

# Chapter 24

## Summary of System Management Configuration Statements

The following sections explain each of the system management configuration statements. The statements are organized alphabetically.

### allow-commands

<b>Syntax</b>	<code>allow-commands "regular-expression";</code>
<b>Hierarchy Level</b>	[edit system login class]
<b>Description</b>	Specify the commands that members of a login class can use.
<b>Default</b>	If you omit this statement and the <code>deny-commands</code> statement, users can issue only those commands for which they have access privileges through the <code>permissions</code> statement.
<b>Options</b>	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If it contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
<b>Usage Guidelines</b>	See “Deny or Allow Individual Commands” on page 208.
<b>Required Privilege Level</b>	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
<b>See Also</b>	<code>deny-commands</code> on page 236, <code>user</code> on page 258

## authentication

<b>Syntax</b>	authentication { (encrypted-password " <i>password</i> "   plain-text-password); ssh-rsa " <i>public-key</i> "; }
<b>Hierarchy Level</b>	[edit system login user]
<b>Description</b>	Authentication methods that a user can use to log into the router. You can assign multiple authentication methods to a single user.
<b>Options</b>	<p>encrypted-password "<i>password</i>"—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.</p> <p>plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password for each user.</p> <p>ssh-rsa <i>public-key</i>—Secure shell (SSH) authentication. Specify the SSH public key. You can specify one or more public keys for each user.</p>
<b>Usage Guidelines</b>	See "Configure User Accounts" on page 210.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	root-authentication on page 248

## authentication-key

<b>Syntax</b>	authentication-key <i>key-number</i> type <i>type</i> value password;
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	<p>Configure NTP authentication keys so that the router can send authenticated packets. If you configure the router to operate in authenticated mode, you must configure a key.</p> <p>Both the keys and the authentication schemes (DES or MD5) must be identical between a set of peers sharing the same key number.</p>
<b>Options</b>	<p><i>key-number</i>—Positive integer that identifies the key.</p> <p><i>type</i>—Authentication type. It can be either md5 or des.</p> <p><i>password</i>—The key itself, which can be 1 to 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.</p>
<b>Usage Guidelines</b>	See "Configure NTP Authentication Keys" on page 217.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	broadcast on page 233, peer on page 244, server on page 249, trusted-key on page 257

## authentication-order

<b>Syntax</b>	authentication-order [ <i>authentication-methods</i> ];
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the order in which the software tries different user-authentication methods when attempted to authentication a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.
<b>Default</b>	If you do not include the authentication-order statement, users are verified based on their configured password.
<b>Options</b>	<p><i>authentication-methods</i>—One or more authentication methods, listed in the order in which they should be tried. It can be one or more of the following:</p> <p>password—Verify the user using the password configured for the user with the authentication statement at the [edit system login user] hierarchy level.</p> <p>radius—Verify the user using RADIUS authentication services.</p> <p>tacplus—Verify the user using TACACS+ authentication services.</p>
<b>Usage Guidelines</b>	See “Configure the Authentication Order” on page 202.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## auxiliary

**Syntax** auxiliary {  
     insecure;  
     speed *baud-rate*;  
     type *terminal-type*;  
 }

**Hierarchy Level** [edit system ports]

**Description** Configure the characteristics of the auxiliary port, which is on the router's craft interface.

**Default** The auxiliary port is disabled.

**Options** insecure—The terminal connection is not secure enough to allow you to enter the superuser password.

**Default:** The connection is secure. It is safe to enter the root password.

speed *baud-rate*—Baud rate of the port. If you change the speed on the auxiliary port, any user currently logged in through this port is logged off the system.

**Values:** 9600, 19200, 38400, 57600, 115200

**Default:** 9600 baud

type *terminal-type*—Type of terminal that is connected to the port.

**Values:** ansi, vt100, small-xterm, xterm

**Default:** The terminal type is unknown, and the user is prompted for the terminal type.

**Usage Guidelines** See "Configure Console and Auxiliary Port Properties" on page 225.

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

## backup-router

**Syntax** backup-router *address* <destination *destination-address*>;

**Hierarchy Level** [edit system]

**Description** Set a default router to use while the local router is booting and if the routing protocol processes fail to start. The JUNOS software removes the route to this router as soon as the software starts.

**Options** *address*—Address of the default router.

*destination destination-address*—(Optional) Destination address that is reachable through the backup router. Include this option to achieve network reachability while loading, configuring, and recovering the router, but without the risk of installing a default route in the forwarding table.

**Default:** All hosts (default route) are reachable through the backup router.

**Usage Guidelines** See "Configure a Backup Router" on page 194.

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

## boot-server

<b>Syntax</b>	boot-server <i>address</i> ;
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	Configure the server that NTP queries when the router boots to determine the local date and time.  When you boot the router, it issues an <code>ntpdate</code> request, which polls a network server to determine the local date and time. You need to configure a server that the router uses to determine the time when the router 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 time.
<b>Options</b>	<i>address</i> —Address of an NTP server. You must specify an address, not a hostname.
<b>Usage Guidelines</b>	See “Configure the NTP Boot Server” on page 215.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## broadcast

<b>Syntax</b>	broadcast <i>address</i> <key <i>key-number</i> <version <i>value</i> > <tll <i>value</i> > ;
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	Configure the local router to operate in broadcast mode with the remote system at the specified <i>address</i> . In this mode, the local router sends periodic broadcast messages to a client population at the specified broadcast or multicast <i>address</i> . Normally, you include this statement only when the local router is operating as a transmitter.
<b>Options</b>	<i>address</i> —Address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. Currently, the multicast address must be 224.0.1.1.  <i>key key-number</i> —(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number. <b>Values:</b> Any unsigned 32-bit integer  <i>tll value</i> —(Optional) Time-to-live (TTL) value to use. <b>Range:</b> 1 through 255 <b>Default:</b> 1  <i>version value</i> —(Optional) Specify the version number to be used in outgoing NTP packets. <b>Values:</b> 1, 2, 3 <b>Default:</b> 3
<b>Usage Guidelines</b>	See “Configure the NTP Time Server and Time Services” on page 215.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## • broadcast-client

<b>Syntax</b>	broadcast-client;
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	Configure the local router to listen for broadcast messages on the local network to discover other servers on the same subnet.
<b>Usage Guidelines</b>	See “Configure the Router to Listen for Broadcast Messages” on page 217.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## • class

<b>Syntax</b>	class <i>class-name</i> { allow-commands " <i>regular-expression</i> "; deny-commands " <i>regular-expression</i> "; idle-timeout <i>minutes</i> ; permissions [ <i>permissions</i> ]; }
<b>Hierarchy Level</b>	[edit system login]
<b>Description</b>	Define login classes.
<b>Options</b>	<i>class-name</i> —A name you choose for the login class.  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Define Login Classes” on page 205.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	user on page 258
<b>Syntax</b>	class <i>class-name</i> ;
<b>Hierarchy Level</b>	[edit system login user]
<b>Description</b>	Configure a user’s login class. You must configure one class for each user.
<b>Options</b>	<i>class-name</i> —One of the classes defined at the [edit system login class] hierarchy level.
<b>Usage Guidelines</b>	See “Configure User Accounts” on page 210.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

## compress-configuration-files

<b>Syntax</b>	compress-configuration-files;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Compress the current operational configuration file. By default, the current operational configuration file is uncompressed, and is stored in the file <code>juniper.conf</code> , in the <code>/config</code> file system, along with the last three committed versions of the configuration. However, with large networks, the current configuration file might exceed the available space in the <code>/config</code> file system. Compressing the current configuration file allows the file to fit in the file system, typically reducing the size of the file by 90 percent. The current configuration file is compressed on the second commit of the configuration after the first commit is made to include the <code>compress-configuration-files</code> statement.
<b>Default</b>	The current operational configuration file is uncompressed.
<b>Usage Guidelines</b>	See “Compress the Current Configuration File” on page 197.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## console

<b>Syntax</b>	<pre>console {   insecure;   speed <i>baud-rate</i>;   type <i>terminal-type</i>; }</pre>
<b>Hierarchy Level</b>	[edit system ports]
<b>Description</b>	Configure the characteristics of the console port, which is on the router's craft interface.
<b>Default</b>	The console port is enabled, and its speed is set to 9600 baud.
<b>Options</b>	<p><b>insecure</b>—The terminal connection is not secure enough to allow you to enter the superuser password. <b>Default:</b> The connection is secure. That is, it is safe to enter the root password.</p> <p><b>speed <i>baud-rate</i></b>—Baud rate of the port. If you change the speed on the auxiliary port, any user currently logged in through this port is forced off the system. <b>Values:</b> 9600, 19200, 38400, 57600, 115200 <b>Default:</b> 9600 baud</p> <p><b>type <i>terminal-type</i></b>—Type of terminal that is connected to the port. <b>Values:</b> ansi, vt100, small-xterm, xterm <b>Default:</b> The terminal type is unknown, and the user is prompted for the terminal type.</p>
<b>Usage Guidelines</b>	See “Configure Console and Auxiliary Port Properties” on page 225.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## default-address-selection

<b>Syntax</b>	default-address-selection;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Use the loopback interface, lo0, as the source address for all locally generated IP packets. The lo0 interface is the interface to the router's Routing Engine.
<b>Default</b>	The outgoing interface is used as the source address.
<b>Usage Guidelines</b>	See "Configure the Source Address for Locally Generated TCP/IP Packets" on page 226 and the <i>JUNOS Internet Software Configuration Guide: Interfaces and Chassis</i> .
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## deny-commands

<b>Syntax</b>	deny-commands " <i>regular-expression</i> ";
<b>Hierarchy Level</b>	[edit system login class]
<b>Description</b>	Specify the commands the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.
<b>Default</b>	If you omit this statement and the allow-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.
<b>Options</b>	<i>regular-expression</i> —Extended (modern) regular expression as defined in POSIX 1003.2. If it contains any spaces, operators, or wildcard characters, enclose it in quotation marks.
<b>Usage Guidelines</b>	See "Deny or Allow Individual Commands" on page 208.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	allow-commands on page 229, user on page 258

## dhcp-relay

<b>Syntax</b>	dhcp-relay (server <i>address</i>   disable);
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure a DHCP relay agent.
<b>Default</b>	DHCP relaying is disabled.
<b>Options</b>	disable—Disable DHCP relaying.  server <i>address</i> —Address of the DHCP or BOOTP server.  <b>Default:</b> disable
<b>Usage Guidelines</b>	See "Configure the Router to Act As a DHCP Relay Agent" on page 227.

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

## diag-port-authentication

**Syntax** diag-port-authentication (encrypted-password "*password*" | plain-text-password);

**Hierarchy Level** [edit system]

**Description** Configure a password for performing diagnostics on the router's SCB, SSB, SFM, or FEB port.

For routers that have more than one SSB, the same password is used for both SSBs.



**Note**

Do not run diagnostics on the SCB, SSB, SFM, or FEB unless you have been instructed to do so by Customer Support personnel.

**Default** No password is configured on the diagnostics port.

**Options** encrypted-password "*password*"—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.

plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password for each user.

**Usage Guidelines** See "Configure a Password on the Diagnostics Port" on page 228.

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

## domain-name

**Syntax** domain-name *domain-name*;

**Hierarchy Level** [edit system]

**Description** Configure the name of the domain in which the router is located. This is the default domain name that is appended to host names that are not fully qualified.

**Options** *domain-name*—Name of the domain.

**Usage Guidelines** See "Configure the Router's Domain Name" on page 193.

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

## domain-search

<b>Syntax</b>	domain-search [ <i>domain-list</i> ];
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure a list of domains to be searched.
<b>Options</b>	<i>domain-list</i> —A list of domain names to search. The list can contain up to six domain names, with a total of up to 256 characters.
<b>Usage Guidelines</b>	See “Configure Which Domains to Search” on page 194.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## full-name

<b>Syntax</b>	full-name <i>complete-name</i> ;
<b>Hierarchy Level</b>	[edit system login user]
<b>Description</b>	Configure the complete name of a user.
<b>Options</b>	<i>complete-name</i> —Full name of the user. If the name contains spaces, enclose it in quotation marks.
<b>Usage Guidelines</b>	See “Configure User Accounts” on page 210.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

## host-name

<b>Syntax</b>	host-name <i>host-name</i> ;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Set the host name of the router.
<b>Options</b>	<i>host-name</i> —Name of the router.
<b>Usage Guidelines</b>	See “Configure the Router’s Name and Addresses” on page 191.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## idle-timeout

<b>Syntax</b>	idle-timeout <i>minutes</i> ;
<b>Hierarchy Level</b>	[edit system login class]
<b>Description</b>	For a login class, configure the maximum time that a session can be idle before the user is logged off the router. The session times out after remaining at the CLI operational mode prompt for the specified time.
<b>Default</b>	If you omit this statement, a user is never forced off the system after extended idle times.
<b>Options</b>	<i>minutes</i> —Maximum idle time. <b>Range:</b> 0 through 100,000 minutes
<b>Usage Guidelines</b>	See “Configure the Timeout Value for Idle Login Sessions” on page 210.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>See Also</b>	user on page 258

## location

**Syntax** location {  
 altitude *feet*;  
 country-code *code*;  
 hcoord *horizontal-coordinate*;  
 lata *service-area*;  
 latitude *degrees*;  
 longitude *degrees*;  
 npa-nxx *number*;  
 postal-code *postal-code*;  
 vcoord *vertical-coordinate*;  
 }

**Hierarchy Level** [edit system]

**Description** Configure the system location in various formats.

**Options** altitude *feet*—Number of feet above sea level.  
 country-code *code*—Two-letter country code.  
 hcoord *horizontal-coordinate*—Bellcore Horizontal Coordinate.  
 lata *service-area*—Long distance service area.  
 latitude *degrees*—Latitude in degree format.  
 longitude *degrees*—Longitude in degree format.  
 npa-nxx *number*—First six digits of the phone number (area code and exchange).  
 postal-code *postal-code*—Postal code.  
 vcoord *vertical-coordinate*—Bellcore Vertical Coordinate.

**Usage Guidelines** See “Configure the System Location” on page 195.

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

## login

```

Syntax login {
    message text;
    class class-name {
        allow-commands [ addresses ];
        deny-commands [ addresses ];
        idle-timeout minutes;
        permissions [ permissions ];
    }
    user user-name {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication authentication;
            (encrypted-password "password" | plain-text-password);
            ssh-rsa "public-key";
        }
    }
}

```

**Hierarchy Level** [edit system]

**Description** Configure user access to the router.

**Options** The statements are explained separately.

**Usage Guidelines** See "Configure User Access" on page 205.

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

## message

**Syntax** message *text*;

**Hierarchy Level** [edit system login]

**Description** Configure a system login message.

**Options** *text*—Text of the message.

**Usage Guidelines** See "Configure a System Login Message" on page 227.

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

## multicast-client

- Syntax** multicast-client <*address*>;
- Hierarchy Level** [edit system ntp]
- Description** For NTP, configure the local router 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 route joins those multicast groups.  
**Default:** 224.0.1.1.
- Usage Guidelines** See “Configure the Router to Listen for Multicast Messages” on page 218.
- Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

## name-server

- Syntax** name-server {  
    *address*;  
}
- Hierarchy Level** [edit system]
- Description** Configure one or more DNS name servers.
- Options** *address*—Address of the name server. To configure multiple name servers, include multiple *address* options.
- Usage Guidelines** See “Configure a DNS Name Server” on page 194.
- Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

## no-redirects

<b>Syntax</b>	no-redirects;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Disable the sending of protocol redirect messages by the router.  To disable the sending of redirect messages on a per-interface basis, include the no-redirects statement at the [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> ] hierarchy level.
<b>Default</b>	The router sends redirect messages.
<b>Usage Guidelines</b>	See “Disable the Sending of Redirect Messages on the Router” on page 226.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	The no-redirects statement in the <i>JUNOS Internet Software Configuration Guide: Interfaces and Chassis</i> .

## ntp

<b>Syntax</b>	ntp { authentication-key <i>number</i> type <i>type</i> value <i>password</i> ; boot-server <i>address</i> ; broadcast < <i>address</i> > <key <i>key-number</i> > <version <i>value</i> > <tll <i>value</i> >; broadcast-client; multicast-client < <i>address</i> >; peer <i>address</i> <key <i>key-number</i> > <version <i>value</i> > <prefer>; server <i>address</i> <key <i>key-number</i> > <version <i>value</i> > <prefer>; trusted-key [ <i>key-numbers</i> ]; }
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the Network Time Protocol (NTP) on the router.
<b>Options</b>	The statements are explained separately.
<b>Usage Guidelines</b>	See “Configure the Network Time Protocol” on page 214.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## peer

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

**Hierarchy Level** [edit system ntp]

**Description** For NTP, configure the local router to operate in symmetric active mode with the remote system at the specified *address*. In this mode, the local router and the remote system can synchronize each other. This configuration is useful in a network in which either the local router 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.  
**Values:** Any unsigned 32-bit integer

*prefer*—(Optional) Mark the remote system as being the 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 NTP version number to be used in outgoing NTP packets.  
**Values:** 1, 2, 3  
**Default:** 3

**Usage Guidelines** See “Configure the NTP Time Server and Time Services” on page 215.

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

## permissions

**Syntax** permissions [ *permissions* ];

**Hierarchy Level** [edit system login class]

**Description** Configure the login access privileges to be provided on the router.

**Options** *permissions*—Privilege type. For a list of types, see Table 7 on page 206.

**Usage Guidelines** See “Configure Access Privilege Levels” on page 206.

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

**See Also** user on page 258

## port

<b>Syntax</b>	port <i>number</i> ;
<b>Hierarchy Level</b>	[edit system radius-server <i>address</i> ]
<b>Description</b>	Configure the port number on which to contact the RADIUS server.
<b>Options</b>	<i>number</i> —Port number on which to contact the RADIUS server. <b>Default:</b> 1812 (as specified in RFC 2138)
<b>Usage Guidelines</b>	See “Configure RADIUS Authentication” on page 199.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## ports

<b>Syntax</b>	ports { auxiliary { insecure; speed <i>baud-rate</i> ; type <i>terminal-type</i> ; } console { insecure; speed <i>baud-rate</i> ; type <i>terminal-type</i> ; } }
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the properties of the console and auxiliary ports, which are located on the router's craft interface.
<b>Options</b>	The statements are explained separately.
<b>Usage Guidelines</b>	See “Configure Console and Auxiliary Port Properties” on page 225.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## processes

**Syntax** processes {  
 inet-process (enable | disable);  
 interface-control (enable | disable);  
 mib-process (enable | disable);  
 ntp (enable | disable);  
 routing (enable | disable);  
 snmp (enable | disable);  
 watchdog (enable | disable) <timeout *seconds*>;  
 }

**Hierarchy Level** [edit system]

**Description** Configure which JUNOS software processes are running on the router.

**Default** All processes are enabled by default.

**Note**

Never disable any of the software processes unless instructed to do so by a customer support engineer.

**Options** timeout *seconds*—(Optional) How often the system checks the watchdog timer, in seconds. If the watchdog timer has not been checked in the specified number of seconds, the system reloads. If you set the time value too low, it is possible for the system to reboot immediately after it loads.

**Values:** 15, 60, 180

**Default:** 180 seconds (rounded up to 291 seconds by the JUNOS kernel)

**Usage Guidelines** See “Configure JUNOS Software Processes” on page 228.

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

## radius-server

<b>Syntax</b>	radius-server <i>server-address</i> { port <i>number</i> ; retry <i>number</i> ; secret <i>password</i> ; timeout <i>seconds</i> ; }
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the Remote Authentication Dial-In User Service (RADIUS).  To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.
<b>Options</b>	<i>server-address</i> —Address of the RADIUS authentication server.  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configure RADIUS Authentication” on page 199.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

## retry

<b>Syntax</b>	retry <i>number</i> ;
<b>Hierarchy Level</b>	[edit system radius-server <i>server-address</i> ]
<b>Description</b>	Number of times that the router attempts to contact a RADIUS authentication server.
<b>Options</b>	<i>number</i> —Number of times to retry contacting a RADIUS server. <b>Range:</b> 1 through 10 <b>Default:</b> 3
<b>Usage Guidelines</b>	See “Configure RADIUS Authentication” on page 199.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	timeout on page 254

## root-authentication

<b>Syntax</b>	root-authentication { (encrypted-password " <i>password</i> "   plain-text-password); ssh-rsa " <i>public-key</i> "; }
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Configure the authentication methods for the root-level user, whose username is "root."
<b>Options</b>	<p>encrypted-password "<i>password</i>"—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.</p> <p>plain-text-password—Use a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password.</p> <p>ssh-rsa <i>public-key</i>—Secure shell (SSH) authentication. Specify the SSH public key. You can specify one or more public keys.</p>
<b>Usage Guidelines</b>	See "Configure the Root Password" on page 196.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>See Also</b>	authentication on page 230

## secret

<b>Syntax</b>	secret <i>password</i> ;
<b>Hierarchy Level</b>	[edit system radius-server <i>server-address</i> ], [edit system tacplus-server <i>server-address</i> ]
<b>Description</b>	Configure the password to use with the RADIUS or TACACS+ server. The secret used by the local router must match that used by the server.
<b>Options</b>	<i>password</i> —Password to use. Can include spaces.
<b>Usage Guidelines</b>	See "Configure RADIUS Authentication" on page 199 and "Configure TACACS+ Authentication" on page 201.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## server

<b>Syntax</b>	server <i>address</i> <key <i>key-number</i> > <version <i>value</i> > <prefer>;
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	For NTP, configure the local router to operate in client mode with the remote system at the specified <i>address</i> . In this mode, the local router can be synchronized to the remote system, but the remote system never can be synchronized to the local router.
<b>Options</b>	<p><i>address</i>—Address of the remote system. You must specify an address, not a hostname.</p> <p>key <i>key-number</i>—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.  <b>Values:</b> Any unsigned 32-bit integer</p> <p>prefer—(Optional) Mark the remote system as being preferred host, which means that, if all other things are equal, this remote system is chosen for synchronization among a set of correctly operating systems.</p> <p>version <i>value</i>—(Optional) Specify the version number to be used in outgoing NTP packets.  <b>Values:</b> 1, 2, 3  <b>Default:</b> 3</p>
<b>Usage Guidelines</b>	See “Configure the NTP Time Server and Time Services” on page 215.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## services

**Syntax** services {  
 finger <connection-limit *limit*> <rate-limit *limit*>;  
 ssh <connection-limit *limit*> <rate-limit *limit*>;  
 telnet <connection-limit *limit*> <rate-limit *limit*>;  
 }

**Hierarchy Level** [edit system]

**Description** Configure the router so that users on remote systems can access the local router using the SSH, Telnet, FTP, and finger network utilities.

**Options** connection-limit *limit*—(Optional) Maximum number of established connections.

**Range:** 1 through 250

**Default:** 75

rate-limit *limit*—(Optional) Maximum number of connection attempts allowed per minute.

**Range:** 1 through 250

**Default:** 150

finger—Allow finger requests from remote systems to the local router.

ssh—Allow SSH access from remote systems to the local router.

telnet—Allow Telnet login from remote systems to the local router.

**Usage Guidelines** See “Configure System Services” on page 227.

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

## single-connection

**Syntax** single-connection;

**Hierarchy Level** [edit system tacplus-server server-address]

**Description** Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt.

**Usage Guidelines** See “Configure TACACS+ Authentication” on page 201.

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

## static-host-mapping

<b>Syntax</b>	static-host-mapping { <i>host-name</i> { inet [ <i>address</i> ]; sysid <i>system-identifier</i> ; alias [ <i>alias</i> ]; } }
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Map a host name to one or more IP addresses and aliases, and configure an ISO system identifier (sysid).
<b>Options</b>	<p>alias <i>alias</i>—(Optional) Alias for the host name.</p> <p><i>host-name</i>—Fully qualified host name.</p> <p>inet <i>address</i>—IP address. You can specify one or more IP addresses for the host.</p> <p>sysid <i>system-identifier</i>—ISO system identifier (sysid). It is the 6-byte sysid portion of the IS-IS NSAP. We recommend that you use the host's IP address represented in binary-coded decimal (BCD). For example, the IP address 208.197.169.18 would be 2081.9716.9018 in BCD.</p>
<b>Usage Guidelines</b>	See "Configure the Router's Name and Addresses" on page 191.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

## syslog

```

Syntax  syslog {
            file filename {
                facility level;
                archive {
                    files number;
                    size size;
                    (world-readable | no-world-readable);
                }
            }
            host hostname {
                facility level;
                facility-override facility;
                log-prefix string;
            }
            user (username | *) {
                facility level;
            }
            console {
                facility level;
            }
            archive {
                files number;
                size size;
                (world-readable | no-world-readable);
            }
        }

```

**Hierarchy Level** [edit system]

**Description** Configure the types of syslog messages to log to files, remote host, user terminals, and the system console.

**Options** archive—Configure how to archive system logging files.

console—Configure the types of syslog messages to log to the system console.

*facility*—Class of log messages. To specify multiple classes, include multiple *facility level* options. It can be one of the facilities listed in Table 10 on page 220.

facility-override *facility*—When sending files to a remote host, override the facility.

file *filename*—Configure the types of syslog messages to log to the specified file. To log messages to more than one file, include more than one file option.

files *number*—Maximum number of system log files. When a log file named *syslog-file* reaches its maximum size, it is renamed as *syslog-file.0*, then as *syslog-file.1*, and so on, until the maximum number of log files is reached. Then, the oldest log file is overwritten.

**Range:** 1 through 1000

**Default:** 10 files

host *hostname*—Configure the types of syslog messages to log to the specified remote host. Specify the IP address or the fully qualified domain name of the host. To log messages to more than one host, include more than one host option.

- level*—Priority of the message. It can be one or more of the priorities listed in Table 11 on page 220.
- log-prefix *string*—When sending log messages to a remote host, prepend a string to the log message.
- no-world-readable—System logging files can be read only by a limited group of users. This is the default.
- size *size*—Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a system log file named *syslog-file* reaches this size, it is renamed as *syslog-file.0*. When the *syslog-file* again reaches its maximum size, *syslog-file.0* is renamed as *syslog-file.1* and *syslog-file* is renamed as *syslog-file.0*. This renaming scheme continues until the maximum number of log files is reached. Then, the oldest log file is overwritten.  
**Syntax:** *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB  
**Range:** 64 KB through 1 GB
- user (*username* | \*)—Configure the types of syslog messages to log to the specified user's terminal session. To log messages to more than one user, include more than one user option. To log messages to the terminal sessions of all users who are currently logged in, specify an asterisk instead of a *username*.
- world-readable—System logging files can be read by anyone.  
**Default:** no-world-readable

**Usage Guidelines** See “Configure System Logging” on page 219.

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

**See Also** The options statement in the *JUNOS Internet Software Configuration Guide: Routing and Routing Protocols*.

## system

**Syntax** system { ... }

**Hierarchy Level** [edit]

**Description** Configure system management properties.

**Usage Guidelines** See “System Management Configuration Statements” on page 187.

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

## • tacplus-server

• **Syntax** tacplus-server *server-address* {  
 •     secret *password*;  
 •     single-connection;  
 •     timeout *seconds*;  
 •     }

• **Description** Configure the Terminal Access Controller Access Control System Plus (TACACS+ ).

• **Hierarchy Level** [edit system]

• **Options** *server-address*—Address of the TACACS+ authentication server.

• The remaining statements are explained separately.

• **Usage Guidelines** See “Configure TACACS+ Authentication” on page 201.

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

## • timeout

• **Syntax** timeout *seconds*;

• **Hierarchy Level** [edit system radius-server *server-address*],  
 • [edit system tacplus-server *server-address*]

• **Description** Configure the amount of time that the local router waits to receive a response from a RADIUS or TACACS+ server.

• **Options** *seconds*—Amount of time to wait.  
 •     **Range:** 1 through 90  
 •     **Default:** 3 seconds

• **Usage Guidelines** See “Configure RADIUS Authentication” on page 199 and “Configure TACACS+ Authentication” on page 201.

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

• **See Also** retry on page 247

## time-zone

<b>Syntax</b>	time-zone <i>time-zone</i> ;
<b>Hierarchy Level</b>	[edit system]
<b>Description</b>	Set the local time zone.
<b>Default</b>	UTC
<b>Options</b>	<p><i>time-zone</i>—Time zone. To have the time zone change take effect for all processes running on the router, you must reboot the router. Specify the time zone either as UTC, which is the default time zone, or use one of the following continent/country/zone primary names:</p> <p>Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek</p> <p>America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Aruba, America/Asuncion, America/Barbados, America/Belize, America/Bogota, America/Boise, America/Buenos_Aires, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Cordoba, America/Costa_Rica, America/Cuiaba, America/Curacao, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/EL_Salvador, America/Ensenada, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Vevay, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Maceio, America/Managua, America/Manaus, America/Martinique, America/Mazatlan, America/Mendoza, America/Menominee, America/Mexico_City, America/Miquelon, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, 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</p> <p>Antarctica/Casey, Antarctica/DumontD'Urville, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/South_Pole</p> <p>Arctic/Longyearbyen</p> <p>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,</p>

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/Fakaofu, 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

**Usage Guidelines** See "Set the Time Zone" on page 213.

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

## trusted-key

<b>Syntax</b>	trusted-key [ <i>key-numbers</i> ];
<b>Hierarchy Level</b>	[edit system ntp]
<b>Description</b>	For NTP, configure the keys you are allowed to use when you configure the local router to synchronize its time with other systems on the network.
<b>Options</b>	<i>key-numbers</i> —One or more key numbers. Each key can be any 32-bit unsigned integer except 0.
<b>Usage Guidelines</b>	See “Configure NTP Authentication Keys” on page 217.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>See Also</b>	authentication-key on page 230, broadcast on page 233, peer on page 244, server on page 249

## uid

<b>Syntax</b>	uid <i>uid-value</i> ;
<b>Hierarchy Level</b>	[edit system login user]
<b>Description</b>	Configure user identifier for a login account.
<b>Options</b>	<i>uid-value</i> —Number associated with the login account. This value must be unique on the router. <b>Range:</b> 100 through 64000
<b>Usage Guidelines</b>	See “Configure User Accounts” on page 210.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

- user

- **Syntax**

```
user user-name {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication {
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
    }
}
```

- **Hierarchy Level** [edit login]

- **Description** Configure access permission for individual users.

- **Options** The statements are explained separately.

- **Usage Guidelines** See “Configure User Accounts” on page 210.

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

- **See Also** class on page 234