

Chapter 23

Configure Miscellaneous System Management

This chapter discusses the following topics:

- Configure Console and Auxiliary Port Properties on page 225
- Disable the Sending of Redirect Messages on the Router on page 226
- Configure the Source Address for Locally Generated TCP/IP Packets on page 226
- Configure the Router to Act As a DHCP Relay Agent on page 227
- Configure System Services on page 227
- Configure a System Login Message on page 227
- Configure JUNOS Software Processes on page 228
- Configure a Password on the Diagnostics Port on page 228

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 default 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 {
    insecure;
    speed baud-rate;
    type terminal-type;
  }
  console {
    insecure;
    speed baud-rate;
    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 `terminal-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.

To change the terminal speed, include the `speed` statement, specifying a *baud-rate* of 19200, 38400, 57600, or 115200. If you change the speed on the auxiliary or console port, any user currently logged in through that port is logged off the router when the terminal resets.

By default, terminal connections to the console and auxiliary ports are secure. That is, it is safe to log in as root and enter the root password. To configure the terminal so that it is not safe for you to enter the root-level password, 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 Configuration Guide: Interfaces and Chassis*.

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 routing 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 more information about how the default address is chosen, see the *JUNOS Internet Software Configuration Guide: Interfaces and Chassis*.

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 to Act As a DHCP Relay Agent

You can configure the router to act as a Dynamic Host Configuration Protocol (DHCP) relay agent. This means that a locally attached host can issue a DHCP or BOOTP request as a broadcast message. If the router sees this broadcast message, it relays the message to a specified DHCP or BOOTP server.

You should configure the router to be a DHCP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server.

To configure the router to act as a DHCP relay agent, include the `dhcp-relay` statement at the [edit system] hierarchy level, specifying the address of the DHCP or BOOTP server:

```
[edit system]
dhcp-relay server address;
```

Configure System Services

For security reasons, no remote access to the router is enabled 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 access using the ssh, Telnet, and finger network utilities. To do this, include the appropriate utility in the services statement at the [edit system] hierarchy level:

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

For each utility, 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:

```
message text;
```

Configure JUNOS Software Processes

By default, all JUNOS software processes are enabled on the router.



Note

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 {
  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 a Password on the Diagnostics Port

If you have been asked by Customer Support personnel to connect a physical console to the router's SCB, SSB, or SFM to perform diagnostics, you can configure a password on the diagnostics port. This password provides an extra level of security on the SCB, SSB, or SFM diagnostics port.

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