JUNIPER NETWORKS

# Junos® OS

## Time Management, Junos OS Release 11.4

Release
11.4

Published: 2011-11-08
Revision 1

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net



*Junos® OS Time Management, Junos OS Release 11.4*


Revision History
October 2011—Revision 1; initial release

The information in this document is current as of the date listed in the revision history.

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

# Table of Contents

# List of Tables



 

PART 1

# Overview

 

CHAPTER 1

# Time Management Overview



## NTP Overview

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.

NTP is defined in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

For Common Criteria compliance, configure NTP to provide accurate timestamps for system log messages.

In 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.

When configuring NTP, you do not actively configure time servers. Rather, all clients also are servers. An NTP server is not believed unless it, in turn, is synchronized to another NTP server—which itself must be synchronized to something upstream, eventually terminating in a high-precision clock.

By default, if the time difference between the local router clock and the NTP server clock is more than 128 milliseconds, the clocks are slowly stepped into synchronization. However, if the difference is more than 1000 seconds, the clocks are not synchronized. On the local router, you set the date and time using the **set date** command. To set the time automatically, use the **boot-server** statement at the **[edit system ntp]** hierarchy level, specifying the address or hostname of an NTP server.

**Related Documentation**

- Synchronizing and Coordinating Time Distribution Using NTP on page 8

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

## NTP Time Server and Time Services Overview

When configuring the Network Time Protocol (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 or switch 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**

- Configuring the NTP Time Server and Time Services
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization

PART 2

# Configuration

CHAPTER 2

# Configuring Time



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

The default local time zone on the router 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 (GMT hour-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.

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;
}
```

**Related Documentation**

- NTP Overview on page 3
- Setting a Custom Time Zone on Routers or Switches Running Junos OS on page 14

## 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 8
2. Configuring the NTP Boot Server on page 8
3. Specifying a Source Address for an NTP Server on page 8

### 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> <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 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 will not be able to synchronize to a time server if the server's time appears to be very far off of the local router's or 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 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.

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.

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.

**Related Documentation**

- NTP Overview on page 3
- NTP Time Server and Time Services Overview on page 4
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization

## Configuring the NTP Time Server and Time Services

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

- Client mode
- Symmetric active mode

- Broadcast mode
- Server mode

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

1. Configuring the Router or Switch to Operate in Client Mode on page 10
2. Configuring the Router or Switch to Operate in Symmetric Active Mode on page 10
3. Configuring the Router or Switch to Operate in Broadcast Mode on page 11
4. Configuring the Router or Switch to Operate in Server Mode on page 11

## 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> <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 12.

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 12. For information about how to configure an NTP boot server, see "Configuring the NTP Boot Server" on page 8. 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 11.

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 12.

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 12.

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> <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 12.

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.

For information about how to configure trusted keys, see "Configuring NTP Authentication Keys" on page 12. 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 10.

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;
```

**Related Documentation**

- NTP Time Server and Time Services Overview on page 4
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization

## Configuring NTP Authentication Keys

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

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

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

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

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

 

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

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

**Related Documentation**

- NTP Time Server and Time Services Overview on page 4
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization

## 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 13
- Configuring the NTP Time Server and Time Services on page 9
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization

## 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 13
- Configuring the NTP Time Server and Time Services on page 9
- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization

## Setting a Custom Time Zone on Routers or Switches Running Junos OS

You can update the time zone database information on routers or switches running Junos OS. This feature simplifies time zone management in devices running Junos OS by allowing for future unforeseen time zone database adjustments. You can configure your router or switch to use a custom time zone database file that you create to meet your requirements by editing an existing time zone database file.

Tasks for setting a custom time zone are:

1. Importing and Installing Time Zone Files on page 14
2. Configuring a Custom Time Zone on page 15

### Importing and Installing Time Zone Files

To import and install time zone files, follow these steps:

1. Download the time zone files archive and untar them to a temporary directory such as **/var/tmp**:

```
# mkdir -p /var/tmp/tz && cd /var/tmp/tz && rm *
# wget 'ftp://elsie.nci.nih.gov/pub/tzdata*.tar.gz'
# tar xvzf tzdata*.gz
africa
antarctica
asia
australasia
europe
northamerica
southamerica
pacificnew
etcetera
factory
backward
systemv
solar87
solar88
solar89
iso3166.tab
zone.tab
leapseconds
yearistype.sh
```

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

2. 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**

3. 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/**.

4. Set the time zone and commit the configuration:

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

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

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

## 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 7
- NTP Overview on page 3
- NTP Time Server and Time Services Overview on page 4

- Example: Configuring NTP as a Single Time Source for Router and Switch Clock Synchronization
- use-imported-time-zones on page 34

CHAPTER 3

# 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 {
        events [ login change-log interactive-commands ];
        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;
                    }
                }
            }
        }
    }
    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 synchronize;
  (compress-configuration-files | no-compress-configuration-files);
  default-address-selection;
  dump-device (compact-flash | remove-compact | usb);
  diag-port-authentication (encrypted-password "password" | plain-text-password);
  dynamic-profile-options {
    versioning;
  }
  domain-name domain-name;
  domain-search [ domain-list ];
  host-name hostname;
  inet6-backup-router address <destination destination-address>;
  internet-options {
    tcp-mss mss-value;
    (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
    icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
    icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
    (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
    (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
    ipv6-path-mtu-discovery-timeout;
    no-tcp-rfc1323-paws;
    no-tcp-rfc1323;
    (path-mtu-discovery | no-path-mtu-discovery);
    source-port upper-limit <upper-limit>;
    (source-quench | no-source-quench);
    tcp-drop-synfin-set;
  }
  location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
  }
  login {
```

```
    announcement text;
    class class-name {
        access-end;
        access-start;
        allow-commands "regular-expression";
        allow-configuration-regexps "regular expression 1" "regular expression 2";
        allowed-days;
        deny-commands "regular-expression";
        deny-configuration-regexps "regular expression 1" "regular expression 2";
        idle-timeout minutes;
        login-tip;
        permissions [ permissions ];
    }
    message text;
    password {
        change-type (set-transitions | character-set);
        format (md5 | sha1 | des);
        maximum-length length;
        minimum-changes number;
        minimum-length length;
    }
    retry-options {
        backoff-threshold number;
        backoff-factor seconds;
        minimum-time seconds;
        tries-before-disconnect number;
    }
    user username {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication {
            (encrypted-password "password" | plain-text-password);
            ssh-rsa "public-key";
            ssh-dsa "public-key";
        }
    }
}
login-tip number;
mirror-flash-on-disk;
name-server {
    address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
    authentication-key key-number type type value password;
    boot-server address;
    broadcast <address> <key key-number> <version value> <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 {
    password-protocol mschap-v2;
    }
    attributes {
        nas-ip-address ip-address;
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;
    }
    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";
    structured-data {
      brief;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
      brief;
    }
  }
  source-address source-address;
```

```
    time-format (year | millisecond | year millisecond);
    user (username | *) {
      facility severity;
      match "regular-expression";
    }
  }
  tacplus-options {
    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;
}
```

## authentication-key

**Syntax** authentication-key *key-number* type *type* value *password*;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Configure Network Time Protocol (NTP) authentication keys so that the router or switch can send authenticated packets. If you configure the router or switch to operate in authenticated mode, you must configure a key.

Both the keys and the authentication scheme (MD5) must be identical between a set of peers sharing the same key number.

**Options** ***key-number***—Positive integer that identifies the key.

**type *type***—Authentication type. It can only be **md5**.

**value *password***—The key itself, which can be from 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.

**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 on page 12
- broadcast on page 26
- peer on page 29
- server on page 30
- trusted-key

## boot-server (NTP)

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

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Configure the 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 will not be able to synchronize to a time server if the server's time appears to be very far off of the local router's or switch's time. You can either configure an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the **ntpdate** request resolves the hostname to an IP address when the router or switch boots up.

**Options**

- ***address***—The IP address of an NTP boot server.
- ***hostname***—The hostname of an NTP boot server.

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

**Related Documentation**

- Configuring the NTP Boot Server on page 8

## broadcast

**Syntax** broadcast *address* <key *key-number*> <version *value*> <ttl *value*>;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Configure the local router or switch to operate in broadcast mode with the remote system at the specified ***address***. In this mode, the local router or switch sends periodic broadcast messages to a client population at the specified broadcast or multicast ***address***. Normally, you include this statement only when the local router or switch is operating as a transmitter.

**Options**

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

**key *key-number***—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.

**Range:** 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**

- Configuring the NTP Time Server and Time Services on page 9

 

## broadcast-client

**Syntax** broadcast-client;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Configure the local router or switch to listen for broadcast messages on the local network to discover other servers on the same subnet.

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

**Related Documentation**
- Configuring the Router or Switch to Listen for Broadcast Messages Using NTP on page 13

## multicast-client

**Syntax** multicast-client <*address*>;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** For NTP, configure the local router or switch to listen for multicast messages on the local network to discover other servers on the same subnet.

**Options** ***address***—(Optional) One or more IP addresses. If you specify addresses, the router or switch joins those multicast groups.

**Default:** 224.0.1.1.

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

**Related Documentation**
- Configuring the Router or Switch to Listen for Multicast Messages Using NTP on page 13

## ntp

**Syntax**

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

**Hierarchy Level** [edit system]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Configure NTP on the router or switch.

The remaining statements are explained separately.

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

**Related Documentation**

- Synchronizing and Coordinating Time Distribution Using NTP on page 8

 

## peer

**Syntax** peer *address* <key *key-number*> <version *value*> <prefer>;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** For NTP, configure the local router or switch to operate in symmetric active mode with the remote system at the specified address. In this mode, the local router or switch and the remote system can synchronize with each other. This configuration is useful in a network in which either the local router or switch or the remote system might be a better source of time.

**Options** ***address***—Address of the remote system. You must specify an address, not a hostname.

**key *key-number***—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.

**Range:** Any unsigned 32-bit integer

**prefer**—(Optional) Mark the remote system as the preferred host, which means that if all other factors are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

**version *value***—(Optional) Specify the NTP 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**

- Configuring the NTP Time Server and Time Services on page 9

## server (NTP)

**Syntax** server *address* <key *key-number*> <version *value*> <prefer>;

**Hierarchy Level** [edit system ntp]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** For NTP, configure the local router or switch to operate in client mode with the remote system at the specified ***address***. In this mode, the local router or switch can be synchronized with the remote system, but the remote system can never be synchronized with the local router or switch.

**Options** ***address***—Address of the remote system. You must specify an address, not a hostname.

key ***key-number***—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address.

**Range:** Any unsigned 32-bit integer

**prefer**—(Optional) Mark the remote system as preferred host, which means that if all other things are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

**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**

- Configuring the NTP Time Server and Time Services on page 9

 

## 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 before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**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***—A valid IP address configured on one of the router or switch interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all **host *hostname*** statements at the **[edit system syslog]** hierarchy level, but not for messages directed to the other Routing Engine or to the TX Matrix router or TX Matrix Plus router in a routing matrix based on a TX Matrix router or TX Matrix Plus router.

**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
- Specifying a Source Address for an NTP Server on page 8
- Specifying an Alternative Source Address for System Log Messages

## system

**Syntax** system { ... }

**Hierarchy Level** [edit]

**Release Information** Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description** Configure system management properties.

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

**Related Documentation**

- System Management Configuration Statements on page 17

## 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/Calcutta, 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/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 7
- System Management Configuration Statements on page 17

## 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**

- Setting a Custom Time Zone on Routers or Switches Running Junos OS on page 14

PART 3

# Administration

 

CHAPTER 4

# Monitoring Commands

## 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.

**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 40

**List of Sample Output** show ntp associations on page 39

**Output Fields** Table 1 on page 38 describes the output fields for the **show ntp associations** command. Output fields are listed in the approximate order in which they appear.

### Table 1: 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. |
| **offset** | Current estimated offset of the peer, in milliseconds. |
| **disp** | Current estimated dispersion of the peer, in milliseconds. |

Table 1: show ntp associations Output Fields *(continued)*

| Field Name | Field Description |
|---|---|
| *peer-name* | Peer name and status of the peer in the clock selection process:<br>• space—Discarded because of a high stratum value or failed sanity checks.<br>• x—Designated "falseticker" by the intersection algorithm.<br>• .—Culled from the end of the candidate list.<br>• – —Discarded by the clustering algorithm.<br>• +—Included in the final selection set.<br>• #—Selected for synchronization, but the distance exceeds the maximum.<br>• *—Selected for synchronization.<br>• 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
==============================================================================
*wolfe-gw.junipe tick.ucla.edu    2 u   43   64  377     1.86    0.319    0.08
```

## show ntp status

**Syntax**
show ntp status
<no-resolve>

**Release Information**
Command introduced in Junos OS Release 11.1 for the QFX 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 38

**List of Sample Output**
show ntp status on page 40

### Sample Output

**show ntp status**

```
user@host> show ntp status
status=0644 leap_none, sync_ntp, 4 events, event_peer/strat_chg,
version="ntpd 4.1.0-a Fri Jun 24 06:40:56 GMT 2005 (1)",
processor="i386", system="JUNOS7.4-20050624.0", leap=00, stratum=2,
precision=-28, rootdelay=6.849, rootdispersion=10.615, peer=38788,
refid=ntp-server.company-a.net,
reftime=c66705d9.06ee0f3c  Fri, Jun 24 2005 15:21:13.027, poll=6,
clock=c6670602.cf6db940  Fri, Jun 24 2005 15:21:54.810, state=4,
offset=0.205, frequency=75.911, jitter=0.396, stability=0.005
```

PART 4

# Index

# Index