

Chapter 25

Summary of System Management Configuration Statements

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

allow-commands

Syntax	<code>allow-commands "regular-expression";</code>
Hierarchy Level	[edit system login class]
Description	Specify the operational mode commands that members of a login class can use.
Default	If you omit this statement and the deny-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.
Options	<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.
Usage Guidelines	See “Deny or Allow Individual Commands” on page 246.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	deny-commands on page 280, user on page 305

authentication

Syntax authentication {
 (encrypted-password "*password*" | plain-text-password);
 ssh-rsa "*public-key*";
 ssh-dsa "*public-key*";
 }

Hierarchy Level [edit system login user]

Description Authentication methods that a user can use to log into the router. You can assign multiple authentication methods to a single user.

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.

ssh-rsa "*public-key*"—Secure shell (ssh version 1) authentication. Specify the ssh public key. You can specify one or more public keys for each user.

ssh-dsa "*public-key*"—Secure shell (ssh version 2) authentication. Specify the ssh public key. You can specify one or more public keys for each user.

Usage Guidelines See "Configure User Accounts" on page 249.

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

See Also root-authentication on page 294

authentication-key

Syntax	authentication-key <i>key-number</i> type <i>type</i> value <i>password</i> ;
Hierarchy Level	[edit system ntp]
Description	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. Both the keys and the authentication schemes (DES or MD5) must be identical between a set of peers sharing the same key number.
Options	<i>key-number</i> —Positive integer that identifies the key. <i>type</i> —Authentication type. It can be either md5 or des. value <i>password</i> —The key itself, which can be 1 to 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.
Usage Guidelines	See “Configure NTP Authentication Keys” on page 257.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
See Also	broadcast on page 277, peer on page 290, server on page 296, trusted-key on page 304

authentication-order

Syntax	authentication-order [<i>authentication-methods</i>];
Hierarchy Level	[edit system]
Description	Configure the order in which the software tries different user-authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.
Default	If you do not include the authentication-order statement, users are verified based on their configured passwords.
Options	<i>authentication-methods</i> —One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following: password—Verify the user using the password configured for the user with the authentication statement at the [edit system login user] hierarchy level. radius—Verify the user using RADIUS authentication services. tacplus—Verify the user using TACACS+ authentication services.
Usage Guidelines	See “Configure the Authentication Order” on page 237.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

auxiliary

Syntax	auxiliary { type <i>terminal-type</i> ; }
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	type <i>terminal-type</i> —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 265.
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 <i>address</i> <destination <i>destination-address</i> >;
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	<i>address</i> —Address of the default router. <i>destination destination-address</i> —(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 227.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

boot-server

Syntax	boot-server <i>address</i> ;
Hierarchy Level	[edit system ntp]
Description	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.
Options	<i>address</i> —Address of an NTP server. You must specify an address, not a hostname.
Usage Guidelines	See “Configure the NTP Boot Server” on page 255.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

broadcast

Syntax	broadcast <i>address</i> <key <i>key-number</i> <version <i>value</i> > <tll <i>value</i> > ;
Hierarchy Level	[edit system ntp]
Description	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.
Options	<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. Values: Any unsigned 32-bit integer <i>tll value</i> —(Optional) Time-To-Live (TTL) value to use. Range: 1 through 255 Default: 1 <i>version value</i> —(Optional) Specify the 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 255.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

• broadcast-client

Syntax	broadcast-client;
Hierarchy Level	[edit system ntp]
Description	Configure the local router to listen for broadcast messages on the local network to discover other servers on the same subnet.
Usage Guidelines	See “Configure the Router to Listen for Broadcast Messages” on page 258.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

• class

Syntax	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>]; }
Hierarchy Level	[edit system login]
Description	Define login classes.
Options	<i>class-name</i> —A name you choose for the login class. The remaining statements are explained separately in this chapter.
Usage Guidelines	See “Define Login Classes” on page 243.
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 305
Syntax	class <i>class-name</i> ;
Hierarchy Level	[edit system login user]
Description	Configure a user’s login class. You must configure one class for each user.
Options	<i>class-name</i> —One of the classes defined at the [edit system login class] hierarchy level.
Usage Guidelines	See “Configure User Accounts” on page 249.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

compress-configuration-files

Syntax	compress-configuration-files;
Hierarchy Level	[edit system]
Description	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.
Default	The current operational configuration file is uncompressed.
Usage Guidelines	See “Compress the Current Configuration File” on page 230.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

console

Syntax	console { type <i>terminal-type</i> ; }
Hierarchy Level	[edit system ports]
Description	Configure the characteristics of the console port, which is on the router’s craft interface.
Default	The console port is enabled and its speed is 9600 baud.
Options	type <i>terminal-type</i> —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 265.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

default-address-selection

Syntax	default-address-selection;
Hierarchy Level	[edit system]
Description	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.
Default	The outgoing interface is used as the source address.
Usage Guidelines	See "Configure the Source Address for Locally Generated TCP/IP Packets" on page 266 and the <i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i> .
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

deny-commands

Syntax	deny-commands " <i>regular-expression</i> ";
Hierarchy Level	[edit system login class]
Description	Specify the operational mode commands the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.
Default	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.
Options	<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.
Usage Guidelines	See "Deny or Allow Individual Commands" on page 246.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
See Also	allow-commands on page 273, user on page 305

dhcp-relay

Syntax	<pre> dhcp-relay { no-listen; maximum-hop-count <i>number</i>; minimum-wait-time <i>seconds</i>; server [<i>address</i>]; interface <i>interface-group</i> { no-listen; maximum-hop-count <i>number</i>; minimum-wait-time <i>seconds</i>; server [<i>address</i>]; } } </pre>
Hierarchy Level	[edit system], [edit system dhcp-relay]
Description	Configures a router or interface to act as a Dynamic Host Configuration Protocol (DHCP) or BOOTP relay agent.
Default	DHCP relaying is disabled.
Options	<p>no-listen—Stops packets from being forwarded on a logical interface, a group of logical interfaces, or router.</p> <p>maximum-hop-count <i>number</i>—In the hops field of the BOOTP header, the maximum number of hops allowed. Default: 4 hops</p> <p>minimum-wait-time <i>seconds</i>—In the secs field of the BOOTP header, the minimum time allowed. Default: 3 seconds</p> <p>server [<i>address</i>]—Sets the IP address or addresses that specify the DHCP server or BOOTP server for the router or interface.</p> <p>interface <i>interface-group</i>—Sets a logical interface or group of logical interfaces with a specific DHCP relay configuration.</p>
Usage Guidelines	See “Configure the Router or Interface to Act as a DHCP/BOOTP Relay Agent” on page 267.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

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 System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), or Forwarding Engine Board (FEB) port.

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



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 272.

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 225.

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

domain-search

Syntax	domain-search [<i>domain-list</i>];
Hierarchy Level	[edit system]
Description	Configure a list of domains to be searched.
Options	<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.
Usage Guidelines	See “Configure Which Domains to Search” on page 226.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

full-name

Syntax	full-name <i>complete-name</i> ;
Hierarchy Level	[edit system login user]
Description	Configure the complete name of a user.
Options	<i>complete-name</i> —Full name of the user. If the name contains spaces, enclose it in quotation marks.
Usage Guidelines	See “Configure User Accounts” on page 249.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

host-name

Syntax	host-name <i>host-name</i> ;
Hierarchy Level	[edit system]
Description	Set the host name of the router.
Options	<i>host-name</i> —Name of the router.
Usage Guidelines	See “Configure the Router’s Name and Addresses” on page 223.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

idle-timeout

Syntax idle-timeout *minutes*;

Hierarchy Level [edit system login class]

Description 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.

Default If you omit this statement, a user is never forced off the system after extended idle times.

Options *minutes*—Maximum idle time.
Range: 0 through 100,000 minutes

Usage Guidelines See “Configure the Timeout Value for Idle Login Sessions” on page 248.

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 305

Interface

Syntax	interface <i>interface-group</i> { no-listen; maximum-hop-count; minimum-wait-time <i>seconds</i> ; server [<i>address</i>]; }
Hierarchy Level	[edit system dhcp-relay]
Description	Configure the router or an interface to act as a Dynamic Host Configuration Protocol (DHCP) or BOOTP relay agent.
Options	<p>server sets the IP address or addresses that specifies the DHCP or BOOTP server for the router or interface. You can include as many addresses as necessary in the same statement.</p> <p>no-listen stops packets from being forwarded on a logical interface, a group of logical interfaces, or router.</p> <p>interface sets a logical interface or a group of logical interfaces with a specific DHCP-relay or BOOTP configuration</p> <p>maximum-hop-count sets the maximum allowed number in the hops field of the BOOTP header. Headers that have a larger number in the hops field are not forwarded. If you omit the maximum-hop-count statement, the default value is 4 hops.</p> <p>minimum-wait-time sets the minimum allowed number of seconds in the secs field of the BOOTP header. Headers that have a smaller number in the secs field are not forwarded. If you omit the minimum-wait-time statement, the default value is 3 seconds.</p>
Usage Guidelines	See “Configure the Router or Interface to Act as a DHCP/BOOTP Relay Agent” on page 267.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

load-key-file

Syntax	load-key-file;
Hierarchy Level	[edit system]
Description	Loads RSA (ssh version 1) and DSA (ssh version 2) public keys from a file. The file is a URL containing one or more ssh keys.
Usage Guidelines	See “Configure the Root Password” on page 229 and. “Configure User Accounts” on page 249.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

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 228.

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";
        ssh-dsa "public-key";
    }
}

```

Hierarchy Level [edit system]

Description Configure user access to the router.

Options The remaining statements are explained separately in this chapter.

Usage Guidelines See "Configure User Access" on page 243.

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 271.

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

mirror-flash-on-disk

Syntax mirror-flash-on-disk;

Hierarchy Level [edit system]

Description Configure the hard drive to automatically mirror the contents of the compact flash. The hard drive maintains a synchronized mirror copy of the compact-flash contents. Data written to the compact flash is simultaneously updated in the mirrored copy of the hard drive. If the flash drive fails to read data, the hard drive automatically retrieves its mirrored copy of the flash disk.



Caution

We recommend that you disable flash disk mirroring when you upgrade or downgrade the router.

You cannot issue the request system snapshot command while flash disk mirroring is enabled.



Note

After you have enabled or disabled the mirror-flash-on-disk statement, you must reboot the router for your changes to take effect. To reboot, issue the request system reboot command.

Usage Guidelines See “Configure Flash Disk Mirroring” on page 228.

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 router joins those multicast groups.
Default: 224.0.1.1.

Usage Guidelines See “Configure the Router to Listen for Multicast Messages” on page 258.

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 { <i>address</i> ; }
Hierarchy Level	[edit system]
Description	Configure one or more DNS name servers.
Options	<i>address</i> —Address of the name server. To configure multiple name servers, include multiple <i>address</i> options.
Usage Guidelines	See “Configure a DNS Name Server” on page 226.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

no-redirects

Syntax	no-redirects;
Hierarchy Level	[edit system]
Description	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.
Default	The router sends redirect messages.
Usage Guidelines	See “Disable the Sending of Redirect Messages on the Router” on page 266.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
See Also	The no-redirects statement in the <i>JUNOS Internet Software Configuration Guide: Interfaces and Class of Service</i> .

no-saved-core-context

Syntax	no-saved-core-context;
Hierarchy Level	[edit system]
Description	Disable core files generated by internal JUNOS processes. Default Core files generated by internal JUNOS processes are now saved along with contextual information in compressed tar files stored under <i>/var/tmp/process-name.core.core-number.tgz</i> for debugging purposes. .
Usage Guidelines	See “Core Dump Files” on page 272
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

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>;
 trusted-key [*key-numbers*];
 }

Hierarchy Level [edit system]

Description Configure the Network Time Protocol (NTP) on the router.

Options The remaining statements are explained separately in this chapter.

Usage Guidelines See “Configure the Network Time Protocol” on page 254.

Required Privilege Level 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 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.

Values: 1, 2, 3

Default: 3

Usage Guidelines See “Configure the NTP Time Server and Time Services” on page 255.

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

permissions

Syntax	<code>permissions [<i>permissions</i>];</code>
Hierarchy Level	[edit system login class]
Description	Configure the login access privileges to be provided on the router.
Options	<i>permissions</i> —Privilege type. For a list of types, see Table 10, “Login Class Permission Bits” on page 245.
Usage Guidelines	See “Configure Access Privilege Levels” on page 244.
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 305

port

Syntax	<code>port <i>number</i>;</code>
Hierarchy Level	[edit system radius-server <i>address</i>]
Description	Configure the port number on which to contact the RADIUS server.
Options	<i>number</i> —Port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2138)
Usage Guidelines	See “Configure RADIUS Authentication” on page 231.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

ports

Syntax	<pre>ports { auxiliary { type <i>terminal-type</i>; } console { type <i>terminal-type</i>; } }</pre>
Hierarchy Level	[edit system]
Description	Configure the properties of the console and auxiliary ports, which are located on the router’s craft interface.
Options	The remaining statements are explained separately in this chapter.
Usage Guidelines	See “Configure Console and Auxiliary Port Properties” on page 265.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

processes

Syntax processes {
 inet-process (enable | disable) failover (alternate-media | other-routing-engine);
 interface-control (enable | disable) failover (alternate-media | other-routing-engine);
 mib-process (enable | disable) failover (alternate-media | other-routing-engine);
 ntp (enable | disable) failover (alternate-media | other-routing-engine);
 routing (enable | disable) failover (alternate-media | other-routing-engine);
 snmp (enable | disable) failover (alternate-media | other-routing-engine);
 watchdog (enable | disable) failover (alternate-media | other-routing-engine)
 timeout *seconds*;
 }

Hierarchy Level [edit system]

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

Default All processes are enabled by default



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

Caution

Options failover (alternate-media | other-routing-engine)—(Optional) For routers with redundant Routing Engines only, switch to backup media if a process fails repeatedly. If a process fails three times in quick succession, the router reboots from the alternate media or the other Routing Engine.

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 “Disable JUNOS Software Processes” on page 271.

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

protocol-version

Syntax	protocol-version;
Hierarchy Level	[edit system services ssh]
Description	Specify secure shell (ssh) protocol version.
Options	protocol version—v1, v2, or [v1 v2] Default: [v1 v2]
Usage Guidelines	See “Configure ssh Protocol Version” on page 270.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

radius-server

Syntax	radius-server <i>server-address</i> { port <i>number</i> ; retry <i>number</i> ; secret <i>password</i> ; timeout <i>seconds</i> ; }
Hierarchy Level	[edit system]
Description	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.
Options	<i>server-address</i> —Address of the RADIUS authentication server. The remaining statements are explained separately in this chapter.
Usage Guidelines	See “Configure RADIUS Authentication” on page 231.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

retry

Syntax `retry number;`

Hierarchy Level `[edit system radius-server server-address]`

Description Number of times that the router attempts to contact a RADIUS authentication server.

Options *number*—Number of times to retry contacting a RADIUS server.
Range: 1 through 10
Default: 3

Usage Guidelines See “Configure RADIUS Authentication” on page 231.

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

See Also `timeout` on page 301

root-authentication

Syntax `root-authentication {
 (encrypted-password "password" | plain-text-password);
 ssh-rsa "public-key";
 ssh-dsa "public-key";
}`

Hierarchy Level `[edit system]`

Description Configure the authentication methods for the root-level user, whose username is “root.”

Options `encrypted-password "password"`—Use MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.

`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.

`ssh-rsa "public-key"`—secure shell (ssh 1) authentication. Specify the ssh public key. You can specify one or more public keys.

`ssh-rsa "public-key"`—secure shell (ssh 2) authentication. Specify the ssh public key. You can specify one or more public keys.

Usage Guidelines See “Configure the Root Password” on page 229.

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

See Also `authentication` on page 274

root-login

Syntax	root-login (allow deny deny-password);
Hierarchy Level	[edit system services ssh]
Description	Control user access through ssh.
Options	<p>allow—Allows users to log on to the router as root through ssh. Default: allow</p> <p>deny—Disable users from logging on the router as root through ssh.</p> <p>deny-password—Allows users to log onto the router as root through ssh when the authentication method (for example, RSA authentication) does not require a password.</p>
Usage Guidelines	See “Configure Root Login” on page 270.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
See Also	“Configure ssh Service” on page 269.

secret

Syntax	secret <i>password</i> ;
Hierarchy Level	[edit system radius-server <i>server-address</i>], [edit system tacplus-server <i>server-address</i>]
Description	Configure the password to use with the RADIUS or TACACS+ server. The secret password used by the local router must match that used by the server.
Options	<i>password</i> —Password to use. Can include spaces.
Usage Guidelines	See “Configure RADIUS Authentication” on page 231 and “Configure TACACS+ Authentication” on page 233.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

• server

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

• **Hierarchy Level** [edit system ntp]

• **Description** For NTP, configure the local router to operate in client mode with the remote system at the specified *address*. 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.

• **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 preferred host, which means that, if all other 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.

• **Values:** 1, 2, 3

• **Default:** 3

• **Usage Guidelines** See “Configure the NTP Time Server and Time Services” on page 255.

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

services

Syntax	<pre> services { finger { <connection-limit limit>; <rate-limit limit>; } rlogin { <connection-limit limit>; <rate-limit limit>; } ssh { root-login (allow deny deny-password); protocol-version [v1 v2]; <connection-limit limit>; <rate-limit limit >; } telnet { <connection-limit limit>; <rate-limit limit>; } } </pre>
Hierarchy Level	[edit system]
Description	Configure the router so that users on remote systems can access the local router through the finger, rlogin, ssh, and telnet, and network utilities.
Options	<p>connection-limit <i>limit</i>—(Optional) Maximum number of established connections. Range: 1 through 250 Default: 75</p> <p>rate-limit <i>limit</i>—(Optional) Maximum number of connection attempts allowed per minute. Range: 1 through 250 Default: 150</p> <p>finger—Allow finger requests from remote systems to the local router.</p> <p>ftp—Allow ftp requests from remote systems to the local router.</p> <p>rlogin—Allow rlogin access from remote systems to the local router.</p> <p>ssh—Allow ssh access from remote systems to the local router.</p> <p>telnet—Allow telnet login from remote systems to the local router.</p> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configure System Services” on page 268.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
See Also	protocol-version on page 293, root-login on page 295, and “Configure ssh Service” on page 269.

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 233.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

static-host-mapping

Syntax	static-host-mapping { <i>host-name</i> { inet [<i>address</i>]; sysid <i>system-identifier</i> ; alias [<i>alias</i>]; } }
Hierarchy Level	[edit system]
Description	Map a host name to one or more IP addresses and aliases, and configure an ISO system identifier (sysid).
Options	alias <i>alias</i> —(Optional) Alias for the host name. <i>host-name</i> —Fully qualified host name. inet <i>address</i> —IP address. You can specify one or more IP addresses for the host. sysid <i>system-identifier</i> —ISO system identifier (sysid). This is the 6-byte sysid portion of the IS-IS Network Service Access Point (NSAP). We recommend that you use the host’s IP address represented in binary-coded decimal (BCD) format. For example, the IP address 208.197.169.18 would be 2081.9716.9018 in BCD.
Usage Guidelines	See “Configure the Router’s Name and Addresses” on page 223.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

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 level—Class of log messages. To specify multiple classes, include multiple *facility level* options. These can include one or more of the facilities listed in Table 13, “System Logging Facilities” on page 260.

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. This can be one or more of the priorities listed in Table 14.
- 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 259.

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 219.

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

tacplus-server

Syntax	<code>tacplus-server server-address { secret password; single-connection; timeout seconds; }</code>
Description	Configure the Terminal Access Controller Access Control System Plus (TACACS+).
Hierarchy Level	[edit system]
Options	<i>server-address</i> —Address of the TACACS+ authentication server. The remaining statements are explained separately.
Usage Guidelines	See “Configure TACACS+ Authentication” on page 233.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

timeout

Syntax	<code>timeout seconds;</code>
Hierarchy Level	[edit system radius-server <i>server-address</i>], [edit system tacplus-server <i>server-address</i>]
Description	Configure the amount of time that the local router waits to receive a response from a RADIUS or TACACS+ server.
Options	<i>seconds</i> —Amount of time to wait. Range: 1 through 90 Default: 3 seconds
Usage Guidelines	See “Configure RADIUS Authentication” on page 231 and “Configure TACACS+ Authentication” on page 233.
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 294

time-zone

Syntax time-zone *time-zone*;

Hierarchy Level [edit system]

Description Set the local time zone.

Default UTC

Options *time-zone*—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:

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/DumontD'Urville, 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/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 253.

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

trusted-key

Syntax trusted-key [*key-numbers*];

Hierarchy Level [edit system ntp]

Description 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.

Options *key-numbers*—One or more key numbers. Each key can be any 32-bit unsigned integer except 0.

Usage Guidelines See “Configure NTP Authentication Keys” on page 257.

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

See Also authentication-key on page 275, broadcast on page 277, peer on page 290, server on page 296

uid

Syntax uid *uid-value*;

Hierarchy Level [edit system login user]

Description Configure user identifier for a login account.

Options *uid-value*—Number associated with the login account. This value must be unique on the router.
Range: 100 through 64,000

Usage Guidelines See “Configure User Access” on page 243.

Required Privilege Level 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";
                ssh-dsa "public-key";
            }
        }

```

Hierarchy Level [edit login]

Description Configure access permission for individual users.

Options The remaining statements are explained separately in this chapter.

Usage Guidelines See “Configure User Access” on page 243.

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 278

