Chapter 5

Managing the System

This chapter describes general tasks associated with managing the E-series router.

This chapter contains the following sections:

Overview

Managing the E-series router involves a variety of tasks. This chapter covers those tasks associated with the router in general rather than specific networking protocols. Each section in the chapter covers a different topic; where appropriate, a section contains an overview of the topic, configuration tasks, and information about monitoring the associated settings.

For additional management information, CLI commands, and procedures, refer to the following table.

Task	Reference
Find detailed information about commands described in this chapter.	*JUNOSe Command Reference Guide A to M* and *JUNOSe Command Reference Guide N to Z*
Configure the system as an SNMP agent.	*Chapter 4, Configuring SNMP*
Set system passwords.	*Chapter 9, Passwords and Security*
Write CLI macros.	*Chapter 10, Writing CLI Macros*
Boot the system.	*Chapter 11, Booting the System*
Manage line modules and SRP modules.	*Chapter 6, Managing Modules*

Platform Considerations

System management is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 and E320 router.

Naming the System

When you receive the router, it has a factory default host name. To rename the router, use the **hostname** command.

hostname

- Use to rename the router.
- The assigned name is displayed in the command-line interface (CLI) prompts.
- Example

  router1(config)#**hostname host1**
  host1(config)#

- There is no **no** version.

Configuring the Switch Fabric Bandwidth

By default, the switch fabric for the ERX-1440, ERX-310, E120, and E320 routers uses a bandwidth weighting ratio of 15:2 for multicast-to-unicast weighted round robin (WRR). In the absence of strict-priority traffic, and when both unicast and multicast traffic compete for switch fabric bandwidth, the switch fabric allocates 15/17ths of the available bandwidth to multicast traffic and 2/17ths of the available bandwidth to unicast traffic.

The **fabric weights** command enables you to specify a ratio for multicast-to-unicast traffic on the router switch fabric. The **no** version of the command reverts the weighting ratio back to its default.

fabric weights

- Use to define the multicast-to-unicast traffic ratio for the switch fabric for the ERX-1440, ERX-310, E120, and E320 routers
- Example

  host1# **fabric weights multicast 2 unicast 1**

- Use the **no** version to return the switch fabric to its default multicast-to-unicast ratio (15:2).

Configuring Timing

You can use the **timing source** command to configure three timing sources for the system. These sources are known as the primary, secondary, and tertiary sources. The system periodically polls the status of the current timing source. If the system discovers that the current source has become unavailable, it polls the timing source you specified as next in line. If this source is available, it switches to this source; if not, it then polls the next source in line. If the lowest source is unavailable, the system maintains the SRP clock as the source.

If you enable auto-upgrade, in the event of a source failure, the system—after switching to a lower source—polls all higher configured sources and automatically switches back to the highest timing source when that source becomes available.

The **timing select** command enables you to specify which source (primary, secondary, or tertiary) the system is to use by default. The system will never attempt to upgrade to a source higher than the selected source.

timing disable-auto-upgrade

- Use to disable the auto-upgrade feature of the system's timing selector.
- The system starts out by setting the operational timing selector to the administratively configured selector. See the **timing select** command.
- Example

  host1(config)#**timing disable-auto-upgrade**

- Use the **no** version to restore the factory default, which is auto-upgrade enabled.

timing select

- Use to specify which of the configured timing sources is used by default.
- Primary timing source is preferred over secondary, and secondary is preferred over tertiary. See the **timing source** command.
- If you enable the auto-upgrade feature, the system does not try to upgrade beyond the administratively configured selector.
- Example

  host1(config)#**timing select secondary**

- There is no **no** version.

timing source

- Use to specify how the SRP module exchanges timing signals with an interface.
- You can specify primary, secondary, and tertiary timing sources.
- You can specify one external source received on an I/O module or IOA other than the SRP I/O module or SRP IOA.
- You can specify two or more internal sources or external sources received through the SRP I/O module or SRP IOA external timing ports.
- On the E120 and E320 routers, you can specify sonet for only two of the available three timing sources (primary, secondary, or tertiary).
- The available sources to choose are:
  - ds1—DS1 interface
  - ds3—DS3 interface
  - e1—E1 interface
  - e3—E3 interface
  - sonet—SONET interface
  - internal—Internal system controller (SC) oscillator
  - line—External timing input on SRP module

- Example

  host1#**timing source secondary sonet 3/0**

- There is no **no** version.

Monitoring Timing

Use the **show timing** command to view the timing settings for the system.

show timing

- Use to display the timing settings and the operational status of the system timing.
- If a timing source fails, the system uses the next time source in the hierarchy, and a message appears in the system log at the *warning* level. If auto-upgrade is enabled, the system upgrades to a higher-priority timing source when one becomes available, and a message appears in the system log at the *notice* level.
- Example

```
host1#show timing
timing: tertiary (failover from primary)
        primary: external SC E1 (A) (ERROR)
        secondary: ds3 3/0 (ERROR)
        tertiary: internal SC oscillator (ok)
        auto-upgrade enabled
```

Using the CLI

Use the commands described in this section to navigate the CLI. For a complete description of the CLI, see *Chapter 2, Command-Line Interface*.

configure

- Use to enter Global Configuration mode.
- Global Configuration mode provides access to other configuration modes, such as Interface Configuration mode. See *Chapter 2, Command-Line Interface*.
- This command allows other commands to be executed from a terminal or a file.
- This command is not allowed for a short time after a warm restart (warm switchover) occurs. This delay allows some applications time to complete their warm-restart initialization. However, if the warm restart is not complete in 5 minutes, the warm start is cancelled and configuration access is restored.
- Example 1

  host1#**configure**
  Configuring from terminal or file [terminal]?
  Enter configuration commands, one per line. End with CNTL/Z.
  host1(config)#

- Example 2

  host1#**configure**
  Configuring from terminal or file [terminal]? **file**
  File name: **system1.scr**
  Proceed with configure? [confirm]
  host1(config)#

- There is no **no** version.

disable

- Use to exit Privileged Exec mode and return to User Exec mode.
- Use to move to a lower Privileged Exec mode level without returning to User Exec mode. Specifying a privilege level after the **disable** command changes the Privileged Exec mode to the lower level that you specify; you do not return to User Exec mode.
- Example 1

  host1#**disable**
  host1>

- Example 2

  host1#**show privilege**
  Privilege level is 10
  host1#**disable 5**
  host1#**show privilege**
  Privilege level is 5

- There is no **no** version.

do

- Use to issue an Exec mode command from any CLI configuration command mode.
- Example

  host1(config)#**do show configuration | begin interface**

- The **do** command functions the same as the **run** command.
- There is no **no** version.

enable

- Use to move from User Exec to Privileged Exec mode.
- Privileged Exec mode allows you to access all other user interface modes. From here you can configure, monitor, and manage all aspects of the router.
- You can access the Privileged Exec commands using one of 16 levels of command privilege. If you do not enter a privilege level and you are not accessing the router through a RADIUS authentication account, the default CLI access level is 10. For information about CLI levels of access, see *Privileged-Level Access* in *Chapter 2, Command-Line Interface*.

- Set a password for this mode by using either the **enable password** or the **enable secret** command in Global Configuration mode. This protects the system from any unauthorized use.
- Once a password is set, anyone trying to use Privileged Exec mode will be asked to provide the password.
- Example 1 (accessing Privileged Exec mode at the default level 10)

  ```
  host1>enable
  password:*******
  host1#
  ```

- Example 2 (accessing Privileged Exec mode at the highest level 15; a password is not set for this example)

  ```
  host1>enable 15
  host1#
  ```

- There is no **no** version.

end

- Use to exit Global Configuration mode or any of the other Configuration modes. You may also use Ctrl + z to exit these modes.
- Executing this command returns you to the User Exec mode.
- Example

  ```
  host1(config)#end
  host1#
  ```

- There is no **no** version.

exit

- Use to exit the current command mode or the system when issued from the User Exec mode.
- Example

  ```
  host1#exit
  host1>
  ```

- There is no **no** version.

help

- Use to display basic information about the interactive help system.
- Example

```
host1#help
Use the help options as follows:

?, or command<Space>? - Lists the set of all valid next keywords or
                        arguments
partial-keyword?      - Lists the keywords that begin with a certain
                        character string
partial-keyword<Tab>  - Completes the partial keyword
```

- There is no **no** version.

run

- Use to issue an Exec mode command from any CLI configuration command mode.
- Example

```
host1(config)#run show configuration | begin interface
```

- The **run** command functions the same as the **do** command.
- There is no **no** version.

sleep

- Use to make the CLI pause for a specified period of time (in seconds).
- Pausing is very useful in configuration script files.
- Example

```
host1#sleep 60
```

- There is no **no** version.

Managing vty Lines

The system supports 30 virtual tty (vty) lines for Telnet, SSH, and FTP services. Each Telnet, SSH, or FTP session requires one vty line. When you connect to the router through a vty line, the number of the vty line is not assigned sequentially; instead, the system assigns the first vty line that passes the host access list check rules.

Configuring vty Lines

By default five vty lines (0–4) are open. You can open additional lines using the **line vty** command. Once lines are open, login is enabled by default. Before users can access the lines, you must configure a password, disable login using the **no login** command, or configure AAA authentication on the lines.

line vty

- Use to open or configure vty lines.
- You can specify a single line or a range of lines. The range is 0–29.
- Example

```
host1(config)#line vty 6 10
host1(config-line)#
```

- Use the **no** version to remove a vty line or a range of lines from the configuration. Lines that you remove will no longer be available for use by Telnet, FTP, or SSH. When you remove a vty line, the system removes all lines above that line. For example, **no line vty 6** causes the system to remove lines 6 through 29. You cannot remove lines 0 through 4.

password

- Use to specify a password on a single line or a range of lines.
- If you enable login but do not configure a password, the system will not allow you to access virtual terminals.
- Specify a password in plain text (unencrypted) or cipher text (encrypted). In either case, the system stores the password as encrypted.
- You can use the following keywords:
  - **0** (zero)—Specifies an unencrypted password
  - **5**—Specifies a secret
  - **7**—Specifies an encrypted password
- Example 1 (unencrypted password)

```
host1(config-line)#password 0 mypassword
```

- Example 2 (secret)

```
host1(config-line)#password 5 y13_x
```

- Example 3 (encrypted password)

```
host1(config-line)#password 7 x13_2
```

- Use the **no** version to remove the password. By default, **no password** is specified.

For more information about configuring security for vty lines, see *Chapter 9, Passwords and Security*.

Monitoring vty Lines

Use the **show line vty** command to monitor vty lines.

show line vty

- Use to display the configuration of a vty line.
- Field descriptions
  - access-class—Access class associated with the vty line
  - data-character-bits—Number of bits per character
    - 7—Setting for the standard ASCII set
    - 8—Setting for the international character set
  - exec-timeout—Time interval that the terminal waits for expected user input
    - Never—Indicates that there is no time limit
  - exec-banner—Status for the exec banner: enabled or disabled. This banner is displayed by the CLI after user authentication (if any) and before the first prompt of a CLI session.
  - motd-banner—Status for the MOTD banner: enabled or disabled. This banner is displayed by the CLI when a connection is initiated.
  - login-timeout—Time interval during which the user must log in.
    - Never—Indicates that there is no time limit
- Example

```
host1#show line vty 0
no access-class in
data-character-bits 8
exec-timeout 3w 3d 7h 20m 0s
exec-banner enabled
motd-banner enabled
login-timeout 30 seconds
```

Clearing Lines

Use the **clear line** command to clear any line on the system (vty or console). Using this command terminates any service, such as an FTP session, on this line and closes any open files.

clear line

- Use to remove any services on a line and close any files opened as a result of services on that line.
- You can specify the absolute number to clear any line. For each line on the system, the absolute number is listed in the line number field of the **show users** command output.
- You can specify the line type and the relative number to clear a specific type of line. For each line on the system, the relative number is listed in the line name field of the **show users** command output.

- Example 1

  host1#**clear line 2**

- Example 2

  host1#**clear line console 0**

- There is no **no** version.

Monitoring the Current Configuration

Use the commands described in this section to monitor the current (running) configuration of the system.

You can use the **show configuration** command to display information when the router is in Automatic Commit mode. In Automatic Commit mode, the system automatically saves any change to the system configuration to nonvolatile storage (NVS).

You can use the **show running-configuration** command to display information when the router is in Manual Commit mode. In Manual Commit mode, any configuration change affects only the current (running) system configuration.

For more information about saving the current configuration in Automatic Commit mode or Manual Commit mode, see *Saving the Current Configuration* on page 235.

Defining the Configuration Output Format

The JUNOSe **show configuration** command displays the entire system configuration. For very large configurations, the show configuration report can take a long time to generate and display.

The **service show-config format** command enables you to run the **show configuration** command using one of two formats—original format (format 1; the default) and a format that provides a much faster output (format 2). Using format 2 can significantly reduce the amount of time it takes to generate and display configurations that contain three or more virtual routers and a large number of interfaces.

The primary difference between format 1 and format 2 output is the way in which each displays layer 2 and layer 3 interface configurations. Table 29 indicates where layer 2 and layer 3 interface configurations appear within the **show configuration** command output when the system is using format 1 or format 2.

Table 29: Output Locations for Layer 2 and Layer 3 Interface Configurations

Format	Layer 2 Only Interfaces	Layer 3 Only Interfaces	Layer 2 and Layer 3 Combination Interfaces
Format 1	Entire configuration appears in the default router output	Entire configuration appears in the layer 3 virtual router output	Layer 2 configuration appears in the default router the layer 3 virtual router output
Format 2	Entire configuration appears in the default router output	Entire configuration appears in the layer 3 virtual router output	Layer 2 configuration appears in the default router output; layer 3 configuration appears in the layer 3 virtual router output

The following examples show the differences between format 1 and format 2 output:

Example 1 Format 1 output

```
virtual-router default
…
interface null 0
interface loopback 0
 ip address 127.0.0.1 255.0.0.0
!
interface ip shAtm50126
 ip share-interface atm 5/0.126
!
interface ip MikeShare2
 ip share-interface atm 5/1.1
!
interface atm 5/0
interface atm 5/0.100 point-to-point
 atm pvc 100 0 100 aal5snap 0 0 0
 encapsulation pppoe
 pppoe sessions 1
!
interface atm 5/0.100.1
 encapsulation ppp
 ppp authentication chap
 ip address 102.0.1.1 255.255.255.0
!
interface atm 5/0.102 multipoint
 atm pvc 1021 0 1021 aal5snap 0 0 0
 atm pvc 1022 0 1022 aal5snap 0 0 0
 atm pvc 1023 0 1023 aal5snap 0 0 0
 ip address 102.0.2.1 255.255.255.0
!
interface atm 5/0.103 point-to-point
 atm pvc 103 0 103 aal5snap 0 0 0
 encapsulation bridge1483
 ip address 100.0.0.1 255.255.255.0
 pppoe
!
pppoe subinterface atm 5/0.103.1
 encapsulation ppp
 ppp authentication pap
 ip address 100.0.1.1 255.255.255.0
!
```

```
interface atm 5/0.104 point-to-point
 atm pvc 104 0 104 aal5snap 0 0 0
 ip address 150.0.1.1 255.255.255.0
 ipv6 address 2000:0:17::1/60
!
interface atm 5/0.126 point-to-point
!
interface atm 5/1
interface atm 5/1.1 point-to-point
interface atm 5/1.100 point-to-point
 atm pvc 100 0 100 aal5snap 0 0 0
 encapsulation pppoe
 pppoe sessions 1
!
interface atm 5/1.100.1
 encapsulation ppp
 ppp authentication chap
!
interface atm 5/1.102 multipoint
 atm pvc 1021 0 1021 aal5snap 0 0 0
 atm pvc 1022 0 1022 aal5snap 0 0 0
 atm pvc 1023 0 1023 aal5snap 0 0 0
!
interface atm 5/1.103 point-to-point
 atm pvc 103 0 103 aal5snap 0 0 0
 encapsulation bridge1483
 pppoe
!
pppoe subinterface atm 5/1.103.1
 encapsulation ppp
 ppp authentication pap
!
interface atm 5/1.104 point-to-point
 atm pvc 104 0 104 aal5snap 0 0 0
!
interface atm 5/1.125 point-to-point
!
interface fastEthernet 0/0
 ip address 10.13.5.196 255.255.128.0
!
interface mlppp joe
!
ip route 0.0.0.0 0.0.0.0 10.13.5.1
ip route 40.0.0.0 255.0.0.0 atm5/0.104
ip route 172.28.32.70 255.255.255.255 10.13.5.1
no ip source-route
!
!
ipv6
!
!
===============================================================================
virtual-router foo
…
interface null 0
interface loopback 0
 ip address 127.0.0.2 255.0.0.0
!
interface atm 5/1.100.1
 ip address 102.0.1.2 255.255.255.0
!
interface atm 5/1.102
 ip address 102.0.2.2 255.255.255.0
```

```
!
interface atm 5/1.103
 ip address 100.0.0.2 255.255.255.0
!
interface atm 5/1.103.1
 ip address 100.0.1.2 255.255.255.0
!
interface atm 5/1.104
 ip address 150.0.1.2 255.255.255.0
 ipv6 address 2000:0:17::2/60
!
ip route 30.0.0.0 255.0.0.0 atm5/1.104
no ip source-route
!
!
ipv6
```

Example 2 Format 2 output

```
service show-config format 2
…
virtual-router default
…
interface atm 5/0
interface atm 5/0.100 point-to-point
 atm pvc 100 0 100 aal5snap 0 0 0
 encapsulation pppoe
 pppoe sessions 1
!
interface atm 5/0.100.1
 encapsulation ppp
 ppp authentication chap
!
interface atm 5/0.102 multipoint
 atm pvc 1021 0 1021 aal5snap 0 0 0
 atm pvc 1022 0 1022 aal5snap 0 0 0
 atm pvc 1023 0 1023 aal5snap 0 0 0
!
interface atm 5/0.103 point-to-point
 atm pvc 103 0 103 aal5snap 0 0 0
 encapsulation bridge1483
 pppoe
!
pppoe subinterface atm 5/0.103.1
 encapsulation ppp
 ppp authentication pap
!
interface atm 5/0.104 point-to-point
 atm pvc 104 0 104 aal5snap 0 0 0
!
interface atm 5/0.126 point-to-point
!
interface atm 5/1
interface atm 5/1.1 point-to-point
interface atm 5/1.100 point-to-point
 atm pvc 100 0 100 aal5snap 0 0 0
 encapsulation pppoe
 pppoe sessions 1
!
interface atm 5/1.100.1
 encapsulation ppp
 ppp authentication chap
```

```
!
interface atm 5/1.102 multipoint
 atm pvc 1021 0 1021 aal5snap 0 0 0
 atm pvc 1022 0 1022 aal5snap 0 0 0
 atm pvc 1023 0 1023 aal5snap 0 0 0
!
interface atm 5/1.103 point-to-point
 atm pvc 103 0 103 aal5snap 0 0 0
 encapsulation bridge1483
 pppoe
!
pppoe subinterface atm 5/1.103.1
 encapsulation ppp
 ppp authentication pap
!
interface atm 5/1.104 point-to-point
 atm pvc 104 0 104 aal5snap 0 0 0
!
interface atm 5/1.125 point-to-point
!
interface fastEthernet 0/0
interface null 0
interface loopback 0
 ip address 127.0.0.1 255.0.0.0
!
interface ip shAtm50126
 ip share-interface atm 5/0.126
!
interface ip MikeShare2
 ip share-interface atm 5/1.1
!
interface mlppp joe
interface fastEthernet 0/0
 ip address 10.13.5.196 255.255.128.0
!
interface atm 5/0.100.1
 ip address 102.0.1.1 255.255.255.0
!
interface atm 5/0.102
 ip address 102.0.2.1 255.255.255.0
!
interface atm 5/0.103
 ip address 100.0.0.1 255.255.255.0
!
interface atm 5/0.103.1
 ip address 100.0.1.1 255.255.255.0
!
interface atm 5/0.104
 ip address 150.0.1.1 255.255.255.0
 ipv6 address 2000:0:17::1/60
!
ip route 0.0.0.0 0.0.0.0 10.13.5.1
ip route 40.0.0.0 255.0.0.0 atm5/0.104
ip route 172.28.32.70 255.255.255.255 10.13.5.1
no ip source-route
!
!
ipv6
!
```

```
!
================================================================================
virtual-router foo
…
interface null 0
interface loopback 0
 ip address 127.0.0.2 255.0.0.0
!
interface atm 5/1.100.1
 ip address 102.0.1.2 255.255.255.0
!
interface atm 5/1.102
 ip address 102.0.2.2 255.255.255.0
!
interface atm 5/1.103
 ip address 100.0.0.2 255.255.255.0
!
interface atm 5/1.103.1
 ip address 100.0.1.2 255.255.255.0
!
interface atm 5/1.104
 ip address 150.0.1.2 255.255.255.0
 ipv6 address 2000:0:17::2/60
!
ip route 30.0.0.0 255.0.0.0 atm5/1.104
no ip source-route
!
```

Customizing the Configuration Output

You can customize the configuration information by including or excluding lines of output based on the keywords described in this section.

Using a keyword with the **show configuration** command might be more effective than using **show configuration | begin**. When **show configuration** is used with a specific keyword, the current configuration is quickly determined and displayed for *only* that specified keyword. Executing **show configuration | begin** causes all output of **show configuration** to be generated, but the output is not displayed until the **begin** criterion is met.

Use the **virtual-router** keyword to display the current configuration of a specified virtual router. You can combine the **virtual-router** keyword with the **category** keyword to display the current configuration of specific settings for a virtual router.

Use the **interface** keyword to display the current configuration of a particular interface. Use the **type** keyword to target specific interface types. You can exclude information about particular types of interfaces using the **exclude-category interface** keyword.You can exclude information about particular types of interfaces using the **exclude-category interface** keyword.

Use the **category** keyword to display the current configuration of a specific group of router settings. The settings are organized in categories by function.

Use the **tag-group** keyword with the **category interfaces** keywords to tag interfaces as belonging to a specific group and display all interfaces within a group.

Use the **tag-group** command to configure an interface tag group. Any number of interfaces can be in a tag group. The following interface types cannot be added to tag groups: tunnel, lag, mlppp, and mlframe-relay. An interface can be in only one tag group.

Table 30 describes the categories of router settings and the type of information displayed for each category.

Table 30: Categories of Router Settings

Category	Configuration Displayed
aaa	Authentication, authorization, and accounting (AAA) settings, such as the default authentication protocol and the RADIUS accounting server
address-assignment	Address assignment settings for Dynamic Host Configuration Protocol (DHCP) and the local address server
flow-management	Flow management settings, such as firewalls, Network Address Translation (NAT), and IP flow statistics
interfaces	Physical interfaces (types and specifiers); this is the only category that displays information about interfaces
ip-protocols	Internet protocols, such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF)
link-layer-forwarding	Link-layer settings, such as bridged interfaces and link-layer interface types
management	Router management settings, such as the CLI, bulk statistics, and Telnet
physical-layer-protocols	Physical layer protocols, such as DS1, DS3, and SONET/SDH
policy	Policy settings, such as policy lists, classifier groups, and rate-limit profiles
qos	Quality of service (QoS) settings, such as traffic class, drop profile, and scheduler profile
system	System-level settings, such as timing, logging, and redundancy
tunneling	Tunneling protocols, such as IP Security (IPSec), Multiprotocol Label Switching (MPLS), and Layer Two Tunneling Protocol (L2TP)

Many of the categories described in Table 30 contain subcategories of router settings. For example, you can specify **show configuration category management cli** to display only the configuration for the CLI. To display the names of subcategories that you can specify for each category, issue the **show configuration category *categoryName* ?** command.

You can combine the **category** keyword with the **virtual-router** keyword to display the current configuration of specific settings for a virtual router.

NOTE: When you specify categories with the **show configuration** command, the output might display additional configuration data that is not explicitly associated with the categories that you specified.

service show-config

- Use to define the **show configuration** command display output.
- Specify format 1 to display the show configuration command output in its original format.
- Specify format 2 to significantly reduce the amount of time it takes to generate and display output for configurations that contain three or more virtual routers and a large number of interfaces.
- Example

  host1#**service show-config format 2**

- Use the **no** version to revert the **show configuration** command output format to its default (format 1).

show configuration

- Use to display the current configuration of the system, a specified virtual router, a specified interface, or a specified category of router settings.
- This command was formerly documented as **show config**; that abbreviation is still supported.
- You can create a configuration script from the output by saving it as a file with the .scr extension.
- This command provides configuration information based on the privilege level of the session (user). The output does not display any configuration data for commands that have privilege levels higher than that of the session. For example, if the session is enabled at level 5, issuing the **show configuration** command displays only output for commands at level 5 and below. For more information, see *CLI Command Privileges* on page 50.
- You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. See *Chapter 2, Command-Line Interface*, for details.
- Example

```
host1#show configuration
! Configuration script being generated on TUE JAN 29 200X 00:31:12 UTC! Juniper Networks Edge Routing
Switch ERX-700
! Version: x.y.z (January 18, 200X 15:01)
! Copyright (c) 1999-200X Juniper Networks, Inc. All rights reserved.

Commands displayed are limited to those available at privilege level 10

! Juniper Networks Edge Routing Switch ERX-700
boot config running-configuration
boot system erx_x-y-z.rel
no boot backup
no boot subsystem
no boot backup subsystem
no boot force-backup
!
! Note:  The following commands are here to ensure that all virtual routers and
! vrfs are created before other commands that may need to reference them.
! These commands will be repeated further on as each virtual router and vrf
! has its configuration presented.
!
virtual-router default
```

```
virtual-router boston
!
ip vrf vpna
virtual-router vrA
!
hostname host1
exception protocol ftp anonymous null
!
controller t1 6/0
 channel-group 2 timeslots 1,3-8,10 speed 64

.
.
.
!
virtual-router vrA
aaa authentication ppp default radius
aaa accounting ppp default radius
!
ip address-pool local
interface null 0
ip bgp-community new-format
no ip source-route
!
snmp-server
!
! End of generated configuration script.
```

Example using **interface** keyword:

```
host1#show configuration interface serial 4/0
interface atm 4/0
 atm vc-per-vp 1024
 atm uni-version 3.0
!
interface atm 4/0.1 point-to-point
 profile pppoe myProfile
 qos-profile myQosProfile
!
interface atm 4/0.2 point-to-point
 qos-profile myQosProfile
 ip description TestIP
!
interface atm 4/0.3 point-to-point
```

Example using **category** keyword:

```
host1#show configuration category system file-system
boot config running-configuration
boot system m.rel
no boot backup
no boot subsystem
no boot backup subsystem
```

show running-configuration

- Use to display the configuration currently running on the router, a specified virtual router, a specified interface, or a specified category of router settings.
- Example

  host1#**show running-configuration**

- Example 2

  host1#**show running-configuration interface serial 4/0**

- Example 3

  host1#**show running-configuration category system file-system**

tag-group

- Use to configure an interface tag group.
- Any number of interfaces can be in a tag group.
- Interface types tunnel, lag, mlppp, and mlframe-relay cannot be added to tag groups.
- An interface can be in only one tag group.
- Example

  host1(config-if)#**tag-group red**

- Use the **no** version to remove the tag group.

Configuring the System Automatically

You can create an autoconfiguration script that runs whenever you reset the router. The following guidelines apply:

- You must name the script autocfg.scr.
- Add the commands desired to configure the system.
- For some configuration tasks, you might need to pause the CLI for about 10 seconds by adding a **sleep** *seconds* command. The exact period must be determined empirically because it depends on your configuration and the software release version.

NOTE: The autocfg.scr script is bypassed if you arm the system to load from a script (not autocfg.scr) through the **boot config** command or **boot backup** command.

Saving the Current Configuration

By default, the system automatically saves any change to the system configuration to nonvolatile storage (NVS). This feature is known as Automatic Commit mode, but has no effect on the CLI prompt. For more information about displaying the current configuration of the system while in Automatic Commit mode, see **show configuration** on page 232.

You can disable this feature by issuing the **service manual-commit** command. In Manual Commit mode (again with no effect on the CLI prompt), any configuration change affects only the current system configuration (the running configuration). For more information about displaying the running configuration of the system while in Manual Commit mode, see **show running-configuration** on page 234.

If you are in Manual Commit mode and want to save the configuration changes to NVS, you must issue either the **write memory** command or the **copy running-configuration startup-configuration** command.

If you change the configuration while in Manual Commit mode and issue the **reload** command without saving the changes to the startup configuration, the system provides a warning, allowing you to save the changes before reloading.

You can use the **include-text-config** keyword with the **copy running-configuration** command to add the text configuration to the system configuration file. If you change from commit mode to manual-commit mode, the configuration that is available at that point in time is written into the .cnf file. A Perl script is provided in the Tools folder on the *E-series System Software* CD shipped with your router that enables you to view the text configuration in a configuration file that contains both binary and text configuration. The Perl script supports multiple platforms. The UsageExtractScrFromCnf.txt file provides an explanation of how to extract the system configuration file, using the extractScrFromCnf.pl script.

NOTE: To avoid any discrepancies between the text-generated file and the system configuration file, do not change the configuration when the **copy running-configuration** command is running.

copy running-configuration

- Use to save the current configuration to a system configuration (*.cnf) file.
- Use the **include-text-config** keyword to add the text configuration to the system configuration file.
- This command is available only if the system is in Automatic Commit mode.
- The destination filename must have a .cnf extension.
- The destination file can be either a local or a network file.
- If you want to restore a previously saved configuration, use the **boot config** *cnfFileName* command.

- Example

  host1#**copy running-configuration system2.cnf**

- There is no **no** version.

copy running-configuration startup-configuration

- Use to save all outstanding (unsaved) configuration changes to NVS.
- This command is an exact alias of the **write memory** command.
- This command is available if the system is in either Automatic Commit mode or Manual Commit mode. If issued while in Automatic Commit mode, the CLI notifies you that the command is not necessary, but allows you to proceed.
- If automatic synchronization between the primary and standby SRP modules is enabled (the default system behavior) and the system is in Manual Commit mode (the nondefault system behavior), issuing this command triggers file system synchronization immediately after the system writes, or commits, all outstanding configuration changes to NVS.
- This command is prevented during the high availability initialization state. If issued during this state, the CLI notifies you of the state and requests that you try again later.
- Example

  host1#**copy running-configuration startup-configuration**

- There is no **no** version.

copy startup-configuration

- Use to copy the previously saved startup configuration to a system configuration (*.cnf) file. If you have made but not saved any configuration changes, those changes are not in the startup configuration.
- This command is available only if the system is in Manual Commit mode.
- Example

  host1#**copy startup-configuration system1.cnf**

- There is no **no** version.

service manual-commit

- Use to stop the system from automatically saving configuration changes to NVS.
- Issuing this command places the system into Manual Commit mode. This mode has no effect on the CLI prompt.
- Issuing this command causes an immediate save of configuration data not yet committed to NVS.
- If issued when high availability is initializing, the CLI notifies you of the state and requests that you try again later.

- Example

  host1(config)#**service manual-commit**

- The **no** version returns the system to Automatic Commit mode; the **no** version has no effect if the system is already in Automatic Commit mode.

write memory

- Use to save all outstanding (unsaved) configuration changes to NVS.
- This command is an exact alias of the **copy running-configuration startup-configuration** command.
- This command is available if the router is in either Automatic Commit mode or Manual Commit mode. If issued while in Automatic Commit mode, the CLI notifies you that the command is not necessary, but allows you to proceed.
- If automatic synchronization between the primary and standby SRP modules is enabled (the default system behavior) and the system is in Manual Commit mode (the nondefault system behavior), issuing this command triggers file system synchronization immediately after the system writes, or commits, all outstanding configuration changes to NVS.
- Example

  host1#**write memory**

- There is no **no** version.

Customizing the User Interface

You can access the CLI through a console connected directly to the system or through a Telnet session. This section describes how you can customize the user interface. Some commands apply to the console, and some commands apply to vty lines that support Telnet sessions.

Setting the Console Speed

You can specify the console speed for only the current console session or for the current console session and all subsequent console sessions.

speed

- Use to set the speed for the current and all subsequent console sessions immediately.
- Example

  host1(config)#**line console 0**
  host1(config-line)#**speed 14400**

- Use the **no** version to revert to the default, 9600 bps.

terminal speed

- Use to set the speed for the current console session.
- Example

  host1#**terminal speed 14400**

- There is no **no** version.

Configuring the Display Terminal

You can specify the number of lines that appear on a terminal screen and the number of characters that appear on a line.

terminal length

- Use to set the number of lines on a screen.
- If a command generates more lines than the number configured, the output pauses after each screen.
- Set the number of lines on a screen in the range 0–512.
- Use 0 for no pausing.
- Example

  host1#**terminal length 25**

- There is no **no** version.

terminal width

- Use to set the width of the display terminal.
- Set the number of characters on a screen line in the range 30–512.
- Example

  host1#**terminal width 80**

- There is no **no** version.

Specifying the Character Set

You can specify the number of data bits per character for the current vty session and for all subsequent sessions on the specified vty lines. This feature allows you to display international characters on the terminal's screen.

data-character-bits

- Use to set the number of bits per character on the terminal's screen for all future sessions on the specified lines.
- Use the default setting, 8, to view the full set of 8-bit international characters. Be sure that the software on other devices in the network also supports international characters.
- Set the number of bits to 7 to view only characters in the standard ASCII set.

- Example

  host1(config)#**line vty 1 3**
  host1(config-line)#**data-character-bits 7**

- There is no **no** version.

terminal data-character-bits

- Use to set the number of bits per character on the terminal's screen for the current session.
- Use the default setting, 8, to view the full set of 8-bit international characters. Be sure that software on other devices in the network also supports international characters.
- Set the number of bits to 7 to view only characters in the standard ASCII set.
- Example

  host1#**terminal data-character-bits 7**

- There is no **no** version.

Configuring Login Conditions

You can issue the **dsr-detect** command to configure the system so that a data set ready (DSR) signal is required to log in to the console. If a session is in progress and the DSR signal is lost, the user is logged out automatically.

host1(config)#**line console 0**
host1(config-line)#**dsr-detect**

DSR is carried on pin 6 of the SRP module's RS-232 (DB-9) connector. The DSR input must be connected to the DSR output of a modem or the DTR output of another data terminal device, such as a terminal server, that supports this signal.

dsr-detect

- Use to require that a DSR signal be detected on the line for a user to log in to the console.
- By default, DSR is not required and DSR detection is disabled.
- Example

  host1(config-line)#**dsr-detect**

- Use the **no** version to remove the DSR requirement for login.

Setting Time Limits for User Login

You can specify a time interval that the CLI waits for a user to provide a password when logging in to the console or a vty line. To do so:

1. Access the line configuration mode using either the **console** or **vty** keyword.
2. Specify the time during which the user must enter the password. For example:

```
host1(config)#line console 0
host1(config-line)#login
host1(config-line)#timeout login response 15
```

timeout login response

- Use to set the time interval that the console or vty lines wait for the user to log in.
- If the interval passes and the user has not responded, the system closes the session or lines.
- Specify an interval in the range 0–300 seconds. A value of 0 means that there is no time limit during which the user must respond.
- The default value is 30 seconds.
- Example

  ```
  host1(config-line)#timeout login response 15
  ```

- Use the **no** version to restore the default interval, 30 seconds.

Setting Time Limits for User Input

You can specify a time interval that the CLI waits for user input on the console or vty lines. To do so:

1. Access the line configuration mode using either the **console** or **vty** keyword.
2. Specify the time during which the user must enter information. For example:

```
host1(config)#line vty 0
host1(config-line)#exec-timeout 4192 13
```

exec-timeout

- Use to set the time interval that the console or vty lines wait for expected user input.
- If the interval passes and the user has not responded, the system closes the session or lines.
- Specify a time limit in the range 0–35791 minutes, and optionally specify the number of seconds.

- By default, there is no time limit.
- Example

  host1(config-line)#**exec-timeout 4192 13**

- Use the **no** version to remove the time limit.

Configuring CLI Messages

You can configure text banners for the CLI to display to users at different times in the connection process.

banner

- Use to configure message-of-the-day (MOTD), login, or exec banner to be displayed by the CLI:
  - motd—Displays the banner when a console or vty connection is initiated.
  - login—Displays the banner before any user authentication (line or RADIUS authentication). The banner is also displayed if user authentication is not configured.
  - exec—Displays the banner after user authentication (if any) and before the first prompt of a CLI session.
- If you do not specify an option, the default behavior is to display the banner as an MOTD.
- The first character in the banner string must be repeated at the end of the string; these characters delimit the banner. The CLI prompts you if you fail to repeat the opening delimiter. All text following the second occurrence of the delimiter is ignored without warning. The delimiter is case sensitive.
- Banner text can span multiple lines. It is truncated after 1,024 characters.
- Insert **\n** where you want the banner text to split and start a new line. Alternatively, you can press Enter on the CLI when you want the text to break. In the second case, you will be prompted for the remainder of the text after you press Enter. To display a backslash as part of the message, it must be immediately preceded by another backslash, like this: \\. Do not use a backslash as a delimiter or end a line with a backslash.
- To insert a **?** character inside the text of a banner, you must enter Ctrl + v before entering the **?** character. Failure to do so may produce undesired results.
- Examples

  host1(config)#**banner motd x This is an MOTD banner x**
  host1(config)#**banner Y This is also an MOTD banner Y**
  host1(config)#**banner "Quotes make good delimiters"**
  host1(config)#**banner Xno space is required between the delimiter and the real banner textX**
  host1(config)#**banner b bad choice for a delimiter; everything after that second b was ignored b**
  host1(config)#**banner "This is one way\nto specify a multiple line banner"**
  host1(config)#**banner "This is another way to specify a**
  Enter remainder of text message. End with the character '"'.
  multiple line banner"

- Use the **default** version to restore the default setting, in which the banner is displayed on all lines.
- You can configure MOTD or exec banners, but not login banners, for the CLI to display on a per-line basis.
- Use the **no** version to remove the banner.

exec-banner

- Use to display an exec banner on a particular line after user authentication (if any) and before the first prompt of a CLI session.
- Banners on the lines are enabled by default; the **no** version does *not* reenable banners on the lines.
- See the **banner** command description for more information about configuring an exec banner.
- Example

  host1(config-line)#**exec-banner**

- Use the **default** version to restore the default setting, in which the banner is displayed on all lines.
- Use the **no** version to disable the exec banner on the line. If both the exec and MOTD banners are enabled on a line, issuing the **no exec-banner** command disables both the exec banner and the MOTD banner. The **no motd-banner** command behaves differently from the **no exec-banner** command.

motd-banner

- Use to display an MOTD banner on a particular line when a connection is initiated.
- Banners on the lines are enabled by default; the **no** version does *not* reenable banners on the lines.
- See the **banner** command description for more information about configuring an MOTD banner.
- Example

  host1(config-line)#**motd-banner**

- Use the **default** version to restore the default setting, in which the banner is displayed on all lines.
- Use the **no** version to disable the MOTD banner on the line. If both MOTD and exec banners are enabled on a line, issuing the **no motd-banner** command disables the MOTD banner and leaves the exec banner enabled. The **no motd-banner** command behaves differently from the **no exec-banner** command.

Monitoring the Console Settings

You can use the following commands to monitor console settings.

show line console 0

- Use to view the parameters configured for all future console sessions and the current console session.
- Example

```
host1#show line console 0
dsr-detect disabled
configured speed 9600, current speed 9600
exec-timeout never
```

show terminal

- Use to view parameters of the current console session.
- Field descriptions
  - Length—Number of lines on the screen
  - Width—Number of characters on each line of the screen
  - data-character-bits—Number of bits per character
    - 7—Setting for the standard ASCII set
    - 8—Setting for the international character set
  - Speed—Speed of the console session
  - dsr-detect—Status of DSR signal detection
    - enabled—DSR signal must be detected for a user to log in to the console.
    - disabled—DSR signal need not be detected for a user to log in to the console.
  - exec-timeout—Time interval that the terminal waits for expected user input
    - Never—Indicates that there is no time limit
  - exec-banner—Status for the exec banner: enabled or disabled. This banner is displayed by the CLI after user authentication (if any) and before the first prompt of a CLI session.
  - motd-banner—Status for the MOTD banner: enabled or disabled. This banner is displayed by the CLI when a connection is initiated.
  - login-timeout—Time interval during which the user must log in.
    - Never—Indicates that there is no time limit
- Example

```
host1#show terminal
Length: 25 lines, Width: 80 columns
data-character-bits: 8 bits per character
Speed: 9600 bits per second
dsr-detect disabled
exec-timeout never
exec-banner enabled
```

```
motd-banner enabled
login-timeout 30 seconds
```

Sending Messages

You can send a message to one or more terminals with the **send** command. You can specify a line number, a console number, or a vty number. You can also send the message to all terminals.

The following command sends the message “hello console” to line 0:

```
host1#send 0 “hello console”
```

The following command sends the message “hello everyone” to all terminals:

```
host1#send * “hello everyone”
```

If you begin the message on the same line as the **send** command, the first character of the message is considered to be a delimiter. You must use the same character to terminate the message. In both examples above, the delimiter was a double quotation mark (**“**).

If you press Enter without typing the second delimiter, the CLI prompts you for more message text and reminds you to complete the message with the delimiter, as shown in the following example:

```
host1#send vty4 XYou can start a message on the same line
 Enter remainder of text message.  End with the character 'X'.
and continue it on subsequent lines; the CLI prompts you for
 Enter remainder of text message.  End with the character 'X'.
more message text until you enter the second delimiterX
 Proceed with send? [confirm]
```

If you do not begin the message on the same line as the **send** command, the CLI prompts you for the message text after you press Enter. The CLI does not recognize delimiters for these messages; you must enter Ctrl + z, as shown in the following example:

```
host1#send 0
 Enter remainder of text message.  End with ^Z.
Good morning, Major Tom^Z
 Proceed with send? [confirm]
```

The receiving terminals display the message without regard to other output currently displayed on the terminal. Pagination is not affected.

The sending terminal is not affected by the state of the intended receiving terminal. For example, if the receiving terminal is flow-controlled off or at a --More-- prompt, the message is still sent, and the sending terminal is available for further commands. The receiving terminal in this case displays the message when subsequently flow-controlled on or when the user responds to the --More-- prompt.

The receiving terminal displays the message, the line number of the sender, the username of the sender if the user was authenticated through RADIUS, and the time the message was sent.

send

- Use to send a message to one or more terminals. You can specify a line number, a console number, or a vty number. You can use the ***** keyword to send the message to all terminals.
- If you begin the message on the same line as the **send** command, the first character of the message is considered to be a delimiter. You must use the same character to terminate the message.
- The CLI prompts you for message text if you do not begin or complete the message on the same line as the **send** command. The CLI reminds you to signal the end of the message either with the delimiter or Ctrl + z.
- Example

  host1#**send 0 "hello console"**

- There is no **no** version.

Managing Memory

The system performs most memory management tasks automatically. The system allocates some memory permanently and some memory temporarily. When applications are deleted, memory that the system assigned temporarily becomes available again.

The system releases available memory on an SRP module or line module automatically if that module requires extra memory for an application. However, you can force the system to release available memory on the primary SRP module if you issue either the **show processes memory** command or the **show utilization** command.

For information about the **show processes memory** command, see *Managing Files* on page 245. For information about the **show utilization** command, see *Chapter 6, Managing Modules*.

NOTE: When you issue the **show utilization** command, the system releases available memory on the SRP module immediately; however, the display appears a few seconds later.

Managing Files

You are responsible for file management. Table 31 shows the types of system files and their corresponding extensions.

Table 31: Types of System Files and Corresponding Extensions

Type of File	Extension	Description
Configuration	*.cnf	Snapshot of the system's configuration
Core dump	*.dmp	File you can create for troubleshooting if a module fails
History	*.hty (reboot.hty)	Details of when and why modules rebooted

Table 31: Types of System Files and Corresponding Extensions (continued)

Type of File	Extension	Description
Log	*.log	A series of messages that describe events that occurred on the system
Macro	*.mac	A macro program
Release	*.rel	Software releases you can install in the system
Script	*.scr	A sequence of CLI commands. When you run a script file, the system executes the commands as though they were entered at the terminal
Secure Shell (SSH) Server public key	*.pub	Host key for the SSH server
Statistics	*.sts	Bulk statistics created when you run the **bulkstats** commands
Text	*.txt	Text file

System files may reside in four locations:

- The system space
- The user space
- A network host
- The standby SRP module

The system space contains files for system operation. For example, the current software configuration is stored in the system space.

The user space is reserved for FTP server operations and has the typical directory structure of a secure FTP server. The root or top level directory is a read-only directory that contains two subdirectories:

- /incoming—Read-write directory to and from which an FTP client can send and retrieve files.
- /outgoing—Read-only directory from which an FTP client can retrieve files.

Users can transfer files through FTP to the user space from a network host and vice versa. However, users cannot access the system space through FTP. To install a file from the user space to the system space, use the **copy** command. For detailed information about transferring files between locations, see *Transferring Files* on page 254.

To conserve NVS and minimize the installation time, files are not stored in both the system space and the user space. When you issue the **copy** command to install a file from user space to system space, the E-series router establishes a link to the file, but does not make a physical copy.

Managing the User Space from a Network Host

If you enable the system's FTP server (see *Configuring the FTP Server* on page 262), you can manage files on the user space from an FTP client on a network host. Table 32 lists the FTP protocol commands that the E-series router supports. Whether you can perform these functions on the user space depends on the features that the FTP client offers.

Table 32: FTP Commands That the System Supports

FTP Command	Function
HELP	List supported commands.
USER	Verify username.
PASS	Verify password for the user.
QUIT	Quit the session.
LIST	List contents of a directory.
NLST	List directory contents using a concise format.
RETR	Retrieve a file.
STOR	Store a file.
CWD	Change working directory.
CDUP	Change working directory to parent.
TYPE	Change the data representation type.
PORT	Change the port number.
PWD, XPWD	Get the name of current working directory.
STRU	Change file structure settings (only stream mode supported).
MODE	Change file transfer mode (only stream mode supported).
PASV	Make the server listen on a port for data connection.
NOOP	Do nothing.
DELE	Delete a file.
MKD, XMKD	Make directory.
RMD, XRMD	Remove directory.
RNFR	Rename from.
RNTO	Rename to.

File Commands and FTP Servers

Commands—**copy**, **configure file**, and **macro**—that invoke a remote FTP server take place in the context of the current virtual router rather than the default virtual router. You must configure the remote FTP server so that any traffic destined for the virtual router can reach the virtual router; typically, you configure the FTP server to reach the default address of the system, which will always be able to reach the virtual router.

Renaming Files

To rename files, use the **rename** command. Table 33 shows the types of files you can rename in different locations.

rename

- Use to rename a local file.
- You can change the base name but not the extension of a file.
- Example

  host1#**rename boston1.cnf boston2.cnf**

- There is no **no** version.

Table 33: File Types You Can Rename

	Destination			
Source	System Space	User Space (Linked Files and Unlinked Files)	Network Host Within a Firewall	Standby SRP Module
System	*.cnf *.dmp *.hty *.log *.mac *.rel *.scr *.txt Nonsystem files	*.cnf *.dmp *.hty *.log *.mac *.scr *.txt	*.sts	None
User Space	*.cnf *.hty (excluding reboot.hty) *.log (excluding system.log) *.mac *.scr *.txt	*.cnf *.dmp *.hty *.log *.mac *.pub *.rel *.scr *.sts *.txt Nonsystem files	None	None
Network Host Within a Firewall	None	None	None	None
Standby SRP Module	None	None	None	None

Deleting Files

Use the **delete** command to delete files in NVS. Table 34 on page 250 shows the types of files you can delete in different locations.

delete

- Use to delete files in NVS.
- To delete a file in user space, specify the incoming or outgoing directory on the FTP server. You can specify the name of a subdirectory in the incoming or outgoing directory.
- You can include an asterisk (*) as a wildcard at any position in a specified filename. The asterisk substitutes for zero or more characters in the name. You cannot use an asterisk in a directory or subdirectory name.
- You cannot delete reboot.hty or system.log files when you use a wildcard.
- When you do not use a wildcard, the CLI deletes the file immediately without prompting you for confirmation. When you use a wildcard, the CLI prompts you for confirmation unless you also specify the **force** keyword; in that case the deletion takes place without confirmation.
- The **force** keyword causes the immediate deletion of the directory or file even when it is not empty. However, if a file in the specified directory, or a specified file, is marked by the file system as in use because it is required for the current operation or configuration, the **force** keyword cannot force the deletion.
- The **force** keyword is ignored when you attempt to delete any .dmp or .tsa file (unless the deletion is issued from a .mac or .scr file); this means that the CLI always prompts for confirmation for these file types.
- Examples

```
host1#delete test-2.txt
host1#

host1#del test*.txt
Delete disk0:test-1.txt? [confirm]        -> press n
disk0:test-1.txt: not deleted (per user request)
Delete disk0:test-2.txt? [confirm]        -> press y
disk0:test-2.dmp: Deleted
Deleted 1 file, matched 2 files

host1#del test*.txt force
disk0:test-1.txt: deleted
disk0:test-2.txt: deleted
Deleted 2 files, matched 2 files
```

```
host1#del *.dmp force
WARNING: The force option is ignored for this file type.
Delete disk0:sample-1.dmp? [confirm]          -> press n
disk0:sample-1.dmp: not deleted (per user request)
Delete disk0:sample-2.dmp? [confirm]          -> press y
disk0:sample-2.dmp: Deleted
Deleted 1 file, matched 2 files

host1#delete /outgoing/test.scr
```

- There is no **no** version.

Table 34: File Types You Can Delete

Location			
System Space	User Space (Linked Files and Unlinked Files)	Network Host Within a Firewall	Standby SRP Module
*.cnf	*.cnf	None	*.dmp
*.dmp	*.dmp		
*.hty	*.hty		
*.log	*.log		
*.mac	*.mac		
*.rel	*.pub		
*.scr	*.rel (deletes *.rel file only and not associated files)		
*.sts	*.scr		
*.txt	*.sts		
	*.txt		
	Nonsystem files		

Monitoring Files

Use the **dir** command to view files in NVS.

NOTE: When high availability is enabled on the router, it is possible that files or file attributes may appear unsynchronized when they are not. When enabled, high availability mirrors configuration changes instantly from the active SRP to the standby SRP. However, although these changes are reflected immediately in memory, the standby SRP NVS is updated at 5 minute intervals.

dir

- Use to show a list of files in NVS.
- Specify a directory path, a local filename, a local device name, or some combination of these to view any local files or directories. You canot use the **dir** command on a network device.
- You can include an asterisk (*) at any position in a specified filename as a wildcard. The asterisk substitutes for zero or more characters in the name. You cannot use a wildcard in a path.
- Bulk statistics .sts files are stored in volatile storage on a RAM disk, and are displayed only when bulkstats is configured.

NOTE: When you issue the **dir** command from Boot mode, a reduced set of file types is displayed.

- Field descriptions
  - file—Name of file or directory (DIR indicates a directory)
  - size—Physical size of file
  - unshared size—Size of file in user space
    - Value of zero indicates that this file has been installed onto the system space and that there is a link to this file.
    - Value other than zero indicates that the file has not been installed onto the system space and equals the physical size of the file.
  - date—Date that file was created
  - in use—An exclamation point (!) indicates that the system is using this file
- Example 1

```
host1#dir
Please wait.....

Active/standby file systems are synchronized.

                                                    unshared
                    file                    size      size
-------------------------------------------------  ---------  ---------
disk0:/incoming <DIR>                              0
disk0:/outgoing <DIR>                              0
disk0:810beta13.cnf                           280944     280944
disk0:800beta12.cnf                           327011     327011
disk0:bng___1.txt                              11092      11092
disk0:bng___2.txt                              11092      11092
```

```
disk0:bng___3.txt                                    11092       11092
disk0:erx701rel.cnf                                 255400      255400
disk0:730beta19.cnf                                 283141      283141
disk0:730beta18.cnf                                 284503      284503
disk0:erx_8-0-0b0-24.cnf                            327404      327404
disk0:7.3run.cnf                                    301635      301635
disk0:80beta_bce_backup.cnf                         333228      333228
disk0:800beta5.cnf                                  300575      300575
disk0:820beta5.cnf                                  311616      311616
disk0:810beta16.cnf                                 297764      297764
disk0:SRP-10Ge_3_SC_08_22_2006_07_39.dmp          153268924   153268924
disk0:SRP-10Ge_3_SC_04_12_2007_09_47.dmp          182385184   182385184
disk0:reboot.hty                                    402368      402368
disk0:system.log                                       702         702
disk0:erx_9-0-0a1-7.rel                           176128192   160912356
disk0:erx_8-1-0b1-2.rel                           164065212   148633854
disk0:erx_8-2-0b1-5.rel                           166117319   150685961
disk0:testing_cat.txt                                21848       21848
standby-disk0:SRP-10Ge_1_SC_08_21_2006_13_48.dmp  153547479   153547479
standby-disk0:SRP-10Ge_1_SC_04_12_2007_10_04.dmp  194849368   194849368
standby-disk0:reboot.hty                            123136      123136
standby-disk0:system.log                               855         855

                                                                      in
                    file                                date (UTC)    use
-------------------------------------------------   ----------------  ---
disk0:/incoming <DIR>                               02/08/2008 15:06:42
disk0:/outgoing <DIR>                               02/08/2008 15:06:42
disk0:810beta13.cnf                                 02/06/2007 15:13:44
disk0:800beta12.cnf                                 09/29/2006 16:31:54
disk0:bng___1.txt                                   02/12/2008 07:05:20
disk0:bng___2.txt                                   02/12/2008 07:05:28
disk0:bng___3.txt                                   02/12/2008 06:59:46
disk0:erx701rel.cnf                                 10/07/2005 13:01:02
disk0:730beta19.cnf                                 07/12/2006 07:21:22
disk0:730beta18.cnf                                 06/19/2006 15:23:46
disk0:erx_8-0-0b0-24.cnf                            11/02/2006 12:23:38
disk0:7.3run.cnf                                    08/21/2006 11:19:52
disk0:80beta_bce_backup.cnf                         10/04/2007 09:01:36
disk0:800beta5.cnf                                  01/02/2007 16:01:36
disk0:820beta5.cnf                                  05/09/2007 14:29:58
disk0:810beta16.cnf                                 03/15/2007 06:58:14
disk0:SRP-10Ge_3_SC_08_22_2006_07_39.dmp            08/22/2006 07:43:14
disk0:SRP-10Ge_3_SC_04_12_2007_09_47.dmp            04/12/2007 09:51:08
disk0:reboot.hty                                    01/09/2008 13:57:02
disk0:system.log                                    11/12/2007 09:56:14
disk0:erx_9-0-0a1-7.rel                             10/04/2007 08:40:06    !
disk0:erx_8-1-0b1-2.rel                             03/15/2007 06:50:32
disk0:erx_8-2-0b1-5.rel                             05/09/2007 14:22:22
disk0:testing_cat.txt                               03/13/2006 17:42:12
standby-disk0:SRP-10Ge_1_SC_08_21_2006_13_48.dmp    08/21/2006 13:51:42
standby-disk0:SRP-10Ge_1_SC_04_12_2007_10_04.dmp    04/12/2007 10:08:38
standby-disk0:reboot.hty                          01/09/2008 13:53:10
standby-disk0:system.log                            04/12/2007 09:47:24

                 Disk capacity
                 -------------
                 Capacity      Free      Reserved
    Device       (bytes)      (bytes)    (bytes)
--------------   ----------   ---------   --------
disk0:          1054900224   167372414   68157440
standby-disk0:  1054900224   153330775   68157440
```

- Example 2

```
host1#dir *.txt
Please wait.....

Active/standby file systems are synchronized.

                                                                  unshared
                     file                                  size       size
-------------------------------------------------   ---------   ---------
disk0:bng___1.txt                                        11092       11092
disk0:bng___2.txt                                        11092       11092
disk0:bng___3.txt                                        11092       11092
                                                                          in
                     file                                date (UTC)       use
-------------------------------------------------   -------------------   ---
disk0:bng___1.txt                                   02/12/2008 07:05:20
disk0:bng___2.txt                                   02/12/2008 07:05:28
disk0:bng___3.txt                                   02/12/2008 06:59:46

                 Disk capacity
                 -------------
                 Capacity      Free      Reserved
    Device       (bytes)      (bytes)    (bytes)
--------------   ----------   ---------   --------
disk0:           1054900224   167372414   68157440
standby-disk0:   1054900224   153330775   68157440
```

- Example 3

```
host1#dir /incoming
                           unshared                          in
    file          size       size         date (UTC)        use
-------------   --------   --------   -------------------   ---
disk0:3-0-0a3-7.rel        256         0    12/19/2000 07:14:01
disk0:srp.exe            30012312      0    12/19/2000 07:14:12
disk0:srpIc.exe           1801208      0    12/19/2000 07:20:32
disk0:srpDiag.exe         6984222      0    12/19/2000 07:22:08

             Disk capacity
             -------------
          Capacity      Free      Reserved
Device    (bytes)      (bytes)    (bytes)
------   ----------   ---------   --------
disk0:    220200960   120616448   36700160
```

- Example 4

```
host1#dir /outgoing
                           unshared                          in
    file          size       size         date (UTC)        use
-------------   --------   --------   -------------------   ---
disk0:test.scr            1204          0   12/18/2000 03:01:04
disk0:foo.scr             1278       1278   12/20/2000 04:02:12

             Disk capacity
             -------------
          Capacity      Free      Reserved
Device    (bytes)      (bytes)    (bytes)
------   ----------   ---------   --------
disk0:    220200960   120616448   36700160
```

- There is no **no** version.

Viewing Files

Use the **more** command to display the contents of a macro, script, or text file. The file can reside in NVS on the primary SRP module, in NVS on the redundant (standby) SRP module, or on a remote server that you access using FTP.

more

- Use to display the contents of a macro, script, or text file that resides in NVS on the primary SRP module, in NVS on the redundant SRP module, or on a remote server that you access using FTP.
- Specify the file you want to display using one of the following formats, depending on the location of the file:
  - *fileName*—Name of the file that resides in NVS on the primary SRP module
  - standby:*fileName*—Name of the file that resides in NVS on the redundant (standby) SRP module
  - *serverName*:*filePathName*—Name of the remote server on which the file resides and the complete pathname of the file
- Example 1—Displays the contents of a text file named erxconfig.txt that resides in NVS on the primary SRP module

  host1#**more erxconfig.txt**

- Example 2—Displays the contents of a macro file named mysetup.mac that resides in NVS on the redundant (standby) SRP module

  host1#**more standby:mysetup.mac**

- Example 3—Displays the contents of a script file named myconfig.scr that resides on a remote server named fileserver1

  host1#**more fileserver1:/startup/scripts/myconfig.scr**

- There is no **no** version.

Transferring Files

You may need to transfer files between the following locations:

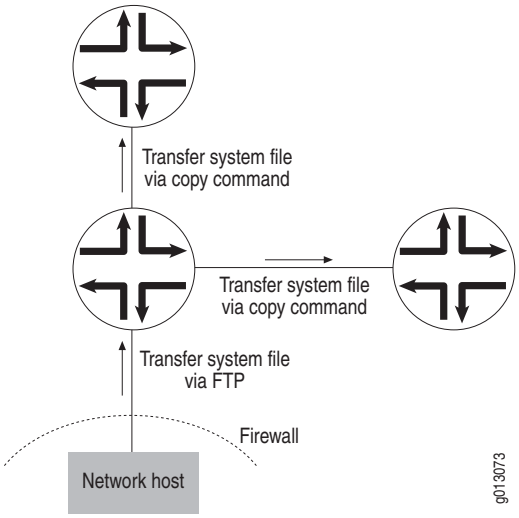
- System space
- User space
- Network host
- Standby SRP module

You can transfer files in any of three ways: the **copy** command, the system's FTP server, or a remote host that is configured as an FTP or a TFTP server. Table 35 on page 257 lists the types of files that you can transfer between the locations using the **copy** command, which activates a hidden FTP or TFTP client on the E-series router.

You can use the system's FTP server to transfer files between a network host and the user space. When a firewall separates the E-series router from the network host, you must use the FTP server to transfer files to the user space. You can then install the files from the user space to the system space by using the **copy** command. However, if there is no firewall between the E-series router and the network host, you can use the **copy** command, the remote FTP server, or the remote TFTP server to transfer files.

For example, you can transfer a file from a network host to an E-series router through FTP, and then transfer the file through the **copy** command from the E-series router to other E-series routers. See Figure 22 on page 255.

Figure 22: Transferring System Files to the E-series Router



References

For more information about file transfer protocols, consult the following resources:

- RFC 959—File Transfer Protocol (FTP) (October 1985)
- RFC 1350—Trivial File Transfer Protocol (TFTP) (Revision 2) (July 1992)

Copying and Redirecting Files

You have two options for copying or redirecting files to or from a remote FTP or TFTP server:

- Include all remote file data in the **copy** command. You can specify remote files using the URL format and the file redirect option for the related **show** commands.
- Use the **host** command to define the host and the appropriate file transfer protocol. FTP is the default if you do not specify a file transfer protocol or when Domain Name System (DNS) service is used to map IP addresses to the hostname.

If you include the remote file data, the **copy** command contains a source and destination filename, either of which (but not both) can be remote files. The following URL format is supported for both source and destination files:

protocol://[username [:password]@]location[/directory]/filename

The location can be a hostname or an IP address.

The two versions of the URL format are as follows:

ftp://[username[:password]@]location[/directory]/filename
tftp://location[/directory]/filename

NOTE: The TFTP protocol does not support username and password. Entering a username and password in the TFTP version results in a command error.

The protocol specified in the command always overrides the protocol associated with the host entry, if any, in the host table. Some protocols, such as FTP, require a username and password with each request. For the URL version of the **copy** command, the following sequence is followed:

- If the command contains a username, the username and password specified in the command are used. The password null is used if the command does not contain a password.
- If the location in the URL is a hostname with a corresponding host entry (created by the **host** command), the username and password of the host entry are used. A host entry that is created without an explicit user name is created with the default username of anonymous and password of null.

The location is the IP address or hostname of the remote file server. The directory/filename is the full path of the file relative to the user login root path.

The characters in the URL format can be encoded. Any of the delimiter characters can be used in the host, username, password, and directory and file fields when added as encoded characters. The encoded characters must be three characters, starting with a percent and followed by the two hexadecimal digits that are the ASCII equivalent. The system converts all printable characters before passing them to the protocol support. Unprintable characters (0-012F and 0x7f-0x7F) are not converted and are passed directly to the protocol. Printable characters (0x20–0x7E) are decoded and all others (0x80–0xFF) are rejected.

In the following example, the username contains the @ delimiter character encoded as %40, and the directory passed to the FTP protocol layer is /dirA/dirB/dirC. The delimiter between the hostname and directory is a forward slash (/) character. To add a slash to the start of the directory specification, add the encoded slash after the host and directory delimiter.

ftp://user%40%40name:pwd@mary/%2fdirA/dirB/dirc/fileA

In the following example, the directory passed to the FTP protocol layer is dirA/dirB/dirC.

ftp://username:pwd@mary/dirA/dirB/dirc/fileA

Using the copy Command

Table 35 shows the types of files that you can transfer between the locations by using the **copy** command.

Table 35: File Types You Can Transfer Using the copy Command

	Destination			
Source	System	User Space (Linked Files and Unlinked Files)	Network Host **Within** a Firewall	Standby SRP Module
System	*.cnf *.hty (excluding reboot.hty) *.log (excluding system.log) *.mac *.scr *.txt	*.cnf *.hty *.log *.mac *.pub *.scr *.txt	*.cnf *.dmp *.hty *.log *.mac *.pub *.scr *.sts *.txt	None
User Space	*.cnf *.mac *.rel *.scr *.txt	*.cnf *.hty *.log *.mac *.pub *.rel (*.rel file only, not files associated with the *.rel file) *.scr *.txt Nonsystem files	None	None
Network Host Within a Firewall	*.cnf *.mac *.rel *.scr *.txt	None	None	None
Standby SRP Module	system.log reboot.hty	system.log reboot.hty *.dmp	system.log reboot.hty *.dmp	None

To transfer files using the **copy** command between the system space and a network host:

1. Determine whether there is a route to the network host, and create one if necessary. See *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

2. Configure the network host as an FTP server, or use a remote host that is configured as a TFTP server.

NOTE: This command takes place in the context of the current virtual router (VR) rather than the default VR. You must configure the FTP server so that any traffic destined for the VR can reach the VR; typically, you configure the FTP server to reach the default address of the E-series router, which will always be able to reach the VR.

3. Add the FTP server to the static host table, and specify the file transport protocol (FTP or TFTP), so that the E-series router can access the network host.
4. (Optional) Specify a source interface to use in FTP packets leaving the router.
5. Copy the files.

copy

- Use to copy a file from one location to another.

NOTE: You cannot copy script (.scr) or macro (.mac) files while in Boot mode. You can copy only .cnf, .hty, and .rel files. If you issue the **dir** command from Boot mode, existing .scr and .mac files are not displayed.

- See Table 35 on page 257 for the types of files that you can copy.
- Specify a network path to copy to or from another device on the network.
- Specify the incoming or outgoing directory to copy to or from the user space.
- Specify a subdirectory name to create a subdirectory within the incoming or outgoing directory in the user space.
- You cannot use wildcards.
- You cannot create or copy over files generated by the system; however, you can copy such files to an unreserved filename.
- Examples

  host1#**copy host1:westford.cnf boston.cnf**
  host1#**copy /incoming/releases/2-8-0a3-7.rel 2-8-0a3-7.rel**
  host1#**copy /shconfig.txt ftp://joe:passwd@173.28.32.156/ftpDir /results/shConfigJoe.txt**

- There is no **no** version.

host

- Use to add or modify an entry to the host table. You can enter the optional username and password in plain text (unencrypted). Or, if you know the correct encrypted forms of the username and password, you can enter the encrypted forms (see below).
- This command supports both IPv4 and IPv6 address formats.
- This command allows network files to be accessible from a host.
- This command supports both FTP and TFTP for copying and redirecting files.

- You cannot invent an encrypted string to be used with the algorithm **8** option. You must use plain text (unencrypted) strings for the initial configuration. The only way to obtain a valid encrypted string is to enable password encryption (by issuing the **service password-encryption** command) and then examine the output of the **show configuration** command. Username and password encryption is made available primarily so that scripts generated from the **show configuration** output can be saved, used, and transferred without fear of password exposure.
- Example

  host1(config)#**host westford 10.10.8.7 ftp user25 easy53**

- To determine the encrypted values for usernames and passwords entered in cleartext, you must do the following:

  1. Issue the **service password-encryption** command. This causes subsequently issued **show configuration** commands to generate encrypted forms of the username and password for this command, as well as for all other commands that support encryption. See *Chapter 9, Passwords and Security*, for more information about the **service password-encryption** command.

  2. Issue the **show configuration** command and search for the **host** command. The encrypted forms are preceded by the number 8.

  3. You can copy and paste the command showing the encrypted forms into a macro or script to use as desired. Specify the number 8 before the username and before the password to enter an encrypted value.

- Example for encrypted values

  ```
  host1(config)#service password-encryption
  host1(config)#host test 10.2.3.4 ftp nick nick
  host1(config)#end
  host1#show config | inc host
  hostname "host1"
  host test 10.2.3.4 ftp 8 CU&I,XM(S 8 X=emZn>'S
  ```

- Use the **no** version to remove a specified host.

ip ftp source-address

- Use to specify an operational interface by IP address as the source interface for FTP packets sent by the system's FTP client.
- This command overrides a setting you configured previously with the **ip ftp source-interface** command.
- If you issue this command, the output of the **show configuration** command includes an entry of the following format:

  ip ftp source-address *ipAddress*

  This entry also appears in the output if you delete an interface or change its IP address after issuing the **ip ftp source-interface** command, in which case the IP address is the one that was configured on the interface before you issued the **ip ftp source-interface** command.

- Example

  host1(config)#**ip ftp source-address 10.10.5.21**

- Use the **no** version to restore the default, in which the source address in the FTP packets is that of the interface where the FTP connection is made.

ip ftp source-interface

- Use to specify an operational interface by interface type and location as the source interface for FTP packets sent by the system's FTP client.
- The interface you specify must have an IP address.
- This command overrides a setting you configured previously with the **ip ftp source-address** command.
- If you issue this command and the interface is valid, the output of the **show configuration** command includes an entry of the following format:

  ip ftp source-interface *interfaceType interfaceSpecifier*

  - *interfaceType*—Type of interface
  - *interfaceSpecifier*—Location of the interface

  For information about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.

- If you delete the interface or change its IP address, the output of the **show configuration** command appears as if you had entered the **ip ftp source-address** command:

  ip ftp source-address *ipAddress*

  - *ipAddress*—IP address of the interface when you issued the **ip ftp source-interface** command

- Example

  host1(config)#**ip ftp source-interface loopback1**

- Use the **no** version to restore the default, in which the source address in the FTP packets is that of the interface where the FTP connection is made.

copy Command Examples

The examples in this section assume that the following host entries have been defined in the host table:

- host mary 172.28.32.156 ftp mike mikePwd
- host joe 172.28.32.99 ftp joe jPasswd

Example 1 Copy a remote file to a local file by using the CLI file **copy** command format. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The username mike and password mikePwd from the host entry mary are used to access the remote file.

copy mary:ftpDir/scripts/autocfg.scr autocfg.scr

Example 2 Copy a local file to a remote fileby using file **copy** command format. The following command creates or replaces the remote file shConfigForJoe.txt in the directory ftpDir/results on the host joe by copying the local file shConfig.txt. The username joe and password jPasswd from the host entry joe are used to access the remote file.

```
copy shConfig.txt joe:ftpDir/results/shConfigForJoe.txt
```

Example 3 Copy a remote file to a local file by using the URL format, use the hostname to specify the location, and specify the user name and password in the command. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The username fred and the password passwd in the command are used; the username and password in the host entry are ignored.

```
copy ftp://fred:passwd@mary/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 4 Copy a remote file to a local file by using the URL format, use the hostname to specify the location, specify the user name in the command, and use the default value of the password. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The username fred from the command and the default password null are used; the username and password in the host entry are ignored.

```
copy ftp://fred@mary/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 5 Copy a remote file to a local file by using the URL format, and use the hostname to specify the location. The protocol TFTP, which does not support usernames or passwords, is the protocol in the URL. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The protocol specified in the command is used; the protocol for the host entry mary is ignored.

```
copy tftp://mary/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 6 Copy a remote file to a local file by using the URL format, use the hostname to specify the location, and use the username and password from the host entry. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The username mike and password mikePwd from the host entry are used.

```
copy ftp://mary/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 7 Copy a remote file to a local file by using the URL format. Use the host's IP address to specify the location. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host 172.28.32.156. Use the username fred to access the remote file.

```
copy ftp://fred@172.28.32.156/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 8 Copy a local file to a remote file by using the URL format, and use the host's IP address to specify the location. The following command creates or replaces the remote file shConfigJoe.txt in the directory ftpDir/results on the host 172.28.32.156 by copying the local file shConfig.txt. The username joe and the password passwd from the command are used to access the remote file.

```
copy shConifg.txt ftp://joe:passwd@172.28.32.156/ftpDir/results/shConfigJoe.txt
```

Example 9 Redirect the output of a command to a remote file by using the URL format, and use the host's IP address to specify the location. Execute **show config**, and redirect the output to the remote file shConfigJoe.txt in directory ftpDir/results on host 172.28.32.156 using username joe and password passwd.

```
show config > ftp://joe:passwd@172.28.32.156/ftpDir/results/shConfigJoe.txt
```

Using TFTP to Transfer Files

You can use TFTP to copy files and redirect output from the E-series router to a remote server if the remote host supports TFTP. Before transferring files by the remote TFTP server, you must use the **host** command to define the host and to specify TFTP as the file transfer protocol.

The maximum file size is 32 MB for file transfer. The release package for JUNOSe Release 6.1.0 and higher-numbered releases includes a split version of all release images that exceed 32 MB. Each chunk is less than 32 MB. You can therefore use TFTP with JUNOSe Release 6.1.0 and higher-numbered releases to transfer large software images. The JUNOSe software copies the split images and reassembles them to full size on the router. The file system on the router does not contain any additional images as a result of this operation.

Configuring the FTP Server

To transfer files by the system's FTP server, you must configure the FTP server and ensure that FTP client software is installed on the network host.

Although you can transfer any type of file by FTP to the E-series router, the principal aim of this feature is to allow the transfer of system files to NVS. You can transfer files by FTP to the user space. You can then install files from the user space onto the system using the **copy** command. It is not possible to access the system files directly through FTP operations.

FTP sessions on the E-series router use the vty lines. The E-series router divides its vty resources between Telnet, SSH, and FTP services. Each FTP session requires one vty line. The FTP service uses the authentication method configured for the vty lines.

Features

The system supports the following FTP features:

- Compliance with RFC 959—File Transfer Protocol (FTP) (October 1985)
- FTP passive mode

- Efficient NVS organization
- User authentication by RADIUS or password checking

FTP Passive Mode

Normally, when a client connects to an FTP server, the client establishes the control channel with the server, and the server responds by opening a data channel to the client. However, when the FTP client and server are on opposite sides of a firewall that prohibits inbound FTP connections, the server cannot open a data channel to the client.

FTP passive mode overcomes this connection limitation. In passive mode, the client opens a control channel to the server, tells the server it wants to operate in passive mode, and opens the data channel to the server. This method of establishing the FTP connection allows both the control channel and the data channel to pass through the firewall in the allowed direction.

Configuring Authentication

Before you enable the FTP server, configure the authentication procedure for the vty lines, as follows:

1. Configure host access lists.
2. Configure user authentication methods.
3. Configure the vty lines to use the host access lists and user authentication methods.

You can specify authentication by a RADIUS server or by password checking. If you choose no authentication service, any client can access the FTP server. For information about authentication on vty lines, see *Chapter 9, Passwords and Security*.

Configuration Tasks

FTP is disabled by default. You must enable the FTP server with the **ftp-server enable** command before the system allows FTP clients to connect.

ftp-server enable

- Use to enable the FTP server and to monitor the FTP port for attempts to connect to the FTP server.
- You can enable the FTP server on the default virtual router only.
- Example

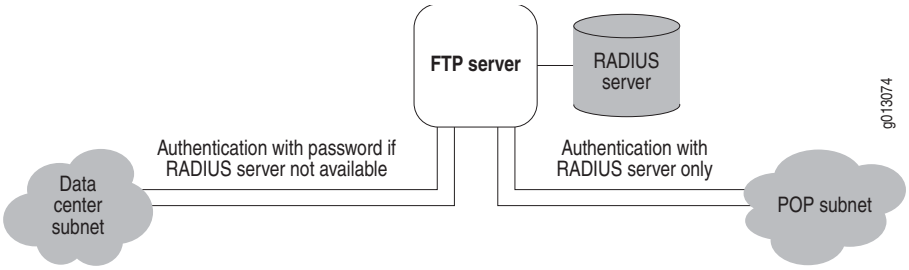
  host1(config)#**ftp-server enable**

- Use the **no** version to terminate current FTP sessions and to disable the FTP server.

Configuration Example

Figure 23 shows the scenario for this configuration example.

Figure 23: FTP Configuration Example



In this example, two FTP lines are required for administrators on the data center subnet, and two more lines are required for users on the POP subnet. The system verifies passwords of administrators on the data center subnet through either a RADIUS server or through simple line authentication if the RADIUS server is unreachable. However, the system verifies passwords of users on the POP subnet only through the RADIUS server.

The following example shows all steps for configuring this scenario, from specifying a RADIUS server to enabling the FTP line:

1. Configure the RADIUS server.

   host1(config)#**radius authentication server 10.6.131.51**
   host1(config-radius)#**key abc123**
   host1(config-radius)#**udp-port 1645**

2. Configure two access lists—one named “DataCenter,” permitting only the data center subnet, and one named “Pops,” permitting only the POP subnet.

   host1(config)#**access-list DataCenter permit 10.6.128.0 255.255.128.0**
   host1(config)#**access-list DataCenter deny any**
   host1(config)#**access-list Pops permit 199.125.128.0 255.255.128.0**
   host1(config)#**access-list Pops deny any**

3. Configure two authentication method lists, named “RadiusAndLine” and “RadiusOnly.”

   host1(config)#**aaa new-model**
   host1(config)#**aaa authentication login RadiusAndLine radius line**
   host1(config)#**aaa authentication login RadiusOnly radius**

4. Configure two FTP lines to be used by data center administrators.

   host1(config)#**line vty 0 1**
   host1(config-line)#**password foobar**
   host1(config-line)#**access-class DataCenter in**
   host1(config-line)#**login authentication RadiusAndLine**

5. Configure the remaining FTP lines to be used by POP administrators.

```
host1(config)#line vty 2 4
host1(config-line)#password foobar
host1(config-line)#access-class Pops in
host1(config-line)#login authentication RadiusOnly
```

6. Enable the FTP server.

```
host1(config)#ftp-server enable
```

Monitoring the FTP Server

Use the **dir** command to monitor files on the FTP server. Use the **show ftp-server** and **show users** commands to monitor settings of the FTP server.

show ftp-server

- Use to display information about the FTP server.
- Field descriptions
  - FTP Server state—Status of the FTP server: enabled or disabled
  - Open connections—Number of open connections to the FTP server
  - Statistics since server was last started—Data about the connection attempts since you enabled the FTP server
  - Statistics since last system reload—Data about the connection attempts since you last booted the system
    - attempts—Number of attempts to connect
    - failed hosts—Number of connection attempts that failed because of disallowed host addresses
    - failed users—Number of connection attempts that failed because users were not authenticated
- Example

```
host1#show ftp-server
FTP Server state: enabled, 0 open connections
Statistics since server was last started:
        attempts: 32
        failed hosts: 5
        failed users: 7
Statistics since last system reload:
        attempts: 35
        failed hosts: 5
        failed users: 8
```

show users

- Use to display information about users of the vty lines.
- Specify the **all** keyword to view information for all configured lines (both connected and not connected).
- Specify the **detail** keyword to view detailed information.

- Field descriptions
  - line number—Number of the line to which the user is connected
  - line name—Name of the line, the service the line offers, and the relative line number
  - user—Name of the user
  - connected from—Location or IP address of the user
  - connected since—Date and time that the user connected to the line
  - idle time—Amount of time it has been since an entry was made from this line (detail only)
  - virtual router—Virtual router used by this line user (detail only)
  - privilege level—Privilege level of this line user (detail only)
  - current command—Command currently being executed by the user over this line (detail only)
- Example 1

```
host1#show users
 line                              connected
number     line name      user       from      connected since
------   --------------   -----   ----------   ----------------
0*       console 0                 console      02/12/2001 19:57
4        vty 3 (ftp)      fred    10.10.0.64   02/12/2001 20:04
5        vty 4 (telnet)            10.10.0.64   02/12/2001 20:04

Note: '*' indicates current user.
```

- Example 2

```
host1#show users detail
 line                              connected                           idle
number     line name      user       from       connected since      time
------   --------------   ----   ------------   ----------------   --------
0        console 0                 console        08/14/2003 08:01   00:23:50
1*       vty 0 (telnet)            10.10.120.90   08/15/2003 10:37
 line    virtual   privilege
number   router      level      current command
------   -------   ---------   -----------------
0        default   10
1*       default   10          show users detail
Note: '*' indicates current user.
```

Copying Partial Releases

You can shorten the time it takes to copy a release from a server and reduce the amount of storage needed for a release. At the default setting, all subsystems are included when you copy a release from a server. Use the **exclude-subsystem** command to specify subsystems that you do not want to copy from the server. Use the **show subsystems** command to verify which files are included and excluded when you copy a release from a server.

Follow this example:

1. Determine which subsystems are included in the release on the server.

   host1#**show subsystems file m:/x/images/x-y-z.rel**

2. Exclude any subsystems in the release that you do not need for the configuration.

   host1#(config)#**exclude-subsystem coc12**
   host1#(config)#**exclude-subsystem oc12s**

3. (Optional) Remove a subsystem from the exclude list.

   host1#(config)#**no exclude-subsystem oc12s**

4. (Optional) Verify the subsystems that will be included and excluded in future release copies.

   host1#**show configuration**
   ...
   exclude-subsystem coc12

5. (Optional) After copying a release, view which subsystems were excluded.

   host1#**show subsystems file x8.rel**

6. (Optional) Determine whether the currently running software is a result of a copy with excluded subsystems. The word "Partial" indicates that subsystems were excluded.

   host1#**show version**
   Juniper Networks, Inc. Operating System Software
   Copyright (c) 200X Juniper Networks, Inc. All rights reserved.
   System Release: x-y-z.rel Partial

exclude-subsystem

- Use to exclude any subsystems that are in a release that you do not need for the system configuration.
- Example

  host1(config)#**exclude-subsystem coc12**

- The subsystems that you indicate are added to the "exclude list." All subsequent release copies will exclude the images for these subsystems from the release copy.

- Example

  host1(config)#**no exclude-subsystem coc12**

- Use the **no** version of this command *with the subsystem name* to remove a subsystem from the exclude list. Use the **no** version of this command *without a subsystem name* to remove *all* subsystems from the exclude list.

show subsystems

- Use to determine which subsystems are included in the current software release on the system or in a specified software release file.
- Specify either a local filename or a remote path and filename to view the subsystems that are included in a software release file other than the current software release on the system.
- Field descriptions
  - Required—Number of bytes of data for the required portion of the release.
  - Included Subsystems—Number of bytes of data for the included subsystems listed. All included subsystems in the release are listed.
  - Excluded Subsystems—Number of bytes of data for the excluded subsystems listed. All excluded subsystems in the release are listed.
- Use the command before you copy a release to verify which subsystems are present in the release.
- Example

```
host1#show subsystems file m:/x/images/x-y-z.rel
oc3
oc12p
oc12a
ge
fe8
coc12
oc12s
```

- Use the command after copying a release to verify which subsystems are included and excluded.
- Example

```
host1#show subsystems file x8.rel
Required: 1423005  bytes
Included Subsystems:  27882192  bytes
oc12p
oc12a
ge
fe8
coc12
oc12s

Excluded Subsystems:  6840211   bytes
oc3
```

Configuring the NFS Client

You can configure a virtual router on the E-series router as a Network File System (NFS) client to provide remote file access for E-series applications that need NFS-based transport.

The system provides NFS client support only for E-series applications designed to use NFS-based transport. Unlike the typical implementation on UNIX workstations, the E-series NFS client does not provide services such as mounting or unmounting of files through the CLI.

This section describes how to configure the NFS client if you are using an E-series application that requires NFS-based transport.

References

The NFS client complies with the following standards:

- RFC 1094—Network File System Protocol Specification (March 1989)
- RFC 1057—Remote Procedure Call Protocol Specification (June 1988)

Prerequisites

The E-series NFS client requires a remote host to act as an NFS server. The remote host must support NFS server protocol version 2 or higher.

Configuration Tasks

To configure a virtual router as an NFS client:

1. Access the virtual router context.
2. Add the remote host to the host table.
3. Configure the remote host as an NFS server for this virtual router.
4. Specify the E-series interface that this virtual router will use to exchange NFS communications with this server.

host

- Use to add or modify an entry to the host table.
- Example

  host1:boston(config)#**host host50 10.2.3.4**

- Use the **no** version to remove a specified host.

ip nfs

- Use to specify the E-series interface that the current virtual router will use to exchange messages with the NFS server.
- Specify either the **source-address** keyword with the IP address of the interface or the **source-interface** keyword with the interface type and specifier. For information about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Issuing this command provides connectivity between the E-series router and the remote host if the network configuration restricts communications between devices.
- Example

  host1:boston(config)#**ip nfs source-address 10.1.1.1**
  host1:boston(config)#**ip nfs source-interface atm 3/2.6**

- Use the **no** version to delete the name server.

ip nfs host

- Use to configure a remote host as an NFS server for the current virtual router.
- Optionally, specify a user identity and a group identity that a user must specify to connect to the remote host. The default user identity is 2001, and the default group identity is 100.
- Example

  host1:boston(config)#**ip nfs host host50 user 1500 group 150**

- Use the **no** version to disassociate this NFS server from the current virtual router.

Monitoring the NFS Client

Use the **show hosts** command (see *Monitoring the System* on page 288) to monitor information about connected NFS servers. Use the **show ip nfs** command to display information about the interface that the current virtual router uses to exchange messages with the NFS server.

show ip nfs

- Use to display information about the interface that the current virtual router uses to exchange messages with the NFS server.
- Field descriptions
  - Source address—IP address of the interface that the current virtual router uses to exchange messages with the NFS server.
  - Source interface—Type and specifier of the interface that the current virtual router uses to exchange messages with the NFS server. For information about interface types and specifiers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.
- Example

```
host1#show ip nfs
Source address is 1.1.1.1
```

Using a Loopback Interface

The loopback interface provides a stable address for protocols (for example, BGP, Telnet, or LDP) to use so that they can avoid any impact if a physical interface goes down.

The loopback interface sends packets back to the router or access server for local processing. Any packets routed from the loopback interface, but not destined to the loopback interface, are dropped.

NOTE: Do not confuse loopback with the null 0 interface. Traffic routed to null 0 is discarded on the line module.

The **no** version deletes the loopback interface.

interface loopback

- Use to access and configure the loopback interface.
- Provides a stable address to minimize impact of a physical interface going down.
- Example

  host1(config)#**interface loopback 20**
  host1(config-if)#**ip address 10.10.20.5 255.255.255.254**

- Use the **no** version to delete the loopback interface.

Using the Telnet Client

The system has an embedded Telnet client that enables you to connect to remote systems. You can configure a Telnet daemon to listen in virtual routers other than the default virtual router. You must be in the context of the desired virtual router to issue the command.

telnet

- Use to open a Telnet connection to a remote system.
- Specify the IP address or name of the remote host.
- You can specify a VRF context in which the request takes place.
- Depending on how the remote system accepts Telnet requests, you can specify a port number or port name through which the system will connect to the remote host. In the Transmission Control Protocol (TCP), ports define the ends of logical connections that carry communications. In most cases, you can accept the default, port number 23, the Telnet port. For more information about port numbers and associated processes, see www.iana.org.
- You can force Telnet to use the IP address of an interface that you specify as its source address.

- Example

  host1#**telnet 192.168.35.13 fastEthernet 0**

- There is no **no** version.

telnet listen

- Use to create a Telnet daemon to listen in a virtual router.
- Example

  host1(config)#**virtual-router 3**
  host1:3(config)#**telnet listen port 3223**

- Use the **no** version of the command to delete the daemon.

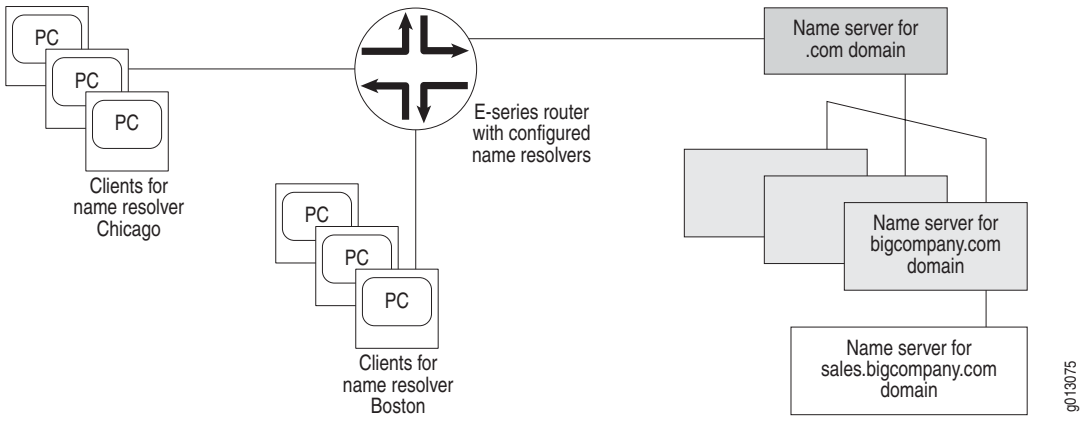
Configuring DNS

You can configure virtual routers to act as *name resolvers* for Domain Name Service (DNS). DNS is a client/server mechanism that maps IP addresses to hostnames.

The name resolver is the client side of DNS and receives address-to-hostname requests from its own clients when they want to contact hosts on other networks. By polling *name servers,* the name resolver learns name-to-address translations for the hosts its clients want to contact.

A name server may provide the translation from its cache or may poll servers lower in the DNS hierarchy to obtain a translation. Typically, name servers at the top of the hierarchy recognize top level domain names and know which servers to contact for information about more detailed domain names. See Figure 24.

Figure 24: DNS Hierarchy Example



DNS messages from a name resolver to a name server must include the domain name for the resolver's clients. Consequently, you must specify a default domain name for the clients. The default domain name is appended to unqualified hostnames (those without domain names).

The name resolver must be able to access at least one name server. Accordingly, you must configure a static route to a gateway that provides access to the name server and assign the name server to the name resolver. For more information, see *Assigning Name Servers* on page 273.

Each virtual router can have its own name resolver and domain name. However, if two virtual routers use the same name servers and belong to the same local domain, you do not need to configure name resolvers on both virtual routers. For more information, see *Using One Name Resolver for Multiple Virtual Routers* on page 274.

References

For more information about the DNS, consult the following resources:

- RFC 1035—Domain Names – Implementation and Specification (November 1987)
- RFC 2308—Negative Caching of DNS Queries (DNS NCACHE) (March 1998)

Assigning Name Servers

To assign name servers to the system:

1. Access the virtual router context.
2. Define static routes to the gateways that provide access to the name servers.
3. Enable the virtual router to query name servers.
4. Specify a default domain name for the hosts.
5. Specify the name servers.

Example

host1(config)#**virtual-router boston**
host1:boston(config)#**ip route 0.0.0.0 0.0.0.0 *gatewayIpAddress***
host1:boston(config)#**ip domain-lookup**
host1:boston(config)#**ip domain-name urlofinterest.com**
host1:boston(config)#**ip name-server 10.2.0.3**
host1:boston(config)#**ip name-server 10.2.5.5**

ip domain-lookup

- Use to enable the system to query the configured DNS name servers when it needs an IP-hostname-to-IP-address translation.
- Domain lookup is disabled by default.
- Example

  host1(config)#**ip domain-lookup**

- Use the **no** version to disable domain lookup.

ip domain-name

- Use to define a default domain name for the clients that a name resolver serves.
- You must define a default domain name for each name resolver. Multiple name resolvers can use the same default domain name.
- If you map an unqualified hostname (one without a domain name) to an IP address with the **host ftp** command, the domain name is appended to the hostname before the name is stored in the host table.
- Example

  host1(config)#**ip domain-name bigcompany.com**

- Use the **no** version to delete the domain name; that is, the domain name will no longer be appended to hostnames in the static host table.

ip name-server

- Use to specify a DNS name server that the system can query for hostname-to-IP-address resolution.
- This command supports both IPv4 and IPv6 addressing formats.
- Example

  host1(config)#**ip name-server 192.168.25.100 1:2:3:4:5:6:7:8:9:0:a:b:c:d:e:f**

- Use the **no** version to delete the name server.

Using One Name Resolver for Multiple Virtual Routers

You can use one name resolver for multiple virtual routers if those virtual routers use the same name servers and belong to the same local domain. To do so, complete the following steps:

1. Configure a name resolver for the first virtual router.
2. Access the context for the second virtual router.
3. Specify that the second virtual router should use the name resolver you configured for the first virtual router.
4. Repeat Steps 2 and 3 for other virtual routers that you want to point to this name resolver.

Example To configure the virtual router *boston* to use the same name servers as the default router, enter the following commands.

host1(config)#**virtual router boston**
host1:boston(config)#**ip domain-lookup transit-virtual-router default**

ip domain-lookup transit-virtual-router

- Use to configure a virtual router to use the name servers you configured for another virtual router.
- Example

  host1:boston(config)#**ip domain-lookup transit-virtual-router default**

- Use the **no** version to stop a virtual router from using the same name servers you configured for another virtual router.

Monitoring DNS

After you configure DNS, you can use the **show ip domain-lookup** command to view information about the name servers.

show ip domain-lookup

- Use to display the name servers that you have specified on the system with the **ip name-server** command.
- Field descriptions
  - Bind to client—Name of the virtual router context in parentheses, followed by the name of the virtual router providing the name resolver
  - Using following Domain Name Servers—Name servers you assigned
  - Using following Local Domain Names—Default domain names you specified
- Example—The virtual router *boston* uses the name resolver on the default virtual router.

```
host1#show ip domain-lookup
Bind to client: (boston)default
Using following Domain Name Servers:
10.2.0.3
11.1.1.1
10.1.1.1
1:2:3:4:5:6:7:8:9:0:a:b:c:d:e:f
Using following Local Domain Names :
urlofinterest.com
concord
```

Troubleshooting the System

You can use **log** commands to discover and isolate problems with the system. For information about using the log commands, see the *JUNOSe System Event Logging Reference Guide*. Juniper Networks Customer Service can use core dump files to troubleshoot line module and SRP module failures.

Creating Core Dump Files

You can enable the system to create a core dump file if a module fails. You can choose to send the core dump file to an FTP server or save the file to NVS. Juniper Networks Customer Service can then access the core dump file and analyze it to determine what went wrong. Local core dumps—stored in NVS—are enabled by default. You can enable the core dump from Boot mode or Global Configuration mode.

CAUTION: Create a core dump file only under the direction of Juniper Networks Customer Service. Network function can be disrupted if you create a core dump file while the system is running in a network.

On the E120 router and the E320 router, the failure of some components on a line module generates multiple core dumps to provide more complete information about system state at the time of the failure. Other E-series routers generate only a single core dump for line module failures. When you contact Juniper Networks Customer Service for assistance, send all of the generated core dump files.

Boot Mode

To enable the core dump from Boot mode:

1. Access Boot mode by reloading the SRP module; then press the mb key sequence (case insensitive) during the countdown.
2. Specify where the system should transfer the core dump file.
3. Set the IP address and mask of the system interface over which you want to send the core dump file.
4. Specify the gateway through which the system sends the core dump file to the FTP server.
5. (Optional) Set a username and password for FTP access to the server where you transferred the core dump file.
6. Reload the operating system.

Example

```
:boot##exception dump 192.168.56.7 CORE_DUMPS
:boot##exception protocol ftp user_name user_password
:boot##exception gateway 192.168.12.3
:boot##exception source 10.10.33.8 255.255.255.0
:boot##reload
```

Global Configuration Mode

To enable the core dump from Global Configuration mode:

1. Access Global Configuration mode.
2. Specify where the system should transfer the core dump file.
3. Set the IP address and mask of the system interface over which you want to send the core dump file.

4. Specify the gateway through which the system sends the core dump file to the FTP server.
5. (Optional) Set a username and password for FTP access to the server where you want to transfer the core dump file.
6. (Optional) View parameters associated with creating a core dump file.

Example

```
host1(config)#exception dump 192.168.56.7 CORE_DUMPS
host1(config)#exception protocol ftp username userpassword
host1(config)#exception gateway 192.168.12.3
host1(config)#exception source 10.10.33.8 255.255.255.0
host1(config)#reload
```

exception dump

- Use to specify where the system should transfer the core dump file.
  - To send the file to an FTP server, enter the IP address of the FTP server and the name of the directory on the server to which the system will transfer the file.
  - To send the core dump file to NVS memory, use the **local** keyword.
- Local core dumps—stored in NVS—are enabled by default.
- Example

  host1(config)#**exception dump 192.168.56.7 CORE_DUMPS**
- Use the **no** version to disable the core dump.

exception gateway

- Use to specify the gateway through which the system sends the core dump file to the FTP server.
- Example

  host1(config)#**exception gateway 10.10.1.15**
- Use the **no** version to return the value to its default (null).

exception protocol ftp

- Use to set a username and password for FTP access to the server where you transferred a core dump file. The default settings are the username anonymous and no password.
- Specify the number 8 before the username and before the password to encrypt these values. By default, the username and password are not encrypted.
- Example

  host1(config)#**exception protocol ftp 8 user_core 8 user_password**
- Use the **no** version to restore the default settings.

exception source

- Use to set the IP address and mask of the system interface over which you want to send the core dump file to the FTP server.
- You can optionally include an IP address mask.
- Example

  host1(config)#**exception source 192.168.1.33 255.255.255.0**

- Use the **no** version to return the value to its default, null.

reload

- Use to reload the software on the router immediately.
- Reloads the system software (.rel) file and the configuration (.cnf) file.
- Reloading the standby SRP causes high availability to be temporarily disabled until the standby SRP reloads and resynchronizes with the active SRP.
- Example

  host1#**reload**

- There is no **no** version.

show exception dump

- Use to display the parameters associated with the core dump operation.
- Field descriptions
  - Dump host IP address—Address of the host where the system is configured to transfer the dump file
  - Dump directory—Name of directory on the host where the system is configured to transfer the dump file
  - Dump protocol—Protocol used to send the core dump file; currently only FTP is supported
  - User name—Name configured for access to the core dump file on the FTP server
  - Password—Password configured for access to the core dump file on the FTP server
  - Interface IP address—Address of the system interface configured to send the core dump file
  - Interface netmask—Mask of the system interface configured to send the core dump file
  - Gateway IP address—Address of gateway configured between the system and the FTP server

- Example

```
host1#show exception dump
Dump host IP address: 192.168.56.7
Dump directory:CORE_DUMPS/
Dump protocol: FTP
User name: user_name
Password: user_password
Interface IP address:
Interface netmask:
Gateway IP address:
```

Managing Core Dump Files

When a core dump occurs on a redundant SRP and you have the router configured to store network core dumps, the SRP that experiences the trouble retains the management Ethernet port to perform the core dump. This prevents the standby SRP from taking over operations until the core dump is complete.

When a router uses local NVS to store a core dump, the SRP does not need the management Ethernet port. However, because of the immense size of local core dump files, using NVS to store core dumps is not practical.

The SRP-120 available on the E120 router and the SRP-320 available on the E120 and E320 routers has a second NVS card which is dedicated to storing core dump files.

The core dump monitor eliminates the impact that core dumps may have on redundant routers by allowing you to manage core dump files in NVS. The core dump monitor allows you to automatically transfer core dump files from NVS to an FTP server location for storage. The core dump monitor can also automatically delete transferred core dump files.

The core dump monitor attempts to delete transferred files when all of the following conditions have been met:

- The router attempts to write a core dump file to NVS.
- NVS contains insufficient space to hold the new core dump file.
- The core dump files have already been transferred from NVS to an FTP server location using the automatic core dump monitor transfer process.

Only those core dump files that have already been transferred from NVS are considered for deletion. Of those, the oldest files are deleted first, and the router generates a log message for each core dump file it deletes.

NOTE: If the router NVS does not contain sufficient space to hold a new core dump file even after deleting all possible core dump files, the core dump fails and the router generates a log message for this condition.

Enabling and Disabling the Core Dump Monitor

The core dump monitor is disabled by default. To enable the core dump monitor, use the **exception monitor** command. Use the **no** version of this command to disable the core dump monitor.

exception monitor

- Use to enable the router core dump monitor and specify the location to which you want the router to transfer core dump files.
- To send the file to an FTP server, enter the IP address of the FTP server and the name of the directory on the server to which the system will transfer the file.
- Enabling the core dump monitor specifies that future core dump files be saved to NVS. See the **exception dump** command for details.
- Example

  host1(config)#**exception monitor 192.168.56.7 CORE_DUMPS**

- Use the **no** version to disable the core dump monitor.

NOTE: You can use the **exception protocol ftp** command to assign a username and password to the targeted FTP server. If you choose not to define a username or password, the router uses the values of "anonymous" and "null," respectively.

Specifying the Core Dump Monitor Interval

To specify the length of time that the router waits between checking for core dump files, use the **exception monitor interval** command. Use the **no** version of this command to revert the core dump monitor interval to its default value of 60 minutes (1 hour).

exception monitor interval

- Use to specify the interval (in minutes) at which you want the router to check NVS for core dump files.
- Example

  host1(config)#**exception monitor interval 1000**

- Use the **no** version to revert the core dump monitor interval to its default value, 60 minutes.

Viewing Core Dump Monitor Status

To view information about core dump monitor status and configuration, use the **show exception monitor** command.

show exception monitor

- Use to display information about the core dump monitor status and configuration.
- Field descriptions
  - Core dump monitor—Status (enabled or disabled) of the core dump monitor
  - Next dump monitor check time—Time at which the core dump monitor will next check for any new core dump files
  - Host—IP address of the FTP host on which the core dump monitor saves core dump files

- Directory—Directory or directory path on the host to where the core dump files are located
- Core dump monitor interval—Time interval (in minutes) at which the core dump monitor checks for any new core dump files
- Files on flash which have been transferred—A list of core dump files in the router NVS that have already been transferred to the FTP host
- Files on flash which have not been transferred—A list of core dump files in the router NVS that have not yet been transferred to the FTP host

- Example

```
host1#show exception monitor
Core dump monitor is enabled
Next dump monitor check time: WED AUG 16 2003 15:50:38 UTC
Host: 10.10.120.99
Directory: monitor
Core dump monitor interval(minutes): 10

Files on flash which have been transferred
------------------------------------------
standby:OC12Atm(P2)_5_IC_ERX-10-16-5b_09_15_2002_11_59.dmp
SRP-5GPlus_1_SC_tImBo-lAb-3_09_18_2002_19_39.dmp

Files on flash which have not been transferred
----------------------------------------------
standby:SRP-10Ge_1_SC_ERX-10-24-36_09_24_2002_11_04.dmp
OC12-SERVER_5_FC1_E_ERX-10-24-36_03_28_2003_12_44.dmp
E3_1_IC_ERX-10-0f-ab_10_08_2002_16_10.dmp
```

Accessing the Core Dump File

If a module fails and saves a core dump file to NVS memory (which can take several minutes), and you have not configured the Core Dump Monitor for automatic transfer, you must transfer the file to a network host before it can be examined. You can transfer the core dump file when the module is back online or has assumed a redundant status. For information about the status of modules, see *ERX Hardware Guide, Chapter 9, Troubleshooting*. To transfer the core dump file to a network host, use the **copy** command.

In a system with two SRP modules, the following behavior applies if you have configured the SRP modules to save core dump files to an FTP server:

- If the primary SRP module fails, it saves the core dump file to the FTP server before the standby SRP module assumes control.

- If the standby SRP module fails, it must save the core dump file to NVS because it has no access to any configured network host.

The **show version** command output indicates the failed SRP module state as not responding during the save process. Consequently, when the failed SRP module recovers and assumes the role of redundant module, the **show version** command output indicates the SRP module state as standby and displays output for the standby SRP. The standby SRP can notify the primary SRP during a core dump. Output from the **show version** command displays core dumping for the Standby SRP.

If the standby SRP boot image encounters a problem loading the diagnostics or operational image, the state of the standby SRP appears as disabled (image error). When standby SRP diagnostics encounter a test failure, the primary SRP is notified and the state is set to hardware error.

You can now transfer the core dump file to a network host for examination. For example, to transfer the file *SRP_1_SC_05_24_2000_02_20.dmp* from NVS of the failed SRP module to the host server1, enter the following command:

```
host1#copy SRP_1_SC_05_24_2000_02_20.dmp
host:/public/server1/SRP-5G_1_SC_05_24_2000_02_20.dmp
```

copy

- Use to copy a core dump file.
- You cannot use wildcards.
- You can copy core dump files only to network locations.
- You cannot create or copy over files generated by the system; however, you can copy such files to an unreserved filename.
- Example

  ```
  host1#copy fault.dmp host:/public/server1/fault.dmp
  ```

- There is no **no** version.

Capturing and Writing Core Dumps

You can capture and write a core dump to a file for an active or a standby SRP module or the line modules. You can store the file on the file system or on a network host. The SRP core dump files are stored on the respective SRP flash memory. The line module core dump files are stored on the active SRP flash memory at the instance of the core dump event. The core dump files are not synchronized between the active and the standby SRP module. You can use the resulting information to help diagnose a problem or to verify whether the core settings are correct (primarily for the network settings).

write core

- Use to reboot the active SRP module, the standby SRP module, or the module in a specified slot, and write the core dump to a file.
- If you specify the **force** keyword, you are prompted for confirmation to reboot when the router is in a state that can lead to loss of configuration data or NVS corruption.

NOTE: The **force** keyword enables you to specify a slot only if that slot is an SRP module slot.

- If you do not specify a reason, Write Core is the default reason recorded in the reboot history.
- Example 1—Prompts for confirmation to reboot

  ```
  host1#write core force
  ```

- Example 2—Reboots the module in slot 7 and writes a core memory file
  host1#**write core slot 7**
- There is no **no** version.

Understanding the Core Dump File

The dump file indicates which module has failed by referencing that module's hardware slot number. The hardware slot number is the slot number designation on the systems's backplane. This slot number is different from the chassis slot number that appears on the front of the chassis and in screen displays (for example, in the display resulting if you issue the **show version** command).

Table 36 shows how the chassis slot numbers relate to the hardware slot numbers.

Table 36: Chassis Slot Numbers Versus Hardware Slot Numbers

Slot Number on Chassis	ERX-7xx Model Hardware Slot Number	ERX-14xx Model Hardware Slot Number	E320 Model Hardware Slot Number
0	1	0	16
1	2	1	17
2	3	2	18
3	4	3	19
4	5	4	20
5	6	5	21
6	7	7	8
7	8	9	10
8	–	10	9
9	–	11	12
10	–	12	13
11	–	13	25
12	–	14	26
13	–	15	27
14	–	–	28
15	–	–	29
16	–	–	30

Tracking IP Prefix Reachability

You can use the **track** command to define an IPv4 prefix object and track its reachability. The **show track** command displays the tracked information for any specified objects.

show track

- Use to display tracking details for the object you specify.
- Field descriptions
  - Track—Name of the object being tracked
  - IP Route—IP prefix being tracked
  - Virtual router—Virtual router on which the object resides
  - First-hop interface—Outgoing interface to reach the prefix
  - changes—Number of times the object has changed state
  - Tracked by—Application that is doing the tracking
- Example

```
host1(config)#show track ERX_Bangalore

Track ERX_Bangalore
 IP Route 1.1.1.0 255.255.255.0 reachability
 in virtual router 1
 Reachability is Up
 First-hop interface is FastEthernet3/0
 2 change(s)
Tracked by:
 Vrrp in virtual router 1
```

show track brief

- Use to display a one-line summary of all objects being tracked.
- Field descriptions
  - Object—Name of the object being tracked
  - Type—Type of object being tracked
  - Parameter—Parameter type being tracked
  - Value—State of the object being tracked
- Example

```
host1(config)#show track brief

Object  Type            Parameter       Value
ERX-WF  IP-route        reachability    Up
ERX-BNG IP-route        reachability    Up
```

track

- Use to create an IPv4 object and to track its reachability.
- The name of the object must be unique for the chassis.
- Use the **vrf** keyword to specify the VRF on which the IP prefix resides.

- Example

  host1(config)#**track ERX_Bangalore vrf VR1 ip-route 10.10.24.6 255.255.0.0 reachability**

- Use the **no** version to delete the object and stop tracking for that object.

Gathering Information for Customer Support

When you report a problem with your router, customer support personnel from the Juniper Networks Technical Assistance Center (JTAC) may request that you issue the **show tech-support** command. This command was created to help streamline the information-gathering process by providing a large amount of router information from one command and avoiding the need to access certain diagnostic commands.

The **show tech-support** command functions like any other show command, and you can issue this command the same way you issue any other show commands on the router. This means that you can redirect the output from the command to a file. For information about redirecting show command output, see *Redirection of show Command Output* on page 40.

Another command that customer support personnel might ask you to use is the **tech-support encoded-string** command. Customer support will provide you with an encoded string of commands that this command then executes.

tech-support encoded-string

- Use to execute an encoded command string provided by Juniper Networks customer support personnel.
- This command requires privilege level 15 access.
- Optionally, specify a slot number on the router.
- Optionally, specify a reliable or fast connection type; fast does not work under some conditions. The default connection type is reliable.
- Example 1

  host1(config)#**tech-support encoded-string debug 1**

- Example 2

  host1(config)#**tech-support slot 0 connection fast encoded-string debug1**

- There is no **no** version.

show tech-support

- Use to display technical support information used by Juniper Networks customer support personnel to assist in troubleshooting the router.
- Example

```
host1#show tech-support
Show Technical Support
------------------------------------------------------------------------------

System Name     : host1
Time            : THU JUL 15 2004 17:12:48 UTC
```

```
System up since : WED JUN 30 2004 16:07:51 UTC
Software release: 1088523900
Boot Flags      : 0x100663296
Slot Number     : 0
Serial Number   : 7100170293
Assembly Number : 3400003701
Assembly Rev    : A07
Description     :

Command List:
CLI:show version
CLI:show boot
CLI:show hardware
CLI:show redundancy
CLI:show environment
CLI:show users detail
CLI:show utilization
CLI:show process cpu
CLI:show process memory
....
```

Managing and Monitoring Resources

The resource threshold monitor (RTM) allows you to set the rising and falling thresholds and trap hold-down times for certain interfaces. You can also view the resource threshold information.

Enabling and Disabling the Resource Threshold Monitor

You may want to set thresholds for certain interface resources on the router. The RTM allows you to specify rising and falling thresholds as well as hold-down times for certain interfaces by using the **resource if-type** and **resource threshold** commands.

resource if-type

- Use to specify rising and falling thresholds and hold-down times for certain interfaces on a slot or systemwide basis.
- Example

  host1(config)#**resource if-type ip slot 4 falling 500**

- Use the **no** version to set the threshold parameter to its default value (for rising, 90 percent of the maximum value of the resource; for falling, 1 percent of the maximum value of the resource; for hold-down time, 300 seconds).

resource threshold

- Use to disable the issuance of trap messages when the router reaches preset threshold limits.
- Example

  host1(config)#**resource threshold disable traps**

- Use the **no** version to reenable traps for resource threshold conditions.

Viewing Resource Threshold Information

The RTM allows you to view information about resource use on the router. The show resource command displays statistical information about resources and their current threshold configurations.

show resource

- Use to display statistical information about resources and their current threshold configurations.
- Field descriptions
  - Resource Threshold Trap—Status (enabled or disabled) of the resource threshold trap
  - type—Interface type
  - location—Location of the interface (system or slot location)
  - max capacity—Maximum capacity of the interface at either the system or slot level
  - current value—Current capacity of the interface at either the system or slot level
  - rising threshold—Rising threshold setting for the interface at either the system or slot level
  - falling threshold—Falling threshold setting for the interface at either the system or slot level
  - hold-down time—Hold-down time setting for the interface at either the system or slot level
- Example 1

```
host1#show resource
Resource Threshold Trap: enabled
                                          max      current    rising
           type               location   capacity    value    threshold
---------------------------   --------   --------   -------   ---------
ip interface                  system        32000         1       28800
ip interface                  slot 3         8192         0        7373
ip interface                  slot 4         4095         0        3686
atm-sub-if interface          system        65536         0       58982
atm-vc interface              system        65536         0       58982
ppp-link interface            system        32768         0       29491
ppp-link interface            slot 3         2048         0        1843
ppp-link interface            slot 4            6         0           5
atm-active-sub-if interface   system        65536         0       58982
                                         falling    hold-down
           type               location   threshold     time
---------------------------   --------   ---------   ---------
ip interface                  system           320         300
ip interface                  slot 3            82         300
ip interface                  slot 4            41         300
atm-sub-if interface          system           655         300
atm-vc interface              system           655         300
ppp-link interface            system           328         300
ppp-link interface            slot 3            20         300
ppp-link interface            slot 4             0         300
atm-active-sub-if interface   system           655         300
```

- Example 2

```
host1#show resource threshold trap
Resource Threshold Trap: enabled
```

Monitoring the System

This section provides basic system commands that allow you to display information about the router's state. The **show configuration** command, for example, allows you to display the router's entire configuration.

baseline show-delta-counts

- Use to configure the system to always display statistics relative to the most recent appropriate baseline.
- The system collects many statistics during its operation. Various **show** commands are available to display these statistics. Baselining allows the user to identify a point in time relative to which such statistics can be reported.
- Typically, the optional **delta** keyword is used with **show** commands to specify that baselined statistics are to be shown. This command applies the "delta" function implicitly.
- Example

  host1#**baseline show-delta-counts**

- Use the **no** version to have access to the total statistics.

show configuration

- Use to display the current (running) configuration of the router, a specified virtual router, a specified interface, or a specified category of router settings.
- See full description and examples in **show configuration** on page 232.

show environment

- Use to display information about the router's physical environment, such as voltage or temperature.
- Optionally, specify the **all** keyword to view both the system environment information and the detailed temperature status table, or specify the **table** keyword to view only the temperature status table.
- The system displays a message if the voltage or temperature exceeds normal operating limits.
- The system enters thermal protection mode if the temperature exceeds maximum operating limits or if the fan system on the E120 router or the E320 router reports a critical error. For information about thermal protection mode on ERX-7xx models, ERX-14xx models, and the ERX-310 router, see *ERX Hardware Guide, Chapter 9, Troubleshooting*. For information about thermal protection mode on the E120 and E320 routers, see *E120 and E320 Hardware Guide, Chapter 9, Troubleshooting*.

- Field descriptions
  - chassis—Number of slots, midplane identifier, and hardware revision number
    - 14Slot—5 Gbps, 14 slot midplane
    - midplaneId7Slot—5 Gbps, 7 slot midplane
    - midplaneIdRx1400—10 Gbps ASIC compatible, 12 line module slots, 2 SRP module slots for ERX-14xx models
    - midplaneIdRx700—10 Gbps ASIC compatible, 5 line module slots, 2 SRP module slots for ERX-7xx models
    - 17 slot—100 or 320 Gbps, 17-slot midplane for the E120 router
    - 11 slot—320 Gbps, 11-slot midplane for the E120 router
  - fabric—Capacity and hardware revision of the fabric
  - fans—Status of fans
  - nvs—Status and capacity of NVS and amount of space used
  - power—States of power feeds
  - AC power—For ERX-310 routers only; states of power feeds
  - srp redundancy—Availability of a redundant SRP module
  - slots: cards missing or offline—Status of each slot
    - online
    - standby
    - offline
    - empty
  - line redundancy—Number of redundancy groups installed
    - width—Number of slots the redundant midplane covers
    - spare—Slot that contains a spare line module
    - primary—Slot that contains the primary line module
  - fabric redundancy—Status of redundancy on the switch fabric on the E120 and E320 routers
    - ok
    - none
  - temperature—Status of the system temperature
  - timing—Source of the timing signal
    - primary—Type and status of the primary timing signal
    - secondary—Type and status of the secondary timing signal
    - tertiary—Type and status of the tertiary timing signal
    - auto-upgrade—Status of the auto-upgrade parameter, which enables the system to revert to a higher-priority timing source after switching to a lower-priority timing source.

- system operational—Status of the system
- slot—Number of the slot in which the module resides
- type—Type of module in the slot on the E120 and E320 routers
- temperature—Temperature of the line module, SRP module, or SFM on the E120 and E320 routers
- processor temperature—Temperature of the line module or SRP module
- processor temperature status—Temperature condition of the line module
  - normal—Temperature is in normal range
  - too hot—Module is too hot; system will go into thermal protection mode if the temperature of any module exceeds 80° C
  - too cold—Module is too cold; system will go into thermal protection mode if the temperature of any module drops below –5° C
- IOA temperature—Temperature of the corresponding I/O module or IOA
- IOA temperature status—Temperature condition of the corresponding I/O module or IOA
  - normal—Temperature is in normal range
  - too hot—Module is too hot; system will go into thermal protection mode if the temperature of any module exceeds 80° C
  - too cold—Module is too cold; system will go into thermal protection mode if the temperature of any module drops below –5° C
- processor temperature ranges—Displays the temperature ranges for the line modules and SRP modules

- IOA temperature ranges—Displays the temperature ranges for the I/O modules on ERX-7xx models, ERX-14xx models, and the ERX-310 router or IOAs on the E120 and E320 routers
- fabric temperature ranges—Displays the temperature ranges for the SRP modules and SFMs on the E120 and E320 routers
- Example 1—Displays the environment of an ERX-7xx model

```
host1#show environment all
    chassis: 14 slot (id 0x3, rev. 0x0)
    fabric: 5 Gbps (rev. 1)
    fans: ok
    nvs: ok (81MB flash disk, 54% full)
    power: A ok, B not present
    AC power: A not present, B not present
    srp redundancy: none
*** slots: cards missing or offline
        online: 6 9
        standby: 8
        offline: 2
        empty: 0 1 3 4 5 7 10 11 12 13
    line redundancy: 1 redundancy group(s)
        width 6, spare 8, primary 9
    temperature: ok
    timing: primary
        primary: internal SC oscillator (ok)
        secondary: internal SC oscillator (ok)
```

```
        tertiary: internal SC oscillator (ok)
        auto-upgrade enabled
*** system operational: no

        processor     processor        IOA           IOA
       temperature   temperature   temperature   temperature
slot   (10C - 70C)     status      (10C - 70C)     status
----   -----------   -----------   -----------   -----------
0          31        normal            30        normal
3          31        normal            30        normal
5          31        normal            30        normal
7          31        normal            30        normal
processor temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
IOA temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
```

- Example 2—Displays the environment of an E320 router

```
host1#show environment all

    chassis: 17 slot (id 0x3, rev. 0x0)
    fabric: 100 Gbps (rev. 1)
    fans: fanSubsystemOk
    nvs: ok (977MB flash disk, 29% full), matches running config
    power: A ok, B not present
    srp redundancy: mode is file-system-synchronization       auto-sync
enabled, switch-on-error enabled
status unknown
*** slots: cards missing or offline
online: 0 6 13
offline: 7
empty: 1 2 3 4 5 11 12 14 15 16
fabric slots: ok
online: 6 7 8 9 10
line redundancy: none
temperature: ok
timing: primary
primary: internal SC oscillator (ok)
secondary: internal SC oscillator (ok)
tertiary: internal SC oscillator (ok)
auto-upgrade enabled
fabric redundancy: ok

*** system operational: no

                             temperature   temperature
slot          type           (10C - 70C)     status
----   ------------------    -----------   -----------
0      LM-4                      42        normal
0/1    GE-4 IOA                  23        normal
6      SRP-100                   32        normal
6      SFM-100                   32        normal
6/0    SRP IOA                   25        normal
7      SFM-100                   30        normal
8      SFM-100                   23        normal
9      SFM-100                   25        normal
```

```
10     SFM-100                  24        normal
13     LM-4                     24        normal
13/0   GE-4 IOA                 23        normal

fabric temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
processor temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
IOA temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
```

- Example 3—Displays the environment on an E120 router

```
host1#show environment all
    chassis: 11 slot (id 0x8, rev. 0x0)
    fabric: 120 Gbps (rev. 1)
    fans: fanSubsystemOk
    nvs: ok (998MB flash disk, 14% full), matches running config
    power: A ok, B not present
    srp redundancy: mode is file-system-synchronization        auto-sync
enabled, switch-on-error enabled
in sync
slots: ok
online: 1 2 6
standby: 7
empty: 0 3 4 5
fabric slots: ok
online: 6 7 8 9 10
line redundancy: none
temperature: ok
timing: primary
primary: internal SC oscillator (ok)
secondary: internal SC oscillator (ok)
tertiary: internal SC oscillator (ok)
auto-upgrade enabled
fabric redundancy: ok

system operational: yes

                 temperature   temperature
slot     type    (10C - 56C)     status
----   --------  -----------   -----------
1      LM-10          37        normal
1/1    GE-8 IOA       35        normal
2      LM-10          37        normal
2/1    GE-8 IOA       39        normal
6      SRP-120        40        normal
6      SFM-120        40        normal
6/0    SRP IOA        30        normal
7      SRP-120        41        normal
7      SFM-120        41        normal
8      SFM-120        31        normal
9      SFM-120        32        normal
10     SFM-120        32        normal
```

```
fabric temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 56C
processor temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 51C
IOA temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 56C
```

- Example 4—Displays the temperature status table on an E120 router

```
host1#show environment table

                  temperature   temperature
slot     type     (10C - 56C)     status
----   --------   -----------   -----------
1      LM-10          37        normal
1/1    GE-8 IOA       35        normal
2      LM-10          37        normal
2/1    GE-8 IOA       39        normal
6      SRP-120        40        normal
6      SFM-120        40        normal
6/0    SRP IOA        30        normal
7      SRP-120        41        normal
7      SFM-120        41        normal
8      SFM-120        31        normal
9      SFM-120        32        normal
10     SFM-120        32        normal

fabric temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 56C
processor temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 51C
IOA temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 56C
```

show fabric weights

- Use to display multicast-to-unicast ratio for the router switch fabric.
- Field descriptions
  - multicast—Ratio value of multicast bandwidth
  - unicast—Ratio value of unicast bandwidth
- Example

```
host1#show fabric weights

Fabric scheduler weights: multicast = 1 , unicast = 8
```

show hosts

- Use to display a list of configured network servers.
- Field descriptions
  - Static Host Table—Information about the connected static hosts
    - name—Name of the host
    - ip address—IPv4 or IPv6 address of the host
    - type of host—Type of host; for example, ftp means an FTP server
  - NFS Host Table—Information about connected NFS servers
    - name—Name of the NFS server
    - userid—Identity for the user
    - groupid—Identity for the group
- Example

```
host1#show hosts
     Static Host Table
     -----------------
name       ip address    type
----       -----------   ----
host1      10.2.0.124    ftp
hFtp       10.5.6.7      ftp
hTftp      10.5.6.7      tftp
    Static Host Table
    -----------------
name        ip address                              type
-----   ---------------------------------------     ----
george   1111:2222:3333:4444:5555:6666:7777:8888   ftp
dsw      10.10.121.42                               ftp
deab     10.6.128.12                                ftp
mFtp     10.10.121.11                               ftp
mTftp    10.10.121.11                               tftp
mary     10.10.121.11                               ftp
sd       10.10.121.80                               ftp

    NFS Host Table
    --------------
name   userid   groupid
----   ------   -------
deab    2001     100
```

show processes cpu

- Use to display the CPU use.
- Field descriptions
  - task name—Name of the process
  - times invoked—Number of times the process has been invoked
  - invocations per second—Frequency of the process invocation
  - total running time (msec)—Time the process has been running
  - percent running time—Percentage of the total running time attributable to this process
  - average time per invocation (usec)—Average number of microseconds per invocation of this process
  - 5 second utilization (%)—CPU use by the process for the last 5 seconds
  - 1 minute utilization (%)—CPU use by the process for the last minute
  - 5 minute utilization (%)—CPU use by the process for the last 5 minutes
- Example

```
host1#show processes cpu
                         Process Statistics
                         ------------------

                                                total
                                 invocations   running    percent
                         times       per        time      running
      task name         invoked     second     (msec)      time
---------------------   -------  -----------  --------   -------
aaaAtm1483Config              1            0         0        0%
aaaServer                    52            0       260        0%
agent1                      399            0      3600        0%
ar1EthHelp               362856            4       590        0%
.
.
.
templateMgr                  48            0       540        0%
timerd                  2346566           32         0        0%
~GONE~                   405202            5    184700        0%
~IDLE~                        0            0       360        0%
~INTERRUPT~             8840490          121     51050        0%

                         average
                           time         5             1             5
                           per        second        minute        minute
                        invocation  utilization   utilization   utilization
      task name           (usec)        (%)           (%)           (%)
---------------------   ----------  -----------   -----------   -----------
aaaAtm1483Config                 0            0             0             0
aaaServer                     5000            0             0             0
agent1                        9022            0             0             0
ar1EthHelp                       1            0             0             0
ar1InternalNetwork              19            0             0             0
.
.
.
~IDLE~                         ---            0             0             0
~INTERRUPT~                      5            0             0             0
```

show processes memory

- Use to display the amount of memory-related resources used by system processes. Because the router allocates memory to system processes in chunks, issuing this command performs a cleanup process to gather unused, available memory for reallocation.
- You can display different output variations by using the **application**, **slot**, and **virtual-router** keywords. In addition, you can combine these keywords in specific ways to display information combinations of application, slot, and virtual router.
- The appearance of parentheses in the output is significant. The parentheses indicate "partial accountability" of the current memory size. In other words, the values are accurate for the row in which they appear, but the memory value used for calculating the sum total for the column may be smaller than the value displayed. This can result in the sum total for the "current size" column not matching the sum of the values that appear within the column. This disparity can occur under shared memory conditions where a portion of the memory size for one or more of the virtual routers may be accounted for elsewhere, resulting in a lower column total.
- Field descriptions
  - Memory usage summary—Statistical information about the memory usage information being displayed
  - application—Name of the application being viewed (if applicable); asterisk (*) if no application is specified
  - router—Name of the virtual router being viewed (if applicable); asterisk (*) if no virtual router is specified
  - app—Application to which the statistics information applies
  - rtr—Virtual router to which the statistics information applies
  - vrf—Virtual routing and forwarding instance to which the statistics information applies
  - _unassoc_—Special virtual router output category that summarizes all memory that is not currently associated with any particular virtual router
  - current size—Amount of memory reserved by the listed application or virtual router
  - utilization—Percentage of reserved memory currently used for the listed application or router
  - headroom—Amount of memory overage available to each listed application or virtual router (if needed); 100% indicates an unlimited headroom (that is, no memory limits are set for the application or virtual router)
- Example 1

```
host1#show processes memory application

*** Memory usage summary (by application, 37 total) ***
    application: *
         router: *

              current
   app         size   utilization headroom
```

```
---------- ------- ----------- --------
aaa             98K           3%     100%
bgp             90K          28%     100%
bridge           1M           4%     100%
cli              3K           8%     100%
dcm             64K           7%     100%
dhcp           644K           0%     100%
dns              4K           6%     100%
dvmrp           36K           0%     100%
ethernet         3K          75%     100%
forwarding      20K          50%     100%
gplaan          52K           0%     100%
igmp             1K           0%     100%
.
.
```

- Example 2

```
host1#show processes memory virtual-router

*** Memory usage summary (by router, 4 total) ***
    application: *
         router: *

          current
   rtr     size   utilization headroom
--------- ------- ----------- --------
_unassoc_   (40M)           7%      99%
default    (339K)          23%     100%
test       (366K)          23%     100%
vr5        (327K)          18%     100%
--------- ------- ----------- --------
Total:        41M           7%      99%
```

- Example 3

```
host1#show processes memory virtual-router vr5 application ip

*** Memory usage summary (by VRF) ***
    application: ip
         router: vr5

    current
vrf  size   utilization headroom
--- ------- ----------- --------
vr5   (19K)          48%     100%
```

show reboot-history

- Use to display the history of system and module resets.
- You can display the current reboot.hty file or a saved reboot history file.
- If you have a redundant router, it can be convenient to copy the redundant module's reboot.hty file to another filename for viewing with this command.
- Field descriptions
  - Entry—Number of entry in the reboot history; numbers range from lowest (most recent reset) to highest (oldest reset)
  - time of reset—Timestamp for reset
  - run state—State of system at reset
  - image type—Type of image running when the record is written

        - boot—Module is running the boot file
        - diagnostics—Module is running the diagnostics file
        - application—Module is running the software file
    - location—Slot that reset; location is offset by two slots at slot 7 and above (the SRP module in slot 6 shows location as slot 7, the SRP module in slot 7 shows location as slot 9, and slots 8-13 show location as 10-15, respectively).
    - build date—Build date of software version
    - reset type—Cause of reset
- Example

```
host1#show reboot-history
*** Entry  1 ***
time of reset: TUE APR 10 2001 20:25:59 UTC
run state: unknown
image type: diagnostics
location: slot (7)
build date: 0x3abf4337 MON MAR 26 2001 13:25:11 UTC
reset type: user reboot, task "scheduler", reason "not specified"
*** Entry  2 ***
time of reset: TUE APR 10 2001 20:25:44 UTC
run state: unknown
image type: diagnostics
location: slot (8)
build date: 0x3abf5d5f MON MAR 26 2001 15:16:47 UTC
reset type: user reboot, task "scheduler", reason "not specified"
*** Entry  3 ***
time of reset: TUE APR 10 2001 20:25:03 UTC
run state: unknown
image type: diagnostics
location: slot (4)
build date: 0x3abf3ee0 MON MAR 26 2001 13:06:40 UTC
reset type: user reboot, task "scheduler", reason "not specified"
```

show running-configuration

- Use to display the configuration currently running on the router, a specified virtual router, a specified interface, or a specified category of router settings.
- See full description and examples in **show running-configuration** on page 234.

show version

- Use to display the armed and running releases for every slot in the router and the operational status of the SRP module and line modules for all E-series routers.
- Use the **all** keyword with the E120 router and the E320 router to display the operational status of the IOAs.
- Field descriptions
    - Model identification
    - Copyright—Copyright details for the system software
    - System Release—Filename, version, and date of the system software currently running on the router

- System running for—How long the router has been running (time elapsed since the last boot of the router), date and time of last boot; does not reflect the uptime of a particular SRP module
- slot—Physical slot that contains the line module
- state—Status of the line module
  - booting—Line module is booting
  - disabled (assessing)—Router is evaluating the status of this line module
  - disabled (admin)—Line module disabled by **slot disable** command
  - disabled (cfg error)—Use of the line module in this slot violates the permitted configuration for the router. For example, the fabric cannot supply sufficient bandwidth to the line module in this position.
  - disabled (image error)—Software for this line module is missing or corrupted
  - disabled (mismatch)—Line module in this slot is a different type from that specified in the software. Correct the condition by inserting the original module, or use the **slot accept** command to find information about the new module.
  - hardware error—Line module has a hardware fault
  - inactive—On ERX routers, either the I/O module is not present or the primary line module is fully booted and ready to resume operation. In the latter case, the standby is currently providing services. On E120 and E320 routers, one of the following conditions exists: the primary line module has no IOAs; or the primary line module has IOAs, but they have failed diagnostics; or the standby line module has taken over for the primary line module, and has control of the IOAs.
  - initializing—Transitional state before the line module proceeds to the online, standby, or inactive state; diagnostics are complete, module is initializing software
  - online—Line module is operating
  - not present—Line module configured for this slot is missing
  - not responding—Line module has a hardware or ROM problem
  - standby—Spare line module or SRP module is fully booted and ready to operate if the primary line module or active SRP module fails
  - unknown—Transitional state while the SRP is initializing
- type—Kind of module; an “e” at the end of an SRP module type (for example, SRP-5Ge) indicates that the module includes error checking code (ECC)
- admin—Status of the slot in the software
  - enabled—Slot is enabled
  - disabled—Slot is disabled
- spare—Line module is a spare for line module redundancy
- running release—Software that is running on the line module

- slot uptime—Length of time for which the module has been operational; a value of --- indicates that the module is not available.
- The following symbols and notices may be displayed at the end of the report:
  - # This release is a result of a subsystem override
  - * This release is a result of a "boot slot" override
  - # The running or armed release on the slot is the same as the armed release for a subsystem. A subsystem is all the line modules of one type, such as OC3.
  - * This release reflects whichever release the router is armed with at startup.

- Example 1—Displays the version of an ERX-7xx model

```
host1#show version

Juniper Edge Routing Switch ERX-700
Copyright (c) 1999-2005 Juniper Networks, Inc.  All rights reserved.
System Release: erx_7-1-0.rel Partial
        Version: 7.1.0 [BuildId 4518]   (December 21, 2005  11:23)
System running for: 25 days, 3 hours, 31 minutes, 5 seconds
        (since THU DEC 22 2005 11:36:41 UTC)

slot  state     type     admin  spare  running release    slot uptime
---- ------- ---------- ------- ----- ------------------ --------------
0    standby SRP-10Ge   enabled  ---  erx_7-1-0.rel           ---
1    online  SRP-10Ge   enabled  ---  erx_7-1-0.rel      25d03h:28m:49s
2      ---      ---       ---    ---         ---              ---
3      ---      ---       ---    ---         ---              ---
4    online  CT3-12     enabled  ---  erx_7-1-0.rel      25d03h:24m:46s
5    online  OC3-4A-APS enabled  ---  erx_7-1-0.rel      25d03h:24m:22s
6    online  GE         enabled  ---  erx_7-1-0.rel      25d03h:24m:44s
```

- Example 2—Displays the version of an E320 router

```
host1#show version
Juniper Edge Routing Switch E320
Copyright (c) 1999-2005 Juniper Networks, Inc.  All rights reserved.
System Release: 7b12.rel
        Version: 7.0.0 [BuildId 3468]   (April 29, 2005  10:46)
System running for: 2 days, 19 hours, 16 minutes, 17 seconds
        (since FRI MAY 13 2005 15:10:54 UTC)

                                    running

slot  state   type    admin  spare  release   slot uptime

---- ------- ------- ------- ----- --------- -------------
0    online  LM-4    enabled  ---  7b12.rel  2d19h:13m:24s
1      ---     ---     ---    ---     ---         ---
2    online  LM-4    enabled  ---  7b12.rel  2d19h:13m:19s
3      ---     ---     ---    ---     ---         ---
4      ---     ---     ---    ---     ---         ---
5      ---     ---     ---    ---     ---         ---
6    online  SRP-100 enabled  ---  7b12.rel  2d19h:14m:48s
6    online  SFM-100 enabled  ---     ---    2d19h:14m:47s
7    standby SRP-100 enabled  ---  7b12.rel       ---
7    online  SFM-100 enabled  ---     ---    2d19h:14m:42s
8    online  SFM-100 enabled  ---     ---    2d19h:14m:44s
```

```
9    online  SFM-10O enabled  ---     ---    2d19h:14m:39s
10   online  SFM-10O enabled  ---     ---    2d19h:14m:40s
11     ---     ---     ---    ---     ---         ---
12   online  LM-4    enabled  ---  7b12.rel  2d19h:13m:13s
13     ---     ---     ---    ---     ---         ---
14   online  LM-4    enabled  ---  7b12.rel  2d19h:13m:08s
15     ---     ---     ---    ---     ---         ---
16     ---     ---     ---    ---     ---         ---
```

- Example 3—Displays the version of an E320 router using the **all** keyword

```
host1#show version all
Juniper Edge Routing Switch E320
Copyright (c) 1999-2006 Juniper Networks, Inc.  All rights reserved.
System Release: 7-3-0.rel
        Version: 7.3.0 [BuildId 5759]   (July 27, 2006  10:40)
System running for: 3 days, 1 hour, 37 minutes, 4 seconds
        (since FRI JUL 28 2006 09:08:14 UTC)

                                                    running
slot  state         type          admin  spare    release     slot uptime
---- ------- ------------------- ------- ----- ------------- -------------
0    online  LM-4                enabled  ---    7-3-0.rel   3d01h:29m:01s
0/0  present 10GE IOA            enabled  ---                      ---
0/1    ---          ---           ---    ---       ---           ---
1    online  LM-4                enabled  ---    7-3-0b.rel  3d01h:26m:36s
1/0  present OC12/STM4-2 POS IOA enabled  ---                      ---
1/1    ---          ---           ---    ---       ---           ---
2    online  LM-10 Uplink        enabled  ---    7-3-0.rel   2d18h:27m:46s
2/0  present 10GE PR IOA         enabled  ---                      ---
2/1    ---          ---           ---    ---       ---           ---
3    online  LM-4                enabled  ---    7-3-0.rel   2d19h:03m:53s
3/0  present 10GE IOA            enabled  ---                      ---
3/1    ---          ---           ---    ---       ---           ---
4    online  LM-10 Uplink        enabled  ---    7-3-0.rel   3d01h:24m:39s
4/0  present 10GE PR IOA         enabled  ---                      ---
                                                    running
slot  state         type          admin  spare    release     slot uptime
---- ------- ------------------- ------- ----- ------------- -------------
4/1    ---          ---           ---    ---       ---           ---
5      ---          ---           ---    ---       ---           ---
5/0    ---          ---           ---    ---       ---           ---
5/1    ---          ---           ---    ---       ---           ---
6    standby SRP-320             enabled  ---    7-3-0.rel        ---
6    online  SFM-320             enabled  ---       ---      3d01h:33m:48s
7    online  SRP-320             enabled  ---    7-3-0.rel   3d01h:34m:04s
7    online  SFM-320             enabled  ---       ---      3d01h:33m:59s
7/0  present SRP IOA             enabled  ---                      ---
8    online  SFM-320             enabled  ---       ---      3d01h:34m:03s
9    online  SFM-320             enabled  ---       ---      3d01h:33m:50s
10   online  SFM-320             enabled  ---       ---      3d01h:33m:53s
11   online  LM-4                enabled  ---    7-3-0.rel   3d01h:26m:43s
11/0 present OC12/STM4-2 ATM IOA enabled  ---                      ---
11/1   ---          ---           ---    ---       ---           ---
12   online  LM-4                enabled  ---    7-3-0.rel   2d18h:26m:59s
12/0 present GE-8 IOA            enabled  ---                      ---
12/1 present GE-8 IOA            enabled  ---                      ---
13   online  LM-4                enabled  ---    7-3-0.rel   2d18h:17m:34s
13/0 present GE-4 IOA            enabled  ---                      ---
13/1   ---          ---           ---    ---       ---           ---
14   online  LM-4                enabled  ---    7-3-0.rel   3d01h:27m:06s
14/0   ---          ---           ---    ---       ---           ---
14/1 present OC12/STM4-2 POS IOA enabled  ---                      ---
```

```
15   online  LM-4                enabled  ---    7-3-0.rel   3d01h:26m:28s
15/0   ---           ---           ---    ---       ---           ---
15/1 present OC12/STM4-2 ATM IOA enabled  ---                     ---
16   online  LM-4                enabled  ---    7-3-0.rel   3d01h:25m:17s
16/0 present OC3/STM1-8 ATM IOA  enabled  ---                     ---
16/1 present OC3/STM1-8 ATM IOA  enabled  ---                     ---
```

- Example 4—Displays the version of an E120 router

```
host1#show version
Juniper Edge Routing Switch E120
Copyright (c) 1999-2007 Juniper Networks, Inc.  All rights reserved.
System Release: 8-2-0b0-9.rel
        Version: 8.2.0 beta-0.9 [BuildId 7030]   (April 2, 2007  13:04)
System running for: 1 day, 8 hours, 38 minutes, 0 seconds
        (since MON APR 09 2007 05:57:30 UTC)

                                        running
slot  state   type    admin  spare    release     slot uptime
---- ------- ------- ------- ----- ------------- -------------
0      ---     ---     ---    ---       ---           ---
1    online  LM-10   enabled  ---  8-2-0b0-9.rel 1d08h:32m:29s
2    online  LM-10   enabled  ---  8-2-0b0-9.rel 1d08h:32m:24s
3      ---     ---     ---    ---       ---           ---
4      ---     ---     ---    ---       ---           ---
5      ---     ---     ---    ---       ---           ---
6    online  SRP-120 enabled  ---  8-2-0b0-9.rel 1d08h:34m:46s
6    online  SFM-120 enabled  ---       ---      1d08h:34m:45s
7    standby SRP-120 enabled  ---  8-2-0b0-9.rel      ---
7    online  SFM-120 enabled  ---       ---      1d08h:34m:35s
8    online  SFM-120 enabled  ---       ---      1d07h:31m:04s
9    online  SFM-120 enabled  ---       ---      1d08h:34m:26s
10   online  SFM-120 enabled  ---       ---      1d08h:34m:30s
```

- Example 5—Displays the version of an E120 router using the **all** keyword

```
host1#show version all
Juniper Edge Routing Switch E120
Copyright (c) 1999-2007 Juniper Networks, Inc.  All rights reserved.
System Release: 8-2-0b0-9.rel
        Version: 8.2.0 beta-0.9 [BuildId 7030]   (April 2, 2007  13:04)
System running for: 1 day, 8 hours, 38 minutes, 6 seconds
        (since MON APR 09 2007 05:57:30 UTC)

                                          running
slot  state    type    admin  spare    release     slot uptime
---- ------- -------- ------- ----- ------------- -------------
0      ---     ---      ---    ---       ---           ---
0/0    ---     ---      ---    ---       ---           ---
0/1    ---     ---      ---    ---       ---           ---
1    online  LM-10    enabled  ---  8-2-0b0-9.rel 1d08h:32m:35s
1/0    ---     ---      ---    ---       ---           ---
1/1  present GE-8 IOA enabled  ---                     ---
2    online  LM-10    enabled  ---  8-2-0b0-9.rel 1d08h:32m:29s
2/0    ---     ---      ---    ---       ---           ---
2/1  present GE-8 IOA enabled  ---                     ---
3      ---     ---      ---    ---       ---           ---
3/0    ---     ---      ---    ---       ---           ---
3/1    ---     ---      ---    ---       ---           ---
4      ---     ---      ---    ---       ---           ---
4/0    ---     ---      ---    ---       ---           ---
4/1    ---     ---      ---    ---       ---           ---
5      ---     ---      ---    ---       ---           ---
```

```
5/0    ---     ---      ---    ---       ---           ---
5/1    ---     ---      ---    ---       ---           ---
6    online  SRP-120  enabled  ---  8-2-0b0-9.rel 1d08h:34m:51s
6    online  SFM-120  enabled  ---       ---      1d08h:34m:51s
6/0  present SRP IOA  enabled  ---                      ---
7    standby SRP-120  enabled  ---  8-2-0b0-9.rel      ---
7    online  SFM-120  enabled  ---       ---      1d08h:34m:41s
8    online  SFM-120  enabled  ---       ---      1d07h:31m:09s
9    online  SFM-120  enabled  ---       ---      1d08h:34m:32s
10   online  SFM-120  enabled  ---       ---      1d08h:34m:36s
```