

## Chapter 25

# Configure Miscellaneous System Management Features

This chapter discusses the following topics:

Configure Console and Auxiliary Port Properties on page 398

Disable the Sending of Redirect Messages on the Router on page 399

Configure the Source Address for Locally Generated TCP/IP Packets on page 399

Configure the Router or Interface to Act as a DHCP/BOOTP Relay Agent on page 400

Configure System Services on page 400

Configure a System Login Message on page 404

Configure JUNOS Software Processes on page 404

Configure the Password on the Diagnostics Port on page 405

Core Dump Files on page 405

Configure a Router to Transfer its Configuration to an Archive Site on page 406

TACACS+ System Accounting on page 408

## Configure 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.

## Disable 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 Internet Software Network Interfaces and Class of Service Configuration Guide*.

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

---

By default, the source address included in locally generated TCP/IP packets, such as FTP traffic, and in UDP and IP packets, such as 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 Internet Software Network Interfaces and Class of Service Configuration Guide*.

For IP packets sent by IP routing protocols (including OSPF, RIP, RSVP, and the multicast protocols, but not including 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, IBGP and multihop 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.

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

---

This feature is configured under the [edit forwarding-options helpers] hierarchy level. For information about how to configure the router or interface to act as a DHCP/BOOTP relay agent, see the *JUNOS Internet Software Policy Framework Configuration Guide*.

## Configure 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, rlogin, ssh, and telnet services.

This section discusses the following topics:

Configure Finger Service on page 400

Configure FTP Service on page 400

Configure rlogin Service on page 401

Configure ssh Service on page 402

Configure telnet Service on page 403

### **Configure 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.

### **Configure 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.

### **Configure rlogin Service**

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

```
[edit system services]
rlogin {
  <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.

## Configure 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.

The following sections explain how to specify the remaining options:

Configure the Root Login on page 402

Configure the ssh Protocol Version on page 403

### Configure 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.

---

## Configure 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 [version];
```

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 [version];
```

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.

---

## Configure 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.

## Configure 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;
```

## Configure 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:

Disable JUNOS Software Processes on page 404

Configure Failover to Backup Media if a Software Process Fails on page 404

### **Disable 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;
}
```

### **Configure 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 three times in quick succession, the router reboots from either the alternative media or the other Routing Engine.

## Configure the Password on the Diagnostics Port

---

If you have been asked by Customer Support personnel to connect a physical console to the router's System Control Board (SCB), System and Switch Board (SSB), or Switching and Forwarding Model (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 "Plain-Text Passwords" on page 25.

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]
user@host# set no-saved-core-context
```

## Configure 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:

Configure the Transfer Interval on page 406

Configure Transfer on Commit on page 406

Configure Archive Sites on page 407

### ***Configure 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.

### ***Configure 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;
```

## Configure 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>:<password>@<host>:<port>/<url-path>;
}
```

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

## 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 [edit system accounting] hierarchy level:

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

This section includes the following topics:

Specify Events on page 408

Configure TACACS+ Accounting on page 409

### Specify 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 ];
```

Specify in *events* one or more of the following:

login—Audit logins

change-log—Audit configuration changes

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

## Configure 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 {
    secret password ;
    single-connection;
    timeout seconds;
    port port-number;
  }
}
```

In the *server-address*, specify 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.

---

In the *port-number*, specify 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.

