ERICSSON

Managing Files

OPERATING INSTRUCTIONS

76/1543-CRA 119 1170/1-V1 Uen G

Contents

1 Directory and File Operations

This document contains information about directory and file operations, software storage, recovering file space, and performing core dump and crash file management.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **`Product Overview`** folder of this Customer Product Information library.

Note: In the following descriptions, the term controller card applies to the Cross-Connect Route Processor (XCRP4) Controller card, including the controller carrier card unless otherwise noted.

The term controller carrier card refers to the controller functions on the carrier card within the SmartEdge 100 chassis. The term I/O carrier card refers to the traffic card functions on the carrier card; these functions are compatible with the similar functions that are implemented on the traffic card that are supported on all other SmartEdge routers.

Note: In this section, the command syntax in the task table displays only the root command; for the complete command syntax, see the full description for the command in the *Command List*.

The SmartEdge router has a local file system on the internal compact-flash card (/flash) and on the mass-storage device (/md), if one is installed in the external slot. You can use them to store configuration files, along with other types of files. To monitor and administer local file storage and releases, perform one or more of the tasks described in Table 1; enter all commands in exec mode. In addition to the tasks listed in Table 1, this section also includes a procedure to recover file space: Section 3 on page 5.

Table 1 Directory and File Operations Tasks

Task	Root Command
Change the current working directory on the local file system.	*cd*

Table 1 Directory and File Operations Tasks

Task	Root Command
Copies a file from a remote file server to the SmartEdge router, from the SmartEdge router to a file server, or from one location to another on the local SmartEdge file system on either the active or standby controller card.	*copy*
Delete a file from the local file system on either the active or standby controller card.	*delete*
Display a list of the files in a directory on the local file system on either the active or standby controller card.	*directory*
Create a file, or open an existing file, on the local file system, using the vi editor.	*edit*
Create a new directory on the local file system.	*mkdir*
Display the contents of a file on the local file system, one page at a time.	*more*
Display the current working directory.	*pwd*
Rename a file or directory on the local file system.	*rename*
Remove a directory from the local file system.	*rmdir*
Save the running configuration to a file on a remote server or the local file system.	*save configuration*
Save a previously written core dump of the operating system to the mass-storage device in the /md partition.	*save seos-core*
Display the current configuration of the SmartEdge router or the contents of a previously saved configuration file on the local file system.	*show configuration*

Note:

The following guidelines apply to copy operations:

- For copy operations that require the use of a transfer protocol, such as File Transfer Protocol (FTP), Secured Copy Protocol (SCP), or Trivial File Transfer Protocol (TFTP), it is assumed that a system is configured and reachable by the SmartEdge router to service these requests.
- You cannot copy a file to the standby controller card while you are connected to the active controller card; you must be connected to the standby controller card.

2 Software Storage Organization

SmartEdge router controllers each have two internal compact-flash memory cards. The SmartEdge router stores its configuration, the operating system, and other system files on one compact-flash card. It stores the low-level software (not accessible from the command-line interface [CLI]) on the other compact-flash card.

Storage on the compact-flash card is divided into three partitions: p01, p02, and **/flash:**

- The p01 and p02 partitions are system boot partitions used to store operating system image files; one is the active partition and one is the alternate partition.

  The active partition always stores the current operating system image files; the alternate partition is either empty or stores the operating system image files from a previous release.

  The controllers in the SmartEdge router ship with the current operating system release, which consists of many files, installed in the active partition, either p01 or p02. The system is configured to automatically load the release installed on the active partition when the system is powered up.

- The /flash partition is configured as a UNIX-based local file system that stores configuration files.

- If you have an active and standby controller, the size of the compact-flash cards in the active and standby controllers need not match.

- Controllers must have at least 192 MB capacity on each compact flash card.

You can also install a 1-GB mass-storage device in the external slot of a controller card for additional storage space. The device is divided into two independent partitions, a UNIX-based file system, **/md**, and a partition to store operating system core dumps.

Note: If you install a mass-storage device in the active controller card, you must also install one in the standby controller card.

3 Recover File Space

Synchronization of system images on the active and standby controller cards usually occurs after a **reload** command (in exec mode) or power cycle. If the system cannot synchronize the controller cards, you might see an error message that the file system is out of space, which means that you must recover file space on the standby and possibly also the active controller card.

For example, if you have installed a mass-storage device in the active controller card and not in the standby controller card, the system creates a /md file system on the internal compact-flash card in the standby controller card. The presence of this /md file system means that file space in the /flash file system in the standby controller card can be exhausted while the /flash file system on the active controller card still has space available. For this reason, the configuration of the active and standby controller cards, including the presence of a mass-storage device, must be identical.

Note: The type of mass-storage device, either a Microdrive (Type II) or a compact-flash (Type I) card is transparent to all file operations; the device types installed in the active and standby controller cards need not match.

Note: For more information on data synchronization of the active and standby controller cards, see the **release sync** command in the *Command List*.

To recover file space on the standby and active controller cards when connected to the active controller card, perform the following steps:

1. List the contents of the **/flash** file system on the controller cards; enter the following commands (in exec mode):

   directory

   directory mate

   Use the **mate** keyword to specify the **/flash** file system on the standby controller.

2. Delete any unused files in the **/flash** file system on the controller cards; to delete a file, enter one of the following commands (in exec mode):

   delete[**crashfile**] **/flash**[*/directory*]*/filename.ext*[**-noconfirm**]

   delete mate[**crashfile**] **/flash**[*/directory*]*/filename.ext* [**-noconfirm**]

3. If you have installed a mass-storage device in the active controller card and not in the standby controller card, list the contents of the **/md** file system on

the standby controller card; enter the following command (in exec mode): **`directory mate /md`**.

4. Delete old and unused files from the **/md** file system on the standby controller card; enter the following command in exec mode:

   `delete mate/md` [**`crashfile`**] [***`/directory`***]***`/filename.ext`*** [**`-noconfirm`**]

5. Force a synchronization of the controller cards; enter one of the following commands (in exec mode):

   `reload standby`

   The system attempts to synchronize the standby controller with the active controller card.

4 Configuring SFTP to Extract Files

You can extract files from the SmartEdge router using an SFTP client connection from an external router.

To configure an SFTP server on SmartEdge router so that an external SFTP client can connect and extract files, do the following:

1. Enter the following syntax to configure service to an SFTP server:

```
[local]Redback#config
Enter configuration commands, one per line, 'end' to exit
[local]Redback(config)#context local
[local]Redback(config-ctx)#service sftp server
```

2. Enable SFTP privileges for a user ID. The following example shows how to enable SFTP privileges for user name **test** with initial privilege level **15**:

```
[local]Redback#config
Enter configuration commands, one per line, 'end' to exit
[local]Redback(config)#context local
[local]Redback(config-ctx)#administrator test
[local]Redback(config-administrator)#privilege start 15
[local]Redback(config-administrator)#
```

3. Save the configuration.

4. Connect to an external router using SFTP, and then login as **test/test** (user name/password).

5 Performing Core Dump and Crash File Management Tasks

If a system malfunction occurs, the operating system can generate one of the following types of core dumps:

- Application (process) core dump caused by process error

  A core dump is usually generated by the operating system as the result of a process internal error. The crash filename is ***proc-name_proc-id***.core, and it is stored in the **/md** directory in the root file system on the internal compact-flash card, or, if a mass-storage device is installed, in the **/md** directory on the device.

  Because the resulting crash file can be very large (50 to 100 MB), a file containing only the most pertinent information is also created (approximately 10 KB) and stored in the **/md** directory in the **/flash** file system on the internal compact-flash card in the active controller card. This crash file is also referred to as a mini core dump; the file name is ***proc-name_proc-id*.mini.core.**

- Packet Processing ASIC (PPA) core dump

  This core dump is generated automatically by the operating system as the result of a major error in the PPA. The crash file name is crashSlot***nnComponent***.gz and it is stored in a directory on the internal compact-flash card for the low-level software until the system uploads it to a remote FTP server or moves it to the **/md** directory.

- Operating system core dump

  This core dump is generated automatically by the operating system as the result of an illegal operation. The core dump is stored in the partition for operating system core dumps on the mass-storage device installed in the active controller card.

  If the operating system kills a faulty process, the system generates core dump and core dump.mini files for the killed process as well as core dump and core dump.mini files for the operating system process that killed it. For example, if the process monitor (PM) process kills a process that has no heartbeat, core dump and core dump.mini files are generated for both the killed process and the PM process.

- Operator-initiated core dump

  You can initiate a core dump using the **process coredump** command (in exec mode). Note the following cautions regarding the generation of core dumps:

Caution!

Risk of data loss. Generating a core dump interrupts the specified process for a brief period, the length of which depends on the size of the binary and the amount of memory used by the process, before the process is automatically restarted by the system. To reduce the risk, do not initiate a core dump while the system is experiencing heavy traffic.

Caution!

Risk of system crash. Allow sufficient time after entering the **`process coredump`** command to allow the SmartEdge router to stabilize. Monitor the SmartEdge router and wait for it to stabilize before entering the **`process restart`** command. Contact technical support before you start and restart multiple processes.

Caution!

Risk of data loss. Because of its size, an operating system core dump cannot be generated if a mass-storage device is not installed.

To create crash files from the core dump you must use the **`save seos-core`** command (in exec mode). Two crash files are created by this command and stored in the /md partition on the same mass-storage device on which the original core dump was stored. File names are netbsd.0.core.gz and netbsd.0.gz.

Crash files can be automatically uploaded to a remote server that is accessed by the FTP if the system has been configured using the **`service upload-coredump`** command (in global configuration mode). For information about this command, see .

Note: We strongly recommend that you upload crash files automatically to a remote FTP server. By configuring this service, you maximize the use of available disk space and improve system stability and performance.

You can display a list of crash files stored on the system using the **`show crashfiles`** command (in any mode).

Note: Crash files provide useful troubleshooting information to technical support and are not intended, nor supported, for general use outside of support employees.

Table 2 lists the tasks to manage core dumps and crash files. Enter **`show`** commands in any mode; enter all other commands in exec mode.

Table 2 Core Dump Management Tasks

Task	Root Command
Delete a file from the local file system on either the active or standby controller card.	*delete*
Initiate a core dump for the specified process and save it in a crash file.	*process coredump*
Display the size, location, and name of any crash files stored on the system.	*show crashfiles*
Upload crash files automatically to a remote FTP server.	*service upload-coredump*
Save a previously written core dump of the operating system to two crash files in the mass-storage device /md directory.	*save seos-core*