote system, you can mark one system preferred by including the **prefer** option:

```
peer address <key key-number> <version value> prefer;
```

See Also • [Configuring NTP Authentication Keys on page 40](#)

Configuring the Router or Switch to Operate in Broadcast Mode

To configure the local router or switch to operate in broadcast mode, include the **broadcast** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
broadcast address <key key-number> <version value> <ttl value>;
```

Specify the broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be **224.0.1.1**.

To include an authentication key in all messages sent to the remote system, include the **key** option. The key corresponds to the key number you specify in the **authentication-key** statement.

By default, the router or switch sends NTP version 4 packets to the remote system. To set the NTP version level to 1, 2, or 3, include the **version** option.

See Also • [Configuring NTP Authentication Keys on page 40](#)

Configuring the Router or Switch to Operate in Server Mode

In server mode, the router or switch acts as an NTP server for clients when the clients are configured appropriately. The only prerequisite for “server mode” is that the router or

switch must be receiving time from another NTP peer or server. No other configuration is necessary on the router or switch.

To configure the local router or switch to operate as an NTP server, include the following statements at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
authentication-key key-number type type value password;
server address <key key-number> <version value> <prefer>;
trusted-key [ key-numbers ];
```

Specify the address of the system acting as the time server. You must specify an address, not a hostname.

To include an authentication key in all messages sent to the time server, include the **key** option. The key corresponds to the key number you specify in the **authentication-key** statement.

By default, the router or switch sends NTP version 4 packets to the time server. To set the NTP version level to 1, or 2, or 3, include the **version** option.

If you configure more than one time server, you can mark one server preferred by including the **prefer** option.

The following example shows how to configure the router or switch to operate in server mode:

```
[edit system ntp]
authentication-key 1 type md5 value "$ABC123";
server 192.168.27.46 prefer;
trusted-key 1;
```

See Also • [Configuring NTP Authentication Keys on page 40](#)

Related Documentation • [Understanding NTP Time Servers on page 22](#)
• [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Configuring the NTP Time Server and Time Services (QFabric System)

To configure the external time server using the CLI:

1. Configure the IP address of the external time server.

```
[edit system ntp]
user@switch# set server address
```

For example, to set an IP address of 10.1.1.1 for your external time server:

```
user@switch# set server 10.1.1.1
```

2. (Optional) Configure the key number to encrypt authentication fields in packets that are sent to the external time server.

```
[edit system ntp]
user@switch# set server address key key-number
```

For example, to set a key number of 1:

```
user@switch# set server address key
```

3. (Optional) Specify the external time server as a preferred host. Doing this enables the switch to synchronize with the external time server.



NOTE: The switch can synchronize with the external time server, but the external time server cannot synchronize with the switch.

```
[edit system ntp]
user@switch# set server address prefer
```

4. (Optional) Specify the NTP version number to be used in outgoing NTP packets.

```
user@switch# set server address version
```

For example, to specify version 3:

```
user@switch# set server address version 3
```

Related Documentation

- [NTP Time Server and Time Services Overview \(QFabric System\)](#)
- [ntp on page 126](#)
- [server](#)

Configuring the Switch to Listen for Broadcast Messages Using NTP

When you are using NTP, you can configure the local switch to listen for broadcast messages on the local network to discover other servers on the same subnet by including the **broadcast-client** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]  
broadcast-client;
```

When the switch detects a broadcast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *broadcast client* mode, in which it listens for, and synchronizes to, succeeding broadcast messages.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

- Related Documentation**
- [Configuring the Switch to Listen for Multicast Messages Using NTP on page 46](#)
 - [Configuring the NTP Time Server and Time Services on page 42](#)
 - [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Configuring the Switch to Listen for Multicast Messages Using NTP

When you are using NTP, you can configure the local switch to listen for multicast messages on the local network to discover other servers on the same subnet by including the **multicast-client** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]  
multicast-client <address>;
```

When the switch receives a multicast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *multicast client* mode, in which it listens for, and synchronizes to, succeeding multicast messages.

You can specify one or more IP addresses. (You must specify an address, not a hostname.) If you do, the router or switch joins those multicast groups. If you do not specify any addresses, the software uses **224.0.1.1**.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

- Related Documentation**
- [Configuring the Switch to Listen for Broadcast Messages Using NTP on page 46](#)
 - [Configuring the NTP Time Server and Time Services on page 42](#)
 - [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Setting the Date and Time

1. Enter operational mode in the CLI.

2. Enter the following command:

```
user@switch> set date YYYYMMDDHHMM.ss source-address
```

For example, the following command sets the date and time.

```
user@switch# set date 201102151010.55
```

3. To set the date and time from an NTP server, enter the following command:

```
user@switch# set date ntp servers
```

For example, the following command sets the date and time from an NTP server:

```
user@switch# set date ntp 192.168.40.1
```

4. To set the date and time from more than one NTP server, enter the same command:

```
user@switch# set date ntp servers
```

For example, the following command sets the date and time from more than one NTP server:

```
user@switch# set date ntp 192.168.40.1 192.168.40.2
```

Related
Documentation

- [set date](#)

Synchronizing and Coordinating Time Distribution Using NTP

Using NTP to synchronize and coordinate time distribution in a large network involves these tasks:

1. [Configuring NTP on page 47](#)
2. [Configuring the NTP Boot Server on page 48](#)
3. [Specifying a Source Address for an NTP Server on page 48](#)

Configuring NTP

- To configure NTP on the switch, include the **ntp** statement at the **[edit system]** hierarchy level:

```
[edit system]
ntp {
  authentication-key number type type value password;
  boot-server (address | hostname);
  broadcast <address> <key key-number> <version value> <tll value>;
  broadcast-client;
  multicast-client <address>;
```

```
peer address <key key-number> <version value> <prefer>;
server address <key key-number> <version value> <prefer>;
source-address source-address;
trusted-key [ key-numbers ];
}
```

Configuring the NTP Boot Server

When you boot the switch, it issues an **ntpdate** request, which polls a network server to determine the local date and time. You need to configure a server that the switch uses to determine the time when the switch boots. Otherwise, NTP will not be able to synchronize to a time server if the server's time appears to be very far off of the local switch's time.

- To configure the NTP boot server, include the **boot-server** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
boot-server (address | hostname);
```

Specify either the IP address or the hostname of the network server.

Specifying a Source Address for an NTP Server

For IP version 4 (IPv4), you can specify that if the NTP server configured at the **[edit system ntp]** hierarchy level is contacted on one of the loopback interface addresses, the reply always uses a specific source address. This is useful for controlling which source address NTP uses to access your network when it is either responding to or sending an NTP client request from your network.

To configure the specific source address that the reply will always use, and the source address that requests initiated by NTP server will use, include the **source-address** statement at the **[edit system ntp]** hierarchy level:

```
[edit system ntp]
source-address source-address;
```

source-address is a valid IP address configured on one of the switch interfaces.



NOTE: If a firewall filter is applied on the loopback interface, ensure that the source address specified for the NTP server at the [edit system ntp] hierarchy level is explicitly included as one of the match criteria in the firewall filter. This enables the Junos OS to accept traffic on the loopback interface from the specified source address.

The following example shows a firewall filter with the source address 10.0.10.100 specified in the from statement included at the [edit firewall filter *firewall-filter-name*] hierarchy:

```
[edit firewall filter Loopback-Interface-Firewall-Filter]
term Allow-NTP {
  from {
    source-address {
      192.168.27.46/16; // IP address of the NTP server
      10.0.10.100/10; // Source address specified for the NTP server
    }
  }
  then accept;
}
```

If no source address is configured for the NTP server, include the primary address of the loopback interface in the firewall filter.

Related Documentation

- [Understanding NTP Time Servers on page 22](#)
- [Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30](#)

Example: Configuring NTP

The Network Time Protocol (NTP) provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse network. NTP uses a returnable-time design in which a distributed subnet of time servers operating in a self-organizing, hierarchical primary-secondary configuration synchronizes local clocks within the subnet and to national time standards by means of wire or radio. The servers also can redistribute reference time using local routing algorithms and time daemons.

This example shows how to configure NTP:

- [Requirements on page 49](#)
- [Overview on page 50](#)
- [Configuration on page 50](#)
- [Verification on page 51](#)

Requirements

This example uses the following software and hardware components:

- Junos OS Release 11.1 or later
- A switch connected to a network on which an NTP boot server and NTP server reside

Overview

Debugging and troubleshooting are much easier when the timestamps in the log files of all switches are synchronized, because events that span a network can be correlated with synchronous entries in multiple logs. We recommend using the Network Time Protocol (NTP) to synchronize the system clocks of your switch and other network equipment.

In this example, an administrator wants to synchronize the time in a switch to a single time source. We recommend using authentication to make sure that the NTP peer is trusted. The **boot-server** statement identifies the server from which the initial time of day and date are obtained when the switch boots. The **server** statement identifies the NTP server used for periodic time synchronization. The **authentication-key** statement specifies that an HMAC-Message Digest 5 (MD5) scheme is used to hash the key value for authentication, which prevents the switch from synchronizing with an attacker's host that is posing as the time server.

Configuration

To configure NTP:

CLI Quick Configuration

To quickly configure NTP, copy the following commands and paste them into the switch's terminal window:

```
[edit system]
set ntp boot-server 10.1.4.1
set ntp server 10.1.4.2
set ntp authentication-key 2 type md5 value "$ABC123"
```

Step-by-Step Procedure

To configure NTP :

1. Specify the boot server:

```
[edit system]
user@switch# set ntp boot-server 10.1.4.1
```

2. Specify the NTP server:

```
[edit system]
user@switch# set ntp server 10.1.4.2
```

3. Specify the key number, authentication type (MD5), and key for authentication:

```
[edit system]
user@switch# set ntp authentication-key 2 type md5 value "$ABC123"
```

Results Check the results:

```
[edit system]
user@switch# show
ntp {
  boot-server 10.1.4.1;
  authentication-key 2 type md5 value "$ABC123"; ## SECRET-DATA
  server 10.1.4.2;
}
```

Verification

To confirm that the configuration is correct, perform these tasks:

- [Checking the Time on page 51](#)
- [Displaying the NTP Peers on page 51](#)
- [Displaying the NTP Status on page 52](#)

Checking the Time

Purpose Check the time that has been set on the switch.

Action Enter the **show system uptime** operational mode command to display the time.

```
user@switch> show system uptime
fpc0:
-----
Current time: 2009-06-12 12:49:03 PDT
System booted: 2009-05-15 06:24:43 PDT (4w0d 06:24 ago)
Protocols started: 2009-05-15 06:27:08 PDT (4w0d 06:21 ago)
Last configured: 2009-05-27 14:57:03 PDT (2w1d 21:52 ago) by admin1
12:49PM up 28 days, 6:24, 1 user, load averages: 0.05, 0.06, 0.01
```

Meaning The output shows that the current date and time are June 12, 2009 and 12:49:03 PDT. The switch booted 4 weeks, 6 hours, and 24 minutes ago, and its protocols were started approximately 3 minutes before it booted. The switch was last configured by user **admin1** on May 27, 2009, and there is currently one user logged in to the switch.

The output also shows that the load average is 0.05 seconds for the last minute, 0.06 seconds for the last 5 minutes, and 0.01 seconds for the last 15 minutes.

Displaying the NTP Peers

Purpose Verify that the time has been obtained from an NTP server.

Action Enter the **show ntp associations** operational mode command to display the NTP server from switch obtained its time.

```
user@switch> show ntp associations
      remote      refid      st t when poll reach  delay  offset  jitter
=====
*ntp.net .GPS.          1 u  414 1024  377    3.435    4.002    0.765
```

Meaning The asterisk (*) in front of the NTP server name, or peer, indicates that the time is synchronized and obtained from this server. The delay, offset, and jitter are displayed in milliseconds.

Displaying the NTP Status

Purpose View the configuration of the NTP server and the status of the system.

Action Enter the **show ntp status** operational mode command to view the status of the NTP.

```
user@switch> show ntp status
status=0644 leap_none, sync_ntp, 4 events, event_peer/strat_chg,
version="ntpd 4.2.0-a Mon Apr 13 19:09:05 UTC 2009 (1)",
processor="powerpc", system="JUNOS9.5R1.8", leap=00, stratum=2,
precision=-18, rootdelay=2.805, rootdispersion=42.018, peer=48172,
refid=192.168.28.5,
reftime=cddd397a.60e6d7bf Fri, Jun 12 2009 13:30:50.378, poll=10,
clock=cddd3b1b.ec5a2bb4 Fri, Jun 12 2009 13:37:47.923, state=4,
offset=3.706, frequency=-23.018, jitter=1.818, stability=0.303
```

Meaning The output shows status information about the switch and the NTP.

- Related Documentation**
- [Understanding NTP Time Servers on page 22](#)
 - *ntp*
 - [Configuring the NTP Time Server and Time Services on page 42](#)
 - [CLI Explorer](#)
 - *Junos OS Baseline Network Operations Guide*

Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization

Debugging and troubleshooting are much easier when the timestamps in the log files of all the routers or switches are synchronized, because events that span the network can be correlated with synchronous entries in multiple logs. We strongly recommend using the Network Time Protocol (NTP) to synchronize the system clocks of routers, switches, and other network equipment.

By default, NTP operates in an entirely unauthenticated manner. If a malicious attempt to influence the accuracy of a router or switch's clock succeeds, it could have negative effects on system logging, make troubleshooting and intrusion detection more difficult, and impede other management functions.

The following sample configuration synchronizes all the routers or switches in the network to a single time source. We recommend using authentication to make sure that the NTP

peer is trusted. The **boot-server** statement identifies the server from which the initial time of day and date is obtained when the router boots. The **server** statement identifies the NTP server used for periodic time synchronization. The **authentication-key** statement specifies that an HMAC-Message Digest 5 (MD5) scheme should be used to hash the key value for authentication, which prevents the router or switch from synchronizing with an attacker's host posing as the time server.

```
[edit]
system {
  ntp {
    authentication-key 2 type md5 value "$ABC123"; # SECRET-DATA
    boot-server 10.1.4.1;
    server 10.1.4.2;
  }
}
```

**Related
Documentation**

- [NTP Overview on page 20](#)
- [Understanding NTP Time Servers on page 22](#)
- [show ntp associations on page 143](#)
- [show ntp status on page 145](#)

CHAPTER 4

Configuring Precision Time Protocols

- [Understanding Transparent Clocks in Precision Time Protocol on page 56](#)
- [IEEE 1588v2 PTP Boundary Clock Overview on page 58](#)
- [IEEE 1588v2 Precision Timing Protocol \(PTP\) on page 61](#)
- [Understanding the PTP G.8275.2 Enhanced Profile \(Telecom Profile\) on page 63](#)
- [Understanding the Precision Time Protocol Enterprise Profile on page 65](#)
- [Configuring Transparent Clock Mode for Precision Time Protocol on page 68](#)
- [Configuring the Precision Time Protocol G.8275.2 Enhanced Profile \(Telecom Profile\) on page 68](#)
- [Configuring Precision Time Protocol Default Profile on page 71](#)
- [Configuring the Precision Time Protocol Enterprise Profile on page 75](#)
- [Configuring Precision Time Protocol Clocking on page 78](#)
- [Configuring a PTP Master Boundary Clock on page 80](#)
- [Example: Configuring a PTP Boundary Clock on page 83](#)
- [Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 86](#)
- [Configuring a PTP Slave Clock on page 90](#)
- [Example: Configuring an Ordinary Slave Clock With Unicast-Negotiation on page 93](#)
- [Example: Configuring an Ordinary Slave Clock Without Unicast-Negotiation on page 96](#)

Understanding Transparent Clocks in Precision Time Protocol

The Precision Time Protocol (PTP) standardized by IEEE 1588 improves the current methods of synchronization used within a distributed network. You can use PTP across packet-based networks including, but not limited to, Ethernet networks. Queuing and buffering delays in the switch can cause variable delay to packets, which affects path delay measurements. Queuing delays vary based on the network load and also depend on the architecture of the switch or the router.

Transparent clocks measure and adjust for packet delay. The transparent clock computes the variable delay as the PTP packets pass through the switch or the router. The switch (QFX5100 or EX4600) or the router (ACX5048, or ACX5096 routers) acts as a transparent clocks only and operates between the master and slave clocks in a distributed network. Transparent clocks improve synchronization between the master and slave clocks and ensure that the master and slave clocks are not impacted by the effects of packet delay variation.

The transparent clock measures the residence time (the time that the packet spends passing through the switch or the router), and adds the residence time into the correction field of the PTP packet. The slave clock accounts for the packet delay by using both the timestamp of when it started and the information in the correction field.

ACX5048 and ACX5096 routers support end-to-end transparent clocks. With an end-to-end transparent clock, only the residence time is included in the correction field of the PTP packets. The residence timestamps are sent in one packet as a one-step process. In a two-step process, estimated timestamps are sent in one packet, and additional packets contain updated timestamps.



NOTE: ACX5048 and ACX5096 routers support only the one-step process, which means that the timestamps are sent in one packet.

You can enable or disable a transparent clock globally for the switch or router. With a global configuration, the same configuration is applied to each interface. If the transparent clock is disabled, PTP packet correction fields are not updated. If the transparent clock is enabled, the PTP packet correction fields are updated.

PTP over Ethernet, IPv4, IPv6, unicast, and multicast for transparent clocks are supported.



NOTE: ACX5048 and ACX5096 routers do not support PTP over IPv6 for transparent clocks.

ACX5048 and ACX5096 routers do not support the following:

- Boundary clock
- Ordinary clock
- Transparent clock over MPLS switched path
- Transparent clock with more than two VLAN tags



NOTE: ACX Series routers do not support transparent clock over MPLS switched path.



NOTE: You might notice higher latency when you use copper SFP ports instead of fiber SFP ports. In this case, you must compensate the latency introduced by the copper SFP ports for the accurate CF (correction factor) measurement.

- Related Documentation**
- [Configuring Transparent Clock Mode for Precision Time Protocol on page 68](#)
 - [e2e-transparent on page 118](#)

IEEE 1588v2 PTP Boundary Clock Overview

The IEEE 1588v2 standard defines the Precision Time Protocol (PTP), which is used to synchronize clocks throughout a network. The standard describes the PTP boundary clock's hierarchical master/slave architecture for the distribution of time-of-day.

- [IEEE 1588v2 PTP Boundary Clock on page 58](#)
- [Clock Clients on page 60](#)

IEEE 1588v2 PTP Boundary Clock

Starting with Junos OS Release 17.3R1, IEEE 1588v2 boundary clock is supported on QFX10002 switches. An IEEE 1588v2 boundary clock has multiple network connections and can act as a source (master) and a destination (slave or client) for synchronization messages. It synchronizes itself to a best master clock through a slave port and supports synchronization of remote clock clients to it on master ports. Boundary clocks can improve the accuracy of clock synchronization by reducing the number of 1588v2-unaware hops between the master and the client. Boundary clocks can also be deployed to deliver better scale because they reduce the number of sessions and the number of packets per second on the master.

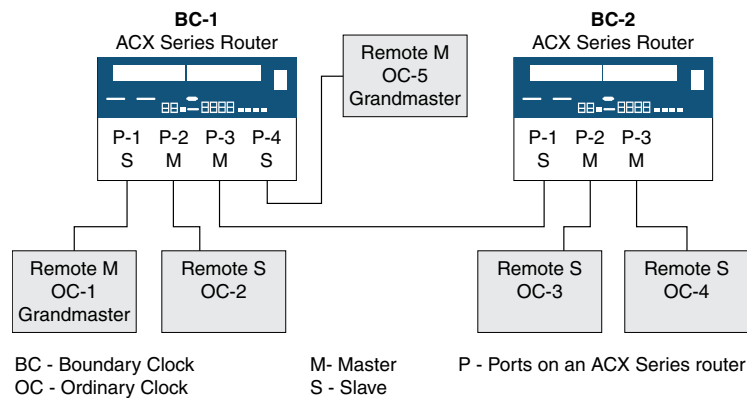
The boundary clock intercepts and processes all PTP messages and passes all other traffic. The best master clock algorithm (BMCA) is used by the boundary clock to select the best configured acceptable master clock that a boundary slave port can see. To configure a boundary clock, include the **boundary** statement at the **[edit protocols ptp clock-mode]** hierarchy level and at least one master with the **master** statement and at least one slave with the **slave** statement at the **[edit protocols ptp]** hierarchy level.

[Figure 1 on page 59](#) illustrates two boundary clocks in a network in which the clock flow is from the upstream node (BC-1) to the downstream node (BC-2).



NOTE: This figure also applies to MX Series routers and QFX Series switches.

Figure 1: Boundary Clocks in a Network



9017867

The first boundary clock—BC-1—has four ports. Each port is configured as follows:

- BC-1 P-1 and BC-1 P-4 are boundary slave ports connected to two grandmaster clocks—OC-1 and OC-5. The grandmasters are included as the clock sources in the slave port configurations. From the packets received on the slave ports, BC-1 selects the best master, synchronizes its clock, and generates PTP packets, which are sent over the master ports—BC-1 P-2 and BC-1 P-3—to the downstream clients.
- BC-1 P-2, a master port, is connected to OC-2, an ordinary remote slave. OC-2 is included as a clock client in BC-1 P-2's master configuration, and so receives PTP packets from BC-1 P-2.
- BC-1 P-3, a master port, is connected to BC-2 P-1, a remote boundary slave port. In this situation, the master port—BC-1 P-3—is included as a clock source in the configuration of the boundary slave port—BC-2 P-1. In addition, the boundary slave port—BC-2 P-1—is included as a clock client in the configuration of the master port—BC-1 P-3. With this configuration, the boundary slave—BC-2 P1—receives PTP packets from BC-1 P3.

The second boundary clock—BC-2—has three ports. Each port is configured as follows:

- BC-2 P-1 is a boundary slave port connected to the upstream master port—BC-1 P3. As described previously, BC-2 P-1 receives PTP packets from BC-1 P3. The master ports—BC-2 P-2 and BC-2 P-3—synchronize their time from the packets received from BC-2 P1.
- BC-2 P-2 and BC-2 P-3, boundary master ports, are connected to ordinary remote slaves—OC-3 and OC-4. OC-3 and OC-4 are included as clock clients in the configuration of the master ports—BC-2 P2 and BC-2 P-3. Both slaves receive PTP packets from the master boundary port to which they are connected.

In this example, the boundary clock synchronizes its clock from the packets received on its slave ports from the upstream master. The boundary clock then generates PTP packets, which are sent over the master port to downstream clients. These packets are timestamped by the boundary clock by using its own time, which is synchronized to the selected upstream master.

Clock Clients

A clock client is the remote PTP host, which receives time from the PTP master and is in a slave relationship to the master.



NOTE: The term *slave* is sometimes used to refer to the clock client.

An device acting as a master boundary clock supports the following types of downstream clients:

- **Automatic client**—An automatic client is configured with an IP address, which includes the subnet mask, indicating that any remote PTP host belonging to that subnet can join the master clock through a unicast negotiation. To configure an automatic client, include the subnet mask in the **clock-client ip-address** statement at the [edit protocols ptp master interface *interface-name* unicast-mode] hierarchy level.
- **Manual client**—A manual client is configured with the **manual** statement at the [edit protocols ptp master interface *interface-name* unicast-mode clock-client ip-address local-ip-address *local-ip-address*] hierarchy level. A manual client does *not* use unicast negotiation to join the master clock. The **manual** statement overrides the **unicast negotiation** statement configured at the [edit protocols ptp] hierarchy level. As soon as you configure a manual client, it starts receiving announce and synchronization packets.
- **Secure client**—A secure client is configured with an exact IP address of the remote PTP host, after which it joins a master clock through unicast negotiation. To configure a secure client, include the exact IP address in the **clock-client ip-address** statement at the [edit protocols ptp master interface *interface-name* unicast-mode] hierarchy level.



NOTE: You can configure the maximum number of clients (512) in the following combination:

- Automatic clients 256.
- Manual and secure clients 256—Any combination of manual and secure clients is allowed as long as the combined total amounts to 256.

Release History Table

| Release | Description |
|---------|--|
| 17.3R1 | Starting with Junos OS Release 17.3R1, IEEE 1588v2 boundary clock is supported on QFX10002 switches. |

Related Documentation

- [IEEE 1588v2 Precision Timing Protocol \(PTP\) on ACX Series Universal Access Routers on page 61](#)
- [Precision Time Protocol Overview](#)

- [Configuring Precision Time Protocol Clocking on page 78](#)
- *Supported IPv4, TCP, and UDP Standards*

IEEE 1588v2 Precision Timing Protocol (PTP)

The IEEE 1588v2 standard defines the Precision Time Protocol (PTP), which is used to synchronize clocks throughout a packet-switched network. This synchronization is achieved through packets that are transmitted and received in a session between a master clock and a slave clock or remote clock client. The clocks used for the distribution of accurate time are in an hierarchical master/slave architecture, which includes boundary clocks, ordinary clocks, and grandmaster clocks. A boundary clock is both a clock source *and* a clock client. An ordinary clock is either a clock source *or* a clock client. However, a grandmaster clock is always a clock source. An ordinary clock on a device is always a clock client. In addition, User UDP over IPv4 and unicast mode are used to transport PTP messages.



NOTE: In ACX Series routers, the grandmaster functionality is supported only on ACX500 router.

The following key PTP features are supported:

- **Boundary clock**—A boundary clock has multiple network connections and can act as a source (master) and a destination (slave or clock client) for synchronization messages. It synchronizes itself to a best master clock through a slave port and supports synchronization of clients to it on master ports. Boundary clocks can improve the accuracy of clock synchronization by reducing the number of 1588v2-unaware hops between the master and the client. Boundary clocks can also be deployed to deliver better scale because they reduce the number of sessions and the number of packets per second on the master.
- **Ordinary clock**—The PTP ordinary clock has a single network connection and can act as a source (master) or destination (slave or clock client) for synchronization messages. On devices, the ordinary clock is a slave, which receives synchronization reference messages from a master, either a grandmaster or a master boundary clock. You cannot configure an ordinary master on a device. However, a boundary clock can provide time to the ordinary slave.
- **PTP grandmaster clock**—The PTP grandmaster clock communicates time information to destination or slave ports. The grandmaster clock is an external device to which the boundary or ordinary clock synchronizes. You cannot configure a grandmaster clock on a device. However, a boundary clock slave or an ordinary clock slave can receive time from a grandmaster clock.
- **Clock source**—A clock source is the PTP master clock to which the slave synchronizes. The clock source is included in the configuration of the slave clock.



NOTE: The term *master* is sometimes used to refer to the clock source.

- Clock client—A clock client is the remote PTP host, which receives time from the PTP master. The clock client is included in the configuration of the master clock.



NOTE: The term *slave* is sometimes used to refer to the clock client.

- PTP over UDP over IPv4—The IEEE1588v2 standard specifies different transport protocols for carrying PTP packets. For example, PTP over Ethernet, PTP over UDP over IPv4, and PTP over UDP over IPv6. ACX Series routers support PTP over UDP over IPv4.
- Unicast mode (IPv4 on Gigabit Ethernet interfaces only)—Unicast mode is a user-to-user protocol used to send a datagram to a single recipient. Unicast mode is used for transporting PTP messages.

**Related
Documentation**

- *Precision Time Protocol Overview*
- [IEEE 1588v2 PTP Boundary Clock Overview on page 58](#)
- [Configuring Precision Time Protocol Clocking on page 78](#)
- *Supported IPv4, TCP, and UDP Standards*

Understanding the PTP G.8275.2 Enhanced Profile (Telecom Profile)

The Precision Time Protocol (PTP) G.8275.2 enhanced profile supports telecom applications that require accurate phase and time synchronization for phase alignment and time of day synchronization over a wide area network. This profile supports partial timing support (PTS) using PTP over IPv4 unicast, ordinary and boundary clocks, and unicast negotiation.

With the G.8275.2 enhanced profile, you can use either boundary or ordinary clocks. Up to 512 downstream slave clocks are supported. Slave clock ports can recover clocks from one-step or two-step master clocks, but master clocks only support one-step PTP.

The G.8275.2 enhanced profile includes the following functionality:

- Support for both ordinary clocks and boundary clocks.
- Support for master-only and slave-only ports.
- Support for node types T-BC-P (BC) and T-TSC-P (OC/BC).
- Support for the alternate best master clock algorithm.
- Support for PTP with or without VLAN encapsulation and for two-way transfer. Unicast PTP over IPv4 transport is required.
- Unicast negotiation with single and multiple TLVs support on the master port. The master accepts single and multiple TLV messages from the remote slave for request, cancel, and ack messages. The master responds with single or multiple TLV messages as appropriate. The “rate” TLV is ignored.
- Reception and transmission of unicast Announce and Sync PTP packets.
- Support for full domain and packet-rate ranges.
- Support for manual mode, rather than unicast negotiation.

With the G.8275.2 enhanced profile enabled, the following parameters can apply:

- Priority1
The allowed (and default) value is 128. (Not user-configurable.)
- Priority2
The range is from 0 to 255, and the default value is 128.
- Domain number
The range is from 44 to 63, and the default value is 44.
- Clock mode
The clock mode can be ordinary or boundary.
- Duration of neighborhood rates
The range is 60 to 1000 seconds, and the default value is 300 seconds.
- clockAccuracy

0xFE

- offsetScaledLogVariance

0xFFFF

- slaveOnly

The allowed values are True and False; the default value is False. (Not user-configurable; the value is set according to the setting of the clock mode: boundary or ordinary.)

- localPriority

The range is 1 to 255; the default value is 128.

Table 3: Announce, Sync, and Delay Request/Response Rate Parameters

| Parameter | Default Value | Allowed Range of Values |
|-----------------------------|---|-------------------------|
| Announce rate | <ul style="list-style-type: none"> • Master: -3 • Slave: 0 | -3 – 0 |
| Delay request/response rate | <ul style="list-style-type: none"> • Master: -6 • Slave: -7 | -7 – -3 |
| Sync rate | <ul style="list-style-type: none"> • Master: -7 • Slave: -6 | -7 – -3 |

**Related
Documentation**

- [Configuring the Precision Time Protocol G.8275.2 Enhanced Profile \(Telecom Profile\) on page 68](#)

Understanding the Precision Time Protocol Enterprise Profile

The enterprise profile is based on Precision Time Protocol (PTPv1) as defined in IEEE 1588-2002. This profile was designed to distribute system time of day (TOD) and clock frequency from a grand master clock to slave clocks within the same network and clock domain, and to use multicast communications. The enterprise profile PTPv2 is not backwards compatible with PTPv1.

With the enterprise profile, you can use either boundary or ordinary clocks. Up to 512 downstream slave clocks are supported. Slave clock ports can recover clocks from one-step or two-step master clocks, but master clocks only support one-step PTP.

The enterprise profile supports PTP over IPv4 and UDP encapsulation, which includes the following functionality:

- Reception and transmission of Multicast Announce and Sync PTP packets.
- Reception of multicast or unicast Delay Request packets for the master clock interfaces.

The Delay Response is sent with the same multicast or unicast transmission to match the request.

- Transmission of unicast Delay Request packets for the slave clock interfaces.

The switch will not transmit Multicast Delay Request packets.

- IPv4 Multicast address of 224.0.1.129 for PTP.
- PTP Interfaces can be trunk or access ports, so the traffic might or might not be part of a VLAN.

The enterprise profile supports dynamic master clock interface and slave clock interface detection as Announce and Delay Request packets are received and supports the following functionality:

- Streams are identified by the clock identity, rather than the IP address.
- Up to four remote master clocks that use the best master clock (BMC) algorithm to select the clock source.
- Up to 512 remote slave clocks with up to 64 logical interfaces.
- Remote devices are ignored when the number of master and slave clocks has reach the limit.

If messages are no longer being received from a remote device; a timeout mechanism is used. Streams are removed if they are no longer receiving packets after a default value of 30 seconds.

To support a 1-Gigabit Ethernet connection to a grandmaster clock, you can use a special interface that is labeled **PTP** on the faceplate of the QFX10002 switch. This interface is named **ptp0** in the Junos OS CLI. This interface only supports encapsulated PTP, ARP, and PING packets to support the grandmaster clock connection. Non-PTP traffic is not supported. You can configure this interface as a slave clock interface to connect to a grandmaster but not as a tagged interface. You can, however, configure 10-, 40-, and 100-Gigabit Ethernet interfaces as master clock, slave clock, and in tagged and untagged configurations.

With the enterprise profile enabled, there are restrictions on which parameters you can configure or cannot configure.

With the enterprise profile enabled, you can configure the following parameters:

- Priority1

The range is from 0 to 255, and the default value is 128.

- Priority2

The range is from 0 to 255, and the default value is 128.

- Domain number

The range is from 0 to 127, and the default value is 0.

- Clock mode

Clock mode can be ordinary or boundary.

- Delay request

The Range -7 to +7 seconds, and the default value is 0 (1pps).

- Sync interval

The range is -7 to +4 seconds, and the default value is 0 (1pps).

With the enterprise profile enabled, you cannot configure the following parameters:

- Announce interval

Default value is 0 (1pps).

- Announce timeout

The announce receipt timeout interval is set for three announce intervals for preferred master clocks, and four announce intervals for all other master clocks. All master clocks will be treated as preferred master clocks, so the announce receipt timeout interval is set to three announce intervals.

- Unicast negotiation

Configuring Transparent Clock Mode for Precision Time Protocol

In a distributed network, you can configure transparent clock for Precision Time Protocol (PTP) for synchronizing the timing across the network. Junos OS supports the **e2e-transparent** CLI statement at the **[edit protocols ptp]** hierarchy level to configure transparent clock for Precision Time Protocol (PTP).



NOTE: Starting in Junos OS Release 17.2 onwards, to configure PTP transparent clock, include the **e2e-transparent** CLI command at the **[edit protocols ptp]** hierarchy level. The **transparent-clock** CLI command to configure transparent clock at the **[edit protocols ptp]** hierarchy level is supported only in Junos OS Release 12.3X54.

To configure the transparent clock mode for Precision Time Protocol (PTP):

1. In configuration mode, go to the **[edit protocols ptp]** hierarchy level.

```
[edit]
user@host# edit protocols ptp
```

2. Specify transparent clock mode:

```
[edit protocols ptp]
user@host# set e2e-transparent
```

Related Documentation

- [Understanding Transparent Clocks in Precision Time Protocol on page 56](#)
- [e2e-transparent on page 118](#)
- [show ptp global-information on page 151](#)

Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile)



NOTE: When you enable the G.8275.2 enhanced profile, you cannot enable any other profile.

- [Configuring Precision Time Protocol and Its Options on page 68](#)

Configuring Precision Time Protocol and Its Options

This topic includes the following tasks:

1. [Configuring PTP Options on page 69](#)
2. [Configuring Slave Clock Options on page 70](#)
3. [Configuring Master Clock Options on page 71](#)

Configuring PTP Options

To configure PTP options:

1. In configuration mode, go to the **[edit protocols ptp]** hierarchy level:

```
[edit]
user@host# edit protocols ptp
```

2. Configure the clock mode as either boundary or ordinary. This attribute is mandatory and has no default value.

The **boundary** option signifies that both master and slave must be configured. The **ordinary** option signifies that only the master, or only the slave, must be configured.

```
[edit protocols ptp]
user@host# set clock-mode (boundary | ordinary)
```

3. Configure the profile type as g.8275.2.enh (the G.8275.2.enh profile type provides the telecom profile). This attribute is mandatory.

```
[edit protocols ptp]
user@host# set profile-type g.8275.2.enh
```

4. (Optional) Configure the PTP domain option with a value from 44 through 63. The default value is 44.

```
[edit protocols ptp]
user@host# set domain domain-value
```

5. (Optional) Configure the **priority2** option with values from 0 through 255. The default value is 128.

The **priority2** value differentiates and prioritizes the master clock to avoid confusion when **priority1-value** is the same for different master clocks in a network.

```
[edit protocols ptp]
user@host# set priority2 priority2-value
```

6. Configure the **unicast-negotiation** option.

Unicast negotiation is a method by which the announce, sync, and delay response packet rates are negotiated between the master clock and the slave clock before a PTP session is established.

```
[edit protocols ptp]
user@host# set unicast-negotiation
```



NOTE: Unicast negotiation, when enabled, does not allow you to commit any packet rate–related configuration.

Configuring Slave Clock Options

Configure the following options after the aforementioned PTP options have been set.

1. Configure the slave clock.

```
[edit protocols ptp]  
user@host# edit slave
```

2. (Optional) Configure the **delay-request** option in the slave node. The range is -7 to -3 seconds, and the default values are -6 for the master and -7 for the slave.

The delay request value is the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.

```
[edit protocols ptp slave]  
user@host# set delay-request delay-request-value
```

3. Configure the interface for the slave.

```
[edit protocols ptp slave]  
user@host# set interface interface-name
```

4. Configure the **unicast-mode** option for the slave.

```
[edit protocols ptp slave interface interface-name]  
user@host# set unicast-mode
```

5. Configure the **transport** option in unicast mode as IPv4.

The encapsulation type for PTP packet transport is IPv4.

```
[edit protocols ptp slave interface interface-name unicast-mode]  
user@host# set transport ipv4
```

6. Configure the clock source and the IP address of the interface acting as the local PTP slave port.

```
[edit protocols ptp slave interface interface-name unicast-mode]  
user@host# set clock-source ip-address local-ip-address local-ip-address
```



NOTE: You must configure this IP address at the [edit interfaces *interface-name*] hierarchy level.

7. (Optional) Configure the priority assigned to the interface acting as the local PTP slave port.

```
[edit protocols ptp slave interface interface-name unicast-mode]  
user@host# set local-priority number
```

Configuring Master Clock Options

Configure the following options after the aforementioned PTP options and slave clock options have been set.

1. Configure the master clock.

```
[edit protocols ptp]  
user@host# edit master
```

2. Configure the interface for the master.

```
[edit protocols ptp master]  
user@host# set interface interface-name
```

3. Configure the unicast mode option for the master.

```
[edit protocols ptp master interface interface-name]  
user@host# edit unicast-mode
```

4. Configure the **transport** option in unicast mode as IPv4.

The encapsulation type for PTP packet transport is IPv4.

```
[edit protocols ptp master interface interface-name unicast-mode]  
user@host# set transport ipv4
```

5. Configure the remote clock source and the IP address of the interface acting as the master.

```
[edit protocols ptp master interface interface-name unicast-mode transport type]  
user@host# set clock-client ip-address local-ip-address ip-address
```

Related Documentation

- [Understanding the PTP G.8275.2 Enhanced Profile \(Telecom Profile\) on page 63](#)

Configuring Precision Time Protocol Default Profile

You can configure the master clock and the slave clock for Precision Time Protocol (PTP) to help synchronize clocks in a distributed system. This time synchronization is achieved through packets that are transmitted and received in a session between the master clock and the slave clock. The default profile is enabled by default. You do not need to enable the **profile-type** statement to use the default profile.

- [Configuring Precision Time Protocol and its Options on page 72](#)

Configuring Precision Time Protocol and its Options

This topic includes the following tasks:

1. [Configuring PTP Options on page 72](#)
2. [Configuring Slave Clock Options on page 73](#)
3. [Configuring Master Clock Options on page 74](#)

Configuring PTP Options



NOTE: For information on how to configure PTP using unicast negotiation, see [“Example: Configuring a PTP Boundary Clock With Unicast Negotiation” on page 86](#).

To configure PTP options:

1. In configuration mode, go to the **[edit protocols ptp]** hierarchy level:

```
[edit]
user@host# edit protocols ptp
```

2. Configure the clock mode as either boundary or ordinary. This attribute is mandatory and has no default value.

The **boundary** option signifies that the clock can be both a master clock and a slave clock. The **ordinary** option signifies that the clock is either a master clock or a slave clock.

```
[edit protocols ptp]
user@host# set clock-mode (boundary | ordinary)
```

3. Configure the PTP domain option with values from 0 through 127. The default value is 0.

```
[edit protocols ptp]
user@host# set domain domain-value
```

4. Configure the **priority1** option with values from 0 through 255. The default value is 128.

The **priority1** value determines the best master clock. The *priority1-value* is also advertised in the master clock's announce message to other slaves.

```
[edit protocols ptp]
user@host# set priority1 priority1-value
```

5. Configure the **priority2** option with values from 0 through 255. The default value is 128.

The **priority2** value differentiates and prioritizes the master clock to avoid confusion when *priority1-value* is the same for different master clocks in a network.


```
[edit protocols ptp]
user@host# set priority2 priority2-value
```

6. Configure the **multicast-mode** option to enable multicast transport.

```
[edit protocols ptp]
user@host# set multicast-mode
```

Configuring Slave Clock Options

Configure the following options after the aforementioned PTP options have been set.

1. Configure the slave clock.

```
[edit protocols ptp]
user@host# edit slave
```

2. (Optional) Configure the **delay-request** option in the slave node with values from -7 through 7. The default value is 0.

The delay request value is the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.

```
[edit protocols ptp slave]
user@host# set delay-request delay-request-value
```

3. Configure the interface for the slave.

```
[edit protocols ptp slave]
user@host# set interface interface-name
```

4. Configure the **multicast-mode** option for the slave. You can set this option when PTP multicast mode of messaging is needed.

```
[edit protocols ptp slave interface interface-name]
user@host# set multicast-mode
```

5. Configure the **transport** option in multicast mode as IPv4.

The encapsulation type for PTP packet transport is IPv4.

```
[edit protocols ptp slave interface interface-name multicast-mode]
user@host# set transport ipv4
```

6. Configure the IP address of the local logical interface.

```
[edit protocols ptp slave interface interface-name multicast-mode]
user@host# set local-ip-address IP address
```

Configuring Master Clock Options

Configure the following options after the aforementioned PTP options and slave clock options have been set.

1. Configure the master clock.

```
[edit protocols ptp]  
user@host# edit master
```

2. Configure the **delay-req-timeout** option for the master.

The maximum timeout for delay request messages is between 30 and 300 seconds. We recommend 30 seconds.

```
[edit protocols ptp master]  
user@host# set delay-req-timeout seconds
```

3. Configure the interface for the master.

```
[edit protocols ptp master]  
user@host# set interface interface-name
```

4. Configure the **multicast-mode** option for the master. You can set this option when PTP multicast mode of messaging is needed.

```
[edit protocols ptp master interface interface-name]  
user@host# set multicast-mode
```

5. Configure the **transport** option in multicast mode as IPv4.

The encapsulation type for PTP packet transport is IPv4.

```
[edit protocols ptp master interface interface-name multicast-mode]  
user@host# set transport ipv4
```

6. Configure the IP address of the interface acting as the local PTP master port.

```
[edit protocols ptp master interface interface-name multicast-mode clock-client  
  ip-address]  
user@host# set local-ip-address local-ip-address
```

7. Configure the interface to be used to connect with the PTP grandmaster clock.

```
[edit protocols ptp master]  
user@host# set interface interface-name
```

If the master clock connection is through a 1-Gigabit Ethernet interface, configure the **ptp0** interface.

This interface is named **ptp0** by default.

```
[edit protocols ptp master]  
user@host# set interface ptp0
```

8. Configure the **multicast-mode** option for the PTP grandmaster clock interface. You can set this option when PTP multicast mode of messaging is needed.

```
[edit protocols ptp master interface]
user@host# set interface-name multicast-mode
```

9. Configure the **transport** option in multicast mode as IPv4.

The encapsulation type for PTP packet transport is IPv4.

```
[edit protocols ptp master interface interface-name multicast-mode]
user@host# set transport ipv4
```

- Related Documentation**
- [Precision Time Protocol Overview](#)
 - [Example: Configuring Precision Time Protocol](#)

Configuring the Precision Time Protocol Enterprise Profile



NOTE: When you enable the enterprise profile, you cannot enable any other profile. Also, unicast negotiation is disabled when you enable the enterprise profile.

- [Configuring Precision Time Protocol and its Options on page 75](#)

Configuring Precision Time Protocol and its Options

This topic includes the following tasks:

1. [Configuring PTP Options on page 75](#)
2. [Configuring Slave Clock Options on page 76](#)
3. [Configuring Master Clock Options on page 77](#)

Configuring PTP Options

To configure PTP options:

1. In configuration mode, go to the **[edit protocols ptp]** hierarchy level:

```
[edit]
user@host# edit protocols ptp
```

2. Configure the clock mode as either boundary or ordinary. This attribute is mandatory and has no default value.

The **boundary** option signifies that the clock can be both a master clock and a slave clock. The **ordinary** option signifies that the clock is either a master clock or a slave clock.

```
[edit protocols ptp]
user@host# set clock-mode (boundary | ordinary)
```

3. Configure the profile type as enterprise. This attribute is mandatory.

```
[edit protocols ptp]
user@host# set profile-type enterprise-profile
```

4. (Optional) Configure the PTP domain option with values from 0 through 127. The default value is 0.

```
[edit protocols ptp]
user@host# set domain domain-value
```

5. (Optional) Configure the **priority1** option with values from 0 through 255. The default value is 128.

The **priority1** value determines the best master clock. The *priority1-value* is also advertised in the master clock's announce message to other slaves.

```
[edit protocols ptp]
user@host# set priority1 priority1-value
```

6. (Optional) Configure the **priority2** option with values from 0 through 255. The default value is 128.

The **priority2** value differentiates and prioritizes the master clock to avoid confusion when *priority1-value* is the same for different master clocks in a network.

```
[edit protocols ptp]
user@host# set priority2 priority2-value
```

Configuring Slave Clock Options

Configure the following options after the aforementioned PTP options have been set.

1. Configure the slave clock.

```
[edit protocols ptp]
user@host# edit slave
```

2. (Optional) Configure the **delay-request** option in the slave node with values from -7 through 7. The default value is 0.

The delay request value is the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.

```
[edit protocols ptp slave]
user@host# set delay-request delay-request-value
```

3. Configure the interface for the slave.

```
[edit protocols ptp slave]
user@host# set interface interface-name
```

4. Configure the **multicast-mode** option for the slave. You can set this option when PTP multicast mode of messaging is needed.

```
[edit protocols ptp slave interface interface-name]  
user@host# set multicast-mode
```

5. Configure the **transport** option in multicast mode as IPv4.

The encapsulation type for PTP packet transport is IPv4.

```
[edit protocols ptp slave interface interface-name multicast-mode]  
user@host# set transport ipv4
```

6. Configure the IP address of the local logical interface.

```
[edit protocols ptp slave interface interface-name multicast-mode]  
user@host# set local-ip-address IP address
```

Configuring Master Clock Options

Configure the following options after the aforementioned PTP options and slave clock options have been set.

1. Configure the master clock.

```
[edit protocols ptp]  
user@host# edit master
```

2. (Optional) Configure the **delay-req-timeout** option for the master.

The maximum timeout for delay request messages is between 30 and 300 seconds. We recommend 30 seconds.

```
[edit protocols ptp master]  
user@host# set delay-req-timeout seconds
```

3. Configure the interface for the master.

```
[edit protocols ptp master]  
user@host# set interface interface-name
```

4. Configure the **multicast-mode** option for the master. You can set this option when PTP multicast mode of messaging is needed.

```
[edit protocols ptp master interface interface-name]  
user@host# set multicast-mode
```

5. Configure the **transport** option in multicast mode as IPv4.

The encapsulation type for PTP packet transport is IPv4.

```
[edit protocols ptp master interface interface-name multicast-mode]  
user@host# set transport ipv4
```

6. Configure the IP address of the interface acting as the local PTP master port.

```
[edit protocols ptp master interface interface-name multicast-mode clock-client  
ip-address]
```

```
user@host# set local-ip-address local-ip-address
```

If the master clock connection is through a 1-Gigabit Ethernet interface, configure the interface named **ptp0** interface.

This interface is named **ptp0** by default.

- Related Documentation**
- *Precision Time Protocol Overview*
 - *Example: Configuring Precision Time Protocol*

Configuring Precision Time Protocol Clocking

In a distributed network, you can configure Precision Time Protocol (PTP) master and slave clocks to help synchronize the timing across the network. The synchronization is achieved through packets that are transmitted and received in a session between the master clock and the slave clock or clock client.

To configure Precision Time Protocol (PTP) options:

1. In configuration mode, go to the **[edit protocols ptp]** hierarchy level.

```
[edit]  
user@host# edit protocols ptp
```

2. Specify the clock as a boundary or ordinary clock. The **boundary** option signifies that the clock can be both a master clock and a slave clock. The **ordinary** option signifies that the clock is a slave clock.

```
[edit protocols ptp]  
user@host# set clock-mode (boundary | ordinary)
```

3. (Optional) Enable PHY Timestamping. The PHY timestamping is disabled by default.

```
[edit protocols ptp]  
user@host# set transparent-clock
```

4. (Optional) Configure the PTP domain with values from 0 through 127. The default value is 0.

```
[edit protocols ptp]  
user@host# set domain domain-value
```

5. (Optional) Specify the DiffServ code point (DSCP) value (0 through 63) for all PTP IPv4 packets originated by the router. The default value is 56.

```
[edit protocols ptp]  
user@host# set ipv4-dscp number
```

6. Specify the master clock parameters.

```
[edit protocols ptp]
```

```
user@host# set master
```

For details about configuring the master clock parameters, see [“Configuring a PTP Master Boundary Clock” on page 80](#).

7. (Optional) Configure the priority value of the clock (0 through 255). This value is used in selecting the best master clock. The *priority1-value* is advertised in the master clock's announce message to clock clients. The default value is 128.

```
[edit protocols ptp]
user@host# set priority1 priority1-value
```

8. (Optional) Configure the tie-breaker in selecting the best master clock (0 through 255). The **priority2** value differentiates and prioritizes the master clock to avoid confusion when the *priority1-value* is the same for different master clocks in a network. The default value is 128.

```
[edit protocols ptp]
user@host# set priority2 priority2-value
```

9. Specify the PTP slave clock parameters.

```
[edit protocols ptp]
user@host# set slave
```

For information about configuring the slave clock options, see [“Configuring a PTP Slave Clock” on page 90](#).

10. (Optional) Enable unicast negotiation. Unicast negotiation is a method by which the announce, synchronization, and delay response packet rates are negotiated between the master clock and the clock client before a PTP session is established.

```
[edit protocols ptp]
user@host# set unicast-negotiation
```



NOTE: Unicast negotiation, when enabled, does not allow you to commit packet rate–related configurations.

Related Documentation

- [IEEE 1588v2 PTP Boundary Clock Overview on page 58](#)
- [Configuring a PTP Master Boundary Clock on page 80](#)
- [Configuring a PTP Slave Clock on page 90](#)
- [Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 86](#)
- [Example: Configuring a PTP Boundary Clock on page 83](#)

Configuring a PTP Master Boundary Clock

A Precision Time Protocol (PTP) master boundary clock sends PTP messages to the clients (ordinary and boundary) so that they can establish their relative time offset from this master's clock or clock reference. You cannot configure an ordinary master clock on a device. The master boundary clock synchronizes time through a boundary slave port. To configure a master boundary clock, you must include the **boundary** statement at the **[edit protocols ptp clock-mode]** hierarchy level and at least one master with the **master** statement and at least one slave with the **slave** statement at the **[edit protocols ptp]** hierarchy level.



NOTE: ACX5048 and ACX5096 routers do not support ordinary and boundary clock.

To configure a PTP master boundary clock, complete the following tasks:

- [Configuring the PTP Master Boundary Clock Parameters on page 80](#)
- [Configuring a PTP Master Boundary Clock Interface on page 82](#)

Configuring the PTP Master Boundary Clock Parameters

To configure the parameters of a PTP master boundary clock:

1. Configure the clock mode.

```
[edit protocols ptp]  
user@host# set clock-mode boundary
```

2. Configure the master clock.

```
[edit protocols ptp]  
user@host# edit master
```

3. (Optional) Specify the log mean interval between announce messages—from 0 through 4. By default, one announce message is sent every two seconds. This configuration is used for manual clock clients. The master boundary clock sends announce messages to manual clock clients as specified in the announce-interval value.

```
[edit protocols ptp master]  
user@host# set announce-interval announce-interval-value
```

4. Configure the interface on which to respond to downstream PTP clients and slaves.

```
[edit protocols ptp master]  
user@host# edit interface interface-name
```

For details about configuring the parameters for the master boundary clock interface, see ["Configuring a PTP Master Boundary Clock Interface" on page 82](#)

5. (Optional) Specify the maximum log mean interval between announce messages—from 0 through 4. The default value is 4.

```
[edit protocols ptp master]
user@host# set max-announce-interval max-announce-interval-value
```
6. (Optional) Specify the maximum log mean interval between delay-response messages—from -7 through 4. The default value is 4.

```
[edit protocols ptp master]
user@host# set max-delay-response-interval max-delay-response-interval-value
```
7. (Optional) Specify the maximum log mean interval between synchronization messages—from -7 through 4. The default value is 4.

```
[edit protocols ptp master]
user@host# set max-sync-interval max-sync-interval-value
```
8. (Optional) Specify the minimum log mean interval between announce messages—from -0 through 4. The default value is 0.

```
[edit protocols ptp master]
user@host# set min-announce-interval min-announce-interval
```
9. (Optional) Specify the minimum log mean interval between delay-response messages—from -7 through 4. The default value is -7.

```
[edit protocols ptp master]
user@host# set min-delay-response-interval min-delay-response-interval
```
10. (Optional) Specify the minimum log mean interval between synchronization messages—from -7 through 4. The default value is -7.

```
[edit protocols ptp master]
user@host# set min-sync-interval min-sync-interval-value
```
11. (Optional) Specify the log mean interval between synchronization messages—from -7 through 4. The default value is -6. This configuration is used for manual clock clients. The master boundary clock sends synchronization messages to manual clock clients as specified in the **sync-interval-value** statement.

```
[edit protocols ptp master]
user@host# set sync-interval sync-interval-value
```

After you have configured the PTP master boundary clock parameters, enter the **commit** command from configuration mode. To complete the configuration of the master boundary clock, complete [“Configuring a PTP Master Boundary Clock Interface” on page 82](#).

Configuring a PTP Master Boundary Clock Interface

After you have configured the master boundary clock parameters, complete the configuration of the master boundary clock by configuring an interface to act in the role of the master clock.

To configure a PTP master boundary clock interface:

1. Configure the interface on which to respond to downstream PTP slaves or clients.

```
[edit protocols ptp master]
user@host# edit interface interface-name
```



NOTE: For the configuration to work, the interface you specify must be configured at the [edit interfaces *interface-name*] hierarchy level.

2. On this interface, configure downstream PTP clients.

```
[edit protocols ptp master interface interface-name]
user@host# edit unicast-mode
```

3. Configure the IP address of the remote PTP host, or configure a subnet mask so that any host belonging to that subnet can join the master clock. You can configure up to 512 clients for each master boundary clock.

```
[edit protocols ptp master interface interface-name unicast-mode]
user@host# edit clock-client ip-address
```



NOTE: You can configure the maximum number of clients (512) in the following combination:

- Automatic clients 256.
- Manual and secure clients 256—Any combination of manual and secure clients is allowed as long as the combined total amounts to 256.



NOTE: When you toggle from a secure slave to an automatic slave or vice versa in the PTP configuration of a boundary clock, you need to delete the existing PTP configuration and issue the commit command, and then you add a new PTP configuration and issue the commit command.

4. Configure the IP address of the interface acting as the local PTP master.

```
[edit protocols ptp master interface interface-name unicast-mode clock-client
ip-address]
user@host# set local-ip-address local-ip-address
```

5. (Optional) When the **unicast-negotiation** statement is configured at the `[edit protocols ptp]` hierarchy level, configure a clock client to immediately receive announce and synchronization messages from the master boundary clock without unicast negotiation.

```
[edit protocols ptp master interface interface-name unicast-mode clock-client ip-address
local-ip-address local-ip-address]
user@host# set manual
```

6. Specify the encapsulation type for PTP packet transport—IPv4. This statement is mandatory.

```
[edit protocols ptp master interface interface-name unicast-mode]
user@host# set transport ipv4
```

After you have configured the PTP master clock interface, enter the **commit** command from configuration mode.

- See Also**
- [Precision Time Protocol Overview](#)
 - [IEEE 1588v2 PTP Boundary Clock Overview on page 58](#)
 - [Configuring Precision Time Protocol Clocking on page 78](#)
 - [Configuring a PTP Slave Clock on page 90](#)
 - [Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 86](#)
 - [Example: Configuring a PTP Boundary Clock on page 83](#)

Example: Configuring a PTP Boundary Clock

This example shows how to configure a Precision Timing Protocol (PTP) boundary clock. A boundary clock must include the configuration of at least one master and at least one slave. The boundary master receives time from a remote master through the slave, and in turn passes that time on to clock clients, which are in a slave relationship to the boundary master. In this example, you configure a master, slave, clock source, and clock client.



NOTE: ACX5048 and ACX5096 routers do not support boundary clock.

- [Requirements on page 83](#)
- [Overview on page 84](#)
- [Configuration on page 84](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX Series switches. QFX Series switches do not support Gigabit Ethernet interfaces. Instead, configure PTP boundary clock parameters on 10-Gigabit Ethernet interfaces.

- An ACX Series router
- Junos OS Release 12.3 or later

Overview

In this example, the slave clock or clock client immediately receives announce and synchronization packets after completion of the configuration.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level:

```
set protocols ptp clock-mode boundary
set protocols ptp slave interface ge-1/3/9.0 unicast-mode transport ipv4
set protocols ptp slave interface ge-1/3/9.0 unicast-mode clock-source 192.1.1.2
  local-ip-address 192.1.1.1
set protocols ptp master interface ge-1/0/0.0 unicast-mode transport ipv4
set protocols ptp master interface ge-1/0/0.0 unicast-mode clock-client 20.20.20.2/32
  local-ip-address 20.20.20.1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a boundary clock without unicast negotiation:

1. Configure the clock mode.

```
[edit protocols ptp]
user@host# set clock-mode boundary
```

2. Configure the slave interface.

```
[edit protocols ptp]
user@host# edit slave interface ge-1/3/9.0
```

3. Configure the upstream unicast PTP master clock source parameters.

```
[edit protocols ptp slave interface ge-1/3/9.0]
user@host# edit unicast-mode
```

4. Configure the encapsulation type for PTP packet transport.

```
[edit protocols ptp slave interface ge-1/3/9.0 unicast-mode ]
user@host# set transport ipv4
```

5. Configure the IP address of the master interface.

```
[edit protocols ptp]
user@host# edit master interface ge-1/0/0.0
```

6. Specify the IP address and subnet of the remote PTP host, and the IP address of the local PTP master interface.

```
[edit protocols ptp master interface ge-1/0/0.0 ]
user@host# edit unicast-mode
user@host# set protocols ptp master interface ge-1/0/0.0 unicast-mode clock-client
20.20.20.2/32 local-ip-address 20.20.20.1
```



NOTE: For the configuration to work, the master interface you specify must be configured with this IP address at the `[edit interfaces interface-name]` hierarchy level.

7. Configure the encapsulation type for PTP packet transport.

```
[edit protocols ptp master interface ge-1/0/0.0 unicast-mode]
user@host# set transport ipv4
```

Results From configuration mode, confirm your configuration by entering the **show** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit protocols ptp]
user@host# show
clock-mode boundary;
slave {
  interface ge-1/3/9.0 {
    unicast-mode {
      transport ipv4;
      clock-source 192.1.1.2 local-ip-address 192.1.1.1;
    }
  }
}
master {
  interface ge-1/0/0.0 {
    unicast-mode {
      transport ipv4;
      clock-client 20.20.20.2/32 local-ip-address 20.20.20.1;
    }
  }
}
```

After you have configured the device, enter the **commit** command from configuration mode.

**Related
Documentation**

- [Precision Time Protocol Overview](#)
- [IEEE 1588v2 PTP Boundary Clock Overview on page 58](#)
- [Configuring Precision Time Protocol Clocking on page 78](#)
- [Configuring a PTP Master Boundary Clock on page 80](#)
- [Configuring a PTP Slave Clock on page 90](#)
- [Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 86](#)

Example: Configuring a PTP Boundary Clock With Unicast Negotiation

This example shows how to configure a boundary clock with unicast negotiation turned on and a mixture of manual, secure and automatic clock clients, which have a slave relationship to the master boundary clock. The unicast negotiation applies to clock sources, which are configured on the slave or clock client. Clock clients, configured on the master, are not affected by unicast negotiation.



NOTE: ACX5048 and ACX5096 routers do not support boundary clock.

In this example, unicast-negotiation is applicable only to clock-sources. For clock clients, the statement **unicast-negotiation** at the **[edit protocols ptp]** hierarchy level is not effective.

- [Requirements on page 86](#)
- [Overview on page 86](#)
- [Configuration on page 87](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX Series switches. QFX Series switches do not support Gigabit Ethernet interfaces. Instead, configure PTP boundary clock parameters on 10-Gigabit Ethernet interfaces.

- An ACX Series router
- Junos OS Release 12.3 or later

Overview

A PTP slave clock or clock client can join a master clock with and without unicast negotiation. With unicast negotiation, the announce, synchronization, and delay response

packet rates are negotiated between the master and the slave or client before a PTP session is established. Without unicast negotiation and after it is configured, the slave or client immediately receives announce and synchronization packets.

A clock client is the remote PTP host, which receives time from the PTP master. The following clock clients are configured in this example:

- **Secure client**—A secure client is configured with an exact IP address, after which, it joins a master clock through unicast negotiation. In this example, the clock client **clock-client 117.117.117.117/32 local-ip-address 109.109.109.53** is a secure client, which means that only this specific host from the subnet can join the master clock through a unicast negotiation.
- **Automatic client**—An automatic client is configured with an IP address, which includes a subnet mask, indicating that any PTP host belonging to that subnet, can join the master clock through a unicast negotiation. In this example, the clock client **clock-client 109.109.109.0/24 local-ip-address 109.109.109.53** is an automatic client. Additionally, this automatic client is configured on the same master clock interface—**109.109.109.53**—as the secure client.
- **Manual client**—A manual client does *not* use unicast negotiation to join the master clock. The **manual** statement overrides the **unicast-negotiation** statement configured at the **[edit protocols ptp]** hierarchy level. As soon as you configure a manual client, it starts receiving announce and synchronization packets. In this example, the clock client **clock-client 7.7.7.7 local-ip-address 7.7.7.53 manual** is the manual client and is configured on a second master clock interface.

Configuration

A boundary clock must include the configuration of at least one master and at least one slave. The boundary master receives time from a remote master through the slave, and in turn passes that time on to clock clients, which are in a slave relationship to the boundary master. In this example, you configure a boundary slave, two Precision Time Protocol (PTP) boundary masters with three different kinds of clock clients—automatic, manual, and secure. Two of the clock clients are configured on the same boundary master.

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level:

```
set protocols ptp clock-mode boundary
set protocols ptp unicast-negotiation
set protocols ptp slave interface ge-0/1/0.0 unicast-mode transport ipv4
set protocols ptp slave interface ge-0/1/0.0 unicast-mode clock-source 10.10.10.50
  local-ip-address 10.10.10.53
set protocols ptp master interface ge-0/1/3.0 unicast-mode transport ipv4
set protocols ptp master interface ge-0/1/3.0 unicast-mode clock-client 117.117.117.117/32
  local-ip-address 109.109.109.53
set protocols ptp master interface ge-0/1/3.0 unicast-mode clock-client 109.109.109.0/24
  local-ip-address 109.109.109.53
set protocols ptp master interface ge-0/1/5.0 unicast-mode transport ipv4
```

```
set protocols ptp master interface ge-0/1/5.0 unicast-mode clock-client 7.7.7.7/32
local-ip-address 7.7.7.53 manual
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a boundary clock with unicast negotiation:

1. Configure the clock mode.

```
[edit protocols ptp]
user@host# set clock-mode boundary
```

2. Enable unicast negotiation.

```
[edit protocols ptp]
user@host# set unicast-negotiation
```

3. Configure the local slave interface from which the boundary master receives time and passes it on to the configured clock clients.

```
[edit protocols ptp]
user@host# edit slave interface ge-0/1/0.0
```

4. Configure the upstream unicast PTP master clock source parameters.

```
[edit protocols ptp slave interface ge-0/1/0.0]
user@host# edit unicast-mode
```

5. Configure the encapsulation type for PTP packet transport.

```
[edit protocols ptp slave interface ge-0/1/0.0 unicast-mode ]
user@host# set transport ipv4
```

6. Configure the PTP master parameters by specifying the IP address of the PTP master clock and the IP address of the local interface.

```
[edit protocols ptp slave interface ge-0/1/0.0 unicast-mode ]
user@host# set clock-source 10.10.10.50 local-ip-address 10.10.10.53
```

7. Configure the first master interface in this example.

```
[edit protocols ptp]
user@host# edit master interface ge-0/1/3.0
```

8. On the first master interface, configure the downstream PTP clock clients.

```
[edit protocols ptp master interface ge-0/1/3.0 ]
user@host# edit unicast-mode
```

9. On the first master interface, configure the encapsulation type for PTP packet transport.


```
[edit protocols ptp master interface ge-0/1/3.0 unicast-mode]
user@host# set transport ipv4
```

10. On the first master interface, configure the PTP master parameters by specifying the exact IP address of the remote PTP host and the IP address of the local PTP master interface.

```
[edit protocols ptp master interface ge-0/1/3.0 unicast-mode]
user@host# set clock-client 117.117.117.117 local-ip-address 109.109.109.53
```

11. On the first master interface, configure a second PTP master by specifying the IP address and subnet of the second remote PTP host and the IP address of the local PTP master interface.

```
[edit protocols ptp master interface ge-0/1/3.0 unicast-mode]
user@host# set clock-client 109.109.109.0/24 local-ip-address 109.109.109.53
```

12. Configure the second master interface with the following parameters: the encapsulation type, the downstream PTP host, the IP address of the local PTP master interface, and the **manual** statement so that this client does not use unicast negotiation.

```
[edit protocols ptp master]
user@host# set interface ge-0/1/5.0 unicast-mode transport ipv4
user@host# set interface ge-0/1/5.0 unicast-mode clock-client 7.7.7
local-ip-address 7.7.53 manual
```

Results From configuration mode, confirm your configuration by entering the **show** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit protocols ptp]
user@host# show
clock-mode boundary;
unicast-negotiation;
slave {
  interface ge-0/1/0.0 {
    unicast-mode {
      transport ipv4;
      clock-source 10.10.10.50 local-ip-address 10.10.10.53;
    }
  }
}
master {
  interface ge-0/1/3.0 {
    unicast-mode {
      transport ipv4;
      clock-client 117.117.117.117/32 local-ip-address 109.109.109.53;
      clock-client 109.109.109.0/24 local-ip-address 109.109.109.53;
    }
  }
  interface ge-0/1/5.0 {
    unicast-mode {
```

```
        transport ipv4;  
        clock-client 7.7.7.7/32 local-ip-address 7.7.7.53 {  
            manual;  
        }  
    }  
}
```

After you have configured the device, enter the **commit** command from configuration mode.

**Related
Documentation**

- [Precision Time Protocol Overview](#)
- [IEEE 1588v2 PTP Boundary Clock Overview on page 58](#)
- [Configuring Precision Time Protocol Clocking on page 78](#)
- [Configuring a PTP Master Boundary Clock on page 80](#)
- [Configuring a PTP Slave Clock on page 90](#)
- [Example: Configuring a PTP Boundary Clock on page 83](#)

Configuring a PTP Slave Clock

The slave port that you configure can be a Precision Time Protocol (PTP) boundary or ordinary clock, depending on the configuration of the **clock-mode** statement at the **[edit protocols ptp]** hierarchy level. An ordinary or boundary slave clock performs frequency and phase recovery based on received and requested timestamps from a master clock—a grandmaster or a boundary clock master.



NOTE: In ACX Series routers, the grandmaster functionality is supported only on ACX500 router.

To configure a PTP slave clock, complete the following tasks:

- [Configuring the PTP Slave Clock Parameters on page 90](#)
- [Configuring the PTP Slave Clock Interface on page 92](#)

Configuring the PTP Slave Clock Parameters

To configure a PTP slave clock.



NOTE: The **clock-class-to-quality-level-mapping quality-level**, **convert-clock-class-to-quality-level**, and **grant-duration** statements are not supported on the QFX10002 switch.

1. Configure the clock mode:

```
[edit protocols ptp]
user@host# set clock-mode (boundary | ordinary)
```

2. Configure the slave clock.

```
[edit protocols ptp]
user@host# edit slave
```

3. (Optional) Specify the rate of announce messages that a PTP slave requests from the master during a unicast-negotiation session—from 0 through 4. The default value is 1.

```
[edit protocols ptp slave]
user@host# set announce-interval announce-interval-value
```



NOTE: The configuration of the `announce-interval` statement is effective only when the `unicast-negotiation` statement is also configured at the `[edit protocols ptp]` hierarchy level.

4. (Optional) Specify the number of announce messages that a slave—configured on an ACX Series router—must miss before an announce timeout is declared—from 2 through 10. The default value is 3.

```
[edit protocols ptp slave]
user@host# set announce-timeout announce-timeout-value
```

5. (Optional) Override the default PTP clock class to Ethernet Synchronization Message Channel (ESMC) mapping and specify the quality level for the PTP timing source.

```
[edit protocols ptp slave]
user@host# set clock-class-to-quality-level-mapping quality-level (prc | prs | sec |
smc | ssu-a | ssu-b | st2 | st3 | st3e | st4 | stu | tnc)
```

6. (Optional) Enable retrieval of ESMC information from the PTP clock class.

```
[edit protocols ptp slave]
user@host# set convert-clock-class-to-quality-level
```

7. (Optional) Specify the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master—from -6 through 3. The default value is 0.

```
[edit protocols ptp slave]
user@host# set delay-request delay-request-value
```

8. (Optional) Specify the grant duration value. When unicast negotiation is enabled, the local PTP slave requests announce, synchronization, and delay-response messages from the master. In each request, the slave asks for the packets to be sent at a specified rate and the slave provides a duration for which the rate is valid. The grant-duration value is specified in seconds. The default grant duration is 300 seconds.

```
[edit protocols ptp slave]
user@host# set grant-duration interval
```

9. Configure the interface for the slave.

```
[edit protocols ptp slave]
user@host# edit interface interface-name
```

For details about configuring the slave interface, see [“Configuring the PTP Slave Clock Interface” on page 92](#).

10. (Optional) Configure the log mean interval between synchronization messages—from –6 through –3. The default value is –6 or 64 synchronous interval messages sent per second

```
[edit protocols ptp slave]
user@host# set sync-interval sync-interval-value
```

After you have configured the PTP slave clock parameters, enter the **commit** command from configuration mode. To complete the configuration of the slave clock, complete [“Configuring the PTP Slave Clock Interface” on page 92](#).

Configuring the PTP Slave Clock Interface

The slave clock interface responds to the upstream PTP master clock.

To configure the PTP slave clock interface:

1. Configure the interface for the slave clock.

```
[edit protocols ptp slave]
user@host# edit interface interface-name
```

2. Configure the upstream unicast PTP master clock source parameters.

```
[edit protocols ptp slave interface interface-name]
user@host# edit unicast-mode
```

3. Configure the IP address of the master, which acts as a source of time for this slave.

```
[edit protocols ptp slave interface interface-name unicast-mode]
user@host# edit clock-source ip-address
```



NOTE: To configure additional master clock sources for the slave, include the **clock-source** statement up to four times. However, synchronization is to only one master clock.

4. Specify the IP address of the interface acting as the local PTP slave port.

```
[edit protocols ptp slave interface interface-name unicast-mode clock-source ip-address]
user@host# set local-ip-address local-ip-address
```



NOTE: For the configuration to work, the interface you specify must be configured with this IP address at the [edit interfaces *interface-name*] hierarchy level.

5. Configure the encapsulation type for PTP packet transport. This statement is mandatory.

```
[edit protocols ptp slave interface interface-name unicast-mode]
user@host# set transport ipv4
```

After you have configured the PTP slave clock interface, enter the **commit** command from configuration mode.

- See Also**
- [Precision Time Protocol Overview](#)
 - [IEEE 1588v2 PTP Boundary Clock Overview on page 58](#)
 - [Configuring Precision Time Protocol Clocking on page 78](#)
 - [Configuring a PTP Master Boundary Clock on page 80](#)
 - [Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 86](#)
 - [Example: Configuring a PTP Boundary Clock on page 83](#)

Example: Configuring an Ordinary Slave Clock With Unicast-Negotiation

This example shows the base configuration of a Precision Time Protocol (PTP) ordinary slave clock *with* unicast-negotiation on an ACX Series router.



NOTE: ACX5048 and ACX5096 routers do not support ordinary clock.

- [Requirements on page 93](#)
- [Overview on page 94](#)
- [Configuration on page 94](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX Series switches. QFX Series switches do not support Gigabit Ethernet interfaces. Instead, configure PTP boundary clock parameters on 10-Gigabit Ethernet interfaces.

- One ACX Series router

- Junos OS Release 12.2 or later

Overview

In this configuration, the ordinary slave clock uses unicast-negotiation and compensates for some network asymmetry.



NOTE: The values in this example are for illustration purposes only. You can set the values for each parameter according to your requirements.

Configuration

To configure an ordinary slave clock with unicast-negotiation, perform these tasks:

- [Configuring an ordinary slave clock with unicast-negotiation on page 94](#)
- [Results on page 95](#)

CLI Quick Configuration

```
set ptp clock-mode ordinary
set ptp domain 110
set ptp unicast-negotiation
set ptp slave delay-request -6
set ptp slave announce-timeout 2
set ptp slave announce-interval 3
set ptp slave sync-interval -5
set ptp slave grant-duration 7200
set ptp slave interface ge-0/1/0.0 unicast-mode transport ipv4
set ptp slave interface ge-0/1/0.0 unicast-mode clock-source 10.10.10.50
local-ip-address 10.10.10.75 asymmetry -4500
```

Configuring an ordinary slave clock with unicast-negotiation

Step-by-Step Procedure

1. Configure the clock mode, domain, and unicast-negotiation:

```
[edit protocols ptp]
user@host# set clock-mode ordinary domain 110 unicast-negotiation
```
2. Configure the announce timeout and the announce interval:

```
[edit protocols ptp]
user@host# set slave announce-timeout 2 announce-interval 3
```
3. Configure the synchronization interval and the grant duration:

```
[edit protocols ptp]
user@host# set slave sync-interval -5 grant-duration 7200
```
4. Configure the slave interface:

```
[edit protocols ptp]
user@host# edit slave interface ge-0/1/0.0
```

5. Configure the unicast transport mode:

```
[edit protocols ptp slave interface ge-0/1/0.0]
user@host# set unicast-mode transport ipv4
```

6. Configure the clock source:

```
[edit protocols ptp slave interface ge-0/1/0.0]
user@host# edit unicast-mode clock-source 10.10.10.50 local-ip-address 10.10.10.75
```

7. Configure the asymmetric path:

```
[edit protocols ptp slave interface ge-0/1/0.0 unicast-mode clock-source 10.10.10.50
local-ip-address 10.10.10.75]
user@host# set asymmetry -4500
```

8. Verify the configuration:

```
[edit protocols ptp slave interface ge-0/1/0.0 unicast-mode clock-source 10.10.10.50
local-ip-address 10.10.10.75]
user@host# top
[edit]
user@host# edit protocols
[edit protocols]
user@host# show
```

See the output for the **show** command in the Results section.

Results

The following output shows the configuration of unicast-negotiation and compensation for some network asymmetry. The **unicast-negotiation** statement includes the parameters for the delay request, announce interval, synchronization interval, and grant duration values. Interface **ge-0/1/0.0** is configured to compensate for an asymmetric path to the PTP master by subtracting 4.5 microseconds from the slave-to-master direction delay calculations.

```
[edit protocols]
user@host# show
ptp {
  clock-mode ordinary;
  domain 110;
  unicast-negotiation;
  slave {
    delay-request -6;
    announce-timeout 2;
    announce-interval 3;
    sync-interval -5;
    grant-duration 7200;
    interface ge-0/1/0.0 {
      unicast-mode {
        transport ipv4;
        clock-source 10.10.10.50 local-ip-address 10.10.10.75 {
          asymmetry -4500;
        }
      }
    }
  }
}
```

```

    }
  }
}

```

Related Documentation

- [IEEE 1588v2 Precision Timing Protocol \(PTP\) on ACX Series Universal Access Routers on page 61](#)
- [slave on page 131](#)
- *unicast-mode*

Example: Configuring an Ordinary Slave Clock Without Unicast-Negotiation

This example shows the base configuration of a Precision Time Protocol (PTP) ordinary slave clock *without* unicast-negotiation on an ACX Series router.



NOTE: ACX5048 and ACX5096 routers do not support ordinary clock.

- [Requirements on page 96](#)
- [Overview on page 96](#)
- [Configuration on page 97](#)

Requirements

This example uses the following hardware and software components:



NOTE: This example also applies to QFX Series switches. QFX Series switches do not support Gigabit Ethernet interfaces. Instead, configure PTP boundary clock parameters on 10-Gigabit Ethernet interfaces.

- One ACX Series router
- Junos OS Release 12.2 or later

Overview

In this configuration, unicast-negotiation is *not* configured, so the PTP slave has no control over the rate of the negotiation. The PTP master (a Brilliant Grand Master or an MX Series router) must be configured with the parameters of the PTP slave, such as announce, synchronization, and delay-response packets to control the rate of the negotiation.



NOTE: The values in this example are for illustration purposes only. You can set the values for each parameter according to your requirements.

Configuration

To configure an ordinary slave clock without unicast-negotiation, perform these tasks:



NOTE: The `ipv4-dscp` statement is not supported on the QFX10002 switch.

- [Configuring an ordinary slave clock without unicast-negotiation on page 97](#)
- [Results on page 98](#)

CLI Quick Configuration

```
set protocols ptp clock-mode ordinary
set protocols ptp ipv4-dscp 46
set protocols ptp slave interface ge-0/2/0.0 unicast-mode transport ipv4
set protocols ptp slave interface ge-0/2/0.0 unicast-mode clock-source 12.1.1.4
local-ip-address 12.1.1.5
```

Configuring an ordinary slave clock without unicast-negotiation

Step-by-Step Procedure

1. Configure the clock mode:

```
[edit protocols ptp]
user@host# set clock-mode ordinary
```
2. Configure the Differentiated Services code point (DSCP) value for all PTP IPv4 packets originated by the device:



NOTE: The `ipv4-dscp 46` statement is not supported on QFX Series switches.

```
[edit protocols ptp]
user@host# set ipv4-dscp 46
```

3. Configure the slave interface:

```
[edit protocols ptp]
user@host# edit slave interface ge-0/2/0.0
```
4. Configure the unicast transport mode:

```
[edit protocols ptp slave interface ge-0/2/0.0]
user@host# set unicast-mode transport ipv4
```
5. Configure the clock source:

```
[edit protocols ptp slave interface ge-0/2/0.0]
user@host# unicast-mode clock-source 12.1.1.4 local-ip-address 12.1.1.5
```

6. Verify the configuration:

```
[edit protocols ptp slave interface ge-0/2/0.0]
user@host# top
[edit]
user@host# edit protocols
[edit protocols]
user@host# show
```

See the output for the **show** command in the Results section.

Results

In this example, the PTP slave on the local interface **ge-0/2/0** is assigned a local IP address of **12.1.1.5**. Unicast-negotiation is not configured so the PTP master must be explicitly configured with the details of the PTP slave (12.1.1.5).

```
[edit protocols]
user@host# show
ptp {
  clock-mode ordinary;
  ipv4-dscp 46;
  slave {
    interface ge-0/2/0.0 {
      unicast-mode {
        transport ipv4;
        clock-source 12.1.1.4 local-ip-address 12.1.1.5;
      }
    }
  }
}
```

Related Documentation

- [IEEE 1588v2 Precision Timing Protocol \(PTP\) on ACX Series Universal Access Routers on page 61](#)
- [slave on page 131](#)
- [unicast-mode](#)

CHAPTER 5

Configuration Statements

- [System Management Configuration Statements on page 100](#)
- [asymmetry on page 107](#)
- [authentication-key on page 108](#)
- [authentication-key on page 109](#)
- [boot-server \(NTP\) on page 110](#)
- [boot-server \(NTP\) on page 111](#)
- [broadcast on page 112](#)
- [broadcast on page 113](#)
- [broadcast-client on page 114](#)
- [broadcast-client on page 114](#)
- [clock-client on page 115](#)
- [clock-mode on page 116](#)
- [clock-source \(PTP Unicast Slave Interface\) on page 117](#)
- [e2e-transparent on page 118](#)
- [interface \(PTP Slave\) on page 119](#)
- [local-priority on page 120](#)
- [local-ip-address \(multicast or unicast mode\) on page 121](#)
- [master on page 122](#)
- [multicast-client on page 123](#)
- [multicast-mode \(PTP Master and Slave Interfaces\) on page 124](#)
- [ntp on page 125](#)
- [ntp \(QFabric\) on page 126](#)
- [peer \(NTP\) on page 127](#)
- [profile-type on page 128](#)
- [server \(NTP\) on page 130](#)
- [slave on page 131](#)
- [source-address \(NTP, RADIUS, System Logging, or TACACS+\) on page 133](#)
- [source-address \(NTP, RADIUS, System Logging, or TACACS+\) on page 134](#)

- [system](#) on page 135
- [time-zone](#) on page 136
- [transport ipv4](#) (PTP Unicast Master and Slave Interface) on page 138
- [trusted-key](#) on page 139
- [unicast-mode](#) (PTP Slave Interface) on page 140
- [use-imported-time-zones](#) on page 140

System Management Configuration Statements

This topic lists all the configuration statements that you can include at the **[edit system]** hierarchy level to configure system management features:

```
system {
  accounting {
    destination {
      radius {
        server {
          server-address {
            accounting-port port-number;
            retry number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
    }
    tacplus {
      server {
        server-address {
          port port-number;
          secret password;
          single-connection;
          timeout seconds;
        }
      }
    }
  }
  enhanced-avs-max;
  events [ login change-log interactive-commands ];
}
archival {
  configuration {
    archive-sites {
      ftp://<username>:<password>@<host>:<port>/<url-path>;
      ftp://<username>:<password>@<host>:<port>/<url-path>;
    }
    transfer-interval interval;
    transfer-on-commit;
  }
}
allow-v4mapped-packets;
arp {
  aging-timer minutes;
```

```

    gratuitous-arp-delay;
    gratuitous-arp-on-ifup;
    interfaces;
    passive-learning;
    purging;
}
authentication-order [ authentication-methods ];
backup-router address <destination destination-address>;
commit {
    delta-export;
    fast-synchronize;
    persist-groups-inheritance ;
    server;
    synchronize
}
synchronize;
(compress-configuration-files | no-compress-configuration-files);
default-address-selection;
dump-device (compact-flash | remove-compact | usb);
diag-port-authentication (encrypted-password "password" | plain-text-password);
dynamic-profile-options {
    versioning;
}
domain-name domain-name;
domain-search [ domain-list ];
host-name hostname;
inet6-backup-router address <destination destination-address>;
internet-options {
    tcp-mss mss-value;
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
    icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
    ipv6-path-mtu-discovery-timeout;
    no-tcp-rfc1323-paws;
    no-tcp-rfc1323;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-port upper-limit <upper-limit>;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
}
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}

```

```

login {
    announcement text;
    class class-name {
        access-end;
        access-start;
        allow-commands "regular-expression";
        ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular
            expression 2";
        allowed-days;
        deny-commands "regular-expression";
        ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular
            expression 2";
        idle-timeout minutes;
        login-script
        login-tip;
        permissions [ permissions ];
    }
    message text;
    password {
        change-type (set-transitions | character-set);
        format (md5 | sha1 | des);
        maximum-length length;
        minimum-changes number;
        minimum-length length;
    }
    retry-options {
        backoff-threshold number;
        backoff-factor seconds;
        minimum-time seconds;
        tries-before-disconnect number;
    }
    user username {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication {
            (encrypted-password "password" | plain-text-password);
            ssh-rsa "public-key";
            ssh-dsa "public-key";
        }
    }
}
login-tip number;
mirror-flash-on-disk;
name-server {
    address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
    authentication-key key-number type type value password;
    boot-server address;
    broadcast <address> <key key-number> <version value> <tll value>;
    broadcast-client;

```

```

multicast-client <address>;
peer address <key key-number> <version value> <prefer>;
source-address source-address;
server address <key key-number> <version value> <prefer>;
trusted-key [ key-numbers ];
}
ports {
  auxiliary {
    type terminal-type;
  }
  pic-console-authentication {
    encrypted-password encrypted-password;
    plain-text-password;
    console {
      insecure;
      log-out-on-disconnect;
      type terminal-type;
      disable;
    }
  }
}
processes {
  process--name (enable | disable) failover (alternate-media | other-routing-engine);
  timeout seconds;
}
}
radius-server server-address {
  accounting-port port-number;
  port port-number;
  retry number;
  secret password;
  source-address source-address;
  timeout seconds;
}
radius-options {
  enhanced-accounting
  password-protocol mschap-v2;
}
attributes {
  nas-ip-address ip-address;
}
enhanced-accounting;
password-protocol mschap-v2;
}
root-authentication {
  (encrypted-password "password" | plain-text-password);
  ssh-rsa "public-key";
  ssh-dsa "public-key";
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
scripts {
  commit {
    allow-transients;
    file filename {
      optional;
      refresh;
    }
  }
}

```

```

        refresh-from url;
        source url;
    }
    traceoptions {
        file <filename> <files number> <size size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
op {
    file filename {
        arguments {
            argument-name {
                description descriptive-text;
            }
        }
        command filename-alias;
        description descriptive-text;
        refresh;
        refresh-from url;
        source url;
    }
    refresh;
    refresh-from url;
    traceoptions {
        file <filename> <files number> <size size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
}
services {
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    flow-tap-dtcp {
        ssh {
            connection-limit limit;
            rate-limit limit;
        }
    }
    ftp {
        connection-limit limit;
        rate-limit limit;
    }
    rest {
        control {
            allowed-sources [ value-list ];
            connection-limit limit;
        }
        enable-explorer;
        http {
            addresses [ addresses ];
            port port-number;
        }
        https {

```



```

    addresses [ addresses ];
    cipher-list [ cipher-1 cipher-2 cipher-3 ... ];
    mutual-authentication {
        certificate-authority certificate-authority-profile-name;
    }
    port port-number;
    server-certificate local-certificate-identifier;
}
traceoptions {
    flag flag;
}
}
service-deployment {
    servers server-address {
        port port-number;
    }
    source-address source-address;
}
ssh {
    root-login (allow | deny | deny-password);
    protocol-version [v1 v2];
    connection-limit limit;
    rate-limit limit;
}
telnet {
    connection-limit limit;
    rate-limit limit;
}
web-management {
    http {
        interfaces [ interface-names ];
        port port;
    }
    https {
        interfaces [ interface-names ];
        local-certificate name;
        port port;
    }
    session {
        idle-timeout [ minutes ];
        session-limit [ session-limit ];
    }
}
xnm-clear-text {
    connection-limit limit;
    rate-limit limit;
}
xnm-ssl {
    connection-limit limit;
    local-certificate name;
    rate-limit limit;
}
}
static-host-mapping {
    hostname {
        alias [ alias ];
    }
}

```

```

    inet [ address ];
    sysid system-identifier;
  }
}
syslog {
  archive <files number> <size size> <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    match-string string-name;
    structured-data {
      brief;
    }
  }
}
host (hostname | other-routing-engine | scc-master) {
  facility severity;
  explicit-priority;
  facility-override facility;
  log-prefix string;
  match "regular-expression";
  source-address source-address;
  structured-data {
    brief;
  }
}
source-address source-address;
time-format (year | millisecond | year millisecond);
user (username | *) {
  facility severity;
  match "regular-expression";
}
}
tacplus-options {
  enhanced-accounting;
  service-name service-name;
  (no-cmd-attribute-value | exclude-cmd-attribute);
}
tacplus-server server-address {
  secret password;
  single-connection;
  source-address source-address;
  timeout seconds;
}
time-zone (GMThour-offset | time-zone);
}
tracing {
  destination-override {
    syslog host;
  }
}

```

```

    }
    use-imported-time-zones;
  }

```

asymmetry

| | |
|---------------------------------|---|
| Syntax | <code>asymmetry <i>number</i></code> |
| Hierarchy Level | <p>For ACX Series and QFX Series:</p> <pre>[edit protocols ptp slave <i>interface</i> <i>unicast-mode</i> <i>clock-source</i> <i>local-ip-address</i>]</pre> <p>For MX Series:</p> <pre>[edit protocols ptp <i>slave</i> interface <i>interface-name</i> <i>multicast-mode</i>], [edit protocols ptp <i>master</i> interface <i>interface-name</i> <i>multicast-mode</i>]</pre> |
| Release Information | <p>Statement introduced in Junos OS Release 15.2 for MX Series routers.</p> <p>Statement introduced in Junos OS Release 17.3 for QFX Series switches.</p> |
| Description | <p>Specify the asymmetry value between the master and the slave. A compensating value for networks in which there is path asymmetry between the 1588v2 slave and master. Specify a positive or negative value that is added to the path delay value from the slave to the master, making the delay symmetric and equal to the path from the master to the slave.</p> |
| Options | <p>number—The asymmetry value is in nanoseconds and can vary from minus (–)100 milliseconds to 100 milliseconds, allowing compensation for up to 1/10 of a second of path asymmetry.</p> |
| Required Privilege Level | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • IEEE 1588v2 Precision Timing Protocol (PTP) on ACX Series Universal Access Routers on page 61 • <i>Precision Time Protocol Overview</i> • <i>Configuring Precision Time Protocol</i> • <i>Example: Configuring Precision Time Protocol</i> |

authentication-key

| | |
|---------------------------------|--|
| Syntax | <code>authentication-key <i>key-number</i> type <i>type</i> value <i>password</i>;</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | <p>Configure Network Time Protocol (NTP) authentication keys so that the router or switch can send authenticated packets. If you configure the router or switch to operate in authenticated mode, you must configure a key.</p> <p>Both the keys and the authentication scheme (MD5) must be identical between a set of peers sharing the same key number.</p> |
| Options | <p><i>key-number</i>—Positive integer that identifies the key.</p> <p><i>type type</i>—Authentication type. It can only be md5.</p> <p><i>value password</i>—The key itself, which can be from 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Configuring NTP Authentication Keys on page 31• broadcast on page 112• peer on page 127• server on page 130• trusted-key on page 139 |

authentication-key

| | |
|---------------------------------|--|
| Syntax | <code>authentication-key <i>key-number</i> type <i>type</i> value <i>password</i>;</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | <p>Configure Network Time Protocol (NTP) authentication keys so that the router or switch can send authenticated packets. If you configure the router or switch to operate in authenticated mode, you must configure a key.</p> <p>Both the keys and the authentication scheme (MD5) must be identical between a set of peers sharing the same key number.</p> |
| Options | <p><i>key-number</i>—An integer in the range of 1 to 65533.</p> <p><i>type type</i>—Authentication type. It can only be md5.</p> <p><i>value password</i>—Key itself, consisting of 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Understanding NTP Time Servers on page 22 • Configuring NTP Authentication Keys on page 40 |

boot-server (NTP)

| | |
|---------------------------------|--|
| Syntax | <code>boot-server (address hostname);</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | <p>Configure the server that NTP queries when the router or switch boots to determine the local date and time.</p> <p>When you boot the router or switch, it issues an ntpdate request, which polls a network server to determine the local date and time. You need to configure a server that the router or switch uses to determine the time when the router or switch boots. You can either configure an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the ntpdate request resolves the hostname to an IP address when the router or switch boots up.</p> <p>If you configure an NTP boot server, then when the router or switch boots, it immediately synchronizes with the boot server even if the NTP process is explicitly disabled or if the time difference between the client and the boot server exceeds the threshold value of 1000 seconds.</p> |
| Options | <ul style="list-style-type: none">• address—The IP address of an NTP boot server.• hostname—The hostname of an NTP boot server. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the NTP Boot Server on page 24 |

boot-server (NTP)

| | |
|---------------------------------|--|
| Syntax | <code>boot-server (address hostname);</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | <p>Configure the server that NTP queries when the router or switch boots to determine the local date and time.</p> <p>When you boot the router or switch, it issues an ntpdate request, which polls a network server to determine the local date and time. You need to configure a server that the router or switch uses to determine the time when the router or switch boots. Otherwise, NTP cannot synchronize to a time server if the server time significantly differs from the local router's or switch's time. You can configure either an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the ntpdate request resolves the hostname to an IP address when the router or switch boots up.</p> |
| Options | <ul style="list-style-type: none"> • address—IP address of an NTP boot server. • hostname—Hostname of an NTP boot server. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Understanding NTP Time Servers on page 22 • Configuring NTP Authentication Keys on page 40 • Synchronizing and Coordinating Time Distribution Using NTP on page 47 |

broadcast

| | |
|--------------------------|---|
| Syntax | <code>broadcast address <key key-number> <routing-instance-name routing-instance-name> <tll value> <version value>;</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. routing-instance-name option added in Junos OS Release 14.1 |
| Description | Configure the local router or switch to operate in broadcast mode with the remote system at the specified address . In this mode, the local router or switch sends periodic broadcast messages to a client population at the specified broadcast or multicast address . Normally, you include this statement only when the local router or switch is operating as a transmitter. |
| Options | <p>address—The broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be 224.0.1.1.</p> <p>key key-number—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.</p> <p>Range: Any unsigned 32-bit integer</p> <p>routing-instance-name routing-instance-name—(Optional) The routing instance name in which the interface has address in the broadcast subnet.</p> <p>Default: The default routing instance is used to broadcast packets.</p> <p>tll value—(Optional) Time-to-live (TTL) value to use.</p> <p>Range: 1 through 255</p> <p>Default: 1</p> <p>version value—(Optional) Specify the version number to be used in outgoing NTP packets.</p> <p>Range: 1 through 4</p> <p>Default: 4</p> |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the NTP Time Server and Time Services on page 27 |

broadcast

| | |
|---------------------------------|---|
| Syntax | <code>broadcast address <key key-number> <version value> <tll value>;</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Configure the local router or switch to operate in broadcast mode with the remote system at the specified address to send periodic broadcast messages to a client population. Normally, you include this statement only when the local router or switch is operating as a transmitter. |
| Options | <p>address—Broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be 224.0.1.1.</p> <p>key key-number—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number (any unsigned 32-bit integer).</p> <p>tll value—(Optional) Time-to-live (TTL) value to use. Range: 1 through 255 Default: 1</p> <p>version value—(Optional) Specify the version number to be used in outgoing NTP packets. Range: 1 through 4 Default: 4</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Understanding NTP Time Servers on page 22 • Configuring NTP Authentication Keys on page 40 • Configuring the NTP Time Server and Time Services on page 42 |

broadcast-client

| | |
|---------------------------------|--|
| Syntax | broadcast-client; |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure the local router or switch to listen for broadcast messages on the local network to discover other servers on the same subnet. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the Router or Switch to Listen for Broadcast Messages Using NTP on page 32 |


broadcast-client

| | |
|---------------------------------|---|
| Syntax | broadcast-client; |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Configure the local switch to listen for broadcast messages on the local network to discover other servers on the same subnet. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Understanding NTP Time Servers on page 22• Configuring NTP Authentication Keys on page 40• Configuring the Switch to Listen for Broadcast Messages Using NTP on page 46 |

clock-client

| | |
|---------------------------------|---|
| Syntax | <code>clock-client <i>ip-address</i>;</code> <code>local-ip-address <i>local-ip-address</i>;</code> |
| Hierarchy Level | [edit protocols ptp master interface <i>interface-name</i> unicast-mode transport ipv4] |
| Release Information | Statement introduced in Junos OS Release 12.2. Statement introduced in Junos OS Release 17.3 for the QFX Series. |
| Description | Configure the IP address of the slave. The remaining statement is explained separately. See CLI Explorer . |
| Options | <i>ip-address</i> —The IP address for the slave. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• <i>Configuring Precision Time Protocol</i>• <i>Example: Configuring Precision Time Protocol</i>• <i>Precision Time Protocol Overview</i>• Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |


clock-mode

| | |
|---------------------------------|--|
| Syntax | clock-mode (boundary ordinary); |
| Hierarchy Level | [edit protocols ptp] |
| Release Information | Statement introduced in Junos OS Release 12.2. Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access Routers. Statement introduced in Junos OS Release 17.3 for the QFX Series. |
| Description | Configure the clock mode as either boundary clock or ordinary clock. The clock mode determines whether the node is going to act as a slave, master, or both. This attribute is mandatory and has no default value. |
| Options | boundary —The clock mode of the node is a boundary clock where the clock acts as both master and slave. <div> NOTE: A boundary clock is not supported on the ACX Series routers for 12.2.</div> ordinary —The clock mode of the node is a system clock where the clock acts either as a master or as a slave. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring Precision Time Protocol• Example: Configuring Precision Time Protocol• Precision Time Protocol Overview• IEEE 1588v2 Precision Timing Protocol (PTP) on ACX Series Universal Access Routers on page 61• Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |

clock-source (PTP Unicast Slave Interface)

| | |
|---------------------------------|---|
| Syntax | <pre>clock-source <i>ip-address</i> { local-ip-address <i>local-ip-address</i>; asymmetry <i>number</i>; }</pre> |
| Hierarchy Level | <p>[edit protocols ptp slave interface <i>interface-name</i> unicast-mode]</p> <p>[edit protocols ptp slave interface <i>interface-name</i> multicast-mode]</p> |
| Release Information | <p>Statement introduced in Junos OS Release 12.2.</p> <p>Statement introduced in Junos OS Release 17.3 for the QFX Series.</p> |
| Description | <p>Configure the parameters of the Precision Time Protocol (PTP) master—clock source—to which this slave synchronizes. You can configure up to four clock sources for one interface, or one clock source for each of four different interfaces.</p> |
| Options | <p><i>ip-address</i>—IP address of the PTP master.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p> |
| Required Privilege Level | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • IEEE 1588v2 Precision Timing Protocol (PTP) on ACX Series Universal Access Routers on page 61 • Precision Time Protocol Overview • Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |


e2e-transparent

| | |
|---------------------------------|--|
| Syntax | e2e-transparent; |
| Hierarchy Level | [edit protocols ptp] |
| Release Information | Statement introduced in Junos OS Release 14.1X53-D25 for the QFX Series. Statement introduced in Junos OS Release 15.1X54-D20 for the ACX5048 and ACX5096 routers. |
| Description | Configure the end-to-end (E2E) transparent clock for Precision Time Protocol (PTP). With an end-to-end transparent clock, only the residence time is included in the timestamp in the packet. Transparent clock functionality is supported on PTP over Ethernet, IPv4, IPv6, unicast, and multicast. With PTP over Ethernet, one or two VLANs are supported. Transparent clock functionality is enabled globally and might be required in scenarios in which the interface on which packets are received and transmitted is unknown. <div> NOTE: ACX5048 and ACX5096 routers do not support PTP over IPv6 for transparent clocks.</div> |
| Options | There are no options. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring Transparent Clock Mode for Precision Time Protocol on page 68 |


interface (PTP Slave)

| | |
|---------------------------------|---|
| Syntax | <pre> interface <i>interface-name</i> { unicast-mode { clock-source <i>ip-address</i> { local-ip-address <i>local-ip-address</i>; asymmetry <i>number</i>; } } transport ipv4; } </pre> |
| Hierarchy Level | [edit protocols ptp slave] |
| Description | The interface on which to respond to the upstream PTP master. |
| Options | The remaining statements are explained separately. See CLI Explorer . |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • IEEE 1588v2 Precision Timing Protocol (PTP) on ACX Series Universal Access Routers on page 61 • Precision Time Protocol Overview • Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |

local-priority

| | |
|---------------------------------|--|
| Syntax | <code>local-priority <i>local priority-value</i>;</code> |
| Hierarchy Level | <pre>[edit protocols ptp] [edit protocols ptp master interface <i>interface-name</i> multicast-mode] [edit protocols ptp master interface <i>interface-name</i> unicast-mode] [edit protocols ptp slave interface <i>interface-name</i> multicast-mode] [edit protocols ptp slave interface <i>interface-name</i> unicast-mode] [edit protocols ptp stateful interface <i>interface-name</i> multicast-mode] [edit protocols ptp stateful interface <i>interface-name</i> unicast-mode]</pre> |
| Release Information | <p>Statement introduced in Junos OS Release 17.1R1.</p> <p>Statement introduced in Junos OS Release 17.4R1.</p> |
| Description | <p> NOTE: The stateful statement is not supported on QFX Series switches that support PTP.</p> <p>Configure a clock's local priority to be used as a tie-breaker in the dataset comparison algorithm, in the event that all other previous attributes of the datasets being compared are equal. The dataset comparison algorithm compares one clock with another by using the datasets representing those clocks, appended with the local-priority attribute. The local priority is assigned to the local clock and is used if needed when the data associated with the local clock is compared with data on another potential grandmaster (or the master) clock.</p> |
| Options | <p><i>local priority-value</i>—The priority value of the clock.</p> <p>Range: 1 through 255</p> <p>Default: 128</p> |
| Required Privilege Level | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> Precision Time Protocol Overview Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |

local-ip-address (multicast or unicast mode)

| | |
|---|--|
| Syntax | <code>local-ip-address <i>local-ip-address</i>;</code> |
| Hierarchy Level | <pre>[edit protocols ptp master interface <i>interface-name</i> multicast-mode] [edit protocols ptp master interface <i>interface-name</i> unicast-mode] [edit protocols ptp slave interface <i>interface-name</i> multicast-mode] [edit protocols ptp slave interface <i>interface-name</i> unicast-mode]</pre> |
| Release Information | Statement introduced in Junos OS Release 17.4 on the QFX Series. |
| Description | Configure the IP address of the interface acting as the slave or the master. |
| <div>  <p>NOTE: You must configure the same IP address at the [edit interfaces <i>interface-name</i>] hierarchy level.</p> </div> | |
| Options | <i>local-ip-address</i> —The IP address of the interface. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • <i>Configuring Precision Time Protocol</i> • <i>Example: Configuring Precision Time Protocol</i> • <i>Precision Time Protocol Overview</i> • Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |

master

List of Syntax [MX Series on page 122](#)
[QFX Series on page 122](#)

MX Series **master** {
 announce-interval *announce-interval-value*;
 clock-step (one-step | two-step);
 sync-interval *sync-interval-value*;
 interface *interface-name* {
 unicast-mode {
 transport ipv4;
 clock-client *ip-address* {
 local-ip-address *local-ip-address*;
 }
 }
 }
 multicast-mode {
 local-priority
 transport 802.3 link-local;
 }
}

QFX Series **master** {
 interface *interface-name* {
 unicast-mode {
 transport ipv4;
 clock-client *ip-address* {
 local-ip-address *local-ip-address*;
 }
 }
 }
 multicast-mode {
 transport (ipv4 | ieee-802.3)
 local-ip-address *local-ip-address*;
 local-priority *local-ip-address*;
 }
 max-announce-interval *max-announce-interval*;
 max-delay-response-interval *max-delay-response-interval*;
 max-sync-interval *max-sync-interval*;
 min-announce-interval *min-announce-interval*;
 min-delay-response-interval *min-delay-response-interval*;
 min-sync-interval *min-sync-interval*;
 sync-interval *sync-interval*;
}

Hierarchy Level [edit protocols ptp]

Release Information Statement introduced in Junos OS Release 12.2.
 Statement introduced in Junos OS Release 17.3 for the QFX Series.

Description Configure the master with parameters.

The remaining statements are explained separately. See [CLI Explorer](#).

| | |
|---------------------------------|--|
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • <i>Configuring Precision Time Protocol</i> • <i>Example: Configuring Precision Time Protocol</i> • <i>Precision Time Protocol Overview</i> • Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |

multicast-client

| | |
|---------------------------------|---|
| Syntax | <code>multicast-client <address>;</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | For NTP, configure the local router or switch to listen for multicast messages on the local network to discover other servers on the same subnet. |
| Options | address —(Optional) One or more IP addresses. If you specify addresses, the router or switch joins those multicast groups. Default: 224.0.1.1. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the Router or Switch to Listen for Multicast Messages Using NTP on page 32 |

multicast-mode (PTP Master and Slave Interfaces)

List of Syntax [MX Series on page 124](#)
[QFX Series on page 124](#)

MX Series `multicast-mode {
 asymmetry number;
 transport 802.3 link-local;
 }`

QFX Series `multicast-mode {
 local-ip-address local IP address;
 local-priority number;
 }
 transport {
 ieee-802.3;
 ipv4;
 }
}`

Hierarchy Level `[edit protocols ptp slave interface interface-name],`
`[edit protocols ptp master interface interface-name]`

Release Information Statement introduced in Junos OS Release 15.2 for MX Series routers.
 Statement introduced in Junos OS Release 17.4 for the QFX Series.

Description Configure multicast transmission of Precision Time Protocol (PTP) packets between the master node and the slave node. The multicast method of transport of PTP packets is applicable in environments in which PTP uses IEEE 802.3 or Ethernet encapsulation for the transmission of PTP packets. Because PTP over Ethernet uses multicast addresses, a slave port can automatically start receiving the multicast announce messages transmitted by the master ports on a network and can also start communicating with the master port with minimal or no configuration. Unlike PTP over IPv4 where IP addresses are used to identify the master and slave ports, with PTP over Ethernet, multicast MAC addresses are used in forwarding of PTP traffic.

On the QFX Series, multicast-mode specifies that PTP should be forwarded with the multicast IPv4 packet format, and is required for the enterprise profile.



NOTE: You can configure only multicast mode or only unicast mode of transmission of PTP traffic on an interface at a point in time.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.

- Related Documentation**

 - [Configuring Precision Time Protocol](#)
 - [Example: Configuring Precision Time Protocol](#)
 - [Precision Time Protocol Overview](#)

ntp

```
Syntax ntp {
    authentication-key number type type value password;
    boot-server address;
    broadcast <address> <key key-number> <routing-instance-name routing-instance-name>
        <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    server address <key key-number> <version value> <prefer>;
    source-address source-address <routing-instance routing-instance-name>;
    trusted-key [ key-numbers ];
}
```

Hierarchy Level [edit system]

| | |
|----------------------------|---|
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
|----------------------------|---|

Description Configure NTP on the router or switch.

The remaining statements are explained separately.

| Required Privilege Level | |
|--------------------------|--|
| system | To view this statement in the configuration. |
| system-control | To add this statement to the configuration. |

- Related Documentation**
- [Synchronizing and Coordinating Time Distribution Using NTP on page 23](#)
 - *NTP Time Synchronization on SRX Series Devices*

ntp (QFabric)

| | |
|---------------------------------|--|
| Syntax | <pre>ntp { authentication-key <i>number</i> type <i>type</i> value <i>password</i>; server <i>address</i> <key <i>key-number</i>> <version <i>value</i>> <prefer>; }</pre> |
| Hierarchy Level | [edit system] |
| Release Information | Statement introduced in Junos OS Release 11.1 for the QFX Series. |
| Description | <p>Configure Network Time Protocol (NTP) on the switch.</p> <p>The remaining statements are explained separately.</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none">• Configuring NTP Authentication Keys (QFabric System) on page 41• Configuring the NTP Time Server and Time Services (QFabric System) on page 45• authentication-key on page 109• <i>server</i> |

peer (NTP)

| | |
|---------------------------------|---|
| Syntax | <code>peer address <key <i>key-number</i>> <version <i>value</i>> <prefer>;</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | For NTP, configure the local router or switch to operate in symmetric active mode with the remote system at the specified address. In this mode, the local router or switch and the remote system can synchronize with each other. This configuration is useful in a network in which either the local router or switch or the remote system might be a better source of time. |
| Options | <p>address—Address of the remote system. You must specify an address, not a hostname.</p> <p>key <i>key-number</i>—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number. Range: Any unsigned 32-bit integer</p> <p>prefer—(Optional) Mark the remote system as the preferred host, which means that if all other factors are equal, this remote system is chosen for synchronization among a set of correctly operating systems.</p> <p>version <i>value</i>—(Optional) Specify the NTP version number to be used in outgoing NTP packets. Range: 1 through 4 Default: 4</p> |
| Required Privilege Level | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring the NTP Time Server and Time Services on page 27 |

profile-type

| | |
|---|---|
| List of Syntax | MX Series on page 128 QFX Series (Enterprise Profile) on page 128 QFX Series (G.8275.2 Enhanced Profile) on page 128 |
| MX Series | profile-type (g.8275.1 g.8275.1.enh) |
| QFX Series (Enterprise Profile) | profile-type enterprise-profile |
| QFX Series (G.8275.2 Enhanced Profile) | profile-type g.8275.1.enh |
| Hierarchy Level | [edit protocols ptp] |
| Release Information | Statement introduced in Junos OS Release 17.1R1. Statement introduced in Junos OS Release 17.3 for the QFX Series. |
| Description | <p>On the MX Series, configure the G.8275.1 or the enhanced G.8275.1 PTP profile for applications that require accurate phase and time synchronization. This profile supports the architecture defined in ITU-T G.8275 to enable the distribution of phase and time with full timing support and is based on the second version of PTP defined in IEEE 1588.</p> <p>On QFX Series switches that support the enterprise-profile feature, you can configure the enterprise profile, which supports IEEE 1588 PTPv2 transport over multicast IPv4. If you do not specify a profile, the IEEE 1588 default profile is enabled by default.</p> <p>On QFX Series switches that support the G.8275.2 enhanced profile feature, you can configure the G.8275.2 enhanced profile, which supports telecom applications that require accurate phase and time synchronization for phase alignment and time of day synchronization over a wide area network. This profile supports PTP over IPv4 unicast, ordinary and boundary clocks, and unicast negotiation.</p> |
| Options | <p>g.8275.1—Enable the G.8275.1 PTP profile.</p> <p>g.8275.1.enh—Enable the enhanced G.8275.1 PTP profile. This profile supports PTP over IPv4.</p> <p>enterprise-profile—Enable the enterprise profile. The enterprise profile supports IEEE 1588 PTPv2 transport over multicast IPv4. When the enterprise profile is enabled, no other profiles can be enabled. Also, unicast negotiation is disabled when you enable the enterprise profile.</p> <p>g.8275.2.enh—Enable the enhanced G.8275.2 PTP profile. This profile supports PTP over IPv4 unicast.</p> |

| | |
|---------------------------------|--|
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• <i>Precision Time Protocol Overview</i>• Configuring the Precision Time Protocol Enterprise Profile on page 75• Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |

server (NTP)

| | |
|--------------------------|---|
| Syntax | <pre>server address { key key; prefer; routing-instance routing-instance; version version; }</pre> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | <p>For NTP, configure the local router or switch to operate in client mode with the remote system at the specified address. In this mode, the local router or switch can be synchronized with the remote system, but the remote system can never be synchronized with the local router or switch.</p> <p>If the NTP client time drifts so that the difference in time from the NTP server exceeds 128 milliseconds, the client is automatically stepped back into synchronization. If the offset between the NTP client and server exceeds the 1000-second threshold, the client still synchronizes with the server, but it also generates a system log message noting that the threshold was exceeded.</p> |
| Options | <p>address—Address of the remote system. You must specify an address, not a hostname.</p> <p>key key-number—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address.</p> <p>Range: Any unsigned 32-bit integer</p> <p>prefer—(Optional) Mark the remote system as preferred host, which means that if all other things are equal, this remote system is chosen for synchronization among a set of correctly operating systems.</p> <p>routing-instance routing-instance—(Optional) Routing instance through which the server is reachable.</p> <p>version value—(Optional) Specify the version number to be used in outgoing NTP packets.</p> <p>Range: 1 through 4</p> <p>Default: 4</p> |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring the NTP Time Server and Time Services on page 27 |

slave

List of Syntax [MX Series on page 131](#)
 [QFX Series on page 131](#)

MX Series `slave {`
 `announce-interval` *announce-interval-value*
 `announce-timeout` *announce-timeout-value*;
 `delay-request` *delay-request-value*;
 `frequency-only`;
 `hybrid`
 `interface` *interface-name* {
 `unicast-mode` {
 `transport` *ipv4*;
 `clock-source` *ip-address* {
 `local-ip-address` *local-ip-address* {
 }
 }
 } **multicast-mode** {
 `hybrid`
 `transport` *802.3 link-local*;
 }
 }
 `sync-interval` *interval*;
 }

QFX Series `slave {`
 `interface` *interface-name* {
 `unicast-mode` {
 `transport` *ipv4*;
 clock-client *ip-address* {
 `local-ip-address` *local-ip-address*;
 }
 }
 }
 multicast-mode {
 transport (*ipv4 | ieee-802.3*)
 local-ip-address *local-ip-address*;
 local-priority *local-ip-address*;
 }
 `max-announce-interval` *max-announce-interval*;
 `max-delay-response-interval` *max-delay-response-interval*;
 `max-sync-interval` *max-sync-interval*;
 `min-announce-interval` *min-announce-interval*;
 `min-delay-response-interval` *min-delay-response-interval*;
 `min-sync-interval` *min-sync-interval*;
 `sync-interval` *sync-interval*;
 }
 }

Hierarchy Level `[edit protocols ptp]`

Release Information Statement introduced in Junos OS Release 12.2.

Statement introduced in Junos OS Release 17.3 for the QFX Series.

Description Configure the slave with parameters.



NOTE: Multicast mode is not supported on the QFX Series.


The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring Precision Time Protocol*
- *Example: Configuring Precision Time Protocol*
- *Precision Time Protocol Overview*
- [Configuring the Precision Time Protocol G.8275.2 Enhanced Profile \(Telecom Profile\) on page 68](#)

source-address (NTP, RADIUS, System Logging, or TACACS+)

| | |
|--|--|
| Syntax | <code>source-address <i>source-address</i> routing-instance <<i>routing-instance-name</i>>;</code> |
| Hierarchy Level | <p>[edit system accounting destination radius server <i>server-address</i>], [edit system accounting destination tacplus server <i>server-address</i>], [edit system ntp], [edit system radius-server <i>server-address</i>], [edit system syslog], [edit system tacplus-server <i>server-address</i>]</p> |
| Release Information | <p>Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. routing-instance option added in Junos OS Release 14.1</p> |
| Description | Specify a source address for each configured IPv4 or IPv6 TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine. |
| Options | <p><i>source-address</i>—A valid IP address configured on one of the router or switch interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all host <i>hostname</i> statements at the [edit system syslog] hierarchy level, but not for messages directed to the other Routing Engine or to the TX Matrix router or TX Matrix Plus router in a routing matrix based on a TX Matrix router or TX Matrix Plus router.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) The routing instance name in which the source address is defined. (Not supported on EX series platforms)</p> |
| <div>  <p>NOTE: On MX Series platforms, this option is supported only under [edit system ntp] hierarchy level.</p> </div> | |
| Default: | The primary address of the interface |
| Required Privilege Level | <p>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</p> |
| Related Documentation | <ul style="list-style-type: none"> • Configuring RADIUS Server Authentication • Specifying a Source Address for an NTP Server on page 24 • Specifying an Alternative Source Address for System Log Messages |

source-address (NTP, RADIUS, System Logging, or TACACS+)

| | |
|---------------------------------|--|
| Syntax | <code>source-address <i>source-address</i>;</code> |
| Hierarchy Level | <code>[edit system accounting destination radius server <i>server-address</i>],</code> <code>[edit system accounting destination tacplus server <i>server-address</i>],</code> <code>[edit system ntp],</code> <code>[edit system radius-server <i>server-address</i>],</code> <code>[edit system syslog],</code> <code>[edit system tacplus-server <i>server-address</i>]</code> |
| Release Information | Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Specify a source address for each configured TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine. |
| Options | <i>source-address</i> —Valid IP address configured on one of the switch interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all host <i>hostname</i> statements at the <code>[edit system syslog]</code> hierarchy level. |
| Required Privilege Level | system —To view this statement in the configuration. system-control —To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• <i>Configuring RADIUS Authentication (QFX Series or OCX Series)</i>• Synchronizing and Coordinating Time Distribution Using NTP on page 47• <i>Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination</i> |

system

| | |
|---------------------------------|---|
| Syntax | system { ... } |
| Hierarchy Level | [edit] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Configure system management properties. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• System Management Configuration Statements on page 100 |

time-zone

| | |
|----------------------------|---|
| Syntax | <code>time-zone (GMT <i>hour-offset</i> <i>time-zone</i>);</code> |
| Hierarchy Level | [edit system] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. GMT <i>hour-offset</i> option added in Junos OS Release 7.4. |
| Description | Set the local time zone. To have the time zone change take effect for all processes running on the router or switch, you must reboot the router or switch. |
| Default | UTC |
| Options | <p>GMT <i>hour-offset</i>—Set the time zone relative to UTC time. Range: -14 through +12 Default: 0</p> <p><i>time-zone</i>—Specify the time zone as UTC, which is the default time zone, or as a string such as PDT (Pacific Daylight Time), or use one of the following continents and major cities:</p> <p>Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek</p> <p>America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Aruba, America/Asuncion, America/Barbados, America/Belize, America/Bogota, America/Boise, America/Buenos_Aires, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Cordoba, America/Costa_Rica, America/Cuiaba, America/Curacao, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/EL_Salvador, America/Ensenada, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Vevay, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Maceio, America/Managua, America/Manaus, America/Martinique, America/Mazatlan, America/Mendoza, America/Menominee, America/Mexico_City, America/Miquelon, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York,</p> |

America/Nipigon, America/Nome, America/Noronha, America/Panama,
 America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince,
 America/Port_of_Spain, America/Porto_Acre, America/Puerto_Rico, America/Rainy_River,
 America/Rankin_Inlet, America/Regina, America/Rosario, America/Santiago,
 America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund,
 America/Shiprock, America/St_Johns, America/St_Kitts, America/St_Lucia,
 America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa,
 America/Thule, America/Thunder_Bay, America/Tijuana, America/Tortola,
 America/Vancouver, America/Whitehorse, America/Winnipeg, America/Yakutat,
 America/Yellowknife
 Antarctica/Casey, Antarctica/DumontDURville, Antarctica/Mawson, Antarctica/McMurdo,
 Antarctica/Palmer, Antarctica/South_Pole
 Arctic/Longyearbyen
 Asia/Aden, Asia/Alma-Ata, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe,
 Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Beirut,
 Asia/Bishkek, Asia/Brunei, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus,
 Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hong_Kong, Asia/Irkutsk,
 Asia/Ishigaki, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka,
 Asia/Karachi, Asia/Kashgar, Asia/Katmandu, Asia/Kolkata, Asia/Krasnoyarsk,
 Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Magadan, Asia/Manila,
 Asia/Muscat, Asia/Nicosia, Asia/Novosibirsk, Asia/Omsk, Asia/Phnom_Penh,
 Asia/Pyongyang, Asia/Qatar, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Seoul,
 Asia/Shanghai, Asia/Singapore, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran,
 Asia/Thimbu, Asia/Tokyo, Asia/Ujung_Pandang, Asia/Ulan_Bator, Asia/Urumqi,
 Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan
 Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe,
 Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia,
 Atlantic/St_Helena, Atlantic/Stanley
 Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Darwin,
 Australia/Hobart, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne,
 Australia/Perth, Australia/Sydney
 Europe/Amsterdam, Europe/Andorra, Europe/Athens, Europe/Belfast, Europe/Belgrade,
 Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest,
 Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Helsinki,
 Europe/Istanbul, Europe/Kaliningrad, Europe/Kiev, Europe/Lisbon, Europe/Ljubljana,
 Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Minsk,
 Europe/Monaco, Europe/Moscow, Europe/Oslo, Europe/Paris, Europe/Prague,
 Europe/Riga, Europe/Rome, Europe/Samara, Europe/San_Marino, Europe/Sarajevo,
 Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn,
 Europe/Tirane, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius,
 Europe/Warsaw, Europe/Zagreb, Europe/Zurich
 Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro,
 Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte,
 Indian/Reunion
 Pacific/Apia, Pacific/Auckland, Pacific/Chatham, Pacific/Easter, Pacific/Efate,
 Pacific/Enderbury, Pacific/Fakaofo, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos,
 Pacific/Gambier, Pacific/Guadacanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston,
 Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas,
 Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea,
 Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Ponape, Pacific/Port_Moresby,
 Pacific/Rarotonga, Pacific/Saipan, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu,
 Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap

| | |
|---------------------------|--|
| Required Privilege | system—To view this statement in the configuration. |
| Level | system-control—To add this statement to the configuration. |

- Related Documentation**
- [Modifying the Default Time Zone for a Router or Switch Running Junos OS on page 35](#)
 - [System Management Configuration Statements on page 100](#)

transport ipv4 (PTP Unicast Master and Slave Interface)

Syntax transport ipv4;

Hierarchy Level [edit protocols ptp slave [interface](#) *interface-name* [unicast-mode](#)],
[edit protocols ptp master interface *interface-name* [unicast-mode](#)]

Release Information Statement introduced in Junos OS Release 12.2.
Statement introduced in Junos OS Release 12.3 for the master interface.
Statement introduced in Junos OS Release 17.3 for the QFX Series.

Description Configure the encapsulation type for Precision Time Protocol (PTP) packet transport.
Currently, IPv4 is the only supported encapsulation type for PTP.



NOTE: This attribute is mandatory in the configuration of a master or a slave clock.

Options ipv4—Encapsulation for PTP packet transport.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

- Related Documentation**
- [IEEE 1588v2 PTP Boundary Clock Overview on page 58](#)
 - [Configuring Precision Time Protocol Clocking on page 78](#)
 - [Configuring the Precision Time Protocol G.8275.2 Enhanced Profile \(Telecom Profile\) on page 68](#)
 - [Configuring a PTP Master Boundary Clock on page 80](#)
 - [Configuring a PTP Slave Clock on page 90](#)
 - [Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 86](#)
 - [Example: Configuring a PTP Boundary Clock on page 83](#)

trusted-key

| | |
|---------------------------------|---|
| Syntax | <code>trusted-key [<i>key-numbers</i>];</code> |
| Hierarchy Level | [edit system ntp] |
| Release Information | Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | For NTP, configure the keys you are allowed to use when you configure the local router or switch to synchronize its time with other systems on the network. |
| Options | <i>key-numbers</i> —One or more key numbers. Each key can be any 32-bit unsigned integer except 0. |
| Required Privilege Level | system—To view this statement in the configuration. system-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Configuring NTP Authentication Keys on page 31• authentication-key on page 108• broadcast on page 112• peer on page 127• server on page 130 |

unicast-mode (PTP Slave Interface)

| | |
|---------------------------------|---|
| Syntax | <pre>unicast-mode { clock-source ip-address { local-ip-address local-ip-address; asymmetry number; } } transport ipv4; }</pre> |
| Hierarchy Level | [edit protocols ptp slave interface <i>interface-name</i>] |
| Release Information | Statement introduced in Junos OS Release 12.2. Statement introduced in Junos OS Release 17.3 for the QFX Series. |
| Description | Configure upstream unicast Precision Time Protocol master clock sources. The remaining statements are explained separately. See CLI Explorer . |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• IEEE 1588v2 Precision Timing Protocol (PTP) on ACX Series Universal Access Routers on page 61• <i>Precision Time Protocol Overview</i> |

use-imported-time-zones

| | |
|---------------------------------|---|
| Syntax | <pre>use-imported-time-zones;</pre> |
| Hierarchy Level | [edit system] |
| Release Information | Statement introduced in Junos OS Release 9.0. |
| Description | Configure a custom time zone from a locally generated time-zone database. |
| Required Privilege Level | admin—To view this statement in the configuration. admin-control—To add this statement to the configuration. |
| Related Documentation | <ul style="list-style-type: none">• Updating the IANA Time Zone Database on Junos OS Devices on page 36 |

CHAPTER 6

Operational Commands

- set date
- show ntp associations
- show ntp status
- show ptp clock
- show ptp global-information
- show ptp master
- show ptp slave
- show ptp lock-status
- show ptp statistics

set date

Syntax `set date (date-time | ntp <ntp-server> <source-address source-address>)`

Release Information Command introduced before Junos OS Release 7.4.

Description Set the date and time.

```
user@host> set date ntp
21 Apr 17:22:02 ntpdate[3867]: step time server 172.17.27.46 offset 8.759252 sec
```

- Options**
- ***date-time***—Specify date and time in one of the following formats:
 - `YYYYMMDDHHMM.SS`
 - `"month DD, YYYY HH:MM(am | pm)"`
 - **ntp**—Configure the router to synchronize the current date and time setting with a Network Time Protocol (NTP) server.
 - ***ntp-server***—(Optional) Specify the IP address of one or more NTP servers.
 - ***source-address source-address***—(Optional) Specify the source address that is used by the router to contact the remote NTP server.

Required Privilege Level view

Related Documentation

- [Setting the Date and Time Locally on page 19](#)

show ntp associations

| | |
|---------------------------------|--|
| Syntax | show ntp associations <no-resolve> |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Display Network Time Protocol (NTP) peers and their state. |
| Options | none —Display NTP peers and their state. no-resolve —(Optional) Suppress symbolic addressing. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • show ntp status on page 145 |
| List of Sample Output | show ntp associations on page 144 |
| Output Fields | Table 4 on page 143 describes the output fields for the show ntp associations command. Output fields are listed in the approximate order in which they appear. |

Table 4: show ntp associations Output Fields

| Field Name | Field Description |
|------------|---|
| remote | Address or name of the remote NTP peer. |
| refid | Reference identifier of the remote peer. If the reference identifier is not known, this field shows a value of 0.0.0.0. |
| st | Stratum of the remote peer. |
| t | Type of peer: b (broadcast), l (local), m (multicast), or u (unicast). |
| when | When the last packet from the peer was received. |
| poll | Polling interval, in seconds. |
| reach | Reachability register, in octal. |
| delay | Current estimated delay of the peer, in milliseconds. |

Table 4: *show ntp associations* Output Fields (continued)

| Field Name | Field Description |
|------------------|---|
| offset | Current estimated offset of the peer, in milliseconds. |
| disp | Current estimated dispersion of the peer, in milliseconds. |
| peer-name | Peer name and status of the peer in the clock selection process: <ul style="list-style-type: none"> • space—Discarded because of a high stratum value or failed sanity checks. • x—Designated "falseticker" by the intersection algorithm. • .—Culled from the end of the candidate list. • — —Discarded by the clustering algorithm. • +—Included in the final selection set. • #—Selected for synchronization, but the distance exceeds the maximum. • *—Selected for synchronization. • o—Selected for synchronization, but the packets-per-second (pps) signal is in use. |

Sample Output

show ntp associations

```

user@host> show ntp associations
  remote      refid      st t when poll reach  delay  offset  disp
=====
*devcie1@example.com  2 u  43   64  377   1.86   0.319   0.08

```


show ntp status

| | |
|---------------------------------|--|
| Syntax | <code>show ntp status</code> <code><no-resolve></code> |
| Release Information | Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| Description | Display the values of internal variables returned by Network Time Protocol (NTP) peers. |
| Options | none —Display the values of internal variables returned by NTP peers. no-resolve —(Optional) Suppress symbolic addressing. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • show ntp associations on page 143 |
| List of Sample Output | show ntp status on page 146 |
| Output Fields | Table 5 on page 145 describes the output fields for the show ntp status command. Output fields are listed in the approximate order in which they appear. |

Table 5: show ntp status Output Fields

| Field Name | Field Description |
|-----------------------------|---|
| status | System status word, a code representing the status items listed. |
| leap_none | Indicates a normal synchronized state with no leap seconds imminent. Other options could be leap_add_sec , leap_del_sec , or leap_alarm , indicating a leap second will be added, deleted, or a leap second requirement is upcoming. |
| sync_ntp | Indicates the current synchronization source, in this case, an NTP server. Other options include sync_alarm and sync_unspec , both indicating that the router has not been synched. |
| x events | Indicates the number of events that have occurred since that last code change. An event is often the receipt of an NTP polling message. |
| event_peer/strat_chg | Describes the most recent event, in this case, the stratum of the peer server changed. |
| version | A detailed description of the version of NTP being used. |
| processor | Indicates the current hardware platform and version of the processor. |

Table 5: show ntp status Output Fields (continued)

| Field Name | Field Description |
|-----------------------|---|
| system | Detailed description of the name and version of the operating system in use. |
| leap | The number of leap seconds in use. |
| stratum | The stratum of the peer server. Anything greater than 1 is a secondary reference source, and the number roughly represents the number of hops away from the stratum 1 server.. Stratum 1 is a primary reference, such as an atomic clock. |
| precision | The precision of the peer clock, how precisely the frequency and time can be maintained with this particular timekeeping system. |
| rootdelay | The total roundtrip delay to the primary reference source, in seconds. |
| rootdispersion | The maximum error relative to the primary reference source, in seconds. |
| peer | An identification number of the peer in use. |
| refid | Reference identifier of the remote peer. If the reference identifier is not known, this field shows a value of 0.0.0.0. |
| reftime | The local time, in timestamp format, when the local clock was last updated. If the local clock has never been synchronized, the value is zero. |
| poll | The NTP broadcast message polling interval, in seconds. |
| clock | The current time on the local router clock. |
| state | The current mode of NTP operation, where 1 is symmetric active, 2 is symmetric passive, 3 is client, 4 is server, and 5 is broadcast. |
| offset | Current estimated offset of the peer, in milliseconds. Indicates the time difference between the reference clock and the local clock. |
| frequency | The frequency of the clock. |
| jitter | Indicates the magnitude of jitter, in milliseconds, between several time queries. |
| stability | A measure of how well this clock can maintain a constant frequency. |

Sample Output

show ntp status

```
user@host> show ntp status
assID=0 status=0544 leap_none, sync_local_proto, 4 events, event_peer/strat_chg,
version="ntpd 4.2.2p1@1.1570-o Tue May 19 13:57:55 UTC 2009 (1)",
processor="x86_64", system="Linux/2.6.18-164.el5", leap=00, stratum=4,
precision=-10, rootdelay=0.000, rootdispersion=11.974, peer=59475,
refid=LOCAL(0),
```

```
reftime=d495c32c.0e71eaf2 Mon, Jan  7 2013 13:57:00.056, poll=10,  
clock=d495c32c.cebd43bd Mon, Jan  7 2013 13:57:00.807, state=4,  
offset=0.000, frequency=0.000, jitter=0.977, noise=0.977,  
stability=0.000, tai=0
```

show ptp clock

Syntax show ptp clock

Release Information Command introduced in Junos OS Release 12.2.
Command introduced in Junos OS Release 12.3 for ACX Series Routers.
Command introduced in Junos OS Release 17.3 for QFX Series switches.

Description (ACX Series, MX80, MX240, MX480, MX960 routers, and QFX Series switches) Display the details of the clock configured on the node.

Options This command has no options.

Required Privilege Level view

Related Documentation

- [IEEE 1588v2 PTP Boundary Clock Overview on page 58](#)
- [IEEE 1588v2 Precision Timing Protocol \(PTP\) on ACX Series Universal Access Routers on page 61](#)
- [Precision Time Protocol Overview](#)

List of Sample Output [show ptp clock on page 150](#)
[show ptp clock \(ACX Series Routers\) on page 150](#)

Output Fields [Table 6 on page 148](#) lists the output fields for the **show ptp clock** command. Output fields are listed in the approximate order in which they appear.

Table 6: show ptp clock Output Fields

| Field Name | Field Description |
|-----------------------|--|
| Slot Number | Number of the FPC or MIC slot. |
| Two-step Clock | Whether the clock provides time information which is a combination of an event message and a subsequent general message: True or False . |
| Clock Identity | Clock identity of the slave or client as defined in IEEE 1588. |
| Total Ports on Device | Total number of PTP ports on the router. |
| Clock Class | Attribute of an ordinary or boundary clock that denotes the traceability of the time or frequency distributed by the grandmaster clock. |
| Clock Accuracy | Indicates the expected accuracy of a clock when it is the grandmaster, or in the event it becomes the grandmaster. |

Table 6: show ptp clock Output Fields (continued)

| Field Name | Field Description |
|-------------------------------|---|
| Log Variance | Represents an estimate of the variations of the local clock when it is not synchronized via PTP to another clock. |
| Clock Priority1 | Priority value of the clock. Lower value takes precedence. |
| Clock Priority2 | Prioritize the masters to avoid confusion when the Clock Priority1 value is the same for different masters in a network. |
| UTC Offset | Offset between International Atomic Time (TAI) and Coordinated Universal Time (UTC) times. The value is 34 seconds as of January 2012. |
| Leap59 | When TRUE , the last minute of the current UTC day has only 59 seconds (instead of the 60 SI seconds). |
| Leap61 | When TRUE , the last minute of the current UTC day has 61 seconds (instead of the 60 SI seconds). |
| Time Traceable | When TRUE , the timescale and the UTC offset are traceable to a primary reference. |
| Frequency Traceable | When TRUE , frequency determining the timescale is traceable to a primary reference. |
| Time Source | Time source external to the Precision Time Protocol (PTP), which provides time and/or frequency as appropriate. The time source is traceable to the international standards laboratories maintaining clocks that form the basis for the International Atomic Time (TAI) and Universal Coordinated Time (UTC) timescales. Examples of these are Global Positioning System (GPS), NTP, and National Institute of Standards and Technology (NIST) timeservers. |
| Delay Req Sending Time | Interval in seconds between the delay-request messages sent by the slave to the master. |
| Steps Removed | Number of boundary clocks between the local clock and the foreign master clock. |
| Slave-only | Set to TRUE , when the system is used in ordinary slave clock mode; otherwise, FALSE . |
| Parent Id | EUI-64 clock identifier of the immediate upstream master clock. |
| GMC Id | EUI-64 clock identifier of the grandmaster clock. |
| GMC Class | Denotes the grandmaster clock's traceability of the distributed time or frequency. |
| GMC Accuracy | Indicates the expected accuracy of the grandmaster clock. |
| GMC Variance | Represents an estimate of the variations of the grandmaster clock. |
| GMC Priority1 | Priority1 -value of the grandmaster clock. |
| GMC Priority2 | Priority2 -value of the grandmaster clock. |

Sample Output

show ptp clock

```

user@host> run show ptp clock
Clock Details:

Slot Number          : 7
Default Data:
Two-step Clock       : FALSE
00:05:85:ff:fe:73:ef:d0
Total Ports on Device : 0
Clock Accuracy       : 49
Clock Priority1      : 128
UTC Offset           : 33
Leap61               : FALSE
Frequency Traceable  : FALSE
Delay Req Sending Time: 0
Slave-only           : NA
Parent Data:
Parent Id            : 00:18:0b:ff:ff:20:01:62
GMC Id               : 00:18:0b:ff:ff:20:01:62
GMC Accuracy         : 254
GMC Priority1        : 0
Global Data:
UTC Offset           : 34
Leap-61              : FALSE
Freq Traceable       : FALSE
Time master          : 160

Clock Identity :
Clock Class       : 255
Log Variance      : -12944
Clock Priority2: 128
Leap59            : FALSE
Time Traceable    : FALSE
Time master       : 0
Steps Removed     : 1

GMC Class         : 52
GMC Variance      : 11952
GMC Priority2      : 0

Leap-59           : FALSE
Time traceable     : FALSE
Time Scale         : FALSE

```

show ptp clock (ACX Series Routers)

```

user@host> run show ptp clock
Clock Details:

Slot Number          : 0
Default Data:
Two-step Clock       : FALSE
84:18:88:ff:fe:c0:7a:00
Total Ports on Device : 0
Clock Accuracy       : 34
Clock Priority1      : 128
UTC Offset           : 0
Leap61               : FALSE
Frequency Traceable  : FALSE
Delay Req Sending Time: 0
Slave-only           : NA
Parent Data:
Parent Id            : 00:00:64:ff:fe:01:01:02
GMC Id               : 00:00:64:ff:fe:01:01:02
GMC Accuracy         : 35
GMC Priority1        : 128
Global Data:
UTC Offset           : 0
Leap-61              : FALSE
Freq Traceable       : FALSE
Time source          : 16

Clock Identity :
Clock Class       : 255
Log Variance      : 15353
Clock Priority2: 128
Leap59            : FALSE
Time Traceable    : FALSE
Time Source       : 0
Steps Removed     : 0

GMC Class         : 80
GMC Variance      : 0
GMC Priority2      : 128

Leap-59           : FALSE
Time tracable     : FALSE
Time Scale         : FALSE

```

show ptp global-information

| | |
|---------------------------------|---|
| Syntax | show ptp global-information |
| Release Information | Command introduced in Junos OS Release 14.1X53-D25 for the QFX Series. |
| Description | Show Precision Time Protocol (PTP)–related global information. |
| Options | This command has no options. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • Understanding Transparent Clocks in Precision Time Protocol on page 56 • Configuring Transparent Clock Mode for Precision Time Protocol on page 68 • Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |
| List of Sample Output | show ptp global-information (Transparent Clock Configured) on page 152 show ptp global-information (Default Profile) on page 152 show ptp global-information (Enterprise Profile) on page 153 |
| Output Fields | <p>Table 7 on page 151 lists the output fields for the show ptp global-information command. Output fields are listed in the approximate order in which they appear.</p> |

Table 7: show ptp global-information Output Fields

| Field Name | Field Description |
|--------------------------|--|
| PTP Global Configuration | Displays if PTP is configured globally. |
| Domain Number | PTP domain with values from 0 through 127. The default value is 0. Only one PTP domain is supported at any given point in time. |
| Clock mode | Clock mode is either boundary or ordinary. |
| Profile Type | IEEE-2008 or Enterprise. |
| Priority Level1 | Priority value of the clock: 0 through 255. The default is 128. The lower value takes precedence. |
| Priority Level2 | Priority value of the clock: 0 through 255. The default is 128. This value is used to differentiate and prioritize the master clocks when the <i>priority1-value</i> is the same for different master clocks in a network. The lower value takes precedence. |
| Unicast Negotiation | Method by which the announce, synchronization, and delay-response packet rates are negotiated between the master and the slave or client before a PTP session is established. Unicast negotiation is enabled or disabled. |

Table 7: show ptp global-information Output Fields (continued)

| Field Name | Field Description |
|--------------------------|---|
| ESMC QL From Clock Class | Denotes whether the conversion from clock class to QL is enabled or disabled. |
| Clock Class/ESMC QL | Denotes the user defined clock class to QL conversion. |
| SNMP Trap Status | Denotes the SNMP trap generation status (Enabled or Disabled). |
| Master Parameters | Delay Request Timeout The default value is 30 seconds. The range is from 30 to 300 seconds. |
| Transparent-clock-config | Displays if transparent clock mode is enabled or disabled. |
| Transparent-clock-status | Display the status of the transparent clock operation. The following status would be displayed: <ul style="list-style-type: none"> • N/A—Transparent clock is not configured. • Active—Transparent clock is configured and working properly. • sync-in-progress—This is a temporary state. During startup, all the PHYs are synchronized with each other. This status can also occur when a new PIC is plugged in to the switch and all the PHYs go through the synchronization cycle again. <p>NOTE: Transparent clock operation is disabled during the synchronization of PHYs.</p> • Inactive—Transparent clock is configured but not working properly. This would indicate a hardware error in PHY timestamping logic. |
| UTC Leap Seconds | The number of UTC leap seconds is 37 seconds by default. You can, however, configure a different value. |

Sample Output

show ptp global-information (Transparent Clock Configured)

```

user@switch> show ptp global-information
PTP Global Configuration:
Transparent-clock-config : ENABLED
Transparent-clock-status : ACTIVE

```

show ptp global-information (Default Profile)

```

user@switch> show ptp global-information
PTP Global Configuration:
Domain number           : 0
Clock mode               : Ordinary
Profile type             : IEEE-2008
Priority Level1          : 128
Priority Level2          : 128
Path Trace              : Disabled
Unicast Negotiation     : Disabled
ESMC QL From Clock Class: Disabled
Clock Class/ESMC QL     : -
SNMP Trap Status        : Disabled

```



```
PHY Time Stamping      : Disabled
UTC Leap Seconds       : 37
```

show ptp global-information (Enterprise Profile)

```
user@switch> show ptp global-information
PTP Global Configuration:
Domain number          : 0
Clock mode             : Boundary
Profile type           : Enterprise
Priority Level1        : 128
Priority Level2        : 128
...
...
```

show ptp master

| | |
|---------------------------------|--|
| Syntax | <code>show ptp master</code> <code><brief detail interface></code> |
| Release Information | Command introduced in Junos OS Release 12.2. Command introduced in Junos OS Release 17.3 for the QFX Series. |
| Description | (MX80, MX240, MX480, MX960 routers, and the QFX Series) Display information about the configured master and the status of the master. |
| Options | brief —Display information about the master in brief. detail —Display information about the master in detail. interface —Display information about the configured interface of the master. |
| Required Privilege Level | View |
| Related Documentation | <ul style="list-style-type: none"> Precision Time Protocol Overview Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |
| Output Fields | Table 8 on page 154 lists the output fields for the show ptp master command. Output fields are listed in the approximate order in which they appear. |

Table 8: show ptp master Output Fields

| Field Name | Field Description |
|---|---|
| Interface | Name of the interface configured for Precision Time Protocol (PTP) on the master. |
| Status | Status of the Precision Time Protocol master: <ul style="list-style-type: none"> • Master or Slave • Active or Inactive • Initializing or Down |
| Local Address | IP or MAC address of the configured master clock. |
| Status (Local address Status) | Status of the local address of the interface: <ul style="list-style-type: none"> • Configured or Not configured • Master or Slave • Active or Inactive |

Table 8: show ptp master Output Fields (continued)

| Field Name | Field Description |
|--|--|
| Status (Remote address Status) | Status of the remote address of the interface on the QFX Series: <ul style="list-style-type: none"> • Configured or Not configured • Master or Slave • Active or Inactive |
| Total Remote Slaves | Number of remote slaves. |
| Slave Address | IP or MAC address of the slave. |
| Status (Slave Address Status) | Status of the address of the slave: <ul style="list-style-type: none"> • Configured or Not configured • Master or Slave • Active or Inactive or Ready |

Sample Output

show ptp master

```
user@host> run show ptp master brief
PTP Master Interface Configured:

Master Interface      Status
ge-7/0/2.0           Master, Active
```

show ptp master detail (Enterprise Profile on the QFX Series)

```
user@host> run show ptp master detail
PTP Master Interface Details:
Interface   : xe-0/0/6:1.0
Status      : Master, Active
Clock Info :
  Local Address: 50.50.50.1      Status: Configured, Master, Active
  Remote Address: 224.0.1.129
  Total Remote Slaves: 1
```

show ptp master detail (Enterprise Profile with dynamically learned master and slave interfaces for each physical interface on the QFX Series)

```
user@host> run show ptp slave detail
PTP Master Interface Details:

Interface   : xe-0/0/31:3.0
Status      : Master, Active
Clock Info :
  Local Address: 10.10.10.2      Status: Configured, Master, Active
  Remote Address: 10.10.10.1      Status: Learned, Slave, Active
  Remote Address: 224.0.1.129    Status: Configured, Slave, Active
  Total Remote Slaves: 2

Interface   : xe-0/0/35:3.0
```

```
Status      : Master, Active
Clock Info :
  Local Address: 10.2.2.1      Status: Configured, Master, Active
  Remote Address: 10.2.2.24    Status: Learned, Slave, Active
  Remote Address: 10.2.2.29    Status: Learned, Slave, Active
  Remote Address: 10.2.2.30    Status: Learned, Slave, Active
  Remote Address: 10.2.2.32    Status: Learned, Slave, Active
  Remote Address: 10.2.2.35    Status: Learned, Slave, Active
  Remote Address: 10.2.2.52    Status: Learned, Slave, Active
  Remote Address: 10.2.2.61    Status: Learned, Slave, Active
  Remote Address: 224.0.1.129  Status: Configured, Slave, Active
Total Remote Slaves: 8
```

show ptp master detail

```
user@host> run show ptp master detail
PTP Master Interface Details:
Interface  : ge-7/0/2.0
Status     : Master, Active
Clock Info :
  Local Address: 10.0.0.1      Status: Configured, Master, Active
  Total Remote Slaves: 0
  Slave IP: 10.0.0.2          Status: Configured, Slave, Active
```

show ptp master detail (with IPv6 addresses for PTP master/slave)

```
user@host> run show ptp master detail
PTP Master Interface Details:
Interface  : ge-0/1/5.0
Status     : Master, Active
Clock Info :
  Local Address: 84:18:88:c0:60:a1 Status: Configured, Master, Active
  Remote Address: [Slave Mac]      Status: Configured, Slave, Active
Total Remote Slaves: 1
```

show ptp interface ge-7/0/2.0

```
user@host> run show ptp master interface ge-7/0/2.0
PTP Master Interface Configured:

Master Interface      Status
ge-7/0/2.0           Master, Active
```

show ptp slave

| | |
|---------------------------------|---|
| Syntax | show ptp slave <brief detail interface> |
| Release Information | Command introduced in Junos OS Release 12.2. Command introduced in Junos OS Release 17.3 for the QFX Series. |
| Description | (MX80, MX240, MX480, MX960 routers, and the QFX Series) Display information about the configured slave and the status of the slave. |
| Options | brief —Display information about the slave in detail. detail —Display information about the slave in detail. interface —Display information about the configured interface of the slave. |
| Required Privilege Level | View |
| Related Documentation | <ul style="list-style-type: none"> <i>Precision Time Protocol Overview</i> Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 68 |
| Output Fields | Table 9 on page 157 lists the output fields for the show ptp slave command. Output fields are listed in the approximate order in which they appear. |

Table 9: show ptp slave Output Fields

| Field Name | Field Description |
|--------------------------------------|---|
| Interface | Name of the interface configured for Precision Time Protocol. |
| Status | Status of the Precision Time Protocol slave: <ul style="list-style-type: none"> • Master or Slave • Active or Inactive • Initializing or Down |
| Interface | Interface configured on the slave. |
| Local Address | IP or MAC address of the local interface. |
| Status (Local address Status) | Status of the local address of the interface acting as the slave: <ul style="list-style-type: none"> • Configured or Unconfigured • Master or Slave • Active or Inactive or Ready |

Table 9: show ptp slave Output Fields (continued)

| Field Name | Field Description |
|--|--|
| Status (Remote address Status) | Status of the remote address of the interface on the QFX Series: <ul style="list-style-type: none"> • Configured or Not configured • Master or Slave • Active or Inactive |
| Total Remote Masters | Number of remote masters. |
| Remote Master | IP or MAC address of the remote node. |
| Status (Slave IP Address Status) | Status of the address of the master: <ul style="list-style-type: none"> • Configured or Unconfigured • Master or Slave • Active or Inactive |

Sample Output

show ptp slave

```
user@host> run show ptp slave
PTP Slave Interfaces Configured:

Slave Interface      Status
ge-7/0/0.0           Slave, Active
```

show ptp slave detail

```
user@host> run show ptp slave detail
PTP Slave Interface Details:

Interface      : ge-7/0/0.0
Status         : Slave, Active
Clock Info
  Local address : 10.10.1.10           Status: Configured, Slave, Active
  Total Remote Masters: 0
  Remote Master: 10.10.1.2           Status: Configured, Master, Active
```

show ptp slave detail (with IPv6 addresses for PTP master/slave)

```
user@host> run show ptp slave detail
PTP Slave Interface Details:

Interface      : ge-0/1/5.0
Status         : Slave, Active
Clock Info
  Local Address 2001:cdba:0000:0000:0000:0000:3257:9653      Status:
Configured, Slave, Active
  Remote Master:: 2001:cdba:0000:0000:0000:0000:3257:9652 Status: Configured,
Master, Active
  Total Remote Masters: 1
```


show ptp lock-status

| | |
|---------------------------------|---|
| Syntax | show ptp lock-status |
| Release Information | Command introduced in Junos OS Release 12.2. Command introduced in Junos OS Release 17.3 for the QFX Series. |
| Description | (ACX Series, MX80, MX240, MX480, MX960 routers, and QFX Series switches) Display information about the lock status of the slave. The output verifies whether the slave is aligned to the grandmaster (master clock) or not. |
| Options | detail —Display detailed information about the lock status of the slave. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • IEEE 1588v2 PTP Boundary Clock Overview on page 58 • IEEE 1588v2 Precision Timing Protocol (PTP) on ACX Series Universal Access Routers on page 61 • Precision Time Protocol Overview |
| List of Sample Output | show ptp lock-status on page 161 show ptp lock-status (ACX Series) on page 161 show ptp lock-status detail (ACX Series) on page 161 show ptp lock-status detail (with IPv6 addresses for PTP master/slave) on page 161 |
| Output Fields | Table 10 on page 160 lists the output fields for the show ptp lock-status command. Output fields are listed in the approximate order in which they appear. |

Table 10: show ptp lock-status Output Fields

| Field Name | Field Description |
|---------------------|---|
| Lock State | State of the slave clock with respect to its master clock: <ul style="list-style-type: none"> • Freerun • Holdover • Phase Aligned • Acquiring • Initializing • Freq locked |
| Phase offset | Time offset information of a slave clock with respect to its master clock. Precision of this time offset is 1 nanosecond. |

Table 10: show ptp lock-status Output Fields (continued)

| Field Name | Field Description |
|--------------------------------|---|
| State since | Date, time, and how long ago the lock status of the PTP client or slave clock changed. The format is State since: year-month-day hour:minute:second:timezone (hour:minute:second ago) . For example, State since: 2002-04-26 10:52:40 PDT (04:33:20 ago) . On ACX Series routers, this field is displayed in Junos OS Release 15.1 and later. |
| Selected Master Details | <p>Details include the following:</p> <ul style="list-style-type: none"> • Upstream Master address—The address of the remote master from which the slave acquires the clock. • Slave interface—The slave interface on this router corresponding to the Master above. <p>NOTE: On ACX Series router, if the PTP lock state is FREERUN, then the Selected Master Details field is not shown.</p> |

Sample Output

show ptp lock-status

```
user@host> run show ptp lock-status
Lock Status:

Lock State      : 5 (PHASE ALIGNED)
Phase offset    : 0.000000001 sec
```

show ptp lock-status (ACX Series)

```
user@host> show ptp lock-status
Lock Status:

Lock State      : 1 (FREERUN)
Phase offset    : 0.000000869 sec
```

show ptp lock-status detail (ACX Series)

```
user@host> show ptp lock-status detail
Lock Status:

Lock State      : 5 (PHASE ALIGNED)
State since     : 2014-09-10 11:24:11 PDT (00:02:51 ago)

Phase offset    : 0.000000030 sec

Selected Master Details:
Upstream Master address : 13.13.13.1
Slave interface         : ge-0/1/5.0
```

show ptp lock-status detail (with IPv6 addresses for PTP master/slave)

```
user@host> show ptp lock-status detail
Lock Status:

Lock State      : 5 (PHASE ALIGNED)
Phase offset    : -0.000000010 sec
```

Selected Master Details:

| | |
|-------------------------|---|
| Upstream Master address | : 2001:cdba:0000:0000:0000:0000:3257:9652 |
| Slave interface | : ge-0/2/0.0 |
| Parent Id | : 84:18:88:ff:fe:c0:34:00 |
| GMC Id | : 00:18:0b:ff:fe:20:03:14 |

show ptp statistics

| | |
|---------------------------------|---|
| Syntax | show ptp statistics <brief detail> |
| Release Information | Command introduced in Junos OS Release 12.3. Command introduced in Junos OS Release 17.3 for the QFX Series. |
| Description | Display information about Precision Time Protocol (PTP) statistics. |
| Options | brief —Display brief statistics about the operation of configured PTP clocks. detail —Display detailed statistics about the operation of configured PTP clocks. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • IEEE 1588v2 PTP Boundary Clock Overview on page 58 • IEEE 1588v2 Precision Timing Protocol (PTP) on ACX Series Universal Access Routers on page 61 |
| List of Sample Output | show ptp statistics on page 164 show ptp statistics (with IPv6 addresses for PTP master/slave) on page 164 show ptp statistics detail on page 164 show ptp statistics detail (with IPv6 addresses for PTP master/slave) on page 165 show ptp statistics detail (Enterprise profile statistics for remote devices on the QFX Series) on page 165 |
| Output Fields | Table 11 on page 163 lists the output fields for the show ptp statistics command. Output fields are listed in the approximate order in which they appear. |

Table 11: show ptp statistics Output Fields

| Field Name | Field Description |
|----------------|--|
| Local Address | IP address of the local PTP master and slave interfaces. |
| Remote Address | IP address of the remote PTP master and slave interfaces. |
| Role | Function performed by an Ethernet interface configured as a slave or master. |
| Stream | Stream ID uniquely identifies the connection between one master and one slave. |
| Received | 1588v2 packets received by the master or slave interface. For the QFX Series, all packets transmitted by the master or slave interface. |

Table 11: show ptp statistics Output Fields (continued)

| Field Name | Field Description |
|--------------------|--|
| Transmitted | 1588v2 packets transmitted by the master or slave interface. For the QFX Series, all packets transmitted by the master or slave interface. |
| Signalling | Packet count for signalling messages: <ul style="list-style-type: none"> Rx—Number of packets received. Tx—Number of packets transmitted. |
| Announce | Packet count for announce messages: <ul style="list-style-type: none"> Rx—Number of packets received. Tx—Number of packets transmitted. |
| Sync | Packet count for synchronization messages: <ul style="list-style-type: none"> Rx—Number of packets received. Tx—Number of packets transmitted. |
| Delay | Packet count for delay request or response messages: <ul style="list-style-type: none"> Rx—Number of packets received. Tx—Number of packets transmitted. |
| Error | Packet count for signal loss errors: <ul style="list-style-type: none"> Rx—Number of packets received with errors. Tx—Number of packets transmitted with errors. |

Sample Output

show ptp statistics

```

user@host> show ptp statistics
Local Address    Remote Address  Role  Stream  Received  Transmitted
2.2.2.2          10.10.20.50    Slave  0        45716     22826
6.6.6.2          6.6.6.1        Master  4        24960     74880

```

show ptp statistics (with IPv6 addresses for PTP master/slave)

```

user@host> show ptp statistics
Local Clock      Remote Clock    Role  Stream
Received Transmitted
ge-0/1/5.0       2001:cdba:0000:0000:0000:0000:3257:9653 Master  4
727205           345698
ge-0/2/0.0       2001:cdba:0000:0000:0000:0000:3256:0101 Master  5
4493776          222524

```

show ptp statistics detail

```

user@host> show ptp statistics detail

```

| Local Address | Remote Address | Role | Stream | Received | Transmitted |
|---------------|----------------|----------|--------|----------|-------------|
| 2.2.2.2 | 10.10.20.50 | Slave | 0 | 47009 | 23470 |
| | Signalling | Announce | Sync | Delay | Error |
| Rx: | 5 | 184 | 23399 | 23426 | 0 |
| Tx: | 45 | 0 | 0 | 23426 | 0 |
| 6.6.6.2 | 6.6.6.1 | Master | 4 | 25600 | 76800 |
| | Signalling | Announce | Sync | Delay | Error |
| Rx: | 0 | 0 | 0 | 25600 | 0 |
| Tx: | 0 | 25600 | 25600 | 25600 | 0 |

show ptp statistics detail (with IPv6 addresses for PTP master/slave)

```

user@host> show ptp statistics detail
Local Clock      Remote Clock      Role Stream      Received Transmitted
ge-0/1/5.0       2001:cdba:0000:0000:0000:0000:3257:9653 Master          4
727205          345698
      Signalling  Announce      Sync      Delay      Error
Rx:          0      33978      347535      345692      6
Tx:          0      0      0      345698      0
Local Clock      Remote Clock      Role Stream      Received Transmitted
ge-0/2/0.0       2001:cdba:0000:0000:0000:0000:3256:0101 Master          5
4493776          2222524
      Signalling  Announce      Sync      Delay      Error
Rx:          0      36819      2234472      2222485      14
Tx:          0      0      0      2222524      0

```

show ptp statistics detail (Enterprise profile statistics for remote devices on the QFX Series)

```

user@host> show ptp statistics detail
Local Clock      Remote Clock      Role Stream      Received Transmitted
xe-0/0/6:0.0     224.0.1.129      Slave          0          0          0
      Signalling  Announce      Sync      Delay      Error
Rx:          0      1688      217905      129833      131
Tx:          0      0      0      130608      0

Local Clock      Remote Clock      Role Stream      Received Transmitted
xe-0/0/6:1.0     224.0.1.129      Master          0          0      80517
      Signalling  Announce      Sync      Delay      Error
Rx:          0      0      0      0      0
Tx:          0      625      79892      0      0

Local Clock      Remote Clock      Role Stream      Received Transmitted
xe-0/0/6:1.0     50.50.50.2       Master          0      249980      249980
      Signalling  Announce      Sync      Delay      Error
Rx:          0      0      0      249980      0
Tx:          0      0      0      249980      0

Local Clock      Remote Clock      Role Stream      Received Transmitted
xe-0/0/6:1.0     50.50.50.3       Master          0      18520      18600
      Signalling  Announce      Sync      Delay      Error
Rx:          0      0      0      18520      0
Tx:          0      0      0      18600      0

Local Clock      Remote Clock      Role Stream      Received Transmitted
xe-0/0/6:1.0     50.50.50.10      Master          0          0          0
      Signalling  Announce      Sync      Delay      Error
Rx:          0      0      0      0      0

```

Tx: 0 0 0 0 0