

## Chapter 25

# Configuring Miscellaneous System Management Features

This chapter discusses the following topics:

Configuring Console and Auxiliary Port Properties on page 428

Disabling the Sending of Redirect Messages on the Router on page 428

Configuring the Source Address for Locally Generated TCP/IP Packets on page 429

Configuring the Router or Interface to Act as a DHCP/BOOTP Relay Agent on page 429

Configuring System Services on page 430

Configuring a System Login Message on page 434

Configuring JUNOS Software Processes on page 434

Configuring the Password on the Diagnostics Port on page 435

Core Dump Files on page 436

Configuring a Router to Transfer its Configuration to an Archive Site on page 436

Specifying the Number of Configurations Stored on the Flash Drive on page 438

Configuring TACACS+ System Accounting on page 438

Enabling the SDX Software on page 440

## Configuring Console and Auxiliary Port Properties

---

The router's craft interface has two ports—a console port and an auxiliary port—for connecting terminals to the router. The console port is enabled by default, and its speed is 9600 baud. The auxiliary port is disabled by default.

To configure the properties for the console and auxiliary ports, include the ports statement at the [edit system] hierarchy level:

```
[edit system]
ports {
  auxiliary {
    type terminal-type;
  }
  console {
    insecure;
    log-out-on-disconnect;
    type terminal-type;
  }
}
```

By default, the terminal type is unknown, and the terminal speed is 9600 baud for both the console and auxiliary ports. To change the terminal type, include the type statement, specifying a *terminal-type* of ansi, vt100, small-xterm, or xterm. The first three terminal types set a screen size of 80 columns by 24 lines. The last type, xterm, sets the size to 80 columns by 65 rows.

By default, the console session is not logged out when the data carrier is lost on the console modem control lines. To log out the session when the data carrier on the console port is lost, include the log-out-on-disconnect statement.

By default, terminal connections to the console and auxiliary ports are secure. When you configure the console as insecure, root logins are not allowed to establish terminal connections. To disable root login connections to the console and auxiliary ports, include the insecure statement.

## Disabling the Sending of Redirect Messages on the Router

---

By default, the router sends protocol redirect messages. To disable the sending of redirect messages by the router, include the no-redirects statement at the [edit system] hierarchy level:

```
[edit system]
no-redirects;
```

To re-enable the sending of redirect messages on the router, delete the no-redirects statement from the configuration.

To disable the sending of redirect messages on a per-interface basis, include the no-redirects statement at the [edit interfaces *interface-name* unit *logical-unit-number* family *family*] hierarchy level, as described in the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

## Configuring the Source Address for Locally Generated TCP/IP Packets

---

By default, the source address included in locally generated Transmission Control Protocol/IP (TCP/IP) packets, such as FTP traffic, and in User Datagram Protocol (UDP) and IP packets, such as Network Time Protocol (NTP) requests, is chosen as the local address for the interface on which the traffic is transmitted. This means that the local address chosen for packets to a particular destination might change from connection to connection based on the interface that the routing protocol has chosen to reach the destination when the connection is established.

To configure the software to select a fixed address to use as the source for locally generated IP packets, include the `default-address-selection` statement at the `[edit system]` hierarchy level:

```
[edit system]
  default-address-selection;
```

If you include the `default-address-selection` statement in the configuration, the software chooses the system default address as the source for most locally generated IP packets. The default address is usually an address configured on the `lo0` loopback interface. For example, if you specified that SSH and Telnet use a particular address, but you also have `default-address-selection` configured, the system default address is used. For more information about how the default address is chosen, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

For IP packets sent by IP routing protocols—including Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Resource Reservation Protocol (RSVP), and the multicast protocols, but not including Intermediate System-to-Intermediate System (IS-IS)—the local address selection is often constrained by the protocol specification so that the protocol operates correctly. When this constraint exists in the routing protocol, the packet's source address is unaffected by the presence of the `default-address-selection` statement in the configuration. For protocols in which the local address is unconstrained by the protocol specification, for example, internal Border Gateway Protocol (iBGP) and multihop external BGP (EBGP), if you do not configure a specific local address when configuring the protocol, the local address is chosen using the same method as other locally generated IP packets.

## Configuring the Router or Interface to Act as a DHCP/BOOTP Relay Agent

---

To configure a router or interface to act as a Dynamic Host Configuration Protocol/bootstrap protocol (DHCP/BOOTP) relay agent, you include statements at the `[edit forwarding-options helpers]` hierarchy level. For more information, see the *JUNOS Policy Framework Configuration Guide*.

## Configuring System Services

---

For security reasons, remote access to the router is disabled by default. You must configure the router explicitly so that users on remote systems can access it. The router can be accessed from a remote system by means of the finger, FTP, JUNOScript clear-text, JUNOScript Secure Sockets Layer (SSL), rlogin, SSH, and Telnet services.

This section discusses the following topics:

Configuring Finger Service on page 430

Configuring FTP Service on page 430

Configuring JUNOScript Clear-Text Service on page 431

Configure JUNOScript SSL Service on page 431

Configuring SSH Service on page 432

Configuring Telnet Service on page 433

### Configuring Finger Service

To configure the router to accept finger as an access service, include the finger statement at the [edit system services] hierarchy level:

```
[edit system services]
finger {
  <connection-limit limit>;
  <rate-limit limit>;
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

*connection-limit limit*—The maximum number of established connections (1 through 250) per minute. By default, the maximum number of establish connections is set to 75 connections per minute.

*rate-limit limit*—The maximum number of connection attempts allowed per minute (1 through 250). By default, the maximum number of connection limits is set to 150 per minute.

### Configuring FTP Service

To configure the router to accept the FTP as an access service, include the ftp statement at the [edit system services] hierarchy level:

```
[edit system services]
ftp {
  <connection-limit limit>;
  <rate-limit limit>;
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

connection-limit *limit*—The maximum number of established connections (1 through 250) per minute. By default, the maximum number of establish connections is set to 75 connections per minute.

rate-limit *limit*—The maximum number of connection attempts allowed per minute (1 through 250). By default, the maximum number of connection limits is set to 150 per minute.

### Configuring JUNOScript Clear-Text Service

To configure the router to accept JUNOScript clear text as an access service, include the `xnm-clear-text` statement at the [edit system services] hierarchy level:

```
[edit system services]
xnm-clear-text {
  <connection-limit limit>;
  <rate-limit limit>;
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

connection-limit *limit*—The maximum number of established connections (1 through 250) per minute. By default, the maximum number of establish connections is set to 75 connections per minute.

rate-limit *limit*—The maximum number of connection attempts allowed per minute (1 through 250). By default, the maximum number of connection limits is set to 150 per minute.

### Configure JUNOScript SSL Service

To configure the router to accept JUNOScript SSL as an access service, include the `xnm-ssl` statement at the [edit system services] hierarchy level:

```
[edit system services]
xnm-ssl {
  <connection-limit limit>;
  <rate-limit limit>;
  <local-certificate name>;
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

connection-limit *limit*—The maximum number of established connections (1 through 250) per minute. By default, the maximum number of establish connections is set to 75 connections per minute.

local-certificate *name*—Name of local X.509 certificate to use. You must import the certificate before you reference it. For more information about how to import an SSL certificate, see “Using JUNOScript SSL Service” on page 663.

rate-limit *limit*—The maximum number of connection attempts allowed per minute (1 through 250). By default, the maximum number of connection limits is set to 150 per minute.

## Configuring SSH Service

To configure the router to accept SSH as an access service, include the SSH statement at the [edit system services] hierarchy level:

```
[edit system services ]
ssh {
  root-login (allow | deny | deny-password);
  protocol-version [v1 v2];
  <connection-limit limit>;
  <rate-limit limit>;
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

connection-limit *limit*—The maximum number of established connections (1 through 250) per minute. By default, the maximum number of establish connections is set to 75 connections per minute.

rate-limit *limit*—The maximum number of connection attempts allowed per minute (1 through 250). By default, the maximum number of connection limits is set to 150 per minute.

This section includes the following topics:

Configuring the Root Login on page 432

Configuring the SSH Protocol Version on page 433

### Configuring the Root Login

By default, users are allowed to log in to the router as root through SSH. To control user access through SSH, include the root-login statement at the [edit systems services ssh] hierarchy level:

```
[edit system services ssh]
root-login (allow | deny | deny-password);
```

allow—Allows users to log in to the router as root through SSH. The default is allow.

deny—Disables users from logging in to the router as root through SSH.

deny-password—Allows users to log in to the router as root through SSH when the authentication method (for example, RSA) does not require a password.



**NOTE:** The root-login and protocol-version statements are supported in JUNOS Release 5.0 and later. If you downgrade to a release prior to release 5.0, the root-login and protocol-version statements are ignored if they are present in the configuration file.

---

### Configuring the SSH Protocol Version

By default, version 2 of the SSH protocol is enabled. To configure the router to use only version 1 of the SSH protocol, include the `protocol-version` statement and specify `v1` at the `[edit system services ssh]` hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 ];
```

To configure the router to use version 1 and 2 of the SSH protocol, include the `protocol-version` statement and specify `v1` and `v2` at the `[edit system services ssh]` hierarchy level:

```
[edit system services ssh]
protocol-version [ v1 v2 ];
```

You can specify `v1`, `v2`, or both versions `[v1 v2]` of the SSH protocol. The default is `v2`.



**NOTE:** The `root-login` and `protocol-version` statements are supported in JUNOS Release 5.0 and later. If you downgrade to a release prior to release 5.0, the `root-login` and `protocol-version` statements are ignored if they are present in the configuration file.

---

### Configuring Telnet Service

To configure the router to accept Telnet as an access service, include the `telnet` statement at the `[edit system services]` hierarchy level:

```
[edit system services]
telnet {
  <connection-limit limit>;
  <rate-limit limit>;
}
```

You can optionally specify the maximum number of concurrently established connections and the maximum number of connections attempted per minute.

`connection-limit limit`—The maximum number of established connections (1 through 250) per minute. By default, the maximum number of established connections is set to 75 connections per minute.

`rate-limit limit`—The maximum number of connection attempts allowed per minute (1 through 250). By default, the maximum number of connection limits is set to 150 per minute.

## Configuring Console Access to PICs

---

By default, there is no password setting for console access. To configure console access to the Physical Interface Cards (PICs), include the `pic-console-authentication` statement at the `[edit system]` hierarchy level:

```
[edit system]
pic-console-authentication {
  (encrypted-password "password" | plain-text-password);
}
```

`encrypted-password "password"`—Use Message Digest 5 (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 command-line interface (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 information about how to create plain-text passwords, see “Specifying Plain-Text Passwords” on page 17.

## Configuring a System Login Message

---

By default, no login message is displayed. To configure a system login message, include the `message` statement at the `[edit system login]` hierarchy level:

```
[edit system login]
message text;
```

## Configuring JUNOS Software Processes

---

By default, all JUNOS software processes are enabled on the router. To control the software processes on the router, you can do the following:

Disabling JUNOS Software Processes on page 435

Configuring Failover to Backup Media if a Software Process Fails on page 435

## Disabling JUNOS Software Processes



**CAUTION:** Never disable any of the software processes unless instructed to do so by a Customer Support engineer.

To disable a software process, specify the appropriate option in the processes statement at the [edit system] hierarchy level:

```
[edit system]
processes {
  disk-monitoring (enable | disable);
  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;
}
```

## Configuring Failover to Backup Media if a Software Process Fails

For routers with redundant Routing Engines, in the event that a software process fails repeatedly, you can configure the router to switch to backup media containing an alternate version of the system, either the alternate media or the other Routing Engine. To configure the switch to the backup media, include the failover statement at the [edit system processes *process-name*] hierarchy level:

```
[edit system processes]
process-name failover (alternate-media | other-routing-engine);
```

*process-name* is one of the valid process names. If this statement is configured for a process, and that process fails four times within thirty seconds, the router reboots from either the alternative media or the other Routing Engine.

## Configuring the Password on the Diagnostics Port

If you have been asked by Customer Support personnel to connect a physical console to a control board or forwarding component on the router (such as the System Control Board [SCB], System and Switch Board [SSB], or Switching and Forwarding Module [SFM]) to perform diagnostics, you can configure a password on the diagnostics port. This password provides an extra level of security.

To configure a password on the diagnostics port, include the diag-port-authentication statement at the [edit system] hierarchy level:

```
[edit system]
diag-port-authentication (encrypted-password "password" | plain-text-password);
```

You can use an MD5 password, or you can enter a plain-text password that the JUNOS software encrypts (using MD5-style encryption) before it places it into the password database. For an MD5 password, specify the password in the configuration.

If you configure the `plain-text-password` option, the CLI prompts you for the password. For information about how to create a plain-text passwords, see “Specifying Plain-Text Passwords” on page 17.

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

## Core Dump Files

---

By default, core files generated by internal JUNOS processes are saved along with contextual information in compressed tar files stored under `/var/tmp/process-name.core.core-number.tgz` for debugging purposes. The contextual information contains the configuration and log messages file.

To turn this feature off, include the `no-saved-core-context` statement at the `[edit system]` hierarchy level:

```
[edit system]
no-saved-core-context;
```

To save the core files only, include the `saved-core-files` statement, specifying the number of files to save at the `[edit system]` hierarchy level:

```
[edit system]
saved-core-files saved-core-files;
```

*saved-core-files* is the number of core files to save and can be a value from 1 through 64.

To save the core files along with the contextual information, include the `save-core-context` statement at the `[edit system]` hierarchy level:

```
[edit system]
save-core-context;
```

## Configuring a Router to Transfer its Configuration to an Archive Site

---

If you want to back up your router’s current configuration to an archive site, you can configure the router to transfer its currently active configuration by FTP periodically or after each commit.

To configure the router to transfer its currently active configuration to an archive site, include statements at the `[edit system archival configuration]` hierarchy level:

```
[edit system archival configuration]
transfer-interval interval;
transfer-on-commit;
archive-sites {
    ftp://<username>:<password>@<host>:<port>/<url-path>;
}
```

This section includes the following topics:

Configuring the Transfer Interval on page 437

Configuring Transfer on Commit on page 437

Configuring Archive Sites on page 437

### **Configuring the Transfer Interval**

To configure the router to periodically transfer its currently active configuration to an archive site, include the `transfer-interval` statement at the [edit system archival configuration] hierarchy level:

```
[edit system archival configuration]
transfer-interval interval;
```

The *interval* is a period of time ranging from 15 through 2880 minutes.

### **Configuring Transfer on Commit**

To configure the router to transfer its currently active configuration to an archive site each time you commit a candidate configuration, include the `transfer-on-commit` statement at the [edit system archival configuration] hierarchy level:

```
[edit system archival configuration]
transfer-on-commit;
```

### **Configuring Archive Sites**

When you configure the router to transfer its configuration files, you specify an archive site to which the files are transferred. If you specify more than one archive site, the router attempts to transfer to the first archive site in the list, moving to the next site only if the transfer fails.

To configure the archive site, include the `archive-sites` statement at the [edit system archival configuration] hierarchy level:

```
[edit system archival configuration]
archive-sites {
  ftp://username@host:<port>url-path password password;
}
```

When you specify the archive site, do not add a forward slash (/) to the end of the URL. The format for the destination filename is  
`<router-name> _juniper.conf[.gz]_YYYYMMDD_HHMMSS`

## Specifying the Number of Configurations Stored on the Flash Drive

---

By default, the JUNOS software saves the current configuration and three previous versions of the committed configuration on the flash drive. The currently operational JUNOS software configuration is stored in the file `juniper.conf.gz`, and the last three committed configurations are stored in the files `juniper.conf.1.gz`, `juniper.conf.2.gz`, and `juniper.conf.3.gz`. These four files are located in the router's flash drive in the directory `/config`.

In addition to saving the current configuration and the current operational version, you can also specify how many previous versions of the committed configurations you want stored on the flash drive in the directory `/config`. The remaining previous versions of committed configurations are stored in the directory `/var/db/config` on the hard disk. This is useful when you have very large configurations that might not fit on the flash drive.

To specify how many previous versions of the committed configurations you want stored on the flash drive, include the `max-configurations-on-flash` statement at the `[edit system]` hierarchy level:

```
[edit system]
max-configurations-on-flash number;
```

*number* can be in the range from 0 to 49.

For more information about how the configuration is stored, see “How the Configuration Is Stored” on page 201.

## Configuring TACACS+ System Accounting

---

You can use TACACS+ to track and log software logins, configuration changes, and interactive commands. To audit these events, include the following statements at the `[edit system accounting]` hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
  tacplus {
    server {
      server-address {
        port port-number;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}
```

This section includes the following topics:

Specifying Events on page 439

Configuring TACACS+ Accounting on page 439

## Specifying Events

To specify the events you want to audit, include the events statement at the [edit system accounting] hierarchy level:

```
[edit system accounting]
events [ events ];
```

*events* is one or more of the following:

login—Audit logins

change-log—Audit configuration changes

interactive-commands—Audit interactive commands (any command-line input)

## Configuring TACACS+ Accounting

To configure TACACS+ server accounting, include the server statement at the [edit system accounting destination tacplus] hierarchy level:

```
[edit system accounting destination tacplus]
server {
  server-address {
    port port-number;
    secret password ;
    single-connection;
    timeout seconds;
  }
}
```

*server-address* specifies the address of the TACACS+ server. To configure multiple TACACS+ servers, include multiple server statements.



**NOTE:** If no TACACS+ servers are configured at the [edit system accounting destination tacplus] statement hierarchy level, the JUNOS software uses the TACACS+ servers configured at the [edit system tacplus-server] hierarchy level.

---

*port-number* specifies the TACACS+ server port number.

You must specify a secret (password) that the local router passes to the TACACS+ client by including the secret statement. Secrets can contain spaces. The secret used by the local router must match that used by the server.

You can optionally specify the length of time that the local router waits to receive a response from a TACACS+ server by including the timeout statement. By default, the router waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

You can optionally maintain one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt, by including the single-connection statement.

## Enabling the SDX Software

---

You can enable JUNOS software to work with the Service Deployment System (SDX) software. The SDX software supports dynamic service activation engine (SAE) functionality on JUNOS routers. To do this, include the following statements at the [edit system services service-deployment] hierarchy level:

```
[edit system services service-deployment]
servers server-address {
  port port-number;
}
source-address source-address;
```

*server-address* is the IPv4 address of the SDX server.

By default, *port-number* is set to 3333 and is a TCP port number.

*source-address* is optional, and is the local IP version 4 (IPv4) address to be used as the source address for traffic to the SDX server.

For more information about SDX software, see the SDX documentation set.

## Configuring the Path MTU Discovery

---

By default, path maximum transmission unit (MTU) discovery on outgoing TCP connections is disabled. To enable path MTU discovery, include the `path-mtu-discovery` statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
path-mtu-discovery;
```

## Configuring Source Quench

---

By default, Internet Control Message Protocol (ICMP) source quench is disabled. You enable source quench when you want the JUNOS software to ignore ICMP source quench messages. To do this, include the `source-quench` statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
source-quench;
```

## Configuring the Range of Port Addresses

---

By default, the upper range of a port address is 5000. You can increase the range from which the port number can be selected to decrease the probability that someone can determine your port number. To do so, include the source-port statement at the [edit system internet-options] hierarchy level:

```
[edit system internet-options]
source-port upper-limit <upper-limit>;
```

`upper-limit < upper-limit>` —Is the upper limit of a source port address and can be a value from 5000 through 65,355.

