Junos® OS

Time Management Administration Guide for Routing Devices

Modified: 2019-06-21

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

Junos® OS Time Management Administration Guide for Routing Devices

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://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

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.

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.xsl;
    }
  }
}
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.xsl; }
```


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 xiii 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`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	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** ***domain-name***
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• 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 *metric*>;**
| (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** **(*string1* | *string2* | *string3*)**
# (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 [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		    route default {
		      nexthop *address*;
		      retain;
		    }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

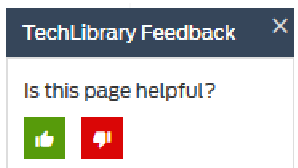
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• 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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide 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 Juniper Care or Partner Support Services 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/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- 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://support.juniper.net/support/requesting-support/.

CHAPTER 1

Configuring Date and Time

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 194

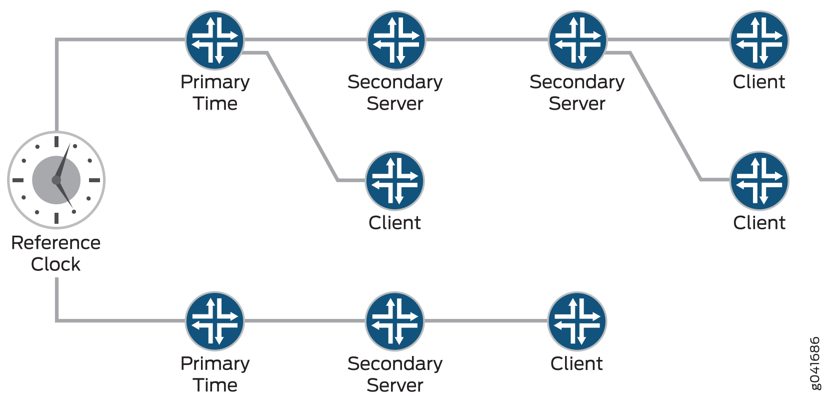
NTP Overview

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. Starting in Junos OS Release 18.2R1, there must be no space in the password for configuring the Network Time Protocol (NTP) authentication-key.

Release History Table

Release	Description
18.2R1	Starting in Junos OS Release 18.2R1, there must be no space in the password for configuring the Network Time Protocol (NTP) authentication-key.

Related Documentation

- Synchronizing and Coordinating Time Distribution Using NTP on page 22
- 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:

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>
    <ttl 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 18
- Understanding NTP Time Servers on page 21
- 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.brhelwig.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 21
- *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:

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 30.

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 30. For information about how to configure an NTP boot server, see "Configuring the NTP Boot Server" on page 22. 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 "$9$EgfcrvX7VY4ZEcwgoHjkP5Q3CuREyv87";
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 30.

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 30.

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 30.

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 30. 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 27.

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 adding 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 21
- 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 18
- Understanding NTP Time Servers on page 21
- **show ntp associations on page 196**
- **show ntp status on page 198**

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 (Message Digest 5 [MD5], SHA1, and SHA2-256 are 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 21
- 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 31
- 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

Automatic Clock Selection Overview

Automatic clock selection is the selection of the best quality clock source by the clock source selection algorithm based on the Ethernet Synchronization Message Channel (ESMC) Synchronization Status Message (SSM) quality level, the configured quality level, and the priority.

Clock Source Selection Algorithm

The clock source selection algorithm is triggered by the following events:

- Changes in the received ESMC SSM quality level (QL)
- Configuration changes. For example, the addition or deletion of a clock source, a change to the QL mode, and so on.
- Signal failure detected on the currently selected source.

When the router is configured with automatic clock selection, the system chooses up to two best upstream clock sources. The system then uses the clock recovered from one of the sources to lock the chassis clock. If an upstream clock with acceptable good quality is not available or if the system is configured in free-run mode, the system uses the internal oscillator.

Clock Selection and Quality Level

Automatic clock selection supports two modes: QL enabled and QL disabled.

- QL disabled— In this mode, the best clock is selected based on the configured ESMC SSM QL. If the QL of the configured clocks are equal, the clock selection is based on the configured priority. If both the configured QL and priority are equal, one of the sources is randomly selected. Absence of the **quality-mode-enable** statement at the [**edit chassis synchronization**] hierarchy level means that QL is disabled.

  NOTE: **The default setting is QL disable.**

- QL enabled—In this mode, the best clock is selected based on the incoming ESMC SSM QL as long as the incoming QL is at least as good as the source's configured QL. If the QLs are equal, the clock selection is based on the configured priority. If both the received QL and the priority are equal, one of the sources is selected randomly.

Selection Mode for the Incoming ESMC Quality

Depending on the configuration, the clock source selection algorithm uses the configured or received ESMC SSM quality level for clock selection. In both configured and received selection modes, the interface qualifies for clock source selection only when the received ESMC SSM quality level on the interface is equal to or greater than the configured ESMC SSM quality level for the interface.

Related Documentation

- External Clock Synchronization Overview for ACX Series Routers on page 33
- Configuring External Clock Synchronization for ACX Series Routers on page 35

- *synchronization*

External Clock Synchronization Overview for ACX Series Routers

The ACX Series Universal Metro routers support external clock synchronization and automatic clock selection for Synchronous Ethernet, T1 or E1 line timing sources, and external inputs. Configuring external clock synchronization and automatic clock selection requires making clock selection, quality level (QL), and priority considerations. The clock source selection algorithm is used to pick the two best upstream clock sources from among all the various sources, based on system configuration and execution criteria such as QL, priority, and hardware restrictions.

Automatic Clock Selection

With automatic clock selection, the system chooses up to two best upstream clock sources. The system then uses the clock recovered from one of the sources to lock the chassis clock. If an upstream clock with acceptable good quality is not available or if the system is configured in free-run mode, the system uses the internal oscillator. The following automatic clock selection features are supported for Synchronous Ethernet, T1 or E1 line timing sources, and external inputs:

NOTE: Automatic clock selection does not apply to the IEEE 1588v2 recovered clock.

Automatic clock selection is supported on the ACX Series routers. Automatic clock selection of the best quality clock source is based on the Ethernet Synchronization Message Channel (ESMC) Synchronization Status Message (SSM) quality level, the configured quality level, and the priority. To configure automatic clock selection, include the **auto-select** option at the [**edit chassis synchronization**] hierarchy level. You can also configure the chassis to lock to the free-running local oscillator, which is the Stratum 3E oscillator, by including the **free-run** option at the [**edit chassis synchronization**] hierarchy level. The **auto-select** option enables the clock source selection algorithm to run. The clock source selection algorithm is triggered by the following events:

- Signal failure detected on the currently selected source
- Changes in the received Ethernet Synchronization Message Channel (ESMC) Synchronization Status Message (SSM) quality level (QL)
- Configuration changes. For example, the addition or deletion of a clock source, a change to the QL mode, and so on.

Automatic clock selection supports two modes on the ACX Series router: QL enabled and QL disabled. To configure QL mode, include the **quality-mode-enable** statement at the [**edit chassis synchronization**] hierarchy level.

- QL disabled—The default setting is disable, which means that when the **quality-mode-enable** statement is not configured, QL is disabled. In this mode, the best clock is selected based on the configured ESMC SSM QL. If the QL of the best clocks are equal, the clock selection is based on the configured priority. If both the configured QL and priority are equal, one of the sources is randomly selected.
- QL enabled—In this mode, the best clock is selected based on the incoming ESMC SSM QL as long as the incoming QL is at least as good as the source's configured QL. If the QLs are equal, the clock selection is based on the configured priority. If both the received QL and the priority are equal, one of the sources is selected randomly.

Clock Source Selection Algorithm

The clock source selection algorithm uses the following logic and restrictions:

- QL must be configured for non-external clocks, whether or not QL is enabled.
- For **network-option option-1**, QL must be configured for external clocks (**gps** or **bits**) whether or not QL is enabled.
- In the case of **network-option option-2**, the default QL for the external clocks is QL_STU, whether or not QL is enabled.
- Configuring priority is optional. When not specified, **gps** has a higher default priority than **bits**, and **bits** has a higher default priority than Gigabit Ethernet, 10-Gigabit Ethernet, and T1 or E1 clock, which have the lowest default priority.
- When QL is enabled, the received QL must be equal to or better than the configured QL for that particular source or else that source will not be considered for clock selection. This is so that a downstream client is guaranteed clock quality of a certain level (that “certain level” being the configured QL).

During clock selection:

- The active source with the highest QL is selected.
- If QL is the same for two or more sources, then the source with the highest priority is selected.
- If two or more sources have the same QL and priority, then the currently active source, if any, among these sources is selected.
- If two or more sources have the same QL and priority, and none of these is currently active, then any one of these may be selected.
- If selection-mode is *configured quality*, then the configured (or default) QL of the selected clock source is used for transmitting ESMC. If selection-mode is *received quality*, then the received QL of the selected clock source is used for ESMC transmit.
- In order to receive or transmit ESMC messages out of an interface, at least one logical interface should be configured on that interface. If the interface is currently not configured with a logical interface, you may do so using the **set interfaces** ***interface-name*** **unit 0** statement at the **edit** hierarchy level.

Related Documentation

- Configuring External Clock Synchronization for ACX Series Routers on page 35
- *Understanding Interfaces on ACX Series Universal Metro Routers*

Configuring External Clock Synchronization for ACX Series Routers

The ACX Series Universal Metro Routers support external clock synchronization for Synchronous Ethernet, T1 or E1 line timing sources, and external inputs. Configuring external clock synchronization requires making clock selection, quality level (QL), and priority considerations. The clock source selection algorithm is used to pick the two best upstream clock sources from among all the various sources, based on system configuration and execution criteria such as QL, priority, and hardware restrictions.

To configure external synchronization on the router, include the **synchronization** statement at the **[edit chassis]** hierarchy level.

Setting the Ethernet equipment clock (EEC) network type

The network type options set the frequency of the configured clock. When **bits** is configured with **option-1** on the ACX router, the Synchronous Ethernet equipment is optimized for 2048 Kbps, the speed of an E1 interface. When **bits** is configured with **option-2** on the ACX router, the Synchronous Ethernet equipment is optimized for 1544 Kbps, the speed of a T1 interface. To set the clock type, use the following command:

```
set chassis synchronization network-option (option-1 | option-2)
```

For **option-1**, QL must be configured for external clocks (**gps** or **bits**) whether or not QL is enabled. For **option-2**, the default QL for external clocks is QL_STU whether or not QL is enabled.

The following output shows an example of the configuration of the **network type** with **option-1**:

```
[edit]
user@host# show chassis
synchronization {
    network-option option-1;
}
```

Setting the clock mode

Clock mode sets the selection of the clock source from a free-running local oscillator or from an external qualified clock. The default clock mode is **auto-select**, which uses the best clock source. To set the clock mode, use the following command:

```
set chassis synchronization clock-mode (free-run | auto-select)
```

The following output shows an example of the configuration of the **free-run** option:

```
[edit]
user@host# show chassis
synchronization {
    clock-mode free-run;
}
```

NOTE: Automatic clock selection does not apply to the IEEE 1588v2 recovered clock.

Setting the quality mode

Specify the expected quality of the incoming clock on this source. The default is disable. To set the synchronization quality mode, use the following command:


```
set chassis synchronization quality-mode-enable
```

The following output shows the configuration of the **quality-mode-enable** statement:

```
[edit]
user@host# show chassis
synchronization {
    quality-mode-enable;
}
```

Setting the selection mode

The selection mode specifies whether the clock source selection algorithm should use the configured or received ESMC SSM quality level for clock selection. In both selection modes (**configured-quality** and **received-quality**), the interface qualifies for clock source selection only when the received ESMC SSM quality level on the interface is equal to or greater than the configured ESMC SSM quality level for the interface. To configure the ESMC SSM quality-based clock source selection mode, use the following command:

```
set chassis synchronization selection-mode (configured-quality | received-quality)
```

The following output shows the configuration of the **selection-mode** statement with the **configured-quality** option and the mandatory **quality-mode-enable** statement:

```
[edit]
user@host# show chassis
synchronization {
    selection-mode configured-quality;
    quality-mode-enable;
}
```

NOTE: For the **selection-mode** statement configuration to take effect, you must set the **quality-mode-enable** statement at the **[edit chassis synchronization]** hierarchy level.

Setting the time interval before a new clock source is selected

For routers operating with Synchronous Ethernet , set the time interval to wait before the router selects a new clock source. After a change in the configuration, the time to wait is between 15 and 60 seconds. After a reboot (restart), the time to wait is from 60 to 180 seconds. After clock recovery (switchover), the time to wait is from 30 to 60 seconds. The default switchover time is 30 seconds and cold boot time is 120 seconds. To set the time interval before a new clock source is selected, use the following command:

```
set chassis synchronization hold-interval (configuration-change | restart |
switchover) seconds
```

The following output shows the configuration of the **hold-interval** statement with the **configuration-change** option:

```
[edit]
user@host# show chassis
```

```
synchronization {
    hold-interval {
        configuration-change 20;
    }
}
```

Setting the synchronization switching mode

The configured switching mode determines the clock source used. In revertive mode, the system switches from a lower to a higher quality clock source whenever the higher clock source becomes available. In non-revertive mode, the system continues to use the current clock source as long as it is valid. The default mode is revertive. To set the synchronization switchover mode, use the following command:

```
set chassis synchronization switchover-mode (revertive | non-revertive)
```

The following output shows the configuration of the **switchover-mode** statement with the **non-revertive** option:

```
[edit]
user@host# show chassis
synchronization {
    switchover-mode non-revertive;
}
```

Setting the clock source

The configured clock source is the candidate for selection by the clock selection algorithm. The clock source can be the router's BITS T1 or E1 interface, GPS, or an interface with an upstream clock source. To set the clock source, use the following command:

```
set chassis synchronization source (bits | gps | interfaces interface-name)
```

The following output shows the configuration of the **source** statement with the **bits** option and the mandatory **network-option** statement. When **bits** is configured with **option-1** on the ACX2000 router, the Synchronous Ethernet equipment is optimized for 2048 Kbps, the speed of an E1 interface.

```
[edit]
user@host# show chassis
synchronization {
    network-option option-1;
    source {
        bits;
    }
}
```

NOTE: For the **source** statement configuration to take effect, you must set the **network-option (option-1 | option-2)** statement at the **[edit chassis synchronization]** hierarchy level.

The **bits** option is not supported on the ACX1000 router.

Setting ESMC transmit interface

The ESMC transmit interface is the interface on which ESMC transmit messages are permitted. To enable ESMC packet transmit, use the following command:

```
set chassis synchronization esmc-transmit interfaces interface-name
```

The following output shows the configuration of the **esmc-transmit** statement:

```
[edit]
user@host# show chassis
synchronization {
    esmc-transmit {
        interfaces ge-0/1/0;
    }
}
```

You can also enable ESMC on all interfaces with the **interfaces all** statement at the preceding hierarchy level.

Setting the synchronization source quality level

Specify the expected quality of the incoming clock on this source. Specific quality-level options are valid depending on the configured **network-option**; **option-1** or **option-2**. Both option-1 and option-2 SSM quality levels are supported. To set the synchronization source quality level, use the following command:

```
set chassis synchronization source (bits | gps | interfaces interface-name)
quality-level (prc | prs |sec | smc | ssu-a | ssu-b | st2 | st3 | st3e | st4 |
stu | tnc)
```

The following output shows the configuration of the **quality-level** statement configured with the **prc** option:

```
[edit]
user@host# show chassis
synchronization {
    source {
        bits {
            quality-level prc;
        }
    }
}
```

Setting the synchronization source priority

Specify a priority level between 1 and 5. When not specified, **gps** has a higher priority than **bits**,and **bits** has a higher default priority than other Gigabit Ethernet or 10 Gigabit Ethernet clock sources, which have the lowest priority. To set the synchronization source priority, use the following command:

```
set chassis synchronization source (bits | gps | interfaces interface-name)
priority number
```

The following output shows the configuration of the **priority** statement:


```
[edit]
user@host# show chassis
synchronization {
    source {
        bits {
            priority 2;
        }
    }
}
```

Setting the synchronization source wait to restore time

A wait-to-restore time can be configured for each port. When a port's signal transitions out of the signal fail state, it must be fault free for the wait-to-restore time before it is again considered by the selection process. The range is from **0** through **12** minutes. The default time is 5 minutes.

To set the synchronization source wait-to-restore time, use the following command:

`set chassis synchronization source interfaces` *`interface-name`* `wait-to-restore` *`minutes`*

The following output shows the configuration of the **wait-to-restore** statement:

```
[edit]
user@host# show chassis
synchronization {
    network-option option-1;
    source {
        interfaces ge-0/1/0 {
            wait-to-restore 2;
        }
    }
}
```

Setting the synchronization source lockout

A lockout may be configured for any source. When a lockout is configured for a source, that source will not be considered by the selection process. To set the synchronization source lockout, use the following command:

`set chassis synchronization source (bits | gps | interfaces` *`interface-name`*`) request lockout`

The following output shows the configuration of the **request lockout** statement:

```
[edit]
user@host# show chassis
synchronization {
    network-option option-1;
    source {
        bits {
            request lockout;
        }
    }
}
```


Setting the forced switch

Force a switch to the source provided that the source is enabled and not locked out. Only one configured source may be force-switched. To set the forced switch, use the following command:

```
set chassis synchronization source (bits | gps | interfaces interface-name)
request force-switch
```

The following output shows the configuration of the **request force-switch** statement:

```
[edit]
user@host# show chassis
synchronization {
    network-option option-1;
    source {
        bits {
            request force-switch;
        }
    }
}
```

Related Documentation

- External Clock Synchronization Overview for ACX Series Routers on page 33
- *synchronization*
- *Interface and Router Clock Sources Overview*

Global Positioning System (GPS) and the ACX Series Routers

Global Positioning System (GPS) is a navigation aid system that uses signals from satellites to calculate the actual position of a GPS-capable receiver. These signals are not only used for determining the position of the receiver on Earth but also as a very accurate time base. There are GPS receivers with 10-MHz clock frequency output synchronized to a GPS satellite. The ACX Series router has a SubMiniature version B (SMB) connector that can take 10-MHz sine-wave input from a GPS receiver. To configure this 10-MHz clock from a GPS receiver as a candidate clock source for chassis synchronization, include the **gps** statement and options at the [**edit chassis synchronization source**] hierarchy level.

NOTE: ACX500 routers do not require an external GPS receiver because the GPS receiver is integrated into the system.

Related Documentation

- External Clock Synchronization Overview for ACX Series Routers on page 33
- Configuring External Clock Synchronization for ACX Series Routers on page 35
- *source*

Integrated Global Navigation Satellite System (GNSS) on ACX500 Series Routers

Global Navigation Satellite System (GNSS) is a navigation aid system that uses signals from satellites to calculate the actual position of a GPS-capable receiver. These signals are not only used for determining the position of the receiver on Earth but also as a very accurate time base.

The ACX500 series router has the GNSS receiver integrated into the system. This eliminates the need to have an external GPS receiver. However, you will need a GPS antenna. The ACX500 series routers support GNSS input through SubMiniature version A (SMA) connector. You can configure the GNSS port and its associated parameters at the [**edit chassis synchronization**] hierarchy level.

You can configure the GNSS port by including the **constellation *gps*]** CLI statement at the [**edit chassis synchronization port gnss**] hierarchy level. If you do not specify a **constellation** option, then the *gps* constellation option is considered by default.

The following is the [**edit chassis synchronization port gnss**] hierarchy level:

```
[edit chassis synchronization]
port gnss client {
   cable-length-compensation {
      time delay-in-nanoseconds;
   }
   constellation [gps];
   anti-jamming;
}
```

NOTE:

- The range for **cable-length-compensation** is from *0 to 50000000* nanoseconds.
- The integrated GNSS receiver in the ACX500 series routers do not support 10-MHz frequency input and output.

ACX500 series routers support grandmaster clock functionality with the integrated GNSS receiver.

Use the **show chassis synchronization gnss** command to check the status of the GNSS receiver. For more information, see *show chassis synchronization*.

Related Documentation

- *show chassis synchronization*
- *source*

Assisted Partial Timing Support on ACX500 Routers Overview

The assisted partial timing support (APTS), which is a Global Navigation Satellite System (GNSS) backed by Precision Time Protocol (PTP), delivers accurate timing and synchronization in mobile backhaul networks.

NOTE: The APTS feature is supported only on the Junos OS Release 12.3X54–D25 for ACX500 router.

On the ACX500 router, the APTS feature helps you to configure PTP slave ports on a GNSS grandmaster serving as the PTP master.

APTS uses GNSS as the primary time reference at cell site locations, or at an aggregation point close to the cell sites. APTS uses network-based timing distribution to assist and maintain the timing during holdover periods when GNSS is unavailable.

To support this feature, you need an APTS node with GNSS source configured at the [**edit chassis synchronization**] hierarchy level and PTP boundary clock configured at the [**edit protocols ptp**] hierarchy level as shown below:

GNSS configuration

```
[edit chassis]
  synchronization {
            network-option <option-1 | option-2>;
            port gnss {
                  client {
                       constellation <constellation-type>;
                      anti-jamming;
                   }
            }
           esmc-transmit {
                 interface <interfaces-name>;
           }
     }
```

PTPoE Configuration

```
[edit protocols]
 ptp {
            clock-mode boundary;
            slave {
                      interface <slave-ptp-ifl> {
                      multicast-mode {
                             transport ieee-802.3 [ link-local ] ;
                      }
                  }
           }
          master {
                interface <master-ptp-ifl> {
                    multicast-mode {
                    transport ieee-802.3 [ link-local ] ;
                  }
               }
        }
```

PTPoIP Configuration

```
[edit protocols]
clock-mode boundary;
    slave {
            interface <logical-interface-name> {
            unicast-mode {
                transport ipv4;
                clock-source <remote-master-ip-address> local-ip-address
<local-slave-ip-address>;
            }
        }
    }
    master {
        interface <logical-interface-name>{
            unicast-mode {
                transport ipv4;
                clock-client <remote-slave-ip> local-ip-address
<local-master-ip>;
            }
        }
    }
   }
```

The priority of clock source would be GNSS first and then PTP.

You can use the **show ptp lock-status detail**, **show chassis synchronization extensive**, and **show chassis synchronization gnss extensive** show commands to monitor and troubleshoot the configurations.

Related Documentation

- *show chassis synchronization*
- *source*

CHAPTER 2

Configuring Time Zones

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 18
- Updating the IANA Time Zone Database on Junos OS Devices on page 46

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 46
2. Configuring a Custom Time Zone on page 48

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 45
- NTP Overview on page 18
- Understanding NTP Time Servers on page 21
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30
- **use-imported-time-zones on page 192**

CHAPTER 3

Configuring Network Time Protocols

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 21
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization on page 30
- *trusted-key*

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 55

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:

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 50
- Synchronizing and Coordinating Time Distribution Using NTP on page 57

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 50

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 50

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 50

Related Documentation

- Understanding NTP Time Servers on page 21
- 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 182

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 56
- Configuring the NTP Time Server and Time Services on page 52
- 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 55
- Configuring the NTP Time Server and Time Services on page 52
- 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 57
2. Configuring the NTP Boot Server on page 58
3. Specifying a Source Address for an NTP Server on page 58

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> <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;
  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 21
- 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 59
- Overview on page 60
- Configuration on page 60
- Verification on page 61

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 61
- Displaying the NTP Peers on page 61
- Displaying the NTP Status on page 62

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 21
- *ntp*
- Configuring the NTP Time Server and Time Services on page 52
- 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 18
- Understanding NTP Time Servers on page 21
- **show ntp associations on page 196**
- **show ntp status on page 198**

CHAPTER 4

Configuring Precision Time Protocols

- Example: Configuring PTP over Ethernet for Multicast Master, Slave, and Dynamic Ports on page 139
- Hybrid Mode on ACX Series Routers Overview on page 147
- Guidelines for Configuring Hybrid Mode on ACX Series Routers on page 149
- Configuring Hybrid Mode and ESMC Quality Level Mapping on ACX Series Routers on page 150
- Example: Configuring Hybrid Mode and ESMC Quality Level Mapping on page 153
- Understanding Timing Defects and Event Management on ACX Series on page 160
- Understanding SNMP MIB for Timing on ACX Series on page 162

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 QFX5100, EX4600, ACX5048, ACX5096, ACX6360-OR, and PTX10001-20C devices act as transparent clocks only and operate 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 , ACX5096, ACX6360-OR, and PTX10001-20C devices 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, which is not supported on ACX6360-OR, and PTX10001-20C devices, estimated timestamps are sent in one packet, and additional packets contain updated timestamps.

NOTE: **ACX5048 , ACX5096, ACX6360-OR, and PTX10001-20C devices 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.

On QFX5100 and EX4600 switches, 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.**

NOTE: **ACX6360-OR and PTX10001-20C devices 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

ACX6360-OR and PTX10001-20C devices do not support the following:

- Boundary, ordinary, master, and slave clocks
- Transparent clock over MPLS switched path
- Transparent clock with more than two VLAN tags
- PTP over Ethernet
- PTP over IPv4
- PTP multicast mode
- Configuration of unicast and broadcast modes.

  Unicast mode is enabled by default.
- Transparent clock in transponder mode
- PTP while MACSec is enabled
- Two-step process

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 85
- **e2e-transparent on page 179**

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 68
- Clock Clients on page 70

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.

ACX5448 router supports PTP boundary clocks for phase and time synchronization using IEEE-1588 Precision Timing Protocol (PTP). The ACX5448 router supports the following features:

- PTP over IPv4 (IEEE-1588v2)
- PTP ordinary and boundary clocks
- One step clock mode operation for PTP Master
- 10Mhz and 1PPS output for measurement purpose

All PTP packets uses the best-effort queue instead of network control queue.

If **clksyncd-service** restart is initiated, then the **show ptp lock status detail** CLI command output of **Clock reference state** and **1pps reference state** fields shows incorrect information. The following is a sample of output for **show ptp lock status detail**:

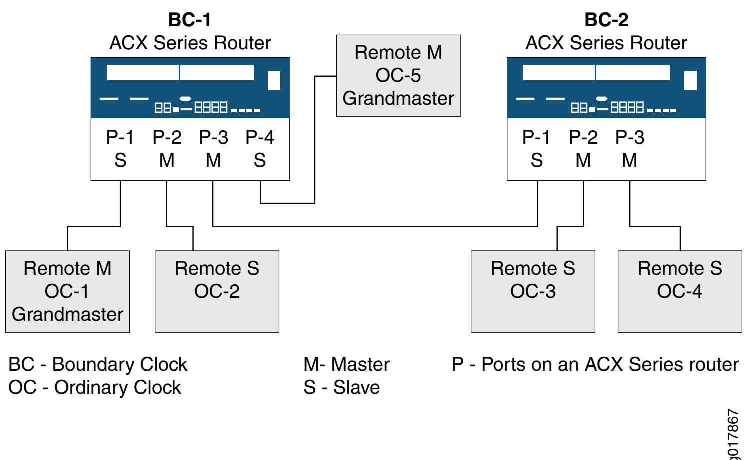
```
user@host> show ptp lock-status detail
Lock Status:

Lock State    : 5 (PHASE ALIGNED)
Phase offset  : 0.000000010 sec
State since   : 2018-11-22 00:38:56 PST (00:10:18 ago)
```

```
Selected Master Details:
Upstream Master address     : 12.0.0.1
Slave interface             : xe-0/0/20.0
Clock reference state       : Clock locked
1pps reference state        : Clock qualified
```

Figure 1 on page 69 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



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 page 71
- *Precision Time Protocol Overview*
- Configuring Precision Time Protocol Clocking on page 103
- *Supported IPv4, TCP, and UDP Standards*

IEEE 1588v2 Precision Timing Protocol (PTP)

Starting with Junos OS Release 19.1R1, on QFX5110 switches, the IEEE 1588v2 Precision Time Protocol default profile supports aggregated Ethernet interfaces and the loopback interface using IPv4 and IPv6 unicast transport.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.
- Support for aggregated Ethernet interfaces.

  You can configure an aggregated Ethernet interface and its configured IP address for PTP streams acting as slaves or masters. IP hashing determines which physical link to use for the PTP traffic flows. Both IPv4 unicast and IPv6 unicast transport are supported.
- Support for loopback interface.

  You can configure a loopback interface (there is only one loopback interface, and it is lo0.0) and its corresponding IP addresses for PTP streams acting as slaves or masters. The IP address configured on lo0.0 is used as the local IP address in the PTP configuration statements, and the remote master or slave IP address is used to identify the destination forwarding direction. You can configure multiple IP addresses on lo0.0, which allows different unique PTP streams to co-exist on lo0.0. Although, the loopback interface is the same for both masters and slaves, the IP addresses must be unique. Both IPv4 unicast and IPv6 unicast transport are supported.

Release History Table

Release	Description
19.1R1	Starting with Junos OS Release 19.1R1, on QFX5110 switches, the IEEE 1588v2 Precision Time Protocol default profile supports aggregated Ethernet interfaces and the loopback interface using IPv4 and IPv6 unicast transport.

Related Documentation

- *Precision Time Protocol Overview*
- IEEE 1588v2 PTP Boundary Clock Overview on page 68
- Configuring Precision Time Protocol Clocking on page 103
- *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.
- Support for aggregated Ethernet interfaces.

  You can configure an aggregated Ethernet interface and its configured IP address for PTP streams acting as slaves or masters. IP hashing determines which physical link to use for the PTP traffic flows. Both IPv4 unicast and IPv6 unicast transport are supported.
- Support for loopback interface.

  You can configure a loopback interface (there is only one loopback interface, and it is lo0.0) and its corresponding IP addresses for PTP streams acting as slaves or masters. The IP address configured on lo0.0 is used as the local IP address in the PTP configuration statements, and the remote master or slave IP address is used to identify the destination forwarding direction. You can configure multiple IP addresses on lo0.0, which allows different unique PTP streams to co-exist on lo0.0. Although, the loopback interface is the same for both masters and slaves, the IP addresses must be unique. Both IPv4 unicast and IPv6 unicast transport are supported.

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	• Master: -3 • Slave: 0	-3 – 0
Delay request/response rate	• Master: -6 • Slave: -7	-7 – -3
Sync rate	• Master: -7 • Slave: -6	-7 – -3

Related Documentation

- Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 86

Understanding the PTP Media Profiles

The PTP media profiles comprise three profiles: SMPTE ST-2059-2, AES67, and AES67+SMPTE ST-2059-2. These profiles support video and audio applications for capture (for example, cameras) to be used in professional broadcast environments. These profiles supports PTP over IPv4 multicast and ordinary and boundary clocks.

Benefits of the PTP Media Profiles

- The PTP media profiles enable multiple video and audio sources to stay in synchronization across multiple devices.

Functionality Common to the SMPTE ST-2059-2, AES67, and the AES67+SMPTE ST-2059-2 Profiles

These profiles include the following functionality:

NOTE: **These profiles do not use an alternate master clock, path trace, unicast message negotiation, alternate time scales, or acceptable master table.**

- Support for both ordinary clocks and boundary clocks as part of the IEEE 1588 PTP specification.
- Support for encapsulating PTP over IPv4/UDP.

  Multicast is required for both PTP over IPv4 and PTP over UDP.
- Support for IEEE 1588 delay request and response method for the path delay measurement.
- Support for the default IEEE 1588 BMCA algorithm.
- Support for standard management packets.
- Support for IGMPv2.

  IGMPv3 is optional.

Understanding the SMPTE Profile

The SMPTE profile is based on the SMPTE ST-2059-2 standard and was created specifically to synchronize video equipment in a professional broadcast environment. The standard allows multiple video sources to stay in synchronization across various equipment by providing time and frequency synchronization to all devices. This standard is used with other SMPTE standards such as SMPTE ST 2059-1, which defines a point in time (the SMPTE Epoch) used for aligning real-time signals, and formula for ongoing signal alignment. Alignment is considered met when two clocks are within 1 microsecond of each other. This implies that each slave should be accurate with +/- .5 microseconds of the central clock.

Understanding the AES67 Profile

The AES67 profile is based on the AES67 standard and supports professional quality audio applications for high performance streaming over IPv4 multicast transport in media networks with low latencies. This profile enables audio streams to be combined at a receiver and maintain stream synchronization. The standard uses IPv4 multicast and IGMP, plus the DiffServ and DSCP fields, to select packet quality of service. Audio devices transmit their content using RTP (Real Time Protocol).

Understanding the AES67+SMPTE ST-2059-2 Profile

The AES67+SMPTE ST-2059-2 profile is based on both the AES67 and SMPTE ST-2059-2 standards and is used in professional audio and video media applications. This profile enables the two standards to operate together over the same network.

Related Documentation

- Configuring the PTP Media Profiles on page 90

PTP over Ethernet on ACX Series Routers Overview

Precision Time Protocol (PTP) is supported over IEEE 802.3 or Ethernet links on ACX Series routers. This functionality is supported in compliance with the IEEE 1588-2008 specification. PTP over Ethernet enables effective implementation of packet-based technology that enables the operator to deliver synchronization services on packet-based mobile backhaul networks that are configured in Ethernet rings. Deployment of PTP at every hop in an Ethernet ring by using the Ethernet encapsulation method enables robust, redundant, and high-performance topologies to be created that enables a highly precise time and phase synchronization to be obtained.

The ACX Series routers can be directly connected to different types of base stations (for example, base transceiver station (BTS) in 2G, NodeB in 3G, and eNodeB in 4G networks) and different types of routers that hand off time- division multiplexing (TDM), ATM, and Ethernet traffic to the base station controller. ACX Series routers must extract the network clock from these sources and pass on synchronization information to the base stations to help the routers synchronize with the base station controller.

Most of the network deployments that use Ethernet contain a minimum of two Ethernet rings, while some of the network topologies might also contain up to three Ethernet rings. Consider a scenario in which the first ring contains aggregation routers (MX Series routers) and the second ring contains access routers (ACX Series routers). In such a network, about 10 or 12 nodes of MX Series routers and ACX Series routers are present in the aggregation and access Ethernet rings.

Some of the 4G base stations that are connected to ACX Series routers need to receive the timing and synchronization information in a packet-based form. Such base station vendors support only packet interfaces that use Ethernet encapsulation for PTP packets for time and phase synchronization. Therefore, any node (an ACX Series router) that is directly connected to a 4G base station must be able to use the Ethernet encapsulation method for PTP on a master port to support a packet-based timing capability.

PTP over Ethernet encapsulation also facilitates an easier, optimal network deployment model than PTP over IPv4. Using IPv4, the nodes (master and slave devices) participate in unicast negotiation in which the slave node is provisioned with the IP address of the master node and requests unicast messages to be sent to it from the master node. A master node is the router that functions as the PTP server where the master clock is located and a slave node is the router that functions as the PTP client where the slave clock is located. Because PTP over Ethernet uses multicast addresses, the slave node automatically learns about the master nodes in the network. Also, the slave node is able to immediately receive the multicast messages from the master node and can begin sending messages to the master node without the need for any provisioning configuration.

An interface on which the master clock is configured is called a master interface and an interface on which the slave clock is configured is called a slave interface. A master interface functions as the master port and a slave interface functions as the slave port. For PTP over Ethernet, apart from configuring a port or a logical interface to operate as a master clock or a slave clock, you can also configure a port or a logical interface to function as both a master clock and a slave clock. This type of port is called a *dynamic port*, *stateful port*, or a *bidirectional port*. Such a stateful port enables the network to more efficiently adapt to the introduction and failure of timing sources by forming the shortest synchronization trees from a particular source. This behavior is implemented as defined by the best master clock algorithm (BMCA) in the *ITU-T G.8265.1 Precision time protocol telecom profile for frequency synchronization* specification.

On both MX Series and ACX Series routers, you can achieve the highest quality performance if you configure every node in a synchronization chain as a PTP boundary clock. In Ethernet ring-based topologies, you can configure a port or a logical interface to function either as a master port or as a slave port to enable redundancy when a node or link failure occurs. This dynamic port or dual-port functionality is in accordance with the IEEE 1588-2008 standard and enables the implementation of PTP in data center or financial applications.

Apart from enabling every node to be available for configuration as a PTP boundary clock, it is also necessary to enable a logical interface to be configured either as a master port or a slave port. When you configure a logical interface or even a shared IP address to be a master port or a slave port, a PTP protocol stack can represent dynamic ports and the PTP application selects the correct state (master or slave) for any specific port in the system based on the output of the default PTP BMCA and the states of other ports in the system.

While an ACX Series router supports the PTP over Ethernet functionality, a Brilliant Grand Master such as an MX Series router or a TCA Series Timing Client does not support PTP over Ethernet. In such a scenario, the ACX Series router functions as a boundary clock with a PTP slave port using IPv4 as the encapsulation mode and master ports using Ethernet as the encapsulation mode for PTP traffic. For example, consider an ACX Series router named ACX1 to have two potential slave interfaces, one that is fixed as a slave-only port using IPv4 on the link toward an MX Series router named MX1, and a dynamic port that functions as a slave port using PTP over Ethernet on the link toward another ACX Series router named ACX2. In addition, ACX1 also contains a port that is a master-only port using PTP over Ethernet and connects to the base station.

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 communication with the master node 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 the forwarding of PTP traffic. The IEEE 1588 standard defines two types of multicast MAC addresses 01-80-C2-00-00-0E (link local multicast) and 01-1B-19-00-00-00 (standard Ethernet multicast) for PTP over Ethernet operations.

Related Documentation

- Guidelines for Configuring PTP over Ethernet on page 79
- Configuring PTP Multicast Master and Slave Ports for Ethernet Encapsulation on page 132
- Configuring PTP Dynamic Ports for Ethernet Encapsulation on page 138
- Example: Configuring PTP over Ethernet for Multicast Master, Slave, and Dynamic Ports on page 139
-

Guidelines for Configuring PTP over Ethernet

Keep the following points in mind when you configure PTP over Ethernet for multicast mode of transmission of PTP traffic:

- You can configure a port or a logical interface to be a master clock for PTP over Ethernet to provide packet-based synchronization to base stations that support time and phase alignment; this configuration is compliant with Annexure F of the IEEE 1588-2008 specification.
- Two multicast MAC addresses are used for PTP over Ethernet: 01-1B-19-00-00-00 and 01-80-C2-00-00-0E. The first address is a more standard Ethernet MAC address that is expected to be flooded by all types of Ethernet bridges and switches and also by a large number of base station vendors. A node with this MAC address can be a node that does not process PTP packets. The second address is a reserved address in the IEEE 802.1Q standard for Ethernet encapsulation that is required to be filtered and not forwarded. This MAC address is used to ensure complete end-to-end support of PTP, instead of transmission of packets through any network element that does not support PTP. This address is the default address for G.8275.1 (PTP Profile for time or phase distribution) and a node with this MAC address is a node that supports processing of PTP packets.
- Both of the MAC addresses, 01-1B-19-00-00-00 and 01-80-C2-00-00-0E, are supported on multiple ports simultaneously to enable maximum flexibility and extension of existing networks for future deployments. A single PTP port is configured for one of the MAC addresses at a time.
- PTP packets are sent with the unique MAC address assigned to each port as the MAC source address. In the PTP packet, the Ethernet frame portion of the packet contains the Destination MAC field. This field contains either of the two MAC addresses, 01-1B-19-00-00-00 or 01-80-C2-00-00-0E. Also, the Ethernet frame portion contains

the Source MAC field that contains the MAC address of the source port and the Ethertype field that contains the PTP Ethertype value of 0x88F7. Apart from the Ethernet frame, the PTP packet contains the PTP payload.

- When you configure a port for PTP over Ethernet to be a slave port, a master port, or both by having a dynamic port that can be either a master port or a slave port depending on the states of the other ports in the PTP application, it is possible to build an easily provisioned, redundant PTP service in an Ethernet ring where every node is configured as a boundary clock.
- A boundary clock can function as a slave clock to a device using IP (such as a TCA Series Timing Client or an MX Series router) on one port and can also function as a slave clock, a master clock, or both on other ports using Ethernet as the encapsulation method. This behavior occurs within a single PTP domain number.
- Best Master Clock Algorithm (BMCA) and the port state machine are supported to determine the states of all the ports in a system and the correct state (master or slave) for a certain port to process PTP packets.
- PTP over Ethernet supports fully redundant and resilient ring-based configurations of up to 10 nodes for a form of fourth-generation (4G) evolution known as Long-Term Evolution-Time Division Duplex (LTE-TDD). ACX Series routers support a single node or link failure and all nodes maintain a phase accuracy of plus or minus 1.5 microseconds matching a common source.
- You can configure the asymmetry value between the master port and the slave port, which indicates a value to be added to the path delay value to make the delay symmetric and equal to the path from the master port to the slave port, on either a dynamic-state port or a slave-only port.
- You cannot enable PTP over Ethernet on Ethernet interfaces that are configured with 802.1Q VLAN tags or contain a user-configured MAC address.
- While you can configure unique PTP slave interfaces or slave ports with different encapsulation mechanisms (such as IPv4 and Ethernet), the boundary clock can use only a single encapsulation method for all of the master ports. Therefore, you must define either IPv4 or Ethernet encapsulation for all the ports or logical interfaces that can possibly function as boundary clock masters. Master ports select the link-local flag based on each port.
- The following limitations apply to the maximum number of ports that you can configure when you use PTP over Ethernet:
  - You can configure a maximum of four slave ports on a router. A slave port or logical interface is defined as any slave-only port configured for IPv4 or Ethernet, or any dynamic port configured for Ethernet.
  - You can configure up to 29 master ports on a router. A master port or logical interface is defined as any master-only port configured for IPv4 or Ethernet, or any dynamic port configured for Ethernet.
  - Any logical interface that you configure as a dynamic port is considered to be both a slave port and a master port, even if it functions only as a slave port or a master port in a network, when the total number of slave ports and master ports on a router is computed.

- In PTP over IPv4 deployment, it is necessary to configure certain basic settings on a PTP master port before the PTP slave ports to connect to the master port. PTP over Ethernet offers a plug-and-play service because any PTP client starts receiving packets and can request delay-response packets from the master port after you configure an interface to be a master.
- PTP over Ethernet is compatible with Junos OS releases earlier than Release 12.3X51. When you perform an upgrade to Release 12.3X51 and later from a previous release on an ACX Series router, you can modify the slave and master ports previously configured for IPv4 to enable PTP over Ethernet based on your network needs.
- You cannot configure a fully redundant PTP ring using IP. A fully redundant PTP ring is supported only when Ethernet encapsulation is used.
- Configuration of dynamic ports in conjunction with Synchronous Ethernet to enable hybrid mode is not supported.
- Multiple PTP timing domains are not supported for PTP over Ethernet, similar to PTP over IPv4. Although a single node can contain interfaces configured for PTP over IPv4 and PTP over Ethernet, both of these interfaces must be part of the same PTP domain.
- SONET/SDH networks define the ability to configure a local priority to a synchronization source in the ITU G.781 standard. Addition of such locally configured priorities to PTP sources to influence BMCA to determine a particular path for PTP packets is not supported.
- Although you can configure a slave port to use either IP or Ethernet simultaneously, a single slave port is selected based on the announce messages it receives from the master port and the PTP event packets are exchanged only with a single master port.
- The IPv4 unicast implementation of PTP enables you to limit the number of slave ports that can be supported simultaneously in the system. With multicast Ethernet-based implementation, in which the master port is not provisioned with the slave port information, the master port cannot limit the number of slave ports that it services. This control must be exercised with proper networking planning and design.

Related Documentation

- PTP over Ethernet on ACX Series Routers Overview on page 77
- Configuring PTP Multicast Master and Slave Ports for Ethernet Encapsulation on page 132
- Configuring PTP Dynamic Ports for Ethernet Encapsulation on page 138
- Example: Configuring PTP over Ethernet for Multicast Master, Slave, and Dynamic Ports on page 139

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 66
- e2e-transparent on page 179
- show ptp global-information on page 204

Configuring a PTP Transparent Clock

ACX Series routers supports transparent clock functionality. A Precision Time Protocol (PTP) Transparent clock measures the residence time of PTP packets as they pass through router. This residence time is added to the Correction Field of the PTP packet.

NOTE: Starting in Junos OS Release 17.1 onwards, to configure transparent clock, include the **e2e-transparent** CLI command at the [**edit protocols ptp**] hierarchy level. Prior to Junos OS Release 17.1, to configure transparent clock, include the **transparent-clock** CLI command at the [**edit protocols ptp**] hierarchy level.

The following points need to be considered while configuring a PTP transparent clock in ACX routers:

- Domain numbers—Transparent clock functionality would compute the residence time for PTP packets belonging to all domains.
- PTP-over-MPLS—Transparent clock functionality do not support PTP carried over MPLS in ACX routers.

The PTP transparent clock functionality is supported on PTP-over-IP and PTP-over-Ethernet (PTPoE).

NOTE: ACX routers do not support PTPoE over VLANs when it works in ordinary clock or boundary clock mode.

To configure a PTP transparent clock:

1. Configure the clock mode:

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

2. Configure the transparent clock:

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

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

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

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

This topic includes the following tasks:

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
   ```

   NOTE: You can configure an aggregated Ethernet interface and its configured IP address for PTP streams acting as slaves or masters.

   For example, to configure a slave using an aggregated Ethernet interface:

   ```
   user@switch# set protocols ptp slave interface ae0.0
   ```

   NOTE: You can configure a loopback interface (there is only one loopback interface, and it is lo0.0) and its corresponding IP addresses for PTP streams acting as slaves or masters. Although the loopback interface is the same for both masters and slaves, the IP addresses must be unique.

   For example, to configure a slave using the loopback interface:

   ```
   user@switch# set protocols ptp slave interface lo0.0
   ```

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 or IPv6.

```
[edit protocols ptp slave interface interface-name unicast-mode]
user@host# set transport (ipv4 | ipv6)
```

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
```

NOTE: You can configure an aggregated Ethernet interface and its configured IP address for PTP streams acting as slaves or masters.

For example, to configure a master using an aggregated Ethernet interface:

```
user@switch# set protocols ptp master interface ae0.0
```

NOTE: You can configure a loopback interface (there is only one loopback interface, and it is lo0.0) and its corresponding IP addresses for PTP streams acting as slaves or masters. Although the loopback interface is the same for both masters and slaves, the IP addresses must be unique.

For example, to configure a master using the loopback interface:

```
user@switch# set protocols ptp master interface lo0.0
```

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 or IPv6.

```
[edit protocols ptp master interface interface-name unicast-mode]
user@host# set transport (ipv4 | ipv6)
```

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 74

Configuring the PTP Media Profiles

NOTE: When you enable any of the PTP media profiles (AES67, AES67+SMPTE, or SMPTE), you cannot enable any other profile.

Configuring the AES67, SMPTE, and AES67+SMPTE Profiles

This topic provides the configuration necessary to enable any of the three media profiles (AES67, SMPTE, and AES67+SMPTE), and includes the following sections.

Optional and Required Parameters for SMPTE ST-2059-2, AES67, and AES67+SMPTE ST-2059-2 Profiles

Table 4 on page 91 and Table 5 on page 91 provide default values and ranges for optional and required PTP parameters:

Table 4: Defaults and Ranges for PTP Parameters

Profile	SM (Synchronization Metadata) TLV	Domain	Priority1	Priority2
SMPTE	Yes	• Default: 127 • Range: 0 through 127	• Default: 128 • Range: 0 through 255	• Default: 128 • Range: 0 through 255
AES67	No	• Default: 0 • Range: 0 through 127	• Default: 128 • Range: 0 through 255	• Default: 128 • Range: 0 through 255
AES67+SMPTE	Yes	• Default: 0 • Range: 0 through 127	• Default: 128 • Range: 0 through 255	• Default: 128 • Range: 0 through 255

Table 5: Defaults and Ranges for PTP Parameters

Profile	Announce	Announce Timeout	Sync	Delay-Req
SMPTE	• Default: -2 • Range: -3 through 1	• Default: 3 • Range: 2 through 10	• Default: -3 • Range: -7 through -1	• Default: -3 • Range: -7 through -3
AES67	• Default: 1 • Range: 0 through 4	• Default: 3 • Range: 2 through 10	• Default: -3 • Range: -4 through 1	• Default: -3 • Range: -7 through -3
AES67+SMPTE	• Default: 0 • Range: 0 through 1	• Default: 3 • Range: 2 through 10	• Default: -3 • Range: -4 through -1	• Default: -3 • Range: -7 through -3

Configuring the PTP Media Profile

To configure the any of the media profiles:

NOTE: On the QFX Series, when you configure either a master or slave port, it must be on the same subnet as the remote device to which it is connected.

NOTE: When either the enterprise or any of the media profiles are enabled, the master and slave ports must be configured in multicast-mode. The master sends the announce and sync packets as multicast IP packets, but the QFX Series slave will send the delay-req packets as unicast IP packets.

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.

   For example:

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

3. Configure the profile type.

   Configuring the profile type is mandatory.

   ```
   [edit protocols ptp]
   user@host# set profile-type (aes67 | smpte | aes67-smpte)
   ```

4. Configure the clock mode.

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

5. Configure the interface for the slave.

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


6. Configure the **multicast-mode** option for the slave.

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

7. Configure the **transport** option in multicast-mode as IPv4.

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

8. Configure the IP address of the interface acting as the local PTP slave port.

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

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

9. Configure the interface for the master.

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

10. Configure the multicast-mode option for the master.

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

11. Configure the **transport** option in multicast-mode as IPv4.

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

12. Configure the local IP address for the master.

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

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

13. (Optional) Configure the PTP domain option.

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

14. (Optional) Configure the **priority1** option.

    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
    ```

15. (Optional) Configure the **priority2** option.

    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
    ```

16. (Optional) Configure the **announce-timeout** option in the slave node.

    The announce timeout value signifies the number of times an announce interval message has to pass through the slave without receiving the announce message—that is, the timeout period for announce messages.

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

17. (Optional) Specify the log mean interval between announce messages.

    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
    ```

18. (Optional) Configure the **sync interval** option for the master clock.

    The sync interval is the logarithmic mean interval between synchronous messages that is sent by the master.

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

19. (Optional) Configure the **delay-request** option in the slave node.

    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
```

20. Verify the lock status of the slave.

NOTE: On the QFX Series, the slave will not lock to the master unless at least eight sync packets per second are received from the master.

For example:

```
user@switch> show ptp lock-status detail
Lock Status:

Lock State    : 5 (PHASE ALIGNED)
Phase offset  : -0.000000202 sec
```

The output shows that the lock state is aligned.

21. Verify the status of the master.

For example:

```
user@switch> show ptp master detail
PTP Master Interface Details:
Interface  : et-0/0/0:31.0
Status     : Master, Active
Clock Info :
Local Address: 192.168.99.42  Status: Configured, Master, Active
Remote Address: 192.168.1.12    Status: Configured, Slave, Active
Total Remote Slaves: 1
```

The output shows that the master is active.

Related Documentation

- Understanding the PTP Media Profiles on page 76

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 96

Configuring Precision Time Protocol and its Options

This topic includes the following tasks:

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 111 .

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 99

Configuring Precision Time Protocol and its Options

This topic includes the following tasks:

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 104.

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 115.

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 68
- Configuring a PTP Master Boundary Clock on page 104
- Configuring a PTP Slave Clock on page 115
- Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 111
- Example: Configuring a PTP Boundary Clock on page 108

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

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 107

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 **syn-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 107.

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 68
- Configuring Precision Time Protocol Clocking on page 103
- Configuring a PTP Slave Clock on page 115
- Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 111
- Example: Configuring a PTP Boundary Clock on page 108

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 109
- Overview on page 109
- Configuration on page 109

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 68
- Configuring Precision Time Protocol Clocking on page 103
- Configuring a PTP Master Boundary Clock on page 104
- Configuring a PTP Slave Clock on page 115
- Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 111

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 111
- Overview on page 112
- Configuration on page 112

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 7.7.7.7
   local-ip-address 7.7.7.53 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 68
- Configuring Precision Time Protocol Clocking on page 103
- Configuring a PTP Master Boundary Clock on page 104
- Configuring a PTP Slave Clock on page 115
- Example: Configuring a PTP Boundary Clock on page 108

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 116
- Configuring the PTP Slave Clock Interface on page 118

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 118.

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 118.

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
   ```

   NOTE: On the QFX Series, you can configure an aggregated Ethernet interface and its configured IP address for PTP streams acting as slaves or masters.

   For example, to configure a slave using an aggregated Ethernet interface:

   ```
   user@switch# set protocols ptp slave interface ae0.0
   ```

   NOTE: On the QFX Series, you can configure a loopback interface (there is only one loopback interface, and it is lo0.0) and its corresponding IP addresses for PTP streams acting as slaves or masters. Although the loopback interface is the same for both masters and slaves, the IP addresses must be unique.

   For example, to configure a slave using the loopback interface:

   ```
   user@switch# set protocols ptp slave interface lo0.0
   ```

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 | ipv6)
```

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 68
- Configuring Precision Time Protocol Clocking on page 103
- Configuring a PTP Master Boundary Clock on page 104
- Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 111
- Example: Configuring a PTP Boundary Clock on page 108

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 120
- Overview on page 120
- Configuration on page 120

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 120
- Results on page 121

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 page 71
- **slave on page 185**
- *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 123
- Overview on page 123
- Configuration on page 123

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 123
- Results on page 124

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 page 71
- **slave on page 185**
- *unicast-mode*

Configuring Precision Time Protocol Over Integrated Routing and Bridging

Junos OS for ACX Series router supports configuring precision time protocol (PTP) over integrated routing and bridging (IRB). You can configure a boundary clock node with PTP (IPv4) over IRB in a master-only mode across single or multiple IRB logical interfaces.

To configure Precision Time Protocol (PTP) over IRB:

1. Configure physical interfaces with Layer 2 encapsulation and create logical units with VLANs.

```
[edit interfaces ge-0/2/1]
flexible-vlan-tagging;
native-vlan-id 130;
encapsulation flexible-ethernet-services;
unit 615 {
    encapsulation vlan-bridge;
    vlan-id 615;
}

[edit interfaces ge-0/0/3]
flexible-vlan-tagging;
encapsulation flexible-ethernet-services;
unit 615 {
    encapsulation vlan-bridge;
    vlan-id 615;
}

[edit interfaces ge-0/1/2]
flexible-vlan-tagging;
encapsulation flexible-ethernet-services;
unit 615 {
    encapsulation vlan-bridge;
    vlan-id 615;
}

[edit interfaces ge-0/2/0]
flexible-vlan-tagging;
native-vlan-id 130;
encapsulation flexible-ethernet-services;
```

2. Configure physical interfaces on a bridge domain.

```
[edit bridge-domains]
bd-615 {
    vlan-id 615;
    interface ge-0/1/2.615;
    interface ge-0/2/0.615;
    interface ge-0/2/1.615;
    interface ge-0/0/3.615;
 }
```

3. Configure a routing instance for the bridge domain where physical interfaces are members of the bridge domain.

```
[edit bridge-domains]
bd-615 {
    vlan-id 615;
    interface ge-0/1/2.615;
    interface ge-0/2/0.615;
    interface ge-0/2/1.615;
    interface ge-0/0/3.615;
    routing-interface irb.615;
}
```

4. Configure an IRB logical interface with IPv4 address.

```
[edit interfaces irb]
unit 615 {
    family inet {
        address 10.255.210.130/27;
    }
}
```

5. Configure PTP boundary clock master on IRB logical interface.

```
[edit protocols ptp]
clock-mode boundary;
priority2 210;
unicast-negotiation;
slave {
    interface ge-0/2/0.0 {
        unicast-mode {
            transport ipv4;
            clock-source 122.25.1.4 local-ip-address 122.25.1.5 {
                asymmetry 680;
            }
        }
    }

master {
    interface ge-0/2/1.0 {
        unicast-mode {
            transport ipv4;
            clock-client 122.25.1.7/32 local-ip-address 122.25.1.6;
        }
    }
    interface irb.615 {
        unicast-mode {
            transport ipv4;
            clock-client 10.255.210.128/27 local-ip-address 10.255.210.130;
        }
    }
}
```

You can use the following commands to monitor and troubleshoot the configuration:

- **show interfaces irb**—View the configured logical IRB interface details.
- **show ptp master detail**—View the configured master and its status along with local and remote client details.

- **show bridge domain**—View the configured bridge domain and the associated physical interfaces and IRB routing instance details.
- **show ptp lock-status detail**—View the PTP lock status details.
- **show ptp port detail**—View the PTP port details.
- **show ptp global-information**—View the configured PTP parameters.
- **show ptp clock**—View the PTP clock information.

Related Documentation

- IEEE 1588v2 PTP Boundary Clock Overview on page 68
- Configuring a PTP Master Boundary Clock on page 104
- Configuring a PTP Slave Clock on page 115
- Example: Configuring a PTP Boundary Clock With Unicast Negotiation on page 111
- Example: Configuring a PTP Boundary Clock on page 108

Configuring PHY Timestamping

The PHY timestamping refers to the timestamping of the IEEE 1588 event packets at the 1-Gigabit Ethernet and 10-Gigabit Ethernet PHY. Timestamping the packet in the PHY results in higher stability of recovered clock. The PHY timestamping on ACX updates the correction field of the packet. ACX supports PHY timestamping in ordinary clock and boundary clock modes.

NOTE: **PHY timestamping is supported only on ACX500 line of routers.**

The following points need to be considered while configuring PHY timestamping in ACX routers:

- PHY timestamping is enabled or disabled on all the PHYs. You cannot selectively enable or disable PHY timestamping on a particular interface.
- When PHY timestamping is enabled, the transparent clock functionality is also enabled.

NOTE: **The PHYs on ACX do not support transparent clock functionality for PTP-over-MPLS. You should not enable transparent clock or PHY timestamping if PTP is transported over MPLS.**

In ACX2000 router, the transparent clock operation is not supported on the 10-Gigabit Ethernet port.

To enable PHY timestamping on ACX routers, configure **clock-mode** (ordinary clock or boundary clock) along with the **transparent-clock** CLI statement at the [**edit protocols ptp**] hierarchy.


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

NOTE: Starting in Junos OS Release 17.1 onwards, to configure transparent clock, include the **e2e-transparent** CLI command at the **[edit protocols ptp]** hierarchy level. Prior to Junos OS Release 17.1, to configure transparent clock, include the **transparent-clock** CLI command at the **[edit protocols ptp]** hierarchy level.

Enabling PHY Timestamping for Ordinary Clock Slave

The following procedure enables you to configure PHY timestamping for ordinary clock slave in ACX:

1. Configure the clock mode as ordinary.

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

2. Configure the transparent clock.

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

3. Configure the interface for slave clock. For information on configuring PTP slave clock interface, see "Configuring a PTP Slave Clock" on page 115.

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

Enabling PHY Timestamping for Boundary Clock

The following procedure enables you to configure PHY timestamping for boundary clock in ACX:

NOTE: PHY timestamping is supported only on ACX500 line of routers.

1. Configure the clock mode as boundary.

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

2. Configure the transparent clock.

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

3. Configure the interface for slave clock. For information on configuring PTP slave clock interface, see “Configuring a PTP Slave Clock” on page 115.

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

4. Configure the interface for master clock. For information on configuring PTP master boundary clock, see “Configuring a PTP Master Boundary Clock” on page 104.

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

Enabling PHY Timestamping for Grandmaster Clock

The following procedure enables you to configure PHY timestamping for grandmaster clock in ACX:

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

1. Configure the clock mode as ordinary.

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

2. Configure the transparent clock.

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

3. Configure the interface for master clock. For information on configuring PTP master boundary clock, see “Configuring a PTP Master Boundary Clock” on page 104.

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

Configuring PHY Timestamping on ACX2200 Routers

The PHY timestamping refers to the timestamping of the IEEE 1588 event packets at the 1-Gigabit Ethernet and 10-Gigabit Ethernet PHY. Timestamping the packet in the PHY results in higher stability of recovered clock. The PHY timestamping on ACX updates the correction field of the packet. ACX2200 supports PHY timestamping in boundary clock mode.

The following points need to be considered while configuring PHY timestamping in ACX routers:

- PHY timestamping is enabled or disabled on all the PHYs. You cannot selectively enable or disable PHY timestamping on a particular interface.
- When PHY timestamping is enabled, the transparent clock functionality is also enabled.

NOTE: The PHYs on ACX do not support transparent clock functionality for PTP-over-MPLS. You should not enable transparent clock or PHY timestamping if PTP is transported over MPLS.

To enable PHY timestamping on ACX2200 routers, configure boundary clock along with **e2e-transparent** CLI statement at the [**edit protocols ptp**] hierarchy.

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

- Enabling PHY Timestamping for Boundary Clock on page 131

Enabling PHY Timestamping for Boundary Clock

The following procedure enables you to configure PHY timestamping for boundary clock in ACX2200 routers:

1. Configure the clock mode as boundary.

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

2. Enable Phy timestamping on boundary clock.

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

3. Configure the interface for slave clock. For information on configuring PTP slave clock interface, see “Configuring a PTP Slave Clock” on page 115.

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

4. Configure the interface for master clock. For information on configuring PTP master boundary clock, see “Configuring a PTP Master Boundary Clock” on page 104.

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

G.703 2.048MHz Signal Type for BITS Interfaces Overview

The ITU-T Recommendation G.703, *Physical/electrical characteristics of hierarchical digital interfaces*, is a standard method for encoding clock and data signals into a single signal. This signal is then used to synchronize various data communications devices, such as switches, routers and multiplexers at a data rate of 2.048 MHz. Both directions of the G.703 signal must use the same signal type. To configure signal type parameters for a building-integrated timing supply (BITS) interface, include the following statements at the [**edit chassis synchronization**] hierarchy level:

```
interfaces bits {
     signal-type (2048khz | e1 | t1);
          e1-options {
               framing (g704 | g704-no-crc4);
          }
          t1-options {
               framing (esf | sf);
          }
     }
}
```

Related Documentation

- *synchronization (ACX Series)*
- *show chassis synchronization*

Configuring PTP Multicast Master and Slave Ports for Ethernet Encapsulation

On an ACX Series router, you can configure a Precision Time Protocol (PTP) master boundary clock with IEEE 802.3 or Ethernet encapsulation of 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. PTP over Ethernet uses multicast addresses for communication of PTP messages between the slave clock and the master clock. The slave clock automatically learns of master clocks in the network, is immediately able to receive the multicast messages from the master clock, and can begin sending messages to the master clock without any pre-provisioning. The master boundary clock synchronizes time through a slave boundary port.

To configure PTP over Ethernet with multicast master and slave ports, you must include the **multicast-mode transport ieee-802.3** statement at the **[edit protocols ptp master interface *interface-name*]** and **[edit protocols ptp slave interface *interface-name*]** hierarchy levels, respectively.

To configure a PTP over Ethernet master boundary clock and slave boundary clock for multicast transmission, complete the following tasks:

- Configuring the PTP over Ethernet Master Boundary Clock Parameters on page 133
- Configuring the PTP over Ethernet Master Boundary Clock Interface on page 135
- Configuring the PTP over Ethernet Slave Clock Parameters on page 136
- Configuring the PTP over Ethernet Slave Clock Interface on page 137

Configuring the PTP over Ethernet Master Boundary Clock Parameters

To configure the parameters of a PTP over Ethernet 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 or slave ports.

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

   For details about configuring the parameters for the master boundary clock interface, see "Configuring the PTP over Ethernet Master Boundary Clock Interface" on page 135

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 **syn-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 the PTP over Ethernet Master Boundary Clock Interface" on page 135.

Configuring the PTP over Ethernet Master Boundary Clock Interface

After you configured the master boundary clock parameters for PTP over Ethernet with multicast transmission of PTP traffic, 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 over Ethernet master boundary clock interface:

1. Configure the interface on which to respond to downstream PTP slave ports 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 multicast as the transmission mode of traffic for PTP clients.

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

3. Specify the encapsulation type for PTP packet transport as Ethernet or IEEE 802.3. This statement is mandatory.

   ```
   [edit protocols ptp master interface interface-name multicast-mode]
   user@host# set transport ieee-802.3
   ```

   Alternatively, specify the encapsulation type as Ethernet with the link-local multicast address to be used in the sending of PTP messages. If you specify the **link-local** attribute, the master clock chooses either of the two MAC addresses defined in the IEEE 1588-2008 standard. When you configure this option, the system attempts to use the 01 -80-C2-00-00-0E MAC address (link-local multicast MAC address) for multicast transmission. If this MAC address is not available, the 01-1B-19-00-00-00 address (standard Ethernet multicast address) is used as the second priority. The standard Ethernet multicast address is used by default. You need to explicitly configure the link-local multicast address.

   ```
   [edit protocols ptp master interface interface-name multicast-mode]
   user@host# set transport ieee-802.3 link-local
   ```

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

Configuring the PTP over Ethernet Slave Clock Parameters

An interface on which the master clock is configured is called a master interface and an interface on which the slave clock is configured is called a slave interface. A master interface functions as the master port and a slave interface functions as the slave port. 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 communication with the master port with minimal or no configuration. You can optionally configure these settings for a slave port that communicates with the master ports using PTP over Ethernet.

To configure a PTP over Ethernet slave clock.

1. Configure the clock mode:

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

2. Configure the slave clock.

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

3. (Optional) Specify the number of announce messages that a slave clock or port—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
   ```

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

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

5. Configure the interface for the slave clock.

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

6. (Optional) Configure the log mean interval between synchronization messages—from **–6** through **-3**. The default value is –6, which means by default, 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 in configuration mode. To complete the configuration of the slave clock, complete “Configuring the PTP over Ethernet Slave Clock Interface” on page 137

Configuring the PTP over Ethernet 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 multicast PTP master clock source parameters.

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

3. Specify the encapsulation type for PTP packet transport as Ethernet or IEEE 802.3. This statement is mandatory.

```
[edit protocols ptp slave interface interface-name multicast-mode]
user@host# set transport ieee-802.3
```

   Alternatively, specify the encapsulation type as Ethernet with the link-local multicast address to be used in the sending of PTP messages. If you specify the **link-local** attribute, the master clock chooses either of the two MAC addresses defined in the IEEE 1588-2008 standard. When you configure this option, the system attempts to use the 01 -80-C2-00-00-0E MAC address (link-local multicast MAC address) for multicast transmission. If this MAC address is not available, the 01-1B-19-00-00-00 address (standard Ethernet multicast address) is used as the second priority. The standard Ethernet multicast address is used by default. You need to explicitly configure the link-local multicast address.

```
[edit protocols ptp slave interface interface-name multicast-mode]
user@host# set transport ieee-802.3 link-local
```

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

Related Documentation

- PTP over Ethernet on ACX Series Routers Overview on page 77
- Guidelines for Configuring PTP over Ethernet on page 79
- Configuring PTP Dynamic Ports for Ethernet Encapsulation on page 138

- Example: Configuring PTP over Ethernet for Multicast Master, Slave, and Dynamic Ports on page 139

Configuring PTP Dynamic Ports for Ethernet Encapsulation

For PTP over Ethernet, you can also configure a port to function as both a slave port and a master port. This type of port is called a dynamic port, a stateful port, or a bidirectional port. Such a dynamic port enables the transfer of frequency for synchronization services, in addition to time and phase alignment, when PTP functionality is not hop-by-hop and you have provisioned master and slave roles or interfaces.

To configure PTP over Ethernet with dynamic or bidirectional ports for multicast mode of transmission, you must include the **multicast-mode** statement at the **[edit protocols ptp stateful interface *interface-name*]** hierarchy level.

To enable a node to function as both a master and a slave port in PTP over Ethernet networks:

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

   ```
   [edit protocols ptp stateful]
   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. Configure the upstream multicast PTP dynamic clock source parameters.

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

3. Specify the encapsulation type for PTP packet transport as Ethernet or IEEE 802.3. This statement is mandatory.

   ```
   [edit protocols ptp stateful interface interface-name multicast-mode]
   user@host# set transport ieee-802.3
   ```

   Alternatively, specify the encapsulation type as Ethernet with the link-local multicast address to be used in the sending of PTP messages. If you specify the link-local attribute, the master clock chooses either of the two MAC addresses defined in the IEEE 1588-2008 standard. When you configure this option, the system attempts to use the 01 -80-C2-00-00-0E MAC address (link-local multicast MAC address) for multicast transmission. If this MAC address is not available, the 01-1B-19-00-00-00 address (standard Ethernet multicast address) is used as the second priority. The standard Ethernet multicast address is used by default. You need to explicitly configure the link-local multicast address.


```
[edit protocols ptp stateful interface interface-name multicast-mode]
user@host# set transport ieee-802.3 link-local
```

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

Related Documentation

- PTP over Ethernet on ACX Series Routers Overview on page 77
- Guidelines for Configuring PTP over Ethernet on page 79
- Configuring PTP Multicast Master and Slave Ports for Ethernet Encapsulation on page 132
- Example: Configuring PTP over Ethernet for Multicast Master, Slave, and Dynamic Ports on page 139

Example: Configuring PTP over Ethernet for Multicast Master, Slave, and Dynamic Ports

In PTP over Ethernet networks, the master sends the announce, synchronization, and delay-response packets using the multicast method. If any unicast delay-request message is received, the master disregards the message and does not send delay-response messages to the slave. A PTP slave receives the multicast announce packets from the master or multiple masters and determines the best master using Best Master Clock Algorithm (BMCA). A slave receives and processes the synchronization from the selected master clock. The slave sends delay-request messages to this master using the multicast method and processes the delay-response messages from the master to establish synchronization.

Both the link-local MAC address and the standard 802.3 multicast MAC address can be present in a system. However, a PTP interface supports only one of the following at a point in time:

- Layer 2 multicast with link-local MAC address
- Layer 2 multicast with standard multicast MAC address
- PTP over IPv4

When you configure both IPv4 and Ethernet encapsulation, the unicast-negotiation configuration applies only to IPv4 encapsulation. It is not effective for PTP over Ethernet operation.

When you configure a logical interface by using the **stateful** statement at the **[edit protocols ptp]** hierarchy level, each interface that you configure as a stateful or dynamic port is considered to be both a master and a slave port. Although an ACX Series router supports up to 32 master ports and 4 slave ports, you can configure only 4 unique logical interfaces as potential PTP masters by using the **stateful** statement because the interface is treated as both a slave and a master interface. You cannot configure the interface that you specify to be a stateful or dynamic port with the **master** or **slave** statements.

This example shows how to configure a master port, slave port, and a dynamic port for PTP over Ethernet and PTP over IPv4 encapsulation, and how to configure unicast and multicast mode of transmission of PTP traffic among the master and slave nodes.

Requirements

This example uses the following hardware and software components:

- An ACX Series router
- Junos OS Release 12.3X51 or later

Overview

While an ACX Series router supports the PTP over Ethernet functionality, a Brilliant Grand Master such as an MX Series router or a TCA Series Timing Client does not support PTP over Ethernet. Consider a sample deployment in which an ACX Series router named ACX1 functions as a boundary clock with a PTP slave port using IPv4 as the encapsulation mode and master ports using Ethernet as the encapsulation mode for PTP traffic. ACX1 contains two potential slave interfaces, one that is fixed as a slave-only port using IPv4 on the link toward an MX Series router named MX2, and a dynamic port that functions as a slave using PTP over Ethernet on the link toward another ACX Series router named ACX2. In addition, ACX1 also contains a port that is a master-only port using PTP over Ethernet and connects to the base station.

In this example, the router uses either interface ge-0/2/0.0 or ge-0/2/1.0 as the selected slave interface based on the announce messages received from the master and the port that was selected using the Best Master Clock Algorithm (BMCA). The interface ge-0/1/4.0 is always in the master state. According to the IEEE 1588 specification, if port ge-0/2/0.0 is selected as the slave interface, interface ge-0/2/1.0 transitions to the master state. If interface ge-0/2/1.0is selected as the slave port, interface ge-0/2/0.0 transitions to the listening state. You can also configure the interface ge-0/1/4.0 as a slave only interface for PTP over Ethernet, if necessary, for completeness of the configuration.

Configuration

In this example, you configure a master port, a slave port, and a dynamic port for PTP over Ethernet and PTP over IPv4 encapsulation. You can also configure unicast and multicast modes of transmission of PTP traffic among the master and slave nodes.

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 interfaces ge-0/1/4 description “to base-station”
set interfaces ge-0/1/4 unit 0 family inet address 7.1.1.37/24
set interfaces ge-0/2/0 description “to MX2”
set interfaces ge-0/2/0 unit 0 family inet address 110.1.1.2/24
set interfaces ge-0/1/4 description “to ACX2”
set interfaces ge-0/1/4 unit 0 family inet address 110.1.1.2/24
set protocols ptp clock-mode boundary
set protocols ptp domain 110
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 110.1.1.250
   local-ip-address 110.1.1.2
set protocols ptp master interface ge-0/1/4.0 multicast-mode transport ieee-802.3
set protocols ptp stateful interface ge-0/2/1.0 multicast-mode transport ieee-802.3
```

Configuring PTP over Ethernet for Multicast Master, Slave, and Dynamic Ports

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 the master, slave, and dynamic interfaces, and a boundary clock with unicast and multicast mode of transmission of PTP packets in PTP over IPv4 and PTP over Ethernet topologies:

1. Configure the master interface, and enter edit mode for the interface.

```
[edit interfaces]
user@host#edit ge-0/1/4
```

2. Configure a description for the interface.

```
[edit interfaces ge-0/1/4]
user@host#set description to base-station
```

3. Configure a logical unit and specify the protocol family.

```
[edit interfaces ge-0/1/4]
user@host#set unit 0 family inet
```

4. Specify the address for the logical interface

```
[edit interfaces ge-0/1/4 unit 0 family inet]
user@host#set address 7.1.1.37/24
```

5. Configure the slave interface, and enter edit mode for the interface.

```
[edit interfaces]
user@host#edit ge-0/2/0
```

6. Configure a description for the interface.

```
[edit interfaces ge-0/2/0]
user@host#set description to-MX2
```

7. Configure a logical unit and specify the protocol family.

```
[edit interfaces ge-0/2/0]
user@host#set unit 0 family inet
```

8. Specify the address for the logical interface

```
[edit interfaces ge-0/2/0 unit 0 family inet]
user@host#set address 110.1.1.2/24
```

9. Configure the stateful interface, and enter edit mode for the interface.

```
[edit interfaces]
user@host#edit ge-0/2/1
```

10. Configure a description for the interface.

```
[edit interfaces ge-0/2/1]
user@host#set description to-ACX2
```

11. Configure a logical unit and specify the protocol family.

```
[edit interfaces ge-0/2/1]
user@host#set unit 0 family inet
```

12. Specify the address for the logical interface

```
[edit interfaces ge-0/2/1 unit 0 family inet]
user@host#set address 110.2.1.1/24
```

13. Configure the clock mode as boundary clock.

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


14. Specify the PTP domain value.

```
[edit protocols ptp]
user@host# set domain 110
```

15. 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-0/2/0.0
```

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

```
[edit protocols ptp slave interface ge-0/2/0.0]
user@host# edit unicast-mode
```

17. Configure the encapsulation type for PTP packet transport.

```
[edit protocols ptp slave interface ge-0/2/0.0 unicast-mode]
user@host# set transport ipv4
```

18. 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 110.1.1.250 local-ip-address 110.1.1.2
```

19. Configure the master interface in this example.

```
[edit protocols ptp]
user@host# edit master interface ge-0/1/4.0
```

20. On the master interface, configure multicast transmission for downstream PTP clock clients.

```
[edit protocols ptp master interface ge-0/1/4.0]
user@host# edit multicast-mode
```

21. On the master interface, configure the encapsulation type as Ethernet for PTP packet transport.

```
[edit protocols ptp master interface ge-0/2/1.0 multicast-mode]
user@host# set transport ieee-802.3
```

22. Configure the dynamic or stateful interface in this example.


```
[edit protocols ptp]
user@host# edit stateful interface ge-0/2/1.0
```

23. On the dynamic interface, configure multicast transmission for downstream PTP clock clients.

```
[edit protocols ptp stateful interface ge-0/2/1.0 ]
user@host# edit multicast-mode
```

24. On the dynamic interface, configure the encapsulation type as Ethernet for PTP packet transport and the link-local multicast address to be used.

```
[edit protocols ptp stateful interface ge-0/2/1.0 multicast-mode]
user@host# set transport ieee-802.3 link-local
```

Results

In 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;
        domain 110;
        slave {
            interface ge-0/2/0.0 {
                unicast-mode {
                    transport ipv4;
                    clock-source 110.1.1.250 local-ip-address 110.1.1.2;
                }
            }
        }
        master {
            interface ge-0/1/4.0 {
                multicast-mode {
                    transport ieee-802.3;
                }
            }
        }
        stateful {
            interface ge-0/2/1.0 {
                multicast-mode {
                    transport ieee-802.3 link-local;
                }
            }
        }
```

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

Verifying the PTP over Ethernet Multicast Dynamic, Master, and Slave Settings

Confirm that the configuration is working properly.

Verifying the PTP Clock Details

Purpose Verify that the PTP clock is working as expected.

Action In operational mode, enter the **run show ptp clock** command to display comprehensive, globally configured clock details.

Meaning The output displays the clock details, such as the encapsulation method used for transmission of PTP traffic and the number of configured stateful or dynamic ports. Although a dynamic port functions as either a slave or a master port, the value displayed in the **Stateful Ports** field denotes the dynamic ports that you explicitly configured. The number of dynamic ports is not computed and displayed in the fields that display the explicitly configured master and slave ports. For more information about the **run show ptp clock** operational command, see **show ptp clock** in the CLI Explorer.

Verifying the Lock Status of the Slave

Purpose Verify that the slave clock is aligned to the master clock by checking the lock status of the slave.

Action In operational mode, enter the **run show ptp lock-status** command to display the lock status of the slave.

Meaning The output displays information about the lock status of the slave. The output shows whether the slave is aligned to the master clock or not, and the interface name configured for PTP on the slave. The **Master Source Port** field displays the address of the master clock when PTP over IPv4 is configured and the multicast MAC address of the source when PTP over Ethernet is configured. For more information about the **run show ptp lock-status** operational command, see **show ptp lock-status** in the CLI Explorer.

Verifying the PTP Options on the Slave

Purpose Verify the PTP options that are set on the slave and the current status of the master.

Action In operational mode, enter the **run show ptp slave** command to display the configured slave.

Meaning The output displays information about the configured slave and the status of the slave. For more information about the **show ptp slave** operational command, see **show ptp slave** in the CLI Explorer.

Verifying the PTP Options and the Current Status of the Master

Purpose Verify the PTP options that are set for the master and its current status.

Action In operational mode, enter the **run show ptp master** command to display the configured options for the master.

Meaning The output displays information about the configured master and the current status of the master. For more information about the **run show ptp master** operational command, see **show ptp master** in the CLI Explorer.

Verifying the Number and Status of the PTP Ports

Purpose Verify the number of PTP ports and their current status.

Action In operational mode, enter the **run show ptp port** command to display the configured ports.

Meaning The output displays information about the number of ports created according to the configuration and their current status. The name of the interface configured for PTP and the number of times a stateful port transitioned from the slave to the master state and vice versa is displayed. For more information about the **run show ptp port** operational command, see *show ptp port* in the CLI Explorer.

Verifying PTP Statistics

Purpose Verify the statistical details of the PTP configuration.

Action In operational mode, enter the **run show ptp statistics** command to display the statistical information regarding the configured PTP clocks.

Meaning The output displays brief or detailed information about the operation of configured PTP clocks. Statistical parameters include information such as the total number of PTP packets transmitted or received by a master or slave interface and the number of various messages (such as announce and synchronization messages) that are sent between a master and a slave. For more information about the **show ptp statistics** operational command, see **show ptp statistics** in the CLI Explorer.

Related Documentation

- PTP over Ethernet on ACX Series Routers Overview on page 77
- Guidelines for Configuring PTP over Ethernet on page 79
- Configuring PTP Multicast Master and Slave Ports for Ethernet Encapsulation on page 132
- Configuring PTP Dynamic Ports for Ethernet Encapsulation on page 138

Hybrid Mode on ACX Series Routers Overview

The combined operation of Synchronous Ethernet and Precision Time Protocol (PTP) is also known as hybrid mode. The following sections explain hybrid mode in detail:

- Hybrid Mode Overview on page 147
- Supporting Platforms on page 148

Hybrid Mode Overview

In hybrid mode, the synchronous Ethernet equipment clock (EEC) on the Modular Port Concentrator (MPC) derives the frequency from Synchronous Ethernet and the phase and time of day from PTP. Time synchronization includes both phase synchronization and frequency synchronization.

Synchronous Ethernet is a physical layer–based technology that functions regardless of the network load. Synchronous Ethernet supports hop-by-hop frequency transfer, where all interfaces on the trail must support Synchronous Ethernet. PTP (also known as IEEE 1588v2) synchronizes clocks between nodes in a network, thereby enabling the distribution of an accurate clock over a packet-switched network. This synchronization is achieved through packets that are transmitted and received in a session between a master clock (commonly called the master) and a slave clock (also known as the slave in PTP terminology). PTP synchronizes both frequency and phase including time of day. The accuracy of clock synchronization depends on factors such as packet delay variation, quality of oscillator used, network asymmetry, and so on.

Synchronous Ethernet and PTP provide frequency and phase synchronization; however, the accuracy in the order of nanoseconds is difficult to achieve through PTP or Synchronous Ethernet and they do not support a large number of network hops. Hybrid mode resolves these issues by extending the number of network hops and also provides clock synchronization accuracy in the order of tens of nanoseconds.

Hybrid mode is configured on the slave. On the slave, you can configure one or more interfaces as Synchronous Ethernet source interfaces.

NOTE: Router clocks are categorized based on the role of the router in the network. They are broadly categorized into ordinary clocks and boundary clocks. The master clock and the slave clock are known as ordinary clocks. The boundary clock can operate as either a master clock or a slave clock.

In hybrid mode, the following **show** commands display information regarding the hybrid status configuration:

- The **show ptp status details** command displays the time and phase plane status.
- The **show chassis synchronization extensive** command displays the frequency plane status.
- The **show ptp hybrid status** command displays the hybrid (combined status of frequency and phase plane) status.
- In hybrid mode, the **show ptp hybrid status** and **show ptp lock-status** commands indicate the lock status as **Phase Aligned** in the output.

For information about configuring hybrid mode, see *Configuring Hybrid Mode and ESMC Quality Level Mapping*. You can use the **show ptp hybrid status** operational command to find the current operating mode.

Supporting Platforms

Hybrid mode is supported on the Juniper Networks ACX Series Universal Metro Routers.

The combined operation is possible only when the PTP client and the Synchronous Ethernet source are on the same device and are traceable to the same primary reference clock (also known as PRC).

When acting as PTP slaves, the ACX Series routers can accept any external Synchronous Ethernet clock as reference and do not support building-integrated timing supply (BITS) input as frequency source in hybrid mode of operation. Only Synchronous Ethernet sources are allowed in hybrid mode. Note that when the selected Synchronous Ethernet reference fails, the router continues to work in PTP mode.

Unified in-service software upgrade (unified ISSU) is not supported when clock synchronization is configured for hybrid mode.

NOTE: To switch between PTP and Synchronous Ethernet modes, you must first deactivate the configuration for the current mode and then commit the configuration. Wait for 30 seconds, configure the new mode and its related parameters, and then commit the configuration.

Related Documentation

- Guidelines for Configuring Hybrid Mode on ACX Series Routers on page 149
- Configuring Hybrid Mode and ESMC Quality Level Mapping on ACX Series Routers on page 150

- Example: Configuring Hybrid Mode and ESMC Quality Level Mapping on page 153

Guidelines for Configuring Hybrid Mode on ACX Series Routers

Keep the following points in mind while configuring hybrid mode on ACX Series routers:

- In a Hybrid Operation, the Frequency Module derives frequency from the Synchronous Ethernet or BITS (T1/E1) clock or 10 MHz clock and Phase from the IEEE-1588v2 (PTPv2). The current deployments are all LTE-TDD based and require a phase accuracy of only 1.5us and it is expected that this performance can be achieved without requiring frequency assist.
- Frequency Plane (Synchronous Ethernet, BITS (T1/E1), 10 MHz) is not impacted by the phase or time plane. The frequency plane derives the frequency from Synchronous Ethernet, BITS (T1/E1) and 10 MHz.
- Phase/Time Plane uses the Frequency which is derived locally from the equipment (Synchronous Ethernet, BITS (T1/E1), 10 MHz). To achieve phase accuracy of less than 1.5us, both Frequency Input source and PTP sources traceable to a primary reference source (PRS) or primary reference clock (PRC). Hybrid mode is supported in a ring topology.
- You can configure the following frequency sources for hybrid node:
  - Synchronous Ethernet 1G, 10G with/without ESMC
  - BITS T1 Clock
  - BITS E1 Clock
  - 10 MHz Clock
  - T1 Interface
  - E1 Interface
- You can configure the following phase sources for hybrid node:
  - PTP IPv4 with or without unicast negotiation
  - PTPoE with or without stateful port
- By enabling the hybrid mode, the convergence time period is reduced and locking happens quickly.
- You can configure the PTP Source as phase or time source for hybrid mode.
- You can configure Layer 2 rings for PTPoE with stateful ports and Synchronous Ethernet with ESMC for Layer 2 ring topologies.
- When you enable hybrid mode, each node generates a phase error of or plus or minus 100 nanoseconds (without Phy Timestamping) or plus or minus 50 nanoseconds with Phy timestamping feature. This phenomenon requires Frequency (SyncE/BITS/10 MHz) source and PTP source must be traceable to same PRC/PRS source.

- Fully redundant and resilient ring based configurations of up to 10 nodes are supported, targeting the 1 microsecond phase requirement for a form of 4G known as Long-Term Evolution-Time Division Duplex (LTE-TDD). A single node or link failure is accommodated and all nodes are able to maintain phase accuracy to be +/- 1us accurate to a common source.
- Hybrid mode for PTP IPv4 rings is not supported.
- Dynamic switchover from Hybrid to PTP mode is not supported in ACX routers.
- BITS T1 Clock with SSM is not supported. BITS E1 Clock with SSM is not supported.
- Hybrid Mode: Time Of Day (TOD) as Phase and Frequency as SyncE/BITS/10 MHz is not supported. Simultaneous PTP IPv4 Ring and SyncE Hybrid Mode are not supported.
- Hybrid Mode with Phy Timestamping feature is not supported only on ACX500 series routers.
- Dynamic Switchover from Hybrid to PTP Mode feature is not supported.
- Hybrid Feature on aggregated Ethernet (**ae-**) interfaces is not supported.
- When you configure hybrid mode, the following processes take place.
  - The best of the configured PTP time sources is selected by the PTP Best Master Clock Algoritm (BMCA).
  - The best of configured chassis synchronization sources is selected by the synchronization source selection algorithm.
  - During the boot-up process, if valid sources are configured at the **[edit chassis synchronization]** hierarchy level and chassis synchronization mode in free-running mode, valid PTP source available case, system continues to operate in hybrid mode (In this case, chassis synchronization is in free-run mode, whereas PTP is in locked mode). When both primary and secondary frequency sources fail, system still works under hybrid mode (In this case, chassis synchronization is in hybrid mode and PTP is in locked mode).

Related Documentation

- Hybrid Mode on ACX Series Routers Overview on page 147
- Configuring Hybrid Mode and ESMC Quality Level Mapping on ACX Series Routers on page 150
- Example: Configuring Hybrid Mode and ESMC Quality Level Mapping on page 153

Configuring Hybrid Mode and ESMC Quality Level Mapping on ACX Series Routers

You can configure hybrid mode (that is, the combined operation of Synchronous Ethernet and Precision Time Protocol (PTP)) on ACX Series routers. The combined operation is possible only when the PTP client and the Synchronous Ethernet source are on the same device and are traceable to the same master. When acting as a PTP slave, the router can accept any external Synchronous Ethernet clock as reference. Note that when the selected Synchronous Ethernet reference fails, the router continues to work in PTP mode.

In hybrid mode, the synchronous Ethernet equipment clock (EEC) on the MPC derives the frequency from Synchronous Ethernet and the phase and time of day from PTP.

The hybrid mode is configured on the slave. On the slave, one or more interfaces are configured as Synchronous Ethernet source interfaces.

The ESMC quality level value is mapped to the clock class value either by mapping the PTP clock class to the ESMC quality level or by configuring a user-defined mapping of PTP clock class to ESMC quality level. The following procedures explain configuring hybrid mode with either of the modes in detail.

- Configuring the Router in Hybrid Mode on page 151
- Configuring Hybrid Mode with Mapping of the PTP Clock Class to the ESMC Quality Level on page 151
- Configuring Hybrid Mode with a User-Defined Mapping of the PTP Clock Class to the ESMC Quality Level on page 152

Configuring the Router in Hybrid Mode

To configure the router in hybrid mode, you must:

1. Configure Synchronous Ethernet options at the **[edit chassis synchronization]** hierarchy level:

   - Configure the **auto-select** mode of operation. You can select the clock source either from a free-run local oscillator or from an external qualified clock.

     When the router is configured with the **auto-select** option, the router chooses up to two best upstream clock sources. It then uses the clock recovered from one of the sources to lock the chassis clock. If an upstream clock with acceptable quality is not available or if the router is configured in free-run mode, the router uses the internal oscillator.

   - Configure the **esmc-transmit** and **network-option** options at the **[edit chassis synchronization** hierarchy level.

   - Configure one or more interfaces at the **[edit chassis synchronization]** hierarchy level as Synchronous Ethernet sources as needed.

2. Configure PTP options at the **[edit protocols ptp]** hierarchy level.

3. Configure hybrid mode options at the **[edit protocols ptp slave]** hierarchy level.

Configuring Hybrid Mode with Mapping of the PTP Clock Class to the ESMC Quality Level

To configure hybrid mode options with mapping of the PTP clock class to the ESMC quality level, perform the following steps:

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

   ```
   [edit]
   ```



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

2. Configure the **convert-clock-class-to-quality-level** option to set the default mapping between the ESMC SSM quality level and the PTP clock class.

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

3. Configure the hybrid mode option on the slave.

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

4. Configure the upstream unicast PTP master interface and IP address of the clock source.

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

5. Configure one or more Synchronous Ethernet source interfaces for the slave as needed.

```
[edit protocols ptp slave ]
user@host# set interface interface1-name unicast-mode clock-source ip-address
user@host# set interface interface2-name unicast-mode clock-source ip-address
```

NOTE: You must first configure these interfaces at the **[edit chassis synchronization]** hierarchy level as Synchronous Ethernet sources. For information about configuring these interfaces, see *synchronization (ACX Series)*.

Configuring Hybrid Mode with a User-Defined Mapping of the PTP Clock Class to the ESMC Quality Level

To configure hybrid mode options with a user-defined mapping of the PTP clock class to the ESMC quality level, perform the following steps:

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

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

2. To override the default mapping option, perform the following steps:

   a. Configure the **clock-class-to-quality-level-mapping** option with one of the quality level values. The quality level values are prc, prs, sec, smc, ssu-a, ssu-b, st2, st3, st3e, st4, stu, and tnc.


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

b. Configure the **clock-class** option for the set quality level. The clock class value ranges from 80 through 109.

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

3. Configure the hybrid mode option on the slave.

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

4. Configure the upstream PTP master interface and the IP address of the clock source.

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

5. Configure one or more Synchronous Ethernet source interfaces for the slave as needed.

```
[edit protocols ptp slave ]
user@host# set interface interface1-name unicast-mode clock-source ip-address
user@host# set interface interface2-name unicast-mode clock-source ip-address
```

NOTE: You must first configure these interfaces at the **[edit chassis synchronization]** hierarchy level as Synchronous Ethernet sources. For information about configuring these interfaces, see *synchronization (ACX Series)*.

Related Documentation

- Guidelines for Configuring Hybrid Mode on ACX Series Routers on page 149
- Hybrid Mode on ACX Series Routers Overview on page 147
- Example: Configuring Hybrid Mode and ESMC Quality Level Mapping on page 153

Example: Configuring Hybrid Mode and ESMC Quality Level Mapping

This example shows the configuration of hybrid mode by mapping the PTP clock class to the ESMC quality level and also by configuring a user-defined mapping of the PTP clock class to the ESMC quality level on ACX Series Routers.

- Requirements for Hybrid Mode Configuration on page 154
- Overview on page 154

Requirements for Hybrid Mode Configuration

This example uses the following hardware and software components:

- One ACX Series router.
- Junos OS Release 12.2R2 or later.

Overview

The combined operation of Synchronous Ethernet and Precision Time Protocol (PTP) is also known as hybrid mode. In hybrid mode, the synchronous Ethernet equipment clock (EEC) on the Modular Port Concentrator (MPC) derives the frequency from Synchronous Ethernet and the phase and time of day from PTP.

You can configure hybrid mode on ACX Series routers. On these routers, the combined operation is possible only when the PTP slave and the Synchronous Ethernet source are on the same device and are traceable to the same master. When acting as a PTP slave, the router can accept any external Synchronous Ethernet clock as reference. Note that when the selected Synchronous Ethernet reference fails, the router continues to work in PTP mode.

Hybrid mode is configured on the slave. On the slave, one or more interfaces are configured as Synchronous Ethernet source interfaces.

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

The ESMC quality level value is mapped to the clock class value either by mapping the PTP clock class to the ESMC quality level or by configuring a user-defined mapping of the PTP clock class to the ESMC quality level. The following examples explain configuring hybrid mode with either of the modes in detail.

To configure the router in hybrid mode, you must:

1. Configure Synchronous Ethernet options at the **[edit chassis synchronization]** hierarchy level:

   - Configure the **auto-select** mode of operation. You can select the clock source either from a free-run local oscillator or from an external qualified clock.

     When the router is configured with the **auto-select** option, the router chooses up to two best upstream clock sources. It then uses the clock recovered from one of the sources to lock the chassis clock. If an upstream clock with acceptable quality is not available or if the router is configured in free-run mode, the router uses the internal oscillator.

- Configure the **esmc-transmit** and **network-option** options at the **[edit chassis synchronization]** hierarchy level.
- Configure one or more interfaces at the **[edit chassis synchronization]** hierarchy level as Synchronous Ethernet sources as needed.

2. Configure PTP options at the **[edit protocols ptp]** hierarchy level.
3. Configure hybrid mode options at the **[edit protocols ptp slave]** hierarchy level.

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

Configuration

Hybrid Mode with Mapping of the PTP Clock Class to the ESMC Quality Level

CLI Quick Configuration

To quickly configure hybrid mode on the ge-1/2/3.0 interface with the clock source IP address as 2.2.2.2, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

[edit]

set protocols ptp slave hybrid
set protocols ptp slave interface ge-1/2/3.0 unicast-mode clock-source 2.2.2.2
set protocols ptp slave convert-clock-class-to-quality-level

Step-by-Step Procedure

To configure hybrid mode on an ACX Series router with mapping of the PTP clock class to the ESMC quality level, perform the following steps:

1. Configure the **convert-clock-class-to-quality-level** option on the slave at the **[edit protocols ptp slave]** hierarchy level.

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

2. Configure hybrid mode on the slave.

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

3. Configure the Synchronous Ethernet mapping option, IP address of the master clock as 2.2.2.2, and the interface ge-1/2/3.0 for hybrid mode on the slave.

```
[edit protocols ptp slave]
```

```
user@host# set interface ge-1/2/3.0 unicast-mode clock-source 2.2.2.2
```

Results

Display the results of the configuration of hybrid mode with the mapping of the PTP clock class to the ESMC quality level:

```
[edit protocols ptp slave]
user@host# show
convert-clock-class-to-quality-level
interface ge-1/2/3.0 unicast-mode clock-source 2.2.2.2
hybrid
```

Hybrid Mode with a User-Defined Mapping of the PTP Clock Class to the ESMC Quality Level

CLI Quick Configuration

To quickly configure hybrid mode on the interface ge-1/2/3.0, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

[edit]

set protocols ptp slave hybrid
set protocols ptp slave hybrid
set protocols ptp slave interface unicast-mode ge-1/2/3.0 clock-source 2.2.2.2
set protocols ptp slave clock-class-to-quality-level-mapping quality-level prc clock-class 80

Step-by-Step Procedure

To configure hybrid mode with a user-defined mapping of the PTP clock class to the ESMC quality level on an ACX Series router, perform the following steps:

1. Configure the **quality-level** option for the **clock-class-to-quality-level-mapping** statement on the slave at the **[edit protocols ptp slave]** hierarchy level and then configure the **clock-class** option for the set quality level if you want to manually override the mapping of the ESMC quality level to the clock class.

   ```
   [edit protocols ptp slave]
   user@host# set clock-class-to-quality-level-mapping quality-level prc clock-class
     80
   ```

2. Configure hybrid mode on the slave.

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

3. Configure the IP address of the master clock as 2.2.2.2 , and the interface ge-1/2/3.0 for hybrid mode on the slave.


```
[edit protocols ptp slave]
user@host# set interface ge-1/2/3.0 unicast-mode clock-source 2.2.2.2
```

Results Display the results of the configuration of hybrid mode with a user-defined mapping of the PTP clock class to the ESMC quality level:

```
[edit protocols ptp slave]
user@host# show
clock-class-to-quality-level-mapping {
  quality-level prc {
    clock-class 80;
  }
}
interface  ge-1/2/3.0 unicast-mode clock-source 2.2.2.2
hybrid
```

Verification

Verifying That the Router Is Operating in Hybrid Mode

Purpose Verify the current mode of operation of the slave.

Action In operational mode, enter the **run show ptp hybrid** command to display the current configuration and current mode of operation of the slave.

In operational mode, enter the **run show ptp hybrid config** command to display the PTP source to Synchronous Ethernet interface mappings.

In operational mode, enter the **run show ptp hybrid status** command to display the current hybrid mode operational status.

Meaning The output displays the current configuration and current mode of operation of the slave. For information about the **run show ptp hybrid** operational command, see *show ptp hybrid*.

Verifying the Quality Level Change on the Transmit Side

Purpose Verify the quality level change on the transmit side of the router.

Action In operational mode, enter the **run show synchronous-ethernet esmc transmit detail** command to display the ESMC transmit interface details.

Meaning The output displays the ESMC SSM quality level transmitted out of various Ethernet interfaces. For information about the **run show synchronous-ethernet esmc transmit detail** operational command, see *show synchronous-ethernet esmc transmit*.

Verifying Global Information Parameters After Mapping of the PTP Clock Class to the ESMC Quality Level in Hybrid Mode

Purpose Verify the global information parameters after mapping of the PTP clock class to the ESMC quality level in hybrid mode by enabling the **convert-clock-class-to-quality-level** option.

Action In operational mode, enter the **run show ptp global-information** command to display the following output:

user@host> **run show ptp global-information**

```
PTP Global Configuration:
Domain number            : 0
Transport Encapsulation : IPv4
Clock mode               : Ordinary
Priority Level1          : 128
Priority Level2          : 128
Unicast Negotiation      : Disabled
ESMC QL From Clock Class: Enabled
Clock Class/ESMC QL      : 84 / (QL SSU-A/SSM 0x4)
Slave Parameters:
  Sync Interval          : -
  Delay Request Interval: -6 (64 packets per second)
  Announce Interval      : -
  Announce Timeout       : 3
Master Parameters:
  Sync Interval          : -6 (64 packets per second)
  Delay Request Interval: -
  Announce Interval      : 1 (1 packet every 2 seconds)
  Clock Step             : one-step
Number of Slaves        : 1
Number of Masters       : 0
```

In operational mode, enter the **run show ptp quality-level-mapping** command to display the following output:

user@host> **run show ptp quality-level-mapping**

```
quality level          ptp clock class
PRC                       84
SSU-A                     92
SSU-B                     96
SEC                       104
```


Meaning The output for **run show ptp global-information** displays the parameters set in Synchronous Ethernet mode and the parameters set for the master and the slave.

The output of **run show ptp quality-level-mapping** displays the default mapping of the clock class to the ESMC quality level.

Verifying Global Information Parameters After Configuring User-Defined Mapping of the PTP Clock Class to the ESMC Quality Level in Hybrid Mode

Purpose Verify the global information parameters after configuring a user-defined mapping of the PTP clock class to the ESMC quality level in hybrid mode by disabling the **convert-clock-class-to-quality-level** option.

Action In operational mode, enter the **run show ptp global-information** command to display the following output:

`user@host>` **run show ptp global-information**

```
PTP Global Configuration:
Domain number           : 0
Transport Encapsulation : IPv4
Clock mode              : Ordinary
Priority Level1         : 128
Priority Level2         : 128
Unicast Negotiation     : Disabled
ESMC QL From Clock Class: Disabled
Clock Class/ESMC QL     :  -
Slave Parameters:
  Sync Interval         : -
  Delay Request Interval: -6 (64 packets per second)
  Announce Interval     : -
  Announce Timeout      : 3
Master Parameters:
  Sync Interval         : -6 (64 packets per second)
  Delay Request Interval: -
  Announce Interval     : 1 (1 packet every 2 seconds)
  Clock Step            : one-step
```

Meaning The output displays the parameters set in Synchronous Ethernet mode and the parameters set for the master and the slave.

Related Documentation

- Guidelines for Configuring Hybrid Mode on ACX Series Routers on page 149
- Hybrid Mode on ACX Series Routers Overview on page 147
- Configuring Hybrid Mode and ESMC Quality Level Mapping on ACX Series Routers on page 150

Understanding Timing Defects and Event Management on ACX Series

Junos OS for ACX Universal Metro Routers supports defect and event management capabilities for timing features. Defects and events are notified in the form of SNMP traps and these SNMP traps are logged into the system log-file (var/log/snmpd). For each of the SNMP traps (timing defects and timing events) that are generated, a message is logged in the clksyncd file (var/log/clksyncd).

Table 6 on page 160 shows the list of SNMP trap notifications for timing defects and events supported in ACX Universal Metro Routers.

Table 6: SNMP trap notifications for timing defects and events

SNMP Trap	Notification Type	Description
jnxTimingFaultLOS	Defects	Denotes loss of signal
jnxTimingFaultEFD	Defects	Denotes exceeded frequency deviation
jnxTimingFaultLOESMC	Defects	Denotes loss of Ethernet Synchronization Message Channel (ESMC)
jnxTimingFaultQLFailed	Defects	Denotes failure in quality level
jnxTimingFaultLTI	Defects	Denotes loss of timing information
jnxTimingFaultPriSrcFailed	Defects	Denotes the failure of primary source
jnxTimingFaultSecSrcFailed	Defects	Denotes the failure of secondary source
jnxTimingFaultPtpUniNegRateReject	Defects	When acting as master, this SNMP trap denotes failure or rejects clients for signaling messages. When acting as a slave, this SNMP trap denotes failure or client stops receiving signaling messages
jnxTimingEventPriSrcRecovered	Events	Denotes the recovery of primary source
jnxTimingEventSecSrcRecovered	Events	Denotes the recovery of secondary source
jnxTimingEventPriRefChanged	Events	Denotes a change in primary reference such as a change in logical interface or a change from SyncE to BITS/external interface)
jnxTimingEventSecRefChanged	Events	Denotes a change in secondary reference such as a change in logical interface
jnxTimingEventQLChanged	Events	Denotes a change in quality level
jnxTimingEventDpllStatus	Events	Denotes the DPLL status (SyncE, BITS, Hybrid)

Table 6: SNMP trap notifications for timing defects and events (continued)

SNMP Trap	Notification Type	Description
jnxTimingEventPtpServoStatus	Events	Denotes the following PTP Servo states: • INITIALIZING • ACQUIRING (Master is elected and servo starts acquiring lock) • PHASE ALIGNED (Locked to Master) • FREERUN (no PTP source available) • HOLDOVER (Slave locked to PTP for more than 12 hours and then loses all the PTP sources)
jnxTimingEventPtpClockClassChange	Events	Denotes a change in PTP clock class
jnxTimingEventPtpClockAccuracyChange	Events	Denotes a change in PTP accuracy
jnxTimingEventPtpGMChange	Events	Denotes a change in PTP grandmaster clock
jnxTimingEventHybridStatus	Events	Denotes the following hybrid states: • INITIALIZING • ACQUIRING (Master is elected and servo starts acquiring lock) • FREQUENCY LOCKED (Frequency locked but acquiring phase) • PHASE ALIGNED (Frequency and phase locked)

To configure and generate timing defects and events trap notifications, include the **timing-events** statement at the [**edit snmp trap-group *trap-group-name* categories**] hierarchy level as shown below:

```
[edit]
snmp {
    trap-group <group-name> {
       categories {
          timing-events;
        }
    }
}
```

The following is a sample configuration for SNMP timing in ACX Series routers:

```
snmp {
    trap-options {
        source-address 10.216.66.139;
    }
    trap-group timingGroup {
        version v2;
        destination-port 8999;
        categories {
```

```
            timing-events;
        }
        targets {
            192.168.120.129;
        }
    }
    traceoptions {
        flag all;
    }
}
```

Related Documentation

- *show chassis synchronization*
- *source*
- Understanding SNMP MIB for Timing on ACX Series on page 162

Understanding SNMP MIB for Timing on ACX Series

Junos OS for ACX Universal Metro Routers supports SNMP get, get-next, and walk management capabilities for timing features. These capabilities are enabled through the PTP MIB, SyncE MIB and GPS MIB timing objects.

NOTE: The PTP MIB and SyncE MIB timing objects are grouped under the **jnxTimingNotfObjects** SNMP MIB object.

Table 7 on page 163 shows the list of SNMP MIB objects supported for SNMP get, get-next, and walk management on ACX Universal Metro Routers.

Table 7: SNMP MIB Objects for get, get-next, and walk management

SNMP MIB	Object	Description
PTP MIB	jnxPtpServoState	Denotes the following PTP Servo states: • INITIALIZING • ACQUIRING • PHASE ALIGNED • FREERUN • HOLDOVER • FREQUENCY LOCKED
	jnxPtpServoStateStr	Denotes the PTP Servo state string: • INITIALIZING • ACQUIRING (Master is elected and servo starts acquiring lock) • PHASE ALIGNED (Locked to Master) • FREERUN (no PTP source available) • HOLDOVER (Slave locked to PTP for more than 12 hours and then loses all the PTP sources)
	jnxPtpClass	Denotes the class of the PTP grandmaster clock.
	jnxPtpGmId	Denotes the PTP grandmaster clock identifier.
SyncE MIB	jnxClksyncQualityCode	Denotes the SSM/ESMC quality level of the locked source in decimal format.
	jnxClksyncQualityCodeStr	Denotes the SSM/ESMC quality level of the locked source in string format
	jnxClksyncIfIndex	Denotes the interface index of the locked source in decimal format.
	jnxClksyncIntfName	Denotes the interface name of the locked source in string format.
GPS MIB	jnxGpsRecvStatus	Displays the status of the GPS receiver.

NOTE:

- The SNMP get and walk management are supported only for scalar objects.
- For SyncE objects, the jnxClksyncQualityCode, jnxClksyncQualityCodeStr, jnxClksyncIfIndex, and jnxClksyncIntfName objects displays only for locked source.

You can use the **show chassis synchronization extensive**, **show ptp lock-status detail**, **show snmp mib get <*MIB-timing-objects*>**, and **show snmp mib walk jnxTimingNotfObjects** show commands for monitoring and troubleshooting purposes.

The following are the sample show command outputs for reference:

show chassis synchronization extensive

user@host> **show chassis synchronization extensive**

```
Current clock status  : Locked
Clock locked to       : Primary
SNMP trap status : Enabled

Configured sources:

Interface           : ge-0/0/7
Status              : Secondary     Index       : 136
Clock source state  : Clk qualified Priority    : Default(8)
Configured QL       : SEC           ESMC QL     : PRC
Clock source type   : ifd           Clock Event : Clock qualified
Interface State     : Up,sec,ESMC Rx(SSM 0x2),ESMC TX(QL SEC/SSM 0xb),

Interface           : ge-0/1/1
Status              : Primary       Index       : 138
Clock source state  : Clk qualified Priority    : Default(8)
Configured QL       : PRC           ESMC QL     : PRC
Clock source type   : ifd           Clock Event : Clock locked
Interface State     : Up,pri,ESMC Rx(SSM 0x2),ESMC TX(QL DNU/SSM 0xf)
```

show chassis synchronization extensive

user@host> **show chassis synchronization extensive**

```
Configured ports:

Name                : auxiliary
Rx status           : active
Rx message          : TL000001433759011353
Current ToD         : Mon Jun  8 10:23:31 2015
Last ToD update     : Mon Jun  8 10:23:30 2015
GPS receiver status : Lost Sync
UTC Pending         : FALSE
UTC Offset          : 35

One PPS status : Active

Configured sources:

Interface           : gps
Status              : Primary       Index       : 1
Clock source state  : Clk failed    Priority    : Default(6)
Configured QL       : PRC           ESMC QL     : DNU
Clock source type   : extern        Clock Event : Clock failed
Interface State     : Up,pri
```

show ptp lock-status detail

user@host> **show ptp lock-status detail**

```
Lock Status:
```

```
Lock State    : 1 (FREERUN)
Phase offset  : 0.000000000 sec
State since   : 2015-05-04 03:13:49 PDT (00:01:45 ago)

Selected Master Details:
Upstream Master address    : 61.1.1.2
Slave interface            : ge-0/1/1.0
Parent Id                  : 40:b4:f0:ff:fe:42:f5:00
GMC Id                     : 40:b4:f0:ff:fe:42:d5:00
```

show snmp mib get <MIB-timing-objects>

user@host> **show snmp mib get jnxGpsRecvStatus.0**

```
jnxGpsRecvStatus.0 = Lost Sync
```

show snmp mib walk jnxTimingNotfObjects

user@host> **show snmp mib walk jnxTimingNotfObjects**

```
jnxClksyncIfIndex.0 = 138
jnxClksyncIntfName.0 = ge-0/1/1
jnxClksyncQualityCode.0 = 2
jnxPtpServoState.0 = 1
jnxPtpClass.0 = 6
jnxPtpGmId.0  = 40:b4:f0:ff:fe:42:d5:00
jnxClksyncQualityCodeStr.0 = PRC
jnxPtpServoStateStr.0 = FREERUN
```

Related Documentation

- *show chassis synchronization*
- Understanding Timing Defects and Event Management on ACX Series on page 160

CHAPTER 5

Configuration Statements

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;
diag-port-authentication (encrypted-password "password" | plain-text-password);
dynamic-profile-options {
    versioning;
}
domain-name domain-name;
domain-search [ domain-list ];
fips {
    level level;
```



```
}
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-keykey-number type type value password;
      boot-server address;
      broadcast <address> <key key-number> <version value> <ttl 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 ];
            portport-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-strings 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";
      match-strings string-name;
      source-address source-address;
      structured-data {
        brief;
      }
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    user (username | *) {
      facility severity;
      match "regular-expression";
      match-strings string-name;
    }
  }
  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;
}
```

boot-server (NTP)

Syntax

boot-server (*address* | *hostname*);

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 server that NTP queries when the router or switch boots to determine the local date and time.

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.

Options

- ***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

- Understanding NTP Time Servers on page 21
- Configuring NTP Authentication Keys on page 50
- Synchronizing and Coordinating Time Distribution Using NTP on page 57

broadcast

Syntax

```
broadcast address <key key-number> <version value> <ttl value>;
```

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

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**.

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).

ttl *value*—(Optional) Time-to-live (TTL) value to use.

Range: 1 through 255

Default: 1

version *value*—(Optional) Specify the version number to be used in outgoing NTP packets.

Range: 1 through 4

Default: 4

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Understanding NTP Time Servers on page 21
- Configuring NTP Authentication Keys on page 50
- Configuring the NTP Time Server and Time Services on page 52

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

- Understanding NTP Time Servers on page 21
- Configuring NTP Authentication Keys on page 50
- Configuring the Switch to Listen for Broadcast Messages Using NTP on page 55

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 Metro 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.

NOTE: A boundary clock is not supported on the ACX Series routers for 12.2.

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

- *Configuring Precision Time Protocol*
- *Example: Configuring Precision Time Protocol*
- *Precision Time Protocol Overview*
- IEEE 1588v2 Precision Timing Protocol (PTP) on page 71
- Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 86

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.
Statement introduced in Junos OS Release 19.2R1 for ACX6360-OR and PTX10001-20C devices

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.

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

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

- Configuring Transparent Clock Mode for Precision Time Protocol on page 85

interface (PTP Slave)

Syntax

```
interface interface-name {
  unicast-mode {
    clock-source ip-address {
      local-ip-address local-ip-address;
    }
  }
  transport ipv4;
  }
}
```

Hierarchy Level

```
[edit protocols ptp slave]
```

Description The interface on which to respond to the upstream PTP master.

Options

unicast-mode—Configure upstream unicast PTP master clock sources

clock-source—Configure the parameters of the PTP.

local-ip-address—Configure the IP address of the local interface acting as the slave.

asymmetry—Specify the asymmetry value between the master and the slave.

transport—Configure the encapsulation type 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 Precision Timing Protocol (PTP) on page 71
- *Precision Time Protocol Overview*
- Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 86

ntp

Syntax

```
ntp {
  authentication-key key-number type md5 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. In both standalone and chassis cluster modes, the primary Routing Engine runs the NTP process to get the time from the external NTP server. Although the secondary Routing Engine runs the NTP process in an attempt to get the time from the external NTP server, this attempt fails because of network issues. For this reason, the secondary Routing Engine uses NTP to get the time from the primary Routing Engine.

NOTE: There must be no space in the password for configuring the Network Time Protocol (NTP) authentication-key.

Options

authentication-key—Configure NTP authentication keys so authenticated packets can be sent.

boot-server—Configure the server that NTP queries when the router or switch boots to determine the local date and time.

broadcast—Configure the local router or switch to operate in broadcast mode with the remote system.

broadcast-client—Configure the local router or switch to listen for broadcast messages on the local network to discover other servers on the same subnet.

multicast-client—Configure the local router or switch to listen for multicast messages on the local network.

peer—Configure the local router or switch to operate in symmetric active mode with the remote system at the specified address.

server—Configure the local router or switch to operate in client mode with the remote system

source-address—A valid IP address configured on one of the router or switch interfaces

trusted-key—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.

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 22
- *NTP Time Synchronization on SRX Series Devices*

ntp (QFabric)

Syntax

```
ntp {
  authentication-key number type type value password;
  server address <key key-number> <version value> <prefer>;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure Network Time Protocol (NTP) on the switch.

Options

authentication-key—Configure NTP authentication keys so authenticated packets can be sent.

server—Configure the switch to operate in client mode with the remote system at the specified server address.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring NTP Authentication Keys (QFabric System) on page 51
- Configuring the NTP Time Server and Time Services (QFabric System) on page 55

profile-type

QFX Series (AES67 Profile)

```
profile-type aes67
```

QFX Series (AES67+SMPTE Profile)

```
profile-type aes67-smpte
```

List of Syntax

QFX Series (AES67 Profile) on page 183
QFX Series (AES67+SMPTE Profile) on page 183
MX Series on page 183
QFX Series (Enterprise Profile) on page 183
QFX Series (G.8275.2 Enhanced Profile) on page 183
QFX Series (SMPTE Profile) on page 183

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
```

QFX Series (SMPTE Profile)

```
profile-type smpte
```

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

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.

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.

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.

On QFX Series switches that support the media profile, you can configure the SMPTE, AES67, and the AES67+SMPTE profiles to support video applications for capture (for example, cameras), video edit, and playback to be used in professional broadcast environments. The standard allows multiple video sources to stay in synchronization across various equipment by providing time and frequency synchronization to all devices. This profile supports PTP over IPv4 multicast and ordinary and boundary clocks.

Options

aes67—Enable the AES67 PTP profile.

aes67-smpte—Enable the AES67+SMPTE PTP profile.

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.

g.8275.1—Enable the G.8275.1 PTP profile.

g.8275.1.enh—Enable the enhanced G.8275.1 PTP profile. This profile supports PTP over IPv4.

g.8275.2.enh—Enable the enhanced G.8275.2 PTP profile. This profile supports PTP over IPv4 unicast.

smpte—Enable the SMPTE PTP profile.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Precision Time Protocol Overview*
- Configuring the Precision Time Protocol Enterprise Profile on page 99
- Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 86

slave

List of Syntax

MX Series on page 185
QFX Series on page 185

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.

Options

announce-interval—Configure the logarithmic mean interval for the announce messages to be sent by the master.

announce-timeout—Specify the number of announce messages a slave must miss before an announce-timeout is declared.

delay-request—Configure the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.

frequency-only—Configure frequency synchronization.

hybrid—Configure the timing and synchronization feature to operate in Sync-E assisted PTP mode of operation.

unicast-mode—Configure the slave in unicast mode.

clock-source—Configure the IP address of the master.

multicast-mode—Configure multicast transmission of PTP packets between the master node and the slave node.

transport 802.3—Configure Ethernet as the encapsulation type for transport of PTP packets.

sync-interval—Configure the logarithmic mean interval for sync interval messages to be sent by the master.

unicast-mode—Configure the master in unicast mode.

clock-client—Configure the IP address of the slave

transport—Configure the encapsulation type for PTP packet transport.

local-ip-address—Configure the IP address of the interface acting as the slave or the master.

local-priority—Configure a clock's local priority to be used as a tie-breaker in the dataset comparison algorithm, if all other attributes of the datasets being compared are equal.

max-announce-interval—Configure the maximum log mean interval between announce messages.

max-delay-response-interval—Configure the maximum log mean interval between delay-response messages.

max-sync-interval—Configure the maximum log mean interval between synchronization messages.

min-announce-interval—Configure the minimum log mean interval between announce messages.

min-delay-response-interval—Configure the minimum log mean interval between delay-response messages.

min-sync-interval—Configure the minimum log mean interval between synchronization messages.

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 86

source-address (NTP, RADIUS, System Logging, or TACACS+)

Syntax

```
source-address source-address;
```

Hierarchy Level

```
[edit system accounting destination radius server server-address],
[edit system accounting destination tacplus server server-address],
[edit system ntp],
[edit system radius-server server-address],
[edit system syslog],
[edit system tacplus-server server-address]
```

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 ***source-address***—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 *hostname*** statements at the **[edit system syslog]** hierarchy level.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring RADIUS Authentication (QFX Series or OCX Series)*
- Synchronizing and Coordinating Time Distribution Using NTP on page 57
- *Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination*

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.

Options This command has no options.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- System Management Configuration Statements on page 167

time-zone

Syntax

```
time-zone (GMT hour-offset | time-zone);
```

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 ***hour-offset*** 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

GMT ***hour-offset***—Set the time zone relative to UTC time.

Range: –14 through +12

Default: 0

time-zone—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:

```
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
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, 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/Guadalcanal, 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 Level

system—To view this statement in the configuration.
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 45
- System Management Configuration Statements on page 167

use-imported-time-zones

Syntax

```
use-imported-time-zones;
```

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

- Updating the IANA Time Zone Database on Junos OS Devices on page 46

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*> <key *key*> <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.

> NOTE: **In Junos OS Evolved, if the ntpd server is running, the set date ntp command fails with the following error message: error: ntpd is already running. To use this command, you must first stop the ntpd server**

- ***ntp-server***—(Optional) Specify the IP address of one or more NTP servers.
- **key *key***—Configure the key to authenticate the NTP server.
- **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 17

List of Sample Output

set date ntp (Junos OS) on page 194
set date ntp (Junos OS Evolved) on page 195

Sample Output

set date ntp (Junos OS)

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



```
22 Jun 10:07:48 ntpdate[51123]: step time server 66.129.255.62 offset -0.013200
sec
```

set date ntp (Junos OS Evolved)

user@host> **set date ntp**

```
-------------------------------
node: re0
-------------------------------
error: ntpd is already running
```

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

- show ntp status on page 198

List of Sample Output

show ntp associations on page 197

Output Fields

Table 8 on page 196 describes the output fields for the **show ntp associations** command. Output fields are listed in the approximate order in which they appear.

Table 8: 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 8: 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: • 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

```
show ntp status
<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 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

- show ntp associations on page 196

List of Sample Output

show ntp status on page 199

Output Fields

Table 9 on page 198 describes the output fields for the **show ntp status** command. Output fields are listed in the approximate order in which they appear.

Table 9: 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 9: 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 68
- IEEE 1588v2 Precision Timing Protocol (PTP) on page 71
- *Precision Time Protocol Overview*

List of Sample Output

show ptp clock on page 203
show ptp clock (ACX Series Routers) on page 203

Output Fields

Table 10 on page 201 lists the output fields for the **show ptp clock** command. Output fields are listed in the approximate order in which they appear.

Table 10: 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 10: 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                    Clock Identity :
00:05:85:ff:fe:73:ef:d0
Total Ports on Device : 0                        Clock Class    : 255
Clock Accuracy        : 49                       Log Variance   : -12944
Clock Priority1       : 128                      Clock Priority2: 128
UTC Offset            : 33                       Leap59         : FALSE
Leap61                : FALSE                    Time Traceable  : FALSE
Frequency Traceable   : FALSE                    Time master    : 0
Delay Req Sending Time: 0                        Steps Removed  : 1
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 Class        : 52
GMC Accuracy          : 254                       GMC Variance     : 11952
GMC Priority1         : 0                         GMC Priority2    : 0
Global Data:
UTC Offset            : 34                        Leap-59          : FALSE
Leap-61               : FALSE                     Time traceable    : FALSE
Freq Traceable        : FALSE                     Time Scale       : FALSE
Time master           : 160
```

show ptp clock (ACX Series Routers)

user@host> **run show ptp clock**

```
Clock Details:
Slot Number           : 0
Default Data:
Two-step Clock        : FALSE                    Clock Identity :
84:18:88:ff:fe:c0:7a:00
Total Ports on Device : 0                        Clock Class    : 255
Clock Accuracy        : 34                       Log Variance   : 15353
Clock Priority1       : 128                      Clock Priority2: 128
UTC Offset            : 0                        Leap59         : FALSE
Leap61                : FALSE                    Time Traceable : FALSE
Frequency Traceable   : FALSE                    Time Source    : 0
Delay Req Sending Time: 0                        Steps Removed  : 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 Class        : 80
GMC Accuracy          : 35                        GMC Variance     : 0
GMC Priority1         : 128                       GMC Priority2    : 128
Global Data:
UTC Offset            : 0                         Leap-59          : FALSE
Leap-61               : FALSE                     Time tracable    : FALSE
Freq Traceable        : FALSE                     Time Scale       : FALSE
Time source           : 16
```


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

- Understanding Transparent Clocks in Precision Time Protocol on page 66
- Configuring Transparent Clock Mode for Precision Time Protocol on page 85
- Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 86

List of Sample Output

show ptp global-information (Transparent Clock Configured) on page 205
show ptp global-information (Default Profile) on page 205
show ptp global-information (Enterprise Profile) on page 206

Output Fields Table 11 on page 204 lists the output fields for the **show ptp global-information** command. Output fields are listed in the approximate order in which they appear.

Table 11: 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 ***priority1-value*** is the same for different master clocks in a network. The lower value takes precedence.

Table 11: show ptp global-information Output Fields (continued)

Field Name	Field Description
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.
ESMC QL From Clock Class	Denotes whether the conversion from clock class to QL is enabled or disabled.
Clock Class/ESMC QLl	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: • **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. NOTE: Transparent clock operation is disabled during the synchronization of PHYs. • **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

```
show ptp master
<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 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

- *Precision Time Protocol Overview*
- Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 86

Output Fields

Table 12 on page 207 lists the output fields for the **show ptp master** command. Output fields are listed in the approximate order in which they appear.

Table 12: 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: • **Master** or **Slave** • **Active** or **Inactive** • **Initializing** or **Down**
Local Adddress	IP or MAC address of the configured master clock.
Status (Local address Status)	Status of the local address of the interface: • **Configured** or **Not configured** • **Master** or **Slave** • **Active** or **Inactive**

Table 12: 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: • **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: • **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 master detail (with IPv6 addresses for PTP master/slave using loopback interface on the QFX Series)

user@host> **run show ptp master detail**

```
PTP Master Interface Details:
Interface   : lo0.0
Status      : Master, Active
Clock Info :
    Local Address: 2001::1:132        Status: Configured, Master, Active
        Remote Address: 2002::1            Status: SECURE AUTO SLAVE,
                                                   Sig State: Ann + Sync
        Remote Address: 3001::1:133        Status: SECURE AUTO SLAVE,
                                                   Sig State: Ann + Sync
    Total Remote Slaves: 2
```

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

- *Precision Time Protocol Overview*
- Configuring the Precision Time Protocol G.8275.2 Enhanced Profile (Telecom Profile) on page 86

Output Fields

Table 13 on page 211 lists the output fields for the **show ptp slave** command. Output fields are listed in the approximate order in which they appear.

Table 13: 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: • **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.

Table 13: show ptp slave Output Fields (continued)

Field Name	Field Description
Status (Local address Status)	Status of the local address of the interface acting as the slave: • **Configured** or **Unconfigured** • **Master** or **Slave** • **Active** or **Inactive** or **Ready**
Status (Remote address Status)	Status of the remote address of the interface on the QFX Series: • **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: • **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 slave detail (with IPv6 addresses for PTP master/slave using AE interface on the QFX Series)

`user@host>` **run show ptp slave detail**

```
PTP Slave Interface Details:

Interface        : ae0.0
Status           : Slave, Active
Clock Info
    Local Address : 2003::b                  Status: Configured, Slave, Active
        Remote Master: 2003::a          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

- IEEE 1588v2 PTP Boundary Clock Overview on page 68
- IEEE 1588v2 Precision Timing Protocol (PTP) on page 71
- *Precision Time Protocol Overview*

List of Sample Output

Output Fields

Table 14 on page 214 lists the output fields for the **show ptp lock-status** command. Output fields are listed in the approximate order in which they appear.

Table 14: show ptp lock-status Output Fields

Field Name	Field Description
Lock State	State of the slave clock with respect to its master clock: • Freerun • Holdover • Phase Aligned • Acquiring • Initializing • Freq locked

Table 14: show ptp lock-status Output Fields (continued)

Field Name	Field Description
Phase offset	Time offset information of a slave clock with respect to its master clock. Precision of this time offset is 1 nanosecond.
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	Details include the following: • **Upstream Master address**—The address of the remote master from which the salve acquires the clock. • **Slave interface**—The slave interface on this router corresponding to the Master above. NOTE: On ACX Series router, if the PTP lock state is **FREERUN**, then the **Selected Master Details** field is not shown.

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 lock-status detail (with IPv6 addresses for PTP master/slave with AE interface)

user@host> **show ptp lock-status detail**

```
Lock Status:

Lock State    : 5 (PHASE ALIGNED)
Phase offset  : -0.000000016 sec
State since   : 2018-10-17 01:53:29 UTC (01:09:37 ago)

Selected Master Details:
Upstream Master address    : 2003::a
Slave interface            : ae0.0
Parent Id                  : 12:34:56:78:9a:bc:de:01
GMC Id                     : 12:34:56:78:9a:bc:de:01
```

show ptp lock-status detail (with IPv6 addresses for PTP master/slave with loopback interface)

user@host> **show ptp lock-status detail**

```
Lock Status:

Lock State    : 5 (PHASE ALIGNED)
Phase offset  : -0.000000016 sec
State since   : 2018-10-17 01:53:29 UTC (01:09:37 ago)

Selected Master Details:
Upstream Master address    : 2003::a
Slave interface            : lo0.0
Parent Id                  : 12:34:56:78:9a:bc:de:01
GMC Id                     : 12:34:56:78:9a:bc:de:01
```


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

- IEEE 1588v2 PTP Boundary Clock Overview on page 68
- IEEE 1588v2 Precision Timing Protocol (PTP) on page 71

List of Sample Output

show ptp statistics on page 218
show ptp statistics (with IPv6 addresses for PTP master/slave) on page 218
show ptp statistics detail on page 219
show ptp statistics detail (with IPv6 addresses for PTP master/slave) on page 219
show ptp statistics (with IPv6 addresses for PTP master/slave using AE and loopback interfaces on the QFX Series)) on page 219
show ptp statistics detail (Enterprise profile statistics for remote devices on the QFX Series) on page 219
show ptp statistics detail (Enhanced Profile statistics for remote devices using AE and loopback interfaces on the QFX Series) on page 220

Output Fields

Table 15 on page 217 lists the output fields for the **show ptp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 15: 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.

Table 15: show ptp statistics Output Fields (continued)

Field Name	Field Description
Received	1588v2 packets received by the master or slave interface. For the QFX Series, all packets transmitted by the master or slave interface.
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: • Rx—Number of packets received. • Tx—Number of packets transmitted.
Announce	Packet count for announce messages: • Rx—Number of packets received. • Tx—Number of packets transmitted.
Sync	Packet count for synchronization messages: • Rx—Number of packets received. • Tx—Number of packets transmitted.
Delay	Packet count for delay request or response messages: • Rx—Number of packets received. • Tx—Number of packets transmitted.
Error	Packet count for signal loss errors: • 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      2222524
```

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 (with IPv6 addresses for PTP master/slave using AE and loopback interfaces on the QFX Series))

user@host> **show ptp statistics**

```
Local Clock       Remote Clock        Role  Stream      Received  Transmitted
ae0.0             2003::a            Slave       0        666694       331379
lo0.0             2002::1           Master       4        696526      1405758
lo0.0             3001::1:133       Master       5        680312      1373318
```

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
```

show ptp statistics detail (Enhanced Profile statistics for remote devices using AE and loopback interfaces on the QFX Series)

user@host> **show ptp statistics detail**

```
Local Clock      Remote Clock       Role  Stream      Received  Transmitted
ae0.0            2003::a            Slave       0       167235        82773
         Signalling     Announce         Sync       Delay       Error
   Rx:           15        1303       83174       82758           0
   Tx:           17           0           0       82761           0
Local Clock      Remote Clock       Role  Stream      Received  Transmitted
lo0.0            2002::1           Master       4        82152       167879
         Signalling     Announce         Sync       Delay       Error
   Rx:          132           0           0       82020           0
   Tx:          132        1320       84407       82020           0
Local Clock      Remote Clock       Role  Stream      Received  Transmitted
lo0.0            3001::1:133       Master       5          131         1450
         Signalling     Announce         Sync       Delay       Error
   Rx:          131           0           0           0           0
   Tx:          131        1319           0           0           0
```